Managing Across the Lifecycle Best Practices

The Art of Service
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 workbook’s primary purpose is to complement the accredited ITIL® Managing Across the Lifecycle program provided by The Art of Service or one of our accredited partners.

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
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FOREWORD</strong></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>1</strong></td>
<td>INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>IT SERVICE MANAGEMENT</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>THE FOUR PERSPECTIVES (ATTRIBUTES) OF ITSM</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>BENEFITS OF ITSM</td>
<td>9</td>
</tr>
<tr>
<td>2.3</td>
<td>BUSINESS AND IT ALIGNMENT</td>
<td>10</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>WHAT IS ITIL®?</td>
<td>13</td>
</tr>
<tr>
<td>3.1</td>
<td>THE SERVICE LIFECYCLE</td>
<td>14</td>
</tr>
<tr>
<td>3.2</td>
<td>MAPPING THE CONCEPTS OF ITIL® TO THE SERVICE LIFECYCLE</td>
<td>16</td>
</tr>
<tr>
<td>3.3</td>
<td>HOW DOES THE SERVICE LIFECYCLE WORK?</td>
<td>18</td>
</tr>
<tr>
<td>3.4</td>
<td>SPECIALIZATION &amp; COORDINATION ACROSS THE SERVICE LIFECYCLE</td>
<td>19</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>COMMON TERMINOLOGY</td>
<td>21</td>
</tr>
<tr>
<td>4.1</td>
<td>WHAT ARE SERVICES?</td>
<td>22</td>
</tr>
<tr>
<td>4.2</td>
<td>PROCESSES &amp; FUNCTIONS</td>
<td>29</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>PRINCIPLES OF SERVICE MANAGEMENT</td>
<td>35</td>
</tr>
<tr>
<td>5.1</td>
<td>BUSINESS UNITS AND SERVICE UNITS</td>
<td>35</td>
</tr>
<tr>
<td>5.2</td>
<td>TYPES OF SERVICE PROVIDERS</td>
<td>36</td>
</tr>
<tr>
<td>5.3</td>
<td>AGENTS</td>
<td>37</td>
</tr>
<tr>
<td>5.4</td>
<td>ENCAPSULATION</td>
<td>38</td>
</tr>
<tr>
<td>5.5</td>
<td>MONITORING AND CONTROL OF IT SERVICE MANAGEMENT</td>
<td>39</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>SERVICE STRATEGY</td>
<td>42</td>
</tr>
<tr>
<td>6.1</td>
<td>OBJECTIVES OF SERVICE STRATEGY</td>
<td>42</td>
</tr>
<tr>
<td>6.2</td>
<td>BENEFITS OF SERVICE STRATEGY</td>
<td>43</td>
</tr>
<tr>
<td>6.3</td>
<td>SERVICE STRATEGY INTERFACES WITH OTHER SERVICE LIFECYCLE PHASES</td>
<td>44</td>
</tr>
<tr>
<td>6.4</td>
<td>MAJOR CONCEPTS OF SERVICE STRATEGY</td>
<td>45</td>
</tr>
<tr>
<td>6.5</td>
<td>SERVICE PORTFOLIO MANAGEMENT</td>
<td>52</td>
</tr>
<tr>
<td>6.6</td>
<td>FINANCIAL MANAGEMENT</td>
<td>65</td>
</tr>
<tr>
<td>6.7</td>
<td>DEMAND MANAGEMENT</td>
<td>77</td>
</tr>
<tr>
<td>6.8</td>
<td>CHALLENGES, CRITICAL SUCCESS FACTORS AND RISKS OF SERVICE MANAGEMENT</td>
<td>83</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>SERVICE DESIGN</td>
<td>89</td>
</tr>
<tr>
<td>7.1</td>
<td>OBJECTIVES OF SERVICE DESIGN</td>
<td>89</td>
</tr>
<tr>
<td>7.2</td>
<td>BENEFITS OF SERVICE DESIGN</td>
<td>90</td>
</tr>
<tr>
<td>7.3</td>
<td>FIVE MAJOR ASPECTS OF SERVICE DESIGN</td>
<td>91</td>
</tr>
<tr>
<td>7.4</td>
<td>SERVICE DESIGN INTERFACES WITH OTHER SERVICE LIFECYCLE PHASES</td>
<td>93</td>
</tr>
<tr>
<td>7.5</td>
<td>SERVICE LEVEL MANAGEMENT</td>
<td>96</td>
</tr>
<tr>
<td>7.6</td>
<td>SERVICE CATALOGUE MANAGEMENT</td>
<td>108</td>
</tr>
<tr>
<td>7.7</td>
<td>SUPPLIER MANAGEMENT</td>
<td>116</td>
</tr>
<tr>
<td>7.8</td>
<td>AVAILABILITY MANAGEMENT</td>
<td>125</td>
</tr>
<tr>
<td>7.9</td>
<td>CAPACITY MANAGEMENT</td>
<td>146</td>
</tr>
<tr>
<td>7.10</td>
<td>IT SERVICE CONTINUITY MANAGEMENT</td>
<td>155</td>
</tr>
<tr>
<td>7.11</td>
<td>INFORMATION SECURITY MANAGEMENT</td>
<td>166</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>SERVICE TRANSITION</td>
<td>172</td>
</tr>
<tr>
<td>8.1</td>
<td>OBJECTIVES OF SERVICE TRANSITION</td>
<td>172</td>
</tr>
<tr>
<td>8.2</td>
<td>BENEFITS OF SERVICE TRANSITION</td>
<td>173</td>
</tr>
<tr>
<td>8.3</td>
<td>INTERFACES TO OTHER SERVICE LIFECYCLE PHASES</td>
<td>174</td>
</tr>
<tr>
<td>8.4</td>
<td>TRANSITION PLANNING AND SUPPORT</td>
<td>176</td>
</tr>
<tr>
<td>8.5</td>
<td>CHANGE MANAGEMENT</td>
<td>179</td>
</tr>
</tbody>
</table>
1 Introduction

The journey for any service management initiative is a challenging and complex one, so how do we steer an optimum path towards results that actually provide the strategic, tactical and operational benefits that are desired? Even when we are relatively successful in gaining executive and senior management commitment, facilitating organizational change and coordinating the large amounts of resources required things can still go horribly wrong. The ‘real world’ gets in the way of course, with operational issues and day-to-day management of the business taking priority over any proposed improvements to service management. The IT department itself is crippled by many different and often conflicting priorities and opinions. There may also be indecision regarding the correct sequence of plans and actions relevant to our organization.

These are just a few of the challenges and questions facing any service management professional, where even a solid understanding of the individual ITIL® processes won’t be enough to ensure success. The real skills and knowledge that are valuable for a service manager in these scenarios however are an understanding of how the business and IT operates, an ability to identify areas of weaknesses or potential threats, along with the skills to develop and execute appropriate plans to improve any aspect of IT service management, including:

- The formalization and utilization of ITIL processes;
- IT services;
- IT staff, customer and user understanding and awareness;
- Supporting tools and technology; and
- IT governance.

In this light, the main objectives for the Managing Across the Lifecycle program are to provide individuals with knowledge and skills in the following key areas:

- Lifecycle positioning and transition;
- Relationships between business and IT, and customer liaison;
- The challenges of value creation;
- Business benefits of IT service management;
- Planning and defining scope;
- Risk management;
- Plan, Do, Check, Act methodology;
- Measuring, monitoring & reporting; and
- Complimentary Guidance and Tool Strategies.
Readers should note that this workbook includes many sections on the surrounding or supporting topics that are not the focus of the exam or program itself.
2 IT Service Management

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; and
- 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: it’s 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.
2.1 The Four Perspectives (Attributes) of ITSM

There are four perspectives (“4P’s”) 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 of ITSM. This includes 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 and software, budgets, tools.

- **Process Perspective:**
  Relates the end-to-end delivery of service-based on-process flows.

Quality IT Service Management ensures that each of these four perspectives are taken into account as part of the continual improvement of the IT organization. These same perspectives need to be considered and catered for when designing new or modified services to succeed in the design, transition and eventual adoption by customers.
2.2 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 knowing their roles and their responsibilities in service provision;
- Learning from previous experience; and
- Demonstrable performance indicators.

In particular reference to the scope of Service Offerings & Agreements, such benefits include:

- Improved capability for supporting business growth and change;
- Improved efficiency of business and IT staff though quality information and knowledge being made available;
- Decreased variance between estimated and actual resource requirements;
- Improved visibility of the state of critical components within the IT infrastructure;
- Improvement in the actual availability of services and systems available to users; and
- Improved uptake and effective use of IT Services by the user community.

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; and
- Suppliers.
2.3 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 the following Figure 2.2 demonstrating business and IT alignment.

Figure 2.2 divides an organization into a number of supporting layers that work towards meeting a number of organizational goals. These layers are communicated by the following:

- **Organization** (What are the key goals for the organization?)
- **CORE Business Processes** (These enable the objectives above to be met)
- **IT Service Organization** (What IT Services are required to enable the effective and efficient execution of the business processes above?)
- **IT Service Management** (The focus here is on the ITIL® processes required for quality delivery and support of the IT Services above)
- **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)
Example to illustrate business and IT alignment:

**Business**: A fashion store.

**What are some of your 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.); and
 Provisioned cost-effectively (Financial Management, Service Level Management).

If we don’t manage the IT Services appropriately we cannot rely on these services to be available when we need them. If this occurs we cannot adequately support our business processes effectively and efficiently. And therefore we cannot meet or support our overall organization’s objectives!
3 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 collection 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); and
- Proprietary knowledge of organizations and individuals.

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

Figure 3.1 – ITIL® V3 Core Volumes

Five volumes make up the IT Infrastructure Library (Version 3).
- Service Strategy;
- Service Design;
- Service Transition;
- Service Operation; and
- Continual Service Improvement.
3.1 The Service Lifecycle

![ITIL® Service Lifecycle Model](image)

**Figure 3.2 – 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).
3.2 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 within the lifecycle, on the guidance provided by the APMG/EXIN ITIL® Service, Offerings & Agreements syllabus. Figure 3.3 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 3.3 – The Major Concepts of ITIL®
NOTES:

- The Service Lifecycle phases (and ITIL® books) are shown through the arrows at the bottom.
- The concepts in dark shading are the V2 ITIL® concepts.
- The concepts not shaded are the new ITIL® V3 concepts.
- The concepts in light 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.
3.3 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 3.4 demonstrates some of the key outputs from each of the Service Lifecycle Phases.

It is important to note that most of the processes defined do not get executed within only one lifecycle phase. As an example we will look at the process of Availability Management and where some activities will get executed throughout Service Lifecycle.

- **Service Strategy Phase**: Determines 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.
3.4 Specialization & Coordination across the Service Lifecycle

Specialization and coordination are necessary in the lifecycle approach. Feedback and control between the functions and processes within and across the elements of the lifecycle make this possible.

Although the dominant pattern in the lifecycle is the sequential progress starting from Service Strategy, followed by Service Design → Service Transition → Service Operation and flowing back to Service Strategy in a feedback loop through Continual Service Improvement, it is not the only pattern of action.

Every element of the lifecycle provides points for feedback and control. The combination of multiple perspectives allows greater flexibility and control across environments and situations. The lifecycle approach mimics the reality of most organizations where effective management requires the use of multiple control perspectives.
4 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 4.1 – The importance of terminology
© Crown Copyright 2007 Reproduced under license from OGC
4.1 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. Alternatively, 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?); and
- Did they offer water as well as normal drinks and beverages?

If just one of these factors doesn’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; and
- The IT organization works proactively to identify potential problems that should be rectified or improvements that could be made.

To help clarify the relationship between IT Services and the business we need to look at the concepts of *Business Units* and *Service Units*. 
4.1.1 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; and
- 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 4.4 – Creating Service Value](image)

**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.

### 4.1.2 Customer Perceptions and Expectations

The customer perceptions of the service are influenced by attributes of a service that are indications of:

- Value;
- Present or prior experiences;
- Relative endowment of competitors; and
- Customers self image or position in the market.

Perceptions of value are also influenced by expectations. Customers have reference values on which they base their perceptions of added value from a service. It is essential for a provider to understand this reference value by considering:

- Extensive and consistent dialogue with customers;
- The prior experiences of customers; and
- Market research and analysis.

Service Providers can use the following formula for understanding and describing the relationship between customer satisfaction, perception and expectations:

\[
\text{Customer Satisfaction} = \text{Customer Perceptions} - \text{Customer Expectations}
\]

For customer satisfaction to be positive, the customer’s perception of the service must outweigh their expectations. To achieve this service should demonstrate and communicate value, influence perceptions and respond to customer preferences.

### 4.1.3 Marketing the value of Services

To assist in the positive marketing of services and service value to customers, service providers should develop a marketing mindset to assist in their approach. A marketing mindset begins with simple questions:
• What is our business?
• Who is our customer?
• What does the customer value?
• Who depends on our services?
• Why are they valuable to them?

A marketing mindset is quite different from engineering or operations mindset. It is all about looking from the outside in, from a customer perspective.

**Fitness for purpose (Utility)** comes from the attributes of the service that have a positive effect on the performance of activities, objects and tasks associated with desired outcomes. Removal or relaxation of constraints on performance is also perceived as a positive effect.

**Fitness for use (Warranty)** comes from the positive effect being available when needed, in sufficient capacity or magnitude, and dependably in terms of continuity and security. For customers, the positive effect is the utility of a service. The assurance of the positive effect is the warranty.

### 4.1.4 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 contains](image)

**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); and
- The Service Level Package (see next page).
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. Service Level Packages include:
- Availability & Capacity Levels;
- Continuity Measures; and
- Security Levels.

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

**Service Package: Broadband Super-User ($69.95 per month)**

**Core Service Package:**
- Internet Connection
- Email Addresses

**Supporting Services Package:**
- Static IP Address
- Spam filtering
- 100MB Web-Space
- VOIP

**Service Level Package:**
- Download Speeds: 8000kbs – 24000kbs (max)
- Download Quota: 30 GB (Shaped to 512kbs after)
- Backup dial-up account
- 98% Availability Guarantee (otherwise rebate offered)
- 24 x 7 Service Desk for Support.

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. When customers have a choice between service providers whose services provide more or less the same utility, but different levels of warranty, they will choose the greater certainty in the support of business outcomes.
4.2 Processes & Functions

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

The ITIL® processes covered in detail by this workbook are:
- Event Management;
- Incident Management;
- Problem Management;
- Request Management; and
- Access Management.
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. Behavioral 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 behavioral aspects that exist. This may be addressed by ensuring the all required stakeholders (e.g. staff members, customers and users etc.) are appropriately involved in the design of processes so that:
They can communicate their own ideas, concerns and opinions that might influence the way in which processes are designed, implemented and improved. Of particular importance may be current behaviors that have not been previously identified which may affect the process design and implementation;

- Stakeholder groups are provided adequate training and education regarding how to perform their role within the process and what value the process provides for; and
- 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.

### 4.2.2 Business Processes

Business outcomes are produced by business processes governed by objectives, policies and constraints. The processes are supported by resources including people, knowledge, applications and infrastructure.

Workflow coordinates the execution of tasks and flow of control between resources, and intervening action to ensure adequate performance and desired outcomes. The workflow of business processes is a factor of business productivity and can span organizational and geographic boundaries.

Service Management should continually seek improvements as to how IT services and the set of IT Service Management processes enhance the capabilities of business processes in achieving their desired outcomes.
4.2.3 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 Service Delivery and Support of IT Services.

![Image of ITIL Functions from Service Operation]

Figure 4.9 – 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 the roles performed by Technical Management and are not necessarily a suggested organizational structure.

4.2.4 Connecting Processes and Functions

It is often said that processes are perfect…until people get involved. This saying comes from misunderstandings of the people involved and a lack of clarity regarding the roles and responsibilities that exist when executing processes.

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**

<table>
<thead>
<tr>
<th></th>
<th>Service Desk</th>
<th>Desktop</th>
<th>Applications</th>
<th>Operations Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>RACI</td>
<td>-</td>
<td>-</td>
<td>CI</td>
</tr>
<tr>
<td>Classification</td>
<td>RACI</td>
<td>RCI</td>
<td>-</td>
<td>CI</td>
</tr>
<tr>
<td>Investigation</td>
<td>ACI</td>
<td>RCI</td>
<td>RCI</td>
<td>CI</td>
</tr>
</tbody>
</table>

*Figure 4.10 – 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 allocated (shows that actions are taking place), with more than one being appropriate where there is shared responsibility.
5 Principles of Service Management

5.1 Business Units and Service Units

A business unit is a bundle of assets with the purpose of creating value for customers in the form of goods and services. Their customers pay for the value they receive, which ensures that the business unit maintains an adequate return on investment. The relationship is good as long as the customer receives value and the business unit recovers cost and receives some form of compensation or profit (depending on the nature of the organization).

A business unit’s capabilities coordinate, control and deploy its resources to create value in the form of business services. Some services simply increase the resources available to the customer; others may increase the performance of the customer’s management, organization, people and/or processes. The relationship with the customer becomes strong when there is a balance between value created and returns generated.
Service units are similar structures to business units, being a bundle of service assets that specializes in creating value in the form of IT services. Business units (customers) and Service units (providers) can be part of the same organization or come from multiple independent organizations.

This relationship enables Business Units to focus on the outcomes provided by services, while the Service Unit(s) focus on managing the costs and risks of providing the service, possibly by spreading these costs and risks across more than one customer or Business Unit. In the context of IT Service Management, the nature of relationship between Business Units and Service Units will affect the approach taken, potentially requiring greater focus on one or more of the following areas:

- Legal requirements and contractual obligations (particularly when the business units are from a different organization to that of the service unit);
- Technical documentation and clarity (particularly when the business units/customers are IT organizations themselves); and
- Risk Management, depending on the number and size of business units/customers being served.

### 5.2 Types of Service Providers

There are three main types of Service Providers, which are distinguished by the relationship between the service provider and customers being supported. For many service providers, they will act in more than one role (e.g. as a Shared Service Provider and External Service Provider) depending on the nature of their organization. An
organization itself may also utilize more than one service provider (e.g. multiple internal service providers and a shared service provider).

**Internal Service Providers:** An internal service provider that is embedded within a business unit. As an example, where an IT department is embedded within a specific business unit such as sales and marketing. Possible reasons why an internal service provider might be used is the business unit’s requirements are very unique or complex compared to others, and/or that the IT Services provide a source of competitive advantage in the market space the business exists in.

**Shared Service Providers:** A service provider that provides shared IT services to more than one business unit. As an example, where there is one IT organization to service all business units in an organization. IT Services may not provide a source of competitive advantage, but instead support effective and efficient business processes.

**External Service Providers:** Service providers that provide IT services to external customers. As an example, the IT service provider from organization X supplying services to organizations Y & Z.

From a customer’s perception there are advantages and disadvantages of each provider type. Whether customers keep a business activity or service provision in-house (aggregate) or decide to outsource (disaggregate) depends on answers to the following types of questions:

- Does the activity require assets that are highly specialized?
- Will those assets be idle or obsolete if the activity is no longer performed?
- How frequently is the activity performed within a period or business cycle?
- Is it frequent or sporadic?
- How complex is the activity?
- Is it hard to define and measure good performance?
- Is it tightly coupled with other activities or assets in the business?
- Would separating it increase complexity and cause problems of coordination?

### 5.3 Agents

Principals employ or hire agents to act on their behalf towards some specific objectives. Agents may be employees, consultants, advisors or service providers. Within the context of Service Management, customers are principals who have two types of agents working for them:

- Service providers; and
- Users.
Service agents act as intermediary agents who facilitate the exchange between service providers and customers in conjunction with users. Service agents are typically employees of the service provider but can also be systems and processes that users interact with in self-service situations. Value for customers is created and delivered through these interlocking relationships between principles and agents.

5.4 Encapsulation

Encapsulation follows three separate but closely related principles:

- **Separation of Concerns**
  - Customers care about affordable and reliable access to the utility of assets, but they are not concerned with structural complexity, technical details or low level operations. They prefer simple and secure interfaces to complex configurations of resources such as applications, data, facilities and infrastructure. Encapsulation hides what is not the customer’s concern and exposes as a service what is useful and usable to them. In simplified terms, it distinguishes the what (is provided) from the how (it is provided).

- **Modularity**
  - Modularity is a structural principle used to manage complexity in a system. Functionally similar items are grouped together to form modules that are self-contained. Modularity contributes to efficiency and economy by reducing duplication, complexity, administrative overheads, and the cost of changes.

- **Loose Coupling**
  - Loose coupling also allows the same set of resources to be dynamically assigned to different users, systems or processes as needed. This has several advantages, including shared services, Demand Management, redundancy, and investment protection for the customer and the service provider. Loose coupling requires good design, particularly of service interfaces, without which there will be more problems than benefits.

Figure 5.3 – Separation of concerns – a fundamental aspect of IT Service Management

© Crown Copyright 2007 Reproduced under license from OGC
5.5 Monitoring and Control of IT Service Management

Control processes are used to manage the utilization or behavior of a device, system or service. Control requires three conditions to be met:

- Actions must ensure behavior conforms to a defined standard/norm;
- Conditions prompting action must be defined, understood and confirmed; and
- Actions must be defined, approved and appropriate for these conditions.

In the context of Service Management, the service provider will use a number of control processes throughout the Service Lifecycle. As an example, Service Operation will:

- Use tools to define what conditions represent normal operations or abnormal operations;
- Regulate performance of devices, systems or services;
- Measure availability; and
- Initiate corrective action, which could be automated or manual.

The two types of control processes are:

**Open Loop processes:** Open loop control processes are those in which the value of the outcome has no influence on the resulting process input. These systems take controlling action based simply on the given inputs. Any changes in inputs results in changes to the actions taken. Effectiveness of open-loop systems depends excessively on foresight in design of all possible conditions associated with outcomes. When there are exceptions open-loop systems are unable to cope or correct the situation.

**Closed-Loop processes:** Control processes in which the value of the outcome has influence (with or without some delay) on the process input in such a manner as to maintain the desired value are closed-loop. Control action in closed-loop systems is goal driven and sensitive to disturbances or deviations. Anti-lock braking systems (ABS) are examples of closed-loop systems. Even in the event where the driver applies too much braking force and resulting in a loss of traction, the ABS detects the locked brakes and immediately adjusts the input, cutting off and reapplying the braking action is rapid succession until the optimal pressure is applied on the wheels.

![Figure 5.4 – Service Management as a closed-loop control system](image-url)
In a similar way Service Management itself is a closed-loop control system, with the capabilities to:

- Develop & maintain service assets;
- Understand performance potential of customer assets;
- Map service assets to customer assets via services;
- Design, develop & operate suitable services;
- Extract service potential from service assets;
- Convert service potential into performance potential;
- Convert demand for customer assets into workload for service assets;
- Reduce customer risk; and
- Control the cost of providing services.

![Monitor Control Loop Diagram]

The most common model for defining control is the Monitor control loop. Although it is a simple model, it has many complex applications within IT Service Management and is an important concept for the Service Lifecycle. Each activity and its output are measured using a predefined norm/standard, to determine whether it is within an acceptable range of performance or quality. If not, action is taken to rectify the situation or to restore normal performance.

Monitor Control Loops can be used to manage:
- Performance of activities in a process or procedure;
- Effectiveness of a process or procedure as a whole;
- Performance of a device; and
- Performance of a series of devices.

Monitor control loops can also be built together to provide multiple levels of feedback and control. In the following figure, the lower level is concerned with monitoring and evaluating individual activity information. At the higher level, the focus is on monitoring and evaluating information relating to the entire process.
When a number of process and lifecycle monitor control loops are built together an IT Service Management monitor control loop is formed. Note: the activities shown can be processes, activities or tasks depending on the level of focus.
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; and
- Strategy and organizational culture and design.

6.1 Objectives of Service Strategy

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; and
- 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.*
6.2 Benefits of Service Strategy

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

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

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

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

- Improved understanding of the IT organization’s customers and market space they exist in;
- Detection and analysis of patterns in the demand for and use of IT services;
- Improved understanding of the costs involved in providing and supporting IT services;
- Identification and communication of the business value provided by IT services;
- Enhanced capabilities for managing the overall portfolio of services, and in particular, optimizing investments into IT; and
- Consistent policies, standards and guidelines by which IT Service Management processes can align to.
6.3 Service Strategy interfaces with other Service Lifecycle phases

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.

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; and
- Identification of patterns of business activity (PBA) and how they affect the demand for IT services.

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 evaluating whether the change can be implemented fast enough to support the strategy; and
- Control and recording of service assets is maintained by Service Asset and Configuration Management.

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; and
- Service Strategy must clearly define the warranty factors that must be supported by Service Operation, with attributes of reliability, maintainability, redundancy and overall experience of availability.

Interfaces with the Continual Service Improvement phase:
- Continual Service Improvement (CSI) will provide the coordination and direction required to implement improvements that best suit the organization’s objectives and requirements.
6.4 Major Concepts of Service Strategy

6.4.1 Value Network

Value networks are an important tool, they provide a strategy for vertically integrating and coordinating the dedicated assets required for product development. However, global sourcing and modern distribution technology have removed the ability of a service provider to compensate for weak performance in one area with strength in another.

A value network can be defined as a web of relationships that generates tangible and intangible value through complex dynamic exchanges through two or more organizations.

In the case of Service Management with the focus on Service Strategy, thought should be given as to what exchanges, both tangible and intangible, are conducted that play a part in creating value for the business and customers. These exchanges can involve multiple organizations, leveraging external capabilities where necessary to complement internal capabilities.

Where rigid supply chains are used by a service provider it limits the ability to meet dynamically changing customer and business requirements. Instead, focusing on high-performance information flows where new types and forms of exchanges can be rapidly created will allow Service Strategy to continually align the provision of IT services that support and direct the organization’s strategic objectives.
When identifying what type of value network is required or currently employed, questions that should be asked include:

- Who are all the participants in the service?
- What are the overall parts of exchange or transactions?
- What are the impacts or deliverables of each transaction on each participant?
- What is the best way to generate value?

### 6.4.2 Critical Success Factors

For every market space there are Critical Success Factors (CSFs) that determine the success of failure of a service strategy. These factors are influenced by such elements as:

- Customer needs;
- Business trends;
- Competition;
- Regulatory environments;
- Suppliers;
- Standards;
- Industry best practices; and
- Technology advancements.

Identifying CSFs for a market space is an essential aspect of strategic planning and development. In each market space, service providers require a core set of assets and capabilities in order to support the Customer Portfolio through a Service Portfolio.

The dynamic nature of market spaces, business strategies and organizations require critical success factors to be reviewed periodically as well as at significant events such as changes to Customer Portfolios, expansion into new market spaces, changes in the
regulatory environment or the emergence of new technologies. Reviews should analyze every market space they support and determine their position with respect to the options that customers have with other service providers. In any given market space there are CSFs that determine whether or not a service provider is competitive in offering services. From a customer perspective, this may include the evaluation of:

- Affordability;
- The number of service channels or delivery platforms;
- The lead times to activate new accounts; and
- The availability of services in areas where customers have business operations.

To assist in this an organization can compare the customer's perception of the services offered against the market space using benchmarks taken from industry averages, competing rivals or most attractive alternatives. An example comparison can be seen below.

![Figure 6.3 – Differentiation in the market space](image)

Appropriate indices or scales are necessary for such comparison. A value curve can be plotted by linking the performance on each scale or index corresponding to a CSF. Market research can determine the value curve that represents the average industry performance or one that represents key competitors. Feedback obtained from customers through periodic reviews or satisfaction surveys is used to plot your own value curve in a given market space or for your Customer Portfolio.

Service Strategies should then seek to create a separation between the value curves, which are nothing but differentiation in the market space. The greater the differentiation, the more distinctive the value proposition offered in your services as perceived by customers. Differentiation is normally created through a better mix of services, superior service designs, and operational effectiveness that allows for efficiency and effectiveness in the delivery and support of services.
6.4.3 The 4 Ps of Service Strategy

At the heart of the service lifecycle is Service Strategy. The four points to Services Strategy are referred to as the 4Ps, which identify the different forms a service strategy may take.

1. **Perspective** – describes a vision, direction and business philosophy of interacting with the customer.
2. **Position** – describes the decision to adopt a well-defined stance that fits the organization’s requirements.
3. **Plan** – describes the means of transitioning from ‘as is’ to ‘to be’. It focuses on the high level actions required to achieve the defined goals and objectives.
4. **Pattern** – describes a series of consistent decisions and actions over time based on the evaluation and analysis of past, current and future needs.

![Figure 6.4 – The 4Ps of Service Strategy](image)

© Crown Copyright 2007 Reproduced under license from OGC

1. **Strategy as a perspective**

The governing set of beliefs, values and sense of purpose shared by the entire organization shapes strategy as a perspective. It some senses it can be compared to mission statements for the IT service provider, as an example “We will provide high-speed connectivity to 98 per cent of the population”.

These strategic perspectives, while often trivialized or disregarded, should not be taken lightly. Unlike plans and patterns, perspectives are not easily changed. Perspective is attained with the help of clarifying questions asked within the context of the service provider’s stakeholders, its customers and its employees.

A clear perspective helps make the value proposition for its customers explicit. It also serves to direct and guide the other views (Ps) of strategy, and through feedback loops will evaluate and analyze changes to perspectives. Questions to help clarify whether an organization’s strategic perspectives are suitable include:
• Does it capture what you need to do for only the next 3-5 years, or does it capture a more timeless essence of your organization’s distinctiveness?
• Is it clear and memorable?
• Does it have the ability to promote and guide action?
• Does it set boundaries within which people are free to experiment?

2. Strategy as a position

Strategy as a position is the communication of how the service provider addresses market space demands and differentiates itself from other providers. Whether their focus is on offering a wide range of services to a particular type of customer, or being the lowest cost option, they define a strategic position in relation to their customers and market space.

There are three broad types of positions, which are:

1. Variety-based positioning
   • Variety-based positioning focuses on a particular variety of customer needs and aims to meet them in distinctive fashion. It requires a relatively narrow portfolio of services but with depth in terms of service levels, options, and packages. Service providers try to meet all the needs of any given customer segment. Success is usually defined in terms of performing exceptionally well in meeting a smaller set of needs.

2. Needs-based positioning
   • In needs-based positioning, service providers choose to provide most or all of the needs of a particular type of customer. It requires a relatively wide catalogue of services covering various aspects of the customer’s business. This is closer to the traditional approach of grouping customers in segments and then aiming to best serve the needs of one or more targeted segments.

3. Access-based positioning
   • In access-based positioning, service providers distinguish themselves through their ability to serve customers with particular needs with respect to location, scale, or structures. They deploy business assets in a manner that best serves
their own business models and strategies. Some organizations will need to be supported with employees that are highly mobile, whereas other organizations may have staff primarily based in a small number of offices.

More than one type of position may be adopted by a service provider, as the more rigid their position, their capabilities to handle market place changes, mergers or acquisitions are increasingly reduced. Questions to validate the position(s) taken can include:

- Does it provide guidance to manage conflicts between competing investments?
- Does it set clear boundaries for where and where not to compete?
- Does it allow freedom to experiment within these constraints?

3. Strategy as a plan

Strategy as a plan is the deliberate course of action charting a path towards meeting defined strategic objectives. The planning horizons are typically long term but lengths may vary across organizations, industries and strategic context. Plans are the direct means of achieving goals and objectives. They commonly focus on financial budgets, managing the portfolio of services, new service development, investments in service assets and improvement plans (as shown in the figure below).

![Figure 6.7 – Strategy as a plan](https://example.com/figure6.7.png)

© Crown Copyright 2007 Reproduced under license from OGC

Plans are linked by the need to achieve certain strategic objectives. As a result, Service Management should be focused on developing and executing a coordinated set of plans that seek to enable their service strategies. An influencing factor in the likelihood of success is the ability to strategically develop, coordinate, execute and control these plans, in which a guiding vision and direction is critical.

4. Strategy as a pattern

Strategy as a pattern is an organization’s fundamental way of doing things. They are the basis of emergent strategies, distinctive patterns in action reinforced over time by repeated success. Patterns are the consequences of perspectives, positions and plans directed by senior leadership in service of a particular customer or market space.

These patterns may not necessarily be documented or clearly observed, however they do in some way provide value in the service provider’s response to strategic, tactical and operational changes. Patterns at first should be tested and evaluated in various forms for
their effectiveness, in which case the pattern may become a part of the organization’s normal mechanisms in the future.

For example, a pattern may be developed over time that ensures any new components being introduced into the infrastructure are sourced from strategic vendors and meet defined standards. This may be a change to the way the provider previously operated, in which different areas of IT could source their own components.

Some of the forms in which service management patterns may emerge include:

- How-to patterns;
- Boundary patterns;
- Priority patterns; and
- Timing patterns.
6.5 Service Portfolio Management

Deciding how to invest money into the IT department can be a challenging task for any organization. The questions that are raised when faced with this dilemma include:

- What are the long-term goals of the service organization?
- What areas of IT deserve to be improved / developed?
- How do we quantify the benefit that will be delivered as a result?
- When should these investments occur?
- What should be the sequence of these investments?
- What areas of IT are no longer necessary or are not cost-justifiable?

To answer these questions, analysis of the relationship between IT services and business processes / business services is required, with enhanced understanding providing guidance into strategic direction of potential service investments and retirements.

In some ways Service Portfolio Management is similar to Financial Portfolio Management. A Financial Manager's primary responsibility is to maintain an optimum portfolio of investments that maximizes the client’s return at an acceptable risk level. When conditions in the property of share market change, the Financial Manager is responsible for observing, anticipating and responding to these changes accordingly.

Service Portfolio Management should be seen in the same light, being a “dynamic method for governing investments into service management across the enterprise and managing them for value” (Service Strategy, p.120).
Figure 6.8: The key role of Service Portfolio Management is to balance the potential risks and value involved with investments into the IT organization.
6.5.1 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; and
- 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?

6.5.2 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 6.2 demonstrates the relationship between the Service Portfolio elements and the various Service Lifecycle phases. In this figure, the areas of the circles are proportional to the resources currently engaged in the corresponding lifecycle phase.

![Figure 6.2: Relationship between the Service Portfolio elements and the various Service Lifecycle phases.](image)

**6.5.3 Benefits**

Effective governance and strategic direction and management of investments into the Service Portfolio is underpinned by understanding and analysis of the relationship that exists between the service provider and the various business processes, services and units being served. When this is adequately facilitated there are many benefits delivered to both IT and the business, including:
• Close alignment between cost-effective investments into the service portfolio and the plans and vision of the business and customer;
• Timely identification of when services should be implemented, maintained, improved and retired;
• Reduction in the conflicts and competition that might exist between organizational units within IT for priority, resources, budget and advancement;
• Improved ability for the IT organization to understand the market, and distinguish the services they provide and how they differ from competitors’ offerings; and
• Improved ability to identify and manage potential risks involved with delivering and supporting services.
6.5.4 Service Portfolio Management Methods

As part of an ongoing and dynamic approach to managing investments into IT Service Management, implementation of Service Portfolio Management should include the following methods:

1. Define
   - Identify all services for capture within the Service Portfolio, develop business cases and validate portfolio data.

2. Analyze
   - Seek methods to maximize portfolio value, align and prioritize and balance supply and demand.

3. Approve
   - Finalize proposed portfolio, authorized services and resources.

4. Charter
   - Allocate and schedule resources, charter services and communicate decisions.

Note the continuous loop that exists within figure 6.3, which means that the portfolio will be continually refreshed as various market spaces and the associated business changes.
6.5.4.1 Define

Before the evaluation of proposed service investments occur, the staff involved should first develop a definitive collection of high-level information for all existing services as well as proposed new/changed service. The main aim of this exercise is to provide understanding about what the potential weaknesses of the service provider are, providing a new position for assessing whether the existing resources and capabilities should be reallocated. As the process will be continually executed, future iterations mean that captured data will be validated on a regular basis. This may occur at defined review periods (e.g. every 6 months), or be in response to a particular event, such as a company merger or economic recession.

Within the portfolio, all services should maintain an associated business case. This provides a model of what a service is expected to achieve, and acts as a justification for the service investment by describing the potential benefits, resources and capabilities required to develop and maintain it.

*The Option Space Tool*

Some organizations make use of a tool called an Option Space (see Figure 6.4), which can provide guidance on decisions for where and when to invest.

![Figure 6.11: Option Space](image-url)
An important element to the Option Space is the Value-to-Cost axis, which represents the ratio of a planned or current service’s value to its cost. When the ratio is greater than 1.0 then the value of the service has been determined to be greater than its cost. Although financial measures are typically the main focus, other factors should also be incorporated, including:

- Primary strategic objectives;
- Regulation and compliance issues;
- Market trends;
- Intangible benefits (e.g. job satisfaction);
- Strategic or business fit;
- Environmental impact; and
- Organizational credibility and perception.

As an example, a financial institution fulfilling legal compliance requirement for data recording and retention may on its own generate a Value-to-Cost measure of greater than 1.0. It is important that these factors are identified and agreed upon as to their relative importance to the organization and the potential risk involved if they are not satisfied.

The other axes will be discussed within the following methods, but as a summary:

- **Customer Needs**: a representation whether the set of customer needs is currently over-served or under-served.
- **Customers**: identification whether the investments are targeted at new customers or existing customers.
- **Market Spaces**: similar to Customers, this axis identifies whether the investment is targeting new market spaces or existing market spaces.
6.5.4.2 Analyze

After suitable data and information has been collected, analysis should be performed to begin drafting the strategic intent for IT. To do so there should be involvement of senior leaders and subject matter experts, who will begin by starting with a defined set of top-down questions that require answering:

- What are the long term goals of both the organization (customers) and service provider?
- What services are required to meet those goals?
- What capabilities and resources are required for the organization to achieve those goals?
- How are we going to achieve these goals?

*Investment Categories*

So that there is an appropriate balance of service investments, three strategic categories are defined to understand the level of potential risk and affect on operations.
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 within existing market spaces, either by more services or more customers.

Run the Business (RTB): RTB investments are centered on maintaining service operations.

Figure 6.13: – Investment categories and budget allocations
© Crown Copyright 2007 Reproduced under license from OGC

These investment categories are then further divided into budget allocations, with the type of service provider affecting the way in which these allocations are usually made.

- **Venture** – Create services in a new market space. There is usually a higher risk level involved as the service provider has no previous history/capabilities in this market space.
- **Growth** – Create new services in existing market space. This may be for the purpose of gaining new customers, or increasing the average revenue per customer.
- **Discretionary** – Provide enhancements to existing services, which should be directed by the identification of underserved customer needs.
- **Non Discretionary** – Maintain existing services. This seeks to maintain the status quo or business as usual for the service provider.
- **Core** – Maintain business critical services.

As demonstrated in figure 6.6, there is an increasing risk scale as you move from investments focused on running the business through to transforming the business. However, it is important to remember that the risk in this case is from the perspective of achieving a suitable return on IT investment, not a risk to the organization as a whole. Organizations will accept a higher level of risk where there is a potential for greater reward in a new service offering or by entering new markets. In other cases, to ensure the continued financial viability of the organization it may be critical to enter a new market space, especially as the profitability of old market spaces reduce.

Part of this stage includes the identification of potential service retirements. Many organizations fail to have clear processes and plans for retiring services, continuing to
deliver and support them once they have outlived their usefulness to the business or when they are no longer compatible with the changed technical architecture. For organizations with a long history this can amount to significant hidden costs, and also presents challenges for acquiring staff with sufficient skills to maintain and support the legacy systems effectively.

### 6.5.4.3 Approve

The previous stages have analyzed potential future investments, leading to the requirement of authorization (or rejection) by the appropriate IT and business staff members. This authorization will produce many outcomes for the services contained within the Service Portfolio, as well as approving the associated resources required to implement and manage these outcomes.

When dealing with existing services, outcomes stemming from investments typically fall into six categories:

- **RENEW:** Where services meet functional fitness criteria but fail technical fitness, investments may be focused on renewing the service to comply with the defined technical architecture and minimum performance levels.

- **REPLACE:** For services that have unclear and overlapping business functionality, investments may used to replace the service in its entirety.

- **RETAIN:** When services utilize self contained assets and have clear process and system boundaries, investments would most likely be authorized to maintain their delivery and support arrangements. Of course, this still means that the services must be aligned with and are relevant to the organization’s strategies to warrant being retained.

- **REFACTOR:** When services that meet the technical and functional criteria of the organization but display fuzzy process or system boundaries, investments may be utilized to refactor the service, including only the core functionality, with common services used to provide the remainder.

- **RETIRE:** For services that do not meet minimum levels of technical and functional fitness, or are no longer aligned to the organization’s strategies, the service may be retired under the control of Change Management. Since the cost of retiring a service may temporarily exceed the cost of maintaining it, its budget allocation can shift from Non-discretionary to Discretionary.
RATIONALIZE: When portfolios that services which are composed of multiple releases of the same operating system, service or application, the service may be rationalized to restructure the services in a logical manner.

It is important that these actions are authorized based on the analysis of the portfolio and potential investments. As an example, figure 6.7 below demonstrates a typical Option Space for an organization focused on expanding their scope of services (a mixture of Growing the Business and Transforming the Business).

The correct prioritization of these investments and focusing appropriate management attention is a challenging role that should be addressed by Service Portfolio Management. Generally speaking, the best opportunities lie in areas where an important customer need remains inadequately served. While these investments should always be considered for their associated costs and risks, over time the portfolio should seek to have greater coverage and support for such areas of opportunity. Conditions that might prevent these opportunities from being taken or cause reason for the demand not to be served are a lack of innovation, inappropriate performance of potential offerings or likely future volatility of a particular market space.
6.5.4.4 Charter

As authorization for service investments occur, the corresponding actions need to be scheduled and communicated to all appropriate IT staff, customers, suppliers and other key stakeholders. Additionally, the budget allocations should be defined to enforce the appropriate planning and allocation of the resources required. In conjunction with this, Financial Management should identify the expected value of each service when documenting financial forecasts and resource plans. This is useful for tracking the progress of service investments throughout their planning, design and transition into the live environment.

As the options from 6.1.4.3 suggest:
- Newly charted and renewed services are handed to Service Design;
- Services being retained are refreshed in the Service Catalogue; and
- Retired Services are handed to Service Transition to manage their removal.

Once chartered, Service Catalogue Management is responsible for ensuring that the correct details regarding those services in use (or ready for deployment) is recorded.

6.5.5 Refreshing the Service 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; or
- 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.
6.6 **Financial Management**

The discipline of Financial Management has for many been a challenging, complex and sometimes controversial area of business, especially when it comes to managing the finances involved in the provision and support of IT services. While arguments will always occur to debate the ‘best’ way in which money is apportioned and spent, particularly in the case of IT difficulties arise in the effective identification of the true costs associated in designing, transitioning, operating and supporting services. As a result, many organizations have struggled to provide appropriate clarity regarding the way in which money is budgeted and accounted for, which from a customer perspective can lead to a lack of confidence and reputation in the service provider.

To counter this, 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.

![Diagram of Financial Management](image)

**Figure 6.15:** – 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.
6.6.1 Goal and objectives

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.

6.6.2 Benefits

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; and
- Greater insight and communication of the value created by IT services.

Figure 6.16: – Shared imperatives framework: business and IT

© Crown Copyright 2007 Reproduced under license from OGC

The Shared imperatives framework illustrates the commonality of interests and benefits between the business and IT, with Financial Management used to assist decision making.
in each of the elements depicted. The process is utilized to generate meaningful critical performance data to assist answering important questions for an organization, such as:

- Is our differentiation strategy resulting in higher profits or revenues, lower costs, or greater service adoption?
- Which services cost us the most, and why?
- What are our volumes and types of consumed services, and what is the correlating budget requirement?
- How efficient are our service provisioning models in relation to alternatives?
- Does our strategic approach to service design result in services that can be offered to a competitive market price, reduce risk or offer superior value?
- Where are our greatest service inefficiencies?
- Which functional areas represent the highest priority opportunities for us to focus on as we generate a CSI strategy?

### 6.6.3 Concepts and principles of Financial Management

#### 6.6.3.1.1 Service Valuation

The output of Service Valuation is an agreed *value* definition for services delivered and the associated funding sought by the business and IT based on this *value*.

![Figure 6.17: Service Valuation](https://example.com/service_valuation.png)

© Crown Copyright 2007 Reproduced under license from OGC

The pricing of a service should reflect the cost-to-value translation required to achieve clarity and positively influence the demand and consumption of services. As shown in the figure above, Service Valuation includes a number of components:
Provisioning value:

Describes the underlying actual cost for provisioning an IT service. Input comes from financial systems, and consists of payment for actual resources consumed by IT in the provisioning of a service. These cost elements include items such as:

- Hardware and software license costs;
- Annual maintenance fees for hardware and software;
- Personnel resources used in the support or maintenance of a service;
- Utilities, data centre or other facilities charges;
- Taxes, capital or interest charges;
- Compliance costs; and
- Transfer costs and internal charging by other business units/processes.

The sum of these actual service costs typically represents the baseline from which the minimum value of a service is calculated as providers are seldom willing to offer a service where they are unable to recover the provisioning cost. The exception to this rule is usually for seeking technology advancements or when the provider runs a service at a loss initially, but over the life of the service costs are reduced in such a way that a profit is generated and maintained.

Service Value Potential:

Describes the value-added component based on the customer’s perception of value from the service or expected utility and warranty (see 4.1.2 Creating Service Value) from using the service, in comparison with what is possible using the customers own assets. Provisioning value elements add up first to establish a baseline. The value-added components of the service are then monetized individually according to their perceived value to estimate the true value of the service. Although there is a wide range of value elements that may be considered, some of the most common examples that are used include:

- Increased automation of a business process;
- Removal or reduction of human resources required to support business process;
- Increased ability for data collection and reporting throughout business process;
- Greater end-user involvement and control throughout business process by using IT service; and
- Removal of physical constraints by means of remote management.

6.6.3.1.2 Demand Modelling

Financial Management works closely with the process of Demand Management (see chapter 6.3) 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.

6.6.3.1.3 Planning Confidence

Within the context of Financial Management, planning provides financial translation and qualification of expected future demand for IT services. In the past this came from the analyzing individual line item expenditures or business cost accounts. In the modern organization, planning focuses on demand and supply variances that result from business strategy, capacity inputs, demand modeling and forecasting.

Planning can be categorized into three main areas, each representing financial results that are required for continued visibility and service valuation:

- **Operating and Capital**: involving the translation of the financial resources consumed by IT, both for capital purchases and the ongoing delivery, support and maintenance required for IT assets. Part of the general and fixed asset ledgers.

- **Demand Planning**: See Demand Modelling, section 6.2.3.1.2.

- **Regulatory and Environmental**: Many compliance factors affect every type of business, which means the Financial Management is responsible for understanding the effects they will have on service value and IT costs. All factors potentially have a large impact on the Total Cost of Ownership (TCO) for IT services, so existing and new environmental, reporting or safety regulations (as examples) need to be considered sufficiently to provide appropriate planning confidence. Without it, decision making, particularly at the strategic level, will be negatively affected.
6.6.4 Financial Management Activities

This section is aimed at providing an overview and sampling of best practices for the methods, activities and techniques within Financial Management, as specific training, education and practical experience in Financial Management and IT Accounting is assumed.

6.6.4.1.1 Service Valuation and IT Accounting

When analyzing a service to define an agreed value, important decisions need to be made in the calculation of various cost elements. While some principles from traditional methods of accounting remain, additional categories and characteristics must be defined to enable identification and tracking of service-oriented expense or capital items. The categories and characteristics that are applicable include:

**Service recording**: the assignment of a cost entry to the appropriate service, or sub-service components.

**Cost Types**: The identified higher level expenses categories, including such types as hardware, software, labor, accommodation etc.

**Cost classifications**: Designating the end purpose of the identified costs, including the following classifications:

- **Capital** – the purchase or disposal of IT assets that provide value and depreciate over a period of time (normally two to five years). Include desktops, servers, switches etc. Organizations heavily invested in fixed capital IT assets (in comparison to their operational costs) may have difficulty adjusting to quickly changing business requirements.
- **Operational** - the costs involved in running the IT department on a day-to-day basis.
- **Direct** – costs that can be directly attributed and charged to a service since it is the only consumer of the expense.
- **Indirect (shared)** – costs that are allocated across multiple services since each service consumes some portion of the expense.
- **Fixed** – costs that don’t vary with time or usage.
- **Variable** – costs that vary based on influencing factors such as time or usage.

Predictability can be addressed through:

- **Tiers** – pricing tiers where plateaus occur and encourage usage efficiencies familiar to the provider
- **Maximum cost** – prescribing the cost of the service based on the maximum level of variability
Average cost – setting the cost based on a historical average of variability, further refined by correcting of any under or over-charging.

**Cost Units** – A cost unit is the identified unit of consumption that is accounted for a particular service or service asset. (E.g. a telecom charging per SMS sent).

Once the fixed and variable costs for each service are identified, steps should be taken to determine the variable cost drivers and range of variability for a service. This assists in calculating any additional amount that should be added to the potential service value, but the inclusion of these extra charges should also be considered in relation to the organization’s existing practices, culture and strategic direction.

Pricing the perceived value portion of a service involves resolving the grey area between actual historical costs, perceived added-value and planned demand variances. When done effectively it enables the actual costs to be recovered, or at the very least enhanced cost visibility and communication of service value.

**6.6.4.1.2 Service provisioning models**

For each service provider there will be many factors that are considered when determining the most appropriate service provisioning model for their organization. The term describes the method by which services are provided, managed and charged for by the service.
provider, and will vary depending on the usage of services and types of customers being served.

- **Managed services:** The more traditional provisioning model where each business unit or customer requiring a service funds the provision of that service for itself only. This is the most expensive model as the resources used are dedicated entirely to a single service entity, with any unused resources or capabilities being lost.

- **Shared services:** Another common provisioning model, where each service is provided to one or more business units or customers through the utilization of shared infrastructure and resources. Using this model provides the potential for more efficient use of resources through increased utilization of existing resources.

- **Utility-based provisioning:** Extends the concept of shared services, with even more services and customers utilizing the same infrastructure and resources. This is made possible by providing services on a utility basis, depended on how much, how often, and at what times the customer needs them. The term utility is used in reference to the provision of utility services such as power, gas and water. While more complex and elusive, it does provide the most cost-effective option for provisioning services. An example of this model can be seen in the offerings made available in Amazon’s S3 (Simple Storage Services) and EC2 (Elastic Computing Cloud).

- **Service provisioning cost analysis:** Statistically ranking the various forms of provisioning (and providers) to determine the most beneficial model.

### 6.6.5 Funding and charging

Funding is the critical component that addresses the financial impacts from changes to current and future demand for IT services and the way in which IT will gain funds to continue operations. Like accounting and provisioning models, the chosen funding model should take into account the organizational culture and business expectations.

**Roll Plan Funding:** As one cycle completes another cycle of funding is added. This plan encourages a constant cycle of funding, however, it only addresses timing and does not necessarily increase accuracy.

**Trigger-Based Funding:** Trigger-based funding occurs when identified critical triggers occur and set off planning for a particular event (such as an accepted Request for Change or updated Capacity Plan). The scope of evaluation and funding will be limited to the action required, however should still comply with any other funding models being utilized.
**Zero-Based Funding:** This form of funding is only enough to bring the balance of the IT financial centre back to zero or to bring the balance of funding of a service back to zero until another funding cycle. The benefit of the model is increased accuracy, as it starts from a clean slate and funds only the actual costs to deliver services. This disadvantage of this model is that it disregards historical data or trends, and has potential for inefficiency because of effort required compared to other models.

In many cases, there will be a requirement to use a combination of these funding models so that ongoing and accurate budgets can be drawn up and so that there are capabilities for managing new and unanticipated requests in terms of their financial requirements.

**6.6.5.1.1 Regaining Funds**

The most common two ways in which to describe the method for replenishing funds incurred in delivering IT services are:

- **Cost centre:** Where funding is based on replenishing only the actual costs incurred in delivering services.

- **Value/profit centre:** Where funding replenishing actual costs and adds a perceived value-added amount. This may be used to run the IT organization at a profit or to fund future developments and improvements to services.

**6.6.6 Chargeback**

A ‘chargeback’ model for IT can provide accountability and transparency, but must be considered as to whether its use is appropriate for the existing organizational culture. Chargeback models vary based on the simplicity of calculations, the level of benefit that the chosen model will bring and the level of detail and clarity provided.

Some example chargeback models include:

- **Notional Charging:** Where costs are recorded but not actually charged to the business units. This could be used in the transition period as charging is being introduced, and can serve to positively influence usage of IT services.

- **Tiered Subscription:** Where varying levels of warranty/utility combinations are offered, such as Bronze, Silver, or Gold package offerings.
• **Metered Usage**: Especially used in utility-based provisioning models, where business unit’s variable chargeback is based on the cost-units consumed during the charging period.

• **Direct Plus**: A simple chargeback model where the direct service costs are passed on with some percentage of indirect costs shared amongst all.

• **Fixed or User Cost**: The most simple chargeback model, where the total cost for a service is divided by an agreed denominator, such as the number of users. It does little to reflect actual costs incurred or resources consumed, but is an easy method to approximate and allocate the costs incurred to multiple business units.

To limit risk in implementing charging, the IT organization should:

• Publicize the program and work with the business to define the charging policy;
• Ensure SLAs are in place and representative of actual service quality provided; and
• Ensure benefits are quantifiable and outweigh the costs to implement charging, and that the benefits can be reported.

### 6.6.7 Implementing Financial Management

The following is an example summary guide on how a phased approach can be used effectively to implement Financial Management.

1. **Plan**
   • Identify organizational influences, such as culture, geographical distribution and types of business units that Financial Management needs to consider.
   • Identify any regulatory or compliance requirements that need to be met.
   • Clarify both business and IT expectations for Financial Management.
   • Determine systems and interfaces that will be interfaced with and provide support to Financial Management.
   • Determine the funding model to be used.
   • Assign roles and responsibilities.
   • Prepare a policy and operating procedures list for the process.

2. **Analyze**
   • Begin in-depth synthesis and analysis of the planning and funding items previously identified (in 1. Plan).
   • Design top-down to identify how both the business and IT expectations for the process will be met, assigning specific responsibilities and tasks to be performed.
• Identify gaps in the collection of financial information, as not all data will be collected into one financial centre.

• Once the accounting of all IT expenditures has been completed, service valuation should be performed, focusing first on service assets, then building value-add pricing into the models, to calculate the total pricing for IT services.

• Ensure that all required Service Management (and other) interfaces are capable of supporting the process, otherwise postpone implementing Financial Management until they are ready (e.g. until a Capacity Plan is produced).

3. Design

• The design phase is where the actual outputs expected from the process are created and assessed.

• Valuation Models should be prepared and tested for appropriateness to the organization and business environment.

• Accounting processes to be used should be finalized and agreed.

• The appropriate chargeback model to be used should be agreed and communicated to all relevant stakeholders.

• Any remaining procedures should be documented to support the execution of the process.

• Any remaining job descriptions should be completed and roles filled.

4. Implement

• Implementation provides the final activation of planned Financial Management process.

• Change Management and Demand Management are the first ITSM processes affected by the introduction.

• Accounting is the first activity that will be utilized, receiving operational financial data for translation.

5. Measure

• For the final stage after implementation, a full cycle needs to be completed by measuring the success achieved by identifying financial trends within funding, valuing and accounting.

• Ensure any correction in pricing is rectified, based on the value perceived and charging allocated.

• Process compliance should be assessed by auditing the activities being performed, and depending on the nature of the business and regulatory or compliance requirements, this may need to be performed by an external organization or body.
• Customer satisfaction with the process should also be assessed, with Service Level Management communicating regularly and identifying any (potential) issues that arise.
6.7 Demand Management

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. This is because before we decide how to design for availability and 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?
- What level of capacity and performance should we support?
- How can we influence demand to reduce our excess capacity needs?
- How do our IT strategic objectives affect our approach? Are we focused on cost-effectiveness?

Poorly managed demand is a particular source of risk for service providers, with potential negative impacts being felt by both the IT organizations and customers. If demand is not accurately predicted and managed, idle (excess) capacity will generate cost without creating associated value that can be appropriately recovered. From the customer perspective most would be highly reluctant to pay for idle capacity unless it provides some value for them.

On the other hand, insufficient capacity can impact the quality of services delivered, potentially limiting the growth desired for services and for the organization as a whole. Accordingly, Demand Management must seek to achieve a balance between the prediction and management of demand for services against the supply and production of capacity to meet those demands. By doing so both the customers and IT can reduce excess capacity needs while still supporting required levels of quality and warranty in agreed services.

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 holidays the
service provider would seek to provide all capacity to meet demand and support higher revenue streams for the business units involved.

### 6.7.1 Goal and objectives

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; and
- 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.

### 6.7.2 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.

Demand occurs at multiple levels. Increased workload in the business can translate to a higher utilization of services by existing employees. At the same time, additional staff members that are employed by the organization can be translated into additional demands to the IT service provider (especially the Service Desk) in terms of service requests and incidents. To manage this, regular communication is required so that the business plans of the customers and business units are synchronized with the service management plans of the service provider.

Financial Management works closely with the process of Demand Management 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.

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; and
- **Continual Service Improvement**: Can identify opportunities to consolidate demand or introduce improved incentives or techniques to be utilized in influencing demand.

Critical to the effective application of Demand Management is a forward-looking Capacity Plan, which should identify how capacity will be produced to meet the predicted demand patterns, including the level of excess capacity deemed appropriate in accordance with the business requirements for service value.
### 6.7.3 User Profiles

Like Patterns of Business Activity (PBA), User profiles should be identified and analyzed for their relationship to the patterns of demand generated in the business. User profiles are defined in the context of the roles and responsibilities within the organization for people, functions, processes and applications. In some cases a user profile will be defined for an automated process, which will have its own demand for supporting services.

When defining user profiles, they will be associated with one or more PBA, which requires both customers and the service provider to have a clear understanding of the business activities and how various roles are related.

The following table is an example of User profiles defined by Demand Management:

<table>
<thead>
<tr>
<th>User profile</th>
<th>Applicable pattern of business activity</th>
<th>PBA code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Executive (UP 1)</td>
<td>Moderate domestic and international travel, highly sensitive information to be protected, high urgency for service requests, communication services need to be highly available.</td>
<td>33B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21A</td>
</tr>
<tr>
<td>Office-based managers</td>
<td>Low domestic and international travel, medium sensitive information, medium urgency for service requests, communication services need to be highly available.</td>
<td>33D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21A</td>
</tr>
<tr>
<td>Office-based staff</td>
<td>No domestic and international travel, low sensitivity information, low urgency for service requests, communication services require medium availability.</td>
<td>33A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21C</td>
</tr>
</tbody>
</table>

In the above table, the PBA code would be referencing previously defined patterns of business activity, which helps clarify when will each type of user will typically generate demand for IT services and what level of demand will there be. This is valuable information which can be used for then predicting the potential impact that adding or removing staff members (users) may have on the demand for IT services and the ability of the IT service provider to meet those demands.

### 6.7.4 Developing differentiated offerings

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 (see section 4.1.3) that suit identified patterns and types of demand.
A Service Package contains

- **Core Service Package**
  - (The basic critical services)

- **Supporting Services Package**
  - (Provides differentiation or more effective use of Core Services)

- **Service Level Packages**
  - (Defines level of utility and warranty provided by Service Package)

**Figure 6.20: – Activity-based Demand Management**

In a basic approach, this may be as simple as Gold, Silver and Bronze offerings to influence the adoption and use of IT services. To clarify how the different processes work together, the following is a summary of the various responsibilities:

- **Service Portfolio Management responsibilities** – to assess, manage and prioritize investments into IT, identifying underserved, well served and over served demand. Manage Service Portfolio, including the definition of services in terms of business value.

- **Demand Management responsibilities** – identify, develop and analyze PBA and user profiles. Build capabilities for predicting seasonal variations and specific events in terms of the associated demand generated. Strategically package services to reduce excess capacity needs while still meeting business requirements. Design and apply techniques where necessary to influence demand.

- **Financial Management responsibilities** – to work with Demand Management to determine value of services (and understand the effect on value by varying levels of capacity and performance), and to develop appropriate chargeback models to be used in influencing demand.

- **Service Level Management responsibilities** – to maintain regular communication with customers and business units, identify any potential issues, promote service catalogue, negotiate and agree relevant SLAs (including the charging mechanisms used to influence demand), ensure correct alignment of Service Packages and Service Level Packages. Generally measure the success of IT and quality of service delivered from the customer perspective, providing feedback to the other processes on issues and potential improvements.
6.7.5 Challenges affecting Demand Management

While integrating Demand Management appropriately with all other aspects involved in Service Offerings & Agreements is challenging in itself, some other specific challenges typically faced include:

- When little or no trend information regarding PBAs and demand is available. It is not possible to produce and stock service output before demand actually materializes;
- Aligning capacity production cycles to PBA, especially when funding of IT has not been adequately planned and synchronized with business plans;
- Customer resistance to Demand Management restrictions, especially in the case of additional costs incurred; and
- Loss of user productivity and business growth by too much restriction applied when managing demand.

6.7.6 Key Performance Indicators (KPIs) of Demand Management

Like the rest of Service Offerings & Agreements, the measurement of success should be assessed using balanced perspective that takes into account the relationships and sometimes conflicting demands between the different processes involved. Some of the specific KPIs for Demand Management include:

- Increased utilization of IT infrastructure;
- Decrease in idle capacity;
- Reduction in capacity and performance related incidents;
- Decrease in number of capacity related incidents;
- Percentage accuracy in predicted demand cycles; and
- Reduction in cost of IT service provision with stable quality levels.
6.8 Challenges, critical success factors and risks of service management

This section will focus on the major challenges, critical success factors and risks that should be considered by a service provider in its approach to service management.

6.8.1 Complexity

IT organizations are complex systems in that they are made up of tightly coupled and interdependent groups of people, processes and technology. As a result, many IT organizations can be seen to be adaptive and self-organizing yet policy resistant. Natural and organic changes are developed and embedded, however any changes that you try to force upon them are resisted. There are multiple reasons for this, including:

- Limited learning horizons;
- Limited ability to observe long-term consequences to decisions and actions;
- A tendency to predict and react, rather than developing continual learning; and
- A mindset that today’s initiatives and solutions will be tomorrow’s problems.

As a consequence, both a modular and holistic view should be taken to service management. It is important to understand the various elements in isolation (e.g. processes, teams, services, components etc.) however they should also be viewed in the light that they work together to produce characteristics of services that define value for customers. When treated only in isolation, some of the most significant consequences of decisions and actions may remain hidden for some time until observed by another group or from a different perspective.

6.8.2 Coordination and control

Many decisions and actions within service management required coordinated and cooperation between multiple teams and individuals. Cooperation problems occur when there is conflict between the needs, views and perspectives of the parties involved. Such an example can be seen in defining what should be the timeframe in which change requests should be approved. These cooperation problems can be solved through constant negotiation, aiming for an agreement in which every party is better off. Unfortunately this is not always possible, especially where the balance of power in a relationship or partnership is particularly lop-sided.

Another possible method for maintaining coordination and cooperation is by the definition of collective views, goals and outcomes towards which all performance is directed. Such views include the definition of service strategies, objectives, policies, rewards and incentives. These are then translated and supported through multiple levels of organizational groups, functions and processes. A Service Knowledge Management System can also provide the capabilities to maintain multiple and distinct control.
perspectives on the same reality. The control perspectives may be taken from a lifecycle phase or process focus, in which the perspective helps to understand what is important and relevant in order to ensure the process (or lifecycle phase) is effective and efficient. Senior management commitment is another factor that will assist in the collaboration and cooperation across multiple perspectives.

### 6.8.3 Preserving value

1. Deviations in performance

In a mature organization, customers are concerned not only with the utility and warranty provided at a defined cost, but also the total cost of utilization (TCU) associated with the service(s) provided. The TCU also includes all costs incurred indirectly in the process of receiving the committed utility and warranty.

While the utility and warranty combines to provide value, it can also be easily lost due to hidden costs that the customer incurs from utilizing a service. Poor management of services over the lifecycle can result in customers paying much more than the price of the service when the effect of hidden costs sets in. As a result, the enduring value for customers turns out to be much lower than the value created, and so eliminating hidden costs is a challenge, a critical success factor and a risk.

2. Operational effectiveness and efficiency

Efficiency goes to waste when outputs or outcomes are not fit for purpose or fit for use. This is highly common in the case of IT services as many aspects of value are often intangible. Effectiveness is the quality of beings able to bring about a desired effect. In the context of services, the two primary effects are utility and warranty. Efficiency may be seen as the ability to provide the ability to serve greater amounts of demand while using the same amount of resources. Particularly in the case of the service lifecycle, improvements to Service Design and Service Operation may drive efficiency gains. Service providers should be mindful of the feedback mechanisms between effectiveness and efficiency, as a change to one can have either a positive or negative effect on the other.
3. Reducing hidden costs

One category of hidden costs is transaction costs, which include costs for resources that service providers spend to determine customer needs, user preferences and quality criteria that underpin value and pricing decisions. Costs are also incurred when changes are made to services themselves, SLA’s and demand in a ‘trial and error’ manner.

Well defined service management processes, measurement systems, automation and communication, should drive down transaction for the service provider. Where possible, the standardization and reuse of service components should occur, so that any resources and effort spent can be applied optimally to the benefit of a greater number of services and customers.

4. Substantiating hidden benefits

One way of reducing asset lock-in is to rent or lease the assets rather than buying them. In a similar way for customers, managed services provide an attractive alternative to asset purchases, offering the utility of an asset without the related lock-in. From a broader perspective, through the development of various technology standards as well as the increased adoption of standardized service management processes, the risk and costs associated with switching service providers has also been reduced.

5. Leveraging intangible assets

The use of intangible assets can increase the scalability of service systems, whereas tangible assets (e.g. office and storage space, financial resources, human resources etc.) cause a loss of opportunity for other competing demands. Intangible assets are generally don’t have an associated opportunity cost as they can be replicated and concurrently deployed to service multiple instances of demand. As an example, knowledge intensive systems can be highly leveraged with virtually zero opportunity costs as they primarily deal with intangible assets. From a service management perspective, the structure of service models, designs and processes can be analyzed to determine the proportion of intangible elements over tangible ones.

Where possible tangible elements should be substituted with intangible ones so that service design becomes more scalable with less opportunity costs. When service elements are well defined, it is possible to increase the throughput of the service delivery system by software-based replication, where software agents supplement human agents by taking care of some or all types of transactions (e.g. bank ATMs and interactive voice response systems).

6.8.4 Risks

Risk is defined as uncertainty of outcome, whether positive opportunity or negative threat. Managing risks requires the identification and control of the exposure to risk, which if materialized may have an impact on the achievement of an organization’s business objectives. Every organization manages its risk, but not always in a way that is visible,
repeatable and consistently applied to support decision making. This is true for many organizations, where one of the greatest risk factors is a lack of accurate information when making decisions. The task of management of risk is to ensure that the organization makes cost-effective use of a risk framework that has a series of well-defined steps. The aim is to support better decision making, through a good understanding of risks and their likely impact.

Service providers in many cases seek to reduce the risks to the customer’s business by taking them on themselves, and where possible, sharing them across multiple customers. Customers compensate the service provider for these risks, primarily through the prices paid for any services consumed. Where charging is not possible or feasible, the service provider should seek to engage their customers in discussions as to how risks can be compensated for in the most appropriate way. The transfer of risks between customers and service providers (both ways) can be seen in the figure 6.23.
There are numerous risks faced by a service provider, including the materialization of:

- Technical instability;
- Loss of control in operations;
- Breaches in information security;
- Breach of regulations; and
- Financial shortfalls.

If the risks materialize the impact is normally measured in financial terms or in a loss of customer, supplier or partner goodwill. While it is easier to measure the financial impact, the impact arising from a loss of goodwill shouldn’t be underestimated. As a guide, the financial measures should then be used as indicators, rather than purely direct measures of risk.

3. Contract risks

Risks that threaten the ability of the service provider to deliver on contractual commitments are strategic risks, because they jeopardize not only operations in the present (short-term consequences), but also the confidence and goodwill of customers in the future (long-term consequences). Supplier contracts are vulnerable to many kinds of risks, including strategic, design, operational and market risks. In the context of the Service Lifecycle, Service Transition is a primary source of guidance for evaluating the risks in contractual commitments, however all lifecycle phases have a role to play in the management of identified risks.

4. Design risks

With the design of any new or modified service there is always a risk that it won’t deliver the expected utility and warranty as desired by the customer. In cases where there is a lack of formalized functions and processes in Service Design, this risk increases as the feedback loop to normalize agreed requirements and service levels may not be effective. Where scalability is a concern, the best designs are those that take into account the required performance potential for predicted demand cycles, but also can tolerate variations within a specified range. From a financial perspective, services should be designed to be economical to operate yet flexible to future improvements and modifications.

5. Operational risks

The operational risks faced organizations can be grouped into two main categories, those affecting the business units and those affecting the service units. Service Management primarily seeks to identify and manage those risks faced by the service units (including the service provider and other suppliers or partners). Risks may be identified such as the under-utilization of assets, failures to deliver sufficient warranty levels or rising costs.
incurred in the delivery and support of services. Constraints that should be considered and managed include:

- Asset specificity;
- Scalability;
- Set-up and training costs;
- Dependencies and relationships; and
- Overloaded assets.

In regards to the scalability of services and overloading of assets, communication should be engaged between the customer representatives, technical specialists and IT architects to evaluate and agree upon a suitable level of idle (buffer) capacity that should be implemented for contingency purposes. In modern environments that make use of virtualization technologies, the service provider may reduce operational risks by being more agile in the production or reduction of capacity.

6. Market risks

A common risk faced by all types of service providers is the choice that their customers have on sourcing decisions and look to sign contracts with other providers in pursuit of better supporting strategic objectives. Reducing the Total Cost of Utilization (TCU) may be one method to persuade customers to stay so that the costs and risks of switching outweigh the potential benefit. Another strategy may be to expand the service catalogue so that the customers’ scope and depth of requirements are perceived to be met.

Two broad strategies that service providers can use to manage market risks are:

- **Differentiation** – developing and improving assets and services that are not adequately provided by competitors; and
- **Consolidation** – developing and improving assets and services that can be utilized to serve a range of consolidated demand sources (e.g. many customers using websites from a single web server).
7 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; and
- 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.

7.1 Objectives of Service Design

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; and
- To ensure consistent design standards and conventions are followed in all services and processes being designed.
7.2 Benefits of Service Design

While many of the processes within Service Design will not be discussed in this workbook, they all require effective communication channels to exist with the business and customers of the IT organization. Without this communication channel it is likely that Services being released to the production environment do not fulfill some basic requirement, whether it is functional, resource or scheduling in nature.

However, if Service Design is implemented successfully and interfaced using a holistic approach coordinated by Service Level Management, the business and IT organization will benefit by:

- Quality services being designed that satisfy agreed business objectives;
- The design of services occurring within the defined constraints, including timescales, costs, human resources, standards, compliance and regulations;
- The design of effective and efficient processes to be used for managing services throughout their lifecycle;
- The ability to identify and manage potential risks and conflicts so they can be removed or mitigated before services are deployed to the production environment;
- The use of consistent measurement practices and metrics for assessing the quality and performance of the IT Service Management processes being used;
- Secure, consistent, scalable and modular architectures; and
- Improved abilities in supporting enhanced business outcomes by transitioning many strategy and design activities into operational tasks.

Figure 7.2: – Service Design involves a balancing act affected by multiple constraints

© Crown Copyright 2007 Reproduced under license from OGC
7.3 Five Major Aspects of Service Design

Service Design should utilize an integrated approach with appropriate scope to include the design of the following five elements. This means that every time a new service solution is produced it is checked against each of the other major aspects to ensure that it will integrate and interface with all of the other services in existence.

7.3.1 Service Solutions

A formal and structured approach is required to produce new and modified services at the right cost, functionality, quality and within the right time frames.

Actions that should be considered include:

- Analyzing agree business requirements;
- Review existing services and infrastructure to identify common or shared functionality;
- Design the proposed service solutions;
- Evaluate and cost the proposed options and alternatives;
- Agree expenditure and budget;
- Re-evaluate and confirm the business benefits including the Return on Investment (ROI);
- Agree upon the preferred solution(s); and
- Perform a Readiness Assessment from a user, customer and IT operations perspective.

7.3.2 Service Management Systems and tools

The use of appropriate management systems and tools will support and automate a number of the Service Design activities. Out of these systems, the Service Portfolio is the most critical management system used to support all processes and describes a provider’s services in terms of business value. It will also provide assist Service Design by tracking the status of all services through the different stages in the lifecycle. Typical status types used include:

- Requirements: a set of outline requirements have been received from the business or IT for a new or changed service;
- Defined: the set of requirements for the new service are being assessed, defined and documented and the SLR is being produced;
- Analyzed: the set of requirements of the new service are being analyzed and prioritized;
- Approved: set of requirements for the new service have been finalized and authorized;
- Chartered: the new service requirements are being communicated and resources and budgets allocated;
- Designed: the new service and its constituent components are being designed and procured if required;
- Developed: the service and its constituent components are being developed or harvested, if applicable;
- Built;
- Tested;
- Released;
- Operational: the service and its constituent components are operational in the live environment; and
- Retired.

### 7.3.3 Technology architectures

The architectural design activities within an IT organization are concerned with providing overall ‘blueprints’ for development and deployment of the IT infrastructure. In particular relevance to IT Service Management, architectural design normally includes the production of following elements:

- IT policies and strategies;
- Technology architectures; and
- Plans and processes for deployment and subsequent operation.

The work of architectural design needs to assess and reconcile many types of needs, some of which may be in conflict with one another. It should ensure that:

- The IT infrastructures, environments, data and applications and external services serve the needs of the business, its products and services;
- The right balance is struck between innovation, risk and cost whilst seeking competitive edge;
- Compliance with relevant architectural frameworks, strategies, policies, regulations and standards; and
- Coordinated interface is provided between IT designers and planners, strategists, business designers and planners.

### 7.3.4 Processes

With the introduction of any new or modified service, the service provider should assess the need for any new or changed processes that are required in order for the effective and efficient design, transition, operation and subsequent improvements of the service.

See chapter 4.2.1 – *Defining processes* for more detail.
7.3.5 Measurement Systems, methods and metrics

For the effective management and control of the design processes and service themselves there needs to be a formalized approach to monitoring and measurement. The chosen measurements and metrics should reflect the quality and success of the design processes from the perspective of the business, customers and users. They also need to reflect the ability of the delivered solutions to meet the identified and agreed requirements of the business.

There are four types of metrics that are typically used to measure capability and performance of processes:

- **Progress**: milestones and deliverables in the capability of the process;
- **Compliance**: compliance to governance, regulatory requirements and compliance of people using the process;
- **Effectiveness**: accuracy and correctness of the process and its ability to deliver the right result and meet the process objectives defined; and
- **Efficiency**: productivity of the process, its speed, throughput and resource utilization.

7.4 Service Design interfaces with other Service Lifecycle phases

Service Design should be implemented with understanding of the many important interfaces that exist with the rest of the Service Lifecycle. These interfaces will enable an effective feedback loop that will allow the continual development of capabilities for designing services and the associated items listed in 5.5. Some of the interfaces include the following:

**Interfaces with the Service Transition phase:**

- Service Transition should be involved early in the design of services, so that the evaluation of the possible risks, resource requirements and other factors involved can occur;
- Service Asset and Configuration Management will provide identification, control and recording of any service assets required for the design of new and modified services;
- Service Validation and Testing will ensure that sufficient levels of configuration and testing are utilized so that there is an appropriate level of reassurance that the service is fit for purpose and fit for use; and
- Release and Deployment will liaise with Service Design to develop the service and deploy it into the production environment.
Interfaces with the Service Operation phase:
- Service Operation should be provided with the appropriate service targets to be delivered upon;
- Service Operation should provide the Service Design teams with identification of the potential issues and resource requirements for delivering and supporting the service;
- The processes, procedures and documentation required for delivering and supporting the service should be transferred to Service Operation staff;
- Service Operation should communicate with Service Design to ensure that the Service Catalogue is maintained with up-to-date information about currently available services; and
- Service Operation should provide the Service Level Manager with reporting information to be delivered back to the business and customers being served.

Interfaces with the Continual Service Improvement phase:
- Continual Service Improvement (CSI) will provide the coordination and analysis of metrics that will identify potential improvements to be carried out (in part by Service Design);
- CSI will be coordinated by Service Level Management, so that potential improvement actions are optimized according to overall business and IT needs; and
- CSI should provide momentum to the Service Lifecycle, including Service Design, so that the performance, quality and overall customer satisfaction of the IT organization continually improves.
Service Design

- Service Assets, Service Components for budgeting and IT Accounting, Service Level Requirements
- Service Acceptance Criteria, Test Plans, Service Transition Plans, Service Design Packages, Configuration Item information, SLAs, OLAs, UCs

---

Service Strategy

- Support Procedures, User Documentation, Service Catalogues, SLAs, OLAs, UCs, Security & Access Policies

---

Service Operation

- Nominated budgets for delivering and supporting services
- Process metrics and KPIs, Service Portfolios

---

Continual Service Improvement

Figure 7.3: – Some Service Design outputs to other lifecycle phases

©The Art of Service
7.5 Service Level Management

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

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

7.5.1 GOALS AND OBJECTIVES

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.

The specific objectives that SLM should seek to achieve are:

- Define, document, agree, monitor, measure, report and review the level of IT services provided;
- Ensure that specific and measurable targets are developed;
- Provide and improve the relationships and communication practices with customers;
- Monitor and continually improve customer satisfaction;
• Ensure that IT and the customers have clear and unambiguous expectation; and
• Ensure that proactive measures to improve the levels of service delivered are implemented whenever it is cost-justifiable to do so.

Care should be taken that SLM does get implemented in such a way that it becomes too focused on agreements and contracts being developed. The underlying goal still remains to ensure consistency and clarity in the quality of IT service delivery and to provide an effective channel for customers to negotiate and communicate with the IT organization.

### 7.5.2 BENEFITS

There are many benefits from both the customer and IT organization’s perspective to having an effective Service Level Management process in place. Some of the tangible benefits include:

• Consistent interfaces to the business for all service-related issues;
• Agreed service targets and required management information provided to business;
• Mechanisms for providing feedback on the cause of any breach to the targets and detail the action taken to prevent the breach from recurring; and
• Reliable communication channels for customers.

In addition to these, some of the intangible benefits of Service Level Management include:

• Develops the trusted relationship between the IT organization with its customers and business representatives;
• Improved understanding and insight as to the actual and potential offerings that can support business processes;
• Improved customer satisfaction as a result on consistent communication and reporting methods; and
• Improved clarity and understanding as to the performance of IT services and how budgets and money is being utilized.

To assist in the adoption of Service Level Management, each organization should develop its own goal/benefits statements the particular approach taken. For example:

**Goal Statement for Organization X:**

Through a process of continual negotiation, discussion, monitoring and reporting the Service Level Management process aims to ensure the delivery of IT Services that meet the requirements and expectations of our customers and end-users.

Our specific objectives for Service Level Management are:
To seek agreement on expected delivery of IT service by gaining an understanding of the Service Level Requirements from nominated personnel;
To oversee the monitoring of service delivery to ensure that the negotiations regarding the service requirements are not ignored and treated as a once off exercise; and
To provide relevant reports to nominated personnel on a regular basis.

7.5.3 Service Level Agreements

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.

The typical contents for an SLA include:

- 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; and
- 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 are not 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.
To assist in ensuring these guidelines are followed, it is useful to have an independent party, who has not been involved with the SLA negotiation and development, to do a final read-through. By doing so it might highlight potential ambiguities and difficulties that can be addressed and clarified.

### 7.5.3.1.1 Service Level Agreement Structures

Due to the wide range of services, customers and business to be addressed by Service Level Management, consideration should be made as to the most appropriate SLA structure that will be meet the organization’s needs. The three common approaches include Service-based, Customer-based and Multi-level SLAs.

**Service-based SLA**

This structure involves the documentation of an SLA for each service, with the SLA covering all the customers of that service. For example, a Point of Sale (POS) service will have an SLA created that covers all the customers who use the POS as part of the retail business processes.

The service-based SLA is usually preferred by IT as it allows a single document to cover a single service for all customers of that service. It means less administration time spent in negotiating different documents with different customers and less time spent on worrying about accommodating different requirements amongst users.

However, there are potential disadvantages that may arise as a result of a service-based structure. These include:

- Difficulties faced when there are varying requirements across the customers involved for a service; and
- Deciding which customers will sign such an agreement, as it may not be appropriate or feasible for all to sign.

In cases where there is a fairly consistent level of service required across all customers (such as e-mail), then service-based SLAs may be an efficient structure to use. The definition of multiple classes of service (e.g. Gold, Silver and Bronze offerings), may also be used within a service-based SLA to enable some flexibility in offerings.

**Customer-based SLAs**

For this structure, an SLA is documented for a specific customer, covering all of the services they are provided with from the IT organization. In effect, this means that if the IT organization is providing services to ten different customers (e.g. Human Resources, Sales and Marketing, Finance etc.) then there would a requirement for ten SLAs to be
created. In most cases this is the preferred option for customers, as it details all their specific requirements in a single document. The potential disadvantage in using customer-based SLAs may occur when there are common requirements for services across most customers. This could result in the duplication of effort in defining and documenting SLAs for each customer. If this is the case, a combination of both of these structures may be appropriate, providing all services and customers are covered, with no overall or duplication.

Multi-level SLAs
Some organizations have chosen to adopt a multi level SLA structure, where each layer has a different level of focus. While the layers chosen should be appropriate to most effectively meet the organization’s needs, a common approach to multi-level SLAs is as follows:

- **Corporate Level**: covers all generic SLA issues to every customer throughout the organization. These targets should be set at a sufficiently high level to serve as a benchmark for all new services introduced.

- **Customer Level**: covers all SLA issues relevant to a particular customer group or business unit, regardless of the service being used.

- **Service Level**: covers all SLA issues relevant to the specific service, in relation to a specific customer group.

![Figure 6.18: – Typical multi-level SLA structure](image)

Other feasible options that could be used for multi-level SLAs include:

- **Geographic region**: covering all customers in that region. This is useful for international organizations where there are varying requirements between the regions being served.
• **Organization**: covering all customers that exist within an organization that is being provided with services. More specific details can then be provided at the customer level.

• **User group**: covering all services being provided to a particular user group.

• **Premium, Enhanced & Standard**: where customers are defined instead in terms of the level of service being offered.

This kind of structure allows SLAs to be kept to a manageable size, avoids unnecessary duplication, and reduces the need for frequent updates. However, it does mean that extra effort may be required to maintain the necessary relationships and links within the Service Catalogue and the Configuration Management System.

### 7.5.4 SERVICE LEVEL MANAGEMENT ACTIVITIES

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

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

**1. Develop contacts and relationships**

Before starting down the path of creating SLAs and any other associated documentation, SLM should begin seeking opportunities to develop relationships with the business and customers, ideally to foster trust and respect from both sides. All following activities that will later be performed should be performed as part of the development of relationships, rather than simply being focused on their own outputs. Some of the typical actions that should be performed to assist in the development of relationships include:
• Proactively market the Service Portfolio and Service Catalogue and the use of the services within all areas of the business;
• Promote service awareness and understanding;
• Identify and communicate the responsibilities of the business, customers and users in relation to IT;
• Regularly plan and facilitate customer and user group sessions to promote the use of IT services; and
• Proactively communicating issues that may affect service quality to customers and users.

2. Designing an SLA framework (already covered, see section 6.5.3.1.1)

3. Determine, document and agree requirements for new services

Before the documentation of SLAs occurs, Service Level Management is required to work with the customers to create a draft of their Service Level Requirements (SLRs). Other areas of IT Service Management will need to be consulted at this point, such as Capacity and Availability Management, as to whether the proposed targets are realistic and can be achieved. While normally an organization will first document SLRs for existing services, practices should be agreed for creating SLRs when new services are being developed or purchased. The SLRs are created to provide the applicable design criteria for services, which will then be an input into a cycle of negotiating, agreeing, documenting and monitoring the associated SLA(s).

4. Negotiate and develop SLAs

As the development of SLAs requires involvement from many internal and external stakeholders, the development of a final SLA will involve multiple cycles and drafts before an agreed document is accepted. The SLRs already captured should provide the majority of the input into the SLA, however over the review period, SLM should ensure that all aspects are adequately described and that the SLA will provide an effective benchmark for the level of IT service quality to be delivered.

For the majority of services being developed, any defined SLA will normally be monitored over the term of a warranty period before its final acceptance, which seeks to ensure that the targets defined can be consistently met, and so that any previously unanticipated issues are accounted for.

5. Review and revise SLAs, underpinning agreements and service scope

When SLAs are being produced, Service Level Management will be required to work in partnership with Supplier Management in the identification and documentation of Operational Level Agreements (OLAs) and Underpinning Contracts (UCs).
Operational Level Agreements are agreements with the other internal IT groups documenting the specific back-to-back targets for each of the elements in the delivery and support of services. Service Level Management is responsible for the documentation and continued maintenance of OLAs.

Underpinning Contracts are agreements with external suppliers documenting the specific back-to-back targets and responsibilities for each of the elements in the delivery and support of services. Supplier Management is responsible for the documentation and continued maintenance of UCs. SLM in coordination is responsible for ensuring that there the Underpinning Contracts in place are aligned to the needs of the business, customers and associated SLAs.

As the Underpinning Contracts are used in managing the provision of products, services or support from an external supplier, they will normally be implemented in a formal manner using documented agreements or contracts. OLAs on the other hand typically aren’t as complicated or as extensive, but in some way clearly identify the back-to-back targets for each support group. This may be included in the job descriptions, internal team metrics or some other appropriate mechanism.

Just like SLAs, OLAs and UCs should be monitored continually, with reports on achievements provided as feedback to the appropriate supplier or managers of each support team.

6. Monitoring service performance against SLAs
Before targets were agreed for documentation in SLAs, it should have been ensured that there were capabilities for effectively monitoring and measuring these targets at the agreed frequency. Many organizations fail to ensure this, and as a result experience a loss of customer faith in the SLM process.

Monitoring must be performed from the customer and user perspective, which means that simply ‘pinging the server’, is not good enough to indicate service availability and performance. Monitoring must include all components forming the end-to-end service (which in itself might be difficult and costly to implement) so that a true picture of the user experience can be gained. The generation of synthetic transactions to monitor the transaction response time of an end-to-end service is the common approach used to monitor service availability and performance for IT services in a production environment.

For describing approaching performance, the SLA may include a statement such as:

‘The services covered by the SLA are designed for high-speed response and no significant delays should be encountered. If a response time delay of more than x seconds is experienced for at least 15 minutes, or a time-out error is displayed, the user should report this immediately to the Service Desk.’

The collection of incident/problem, service request handling achievement should also be provided by their relevant process managers, which will need to be compared against the targets documented in the SLAs. While technical instability may well be the cause of many user disruptions, the quality of response from the IT organization plays a major factor in forming a positive or negative experience for the customer and users. Where possible the collection and synthesis of these metrics should be automated by using integrated Service Management Tools, and complemented by the manual collection of customer feedback and random satisfaction surveys.

7. Produce service reports

Service Level Management reports help identify future trends and allow review of the “health” of the process. Setting a security level on certain reports may be appropriate as well as categorizing the report as Strategic, Operational or Tactical. The acid test for a relevant report is to have a sound answer to the question; “What decisions is this report helping management to make?”

While operational reports will normally be produced on a frequent basis, exception reports should be produced whenever an SLA is broken or when defined thresholds are breached. The SLA should document all agreed reporting requirements, including the contents and frequency of reports, which can also be used for service review meetings to be held at a later date.

The workload for collating and producing these reports should not be underestimated, and unless SLM is appropriately staffed those involved can easily be consumed by the
workload involved here. To assist, SLM should be provided with business oriented reports from other areas of service management, so that the time and effort required to manage and communicate them to customers is reduced.

8. Conduct service reviews and instigate improvements within an overall Service Improvement Plan (SIP)

Periodic review meetings must be held on a regular basis with customers to review the service achievements in the last period and to preview any issues for the coming period. SLM needs to foster the relationship with customers and gain commitment that they will be proactively involved in the meetings, highlighting the importance of the meetings and mutual benefits for both parties. So that the meetings are effective, actions must be placed on the customer and service provider as appropriate to improve weak areas where targets are not being met. All actions must be taken as minutes, and progress should be reviewed at the next meeting to ensure that action items are being followed up and properly implemented.

Particular attention should be focused on each breach of service level to determine exactly what caused the loss of service and what can be done to prevent any recurrence. Reports should also be produced on the progress and success of the Service Improvement Plan (SIP), such as the number of SIP actions that were completed and the number of actions that delivered their expected benefit.

Where necessary, Service Level Management should also identify particular aspects covered in OLAs and UCs that might need improvement, or where allocation of resources are not optimal in accordance with business needs.

9. Collate, measure and improve customer satisfaction

While SLM will certainly be concerned with ensuring appropriate performance and quality in the services delivered to customers, the importance of ‘soft’ issues and their affect on customer satisfaction should not be underestimated. Despite frequent disruptions customers may still generally feel positive (especially if IT seems to be seeking to address and correct the issues). At the same time, when SLA targets are being met customers may feel dissatisfied (e.g. for the general helpfulness of Service Desk staff).

So that the soft issues can be monitored, SLM activities should include some of the following methods:

- Periodic questionnaires and customer surveys;
- Customer feedback from service review meetings;
Feedback from Post Implementation Reviews (PIRs) conducted as part of the Change Management process on major changes, releases, new or changed services etc;

- Telephone perception surveys (perhaps at random on the Service Desk, or using regular customer liaison representatives);
- Satisfaction survey handouts (left with customers following installations, service visits etc.);
- User group or forum meetings; and
- Analysis of complaints and compliments.

Improvement actions developed to improve elements of customer satisfaction should be documented and implemented as part of the ongoing SIP.

10. Managing complaints and compliments

Too often customers and IT focus on the issues and frustrations currently occurring, and forget the successes that have been achieved by both groups over time. Accordingly, SLM should ensure that there are mechanisms for recording and managing both complaints as well as compliments (normally via the Service Desk). While complaints should be escalated to the appropriate parties and resolved to the satisfaction of the originator, compliments should be also promoted and communicated to IT staff, customers and users on a regular basis.

7.5.5 TRIGGERS AND INTERFACES

Several triggers will cause reason for the execution of SLM activities, including:

- Request for Changes (RFCs);
- SLA breaches;
- Compliments and complaints;
- Actions identified from service review meetings;
- Customer satisfaction surveys;
- Financial and budget exceptions; and
- Changes in strategy or policies.

To enable effective execution, typical inputs to SLM include:

- Business Information – strategy plans, financial plans etc;
- Business Impact Analysis – information on impact, risk etc;
- Business Requirements – agreed, new, changed requirements;
- Service Strategy – policies and constraints;
- Service Portfolio and Service Catalogue;
- Change information – change schedule;
- Customer and user feedback; and
- Other – including advice from other processes (e.g. Capacity Management, SLAs, SLRs and OLAs and past service reports etc).

Information produced by SLM as outputs include:

- Service Reports – detailing service level achievements, breaches, outcomes from discussions;
- Service Improvement Plan – inc. all services and processes;
- Service Quality Plan – overall improvement of service quality;
- Document templates – format and content for SLAs etc;
- Service Level Agreements – targets and responsibilities etc;
- Service Level Requirements – SLRs for new and changed etc;
- Operational Level Agreements – each internal support team;
- Service Review Meeting minutes and actions;
- SLA Review and service scope review meeting minutes; and
- Revised contracts – e.g. changes to SLAs and SLRs etc.

### 7.5.6 KEY PERFORMANCE INDICATORS (KPIS) OF SERVICE LEVEL MANAGEMENT

Care should be taken when designing the appropriate metrics to be used by SLM, as inadequate coverage of objective and subjective measures will mean that the customer and IT perspectives may not be suitably represented.

Some of the metrics typically used include:

- Per cent reduction in SLA targets missed;
- Per cent reduction in SLA targets threatened;
- Per cent increase in customer perception and satisfaction of SLA achievements, via service reviews and customer satisfaction survey responses;
- Per cent reduction in SLA breaches caused because or 3rd party support contracts (UC); and
- Per cent reduction in SLA breaches caused because of internal OLAs.

Further KPI’s can be agreed for managing business interface:

- Increased per cent of services covered by SLAs;
- Documented and agreed SLM processes and procedures;
- Reduction in the time taken to respond to/implement SLA requests;
- Increased per cent of SLA reviews completed on time;
- Reduction in per cent of outstanding SLAs for annual renegotiation;
- Reduction in the per cent of SLAs requiring corrective changes;
- Per cent increase in the coverage of OLAs and 3rd party contracts; and
• Documented evidence that issues raised at review meetings are being followed up and resolved.

7.6 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 Design. 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.
7.6.1 Goals and objectives

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

7.6.2 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); and
• 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.

7.6.3 Benefits

By ensuring the development and constant upkeep of an accurate Service Catalogue, many benefits will be delivered to both customers and also the IT organization, including:

• An accepted, widely accessible and consistent central source of information;
• Ensures all areas of the business can view an accurate, well communicated picture of all IT services, their details and status;
• Contains customer-facing view of IT services in use, how they are intended to be used, business processes they enable and the quality of service to be expected; and
• Reduction in the resources required for Service Level Management and other associated processes/staff in managing communication with customers in relation to information already captured by the Service Catalogue.

7.6.4 What should the Service Catalogue represent?

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

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

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

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

- **Business Services** – that what is actually used and seen by the customer.
- **Supporting Services**, including further definition as:
  - Infrastructure Services.
  - Application Services.
  - Network Services.
  - Data Management Services.
- **Shared and Commodity Services**.
- **Externally provided Services** – those provided/managed by a 3rd party
  organization.

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

<table>
<thead>
<tr>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
</tr>
<tr>
<td>SERVICE A</td>
</tr>
<tr>
<td>E.g. Accounts System</td>
</tr>
<tr>
<td>E.g. Email</td>
</tr>
<tr>
<td>E.g. Intranet</td>
</tr>
<tr>
<td>E.g. Internet</td>
</tr>
<tr>
<td>Service x</td>
</tr>
<tr>
<td>Service x</td>
</tr>
<tr>
<td>Service x</td>
</tr>
</tbody>
</table>

Figure 6.15: – Identifying customers of defined services

In the earlier stages of process implementation, the Service Catalogue will normally be
recorded by means of a matrix, table or spreadsheet. However, as time progresses and
maturity of Service Management develops, many organizations will begin to integrate and
maintain their Service Catalogues (and Service Portfolios) as part of the Configuration Management Systems. When this occurs and Services themselves are represented as a Configuration Item (CI), it provides the capability for identifying and relating the effect of incidents and problems on services offered. As this becomes more widely adopted throughout more Service Management activities, the need to ensure that modifications to the Service Portfolio and Service Catalogue are controlled by Change Management significantly increases.

After the investigation and definition of services occur and discussions held with customers, IT staff and external suppliers, the information and knowledge gathered will be structured to produce a meaningful Service Catalogue. In effect, the knowledge and information of the Service Catalogue is logically divided into two aspects:

- **A Business Service Catalogue** which 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.

- **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 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.
Service Level Management should provide input as to the various internal (Operational Level Agreements) and external (Underpinning Contracts) that are required to support the service.

### 7.6.5 Service Catalogue Management Activities

As the nature of Service Catalogue's can vary greatly as can their method of implementation, the activities required to design and maintain them will need to be evaluated appropriately. As a minimum the activities within Service Catalogue Management process should include:

- Agreeing and documenting a service definition with all relevant parties;
- Interfacing with Service Portfolio Management to agree the contents of the Service Portfolio and Service Catalogue;
- Producing and maintaining a Service Catalogue and its contents, in conjunction with the Service Portfolio;
- Interfacing with the business and IT Service Continuity Management on the dependencies of business units and their business processes with the supporting IT services contained within the Business Service Catalogue;
- Interfacing with support teams, suppliers and Configuration Management on interfaces and dependencies between IT services and the supporting services, components and CIs contained within the Technical Service Catalogue; and
- Interfacing with Business Relationship Management and Service Level Management to ensure that the information is aligned to the business and business process.
7.6.6 Triggers and Interfaces

When implemented effectively, Service Catalogue Management should play an integral part of a coordinated approach for managing Service Offerings & Agreements. The major trigger resulting in modification or addition to the Service Catalogue are Request For Changes (RFCs) from Change Management, which should be identifying and evaluating changes in the business and customer requirements for services. This includes the addition of new services, modifications to and retirement of existing services.

Potential triggers and interfaces to consider when implementing Service Catalogue Management are shown below:

![Figure 6.17: – Triggers and interfaces for Service Catalogue Management](image)

**Figure 6.17: – Triggers and interfaces for Service Catalogue Management**
7.6.7 Key Performance Indicators (KPIs) of Service Catalogue Management

Demonstrated success of the Service Catalogue Management process is typically seen in the form of two main metrics:

- The number of services recorded and managed within the Service Catalogue as a percentage of those being delivered and transitioned in the live environment. This indicates the effective coverage of the service catalogue and value, especially from the customer perspective; and
- The number of variances detected between the information contained within the Service Catalogue and the ‘real world’ situation. This includes services missing from the catalogue or those that should be removed, as well as informational detail being incorrect (e.g. incorrect pricing).

Other measurements that may also be applicable include:

- Business users’ awareness of the services being provided, i.e. percentage increase in completeness of the Business Service Catalogue against operational services;
- Improved IT staff awareness of available services and the supporting services and components; and
- Utilization of self-help mechanisms associated with the Service Catalogue (e.g. procurement, Frequently Asked Questions, ability to log and track Service Requests and Incidents).
7.6.8

7.7 Supplier Management

To quote a long established phrase that most have heard, “No man is an island”. The phrase comes from a longer quotation by John Donne (1572-1631); and while himself a Christian, the concept is shared by many religions, principally Buddhism. The general meaning of the phrase (and longer quotation) is that human beings do not thrive when isolated from others, we are all connected and therefore events and changes affecting another human being affects us all.

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

What does this mean for IT Service Management and the practices involved in Service Offerings & Agreements? Well based on this principle, we need to ensure that we carefully evaluate, select, manage and review any suppliers who will be involved in some way in the delivery and support of IT services, and be sure to develop and foster the relationship in a mutually beneficial way. As many organizations have found out recently, the death of a supplier (caused by a severe economic downturn) may well mean their own future existence could be short lived. “...never send to know for whom the bell tolls; it tolls for thee”.

7.7.1 Goal and objectives

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; and
- Maintain a supplier policy and a supporting Supplier and Contract Database (SCD).

Each service provider will have a formal process (and often specific department responsible) for the management of all suppliers and contracts. The processes should
adapt to cater for the importance of the supplier and/or the contract and the potential business impact on the provision of services.

### 7.7.2 Benefits

When implemented effectively as part of a coordinated approach to Service Offerings & Agreements, Supplier Management can provide benefits such as:

- Improved alignment of services to meet business needs;
- Improved response and resolution for escalated incidents and service requests to suppliers;
- Increased per cent of agreements with suppliers documented in Underpinning Contracts;
- Optimized use of resources through economies of scale provided by external suppliers;
- Improved relationship between suppliers and the service provider; and
- Performance of suppliers is measured and reported frequently.

---

**Figure 6.20: – Roles and interfaces for Supplier management**

© Crown Copyright 2007 Reproduced under license from OGC
7.7.3 Type of Supplier Arrangements

The arrangements can take between the service provider and their external suppliers can take many forms. The chosen arrangement will normally be based on the type of external support required, capabilities of both the service provider and supplier and the size of the contract being evaluated.

The typical arrangements formed with external suppliers include:

**Co-sourcing:** An informal combination of in-sourcing and outsourcing, using a number of outsourcing organizations working together to co-source key elements within the lifecycle. For large contracts involving potentially high risks and costs, it is unlikely that informal arrangements will be utilized.

**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 functions(s) in a low cost location. Common examples are human resources, 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. Forms of consulting fall within this type.

**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 required for building the service components themselves.

7.7.4 Underpinning Contracts

The contents of a basic underpinning contract or service agreement (if binding legal commitments are deemed unsuitable) includes, but is not limited to, the following:

- Basic terms and conditions;
• Service description and scope;
• Service standards;
• Workload ranges;
• Management Information;
• Responsibilities and dependencies;
• Service debit and credit regime (incentives and penalties applicable);
• Additional performance criteria;
• Confidentiality and announcements;
• Intellectual property rights and copyright;
• Termination rights of each party; and
• Obligations at termination and beyond.

7.7.5 Supplier Management Activities

Depending on the value, importance, risk and impact (see Supplier Categorization, section 6.6.6) of the supplier arrangement being formed, the following methods and activities will be scaled appropriately based on the requirements of the situation.

7.7.5.1.1 Evaluation of new suppliers and contracts

When selecting a new supplier there are a multitude of factors that may influence the decision on the type of arrangement or choice of supplier, including such items as:

• Existing relationships;
• Politics within the organization;
• Availability of ‘off the shelf’ products and services;
• Price;
• Reputation in the market place;
• Location;
• Risk; and
• Certification against relevant ISO standards.

Regardless of what influences the final decision, it is important that any reasoning is identified and the impact fully assessed to ensure costly mistakes are avoided.

Formal partnering relationships established at an executive level are a change from traditional arrangements, where the supplier acts subordinately to the customer organization. In these cases there are mutually beneficial reasons for strategic partnerships, with the relationship being characterized by:

• **Strategic alignment**: of culture, values and objectives, leading to an alignment of business strategies;
• **Integration**: a close integration of the processes of both organizations;
- **Information flow**: good communication and information being exchanged, especially at the strategic level;
- **Mutual trust**: between the two organizations within the relationship;
- **Openness**: when reporting service performance, risks and costs;
- **Collective responsibility**: for tasks to be performed and goals achieved; and
- **Shared risk and reward**: to agree how investment costs and resulting benefits are shared.

### 7.7.6 Supplier Categorization

![Figure 6.21: Supplier Categorization](image)

Supplier Management should be flexible, with more time and effort given to managing key suppliers than to less important suppliers (see above). To do this there must be a process for categorizing suppliers in accordance to their overall importance. A common method for categorization is assessing risk and impact associated with using the supplier, together with the value and importance of the supplier.

The outcomes of supplier categorization are typically defined into the following categories:

- **Strategic**: Seen in significant partnering relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans. Greatest focus is maintained for this category of suppliers.
**Tactical:** Involving partnering with suppliers for significant commercial activity and business interaction. These relationships would normally be overseen by middle management and would involve regular contact, reviews and improvement programs.

**Operational:** Used when partnerships with suppliers involve the operational management or support of products or services. Normally managed by junior operational management and involve infrequent but regular contact and review.

**Commodity:** When partnerships with suppliers exist to provide low value or readily available products/services which could be alternatively sourced easily.

### 7.7.6.1.1 Maintenance of the Supplier and Contracts Database (SCD)

To assist in improving the efficiency of managing supplier contracts and agreements and ensuring auditability of all required information, a Supplier and Contracts Database (SCD) should be established, together will clearly identified roles and responsibilities.

![Figure 6.22: – Supplier and Contracts Database (SCD)](image)

© Crown Copyright 2007 Reproduced under license from OGC

Ideally the SCD should form an integrated element of a comprehensive CMS or SKMS, 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. This will also contribute to the information held in the Service Portfolio and Catalogue.

When implemented correctly, the SCD can be used to promote preferred suppliers and prevent purchasing of unapproved or incompatible items. By coordinating and controlling the buying activity, the organization is more likely to be able to negotiate preferential rates.

The SCD should contain at least the following items:

- Supplier details;
- Summary of product/service;
- Ordering processes; and
- Contract details.

### 7.7.6.1.2 Supplier and Contract Management and Performance

Within the Service Operation lifecycle phases (but still an activity of Supplier Management) the organization will need to ensure that there are integrated processes in place for managing the daily interfaces and communication that will occur with the supplier. As an example:

- How will incidents be passed from the Service Desk and other lines of support to the supplier?
- Will both the organization and supplier use the same database for incidents and requests?
- Is the supplier expected to conform to the organization’s Change Management (or other) processes?

Once agreed on all required matters, two levels of formal review will need to take place throughout the contract lifecycle to minimize risk and ensure the business realizes maximum benefit from the contract:

- **Service/Supplier performance reviews** – reports on performance should be produced on a regular schedule based on the category of supplier and should form the basis of service review meetings.

- **Service, service scope and contract reviews** – also conducted on a regular basis, at least annually for major suppliers. The goal of these reviews is the review of the service, overall performance, service scope and targets and the contract, together with any associated agreements. Typical topics include:
  - Service Performance against targets;
  - Incidents and problem reviews, including any escalated issues;
  - Business and customer feedback;
Initiatives to improve the services provided by the supplier are controlled through SIPs, dealing with any failures, weaknesses or opportunities identified. Satisfaction surveys should also complement any performance reports, as just in the case of SLAs, while breaches may not have occurred there may still be dissatisfaction with the service.

7.7.6.1.3 Contact renewal and/or termination

Contract reviews must be undertaken on a regular basis to ensure the contract is continuing to meet business needs. Contract reviews assess the contract operation holistically and at a more senior level than service reviews that are undertaken at an operational level.

These reviews should consider:

- How well the contract is working and its continued relevance;
- Whether any changes are needed;
- What is the future outlook for the relationship;
- Commercial performance of the contract, reviews against benchmarks;
- Guidance on future contract direction; and
- Supplier and contract governance.

When there has been an identified need for the change of supplier, normal steps to perform include:

- Performing Impact and Risk Analysis on the supplier transition;
- Making commercial assessment of the exit costs;
- Seeking legal advice on the termination terms, applicable notice periods and mechanisms, and any other consequences; and
- Reassessing the market to assess benefits for changing suppliers.

These elements should always be agreed when forming the agreement with the supplier, but should be reviewed when a transition is being considered and executed.

7.7.7 Key Performance Indicators (KPIs) of Supplier Management

KPIs indicating the performance and quality of the Supplier Management process can be grouped into the following categories:

- Business protected from poor supplier performance or disruption.
- Increase in the number of suppliers meeting the targets within the contract.
- Reduction in the number of breaches of contractual targets.

- **Supporting services and their targets align with business needs and targets.**
  - Increase in the number of service and contractual reviews held with suppliers.
  - Increase in the number of supplier and contractual targets aligned with SLA and SLR targets.

- **Availability of services is not compromised by supplier performance.**
  - Reduction in the number of service breaches caused by suppliers.
  - Reduction in the time required to resolve escalated incidents and problems.

- **Clear ownership and awareness of supplier and contractual issues.**
  - Increase in the number of suppliers with nominated supplier managers.
  - Increase in the number of contracts with nominated contract managers.
7.8 Availability Management

The identification of the patterns and size of demands for IT services (by Demand Management) will lead to a further analysis of what availability levels will need to be provided in any new or modified service offerings under development. However, simply knowing that there will be some demand does not mean that it will be automatically served by the IT organization, for reasons of cost-effectiveness, security or because of some dependence on other services or infrastructure components. Additionally, the provision of availability isn’t just a matter of ensuring that the various IT hardware and software components are available, it also requires that adequate support arrangements and processes are in place to assist in the identification and resolution of any service-affecting disruptions.

Availability Management plays a very important (but often misunderstood) role within the Service Design phase, ensuring that the requirements for availability of services and associated resources are clearly understood and achieved in the most optimal fashion.

Why is all of this so important? From a user and customer perspective, the availability (or unavailability) of services being provided has a large impact on their perception and satisfaction experienced. Additionally, through effective planning, communication and support processes, even in the event of disruption the satisfaction of customers and users can be maintained.

7.8.1 Goals and objectives

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 objectives include providing the capabilities to:
- Produce and maintain an up-to-date Availability Plan;
- Provide advice and guidance;
- Ensure availability achievements meet or exceed agreed targets;
- Assist with diagnosis and resolution of availability related incidents and problems;
- Assess impact of all changes on the Availability Plan; and
- Ensure frequent proactive measures are taken to optimize and improve the availability of services are implemented where it is cost-justifiable.
7.8.2 Scope

While primarily a Service Design process, there are many elements involved in Availability Management that interact throughout the Service Lifecycle. Using a combination of both proactive and reactive activities, the scope of the process covers design, implementation, measurement, management and improvements of IT service and component availability.

In order to achieve a balance between cost-effectiveness and appropriate quality, Availability Management is involved in the determination and fulfillment of the requirements for availability, including an in-depth understanding of:

- The current business processes, their operation and requirements;
- Future business plans, objectives and requirements;
- Service targets and the current IT service operation and delivery;
- IT infrastructure, data, applications and environments and their performance (in terms of stability, redundancy, useful life span); and
- Business impacts and priorities in relation to the services and their usage.

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

While implementations will vary depending on the organizational requirements for Availability Management as well as a number of both internal and external influencing factors, as a general guide the process should include some adoption of the following activities:
Proactive Activities (primarily executed in Service Design and Service Transition):

- The development and maintenance of an Availability Plan, which documents the current and future requirements for service availability, and the methods used to meet these requirements;
- Development of a defined set of methods, techniques and calculations for the assessment and reporting of availability;
- Liaison with IT Service Continuity Management and other aligned processes to assist with risk assessment and management activities; and
- Ensuring consistency in the design of services and components to align with the business requirements for availability.

Reactive Activities (primarily executed in Service Operation and Continual Service Improvement):

- Regular monitoring of all aspects of availability, reliability and maintainability, including supporting processes such as Event Management for timely disruption detection and escalation;
- Regular and event-based reporting of service and component availability;
- Ensuring regular maintenance is performed according to the levels of risk across the IT infrastructure; and
- Assessing the performance of and data gathered by various Service Operation processes such as Incident and Problem Management to determine what
improvement actions might be made to improve availability levels or the way in which they are met.

### 7.8.3 Guiding principles in the adoption of Availability Management

In many instances the principles of Availability Management are lost when the process is implemented in an organization that may not have developed a “service focus” centred on the experience of customers and users. In situations like these it is common to see the level of availability calculated by such criteria as “the ability to ping the XYZ server”. While this server may well be a vital component for a given service, there are many other factors that can also affect and disrupt service, all of which do impact the user experience of availability. To avoid this approach, Availability Management should be implemented with a strong emphasis on understanding and meeting the needs of the business and customers. Principles that should underpin such an approach include the following:

- Service availability is at the core of customer and user satisfaction, and in many cases business success;
- Unavailability can be properly managed through effective processes and communication to still achieve user, customer and business satisfaction;
- Service availability is only as good as the ‘weakest link in the chain’. If an external supplier is that weak point, then consideration needs to be given as to how to manage that weakness. Addressing other Single Points of Failure (SPOF) within the IT infrastructure can also greatly improve availability;
- Availability Management is both proactive AND reactive, the more disruptions that can be predicted and circumvented, the higher the level of service availability; and
- The costs of addressing availability later in the lifecycle of a service are much higher than those incurred in designing the service effectively from the start. Additionally, once a service develops a poor reputation (perhaps from frequent unavailability) it becomes difficult to change the image.

### 7.8.4 Basic Concepts for Availability Management

The following concepts are fundamental to the understanding and application of Availability Management and will be referenced throughout the rest of the chapter.
<table>
<thead>
<tr>
<th>Terminology</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Availability</td>
<td>The ability of a service, component or CI to <em>perform its agreed function when required</em>. It is typically measured and reported as a percentage using the following formula:</td>
</tr>
</tbody>
</table>
|                  | \[
|                  | \text{Availability (\%)} = \frac{\text{Agreed Service Time} - \text{Downtime}}{\text{Agreed Service Time}} \times 100\% \]
|                  | This means that if a service is only partly functional, or the performance is degraded to a point outside of normal service operation, then the service should be classed as unavailable.                                                                 |
| 2. Service Availability | Involves all aspects of service availability and unavailability and the impact of component availability, or the potential impact or component unavailability on service availability.                                                                                     |
| 3. Component Availability | Involves all aspects of component availability and unavailability.                                                                                                                                                  |
| 4. Reliability   | A measure of how long a service, component or CI can perform its agreed function without interruption. This metric provides an understanding of the frequency of disruption and is often reported as Mean Time Between Service Incidents (MTBSI) or Mean Time Between Failures (MTBF). It is typically calculated with the formulas: |
|                  | \[
|                  | \text{Reliability (MTBSI)} = \frac{\text{Available time in hours}}{\text{Number of service disruptions}} \]
|                  | \[
|                  | \text{Reliability (MTBF)} = \frac{\text{Available time in hours} - \text{Total Downtime in hours}}{\text{Number of service disruptions}} \]
| 5. Maintainability | A measure of how quickly and effectively a service, component or CI can be restored to normal operation after a failure. This metric is typically measured and reported as the Mean Time to Restore Service (MTRS), which includes the entire time from the start of the disruption until the full recovery. The following formula is normally used: |
|                  | \[
|                  | \text{Maintainability (MTRS)} = \frac{\text{Total downtime in hours}}{\text{Number of service disruptions}} \]
<p>|                  | <strong>EXAMPLE:</strong> For a service that is provided 24 x 7 and running for a reporting period of 5020 hours with only two disruptions (one of 6 hours and one of 14 hours), the following metrics would result: |</p>
<table>
<thead>
<tr>
<th>Availability (%)</th>
<th>[ \frac{5020 - 20}{5020} \times 100% = 99.60% ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability (MTBSI)</td>
<td>[ \frac{5020}{2} = 2510 \text{ hours} ]</td>
</tr>
<tr>
<td>Reliability (MTBF)</td>
<td>[ \frac{5000}{2} = 2500 \text{ hours} ]</td>
</tr>
<tr>
<td>Maintainability (MTRS)</td>
<td>[ \frac{20}{2} = 10 \text{ hours} ]</td>
</tr>
</tbody>
</table>

**6. Serviceability**

The ability of an external (third-party) supplier to meet the terms of their contract. Often this contract will include agreed levels of availability, reliability and/or maintainability for a supporting service or component.

**7. Vital Business Function (VBF)**

Defined business critical elements of a business process that are supported by an IT service. While many functions are supported by IT, we typically prioritize our efforts and resources around supporting the critical elements, including the use of redundant and highly resilient components.

Certain VBFs may need special designs which are now used commonly in key infrastructure components (such as servers), which include the following four concepts:

- **High Availability**
  - A characteristic of the IT service that minimizes or masks the effects of component failure to the users of a service.

- **Fault tolerance**
  - The ability of a service, component or CI to continue to operate correctly after failure of a component part.

- **Continuous operation**
  - An approach or design to eliminate planned downtime of an IT service. This may mean that individual components are disrupted during maintenance, but the IT service as a whole remains available.

- **Continuous availability**
  - An approach or design to achieve theoretical 100% level of service availability. Multiple design factors will support this to occur, but more stringent requirements will also be assessed first, including environmental and other factors.
7.8.5 Availability Management Activities & Techniques

The following activities for Availability Management have been grouped into either proactive (primarily in Service Design or Service Transition) or reactive activities (those part of Service Operation or Continual Service Improvement).

7.8.5.1 The proactive activities of Availability Management

The following activities are those that should be consistently utilized in the planning and design of services (as part of a coordinated approach including Service Strategy, Service Design and Service Transition).

1. Identifying the business requirements for availability

Availability Management should work in conjunction with other Service Design processes such as Service Level Management, Information Security Management and Capacity Management so that the requirements for availability can be understood, both in terms of the business and customer requirements, but also for the impact and dependency or relationship with other aspects of Service Design. For example, understanding what level of capacity is required in order to sustain a certain level of availability.

While Service Level Management will act as the primary process by which discussions are held with customers to define their requirements, as a minimum Availability Management should produce the following:

- Definition of the Vital Business Functions (VBFs). So that efforts and resources are optimized around those critical elements of business processes being supported by IT services. As one of the first inputs into Availability Management, Service Level Management should seek to ensure that when defining and refining the customers' and businesses’ requirements, special consideration is given to identifying which elements must be protected, as opposed to those functional elements that may not be as business-critical. Various techniques will then be utilized to protect those VBFs such as implementing redundant and fault tolerant systems as well as protecting any potential Single Point of Failure (SPOF);
- Definition of what actually constitutes IT service downtime, including the minimum functional and performance levels that are required;
- Definition of the business impact caused by a loss of the IT service, together with the associated risk of this occurring;
- The required service hours (e.g. Monday to Saturday, 6am to 6pm);
- An assessment of the relative importance of different working periods (e.g. between 4pm and 6pm is most critical);
- Quantitative availability requirements, including the maximum length of disruption that can be sustained, and the frequency of disruption that can be tolerated;
• Specific security requirements; and
• Capabilities for service backups and recovery of service following disruptions.

As this will be an iterative process which includes elements of Service Strategy, there will be multiple assessments as to whether an effective balance has been proposed between availability and cost. The steps to assist in defining this balance include:

• Determining the business impact caused by a loss or degradation of service (user productivity losses & other financial impacts felt);
• Determining the requirements (both internal and external) for supporting the proposed service availability levels;
• Through assessment with the associated business or customers, determine whether the costs identified in meeting the proposed availability levels are justified; and
• Where these are seen as cost-justified, begin to define the availability, reliability, maintainability and serviceability requirements for documentation into Service Level Agreements, Operational Level Agreements and Underpinning Contracts.

2. Designing for availability

Once an agreed level of availability is defined by balancing the business requirements for availability against the resources required to sustain it, Availability Management will utilize a number of components, techniques, processes and supporting systems to ensure the service is designed appropriately and can be supported in Service Operation. Some of the elements required in order to meet increasing service availability levels include:

• Quality controlled components and products;
• Systems Management (including monitoring and, diagnostic and recovery capabilities);
• Service Management processes (including Event, Incident and Problem Management);
• High availability-designs (including the elimination of SPOFs and the implementation of redundant components and systems to minimize or avoid disruption); and
• Special Solutions with full redundancy, through the use of multiple redundant components, systems and sites with strict testing and quality assurance measures being used for each of these elements.
3. **Designing for recovery**

These activities are concerned with ensuring that in the event of an IT service failure or disruption, the service and its various supporting components can be restored as quickly as possible so that business operations can resume. In many cases there won’t be any business justification to build a highly-available service, however suitable availability levels may still be provided by swift and effective resolutions to manage any disruptions that do occur.

Some of the elements involved in designing for recovery include:

- Implementing Systems management for monitoring and escalating any Events that may lead to a service disruption;
- Developing internal and external processes and procedures to be used to maintain availability and resolve disruptions; and
- Improving the capability of the people involved in Service Operation with ongoing training and awareness sessions.

To assist in this goal, there should be appropriate communication and shared involvement for these activities between both the staff involved in design as well as those involved in the operation and support of services.

The actual capabilities and mechanisms used for the recovery of service disruptions will be covered by in section 6.3.5.2 *The reactive activities of Availability Management*.

---

*Figure 6.4: – The various elements required to provide Service Availability*

© Crown Copyright 2007 Reproduced under license from OGC
Component Failure Impact Analysis (CFIA) can be used to predict and evaluate the impact on IT service arising from component failures within the technology. The output from CFIA can be used to identify where additional resilience and redundancy should be considered to prevent or minimize the impact of component failure to the business operation and users.

This is particularly important during the Service Design stage, where it is necessary to predict and evaluate the impact on IT service availability arising from component failures with the proposed IT Service Design. CFIA is a relatively simple technique that can be used to provide this valuable information. In addition, it can also be applied to identify impact and dependencies on IT support organization skills and competencies amongst staff supporting the new service. This activity is often completed in conjunction with IT Service Continuity Management and Capacity Management.

The outputs of CFIA are used in a number of ways in both planning for availability as well as planning for recovery. These include:

- The impact that component failure can have on users and business operations;
- Component and people dependencies;
- Relative component recovery sequences timeframes;
- Identified areas where specific recovery plans and procedures may be required; and
- Identified components that may need some risk reduction measures implemented.

One of the main methods for performing a CFIA is by developing a matrix that illustrates what IT services depend on what component Configuration Items (CIs). This may come from the Configuration Management System or from other sources of infrastructure information. This matrix will be populated using the following rules:

- Leave a blank when a failure of the CI does not impact a service in any way;
- Insert an ‘X’ when the failure of the CI causes the service to be inoperative;
- Insert an ‘A’ when there is an alternative (e.g. redundant) CI to provide the service; and
- Insert an ‘M’ when there is an alternative CI, but it requires manual intervention for the service to be recovered.

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Service 1</th>
<th>Service 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC 1</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Laptop 1</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Switch 1</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WAN</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Switch 2</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Switch 3</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Data Centre</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Once completed there will be consideration into the following aspects:

- If a CI has a large number of Xs this indicates it is critical to a number of services and its failure can result in a high impact to the business. It may also indicate that this particular CI is a potential Single Point of Failure; and

- If an IT service has a large number of Xs it indicates it is a potentially complex configuration that has a higher vulnerability level to failure.

The same exercise as above can be completed from a different perspective; instead mapping how the components of a single IT service relate to Vital Business Functions and various user groups.

While the above example is a valuable for understanding particular risks in the infrastructure and IT services, an advanced CFIA can provided a more detailed analysis including such fields as:

- **Component availability weighting**: a weighting factor based on the impact of failure or service as a whole. As an example, this might be based on the percentage of users from the entire user community being affected (e.g. 500 out of 2000 users would be 0.25 or 25 per cent);

- **Probability of failure**: based on the reliability of the component or service, typically measured in MTBF;

- **Recovery time**: the predicted recovery time for the service or CI;

- **Recovery procedures**: to verify that an effective recovery procedure exists;

- **Device independence**: used to verify CIs where necessary have been implemented independently; and

- **Dependency**: to show dependency between CIs.

### 5. Single Point of Failure Analysis

A Single Point of Failure (SPOF) Analysis can be performed to identify the components that have no backup or fail-over capabilities, and have the potential to cause disruption to the business if it fails. For any SPOFs detected, the information gained from a CFIA can be used to evaluate whether the cost for its remediation can be justified.
6. **Fault Tree Analysis**

By performing a Fault Tree Analysis (FTA) either in the design of services or as part of a review of a Major Incident or Problem it provides an understanding of the chain of events that causes a disruption to IT services. The analysis makes use of Boolean notation for the events that occur in the fault tree, and are combined using a number of logic operators to understand the potential result.

![Fault Tree Analysis Diagram](image)

**Figure 6.5: – Example Fault Tree Analysis**

© Crown Copyright 2007 Reproduced under license from OGC

The typical logic operators used for understanding the combination of events include:
- **AND-gates**: where the result occurs only when all input events occur simultaneously;
- **OR-gates**: where the result occurs when one or more of the input events occur;
- **Exclusive OR-gate**: where the result only occur when one and only one of the input event occurs; and
- **Inhibit gate**: where the result only occurs when the input condition is not met.

7. **Risk Analysis and Management**

As part of the coordinated approach by the various Service Lifecycle processes in regards to Risk Analysis and Management, Availability Management should contribute by identifying potential risks to and inherent in the infrastructure, provide analysis of vulnerability to these risks and the impacts associated with them, and what countermeasures might be used to mitigate this risks in a cost-effective manner.
All organizations should define their own formal approach to Risk Analysis and Management to ensure complete coverage and sufficient confidence in their strategy. A generic framework that can be applied across all areas of an organization to assist in this is Management of Risk (M_o_R) which is another best practice framework published by the Office of Government Commerce (OGC). This framework adopts a systematic approach for the identification and assessment of risk and implementation associated countermeasures.

Some of the key elements focused on by the M_o_R framework include providing direction for organizations to:

- Develop a transparent, repeatable and adaptable framework;
- Communicate the risk policy and its benefits clearly to all staff and stakeholders;
- Assign accountability and responsibility to key individuals in senior management;
- Ensure the culture of the organization is motivated to embed risk management initiatives;
- Ensuring that risk management supports the organization’s objectives; and
- Adopting a no-blame approach to monitoring and reviewing risk assessment activities.

![Image of Risk Analysis and Management](https://via.placeholder.com/150)

**Figure 6.6: – Risk Analysis and Management**

© Crown Copyright 2007 Reproduced under license from OGC

More information regarding risk management will also be covered in 6.5: IT Service Continuity Management.

8. **Planned and preventative maintenance**

All IT components should be subject to a planned maintenance strategy. The frequency and levels of maintenance required varies from component to component, taking into
account the technologies involved, criticality and the potential business benefits that may be introduced.

Planned maintenance activities enable the IT support organization to provide:

- Preventative maintenance to avoid failures;
- Planned software or hardware upgrades to provide new functionality or additional capacity;
- Business requested changes to the business applications; and
- Implementation of new technology and functionality for exploration by the business.

Where the business hours required for services is not 24/7 then the scheduled maintenance can be performed outside of business hours without impacting IT service availability. Even in the case of services that are designed for continuous availability, there are typically some time periods that are less critical that might need to be used for maintenance, with degraded performance of the service potentially being an accepted result. Once the agreed schedule for planned and preventative maintenance has been defined and agreed, these will normally be documented in:

- SLAs, OLAs and Underpinning Contracts;
- Change Management Schedules;
- Release and Deployment Management Schedules; and
- Intranet/Internet pages that communicated schedules and unscheduled outages to the end-user community.

9. Production of the Projected Service Outage

Availability Management is also responsible for the documentation and communication of the Projected Service Outage (PSO) document, which consists of any variations to agreed levels of service availability in SLAs based on input from:

- The change and release schedules;
- Planned and preventative maintenance schedules;
- Testing schedules; and
- IT Service Continuity Management and Business Continuity Management testing schedules.

The PSO is used to ensure that all variations to agreed availability levels are understood and agreed by all relevant stakeholders. During its use any additional maintenance windows that might be required should be communicated appropriately by the Service Desk to all relevant parties.
10. Continual review and improvement

As part of the Continual Service Improvement phase, Availability Management should seek to ensure that any previous issues and missed targets are considered for their appropriate correction. However, even if a service provider may have met all their agreed targets for service availability in the previous reporting period, there will still be improvement actions that can be developed in some way. Why? Because the business requirements for availability always change!

As a result it is important that Availability Management does seek to continually identify ways in which to optimize the availability of the IT infrastructure, by either increasing availability or reducing the costs and resources required to do so. Other potential improvement actions may result in more qualitative benefits, such as enhanced user and customer satisfaction during disruptions that occur.

To ensure that critical business developments and changes are also considered, other input should be evaluated on a regular basis from ITSCM, particularly from the updated Business Impact Analysis and Risk Analysis exercises.

7.8.5.2 The reactive activities of Availability Management

The following activities are those that should be consistently utilized in the ongoing delivery and support of IT services in regards to availability. Although under the overall responsibility of Availability Management, they do include operational activities performed by a range of staff, including those involved in Service Operation.

Monitor, measure, analyze and report service and component availability

While many organizations have monitored availability traditionally from a component perspective, they have not necessarily been able to utilize this information to be understand the business and user experience of availability. Typical measures focus on different aspects of availability and reported as availability percentages, time lost and frequency of failure. These traditional measures include:

- Per cent available;
- Per cent unavailable – which might be better used to emphasize shortcomings of availability;
- Duration of downtime (in hours and minutes);
- Frequency of failure – demonstrating the number of failures during the reporting period; and
- Impact of failure - the real measure of unavailability, which requires close integration with effective Incident and Problem Management processes.
However, many organizations and businesses have realized that these traditional methods for reporting availability are no longer adequate in communicating the user and business experience of availability and unavailability. Alternatively, when the objectives for monitoring and reporting are defined in the context of the business and user perspective a more representative view of the overall quality of IT services is achieved. Some methods that might be employed with this approach include defining:

- Impact by user minutes lost – calculated by multiplying the length of disruption by the number of users affected; and
- Impact by business transaction – calculated by assessing the number of business transactions that could not be processed during the period of disruption.

In any case, the methods utilized by Availability Management should be appropriate to the organization’s business processes and operational models. If there are a wide range of automated and electronic processing actions performed without actual user involvement, then simply measuring based on user impact will not be sufficient.

To enable efficiency of the process, Availability Management should seek to implement and integrate all useful (but cost-effective) monitoring systems, information sources and reporting mechanisms to reduce the complexity and resources required for information gathering, analysis and reporting. When done effectively, it will also streamline the production of the agreed regular reports, including normal monthly availability reporting, the Availability Plan, Service Failure Analysis (SFA) and CFIA reports.

**Unavailability analysis**

As part of justifying the costs of implementing and executing the Availability Management process, analysis should be made as to the actual costs incurred during periods of disruption or unavailability. The tangible costs are typically well defined and understood, such as:

- Lost user productivity;
- Lost IT staff productivity;
- Overtime payments;
- Lost revenue;
- Wasted goods and materials;
- Imposed fines or penalty payments; and
- Injuries or potential safety incidents caused.

While these are of course important, there are also a number of intangible costs that can also have potentially long-lasting negative effects on the organization and the service provider. Such intangible costs of unavailability include:

- Loss of customers;
- Loss of customer satisfaction;
- Loss of business opportunity;
- Damage to business reputation;
- Loss of confidence in the IT Service Provider; and
- Damage to staff morale.

While they may be difficult to measure they shouldn’t be simply dismissed, and should form part of the focus of customer and user surveys performed by Service Level Management.

**The Expanded Incident Lifecycle**

As already discussed earlier in the principles of Availability Management, even when disruptions occur there are still methods that can be utilized by which user and customer satisfaction is still maintained. One way to help achieve this goal is by ensuring that the duration of any disruption is minimized so that normal business operations are resumed as quickly as possible and the impact on the associated business processes and users is reduced. By analyzing the various time elements making up those disruptions it will help Availability Management target any improvement actions, be it through technology enhancements, additional documentation and procedures or staff training and education. This is can be performed by analyzing the ‘expanded incident lifecycle’, which breaks down all the major stages through which all incidents progress.

The major stages of incidents can be classed as:

![Diagram of the expanded incident lifecycle](image_url)

*Figure 6.7: – The expanded incident lifecycle*

© Crown Copyright 2007 Reproduced under license from OGC
1. Incident detection
2. Incident diagnosis
3. Incident repair
4. Incident recovery
5. Incident restoration.

Each stage, and the associated time taken, influences the total downtime perceived by the user and business. By evaluating each of the stages it enables Availability Management to identify potential areas of inefficiency that result in a longer disruption to the user. These improvements may be focused on the detection mechanisms, the documentation supporting diagnosis, repair and recovery, the escalation procedures utilized or any other activity or task involved during the incident lifecycle. As a consequence, Availability Management needs to work closely with Incident and Problem Management to ensure any improvement actions optimize the use of resources and prevent the recurrence of the incidents where possible. Event Management may also be coordinated to ensure that there is appropriate coverage of CIs with the ability to detect events that may lead to service disruptions.

1. Incident detection

This stage encompasses the time between the actual failure or disruption to a CI or IT service occurring and the moment at which the service provider is made aware of that incident. A variety of tools and systems should be employed that have capabilities to detect events and incidents and, consequently reduce the detection timeframe that occurs. For critical CIs, the same systems and tools should also be utilized to trigger automated recovery with scripted responses. When implemented effectively many incidents will be detected and resolved before the users have even been impacted in any noticeable way.

2. Incident diagnosis

This stage encompasses the timeframe between which the IT service provider has been made aware of the incident to the time where the underlying cause of the incident has been determined. Particularly at this stage there is an appropriate balance that needs to be developed between the need to capture diagnostic data and the need to have the incident restored. While capturing a range of diagnostic data will often extend the restoration time, it will also enhance the capabilities for preventing the recurrence of those incidents.

Other than information potentially gathered from users, input for the successful diagnosis of the incident may come from:

- Data captured by the failing CI(s);
3. Incident repair

This stage encompasses the repair time required for the incident, including both the automated and manual techniques that might be needed. The repair time is shown independently from the recovery time, with this stage focusing on the actual techniques that initiate the resolution of the incident, including:

- Actions to repair or restart a failed CI;
- Activities performed by external suppliers for the repair of CIs under their control; and
- Documentation of the procedures used to assist in the future diagnosis and repair of similar incidents.

The agreed timeframes for the response and repair of incidents should be documented in SLAs, OLAs and Underpinning Contracts, and continuously monitored for compliance.

4. Incident recovery

This stage encompasses the activities to recover service availability (but distinct from the repair activities previously mentioned). This can include activities such as:

- The initiation for backups to be effectively restored;
- The activities required to recover lost or corrupt data;
- Utilizing spare equipment (including those within the Definitive Spares) to be implemented in the production environment to facilitate recovery; and
- The actions and time required to restore an image to a desktop machine following a failure.

When designing new IT services the recovery requirements for each supporting component CI should be identified as early as possible to facilitate the development of the associated recovery plans and procedures to be used when failures occur.

5. Incident restoration

This stage encompasses the time from when the recovery steps are completed, through to the time that the service provider has confirmed that normal business and IT service operation has resumed. In some situations, this will be performed by Service Desk staff, who simply call the affected users for confirmation that service been restored to them. In other cases, particularly those which support automated business processes, a synthetic
transaction or user-simulation test script may need to be executed to ensure that the restored IT service is working as expected.

**Service Failure Analysis**

Service Failure Analysis (SFA) is a technique designed to provide a structured approach to identifying the underlying causes of service interruptions to the user and business operations. SFA utilizes a variety of sources to assess where and why shortfalls in availability are occurring. This technique enables a holistic view to be taken to drive improvements to the IT support organization, processes, procedures and tools. The staff utilized in an SFA would typically be those also involved in Incident and Problem Management, so the activities here will be jointly performed by these processes.

Some of the key high-level objectives of SFA are to:

- Improve the overall availability of IT services by producing a set of improvements for implementation or input into the plan;
- Identify underlying causes of service interruption to users;
- Enable enhanced levels of service availability without incurring major costs;
- Assess the effectiveness of the IT support organization and key processes;
- Develop cross-functional teams to reduce silos that may exist;
- Produce detailed reports of major findings and recommendations; and
- Ensure that Availability improvements derived from SFA-driven activities are measured.

![Figure 6.8: The high-level structure for a Service Failure Analysis (SFA)](image)
7.8.6 Challenges faced by Availability Management

Some of the major challenges faced when implementing or operating Availability Management include:

- A lack of business commitment to the process;
- A lack of timely communication and consultation regarding future business plans and strategies;
- Lack of appropriate systems management tools to make reporting an efficient activity; and
- The focus is incorrectly placed on the technical perspective of availability rather than the business and user perspective.

7.8.7 Key Performance Indicators (KPIs) of Availability Management

The metrics for evaluating effective provision of service availability and reliability are:

- 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 MRBSI; and
- Reduction in MTRS.

The metrics for evaluating business alignment of Availability Management are:

- Percentage improvement in user and business satisfaction of services (including availability levels);
- Percentage reduction in business critical time failures; and
- Percentage reduction in the number of transactions not able to be processed.

The metrics for evaluating efficiency of Availability Management are:

- Percentage reduction in the cost of unavailability;
- Percentage reduction in the costs involved in Service Delivery;
- Percentage reduction in the overtime hours worked as a result of unavailability;
- Reduced time to document Availability Plan; and
- Reduced time required to complete SFA.
7.9 Capacity Management

7.9.1 Goals and objectives

The primary goal of Capacity Management is to ensure that cost-justifiable IT capacity in all areas of IT exists and is matched to the current and future agreed needs of the business in a timely manner.

Other objectives of Capacity Management are to:
- Produce and maintain an up-to-date Capacity Plan;
- Provide advice and guidance;
- Ensure service performance meets or exceeds agreed targets;
- Assist with diagnosis and resolution of performance and capacity related incidents and problems;
- Assess impact of all changes on the Capacity Plan, services and resources; and
- Ensure proactive measures to improve performance of service are implemented, where cost-justifiable.

7.9.2 Scope

While the focal point of Capacity Management is to ensure adequate performance and capacity of IT services are being developed and already delivered, there are many supporting elements including IT components, product and software licenses, physical sites, human resources and third party products that will all need to be managed appropriately for this goal to be achieved. As a result, while many activities will be the responsibility of other IT Service Management or general organizational management processes (such as managing human resources), Capacity Management will be involved in the high level planning of each of these elements.

As a general guide, Capacity Management seeks to understand and support:
- The current business operation and its requirements, through the patterns of business activity (provided by Demand Management);
- The future business plans and requirements (provided by Service Portfolio Management);
- The agreed service targets for performance and capacity (provided by Service Level Management); and
- All areas of IT technology in regards to the requirements for capacity and performance.

When implemented effectively, Capacity Management can help to ensure that there are no surprises with regard to service and component design and performance.
7.9.3 Principles of Capacity Management

In coordination with the processes of Financial Management and Demand Management, Capacity Management seeks to provide a continual optimal balance between supply against demand, and costs against resources needed.

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

In the above figure, capacity is only implemented when disruptions begin to occur as demand has exceeded supply. While the implemented capacity does work to resolve the disruptions, there are some consequences to this type of reactive behavior including:
• IT infrastructure components being purchased that don’t optimally fit the requirements or architecture;
• Budget overruns for the unforeseen and unanticipated purchases;
• Periods of time where there are potentially large amounts of excess capacity;
• Reduced customer and user satisfaction with the affected IT services; and
• A general negatively affected perception of the IT organization as a whole.

7.9.4 Capacity Management Activities

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

7.9.4.1 Business Capacity Management

Business Capacity Management is the sub-process that covers the activities responsible for ensuring that the future business requirements for IT services are considered and evaluated in terms of their potential impact on capacity and performance. As business plans, operations and processes continually change, this will consequently affect the service provider’s ability to satisfy the business and customers requirements, including those already documented in SLAs.

Some of the primary inputs into Business Capacity Management that trigger the activities here come from:
• Project and Program Management;
• Change Management;
• Service Portfolio Management (as investments are evaluated and authorized);
• Patterns of Business Activity (from Demand Management); and
• New Service Level Packages and Service Level Requirements (from Service Level Management).

The activities that are recommended to be performed within the context of Business Capacity Management are:
• Assisting with the development of Service Level Requirements;
• To design, procure or amend service configuration;
• To advise on appropriate or revised SLA targets;
• To support SLA negotiations; and
• To assist in the evaluation and control of proposed Change Requests.

When Capacity Management is provided with early opportunities to be involved with these processes then the planning and design of IT capacity and performance can be closely
aligned with business requirements and provisioned in an optimal and cost-effective manner.

7.9.4.2 Service Capacity Management

The primary focus of the Service Capacity Management sub-process is to monitor and analyze the use and performance of IT services and ensure that they meet their agreed SLA targets. The regular monitoring of service capacity and performance, and comparison against normal service levels will identify trends, breaches or any near misses that might occur.

As a result, this process will need to work closely with Service Level Management to understand the agreed levels of service and to report back any targets achieved and breached, and concerns or advice in regards to capacity and performance issues. There will also need to be process integration with Incident and Problem Management so that there is early detection of disruptions where the root cause may be due to insufficient capacity being provided, as well as appropriate action taken to resolve the disruption so that agreed business targets are still met.

7.9.4.3 Component Capacity Management

The objective of Component Capacity Management is to ensure that the implementation and management of each of the individual components that support IT services is performed effectively to deliver optimum capacity and performance to meet business needs. This includes the constant monitoring and analysis of each component to understand the performance, capacity and utilization characteristics that exist. This sub-process is a vital component to the overall quality of Capacity Management, as each component does have a finite capacity that, when reached, will begin to impact on the service levels being delivered and business operations being supported.

While much of the actual monitoring will be performed within Service Operation, the direct feedback should be provided to Component Capacity Management to interpret this data and take corrective action where necessary. There is a proactive side to the sub-process as well, and where possible there should be forecasting of any issues or events that might occur so that proper planning and preventative maintenance can be performed.

Other than the previously mentioned elements, there are three typical activities that occur within the Component Capacity Management sub-process:
1. **Exploitation of new technology**

As new technologies emerge, the IT service provider should seek to evaluate whether they might be able to deliver enhanced capacity and performance levels in a more cost-effective manner than those already used. Recent examples of technologies that have been used successfully in this manner include virtualization, cloud computing and blade server implementations.

2. **Designing resilience**

In conjunction with Availability Management, there should be analysis as to where it is cost-effective to build resilience into the infrastructure, by assisting in techniques such as a Component Failure Impact Analysis (CFIA) and other risk assessment management activities. Depending on the availability levels that have been agreed, Capacity Management will evaluate what level of spare capacity of infrastructure components are required to meet these targets, and strive to ensure these requirements are considered early in the design stage of new or modified services.

3. **Threshold management and control**

Within Service Operation, there should be an ongoing set of monitoring and control activities that assist in providing assurance that agreed service levels are being delivered and protected. In the context of Capacity Management, there should be thresholds set for various components and services that raise warnings and alarms when approached or breached. Event Management will be primarily involved to support this capability and ensure that an appropriate level of capacity events are monitored and escalated to avoid staff being flooded with alerts.

### 7.9.4.4 Common Capacity Management Activities

So that each of the three sub-processes of Capacity Management operate effectively, there are some common activities that should be employed at each level (when necessary). The two most important activities in this regard are:

1. **Modelling and trending**

One of the major benefits provided to the Service Design phase by Capacity Management, is the capability to predict the behavior of IT services under certain conditions. This may be a given volume of utilization by users, a particular type of use or a combined variety of work being performed.
There are many different types of modeling techniques that rely heavily on simulation and mathematical calculations, so depending on the size and complexity of the new or modified service offering, there may be very little or quite comprehensive modeling performed.

The main techniques utilized for modeling include:

- **Baselining** – where a baseline of current performance and capacity levels is identified and documented;
- **Trend analysis** – where services and components are monitored over time for their utilization to assist in the identification of trends and the potential forecasting of future utilization and performance levels;
- **Analytical modeling** – where mathematical techniques are used to predict the performance levels that might be achieved under certain conditions or after making modifications to the infrastructure. Analytical modeling is typically quicker and cheaper to perform than Simulation Modeling, but also typically provides less accurate results; and
- **Simulation modeling** – where a set of discrete events are modeled and compared against a defined hardware configuration. This will often involve simulation transactions across the service and infrastructure, and as a result will typically yield more accurate results.

2. **Application Sizing**

Application sizing is an activity that begins during the early design of a new or modified service and ends when the service has been accepted into the production environment. The sizing activities relate to all elements and components required for service, including estimation of the required capacity levels of hardware, data, environments and applications that are involved.

The main objective is to accurately estimate the resource requirements needed to support a proposed change and ensure that it meets its required service levels. This includes consideration as to the resilience measures that might be required to deliver a set level of capacity, performance and availability. This will be an iterative process, including constant negotiation with Service Level Management to define a cost-effective approach that satisfies the business objectives.

While some aspects of quality may be improved after implementation (including adding additional hardware and other components), in most cases quality must be built in from the start, otherwise much higher costs are incurred trying to fix issues once the service is in production.
7.9.4.5 Operational Activities of Capacity Management

Whereas the previously mentioned activities of application sizing and modeling are those primarily executed in the design stages of a service, the following activities are the common *operational* activities that are performed across the three sub-processes. The major difference between the sub-processes and their use of these activities comes down to the data being collected and the perspective from which it is analyzed. For example, Component Capacity Management is concerned with the performance of individual components, where Service Capacity Management is concerned with the performance of the entire service, monitoring transaction throughput rates and response times.

![Figure 6.10: The operational activities of Capacity Management](https://example.com/figure6.10.png)

© Crown Copyright 2007 Reproduced under license from OGC

1. Utilization monitoring

The monitoring applied should be specific to a particular CI, whether it is an IT service, an operating system, a hardware configuration or application. It is important that the monitors can collect all the data required by Capacity Management for each of the three sub-processes.

Some of the typical monitored data collected include:

- Processor utilization;
- Memory utilization;
- Per cent processor per transaction type;
- Input/output rates;
- Queue lengths;
- Disk utilization;
- Transaction rates;
- Response times;
- Database usage;
- Index usage;
- Hit rates;
- Concurrent user numbers; and
- Network traffic rates.

When collecting data intended for use by the Service Capacity Management sub-processes, the transaction response time for services may be monitored and measured by:

- Incorporating specific code within client and server applications software;
- Using ‘robotic scripted systems’ with terminal emulation software;
- Using distributed agent monitoring software; and
- Using specific passive monitoring systems.

2. Analysis

The data collected by the various monitoring activities and mechanisms will then be used to identify trends, baselines, issues and conformance or breaches to agreed service levels. There may be other issues identified such as:

- Bottlenecks within the infrastructure;
- Inappropriate distribution of workload across the implemented resources;
- Inefficiencies in application design;
- Unexpected increased in workloads and input transactions; and
- Scheduled services that need to be reallocated.

3. Tuning

After analysis of collected data has occurred, there may be some corrective action that is required in order to better utilize the infrastructure and resources to improve the performance of a particular service. Examples of the types of tuning techniques that might be used include:

- Balancing workloads – transactions may arrive at the host or server at a particular gateway, depending where the transaction was initiated; balancing the ratio of initiation points to gateways can provide tuning benefits;
- Balancing disk traffic – storing data on disk efficiently and strategically, e.g. striping data across many spindles may reduce data collection;
- Definition of an acceptable locking strategy that specifies when locks are necessary and the appropriate level, e.g. database, page, file, record and row delaying the lock until an update is necessary may provide benefits; and
- Efficient use of memory – may include looking to utilize more or less memory depending upon the circumstances.
Before implementing any of the recommendations arising from the tuning techniques, it may be appropriate to consider using one of the on-going activities to test the validity of the recommendation.

4. Implementation

The objective of implementation is to control the introduction of any changes identified into the production environment. Depending on the changes required, this may be implemented via a normal change model (using all the normal steps of Change Management) or a standard change where there is already change approval and an established procedure for the work required.

1.1.1 Challenges affecting Capacity Management

The main challenges that effect the successful implementation and execution of Capacity Management include:
- Persuading the business to provide information on its strategic business plans;
- Combining Component Capacity Management data into a set of integrated information that can be analyzed in consistent manner to provide details of the usage of all components of the services; and
- Handling the amounts of information produced by Capacity Management, especially in the sub-processes of Component Capacity Management and Service Capacity Management.

1.1.2 Key Performance Indicators (KPIs) of Capacity Management

Measures for evaluating the performance and contributions of the Capacity Management process include:
- Production of workload forecasts on time;
- Percentage accuracy of forecasts of business trends;
- Timely incorporation of business plans into the Capacity plan;
- Reduction in the number if variances from the business plans and Capacity plans;
- Increased ability to monitor performance;
- Timely justification and implementation of new technology in line with business requirements;
- Reduction in the use of old technology, causing breached SLAs due to problems with support or performance;
- Reduction in last minute buying to address urgent performance issues;
- Reduction in over-capacity of IT; and
- Accurate forecasts of planned expenditure.
7.10 IT Service Continuity Management

7.10.1 Goals and objectives

The primary goal of IT Service Continuity Management (ITSCM) is to support the overall Business Continuity Management practices of the organization by ensuring that the required IT Infrastructure, and the IT service provision, can be recovered within the required and agreed business time scales.

Other objectives include to:
- Maintain a set of IT Service Continuity Plans and IT recovery plans;
- Complete regular Business Impact Analysis (BIA) exercises;
- Conduct regular Risk Analysis and Management;
- Provide advice and guidance;
- Ensure appropriate continuity and recovery mechanisms are in place;
- Assess the impact of all changes on ITSCM plans and procedures;
- Ensure that proactive measures to improve the recovery mechanisms for services are implemented; and
- Negotiate and agree on necessary contracts with suppliers (with Supplier Management).

7.10.2 Scope

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

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

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

- The agreement of the scope of the process and the policies adopted;
- Business Impact Analysis (BIA) to quantify the impact a loss of IT service would have on the business;
- Risk Analysis;
- Production of an overall ITSCM strategy that must be integrated into the BCM strategy;
- Production of ITSCM plans;
- Testing of plans; and
- Ongoing education and awareness, operation and maintenance of plans.

### 7.10.3 Principles of IT Service Continuity Management

A lifecycle approach should be adopted when setting up and operating an ITSCM process. This diagram shows the lifecycle of ITSCM, from initiation through to continual assurance that the protection provided by the plan is current and reflects all changes to identified risks, services and service levels.

![Figure 6.11: Lifecycle of IT Service Continuity Management](image)

© Crown Copyright 2007 Reproduced under license from OGC

If there has already been extensive work performed in the context of Business Continuity Management (BCM- focusing on the capabilities and resources required to continue business operations during and following a disaster), then this will provide excellent input into the initiation of IT Service Continuity Management. However, in many cases the work of BCM has not yet been performed or is still ongoing, in which case these two aligned processes should work together so that an appropriate strategy can be developed and cost-effective decisions can be made. In other scenarios where BCM is entirely absent,
ITSCM is required to fulfill many of the requirements and activities of BCM. This chapter, however, will assume that BCM process has been established and appropriate plans and documents are in place.

7.10.4 IT Service Continuity Management Activities & Techniques

The activities of ITSCM are divided into the lifecycle stages as shown in the previous diagram.

7.10.4.1 Stage 1 – Initiation

The initiation stage covers the activities required to align IT Service Continuity Management to Business Continuity Management and to define the overall approach taken. These activities are:

1. Policy setting

A policy should be established and communicated as soon as possible to set out the management intention and objectives for the BCM and ITSCM initiatives.

2. Specify terms of reference and scope

Part of the policy documented will cover the scope and responsibilities of the staff involved. This includes tasks such as risk assessments, BIAs and the ‘command and control’ structure required to manage the business interruption. Other issues considered are any outstanding audit issues, regulatory, insurance or client requirements and compliance with other standards such as BS7999 (Security Management) or ISO 20000.

3. Allocate resources

The development of a suitable environment for BCM and ITSCM to operate requires considerable resources in terms of money and staffing. Depending on the maturity of the organization, external consultants may be required to assist with the various activities, and there may be a requirement for some training and education so that the stage 2 activities can be performed.

4. Define the project organization

Successful implementations have shown that it is beneficial to use a standard project planning methodology such as PRINCE 2 PMBOK, complemented by project-planning tools. The appointment of an experienced project manager who reports to a steering committee and guides the work groups is a vital factor for success.
5. **Agreed project and quality plans**

One of the controlling elements in the project will be quality plans that ensure deliverables are achieved to an acceptable level of quality. The extent to which these activities need to be considered during the initiation process depends on the contingency facilities that have been applied within the organization. This activity also provides a vehicle by which to communicate the resource requirements for the project, thus working towards gaining ‘buy-in’ from management and all necessary stakeholders.

7.10.4.2 **Stage 2 – Requirements and Strategy**

Stage 2 covers the activities that evaluate the requirements for continuity as well as the development of an overall strategy in regards to the plans, measures and practices that will be used.

1. **Requirements – Business Impact Analysis (BIA)**

The Business Impact Analysis (BIA) seeks to quantify the range of impact that a loss of service will have. Some forms quantified for the damage a loss of service may cause include:

- Lost income and incurred costs through overtime payments or fines paid;
- Damaged reputation;
- Decreased competitive advantage;
- Decreased customer satisfaction and perception of the IT service provider;
- Potential threat of injury or loss of life;
- Immediate and long-term; and
- Breach of law, regulations and compliance requirements.

Each form of impacts is measured against particular scenarios for each business process, such as an inability to invoice for a period of 3 days leading up to Christmas.
The level of impact felt by business operation will also change depending on the length of disruption. Figure 6.12 shows how some disruptions will immediately cause a significant impact on business operations, whereas other disruptions won’t impact immediately, but grow over the length of time that the disruption endures. This analysis will influence the approach and measures taken, primarily either being focused on risk reduction (being able to withstand failures) or recovery (to bring back the affected IT services over a period of time).

Some other aspects identified by the BIA include:

- Staffing and skills necessary to continue operating at acceptable levels;
- Time within which minimum staffing, facilities and services should be recovered;
- The time within which all required business processes and operations should be partially and fully recovered; and
- The relative priority of each business process being supported by IT services.

The views represented by the BIA should encompass all levels of the organization as well as any other stakeholders that might be affected.
2. Requirements – Risk Analysis

Another activity performed in order to determine the requirements of IT Service Continuity Management is that of Risk Analysis. This involves the assessment of the existing threats that might cause disruption as how vulnerable the organization is to that threat. This activity as a result is a joint responsibility of ITSCM, Availability Management and Information Security Management.

A standard and defined methodology should govern the use of Risk Analysis and Risk Management activities within the organization. One particular methodology that might be used is the Management of Risk (M_o_R) framework, which is shown in the figure to the right.

The M_o_R approach adopts the following principles when applied:

- **M_o_R principles** which are derived from corporate governance principles and are essential for developed good practices for risk management.
- **M_o_R approach** which documents the agreed approach for the organization, including dynamic documents such as:
  - Risk Management policy;
  - Process guides;
  - Plans;
  - Risk registers; and
  - Issue logs.
- **M_o_R processes** which consist of four main steps:
  - Identifying threats and opportunities;
  - Assessing the effect of threats and opportunities;
  - Planning to reduce the threats and maximizing opportunities; and
  - Implementing the corrective action and reviewing where the results do not meet expectations.
- **Embedding and reviewing M_o_R** to continually review and improve the practices for Risk Management.
- **Communication** which ensures that appropriate communication occurs, with plans documented to ensure staff members and stakeholders know their responsibilities and who the audience for communication should be.
Using their chosen methodology, the organization should develop and maintain a risk profile, which classifies risks on scales of severity and likelihood to occur. This profile will also show which risks have been determined to be acceptable, and for those deemed unacceptable there are some risk reduction or recovery measures required.

3. **IT Service Continuity Strategy**

The results of the BIA and Risk Analysis will be used by BCM and ITSCM to begin developing appropriate strategies in response. Overall, the strategy should represent a balance between risk reduction and recovery options, as well as a balance between the cost of developing and maintaining these options against the impact felt if the risks do eventuate.

Typical measures for used for *risk reduction* include:
- UPS and backup power systems to computers, servers and other infrastructure;
- Systems designed with fault tolerance when any downtime is unacceptable (involves multiple redundancy with load sharing and/or automated failovers);
- RAID arrays for disk storage;
- Spare equipment such as routers, switches, desktops and laptops to be used in the case of component failure;
- Off-site storage for backups and for failover systems; and
- Multiple suppliers for critical sub-services (e.g. WAN and internet connections).

Typical measures for *recovery* include:
- *Manual workarounds* – such as using paper-based systems for a limited timeframe;
• **Reciprocal arrangements** – where two or more organizations share the costs associated in developing and operating some shared facilities that can be used in the case of a disaster occurring;

• **Gradual recovery** – aka. ‘cold standby’ where the recovery facilities provide empty accommodation equipped with power, network cabling and telecommunications connections. Over the course of the disruption the provider moves in and configures any infrastructure required to recover service;

• **Intermediate recovery** – aka. ‘warm standby’ where the recovery facilities (often provided by third parties) provide the accommodation for necessary staff and house’s preinstalled infrastructure to be used for recovery. The actual recovery however will take some time as the infrastructure will need to be re-configured as well as ensuring that applications and data can be restored from backups;

• **Fast recovery** – aka. ‘hot standby’ where the recovery facilities house dedicated infrastructure for the organization to utilize in the case of disruption. In the event of a failure the organization can then initiate failover to the recovery site, initiate any backups to restore and recover service within a 24 hour period; and

• **Immediate recovery** – aka ‘hot standby’ provides recovery facilities that support the immediate restoration of services, with potentially no visible impact on the business operations itself. This is often implemented in such a way that the organization houses dedicated equipment at an alternative site (often far enough away to not be affected by the same risk such as blackouts or weather events). In some cases the IT services actually being protected by this recovery option will only be those that support a vital business function.

It is important that the strategy includes a combination of measures, so that the balance between cost and risk as well as prevention and recovery is obtained. The plan should document where staff will be located, as well as how other critical services are managed such as power, water, telecommunications, couriers and information management.

### 7.10.4.3 Stage 3 – Implementation

Once the defined strategy has been approved, the IT Service Continuity Plans need to be produced and integrated with the Business Continuity Plans (BCP). Whereas the BCP documents what IT services are required and the timescales for their expected recovery, the IT Service Continuity Plans address all the activities required to ensure the service, facilities and resources needed are delivered in an acceptable operational state within the agreed timescales. These plans also document the resilience measures built into the infrastructure that enable recovery, as well as information to facilitate decisions regarding whether to invoke the plans or not. This element is especially important, as the people normally responsible to make these decisions may be injured or unavailable.
The plan should be under the control of Change Management to ensure integrity, but also be made widely available to key staff at all times. This requires both electronic and physical (multiple) copies to be maintained, as well as some off-site storage of these documents. To facilitate its use in the case of disaster there should be a checklist that covers specific actions that are required during all stages of the recovery, including those actions to evaluate whether normal service operation has resumed.

Other documents that will also be integrated with the BCP and IT Service Continuity Plans are the:
- Emergency Response Plan;
- Damage Assessment Plan;
- Salvage Plan;
- Vital Records Plan;
- Crisis Management and Public Relations Plan;
- Accommodation Plan;
- Security Plan;
- Personnel Plan;
- Communication Plan; and
- Finance and Administration Plan.

**Testing**

As any recovery plans are being implemented, there is a requirement for sufficient testing to be undertaken to ensure the plan’s effectiveness, including walk-through tests, full and partial tests and, a scenario test. These tests will also need to be conducted as part of Stage 4 – *Ongoing operation* as required.

### 7.10.4.4 Stage 4 – Ongoing Operation

As part of the continual assurance that the recovery plans will be successfully utilized if/when necessary, there are a set of operational activities that should be performed in accordance to the documented policy. These activities consist of the following:

- *Education, awareness and training* – this should cover the organization and the IT organization, for service continuity specific items. This ensures that all staff are aware of the implications of Business and IT Service Continuity and consider them part of their normal role and activities. The various testing activities can also provide parts of the training required to ensure staff understand their role and how to respond in the case of a disaster.

- *Reviews* – a regular review of all of the deliverable from the ITSCM process needs to be undertaken to ensure that they remain current. With respect to IT, this is required whenever there is a major change to the IT Infrastructure, assets or
dependencies such as new systems or networks or a change in service providers, as well as when there is a change in business direction and strategy or IT strategy.

- **Testing** – following the initial testing it is necessary to establish a program of regular testing to ensure that the critical components of the strategy are tested at least annually or as directed by senior management or audit. It is important that any changes to the IT Infrastructure are included in the strategy, implemented appropriately and tested to ensure they function correctly.

- **Change Management** – following tests and reviews, and day-to-day changes, there is a need for the ITSCM plan to be updated. ITSCM must be included as part of the existing Change Management process to ensure all changes are reflected in the contingency arrangements provided by IT or external suppliers.

- **Invocation** – Invocation is the key component of the BCP and IT Service Continuity Plan, so guidance should be provided to support the decision-making process regarding whether to invoke the recovery plans. This decision should take into account the extent and scope of damage, the likely length of disruption and unavailability, and the time at which the disruption occurred (e.g. occurred during a non-business critical time of the year).

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 (they may not be full-time roles, but are instead a ‘hat’ they wear when required). See the following table for an example of how responsibilities for ITSCM are typically assigned.
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board</td>
<td>• Crisis Management</td>
</tr>
<tr>
<td></td>
<td>• Corporate/Business decisions</td>
</tr>
<tr>
<td></td>
<td>• External affairs</td>
</tr>
<tr>
<td>Senior Mgmt</td>
<td>• Co-ordination</td>
</tr>
<tr>
<td></td>
<td>• Direction and arbitration</td>
</tr>
<tr>
<td></td>
<td>• Resource authorization</td>
</tr>
<tr>
<td>Management</td>
<td>• Invocation of continuity or recovery</td>
</tr>
<tr>
<td></td>
<td>• Team Leadership</td>
</tr>
<tr>
<td></td>
<td>• Site Management</td>
</tr>
<tr>
<td></td>
<td>• Liaison &amp; Reporting</td>
</tr>
<tr>
<td>Supervisors and Staff</td>
<td>• Task execution</td>
</tr>
<tr>
<td></td>
<td>• Team membership</td>
</tr>
<tr>
<td></td>
<td>• Team and Site Liaison</td>
</tr>
</tbody>
</table>

### 7.10.5 Key Performance Indicators (KPIs) of ITSCM

The metrics typically used to evaluate the performance of the IT Service Continuity Management process include:

- Regular Audits of the ITSCM plans to ensure that at all times the agreed recovery requirements of the business can be achieved;
- All service recovery targets agreed and documented in SLAs are achievable within the ITSCM plans;
- Regular and comprehensive testing of ITSCM plans;
- Regular reviews are undertaken, at least annually, of the business and IT continuity plans with the business areas;
- All necessary ITSCM contracts with third parties are documented and reviewed; and
- Overall reduction in the risk and impact of possible failure of IT services.
7.11 Information Security Management

7.11.1 Goals and objectives

The goal of the Information Security (ISM) process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities. This goal has two equally important focuses:

- Meeting external security requirements; and
- Meeting internal security requirements.

The objectives of Information Security Management is to protect the interests of those relying on information and the systems and communications that deliver that information, from any harm resulting from failures of availability, confidentiality or integrity. These objectives are met when:

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

7.11.2 Scope

The process should be the focal point for all IT security issues, and must ensure that an Information Security Policy is produced, maintained and enforced, that covers the use and misuse of all IT systems and services. This will include understanding:

- Business Security Plans;
- Current business operation and it’s security requirements;
- Future business plans and requirements;
- Legislative requirements;
- Obligations and responsibilities; and
- Business and IT risks and their management.

As a guide, the Information Security Management process should include activities to:

- Produce, maintain, distribute and enforce the ISM policy and supporting security policies;
- Understand the agreed current and future security requirements of the business and the existing Business Security Plans;
Implement a set of security controls that support the ISM policy and manage associate risks;
Document all security controls, together with the operation and maintenance of the controls and their associated risk;
Manage all suppliers and contracts regarding access to systems and services, in conjunction with Supplier Management;
Manage all security breaches and incidents associated with all systems and services;
Proactively improve security controls and security risk management and the reduction of security risks; and
Integrate security aspects with all other IT Service Management processes.

7.11.3 Principles of Information Security Management

7.11.3.1 Information Security Management Policy

A consistent set of policies and supporting documents should be developed to define the organization’s approach to security, which are supported by all levels of management in the organization.

These policies should be made available to customers and users, and their compliance should be referred to in all SLRs, SLAs, contracts and agreements. The policies should be authorized by top executive management within the business and IT, and compliance to them should be endorsed on a regular basis. All security policies should be reviewed and, where necessary, revised on at least an annual basis.

The overall Information Security Policy should consist of a number of sub-components or sub-policies, covering:
- The use and misuse of IT assets;
- Access control;
- Password control;
- E-mail;
- Internet;
- Anti-virus;
- Information classification;
- Document classification;
- Remote access;
- Supplier access; and
- Asset disposal.

7.11.3.2 The Information Security Management System (ISMS)

The ISMS contains the standards, management procedures and guidelines that support the Information Security Management policies. Using this in conjunction to an overall
framework for managing security will help to ensure that the Four Ps of People, Process, Products, and Partners are considered as to the requirements for security and control.

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

1. **Plan**

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

2. **Implement**

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

3. **Control**

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

- Ensure the framework is developed to support Information Security Management;
- Develop an organizational structure appropriate to support the Information Security Policy;
4. **Evaluate**

The evaluate element of the ISMS is focused on ensuring:
- Regular audits and reviews are performed;
- Policy and process compliance is evaluated; and
- Information and audit reports are provided to management and external regulators if required.

5. **Maintain**

As part of Continual Service Improvement, the maintain element seeks to:
- Improve security agreements as documented in SLAs and OLAs; and
- Improve the implementation and use of security measures and controls.

### 7.11.4 Information Security Management Activities

The activities of Information Security Management are involved in multiple phases of the Service Lifecycle, including the:
- Development and maintenance of the Information Security Policy;
- Communication, implementation and enforcement of the security policies;
- Assessment and classification of all information assets and documentation;
- Implementation and continual review of appropriate security controls;
- Monitoring and management of all security incidents;
- Analysis, reporting and reduction of the volumes and impact of security breaches and incidents; and
- Scheduling and execution of security reviews, audits and penetration tests.

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

**Security Controls**

The set of security controls should be designed to support and enforce the Information Security Policy and to minimize all recognized and potential threats. The controls will be considerably more cost effective if included within the design of all services. This ensures continued protection of all existing services and that new services are accessed in line with the policy.
There are various security threats to our infrastructure and we want to prevent or reduce the damage of these as much as possible. Prevention/Risk reduction measures assist us to do this. *E.g. Antivirus systems, firewalls etc.*

- 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. *E.g. Antivirus systems quarantining an affected file.*
- After this process we need to review how and why the breach occurred and how successful we were in responding to the breach.

To assist in identifying what controls are missing or ineffective, a matrix can be developed that analyzes each of the control measures used for the different perspectives of security that need to be protected and controlled.
7.11.5 Challenges affecting Information Security Management

The typical challenges faced when implementing and executing this process are:

- Management commitment;
- Staff commitment;
- Low priority compared to current work issues;
- Weak or non-existing Business Security Management (& Plan); and
- Conducting thorough testing of countermeasures.

7.11.6 Key Performance Indicators (KPIs) of Information Security Management

The metrics commonly used to evaluate process effectiveness and performance of Information Security Management include:

- Business protected against security violations;
- Determination of clear and agreed policy;
- Security procedures are justified;
- A mechanism for improvement;
- Integral part of all IT and ITSM processes; and
- Effective marketing and education.
8 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:

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

8.1 Objectives of Service Transition

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; and
- To build, configure, test and deploy quality Releases into operation in the most efficient manner while also minimizing disruption to the business and customers.
8.2 Benefits of Service Transition

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; and
- Less variation from resources plans.

Figure 8.2: – Scope of Service Transition
© Crown Copyright 2007 Reproduced under license from OGC
8.3 Interfaces to other Service Lifecycle Phases

Service Transition rests between the phases of Service Design and Service Operation, with the majority of day-to-day interfaces involved between these three. However there are other inputs and outputs that exist with Service Transition and the Service Lifecycle.

Inputs from the Service Strategy phase:
- Service Portfolio Information;
- Customer and Business Portfolios;
- Supplier and Vendor Contracts Information;
- Policies;
- Organizational Strategies;
- Constraints, Compliance Obligations, Regulations;
- Architectures; and
- Service Management Plan (a requirement of ISO/IEC 20000).

Inputs from the Service Design phase:
- Service Definitions;
- Service Architecture & Structure (including core and supporting services);
- Cost models;
- Capacity/Resource models;
- Availability and Capacity plans;
- Acceptance Criteria; and
- Request For Change (RFC) to initiate the required changes to the environment.

Outputs from the Service Transition phase:

The primary outputs from Service Transition are to Service Operation and the customer and end-user community being served. The following outputs are typically delivered as following successful execution of Service Transition:
- Approved Service Release packages and associated deployment packages;
- Updated Service Packages;
- Updated Service Catalogues and Service Portfolios; and
- Documentation and Early Life Support for a transferred or decommissioned service.
Service Transition

- FSC, Testing and Validation Results, PIR
- Testing and Validation Results, Changes to IT infrastructure & services, Guidance for SLAs, OLAs, and UCs, Configuration Item information (CMDB)
- Initial End User Support, Known Errors from Development, Release Packages, Change Authorization, CMDB
- Testing and validation results, process metrics for improvements, IT infrastructure audits

Service Strategy

Service Design

Service Operation

Continual Service Improvement

Figure 8.3: – Some outputs to other lifecycle phases.
8.4 Transition Planning and Support

8.4.1 Goals and objectives

The primary goals of Transition Planning and Support are to:

- Plan and coordinate the resources to ensure that the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operations; and
- Identify, manage and control the risks of failure and disruption across all of the service transition activities.

Other objectives include:

- Plan and coordinate the resources to establish successfully a new or changed service into production within the predicted cost, quality and time estimates;
- Ensure all parties adopt the common framework of standard re-useable processes and supporting systems in order to improve the effectiveness and efficiency of an integrated planning and coordination activities;
- Provide clear and comprehensive plans that enable the customer and business change projects to align their activities with the Service Transition plans; and
- Coordinate activities across projects, suppliers and service teams.

8.4.2 Transition Planning and Support activities

![Figure 8.4: The activities of Transition Planning and Support](image)
1. Transition Strategy

The Service Transition strategy defines the overall approach to organizing Service Transition and allocating resources. For each stage included in the Transition Strategy, there will be an exit and entry criteria and a list of mandatory deliverables from the stage.

2. Prepare for Service Transition

The preparation activities include:

- Review and acceptance of inputs from the other four service lifecycle phases;
- Review and check input deliverables;
- Identify, raise and schedule Request For Changes (RFCs);
- Check that any required configuration baselines are recorded; and
- Check transition readiness.

3. Plan and coordinate Service Transition

The typical elements involved in the effective planning and coordination of a service transition are:

- Planning an individual Service Transition;
- Integrated planning with other transitions and projects;
- Adopting program and project management best practices; and
- Reviewing the plans for accuracy and completeness.

4. Advice

Service Transition should provide support for all stakeholders to understand and be able to follow the Service Transition framework of processes and supporting systems and tools. The role of Transition, Planning and Support is to proactively support communication and awareness and to seek opportunities to work with Project Managers to establish Service Transition processes into projects.

5. Administration

Transition, Planning and Support should also provide administration mechanisms for:

- Managing Service Transition changes and work orders;
- Managing issues, risks, deviations and waivers;
- Managing support for tools and Service Transition processes;
- Communications to stakeholders; and
- Monitoring Service Transition performance to provide input to the CSI phase.

6. Progress monitoring and reporting

Service Transition activities require monitoring against the intentions set out in the transition plan, including:
Measuring and monitoring release and deployment;
Maintaining an overview of actual costs, timeframes, resources against those estimated;
Management reports on status; and
Amendments to plans.

1.1.1 Challenges affecting Transition Planning and Support

As the process has such a wide scope of concern, most of the challenges affecting Transition Planning and Support are caused by inadequate communication and collaboration mechanisms and processes. Some of the typical challenges faced include:

- Project Managers unaware of the need to adopt transition standards, policies and procedures;
- Ensuring all relevant parties understand the rules and guidelines and have the skills to apply them;
- Ensuring that the Service Transition and release plans are up-to-date; and
- Ensuring stakeholders are kept up-to-date with logistics and deployment plans.

1.1.2 Key Performance Indicators (KPIs) of Transition Planning and Support

Example measures that are typically used for evaluating the performance and contribution of Transition Planning and Support include:

- The number of releases implemented that met customers requirements in terms of cost, quality, scope and release schedule;
- Reduced variation of actual versus predicted scope, quality, cost and time;
- Increased customer and user satisfaction with plans and communications; and
- Reduction number of issues, risks and delays caused by inadequate planning.
8.5 Change Management

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

Changes arise for a number of reasons, e.g.:
- From requests of the business or customers, seeking to improve services, reduce costs or increasing ease and effectiveness of delivery and support; or
- From internal IT groups looking to proactively improve services or to resolve errors and correct service disruption.

The process of Change Management typically exists in order to:
- Optimize risk exposure (defined from both business and IT perspectives;
- Minimize the severity of any impact and disruption; and
- Deliver successful changes at the first attempt.

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

8.5.1 Goals and Objectives

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’s purpose is also to ensure that:

1. All Changes to service assets and configuration items (CIs) are recorded in the Configuration Management Systems (CMS).
2. Overall business risk is optimized.

### 8.5.2 Scope

The term *change* is often defined in varying ways, however the best definition of a service change is:

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

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

*Figure 8.5: Scope of Change Management for IT Services*

© Crown Copyright 2007 Reproduced under license from OGC
Figure 8.4 demonstrates the typical scope of the Change Management process for an IT Service Provider and how it interfaces with the business and suppliers at strategic, tactical and operational levels. As discussed in Service Strategy, Service Portfolios provides the clear definition of all planned, current and retired services.

### 8.5.3 Designing and Planning

It is generally advised that the Change Management process should be planned in conjunction with Release & Deployment, and Service Asset & Configuration Management. These processes together will help in the evaluation of impact, needs, timings and overall risk for changes being assessed.

The checklist of typical requirements when designing the Change Management process includes:

- Regulatory, policy or other compliance requirements;
- Documentation requirements;
- Identification of impact, urgency and priority codes for changes;
- Roles and responsibilities involved;
- Procedures required;
- Interfaces to other Service Management processes (e.g. Problem Management);
- Toolset requirements to support Change Management; and
- Configuration Management interfaces.

### 8.5.4 Change Management Policies

There must be policies and standards defined that clarify, for internal and external providers, who must do what, when and what the consequences of non-compliance to the policy will be. These policies are typically created with information relating to:

- Creating a culture of Change Management – with zero tolerance on unauthorized changes;
- Aligning the service Change Management process with business, project and stakeholder Change Management;
- Prioritization of changes;
- Establishing accountability and responsibilities;
- Segregation of duty controls;
- Establish a single focal point for changes;
- Prevent people who are not authorized to make changes from accessing production environment;
- Integration with other Service Management processes;
- Change windows;
- Performance and risk evaluation; and
• Performance measures for the process.

8.5.5 Change Models

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

• What steps should be taken to manage the change;
• Roles and Responsibilities;
• Timescales and thresholds for actions; and
• Escalation procedures.

Change Models defined within ITIL include the following:

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

See Figure 6.3 for the example process flow for normal changes.

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

The main elements of a standard change are that:

• Authority is effectively given in advance;
• The tasks are well known, documented and proven;
• There is a defined trigger to initiate the Request For Change (RFC);
• Budgetary approval is typically defined or controlled by the requester; and
• The risk is usually low and always well understood.
Over time and as the IT organization matures the list of standard changes should increase in order to maintain optimum levels of efficiency and effectiveness.

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

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

To enable this to occur, methods of assessment and documentation are typically modified, with some documentation taking place after the change has occurred.
8.5.6 Triggers and Interfaces

Requests for Change can come from anywhere within service lifecycle or from interfaces with the business, suppliers or other stakeholders. The inputs required for the change and outputs produced will vary depending on the type defined and whether it is strategic, tactical or operational in nature.

Normal inputs include:
- Request for Changes (RFC);
- Policy and strategies for change and release;
- Plans (change, transition, release, deployment, test, evaluation and remediation);
- Current change schedule and projected service outage (PSO);
- Current or affected assets and configuration items; and
- Test results, test report and evaluation reports.

Normal outputs from the process will be:
- Rejected RFCs;
- Approved RFCs;
- Changes to services, infrastructure components resulting from approved RFCs;
- Updated change schedule;
- Revised PSO;
- Authorized change plans; and
- Change decisions, documents, records and reports.

Interfaces with other service lifecycle processes should also be considered for a coordinated approach to quality service management. Additionally the integration of Change Management with Business Change processes, project management and supplier management is recommended to enable seamless level of IT quality to be delivered.
There can be various types of Change Requests to initiate the execution of Change Management processes, including:

- RFCs;
- Service Desk calls; and
- Project Initiation Documents.

Different types of change require different types of change request. An organization needs to ensure that appropriate procedures and forms are available to cover the anticipated requests from the different parties and stakeholders involved. Avoiding a bureaucratic approach to documenting a minor change alleviates some of the cultural barriers and resistance that may exist when adopting the Change Management process.
8.5.7 Change Management Activities

The following diagram represents the typical activities involved for normal changes that have been identified. The actual steps and procedures need to be further refined depending on any specific Change Models that have been created.

Overview of Important Steps:
1. The RFC is recorded.
2. Review the RFC for classification and prioritization.
3. Assess and evaluate the change – may require involvement of CAB or ECAB.
4. Authorization or rejection of the change.
5. The change is scheduled.
6. Work orders are issued for the build of the change (but carried out by other groups).
7. Change Management coordinates the work performed.
8. The change is reviewed.
9. The change is closed.
1. The RFC is recorded.

The change is raised by a request from the initiator. The level of information recorded for a change depends largely on the size and impact of the change. Some information is recorded initially and some information updated as the change document progresses through its lifecycle. This may be recorded directly on the RFC form and details of the change and actions may be recorded in other documents and referenced from the RFC such as business cases.

For a major change with significant organizational and/or financial applications, a change proposal may be required, which will contain a full description of the change together with a business and financial justification for the proposed change. The change proposal will include sign off by appropriate levels of business management.

2. Review the RFC for classification and prioritization.

To ensure Change Management is using an appropriate level of control based on factors of risk, cost and complexity, an initial review should act as a filtering mechanism to apply the correct Change Model to be used (classification), identify the relative priority of the change, and to ensure that the required details are supplied. Procedures should stipulate that, as changes are logged, Change Management reviews each change request and return any that are:

- Totally impractical;
- Repeats of earlier RFCs; or
- Incomplete submissions.

These requests will be returned to the initiator, together with brief details of the reason for the rejection, and the log should record this fact. There should be an opportunity to appeal, via normal management channels, and should be incorporated within the procedures.

3. Assess and evaluate the Change.

All changes will be assessed for their relative potential impact, risk and resource requirements. Depending on the Change Model that has been applied, this assessment may require involvement from:

- Only the Change Manager and Change Owner for local authorization;
- The Change Advisory Board (representing all key stakeholders);
- The IT Management (Steering) Board; or
- Business Executive Board.
The scope of potential impacts on services for failed changes is wide, so the assessment needs to identify potential for:

- Impact on customer's business operation;
- Effect on SLAs, baselines, service models, security etc;
- Impact on other services;
- Impact on non-IT infrastructures;
- Effect of not implementing;
- Cost and staffing implications;
- Current Change Schedule;
- Ongoing resources required after implementation; and
- Impact on continuity plan, capacity plan, security plan, test environments, and any Service Operation practices.

The following table describes the type of hierarchical structures that may be used for different levels of change authorization. A degree of delegated authority may also exist within an authorization level. Formal authorization is obtained for each change from a change authority that may be a role, person or a group of people. The levels of authorization for a change should be judged by:

- Type;
- Size;
- Risk;
- Financial implications; and
- Scope.

<table>
<thead>
<tr>
<th>Level</th>
<th>Change Authority</th>
<th>Potential Impact/Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business Executive Board</td>
<td>High cost/risk change - Executive decision</td>
</tr>
<tr>
<td>2</td>
<td>The IT Management (Steering) Board</td>
<td>Change impacts multiple services/organizational divisions</td>
</tr>
<tr>
<td>3</td>
<td>Change Advisory Board (CAB) or Emergency CAB (ECAB)</td>
<td>Change impacts only local/ service group</td>
</tr>
<tr>
<td>4</td>
<td>Change Manager</td>
<td>Change to a specific component of an IT Service</td>
</tr>
<tr>
<td>5</td>
<td>Local Authorization</td>
<td>Standard Change</td>
</tr>
</tbody>
</table>
The *7 Rs of Change Management* provide a set of guiding questions that need to be answered as part of the overall assessment for changes. These questions are:

1. Who RAISED the change?
2. What is the REASON for the change?
3. What is the RETURN required from the change?
4. What are the RISKS involved in the change?
5. What RESOURCES are required to deliver the change?
6. Who is RESPONSIBLE for the build, test and implementation of the change?
7. What is the RELATIONSHIP between this change and other changes?

**4. Authorization or rejection of the change.**

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?

When authorizing changes, it is important to consider both the implications of performing the change, as well as the impacts of *not* implementing the change. This also requires empowering the Change Manager with an appropriate level of authority as their primary role is to protect the integrity of the IT infrastructure and the services provided to customers.

**5. The change is scheduled.**

The assessment of the change will have provided an estimation of the resource requirements for delivering a successful change. Change Management will need to coordinate with Release and Deployment Management so that any activities required for the build, test or implementation of the change will be scheduled when resources are available and when they least impact on live services or business critical times.

The timing of events and eventual implementation will be communicated via the Change Schedule, and visible to the appropriate IT staff members, customers and end-users. Any service disruption is documented in with the Projected Service Outage (PSO). This details any revised Service Level Agreement and service availability targets because of the events in the Change Schedule, in addition to any planned downtime from other causes such as planned maintenance and data backups.
6. **Work orders are issued for the build of the change (but carried out by other groups).**

Change Management will coordinate with Release and Deployment to identify the groups or individuals responsible for the implementation of the various elements making up the Change. This will be greatly influenced by the availability of staff and any Release policies defining how and when changes are released to the live environment.

7. **Change Management coordinates the work performed.**

Change Management plays a co-ordination role as implementation is the responsibility of others (under the direction of Release and Deployment management or from Project Management groups).

This is an oversight role to also ensure that all changes that can be, are thoroughly tested. In all cases involving changes that have not been fully tested, special care needs to be taken during implementation.

Remediation Planning is a critical element during the coordination of changes. Ideally, no change should be approved without having explicitly addressed the question of what to do if it is not successful. There should be a back-out plan that will restore the organization to its initial situation, through reloading a baselined set of Configuration Items.

Only by considering what remediation options are available before instigating a change, and by establishing that the remediation is viable, can the risk of the proposed change be determined and the appropriate actions taken.

8. **The change is reviewed.**

On completion of the change, the results should be reported for evaluation to those responsible for managing changes, and then presented as a completed change for stakeholder agreement. Major changes will require more customer and stakeholder input throughout the entire process.

The review should confirm that the change has met the defined objectives, that the initiator and stakeholders are happy with the results and that there have been no unexpected side-effects. Lessons learned should be embedded into future changes as part of continuous improvement. This includes whether the request should be developed as a standard change or whether another change model is more appropriate for future management of similar requests.
Two types of reviews are performed for normal changes:

- The review of a *service change* – immediately visible to the customer and scheduled for discussion at the next service level management review meeting.
- An *infrastructure change* – concerned with how IT delivers rather than what IT delivers, which will be (almost) invisible to the customer.

Change Management must review new or changed services after a predefined period has elapsed. This process will involve CAB members, since change reviews are a standard CAB agenda item. When a change has not achieved its objectives, Change Management (or CAB) will decide what follow-up action is required.

9. **The Change is closed.**

If the change review was satisfactory or the original change is abandoned (e.g. the needs for the change is decreased or disappears) the RFC should be formally closed in the logging system. These records will be kept for a period of time based on business, compliance, archiving or other policy requirements that have been defined.

### 8.5.8 Roles and Responsibilities within Change Management

**Change Advisory Board (CAB)**

The CAB is a body that assists the Change Manager is evaluating and approving changes that have been requested. The CAB is not necessarily a physical meeting of people, but can be enabled with the use of technology such as video-conferencing. Members of the CAB are made up by IT staff, customers, suppliers and other stakeholders in such a way that all changes that impact their domain can be appropriately assessed from business, technical and support viewpoints. 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; and
- 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. Standard items for the CAB agenda include:

- Failed, unauthorized or backed-out changes;
- RFCs to be assessed by the CAB ordered by priority;
- Current and outstanding changes;
- Concluded changes for review;
- Identified process issues or improvements; and
- Advance notice of RFCs expected for review at next CAB meeting.

In order to maintain an effective meeting, CAB members should come prepared with any documentation that was produced as part of their evaluation or advice on current changes. Ultimately the final decision to authorize changes will rest with the Change Manager or whichever body or person has been delegated for this in the organization (typically the IT director or service manager).

**Emergency Change Advisory Board (ECAB)**

For Emergency Changes, a separate defined procedure and authorization mechanisms should exist and be clearly documented and understood. As it will not always be possible to convene a full CAB meeting, an ECAB would be used instead, which is a sub-group that will provide the assistance for the evaluation of Emergency Changes. This may be three or four members of the normal CAB who between them have the best overview of the potential risks and impacts of implementing the Emergency Change.

While complete testing may not be possible, it is still important to apply an appropriate level of testing as well as define any roll-back mechanisms relative to the potential risk and impact identified.

### 8.5.9 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. Metrics should be linked to business goals whenever practical, and to cost, availability, reliability and customer satisfaction.
These metrics include:

- Number of RFCs (Accepted/Rejected);
- Number and per cent 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;
- Number of disruptions (incidents and problems) caused by unsuccessful changes;
- Level of variance between estimated and actual resources and time required for changes;
- Frequency of change (by service, business area etc.);
- Number of changes (by change type);
- Number of changes recorded and tracked using automated tools;
- Staff utilization; and
- Number of unauthorized changes detected by Configuration Management.

8.5.10 Challenges affecting Change Management

Implementing Change Management should be managed with particular sensitivity and awareness due to the often large cultural changes that will need to take place. This will need to be addressed by developing stakeholder awareness at all stages during the implementation project, including gaining feedback about their needs, expectations and ideas.

Depending on the current maturity of informal change management practices, it may be appropriate to run a pilot for Change Management, in order to identify the potential successes and failures and to better refine and scale according to the organization’s needs. Over time, the scope of Change Management should eventually include the customers and end-users just as much as IT staff members themselves, as there can be many instances where service quality can be negatively impacted as a result of changes executed by the end-user community.
Typical challenges that affect the success of Change Management include:

- Change in culture - 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; and
- Commitment of management.
8.6 Release and Deployment Management

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

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

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

8.6.1 Goals and Objectives

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

Other objectives of Release and Deployment are:

- To define and agree upon Release policies, and Release and Deployment plans with customers and stakeholders;
- Ensure the integrity of constructed release packages and that they are recorded accurately in the Configuration Management System (CMS);
- Ensure that all release packages can be tracked, installed, verified, uninstalled or backed out if necessary;
- Ensure the required skills and knowledge is transferred to support staff, customers, end-users, suppliers and any other relevant stakeholders; and
- There is minimal unpredicted impact on the production services, customers and service operations.
8.6.2 Scope

Release and Deployment works closely in conjunction with the other Service Transition processes to enable the quality transition of services. The role played specifically by Release and Deployment is to build, package, validate and distribute authorized service changes to the target systems or users. A release is a collection of authorized changes to an IT service.

8.6.3 Benefits

When identifying the benefits that Release and Deployment provides for, it is important to remember that it should be utilized in conjunction with the other Service Transition processes. As a result, improvements in the metrics defined for Release and Deployment may be at the expense of the other transition processes. Typical benefits seen as a result of improved Release and Deployment are:

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

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

8.6.4 Terminology

Release Unit:

A ‘release unit’ describes the portion of a service or IT infrastructure that is normally released together according to the organization’s release policy. When defining the most appropriate release unit structure, the following factors should be taken into account:

- The ease and amount of change necessary to release and deploy the release unit;
- The amount of resources needed to build, test and distribute a release unit;
- The complexity of interfaces between the proposed unit and the rest of the services and IT infrastructure; and
The storage and resources available in the build, test, distribution and live environments.

Based on these factors, it may mean that for critical applications the release unit is the complete set of application components and for optional features or add-ons only the single component itself.

![Figure 8.8: Simplified example of release units for an IT service](image_url)

**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. Like the definition of release units, factors such as the modularity of components, the amount of change occurring and resources required will be considered when formulating a complete Release Package.

**Release Identification:**

The unique release identification scheme which is normally defined in the Release Policy and conforms to any standards defined by Service Asset and Configuration Management. Typical identification schemes include the following examples:

- **Major Release:** Banking_System v1, v2, v3 etc.
  - Major roll-out of new hardware and/or software.
- **Minor Release:** Banking_System v1.1, v1.2, v1.3 etc.
  - A few minor improvements and fixes to Known Errors.
- **Emergency Fix:** Banking_System v1.1.1, v1.1.2 etc.
  - A temporary or permanent Quick Fix for a Problem or Known Error.
Definitive Media Library (DML):

The secure library where the definitive authorized versions of all media CIs (typically software) are stored and protected. The DML should include definitive copies of purchased software (along with license documents and any controlled information) as well as software developed on site. The DML includes both electronic and physical copies of definitive software releases, with Release and Deployment being responsible for any additions, modifications, removals or maintenance that needs to be performed.

![Diagram of DML and CMDB](image)

Figure 8.9: The use of the DML by Release and Deployment

© Crown Copyright 2007 Reproduced under license from OGC

Definitive Spares:

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. Like the DML, details of these assemblies are recorded in the CMDB, and
their management and deployment the responsibility of the Release and Deployment process.

**Build Management:**

The software, hardware and documentation that comprise a release unit should be assembled in a controlled manner to ensure a repeatable process. This should include automation where possible for its compilation and distribution, which for large organizations can significantly reduce the Total Cost of Ownership (TCO) for the services involved.

**8.6.5 Triggers and Interfaces**

The primary interfaces of release and deployment exist with Change Management and the surrounding Service Transition processes. Other inputs will also be provided from Service Strategy and Service Design to ensure that the requirements for value provision have been met.

The inputs to release and deployment include:
- Authorized RFCs;
- Service Packages;
- Service Design Package;
- Service Acceptance Criteria;
- Service Management policies and standards (including the Change Policy);
- Build Models and plans; and
- Exit and entry criteria for each stage of release and deployment.

The outputs include:
- Release and deployment plan;
- Updated RFCs for any required activities;
- Updated service catalogue reflecting any service changes;
- New or modified service;
- New or modified processes;
- Skilled and knowledgeable support staff;
- End-users with capabilities to use the service;
- SLAs, OLAs, UCs;
- Deployment plans and packages; and
- Service Transition Report.
8.6.6 Release Design Options and Considerations

When planning individual releases or defining the policies that should exist, consideration about the potential impact and need for resources will affect how releases will be deployed to the target locations. The common options for deploying releases are described below:

**Big Bang or Phased**

**Big Bang:** Where 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.

**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.

* * Additional Workstations

Figure 8.10: Options for ‘big bang’ and phased rollouts.
© Crown Copyright 2007 Reproduced under license from OGC
Push or Pull

The Push Approach: 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 forms is the use of a 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. 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. The use of ‘Pull’ updating a release over the internet has made this concept significantly more pervasive. A good example is virus signature updates, which are typically pulled down to update PCs and servers when it best suits the customer; however at times of extreme virus risk this may be overridden by a release that is pushed to all known users.

Pull approaches do not rest so heavily on accurate configuration data and they can trigger an update to user records. This may be through new users appearing and requesting downloads or expected users not doing so, triggering investigation into their continued existence.

Automated or Manual

Automation: 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. Typical examples of activities that are capable of a degree of automation are:

- Discovery tools to aid release planning;
- Automated builds to reduce time taken. This in turn can resolve scheduling conflicts and delays; and
- Automated configuration baselines procedures save time and reduce errors in identifying the status of CIs and releases during build, test and deployment etc.

Manual: Important to monitor and measure the impact of many repeated manual activities as they are likely to be inefficient and error prone. This will ultimately slow down the release team and create resource and capacity issues that affect the agreed service levels.
8.6.7 **Release Policy**

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

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

8.6.8 **Release and Deployment Activities**

<table>
<thead>
<tr>
<th>Release policy &amp; planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design &amp; develop or order &amp; purchase</td>
</tr>
<tr>
<td>Build &amp; configure release</td>
</tr>
<tr>
<td>Release testing &amp; acceptance</td>
</tr>
<tr>
<td>Deployment planning</td>
</tr>
<tr>
<td>Communication, preparation &amp; training</td>
</tr>
<tr>
<td>Logistics, Delivery &amp; installation</td>
</tr>
</tbody>
</table>

**Key Points:**

The Release Policy is the overarching strategy for releases and was derived from the Service Design phase of the Service Lifecycle.

The Release Plan is the operational implementation for each release.

The Deployment Plan is the documented approach for distributing a single release.

*Figure 8.11: Phases and activities of Release and Deployment*
Overview of Important Steps:
1. Release planning.
2. Preparation for build, test and deployment.
4. Service test and pilots.
5. Plan and prepare for deployment.
7. Verify deployment.
9. Review and close the deployment.
10. Review and close Service Transition.

1. Release Planning

Any plans created for the release and deployment will need to be integrated with the overall Service transition plan, and conform to any policies that have been defined. For each release, plans should be authorized by Change Management and used to assist in the evaluation of the risk, impact and resource requirements for components of the change. Typically the release and deployment plans should document the:

- Scope and content of the release;
- The risk assessment for the release;
- Affected stakeholders;
- Teams responsible for the release; and
- Communication strategy to be used during the release and deployment process.

Plans should take into account the acceptance criteria that exist for the release and when authorization points will verify a pass or fail. The processes of Evaluation and Service Validation and Testing will be integrated here to assist in the determination whether to continue, pause or revert to previous stages of the release.
Build and test planning

The approach taken for building, testing and maintaining the controlled environments to production will need to be planned in order to enable optimum use of resources for the development of the release. The activities that occur here are:

- Developing build plans based on the Service Design Package and defining any environment requirements;
- Scheduling the resources and time required to setup the environments;
- Testing the build and compilation procedures;
- Scheduling the build and compilation activities;
- Assigning resources, roles and responsibilities for any key activities; and
- Defining the build exit and entry criteria.

Environments that may be utilized during this period include:

- Build environments;
- Testing and integration environments;
- Deployment environments;
- Pilot environments; and
- Backup and recovery environments.

Utilizing Pilots

Pilots may be useful for testing the service with a group of participants that are representative of the broader end-user community. For this to be effective the scope needs to be carefully determined, as being either too large or too small will likely result in some negatively impact to the overall success and quality of the release and deployment process.

Pilots should include mechanisms by which feedback can be gathered about various aspects of the release and associated processes. For complex releases or in large and diverse organizations it may be appropriate to use more than one pilot for address the different implementation and support issues that exist.

Deployment Planning

There are many factors that will be considered when choosing the most appropriate deployment strategy (refer back to deployment options). Questions that must be answered include:

1. What needs to be deployed?
2. Who are the users?
3. Are there location dependences?
4. Where are the users?
5. Who else needs to be prepared well in advance? (training, security etc)
6. When does the deployment need to be completed?
7. Why is the deployment happening?
8. What are the critical success factors and exit criteria?
9. What is the current capability of the service provider?

Financial/Commercial Planning

Where necessary, various financial and commercial factors will need to be assessed before the deployment activities, including:

- Working capital;
- Contracts and licenses;
- Funding; and
- Intellectual property requirements.

2. Preparation for build, test and deployment

Before the actual building of the release occurs, the release design must be validated against the requirements defined for the new or changed service offering. This should be an independent evaluation that checks the release will deliver the predicted outcomes, and any issues documented in an interim evaluation report.

Training of involved release and deployment staff

In many cases the introduction of a release may require additional training for the release, deployment, build and test teams. Such training could be related to the:

- Service management processes to be used;
- Changes in security or health and safety procedures;
- Understanding of the Service Design documentation and plans; and
- Technology being utilized for the release.
3. Build and test

Wherever possible, repeatable practices and reusable components should be utilized during the build and test of releases. This includes managing the:

- Build, test and packaging environments;
- Compilation and packaging tools; and
- Configuration of the releases themselves:
  - Version control;
  - Documentation templates for testing and validation; and
  - Access rights and security procedures.

Release and build documentation

Documentation templates, procedures, knowledge bases and other guidance should be consistently available to support the release team in the activities performed. Typical documentation that will be used by the release teams include:

- Contract agreements;
- Purchase requests;
- Health and Safety guidelines;
- Security policies;
- License agreements; and
- Procedures for:
  - Distributing software;
  - Delivering, moving and installing equipment;
  - Wiping sensitive data and media; and
  - Publishing, sharing and archiving knowledge, information and data.

Acquire and test required components

Release and Deployment should be interfaced with the organization’s existing procurement processes to acquire any required components for the release. This will save time and effort in verifying assets, capturing and recording information, ensuring proof of license and triggering updates to the Asset Management System.

As part of the overall Service Validation and Testing, each of the individual components should be tested to verify that any quality criteria has been met, initiating action where quality criteria is not met.
Release Packaging

Build management procedures, tools and checklists should be utilized as part of the release packaging, to provide repeatable practices and expected outcomes. When a definitive package has been assembled, a baseline should be taken of the release package and the correct versioning and naming conventions applied.

Managing the build and test environments

The need for multiple environments in which to build and test will depend on the size, complexity, frequency and impact of the releases being managed. Test environments should be protected using a range of testing best practices (see also Service Validation and Testing), and appropriate access to these environments given based on the priorities defined.

Automating the installation of systems and software reduces the workload of people, but also requires testing of the scripts and mechanisms that will be used.

4. Service testing and pilots (See Service Validation and Testing)

As part of a coordinated effort with Service Validation and Testing, testing and validation must be performed at multiple levels. With particular focus on the release itself, service rehearsals may be used, which simulates as much of the service as possible in an extensive and widely involved practice session. This would normally occur after other pilots have run, and is designed to be the last measure to detect any potential issues that will arrive during or after the deployment to the live environment.

Pilots

Previous planning should have already identified what pilots will be used as part of the overall release and deployment. Key actions to take during pilots are:

- Training of any people involved;
- Documentation of any required procedures;
- Continual communication and engagement with customers and users;
- Determine the levels of support required for the actual release;
- Discover and fix issues wherever possible before the final deployment; and
- Document improvements where appropriate and incorporate them into future plans.
5. Plan and prepare for deployment

At this stage the focus is to prepare the organization and people for organizational change and to refine and deployment plans that have been documented. These plans should include guidance regarding:

- Risk mitigation plans;
- Disposal and retirement plans;
- The logistics for delivery;
- Knowledge transfer;
- Mobilizing users to be ready to use the service; and
- Mobilizing the support staff for service readiness.

![Figure 8.12: Example set of deployment activities](image-url)

© Crown Copyright 2007 Reproduced under license from OGC
6: Perform transfer, deployment and retirement

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; and
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’.

7: Verify deployment

Once the activities for the deployment of releases are finished, verification should occur that users are capable of operating the service. Verification should ensure that:

- The service/release components are in place by means of a configuration audit;
- Documentation has been updated accordingly;
- Roles and responsibilities have been correctly assigned; and
- The measurement and reporting systems are established to measure performance of the service.

Any noted deviations from plans or other items raised should be documented in order to improve future implementations and processes used.

8: Early Life Support

The quality of transition to Service Operation is a crucial element to the success of the overall service change that is being implemented. Rather than simply hand off support post-deployment, the release and deployment teams should assist in managing any calls, incidents and problems that are detected in the early of the new or modified service. This enables more stability in this vulnerable period, increased customer and user satisfaction, enhanced learning and better momentum for continual improvement. The resource allocation from these teams will then be gradually reduced while Service Operation takes on more responsibility for support.
The example shown in the figures above demonstrate how the number of incidents for deployment A was significantly reduced through the use of Early Life Support, including the training of users and staff, and the transfer of knowledge to service desk staff (including knowledge base articles).

The acceptance criteria for finalizing Early Life Support should be agreed early in the process, which might include such conditions as:

- Users can use the service effectively and efficiently for their business activities;
- Service delivery is managed and controlled across any service provider interfaces;
- Service levels and performance standards are being consistently achieved;
- Stakeholder groups verify the transfer of required knowledge; and
- All deliverables required for the release have been signed off.
9: Review and close the deployment

A formal review of deployments should be performed for all releases of a determined level of size, impact, cost or risk to the organization. The review seeks to ensure that all requirements for the release have been met and to identify any potential improvements that can be made. Items that should be reviewed include:

- Any quality criteria deviations that exist;
- Any open actions or necessary fixes that have been identified;
- Review open changes;
- Review performance targets and achievements;
- Experiences and feedback from customers, users and staff involved with the deployment;
- All problems and known errors are documented and accepted by the business and/or suppliers; and
- Check that any redundant assets (including licenses) have been removed.

10: Review and close Service Transition

The final step required in finalizing the completion of Service Transition is a formal review appropriate to the relative scale of the change. This will utilize the process of Evaluation and is driven by Change Management, which will verify successful completion and that the handover to Service Operation is complete.

The “lessons learnt” should be documented to provide any improvement opportunities that can be made and developed by Continual Service Improvement for future transitions.

Figure 8.15: Transitioning New and Changed Services into Operation
Note how Change, Release and Deployment, Service Validation and Testing and Service Asset and Configuration Management work together for the transition of new or modified Services.

### 8.6.9 Key Performance Indicators (KPIs) of Release & Deployment Management

**Service Provider metrics:**
- Reduced resources and costs to diagnose and fix incidents and problems in deployment and production;
- Reduced discrepancies in configuration audits;
- Increased accuracy in deployment of software;
- Increased compliance with software license requirements and reduced over-subscriptions; and
- Reduced time and resources consumed by build, package, test and deployment activities.

**Customer metrics:**
- Decreased variance in service performance against predicted performance;
- Reduced number of incidents during Early Life Support;
- Increased customer and user satisfaction; and
- Faster adoption of new and modified services amongst end-user community.
8.7 Service Validation and Testing

8.7.1 Goals and Objectives

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.

8.7.2 Scope

The concepts of Service Validation and Testing can be applied throughout the entire service lifecycle to quality assure any aspect of a service and the provider’s capability to deliver and support it. This will require that the all components and providers that are involved in the end-to-end service are considered as part of the approach for Service Validation and Testing.

The processes of Change, Release and Deployment and Evaluation will need to be interfaced with Service Validation and Testing, which in turn will ensure the appropriate levels of testing are performed for the build, test and deployment activities of the releases required.

8.7.3 Benefits

Insufficient testing practices will usually always result in some level of service failure. Depending of the criticality, size and number of end-users or customers affected, this can result in long-lasting effects on the reputation and success of the provider and business; in extreme circumstances even injury or death.

The process of Service Validation and Testing can be used as an opportunity to clarify that it is impossible to guarantee exact levels of performance and quality, but instead that an
appropriate level of confidence can be achieved with appropriate testing and safeguards in place.

8.7.4 Policies and Principles

Service Quality Policy

Consideration needs to be given to defining the meaning of service quality. Service Strategy should provide guidance regarding the approach and standards for quality, from the perspectives of:

- Level of excellence;
- Value for money;
- Conformance to specification; and
- Meeting or exceeding expectations.

While a balanced approach to these perspectives should be maintained, any dominant focus will influence how services are designed, operated, measured and controlled. In addition to these overall guidance provided by Service Strategy, more detailed service level metrics will be developed during the Service Design phase and handed over as part of the Service Design package.

Risk Policy

Risk policies are designed to influence how a service provider manages risk, including the level of change control, validation and testing and security provision for services being offered. As different segments will have varying attitudes and perspectives regarding risk, the level of confidence established in services will change depending on the safety criticality or compliance factors that apply.

Release Policy

The documented policy describing the approach, type and frequency for releases will have a large impact of the levels of testing and validation used. As the frequency of releases increases so does the requirement for consistent and reusable test models and automated testing mechanisms.

Change Management Policy

Like the Release policy, any documented change windows will influence the level of testing that can be provided for throughout Service Transition. In the case of a release that is behind schedule but still needs to be deployed within a defined change window, what sacrifices will be made in order achieve the proposed distribution date?
Typical elements within Change Management policies that relate to testing include:

- The integration of testing within the service lifecycle and projects;
- Using a risk-based approach to testing;
- Engaging all appropriate stakeholders throughout the project and service lifecycle for testing; and
- Automation of testing mechanisms.

When constructing a Service Design package there are many influencing constraints that influence how a new or modified service will be developed and built (see figure above). Service Validation and testing should verify that these boundaries are correctly defined and that the service can be transitioned within those boundaries. Within these constraints, the primary focus of service validation is ensuring that the required service utility and warranty (see below) has been delivered by the new or modified service.
Test Strategy

A test strategy describes the overall approach to organizing testing and validation, including the allocation of the enabling resources required. It may apply to the whole organization, a set of services or a single service. The typical contents of a test strategy document include:

- The purpose, goals and objectives of service testing and validation;
- Scope and organizations;
- Applicable standards, legal and regulatory requirements;
- Service Management policies, processes and practices applicable to testing;
- Test models used;
- Test process activities (planning and estimation, documentation, control, execution etc);
- Test metrics;
- Service Provider interfaces;
- Test criteria;
- Roles and responsibilities;
- Environment requirements; and
- Deliverables.

8.7.5 Test Models

A test model describes a test plan, the scope of a test and the test scripts that define how each element will be tested. It ensures that testing is a repeatable process and that the defined deliverables are achieved. Test models should be structured so that:

1. There is traceability to the initial design requirements and criteria.
2. All activities can be measured and audited.
3. That test elements can be reused or changed.
See the Service V Model for examples of test models used according to the different levels of testing and validation that apply.

### 8.7.6 Testing Approaches and Techniques

Any test strategy needs to provide for a range of perspectives in order to determine whether the service will deliver as required. From the high level business perspective through to the technology perspective, different test models will ensure that each level is sufficiently tested and validated against that the requirements and any criteria are met.

Using techniques such as the Service V model (see below) for Service Validation and Testing, provides a framework to help organize the levels of Configuration Items that are needed and the associated testing and validation activities within and across stages of the change.

![The Service V Model](image)

*Figure 8.18: The Service V Model*

© Crown Copyright 2007 Reproduced under license from OGC
The Service V Model is a concept of establishing acceptance requirements against the various levels of requirements that apply in order to justify release to the customer for trial and assessment.

The left hand side represents the specification of the service requirements down to the detailed Service Design. The right hand side focuses on the validation and test activities that are performed against the specifications defined on the left hand side, and there is direct involvement by the equivalent party on the right hand side.

It shows that service validation and acceptance test planning should start with the definition of the high level requirements. It also describes that the person/group or sign off on the requirements on the left side should be involved on the right side to accept that the requirements have been met.

The actual tests required at each level should reflect the approach to risk and level of confidence that is required for the service change being transitioned. There are many frameworks and sources of guidance focused specifically on testing e.g. Test Management Approach (TMAP) that provide more details about the specific types of testing activities that can be performed. These normally include:

- Usability testing;
- Accessibility testing;
- Process and procedure testing;
- Knowledge transfer and capability testing;
- Performance, capacity and resilience testing;
- Volume, stress, load and scalability testing;
- Availability, backup and recovery testing;
- Security testing;
- Logistics, deployment and migration testing;
- Build, packaging and distribution testing; and
- Operability and maintainability testing.
8.7.7 Service Validation and Testing activities

Depending on the relative size of the service change, the activities shown in the figure above may need to be increased or decreased in effort and scope for confidence in service quality, or run in sequence or in parallel depending on available resources and testing interdependencies.

1. Test Management

Test Management is the overall coordination, control and reporting of the validation and testing activities that are performed during Service Transition. This is an activity best suited to be carried out by the Service Test Manager as it involves the coordination of resources based on the analysis of a range of test metrics and management of any issues or conflicts that arise.

Test Management typically involves tasks such as:
- Planning and scheduling test resources;
- Prioritizing and scheduling the sequence of testing events;
- Managing any non-conformance, issues and risks;
- Ensuring any incoming known-errors from development and their documentation items are processed;
- Monitoring progress; and
- Monitoring overall performance and quality of the process.
2. Plan and design test

This should be started early in the service lifecycle, and includes:
- Resourcing;
- Ensuring capability for tests required;
- Acquiring any business/customer resources that are required;
- Schedule of milestones and deliverable dates;
- Entry and exit points; and
- Financial requirements – budgeting and funding.

3. Verify Test Plan and Test Design

Review the test plans and designs to verify that the test models used are appropriate for the levels of risk that exist and the level of confidence that needs to be assured for the service change. Checks should also be performed to verify that the test scripts are complete and accurate.

4. Prepare Test Environment

There may be configuration required in order to make use of the test environment. A baseline should also be captured of the initial test environment for any later comparison in the release process.

5. Perform tests

Any tests required will be performed, using either manual or automated mechanisms. Any exceptions that are raised from the test activities should be documented for future re-tests. Based while the outputs from testing will vary depending on the test model defined, they typically include:
- Actual results showing proof of appropriate levels testing;
- Problems, errors and any non-conformance that need to be resolved;
- Resolved problems and errors; and
- Sign off from test agents and stakeholders.
6. Evaluate exit criteria and report

Documented results from the testing activities must be compared to the expected results. Any exceptions can be defined as:

- Pass/fail;
- Risk to the business/service provider; or
- Change in expected value outcome (including higher costs to deliver benefits).

7. Test clean up and closure

If testing is complete for a given release, the environment should be cleaned or restored to the initial state. Along with the exit criteria documentation, other reports submitted will communicate the effectiveness of the utilized test model and process used, the decision to buy or build and any other identified improvements that can be made.

8.7.8 Triggers and Interfaces

The key inputs into the Service Validation and Testing process are:

- The Service Design Package, including the associated operation, capacity, financial models and detailed design and interface specifications;
- The service package – the combination of core and supporting services that provide the utility and warranty required from the customers and business;
- The service provider interfaces, including both internal and external boundaries that exist;
- Release and Deployment plans;
- Acceptance criteria; and
- Request For Change (RFC).

The key outputs from Service Validation and Testing are reports provided to Service Evaluation. These reports document:

- Testing activities carried out (including the information on the test model used);
- Configuration baselines for the testing environments;
- Results from tests; and
- Analysis of the results (identifying reasons for exception, risks identified and other issues encountered).
Other outputs (used by all elements of the Service Lifecycle):

- Updated data, information and knowledge in the CMS and SKMS (see Knowledge Management);
- Test incidents, problems and error records;
- Improvement ideas for Continual Service Improvement; and
- Feedback for any third party relationships including suppliers, vendors and partners.

8.7.9 Key Performance Indicators (KPIs) of Service Validation and Testing

Service Provider metrics:

Internal metrics from the service provider’s perspective are primarily concerned with the effective and efficient execution of the Service Validation and Testing process. These include:

- Reduced error rate in later testing stages or production;
- Number of known errors documented in earlier testing phases;
- Effort and cost to configure testing environment;
- Reduction of repeat errors;
- Re-use of testing data;
- Percentage of errors at each lifecycle stage; and
- Percentage of incidents and errors caused by externally supplied/controlled component.

Business/Customer metrics:

The primary purpose for testing and validation is to provide a level of confidence in the value being created by a new or modified service. The effectiveness of testing and validation in providing this confidence can be measured by:

- Early validation that the service will deliver the predicted value;
- Reduction in the impact of incidents and errors in the live environment due to transitioned services;
- More effective use of the service by the end-user community;
- Clear understanding of roles and responsibilities for the transitioned service; and
- Reduced cost and resources required due to customer and end-user involvement.
8.8 Service Evaluation

Evaluation is a generic process that considers whether the performance of something is acceptable, value for money is appropriate and whether it will be accepted to be built/purchased/deployed etc.

8.8.1 Goals and objectives

The purpose of evaluation is to provide the capability for consistent and standardized methods that can determine the performance and value of a service change. The actual performance of a change is assessed and compared against the predicted performance, with any deviations between the two being managed for risk.

When interfaced with Change Management, evaluation will assist in providing accurate information and in managing stakeholders’ expectations. This adds value by:

- Evaluating the intended effects and as much of the unintended effects as is reasonably practical for the service change being transitioned; and
- Providing timely and accurate information to assist Change Management is deciding whether a service change will be approved or rejected.

8.8.2 Scope

Within Service Transition, the process considers the evaluation of new or changed services defined by Service Design, during deployment and before final transition to service operations.

The importance of evaluating the actual performance of any service change against its anticipated performance is an important source of information to service providers to help ensure that expectations set are realistic and to identify that if there are any reasons that production performance does not meet what was expected. Continual Service Improvement can benefit by identifying areas that can be analyzed for future improvements to the process of change and evaluation.
8.8.3 Benefits

Change Management is the primary beneficiary of enhanced evaluation, with improved capabilities in the determination of the value being delivered by a service change and whether any identified risks are unacceptable to the business, customers or existing IT services.

8.8.4 Principles of Evaluation

The Evaluation process follows the Plan-Do-Check-Act (PDCA) model to ensure consistency across all evaluations. When performed correctly, the PDCA model allows enhanced improvement and organizational learning to occur while managing risks that may affect the success of the improvement action or initiative.

![Plan-Do-Check-Act (PDCA) Model](image)

8.8.5 Evaluation Activities

The key activities of Service Evaluation are shown in the figure below. These activities are:

1. Plan the evaluation.
2. Evaluate Predicted Performance.
3. Evaluate Actual Performance.
4. Risk Management.
1. Plan the evaluation

The key factor in planning the evaluation is the consideration of the perspectives required, including the business, customers, end-users, service provider, suppliers and other key stakeholders. When all the appropriate stakeholders are involved in the evaluation, it assists in understanding all of the intended and unintended effects of the service change being transitioned. If the RFC and associated change documentation is ambiguous, it could mean the implications are not fully understood and it will be more difficult to identify the most suitable roles to include for evaluation.

The change documentation should already specify what the intended effects of the change will be and how they will be measured. It these are unclear or ambiguous the evaluation should stop, with a recommendation for further analysis to be communicated back to Change Management.
Through evaluation the involved stakeholders can also identify any potential effects that have not already been identified, which can, depending on the risk, require further analysis through Change Management.

2. Evaluate Predicted Performance

Using the input Service Design Package (including all relevant Acceptance criteria), a comparison is made with the predicted performance, evaluating whether any differences will cause unacceptable risks. An interim evaluation report will be provided to Change Management, highlighting the outcomes of this comparison, together with a recommendation whether to reject or accept the service change in its current form.

3. Evaluate Actual Performance

After the service has been implemented, a report on the actual performance is generated by service operations and compared against the Service Design Package and performance models defined. Like before, an evaluation is made as to whether the actual performance is creating unacceptable risks or if there have been any unintended effects that have occurred.

The second interim report produced describes the outcome of this evaluation and provides a recommendation to Change Management whether the service change should be rolled back.
4. Risk Management

The evaluations that are performed are designed to manage the risks that might be introduced as a result of the service change. If a risk is determined to require mitigation, plans should be made as to how the threat may be removed, or how recovery techniques can be used to increase the resilience of a service.

![Figure 8.22: Example Risk Profile](https://example.com/risk_profile)

© Crown Copyright 2007 Reproduced under license from OGC


The evaluation report is provided to Change Management, with both interim and final reports being delivered. The evaluation report contains the sections:

- Risk Profile;
- Deviations report;
- Qualification statement (for critical services in regulated environments, e.g. military);
- Validation statement; and
- Recommendations.
8.8.6 Triggers and Interfaces

Triggers:
- Request for Evaluation from Change Management or Service Transition Manager.
- Project Management request for Evaluation.

Inputs:
- Service Design Package (and Acceptance Criteria).
- Test results.
- Associated Service Package.

Outputs:
- Evaluation Reports for Change Management.

8.8.7 Key Performance Indicators (KPIs) for Service Evaluation

Service Provider:
- Reduced failed designs that have been transitioned.
- Reduced cycle time to perform an evaluation.

Business/customer:
- Reduced variance between estimated and actual performance.
- Reduce number of incidents against transitioned service.
8.9 Service Asset and Configuration Management

8.9.1 Goal and objectives

The goal of Service Asset and Configuration Management is to support the agreed IT service provision by managing, storing, controlling and providing information about Configuration Items (CIs) and Service Assets throughout their life cycle. Quality and timely information supplied about CIs and Service Assets will enhance the effectiveness and efficiency of other Service Management processes, and in particular, those used within Service Transition.

Other objectives include:
- To support the business and customer’s control objectives and requirements;
- To minimize the number of quality and compliance issues caused by improper configuration of services and assets; and
- To optimize the service assets, IT configurations, capabilities and resources.

8.9.2 Scope

Asset Management:

The scope of Asset Management includes any IT or service asset used within the Service Lifecycle. It provides a complete inventory of assets and defines who is responsible for their control.

Configuration Management:

Identifies, documents, baselines and maintains Configuration data so that changes to the IT infrastructure can be controlled. It provides a logical model of the infrastructure, recording services, assets and infrastructure and the relationships that exist between them.

It may cover non-IT assets or business products used or involved in the delivery and support of services.
8.9.3 Benefits

The majority of benefits enabled by effective Service Asset and Configuration Management can be seen in improvements of other Service Management processes. By having quality asset and configuration data available, the benefits to other processes include:

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

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

- Better adherence to standards;
- Greater compliance to legal and regulatory obligations; and
- Optimum software licensing by ensuring correlation between licenses needed against the number purchases.

8.9.4 Policies and principles of Service Asset and Configuration Management

There should be clear definition of the scope and objectives for Service Asset and Configuration Management is being planned, which will include how it will interface with existing Change and Release Policies. Asset policies may be applicable for certain asset types (e.g. desktops) and will define how the type of asset will be purchased, managed and disposed accordingly. Initially, the focus may be managing assets and services that are business critical or required as part of legal or regulatory compliance obligations, but over time should begin to include a greater scope of the IT infrastructure.
The Configuration Model:

The development of a configuration model is one of the primary objectives of Configuration Management. The model aims to show the elements making up the infrastructure, attributes describing those elements, and the relationships that exist. Configuration Models assist the IT department in:

- Assessing the impact and cause of incidents and problems;
- Assess the impact of proposed changes;
- To plan and design new or changed services;
- To plan technology upgrades;
- To plan and deploy release packages; and
- To optimize asset utilization, resources and costs.

This should become the SINGLE, COMMON representation of the IT infrastructure, used by all of IT Service Management, the business, customers and any other involved party. The level of information recorded can vary, with more detail applied for complex or critical infrastructure and services, or those with particular compliance needs.

Figure 8.23: Example of a Configuration Model
### 8.9.5 Terminology

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Item (CI):</td>
<td><strong>ANY</strong> component that supports an IT service (except people). <strong>Example:</strong> IT components or associated items such as Request for Changes, Incident Records, Service Level Agreements.</td>
</tr>
<tr>
<td>Attribute:</td>
<td><strong>Specific</strong> information about CIs. <strong>Example:</strong> Size of RAM, hard drive, bandwidth.</td>
</tr>
<tr>
<td>CI Level:</td>
<td>Recording and reporting of CIs at the level that the <strong>business requires</strong> 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.</td>
</tr>
<tr>
<td>Status Accounting:</td>
<td>Reporting of all <strong>current and historical</strong> data about each CI throughout its lifecycle. <strong>Example:</strong> Under Development, being tested, live, withdrawn etc.</td>
</tr>
<tr>
<td>Configuration Baseline:</td>
<td>Configuration established at a specific point in time. Captures both the structure and details of a configuration. Used as a reference point for later comparison (e.g. After major changes, disaster recovery etc).</td>
</tr>
</tbody>
</table>

### 8.9.6 The Configuration Management System (CMS)

The CMS is a set of one or more connected information sources that provide a logical model of the IT infrastructure. It captures Configuration Items (CIs) and the relationships that exist between them. The figure below demonstrates a simplified representation of the CMS.
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.
Figure 8.25: Example of a Configuration Management System

© Crown Copyright 2007 Reproduced under license from OGC
1. Management and Planning

Planning for configuration management should seek to define the objectives, scope and level as early as possible, as well as how these objectives will be achieved. Depending on the scale of implementation, a formal project may be appropriate to plan, manage and control the work performed and deliverables required.

The development of a Configuration Management plan should document the overarching strategy for Configuration Management, including the scope and level, what activities are performed and how the process will be controlled. The scope and level needs to be carefully chosen, as many implementations fail when organizations try to achieve too much, too soon with Configuration Management. Instead, an approach driven by continual improvement should be taken, that seeks to develop the maturity and scope of Configuration Management, and to increase value provided by its use.
Example contents of a Configuration Management Plan:

- Context and Purpose
- Scope
  - Applicable Services
  - Environments and infrastructure
  - Geographical Locations
- Requirements
  - Links to policy, strategy, Service Management and contractual requirements
  - Summarize accountability, traceability, auditability requirements
  - Link to requirements for the Configuration Management System (CMS)
- Applicable policies and standards:
  - Change Management, Release, Transition Policies
  - ISO/IEC 20000, 197000/1
- Organization for Configuration Management
  - Roles and responsibilities
  - Change and configuration control boards
  - Authorization mechanisms, for establishing baselines, changes and releases
- Asset and Configuration Management Systems and Tools
  - Configuration Identification
  - Version management
  - Interface management
  - Supplier management
  - Release and deployment
  - Build Management
  - Establishing and maintaining configuration baselines
  - Maintaining the CMS
  - Reviewing and auditing the integrity of configurations and the CMS
- CMS Housekeeping
  - Data migration
  - Backups
  - Archiving Data
- Links to business processes/customer capabilities
  - Financial Management
  - Procurement
  - Project Management
  - Customer Service
  - Human Resources
2. Identification:

Identification includes the selection, detection, labeling and registration of CIs. It is the activity that determine 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; and
- Documentation.

Identification is also used to define the approach and techniques utilized by Configuration Management, including the specification of:

- How the classes and types of assets and CIs are to be selected, grouped and classified;
- The approach to identification, including the naming and labeling conventions to be used; and
- Define the roles and responsibilities for the owner or custodian of CIs.

![Figure 8.27 – Example configuration breakdown for an IT Service](image-url)
The identification activity includes the tasks:
1. Defining and documenting selection criteria for CIs;
2. Select CIs for recording based on selection criteria;
3. Name and label CIs;
4. Specify the relevant attributes for each CI;
5. Specify when each CI is brought under the control of Configuration Management; and
6. Identify the owner responsible for each CI item.

Some identification tasks explained:

1. Defining and documenting selection criteria for CIs.
2. Selecting CIs for recording based on selection criteria.

The configuration model should provide information describing the relationship and composition of CIs in each structure. As discussed earlier, an important part of Management and Planning is deciding the level at which recording is to occur and control will be exercised. This should be performed using a top down approach, where top-level CIs are broken down into components, which in turn may be CIs themselves. When choosing the appropriate level, it involves weighing up the benefit that the information will bring against the cost and effort required to maintain accurate information for each CI. Generally, CI information is valuable if it facilitates the management of change, the identification and resolution of incidents and problems, or must be recorded for legal and regulatory compliance.

The figure showing an example configuration breakdown for an IT service describes how the service is broken into relative component CIs, some of which are document CIs, and describes the relationships that exist between CIs.

3. Name and Label CIs

Configuration Management should work with Release and Deployment to establish policies regarding the naming conventions of CIs, baselines, builds and releases and assemblies. Each individual CI should be uniquely identifiable using an identifier and version reference. The version describes the exact instance of what may be considered the same CI. Naming conventions should also take into account any existing corporate or supplier structures.
Physical CIs should be labeled with the identifier and version so that they can be easily identified in the physical environment. Measures are required to ensure that:

- Identifiers printed on tags are unique;
- Tags are difficult to remove or can be identified if removed; and
- Tags are attached at a fixed, visible and accessible spot depending on the CI type.

Adding a barcode to the tag can also improve the efficiency and reliability of any reviews or audits that are performed over time.

For releases, identification includes a reference to the CI that it represents and a version number that will normally have two or three parts. As an example:

- Major releases: Banking_System v.1, v.2, v.3 etc.
- Minor releases: Banking_System v.1.1, v.1.2, v.1.3 etc.
- Emergency fix releases: Banking_Systen v.1.1.1, v.1.1.2 etc.

4. **Specify the relevant attributes for each CI**

Attributes are recorded that describe specific characteristics that are valuable for the management and control of change, and general management of each CI.

Typical CI attributes include:

- Unique identifier/label for CI;
- CI type;
- Name/description;
- Version;
- Location;
- Supply date;
- License details and expiry date;
- Owner/Custodian;
- Status;
- Supplier/source;
- Related documents;
- Historical data;
- Relationships to other CIs; and
- Applicable SLA(s).
3. Configuration Control:

Configuration Control is used to ensure that only authorized and identifiable CIs are recorded from receipt to disposal, in order to protect the integrity of the CMS. Control occurs anytime the CMS is altered, including:

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

Methods to ensure Configuration Control are wide ranging and include a mix of manual and automated mechanisms, with interfaces into existing asset management systems, service management tools, procurement systems etc. Control should be passed from the project or supplier to the service provider at the scheduled time and with accurate configuration records. For small organizations, Configuration Control may be primarily utilized by a Configuration Librarian, however for large and complex infrastructures, more automated mechanisms and delegation of authority for CI upkeep will be required.

4. Status Accounting:

Status Accounting provides the capability for the reporting of all current and historical data concerned with each CI throughout its lifecycle. Each CI will progress through various states, with each state being of significance to the management of the CI.

Typical states include:

- Registered;
- Development or draft;
- Approved;
- Installed;
- Under Change/Maintenance; and
- Withdrawn.

The use of status reporting will provide information on:

- Configuration baselines;
- Latest software item versions;
- The person responsible for status change;
- CI change/incident/problem history; and
- Changes implemented and in progress.
Status reports of assets for a business unit are often required by financial management for budgeting, accounting and charging. For the service provider, reports on the number of software license holdings can be used to assess any over or under licensing in the software environment.

**Verification and Audit:**
Reviews and audits should be used to verify the existence of CIs, checking that they are correctly recorded in the CMS and that there is conformity between the documented baselines and the actual environment to which they refer. Specifically, the results ensure:

- Conformity between the CMs and live environment;
- The physical existence of CIs match those recorded in the CMs; and
- The appropriate configuration documentation is provided before a release.

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; and
- At other determined regular intervals.

Any unregistered or unauthorized CIs detected during an audit should be recorded and investigated, with corrective action taken to rectify the exception and to address possible issues with procedures and the behavior of staff.

Automated tools should be utilized for regular checks, with corrective measures restoring CIs to a baselined version where exceptions are found (e.g. a desktop found with unauthorized software installed). Continual training and awareness campaigns should be maintained so that staff understand the importance of Configuration Management, the procedures required, and what implications and non-conformance can have.

### 8.9.8 Triggers and Interfaces

Most updates to the CMS are triggered by:

- Change requests;
- Incidents and Problems;
- Purchase orders;
- Service Requests; and
- Exceptions found during reviews and audits.
While almost every aspect of Service Management is supported by the information maintained within the CMS, some important interfaces are:

- Change Management, using CMS data for the assessing the impact of changes;
- Financial Management, using the CMS to capture key financial information;
- Capacity Management, using CMS data to identify potential bottlenecks in the infrastructure; and
- Availability Management, using CMS data to identify single points of failure and for component failure analysis.

Most important out of all the Service Lifecycle relationships however, are those maintained with the other Service Transition processes as discussed in this volume.

### 8.9.9 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; and
- 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; and
- To support the information needs of other ITIL® processes.

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

- Service Asset Manager;
- Configuration Manager;
- Configuration Analyst;
- Configuration Administrator/Librarian;
- CMS/Tools Administrator; and
- Change Manager (all Changes to CIs must be authorized by Change Management).
8.9.10 **Key Performance Indicators (KPIs) for Service Asset & Configuration Management**

Much of the focus for determining the value contribution of Configuration Management requires analyzing improvements seen in the other Service Management processes. Potential metrics demonstrating this contribution include:

- Improved speed for Incident and Problem Management for identifying and analyzing the cause and potential effect;
- Improved ratio of used licenses against paid for licenses, should be very close to 100 per cent;
- Percentage re-use and redistribution of under-utilized assets and resources;
- Improved alignment between provided maintenance and business support; and
- Improvement in maintenance scheduling and management for CIs.

Other metrics focused on the effectiveness and efficiency of the process specifically include:

- Improved quality and accuracy of configuration information;
- Decreasing number of exceptions detected during audits;
- Improved utilization of automation; and
- Increased efficiency for activities performed.
8.10 Knowledge Management

The quality of decision making within the Service Lifecycle depends on the ability and understanding of those parties involved, the understanding of the benefits and consequences of actions taken, and the analysis of any of the surrounding issues involved. All of this in turn depends on the availability of accurate and timely knowledge, information and data, provided in a way that can be easily accessed and interpreted by the appropriate parties.

8.10.1 Goal and Objectives

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.

The objectives of Knowledge Management are:

- Enabling the service provider to be more efficient and improve quality of service, increase satisfaction and reduce the cost of service;
- Ensuring staff have a clear and common understanding of the value that their services provide to customers and the ways on which benefits are realized for the use of those services; and
- Ensuring that, at a given time and location, service provider staff have adequate information on:
  - Who is currently using their services;
  - The current states of consumption;
  - Service delivery constraints; and
  - Difficulties faced by the customer in fully realizing the benefits expected from the service.

8.10.2 Scope

While Knowledge Management is found, and primarily explained within the context of Service Transition, it is a process used by all elements of the Service Lifecycle to improve the decision making that occurs.

What is not considered to be within the scope of Knowledge Management is the detailed Configuration Item information that is captured and maintained by Service Asset and Configuration Management (but is interfaced with the same tools and systems).
Benefits:
With particular focus on Service Transition, knowledge is one of the important elements that need to be transitioned as part of the service changes and associated releases being managed. Examples where successful transition requires effective Knowledge Management include:

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

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

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

8.10.3 Challenges faced by Knowledge Management

- Getting staff to use the systems;
- The time required to record relevant information and knowledge after actions are completed;
- Managing information and knowledge that is no longer correct or relevant for the organization; and
- Designing a system that can scale with an organization as it 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.
8.10.4 Policies and principles of Knowledge Management

Data, Information, Knowledge, Wisdom (DIKW)

Knowledge Management is usually seen within the context of the DIKW structure seen below.

![Moving from data to wisdom](image)

**Data:**
Data is a set of discrete facts. Most organizations capture significant amounts of data every day. Knowledge Management activities seek to improve the capabilities for capturing, analyzing, synthesizing data and transforming it into information.

**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 Management focuses on measures for capturing, finding and reusing information so that work is not duplicated.

**Knowledge:**
Knowledge is composed of the experiences, ideas, insights and judgments from individuals and from their peers. This usually requires the analysis of information, and is applied in such a way to facilitate decision making.
Wisdom:
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 the ability to use knowledge to make correct judgments and decisions.

8.10.5 The Service Knowledge Management System (SKMS)

![Figure 8.29: Components making up the Service Knowledge Management System]

SKMS: Service Knowledge Management System (SKMS):

The SKMS describes the complete set of tools and databases that are used to manage knowledge and information, including the Configuration Management System as well as other tools and databases. The SKMS stores, manages, updates and presents all information that an IT service provider needs to manage the full lifecycle of its services. The main purpose of the SKMS is to provide quality information so that informed decisions can be made by the IT service provider.
Whereas the CMS focuses on providing information relating to the configuration of the IT infrastructure, the SKMS has a broader scope (as implied by the diagram) which includes anything pertaining to the needs of service management, including:

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

### 8.10.6 Knowledge Management Activities

The activities of Knowledge Management can be grouped into the following elements:

1. Knowledge Management strategy.
2. Knowledge transfer.
3. Data and information management.
4. Using the service knowledge management system.

#### 1. Knowledge Management Strategy

An overall strategy for Knowledge Management (for IT Service Management) should be developed that describes the approach taken by the organization, and how it fits within the larger concept of Knowledge Management (corporate-wide) practices already in place.

The strategy will address:

- Governance Model;
- Organizational changes;
- Establishing roles and responsibilities;
- Policies, processes, procedures and methods for KM;
- Technology and other resource requirements; and
- Performance measures.

The strategy should identify and plan for the capture of relevant knowledge and the consequential information and data that will support it. This will include:

- Assisting an organization to identify knowledge that will be useful;
- Designing a systematic process for organizing, distilling, storing and presenting information in a way that improves peoples understanding in relevant areas;
- Accumulating knowledge through processes and workflow;
- Generating new knowledge;
- Accessing valuable knowledge from outside sources; and
- Capturing external knowledge from diverse sources such as databases, websites, employees, suppliers and partners.
2. Knowledge transfer

Throughout the service lifecycle, an organization will capture, manage and provide knowledge though problem solving, dynamic learning, strategic planning and decision making. To support this, many of the service management processes will be interfaced with knowledge management so that knowledge transfer can occur from one unit to another (or several). Traditional knowledge transfer relied on formal face-to-face training and documentation, with representatives of each group cascading the knowledge to their working colleagues. In the modern age however, this is supported by a range of techniques including:

- ‘Hands-on’ (tactile) learning;
- Knowledge visualization (visuals, diagrams, images, photographs etc);
- Seminars, webinars and advertising;
- Journals and newsletters; and
- Awareness sessions.

3. Data and Information Management

For efficiency purposes, Knowledge Management must define what inputs will provide data and information, and how this will be used for decision making at all levels. This covers the monitoring, capture, use and distribution of data and information, and what mechanisms can be utilized to reduce the manual workload required.

The three main elements involved are:

- Establishing data and information requirements:
  - Defines the policies and standards to follow when collecting and using data and information;
  - Encourages the use of common and uniform content;
  - Establishes the requirements for security, privacy and ownership;
  - Defines access requirements; and
  - Considers any interfaces required to Change Management.

- Establishing data and information management procedures:
  - Defines procedures for the storage and retrieval of data and information;
  - Establishes procedures for adequate backup and recovery of data;
  - Identifies the review and audit procedures required; and
  - Implements the mechanisms required to capture, store and retrieve data and information from desired sources.

- Evaluation and improvement:
  - Seeks continuous improvement for the capture, use and re-use of data and information; and
  - Identifies data and information sources that are no longer needed.
4. Using the SKMS

A service provider must first establish a SKMS that can be shared, updated and used by its operating entities, partners and customers. All training and knowledge material needs to be aligned to the business perspective. Materials to be included are:

- Business language and terminology; and
- Business processes and where IT underpins them.

8.10.7 Triggers and Interfaces

As previously discussed, Knowledge Management provides value and capabilities throughout the entire Service Lifecycle, and is used in different contexts depending on the requirements for information and knowledge. Some of the primary interfaces however, are those within the processes of Service Operation and those within Service Transition.
Service Operations – Errors within the service detected during transition will be recorded and analyzed and the knowledge about their existence, consequences and workarounds will be made available to Service Operations in an easy-to-use fashion:
- Front line incident management staff, on service desk and second-line support, are the point of capture for much of the everyday ITSM data.
- Problem Management staff will be key users of collected knowledge and typically responsible for the normalization of data capture by means of developing and maintaining scripts supporting data capture within Incident Management.

Service Transition – Staff capture data of relevance through all lifecycle phases and so need to be aware of the importance of collecting it accurately and completely. Service Transition staff capture data and information:
- Relevant to adaptability and accessibility of the service as designed, to be fed back, via CSI, to Service Design; and
- ‘Course corrections’ and other adaptations made to the design required during transition. Awareness and understanding of these will make future transitions easier.

8.10.8 Key Performance Indicators (KPIs) of Knowledge Management

When planning to implement Knowledge Management, thought should be given as to how the benefits will be measured how to make these benefits visible to all levels of the organization.

Normal measures for the benefits of Knowledge Management include:
- Successful implementation and early life operation of new and changed services with few knowledge-related errors;
- Increased responsiveness to changing business demands;
- Improved accessibility and management of standards and policies;
- Knowledge dissemination;
- Reduced time and effort required to support service;
- Reduced time to find information for diagnosis and fixing incidents and problems;
- Reduced dependency on personnel for knowledge;
- Reduction in the ‘user error’ category of incidents;
- Enhanced customer experiences and satisfaction; and
- Reduced time for transition and duration of early life support.
Measures directly relevant to the service provider are:
- Usage of the knowledge bases;
- Contributions made to knowledge bases;
- Errors reported by staff or in audits;
- Degree of re-use for information and knowledge;
- Satisfaction of staff with training and knowledge transfer methods; and
- Involvement of staff in knowledge gathering exercises (e.g. forums).

Figure 8.31 Contribution of knowledge to effectiveness of support staff
© Crown Copyright 2007 Reproduced under license from OGC
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.

Objectives of Service Operation

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; and
- Supporting operations through new models and architectures such as shared services, utility computing, web services and mobile commerce.
9.1 Benefits of Service Operation

Service Operations is where plans, designs and optimizations are executed and measured, and from a customer viewpoint where the actual value of IT is seen. Specific benefits delivered as a result of improved Service Operation includes:

- Effectiveness and efficiency in IT Service delivery and support;
- Increased return on investment (ROI);
- Increased value on investment; and
- Increase customer and user satisfaction.

As Service Operation is the most visible aspect of the service lifecycle and IT organization, it brings certain challenges that need to be considered. These include:

- Once a service has been designed and tested it is expected to run within the budget and ROI targets established much earlier in the lifecycle. Generally, planning of costs for the ongoing management of services is ineffective. It is relatively easy to quantify the costs of a project, but very difficult to quantify what the service will cost after three years of operation.
- Obtaining funding during the operational phase can be difficult. Design flaws may need to be fixed, but as this is not part of the original value proposition there can be a reluctance to provide more funds. Most organizations do not have a formal policy/procedure to review operational services for design and value – issues are generally left to Incident/Problem Management to resolve.
- Additional funding for tools and training aimed at improving the efficiency of a service in Service Operation can be equally as difficult to get. Partly, because the expectation is the costs are built in to the cost of the service from the beginning and because they are directly linked to the functionality of a specific service.

These are challenges that should be considered in any implementation or improvement of Service Operation, requiring analysis of how the other service lifecycle phases in turn will be affected. Generally, the benefits that will be seen after implementation/improvement can be divided into two categories:

**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 Service Transition (e.g. deployment of new tools, changes to process designs, reconfiguration of the infrastructure).

**Short term:** Improvement of working practices within the Service Operation processes, functions and technology itself. Generally these are smaller improvements that do not mean changes to the fundamental nature of a process or technology (e.g. tuning, training, personnel redeployment).
9.2 Interfaces to other Service Lifecycle Phases

As the focal point for delivering and managing IT services, there are many interfaces that connect Service Operation within the rest of the service lifecycle.

Inputs from the Service Strategy phase:
- Service Portfolio Information;
- Customer and Business Portfolios;
- Supplier and Vendor Contracts Information;
- Policies;
- Organizational Strategies;
- Constraints, Compliance Obligations, Regulations;
- Architectures; and
- Service Management Plan (a requirement of ISO/IEC 20000).

Inputs from the Service Design phase:
- Service Definitions;
- Service Architecture & Structure (including core and supporting services);
- Cost models;
- Capacity/Resource models;
- Availability and Capacity plans;
- Acceptance Criteria;
- Request For Change (RFC) to initiate the required changes to the environment; and
- Service Level Agreements, Operational Level Agreements, and Underpinning Contracts.

Inputs from the Service Transition phase:
- Release Packages, including all new/modified software, hardware, documentation and associated knowledge transfers;
- Requests for evaluation for change assessments;
- Change Models and associated procedures, primarily those catering for normal changes;
- Service Asset and Configuration data;
- Knowledge, information and data to be utilized during Service Operation; and
- Pilot service changes, including testing and validation by the pilot end-user community.

Inputs from the Continual Service Improvement phase:
- Service Improvement Plans impacting on Service Operations;
- Guidance for measuring and reporting to be conducted during Service Operations;
- Improvement initiatives to processes and functions; and
- Refined models and SLA targets.
Figure 9.2: Some outputs to other lifecycle phases.
9.3 Principles of Service Operation

As the centre point for the majority of activity in an IT organization, Service Operation will be faced with many challenges in achieving a balance between all varying objectives defined and perspectives that are required. Perspectives that are considered include:

- Technology – focusing on ensuring a consistent architecture, the effective functioning of individual components and continually investigating and leveraging new technologies being developed;
- IT Service Management – focusing on executing and performing the processes that optimize the cost and quality of service delivered; and
- Organization – focusing on the capabilities being provided that enable the business to meet its objectives, enhanced productivity for users and support for future business growth.

The following sections examine the balances that must be addressed and achieved by Service Operation in light of the perspectives described above.

9.3.1 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.
1. **Internal IT view versus external business view**

The most fundamental conflict in all phases of the ITSM Lifecycle is between the view of IT as a set of IT services (the external business view) and the view of IT as a set of technology components (internal IT view).

The **external view** of IT is the way in which services are experienced by their users and customers. They do not always understand or care about the details of what technology is used to manage those services. All they are concerned about is that the services are delivered as required and agreed.

The **internal view** of IT is the way in which IT components and systems are managed to deliver the services. Since IT systems are complex and diverse, this often means that the technology is managed by several different teams or departments – each of which is focused on achieving good performance and availability of its systems.

*Figure 9.3: – Achieving a balance between internal and external focus*

© Crown Copyright 2007 Reproduced under license from OGC
### Examples of internal focus (extreme)

- Improvement initiatives focus on the efficiency of internal processes and how to improve the stability of core infrastructure.
- Metrics focus on SLA elements for individual calls/requests, such as call pickup & call resolution timeframes, and the number of escalations required.
- Changes are primarily assessed from the perspective of protecting the IT infrastructure and current service levels agreed.
- Procedures focus on how to manage the technology.
- Budgets allocated around technology improvements or initiatives seeking long term cost reduction.

### Examples of external focus (extreme)

- Improvement initiatives focus on improving business outcomes or the user experience, with little regard as to how this will be delivered.
- Metrics focus on the customer experience including satisfaction levels and effectiveness of communication with IT.
- Changes are primarily assessed from the perspective of delivering enhanced capabilities for business processes, opportunities and growth.
- Procedures focus on what needs to be achieved and less on how it needs to be done.
- Budgets allocated by projects associated with business units. Less visible business units and common IT capabilities are often underfunded.

Achieving this balance is particularly difficult given the nature of service management and its focus on structuring services around the needs of customers and the business. But by neglecting the internal needs of the IT department or to not satisfactorily plan for how services will be delivered, the quality of service experienced by customers and the business will ultimately suffer.

Developing Service Operation with capabilities that achieve a balance between internal and external focus requires effective communication practices and an approach that is reflected in all aspects of the service lifecycle. Factors that will support the ability to achieve this balance include:

- Communication and understanding of the strategic objectives for the IT department;
- Understanding about the portfolio of services being offered to the business and what value they create;
- Understanding about the strengths, weaknesses, priorities and risks that affect the IT organization in its approach to delivering services;
- Different metrics that report the service achievements to those used for reporting on the effectiveness and efficiency of Service Operation;
- Involvement of IT Operations staff in the design and transition phases for services; and
- Clear communication and training plans that extend to service operations, rather than being limited to projects
- Budgets that allocate funds to common operation capabilities as well as specific business unit projects.

2. Stability versus responsiveness

As discussed in section 4.1.1: Creating Service Value, to truly provide the desired value in services, both service utility (functionality) and service warranty (availability and performance) need to be of satisfactory levels and meet customer requirements. But as the business changes so do the demands for the functionality and performance to be provided. This presents a challenge to the IT organization, in that every time new and modified services are transitioned into the production environment, there is the potential for disruption and negative impact on the IT infrastructure, services and associated customers.

Service Operation needs to be managed with consideration as to how to balance the needs for change against the requirements for stability (or availability) for IT services. Part of this consideration is planning how emergency changes will be managed in such a way that their implementation doesn’t impact on service quality.

![Figure 9.4: Achieving a balance between stability and responsiveness](image-url)

**Figure 9.4: Achieving a balance between stability and responsiveness**

© Crown Copyright 2007 Reproduced under license from OGC
### Examples of stability focus (extreme)

- Improvement initiatives focus on how to improve the stability of core infrastructure, or supporting IT service management processes.
- Customers and business units indicate lowered satisfaction IT despite SLA targets for availability and responsiveness being met.
- All new technology and services must fit within existing technology architectures, any exceptions are rejected.
- Procedures focus on how to manage the technology and reduce service disruption.
- Capacity Management forecasts requirements based on current workloads and utilization levels. Tuning and demand management are the major activities performed.

### Examples of responsiveness focus (extreme)

- Improvement initiatives focus on improving business outcomes, support for new market spaces and business opportunities. Potential impact on existing services may not be appropriately assessed.
- Routine tasks begin to be missed or ignored as IT staff are busy working on new projects and service changes.
- Technology is implemented with little assessment as to any incompatibility or over-provisioning that may occur.
- Procedures focus on what needs to be achieved and how to reduce bottlenecks in the Change and Request processes.
- Capacity Management forecasts projections based on patterns of business activity and does not take into account current IT workloads and utilization.

While it is unlikely that many organizations display any of the above characteristics exactly, they are useful for indicating which focus they are more aligned to. Developing Service Operation that achieves a balance between stability and responsiveness requires the following:

- Utilization of technologies that can be adapted and modified effectively (such as virtual servers);
- Strong links between Service Level Management (SLM) and the Service Operation processes, so that the operational activities deliver value to business operations;
- Integrate Change Management early in the lifecycle, so that business, technical and manageability requirements can be assessed and provided;
- Strong relationships with the business and open lines of communication. This assists IT in being involved in decisions regarding business change; and
- Develop training for both IT and business staff about the value of the service operation processes and how they are used.
3. Quality of service versus cost of service

Many IT organizations are expected to consistently deliver stable (or higher) levels of quality with continually reduced budgets and costs. When faced with this situation, most organizations are affected by some loss of service quality, which in some extreme circumstances have the potential to cost much more than it would have to fund the service appropriately.

Ideally Service Operation should seek to deliver consistent levels of quality to the business and customers while keeping costs and resource utilization at optimal (not lowest) levels.

Achieving the optimum balance is important. If too much focus is on cost, the likely result is an IT organization that delivers sub-standard services, putting the associated customers and business at risk. On the other hand, too much focus on quality will ultimately lead to higher costs, and quality levels that are greater than the business requirements stipulate. There is no simple calculation to determine whether optimum balance has been reached, but instead constant communication driven by SLM will help to understand and recognize the warning signs that the balance is being threatened.
The figure above demonstrates the spending required for making improvements to the quality of services. In some cases, funds are needed to make the improvements, in others improvements can be made with reduced costs. As shown in the figure, an optimum range exists where a balance can be achieved between effective levels of quality and acceptable costs. Above this range, the costs to make further improvements (e.g. improving availability levels from 98% to 99.7%) become significantly more expensive, in many cases to the point of not being economically viable.
### Examples of quality focus (extreme)

- Business cases are not created for expenditure within/on IT. Spending instead is authorized by IT/business managers based on a desired outcome or current requirement not being filled.
- High availability levels are provided for all services, rather than varying levels dictated by business criticality and priority.
- New technologies are continually implemented in order to stay in touch with other competitors and to increase customer satisfaction levels.
- The portfolio of services is continually refreshed, seeking to improve the value being created by all IT services.

### Examples of cost focus (extreme)

- Any spending on IT is subject to approval, requiring justification as to what efficiency savings it will enable, or other potential business benefits. Common activities and basic requirements like training are often ignored.
- IT Service Continuity measures are underfunded, as no major disruption has occurred in the past.
- Technology implementations focus on removing constraints in business processes, such as reducing the full-time employee (FTE) requirements of the organization.
- Investments into IT are usually linked to projects and linked into enhancing the efficiency of business processes/units.
4. Reactive versus Proactive

A reactive organization is one which does not act unless it is prompted to do so by an external driver, e.g. a new business requirement, an application that has been developed or escalation in complaints made by users and customers. An unfortunate reality in many organizations is the focus on reactive management mistakenly as the sole means to ensure services that are highly consistent and stable, actively discouraging proactive behavior from operational staff.

A proactive organization is always looking for ways to improve the current situation. It will continually scan the internal and external environments, looking for signs of potentially impacting changes. Proactive behavior is usually seen as positive, especially since it enables the organization to maintain competitive advantage in a changing environment. However, being too proactive can be expensive and can result in staff being distracted. The need for proper balance is reactive and proactive behavior often achieves the optimal result.

![Figure 9.7: Achieving a balance between extremely reactive and extremely proactive](image)

Generally, it is better to manage IT services proactively, but achieving this is not easily planned or achieved. This is because building a proactive IT organization is dependent on many variables, including:

- The maturity of the organization;
- The culture of the organization;
- The role that the IT plays in the business and the mandate that IT has to influence the strategy and tactics of the business;
- The level of integration of management processes and tools; and
- The maturity and scope of Knowledge Management in the organization.
While proactive behavior in Service Operation is generally good, there are also times where reactive behavior is needed. The role of Service Operation is therefore to achieve a balance between being reactive and proactive. This will require:

- Formal Problem Management and Incident Management processes, integrated between Service Operation and Continual Service Improvement;
- The ability to be able to prioritize technical faults as well as business demands. This needs to be done during Service Strategy and Design;
- Data from Configuration and Asset Management to provide data when required, saving projects time and making decisions more accurate; and
- Ongoing involvement of SLM in Service Operation.

<table>
<thead>
<tr>
<th>Extreme Reactive</th>
<th>Extremely Proactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IT Department responds to business needs and incidents only after they are reported.</td>
<td>• IT Department anticipates business before they are reported and problems before they occur.</td>
</tr>
<tr>
<td>• Capacity Management waits until there are capacity problems and then purchases surplus capacity to last until the next capacity related incident.</td>
<td>• Capacity Management anticipates capacity problems and spends money on preventing these - even when the scenario is unlikely to happen.</td>
</tr>
<tr>
<td>• No ITSCM plans exist until after a major event or disaster.</td>
<td>• Over-planning (and over-spending) of IT Recovery options. Usually immediate recovery is provided for most IT services, regardless of their impact of priority.</td>
</tr>
<tr>
<td>• ITSCM plans focus on recovering key systems, but without ensuring that the business can recover its process.</td>
<td></td>
</tr>
<tr>
<td>• Changes are often not logged, or logged at the last minute as Emergency Changes.</td>
<td>• Changes are requested and implemented even when there is no real need, i.e. a significant amount of work done to fix items that are not broken.</td>
</tr>
<tr>
<td>• Changes are poorly tested and controlled, resulting in a high number of incidents.</td>
<td></td>
</tr>
</tbody>
</table>
9.4 Event Management

For Service Operation to be successful in its goal of effective and efficient delivery and support of services, there is a strong requirement for the status of the infrastructure to be clearly visible, and to have capabilities for detecting any deviation from normal service operation. Typically this is made possible by two types of tools:

- Active monitoring tools that continually ‘ping’ Configuration Items (CIs) to determine their status and availability; and
- Passive monitoring tools that detect and escalate alerts or communications generated by CIs.

When performed effectively, the workload of Incident and Problem Management can be reduced, and improve the overall quality of service experienced by customers and end-users. However care needs to be taken that an appropriate balance is maintained that provides the foundation for effective Service Operation, but doesn’t overwhelm IT staff with alerts and notifications.

![Image](image-url)

*Figure 9.8: Event Management provides increased visibility regarding the status of IT infrastructure*

9.4.1 Goals and Objectives

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.

### 9.4.2 Scope

Event Management can be applied to any aspect of Service Management that needs to be controlled and which can be automated. These include:

- CIs - to provide visibility of functioning and failing components, or to understand when other changes have occurred in the infrastructure;
- Environmental conditions – such as increases in the temperature of servers and facilities;
- Software license monitoring – used to maintain optimum licensing utilization;
- Security – to perform security checks and to detect exceptions or intrusions; and
- Normal activity – such as tracking the activity and performance of an IT service.

It is important to note the difference between monitoring and Event Management. While the two areas are related, Event Management focuses on the generation and detection of notifications about the status of the IT infrastructure and services. Monitoring on the other hand has a broader scope, which will include monitoring CIs that do not generate events or alerts. So when implementing Event Management, consideration should be made as to what monitoring activities and techniques should be interfaced to generate alerts and notifications that will provide value to the IT groups and wider organization.
9.4.3 Benefits

The value to the business of implementing the Event Management process is generally indirect, but it is possible to determine the basis for its value. For example:

- It provides mechanisms for early detection of incidents;
- It enables some types of automation activity to be monitored by exception;
- It shows signal status changes or exceptions that allow the appropriate person or team to perform early response; and
- It provides a basis for automated operations, increasing efficiency and allowing human resources to be better utilized.
9.4.4 Event Management Activities

Figure 9.9: – Typical Activities of Event Management
© Crown Copyright 2007 Reproduced under license from OGC
Activities of Event Management

1. Event occurs.
2. Event notification.
3. Event detection.
4. Event filtering.
5. Significance of event.
7. Trigger.
9. Review actions.
10. Close event.

1. Event occurs

As services are being delivered there will be many events occurring, however not all of them will be captured or detected. It is the role of Service Design and Service Transition to ensure that new and modified services have the capability for event detection and notification as appropriate to the requirements of service management.

Instrumentation is the definition of what can be monitored about CIs and the way in which their behavior can be affected. This includes making decisions such as:
- What needs to be monitored?
- What type of monitoring is required?
- What constitutes an event for this CI?
- What type of information needs to be communicated?
- Who needs to be informed?
- How will events be generated?
- Does the CI already have event generation mechanisms as a built-in feature?
- Where will events be logged and stored?

2. Event notification

Many CIs will already include mechanisms to communicate information about their status and other items of interest. This will typically occur in two ways:
- The device is interrogated by a management tool, often known as polling; or
- The CI generates a notification when certain conditions are met.

In many cases, event notifications are generated using open standards such as SNMP (Simple Network Management Protocol). If Service Operation is involved in the Service Design phase, it provides possibilities for defining which events need to be generated, which would then be tested during Service Transition. This will likely be assessed and modified once the transition has finished, as over time it may occur that too many events
are being generated, or not enough, to effectively manage the CI. The general rule of thumb is that business critical CIs (at the very least) are deployed with the ability to generate event notifications.

A key principle that should be followed is the transmission of meaningful data in notifications. When operators are faced with coded error messages it decreases the efficiency of understanding and response to events. Additionally, this data should include notification of the appropriate party who should be alerted. Without this quality information events will be missed, or there can be the potential for duplication of effort in the response to events.

3. Event detection

As event notifications are generated, the established active and passive monitoring tools will detect, read and interpret the meaning of the event. The use of management tools specifically designed for this purpose can improve the efficiency of event detection, which will typically include additional filtering and escalation mechanisms that can be defined.

4. Event filtering

Filtering is a critical element for Event Management that will prevent operations staff from being overwhelmed with high volumes of event notifications. If there are too many events notifications staff could develop a habit of ignoring events and alerts. Too few alerts and the benefits may not be delivered. Continual tweaking is needed to maintain the correct balance between escalating and ignoring events.

When the management tool is instructed to ignore, the event will usually be logged to a file associated with the device. Filtering may also be used to only escalate an alert for the first event, with future alerts being suppressed (but events still being logged). When conditions allow an event to be escalated, the next step is to understand what type of event has occurred (operational, exception or unusual).

5. Significance of events

While there may be many categories of events that can be defined for any IT organization, it is generally recommended that at least three broad categories are included:

- Events that signify regular operation:
  - Alerts indicating that a backup job was completed successfully;
  - Notifications that a scheduled workload has completed;
  - A user has logged in to use an application; and
  - An email has reached its intended recipient.
- Events that signify an exception:
  - Alerts indicating that a backup job failed;
  - User attempts to log on to an application with the incorrect password;
  - Unusual situation has occurred in a business process that may indicate an exception requiring further business investigation; and
  - Device’s CPU is above the acceptable utilization rate.

- Events that signify unusual, but not exceptional operation:
  - Alert indicating a backup job has taken longer than 30 minutes to finish;
  - Server’s memory utilization reaches within 5 per cent of its highest acceptable performance level; and
  - Completion time of a transaction is 100 per cent longer than normal.

6. Event correlation

When the significance has been determined, correlation is used to compare the event with a set of criteria and rules in a specific order. The rules may have either a technical or business focus, but the underlying reason for correlation is to determine the level and type of business impact of the event.

A ‘Correlation Engine’ should be programmed during the Service Design phase, utilizing the guidelines provided by Service Operation. Correlation Engines will use a number of factors to make decisions, including:

- The categorization of the event;
- The number of similar events have occurred;
- Number of CIs generating similar events;
- Whether the event indicates an exception;
- A comparison against defined threshold levels (e.g. utilization levels); and
- Whether further information is required to investigate further.

These factors should also be used to set a priority level for the event, in order to define the appropriate level of response from the operations group.

7. Trigger

If an event is recognized by the Correlation Engine, defined rules should govern the response that is required. This mechanism is called a trigger. Examples of triggers include:

- Responses that execute scripts for actions such as rebooting devices, backups and recovery;
- Communication systems used to notify personnel by means of email or SMS;
- Security responses that restrict access to a particular user, CI or service;
• Triggers that initiate the generation of an incident record (in order to trigger the execution of the Incident Management process); or
• Triggers that initiate the archiving or removal of data, records and information.

It is possible for more than one trigger to occur, for example, to generate an incident record and to execute a script that will reboot a failed CI. This is particularly applicable to critical CIs, where communication to IT staff members will normally occur in association with any other action to be performed.

8. Response Selection

There are many options for response that will be triggered by Event Management. This will be determined by the level of control and visibility for the IT infrastructure as well as the use of technology for monitoring, correlation and response to events. Typical options for response are:

• The event is logged, with any subsequent actions also being recorded. This provides useful input into other Service Operation processes such as Incident and Problem Management.
• Auto response, where responses will be executed without human intervention and checks performed that the response was successful.
• Alert and human intervention, where a defined person/group will be notified so that the appropriate skills can be used to deal with the event. Without meaningful event alerts being transmitted, human response will require extra time to be spent gathering the required information.
• The generation of an incident or change record.
• Link to an existing problem record.
• Special responses where normal processes may not be applicable. An example of this is the failing of a backup power generator or air conditioning unit.

9. Review actions

Depending on the level of event that has occurred and the associated response actions that took place, there may be a need to verify that the event has been handled appropriately, or to provide opportunity for improvement in the handling of future events.

Where associated change or incident records are raised, there should not be duplication of effort, but instead they may form part of the reviews occurring within the Change and Incident Management processes. Regular audits should also be performed to verify compliance to the process and to detect any exceptions or detrimental behaviors.
10. Close event

Event closure works very differently to the typical closure mechanisms used for other processes such as Incident Management. As the majority of events are informational and only used as an input to other processes, no closure action is needed. For auto-response events, closure will usually be automated after verification that the response was successful. The alternative is that once the response is successful, a second event is generated that indicates effective closure. Where events triggered the generation of an incident, problem or change, closure will occur by creating a link to the associated record created.

9.4.5 Triggers and Interfaces

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; and
- 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.

The inputs to Event Management will vary depending on what interfaces have been implemented, with typical items being:

- Exceptions to CIs within the visibility of Event Management;
- Exceptions to automated processes;
- The completion of an automated routine;
- A status change in a device, database or document management system;
- Breach of utilization, performance or capacity thresholds; and
- Access to a service, application or database by a user or routine job.
Figure 9.10: Typical Interfaces for Event Management

Change Management
Inputs: RFCs, RSC, PSOs. Changes to monitoring/Event Management requirements.
Outputs: Event data history for RFC assessments. Process event reporting, RFCs relating to generated Events.

Access Management
Inputs: Group policies and access levels. Systems/CIs relevant for monitoring access events.
Outputs: Events signifying authorised & unauthorised access. Access logs and history. Trends in user access events.

Information Security Management

Incident Management
Inputs: Definition of exceptions and normal conditions. Incident information, past trends and relevant CIs requiring more detailed/frequent monitoring.
Outputs: Events signifying exceptions or unusual conditions for further investigation.

Service Asset & Configuration Management
Inputs: Configuration and Asset data required for Monitoring and Event Management. Status Accounting for Change/Incident/Problem affected CIs.
Outputs: CI status updates. CI reviews/audit information.

Capacity Management
Outputs: Events signifying breach of Capacity or performance thresholds. Process reporting for capacity and effort prediction. Level of monitoring required and number of Events detected and managed.

Financial Management
Outputs: Process reporting for refining cost and effort predictions. Events demonstrating exception to budgets, costing and charging models.

Release & Deployment Management
Inputs: Release Units, Definitive Media Library (DML) and Definitive Spares (DS) components. Support documentation and procedure relating to new Releases. List of CIs from release requiring monitoring with associated procedures.
Outputs: Events generated during distribution, during roll backs or Release reviews.

Event Management

Types of Events:
- Signifying Normal Operation
- Signifying Exception
- Signifying Unusual Conditions

Activities:
- Event Notification
- Event Detection
- Event Filtering, Event Correlation
- Trigger, Response Selection
- Review Actions, Close Event

Service Level Management
Inputs: SLRs, SLAs, OLAs, Service Descriptions, Specific monitoring responsibilities and KPIs. Process improvements and customer feedback. Develop classification scheme for prioritization of Events/CIs.
Outputs: Process event reporting. Exceptions and breaches of agreed targets for Event Management. Identified bottlenecks or process issues.

Service Catalog Management
Inputs: New, modified or removed Service Catalog components. Service Descriptions, Shared documentation for Services.

Problem Management
Inputs: CIs designated as vulnerable and requiring more rigorous and detailed monitoring for Event Management. Known Errors and associated Workarounds for responding to Events. Problem Resolution for those spawned from Events.
Outputs: Events escalated to be linked to a new or existing Problem record. Provides the mechanism to reassess or change priority for Problems.

Service Desk:
Responsibilities:
- Monitor and manage events for CIs owned by the Service Desk
- Escalate appropriate events
- Check relevant infrastructure performance against agreed targets and SLAs
- Manage user communication, updates and queries
- Report metrics regarding Event Management

2nd Line (Technical, IT Ops and Application Management)
Responsibilities:
- Develop capabilities for monitoring and event notification within IT infrastructure
- Manage events
- Escalate to Incident/Problem Management
- Report process metrics, effort taken and trends
- Identify process improvements
9.4.6 Key Performance Indicators (KPIs) for Event Management

With the focus on measuring and reporting the effectiveness and efficiency of Event Management, typical metrics that should be included are:

- The number of events (grouped by category);
- The number of events (grouped by significance);
- The number and percentage of events that required human intervention and whether this was performed;
- The number and percentage of events managed with automated responses and whether this was successful;
- The number of events that were escalated to incidents, problems and changes;
- The resource requirements for monitoring and responding to events;
- The number of repeat escalated events (for improvement of the Correlation Engine); and
- The number and ratio of events compared with the number of incidents.

Event Management should also be assessed for its contribution to overall Service Operation and the support of defined business objectives. The challenge in analyzing these metrics is to understand whether the benefits came from Event Management as opposed to other sources. These include:

- Reduced SLA breaches;
- Reduced times required for diagnosis and root-cause analysis of problems;
- Reducing ratio of high priority incidents;
- Reduced Mean Time to Restore (MTTR) for incidents;
- Improved availability levels; and
- Improved delivery of capacity and performance, with fewer capacity related incidents.
9.5 Incident Management

Incident Management has developed over time to become one of the most visible and mature ITIL processes for any organization, largely driven by the need to reduce the business impact of disruptions to IT services. While any effective implementation does balance the efforts towards the various phases of the Service Lifecycle, as Incident Management can be easily demonstrated to have a business benefit, it typically receives more attention and funding than other areas of service management. This section will explain the activities and techniques that represent best practices for Incident Management.

9.5.1 Goals and Objectives

The goal of Incident Management is 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.

9.5.2 Scope

Incident Management can be utilized to manage any event which disrupts, or has the potential to disrupt an IT service and associated business processes. Careful distinction needs to be made between the role of Event Management and Incident Management, as only events that indicate exception to normal service operation and are determined by the Event Correlation engine to be significant are escalated to Incident Management. This means that incident records may be generated as a result of:

- End-users calling the Service Desk to notify of a disruption to their normal use of IT services;
- Events representing an exception that are resolved using automated means, with an associated incident record also being generated for informational purposes;
- An IT staff member noticing that a component of the IT infrastructure is behaving abnormally, despite no current impact on the end-user community;
- An end-user logging an incident using self help means, which is then resolved by IT operations staff; or
- An external supplier observes that a portion of the IT infrastructure under their control is experiencing issues, and logs an incident ticket via email.
While the process of Request Fulfillment does typically operate in a similar fashion to Incident Management, a service request does not involve any (potential) disruption to an IT service.
Designing and planning

For Incident Management to achieve the defined objectives, planning needs to consider how the process will be designed to provide effective and efficient resolution of all incidents. As there will be a range of incidents with varying levels of business impact and urgency, the process will need to have mechanisms in place to classify incidents consistently and provide appropriate levels of response.

Timescales and priority levels

It is essential that timescales are agreed and communicated for all incident handling stages and will be based on the overall incident response and resolution targets with SLAs. These timescales will be dependent on the priority level of the incident e.g. major incidents. Service Management tools should be used to automate timescales and escalate the incident as required to the appropriate level or group.

Service Level Management should ensure that agreed timescales for incidents are consistently met by also developing agreements with internal IT groups (Operational Level Agreements) and external suppliers (Underpinning Contracts) as part of a seamless quality of IT delivery and support.

Incident Models

Incident Models provide a pre-defined set of steps and procedures that should be used to manage previously seen and documented incidents. They are used to help provide efficient resolution to the most frequently occurring (80 / 20 rule) or specialized incidents. Incident Models should define:

- The steps that should be taken to handle the incident;
- The chronological order these steps should be taken in, with any dependencies or co-processing defined;
- Responsibilities, who should do what;
- Timescales and thresholds for completion of actions;
- Escalation procedures, who should be contacted and when; and
- Any necessary evidence-preservation activities.

Any service management tools that are used for Event and Incident Management should be utilized with the defined incident models that can automate the handling, management and escalation of the process.

Specialized incidents include those which need routing to particular groups or ITIL processes. An example of this is for capacity related incidents, in which the model would define what impact reduction measures could be performed before routing the incident to Capacity Management.
**Major incidents**

For those incidents that result in significant or organization-wide business impact, planning needs to consider how separate procedures should be used with shorter timescales and greater urgency to provide appropriate response and resolution. The first requirement is to define what constitutes a major incident for the organization and customers, with reference to the incident prioritization mechanisms that are used.

The key role of separate major incident procedures is to establish a fast and coordinated response that can manage and resolve the issues at hand. This may require the establishment of a team with the immediate focus of resolving the incident and reducing the associated business impact. The Service Desk maintains responsibility throughout the process so that users are kept fully informed of the incident status and progress for resolution.

Problem Management will typically be involved when major incidents occur, though the focus is not the resolution of the incident. Instead, Problem Management seeks to identify the root cause of the incident, how this can be removed and if there are any other areas of the infrastructure where this could occur (e.g. replicated infrastructure across multiple locations).

**9.5.3 Benefits**

Incident Management is highly visible to the business, and it is therefore easier to demonstrate its value than most areas in Service Operation. For this reason Incident Management is often one of the first processes to be implemented in Service Management projects.

The added benefit of implementing Incident Management first is that it can be used to highlight other areas that need attention – thereby providing a justification for expenditure on implementing other processes. Other benefits include:

- Improved ability to detect and resolve incidents, which results in lower downtime to the business, which in turn means higher availability of the service.
- Ability to align IT activity to real-time business priorities. This is because Incident Management includes the capability to identify business priorities and dynamically allocate resources as necessary.
- Ability to identify potential improvements to services. This happens as a result of understanding what constitutes an incident and also from being in contact with the activities of business operational staff.
- The Service Desk can, during its handling of incidents, identify additional service or training requirements found in IT or the business.
9.5.4 Incident Management Activities

Figure 9.12: – Typical activities for Incident Management
© Crown Copyright 2007 Reproduced under license from OGC
Overview of steps:

1. Incident identification.
2. Incident logging.
3. Incident categorization.
4. Incident prioritization.
5. Initial diagnosis.
6. Incident escalation.
7. Investigation and diagnosis.
8. Resolution and recovery.
9. Incident closure.

1. Incident identification

The implementation of Incident Management should consider the range of sources where incidents can be identified. These typically include:

- Customers and end-users;
- External customers (of the business);
- IT staff members;
- Automated mechanisms, including those governed by Event Management; and
- External suppliers.

In the case of those detected by automated mechanisms, all key components should be monitored so that failures or potential failures are detected early so that the Incident Management process can be started quickly. In this way many incidents can be resolved before they have an impact on business operations and the end-user community.

2. Incident logging

All incidents, regardless of source, must be recorded with a unique reference number and be date/time stamped. While this can be easily managed for automated mechanisms, positive behaviors need to be developed for IT staff and end-users to ensure the consistent recording of identified incidents. It may also be necessary to record more than one incident for any given call/discussion so that a historical record is kept and that time/work tracking can be performed.

Incident records will be updated over the lifecycle of the incident in order to assist other support groups when it is escalated or returned. An example template showing information that is typically utilized for incident records is described below.

The following definitions apply for the below tables:

- **Read Only**: No data may be entered into the field.
• **System Generated**: The application will automatically generate the correct value(s).

• **Check Box**: A box, that when clicked will then show a mark indicating that the box has been activated.

• **Linked Record**: Means that the field provides a button for the user to click on, which will take them to a list of records in the database, at which point they may choose a value to populate the field with.

• **User Defined**: Field allows the user to enter any value that they wish.

• **User Defined Array**: Field is considered a large text box which will allow the user to type multiple lines of text.

• **Drop Box**: Field allows the user to click on a drop-down list of information, where they are allowed to make one selection to populate the field.

• **Drop Box – Nested**: The values in this field are dependent on the values listed in the above Drop Box.

• **Break in Format**: Indicates where there will be a visual break in sets of information captured on the Incident Ticket.

### 3. Incident categorization

During the initial logging of the incident a category is assigned so that the exact type of incident is recorded. This information is important to allow effective escalation, trend analysis of incidents and future infrastructure improvements. Multi-level categorization is typically used for Incident Management, where the service management tool is populated with up to three of four levels of category details.
4. Incident prioritization

An agreed prioritization matrix should be used to determine the appropriate timescales and effort applied for response and resolution to identified incidents. The general formula by which to calculate incident priority is:

**IMPACT + URGENCY = PRIORITY**

- **Impact**: Degree to which the user/business is affected by the incident(s).
- **Urgency**: Degree to which the resolution of the incident can be delayed.

For following factors are usually taken into account for determining the impact of an incident:

- The number of users being affected;
  - (e.g. single user, multiple users, entire business unit, organization wide)
- Possible risk of injury or death;
- The number of services affected;
- The level of financial loss;
- Effect on credibility and reputation of business; and
- Regulatory or legislative breaches.

Urgency is calculated by assessing when the potential impact of the incident will be felt. In some cases, the incident resolution can be delayed when the disruption to an IT service (e.g. payroll) has not yet affected business operations (but will if the service is not available in three days time).

![Figure 9.14: Example incident prioritization matrix](image)

The prioritization matrix above would be accompanied by agreed timelines for resolution.
E.g.  
- Priority 1 = Critical = 1 hour target resolution time
- Priority 2 = High = 8 hours
Priority 3 = Medium = 24 hours  
Priority 4 = Low = 48 hours +

Service Level Management will develop these agreed timelines with the business and customers, with frequent reviews performed for any modifications that may be required. In all cases clear guidance as to how to correctly determine priority should be provided, with examples demonstrating the use of the priority coding system.

Despite extensive planning, there will always be rare occasions where normal priority levels will need to be overridden. When this occurs, normal escalation via line management (e.g. a service desk employee transfers this to the service desk manager) to verify the required need for deviation from normal processes. While the treatment of VIP users (executives, politicians etc) may occur like this, it is more effective to have these situations built into the prioritization matrix. In cases where an integrated suite of service management tools are used, references to associated SLAs make it more efficient to determine the appropriate incident priority.

4. Initial diagnosis

For calls forwarded to the Service Desk, the staff member will use pre-defined questioning techniques to assist in the collection of useful information for the incident record. At this point the Service Desk analyst can begin to provide some initial support by referencing known errors and simple diagnostic tools. Where possible the incident will be resolved using these sources of information, closing the incident after verifying the resolution was successful.

For incidents that can’t be resolved at this stage and the user is still on the phone, the Service Desk analyst should inform the user of the next steps that will be taken, give the unique incident reference number and confirm user contact details for follow-ups.

5. Incident escalation

If the Service Desk analyst requires assistance from other groups due to an inability to resolve the incident or because of specialized circumstances (e.g. VIP user), escalation will be utilized to transfer the incident to the appropriate party or group. Rules for escalation should be defined when implementing Incident Management and agreed upon by all involved groups and stakeholders.

The two forms of escalation that are typically used are functional (horizontal) and hierarchical (vertical) escalation. Escalations can also be combined.

- Functional escalation:
  - When initial diagnosis has exhausted known sources of information (e.g. known errors, knowledge bases, supplier documentation) or when target
times for first-point resolution have been exceeded, the incident should be escalated for further support.

- In most IT organizations, the Service Desk (first-line support) is supported by specialized tiers of support (second-line, third-line) which may be internal or external to that organization. Timeframes should also be defined that govern how long each tier or support can manage an incident before it is escalated to the next group. For calls escalated to external suppliers, Underpinning Contracts should be used to define the requirements for response and resolution of those escalated incidents.

- Hierarchical escalation:
  - Typically utilized for serious (major) incidents or for specialized circumstances (VIP users or for escalating incidents that may breach SLA targets), escalation transfers the incident to the appropriate IT managers, or at least notifies them of the incident details and situation.
  - Hierarchical escalation continues up the management chain as necessary, for example: Service Desk analysts → Service Desk manager → Service Operations manager → Service Manager → Chief Information Officer.

While escalation may transfer responsibility for further investigation and resolution by other parties, the Service Desk should retain ownership of the incident, being responsible for tracking progress, keeping users informed and confirming incident closure. Updates to the incident record should also note what escalation has occurred and the actions performed by each group.

**Figure 9.15: Escalation Graph**

### 6. Investigation and diagnosis

Each of the support groups involved with the incident handling will investigate and diagnose what has gone wrong – and the activities carried out should be fully documented,
as part of the incident record to maintain a complete and historical record. Care should be taken that activities are coordinated when multiple groups are involved so that any solutions put in place don’t conflict.

The investigation is likely to include such actions as:

- Establishing exactly what has gone wrong or what is being sought by the user;
- Understanding the chronological order of events;
- Confirming the full impact of the incident, including the number and range of users affected;
- Identifying any events that could have triggered the incident;
- Knowledge searches looking for previous occurrences by searching previous Incident/Problem Records and/or Known/Error databases etc; and
- Seeking knowledge from system developers as to possible guidance for resolution.

7. Resolution and recovery

When a potential resolution has been identified it should be applied and tested in a controlled manner. The specific requirements for performing this will vary depending on the elements required for resolution, but could involve:

- Guiding the user to perform specific actions on their own equipment;
- Specialist support groups performing specific actions on the infrastructure (such as rebooting a server);
- External suppliers performing updates on their infrastructure in order to resolve the incident; and
- The Service Desk or other specialist staff controlling a user’s desktop remotely in order to resolve the incident.

When the potential resolution has been applied, testing should be used to verify the success and that the service has been fully restored to the affected user(s). At all times the incident record should be updated, with any lessons learned for future improvement documented and translated into live knowledge bases or known error databases where necessary. Once the actions for resolution are complete the incident should be transferred back to the Service Desk for closure.
8. Incident Closure

Depending on the nature of the incident (level of impact, users affected etc), the Service Desk may be required to call the affected users and confirm that the users are satisfied that the resolution was successful and that the incident can be closed. For other incidents, closure mechanisms may be automated and communicated via email. Closure mechanisms, whether automated or manual, should also check for the following:

- Closure categorization, with comparison to the initial categorization to ensure accurate historical tracking;
- User satisfaction survey, usually be email or web-forms for an agreed percentage of random incidents;
- Incident documentation, ensuring all required fields are completed satisfactorily;
- Potential problem identification, assisting Problem Management in the decision whether any preventative action is necessary to avoid this in the future.

When the requirements for incident documentation are complete, the incident should be closed via agreed methods.

In some cases there will be a need to re-open incidents, which should have pre-defined rules governing these situations. Such rules may be based on the timeframe since initial closure or for those incidents closed via automated mechanisms. If an incident recurs outside of these defined rules, then a new incident should be opened, with links to the previous incident(s).

1.1.3 Triggers and Interfaces

The identification and recording of an incident can occur in many ways (see 1. Incident identification), so any planning and continual improvement of Incident Management should evaluate how incidents can be effectively identified using automated and manual methods. Other interfaces within service management that should be maintained are:

- **Service Level Management**: Agreed targets and timeframes for response, escalation and resolution should be developed and are vital for Incident Management being effective in meeting its goals. Agreements will include:
  - Appropriate incident response and resolution times;
  - Impact definitions;
  - Service definitions;
  - Rules for identifying incidents; and
  - Expectations for providing feedback to users.
• **Availability Management:** Analyzing metrics from the expanded incident lifecycle will identify areas that can be improved in order to optimize the levels of availability provided to the business and users.

• **Security Management:** Policies and methods should be defined to describe what actions should be taken when incidents indicate a breach or potential weakness in security levels.

• **Configuration Management:** The implementation of Incident Management should utilize Configuration Management for recording or retrieving information and status updates about services and associated infrastructure components recorded as Configuration Items (CIs). Typically the service management tools used for Incident Management will have in-built access for viewing and modifying the Configuration Management System (CMS) in a controlled manner.

• **Problem Management:** While Incident Management is used to reduce the business impacts of incidents occurring, Problem Management provides the capabilities for identifying and eliminating the root-cause of incidents. Coordination between the processes should ensure that Incident Management is utilized to identify potential problems, and that Problem Management is used to reduce recurring incidents and to share knowledge and information for the purpose of improving the first-line resolution of incidents.

### 9.5.5 Key Performance Indicators (KPIs) of Incident Management

Incident Management will be continually measured to determine the effectiveness and efficiency achieved in meeting the objectives defined. These metrics should cater for multiple perspectives, including the business, end-users, IT staff, use of financial and human resources, and the overall contribution to the role of IT Service Management.

**Metrics:**

**Objective - Minimizing the business impact of incidents**
- Percentage of incidents resolved at first contact.
- Average call time with no escalation.
- Percentage of incidents resolved within agreed timeframes (grouped by priority).
- Average time to resolve incidents.

**Objective – Contribute to the identification of Problems**
- Number and percentage of incidents grouped by category.
- Percentage of incidents incorrectly categorized.
- Number of incidents linked to existing problem records.
Objective – Develop effective Service Management
- Customer satisfaction.
- Average time second line groups to respond.
- Percentage of calls that bypass first line (Service Desk).
- Cost per incident.
- Resources used for managing incidents (grouped by priority).

Reports should be produced under the authority of the Incident Manager, who should draw up a schedule and distribution list. Distribution lists should at least include IT Service Management, specialist support groups and customers.

9.5.6 Challenges of Incident Management

While Incident Management is typically found to be the most mature of an organization’s IT Service Management processes, many challenges will exist that should be overcome through implementation and continual improvement. These include:
- The ability to detect incidents as early as possible through Event Management;
- Convincing all staff that all incidents must be logged and recorded;
- Developing standards and guidelines for the level of detail and language to be used in incident records and associated documentation;
- Developing coordination between multiple groups for major incidents;
- Availability of information about problems and Known Errors;
- Integration into the CMS to determine relationships, current status and historical data;
- Ability to associate incidents with defined SLA targets and timeframes; and
- Lack of commitment from staff and management.
9.6 Problem Management

9.6.1 Goals and Objectives

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; and
- To minimize the impact of incidents that cannot be prevented.

9.6.2 Scope

Clear distinction should be made between the purpose, scope and activities of Problem Management and those of Incident Management. In many cases staff may not clearly understand the distinction, and as a result not utilize their efforts in the most effective and efficient manner.

What is the difference between Incident Management and Problem Management?

Analogy: If our gardens and lawns were 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 is a simple explanation showing the difference between Incident Management and Problem Management. Incident Management is not concerned with the root cause, and only addresses the symptoms as quickly as possible. Problem Management however takes a long-term focus and approach in order to prevent the symptoms (weeds) from occurring again.
For most implementations of Problem Management the scope includes:
- The activities required to diagnose the root cause of incidents and to determine the resolution to those problems;
- Activities that ensure that the resolution is implemented through the appropriate control procedures, usually through interfaces with Change Management and Release & Deployment Management; and
- Proactive activities that eliminate errors in the infrastructure before they result in incidents and impact on the business and end-users.

### 9.6.3 Benefits

Problem management should be used in coordination with Incident and Change Management processes to ensure service availability and quality are improved. When incidents are resolved, information about the resolution is recorded. Over time this organizational learning is used to speed up the resolution time and identify permanent solutions.

Other benefits of Problem Management include:
- Higher availability of IT services;
- Higher productivity of business and IT staff;
- Reduced expenditure on workarounds or fixes that do not work; and
- Reduction in duplicated costs and effort in fire-fighting or resolving repeat incidents.

![Diagram of Problem Management](image-url)

**Figure 9.16: The basic concepts of Problem Management**
9.6.4 Problem Management Activities

The activities of Problem Management are divided into two major sub-processes:

- Reactive Problem Management: typically driven by the identification of repeat or major incidents, and executed within the role of Service Operation.

- Proactive Problem Management: which is initiated in Service Operation, but generally managed and driven by Continual Service Improvement.

Figure 9.17: Typical activities of Problem Management

© Crown Copyright 2007 Reproduced under license from OGC
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.

1. Problem detection

The detection of problems can occur in multiple ways, so planning for the implementation of Problem Management should consider what interfaces need to be developed to cater for these various sources. Typically these include:

- Problems detected as a result of multiple incidents that have been raised by automated means (under the control of Event Management);
- Problems detected at the Service Desk based on a large volume of like high impact incidents, requiring a problem to be logged straight away;
- Problems detected by the Service Desk or other technical support groups based on incident investigation;
- Problems detected as a result of external suppliers notifying of errors in the infrastructure/applications under their control; and
- Trend analysis of incidents, found as part of the execution of Proactive Problem Management.

2. Problem logging

Like incidents, all detected problems (regardless of source) must be recorded with a unique reference number and be date/time stamped to enable full historical tracking, control and escalation. Where possible, the same service management tools should be used to record incident and problem records, so that any relevant details can be copied/referenced from incidents to associated problems.

Normally this will include such details as:

- User details;
- Service details;
- Equipment details;
- Date/time of recording;
- Categorization and priority details;
- Incident descriptions/symptoms; and
- Details of actions taken.

See (6.2.4 -Incident logging) for more details.

### 3. Problem categorization

To ensure consistency and to allow for effective matching, detection and reporting, both incidents and problems should be categorized in the same way. Multi-level categorization is typically used, where the service management tool is populated with up to three of four levels of category details. Over time, continual improvement should seek ways to improve the categorization techniques used.

![Figure 9.18: Multi-level problem categorization](image)

© Crown Copyright 2007 Reproduced under license from OGC

### 4. Problem prioritization

While incidents and problems will have similar elements to their priority coding systems, problem prioritization will also take into account the frequency and impact of the related incidents. This is important in order to give involved staff some understanding of the relative severity of problems, and what level of response and investigation is required.

Due to the long-term focus of Problem Management, prioritization will also consider the severity of the problem from an infrastructure perspective, including:

- Can the system be recovered, or does it need to be replaced?
- How much will it cost?
- How many people, with what skills, will be needed to fix the problem?
How long will it take to fix the problem?
How extensive is the problem (e.g. how many CIs are affected)?

Depending on the nature and severity of the problem, it may require a single person, small group or dedicated problem investigation team, so priority needs to be assigned correctly to initiate the appropriate response.

5. Problem investigation and diagnosis

Problem Management should coordinate an investigation to try to diagnose the root cause of the problem. The speed and nature of this investigation will vary depending upon the impact, severity and urgency of the problem. Like Incident Management, the Configuration Management System should be used to help assess the level of impact and to assist in diagnosing the exact point of failure.

Where necessary, recreating the failure in a test environment can assist in determining reason(s) for disruption and then to try various solutions to the problem in a safe and controlled manner. To do this effectively without causing further disruption to the users, a test environment that mirrors the production environment is required.

Brainstorming often occurs at this stage, involving all appropriate IT staff, customers and suppliers to collectively gain intelligence and ideas. Many research studies have been performed into other effective techniques that assist in the analysis, diagnosis and resolution of problems. Some of the most widely used techniques include:

**Kepner and Tregoe:**

Charles Kepner and Benjamin Tregoe developed a method for analyzing problems. Their theory states that problem analysis should be a systematic process of problem solving and should take maximum advantage of knowledge and experience. They distinguish the following five phases for problem analysis:

1. Defining the problem;
2. Describing the problem with regard to identity, location, time and size;
3. Establishing possible causes;
4. Testing the most probable cause; and
5. Verifying the true cause.

Depending on time and available information, these phases can be applied with various levels of effort and resources.
Pareto Analysis:

Pareto analysis is a very simple technique that helps you to choose the most effective changes to make. It uses the Pareto principle – the idea that by doing 20 per cent of work you can generate 80 per cent of the advantage of doing the entire job. Pareto analysis is a formal technique for finding the changes that will give the biggest benefits. It is useful where many possible courses of action are competing for your attention, in this case where multiple solutions exist for an identified problem, or when choosing which problem to address first.

To use the Pareto analysis technique:

1. List the problems you face, or the options you have available;
2. Group options where they are facets of the same larger problem;
3. Apply an appropriate score to each group; and
4. Work on the group with the highest score.

Ishikawa Diagrams:

Ishikawa diagrams were proposed by Kaoru Ishikawa in the 1960s, initially used to improve quality management processes in the Kawasaki shipyards, and in the process became one of the founding fathers of modern management. It is known as a fishbone diagram because of its shape, similar to the side view of a fish skeleton.

Figure 9.19: Example of an Ishikawa diagram used for Problem Management

An Ishikawa diagram is typically the result of a brainstorming session in which members of a group offer ideas on how to improve a product, process or service. The main goal is represented by the trunk of the diagram, and primary factors are represented as branches.
Secondary factors are then added as stems, and so on. Creating the diagram stimulates discussion and often leads to increased understanding of a complex problem.
Pain Value Analysis:

This technique adopts a broader view of the impact caused by an incident/problem, where a more in-depth analysis determines exactly what level of pain has been caused to the organization/business involved. A formula that can calculate this pain level is required, which often includes such factors as:

- The number of people affected;
- The duration of the downtime caused; and
- The cost to the business (if this can be effectively modeled).

Chronological Analysis:

This technique analyses all of the events and actions that have occurred in order to see the relationship between them, or to discount any which should not be associated in the series. This requires consistent recording and documentation so that an accurate timeline of events can be understood.

5. Workarounds

While investigation into the root cause of problems and the development of appropriate solutions is still being undertaken, effort should be made as to how workarounds might be used to reduce the user/business impact until the permanent resolution is available. Workarounds are a set of predefined steps to take as a means of reducing or eliminating the impact of an Incident or a Problem (e.g. restarting a failed Configuration Item). Workarounds for problems are documented with the Known Error records in the Known Error Database (KEDB).

Although workarounds can be developed by any involved party (Service Desk analysts, technical specialists or external suppliers), they should be analyzed by Problem Management before being formally recorded in the KEDB. Where workarounds do provide temporary relief from the associated symptoms and impact, it is important to continue to track any related incidents so that future effort and resources in developing a permanent solution can be justified.

6. Raising a Known Error record

So that effective matching can occur, a Known Error record should be created within the KEDB as soon as the diagnosis is complete (and/or a valid workaround has been identified). This improves the visibility of the information required to match associated incidents and to find appropriate workarounds as a temporary means to overcoming disruption.
Where there is some benefit to creating a Known Error record earlier in the Problem Management process (i.e. before diagnosis is complete), it can be created as soon as it becomes useful to do so. In these cases, any further actions performed during its investigation and diagnosis would subsequently be captured.

7. Problem resolution

When a successful resolution has been identified and tested, approval should be sought for its implementation to the production (live) environment. Depending on the nature and scope of service management already in place and resolution to be implemented, this typically involves raising a Request for Change (RFC) for approval, either by a Change Advisory Board (CAB), or Emergency CAB for serious and urgent issues. Once the appropriate change evaluation and authorization has occurred, the change should be scheduled according to normal Change and Release policy requirements. There may be some problems for which a Business Case for resolution cannot be justified (e.g. where the impact is limited but the cost of resolution would be extremely high). In such cases, a decision may be taken to leave the Problem Record open but to use a workaround description in the Known Error Record to detect and resolve any recurrences quickly.

8. Problem closure

When any changes and post implementation reviews have been successfully completed, and the resolution has proved to be effective, the problem record should be formally closed, with an update made to any associated incident records that are still open. This closure activity should also check that all required fields and documentation items are complete, and that the status has been updated to reflect the successful resolution of the error.

9. Major Problem reviews

The priority coding system used for Problem Management should provide special distinction for Major Problems. Like Major Incidents, these are problems with the highest level of impact (see problem prioritization) that result in major business/organizational disruption. After successfully implementing solutions to a Major Problem, a review should be conducted in order to assess:

- What was done correctly?
- What was done wrong?
- What could be done better in the future?
- Could this problem/error be replicated in any other portion of the infrastructure?
- Was there any third-party responsibility?
- Are there any follow-up actions needed?
Such reviews are an important pass of continual improvement, with any lessons learned being documented in appropriate procedures, work instructions, diagnostic scripts or Known Error records. The Problem Manager facilitates the session and documents any agreed actions.

The knowledge learned from the review should be incorporated into a service review meeting with the business customer to ensure the customer is aware of the actions taken and the plans to prevent future major incidents from occurring. This helps to improve customer satisfaction and assure the business that Service Operations is handling major incidents responsibly and actively working to prevent their future recurrence.

9.6.5 Proactive Problem Management

The three main activities that normally make up the sub-process of Proactive Problem Management are:

Major Problem Reviews (see 6.3.4 - 9. Major Problem reviews)

Trend Analysis
- Review reports from other processes (e.g. trends in incidents, availability levels, relationships with changes and releases); and
- 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; and
- 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).

1.1.4 Managing Known Errors from the Service Transition Phase

It is likely that during the testing of new applications, systems or releases a prioritization system will be used to eradicate the more serious faults. However, it is possible that minor faults are not rectified – often because of the balance that has to be made between delivering new functionality to the business as quickly as possible and ensuring totally fault-free code or components.

Where a decision is made to release something into the production environment that includes known deficiencies, these should be logged as Known Errors in the KEDB,
together with details of workarounds or resolution activities. There should be a formal step in the testing sign-off that ensures that this handover always takes place.

History indicates that if this does not happen, it will lead to far higher support costs when the users start to experience the faults and raise incidents that have to be re-diagnosed and resolved from the beginning again.

### 1.1.5 Triggers and Interfaces

When viewed in the context of Service Operations, the majority of problem records will be raised as a result of one or more incidents identified to be of a single root cause. This identification can occur in many ways, through formal and informal, manual and automated measures. Throughout the lifecycle of these problem records, information will be passed to and from Problem Management to assist in the effective and timely investigation, diagnosis and resolution of errors. In this context, the primary interfaces with Incident Management have already been discussed within chapters 6.2 and 6.3.

Other key interfaces that exist include:

- **Service Strategy:**
  - *Financial Management* – for providing modeling of the business impact and financial cost of identified problems, including the development of a business case for their resolution.

- **Service Design:**
  - *IT Service Continuity Management* – for providing guidance and measures as to the possible invocation of recovery mechanisms.
  - *Service Level Management* – for providing feedback as to the customer impact of problems/Known Errors, and their general satisfaction with Problem Management.
  - *Capacity Management* – for assisting with investigations into capacity and performance-related problems.
  - *Availability Management* – for determining strategies to improve availability and reduce downtime. Proactive Problem Management is a typical supported role, analyzing vulnerable areas of the infrastructure (e.g. single points of failure) to prevent future problems.

- **Service Transition**
  - *Change Management* – RFCs should be raised when requiring a change to controlled CIs in order to implement a permanent solution. Change Management should also review whether the change has delivered a successful solution to the problem/Known Error.
- **Release & Deployment** – any Known Errors detected during the development and testing of new and modified services, systems and applications should be documented and communicated to Problem Management.
- **Configuration Management** – the Configuration Management System (CMS) should be used to assist in the evaluation of impact for problems/Known Errors, and to provide historical tracking for the relationships between CIs, incidents, problems and Known Errors.

- **Continual Service Improvement**
  - **CSI (7 Step) Improvement Process** – used to identify, coordinate and drive improvements, which may involve the documentation and resolution of problems/Known Errors.

![Figure 9.20: The Service Knowledge Management System](image)

© Crown Copyright 2007 Reproduced under license from OGC

The Known Error Database (KEDB) should be interfaced with various elements of an organization’s Service Knowledge Management System (SKMS) so that relationships can be created and understood between incidents, problems, known errors, CIs, changes and releases.
9.6.6 Key Performance Indicators (KPIs) for Problem Management

Measures that can be used to demonstrate the effectiveness and efficiency of the Problem Management process include:

- The number of problems grouped by status (open, closed, known errors etc);
- The number of RFCs created by Problem Management;
- The number of workarounds developed for Known Errors and incidents;
- The percentage of incidents resolved at first contact (should be increasing);
- The average time to resolve incidents (should be decreasing);
- The average time to close problems;
- Customer satisfaction levels;
- Average costs for solving problems;
- Number and percentage of problems that were resolved within SLA limits;
- Percentage of incidents not linked to problems and known errors; and
- The number of major problem reviews conducted.
9.7 Request Fulfillment

The primary purpose of this process is to provide effective and efficient capabilities for fulfilling requests, questions and queries that are placed upon the IT department by users. Without a separate process it is likely that Change Management would be flooded by a large volume of low risk standard changes, creating bottlenecks and affecting the quality of assessment and coordination for normal changes.

9.7.1 Goal and objectives

Request Fulfillment 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; and
- To assist with general information, complaints or comments.

9.7.2 Scope

The scope of Request Fulfillment 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 Fulfillment 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); and
- Users wishing to have common services and applications installed for their use.

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

Standard Change: A pre-approved change that is low risk, relatively common and follows a procedure or work instruction. There may still be authorization from other groups such as Human Resources; however Change Management will not need to approve each execution of the standard change.
9.7.3 Benefits

Through effective and efficient access to standard services from the IT department, the business and customers can be supported in improved productivity of staff and/or higher quality in business services and products offered. This is achieved by reducing the bureaucracy involved in making requests and centralizing the end-to-end management of those requests. Increased customer and user satisfaction can also be developed as a result of quality Request Fulfillment.

9.7.4 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; and
- 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.

9.7.5 Request Fulfillment Activities

![Figure 9.21: Typical Activities for Request Fulfillment](image)
1. **Menu selection**

Where practical, some mechanism of self-help should be utilized so that users can generate Service Requests using technology that interfaces with existing Service Management tools. This might be via a website that offers users a menu driven interface, where they can select common services and provide input details. In some instances the Fulfillment of the Service Request can be entirely automated using workflow, ERP, software deployment and other tools. For others, manual activities will be required to fulfill the request using resources from the IT department, suppliers or other parties involved in the provision of IT services.

2. **Financial Approval**

While the Service Request may already have approval from Change Management, there may be some form of financial approval that is required when there are financial implications (usually those above a defined dollar amount). It may be possible to agree upon fixed prices for ‘standard’ requests, otherwise the cost must be estimated and submitted to the user/customer for financial approval (who may in turn require their own line management/financial approval).

Where financial approval is involved, an agreed process for charging should follow in the later steps in accordance with the organization’s financial management policies.

3. **‘Other’ Approval**

Where there may be compliance and regulatory implications for the service request, wider business approval may be needed. These approval mechanisms should be built into the request models as appropriate. Change Management should establish that there are mechanisms in place to check for, and safeguard these conditions in order for the standard change to be qualified for preapproval.

4. **Fulfillment**

The tasks required for Fulfillment will vary depending on the characteristics of the service request at hand. Some requests can be fulfilled using only automated mechanisms. Others may be fulfilled by the Service Desk at the first-line, or escalated where necessary to internal or external specialist groups.

To ensure compatibility, Request Fulfillment should be interfaced with existing procurement and supplier processes; however the Service Desk should maintain control and visibility for all requests regardless of where it is fulfilled.
5. Closure

When the Service Request has been fulfilled, it should be referred back to the Service Desk to initiate closure. This should include some verification that the request has been satisfied using either confirmation with the end-user or other automated means.

9.7.6 Triggers and Interfaces

Most service requests will be triggered through users calling or emailing the Service Desk, or by using a self-help option to make their request. The primary interfaces within Service Management are those with the Service Desk and Incident Management:

- Some requests will be triggered during the use of Incident Management (e.g. a request is made to have a faulty printer serviced); and
- The Service Desk acts as the primary party responsible for managing Service Requests, and maintains visibility for those requests escalated to specialist groups.

Interfaces with Release and Deployment, and Service Asset and Configuration Management are also important as:

- Requests for deployment of software may involve pre-defined releases that can be automatically deployed, utilizing the Definitive Media Library (DML) where necessary;
- Checks will need to be made for any license requirements for deployed software; and
- The Configuration Management System (CMS) will need to be updated after any deployment or change in the configuration of IT infrastructure.

Change Management should be continually transferring standard changes to Request Fulfillment as maturity is gained in dealing with those changes.
Outputs: Escalated Service Requests, Process metric reporting, Request Models, exceptions.

Access Management
Inputs: Modified access rights, exceptions or denied requests. Group policies and access levels.
Outputs: Standard Changes & Service Requests regarding provision or modification of Access. Request Models and agreed targets.

Information Security Management
Inputs: Information Security Policy, Controls and documentation of security procedures.

Incident Management
Outputs: Exceptions and Incidents relating to Request Fulfilment. Request Models.

Service Asset & Configuration Management
Inputs: Configuration and Asset data required for Request Fulfilment. Baseline CIs for duplication.
Outputs: New, modified and removed CIs. Review/audit data collected. Controlled documentation/procedures captured as CIs.

Change Management
Outputs: Escalated Service Requests, Process metric reporting, Request Models, exceptions.

Capacity Management
Outputs: Service Requests & Standard Changes requiring provisioning of Capacity or advice. Process reporting to assist with effort and capacity prediction.

Financial Management

Release & Deployment Management
Inputs: Release Units, Definitive Media Library (DML) and Definitive Spares (DS) components. Build and assembly instructions for Service Requests and Standard Changes.
Outputs: Escalated Service Requests.

Request Fulfilment
Activities:
- Menu Selection
- Financial Approval
- Other Approval
- Fulfilment
- Closure
- Other
  - Create Request Models
  - Document Process Scope, Activities, Roles and Responsibilities

Service Level Management
Inputs: SLRs, SLAs, OLAs, Service Descriptions. Process Improvements and customer feedback. Develop classification scheme for prioritization of Service Requests.
Outputs: Process metric reporting. Exceptions and breaches of agreed targets for Service Requests. Identified bottlenecks or process issues.

Service Catalog Management
Outputs: Common Service Requests relevant for the Service Catalog. Self-service procedures utilised for Requests and Standard Changes. FAQs and support documentation.

Supplier Management
Outputs: Escalation of Service Requests and Standard Changes. Request Models and agreed targets.

Service Desk:
Responsibilities:
- Provide single point of contact for all Service Requests and Standard Changes.
- Resolve at first line appropriate documented Service Requests and Standard Changes.
- Escalate to 2nd line those that cannot be resolved.
- Manage user communication, updates and closure.
- Report metrics regarding Request Fulfilment.

2nd Line (Technical, IT Ops and Application Management)
Responsibilities:
- Document procedures for Service Requests and Standard Changes relevant to technology/application group.
- Manage escalated Service Requests.
- Develop Self Help capabilities for Request Fulfilment.
- Report process metrics, effort taken and breaches.
- Identify process improvements.
9.7.7 Key Performance Indicators (KPIs) for Request Fulfillment

Metrics will be broken down by the request type for each appropriate reporting period. These include:

- The total number of service requests;
- Percentage of service requests successfully fulfilled;
- The size of current backlogs for service requests;
- Mean elapsed time for handling service requests;
- The average cost per service request;
- Levels of client satisfaction; and
- Utilization of self-help mechanisms.
9.8 Access Management

Access Management is the operational execution of the policies, rules, processes and architectures implemented by Information Security and Availability Management within the Service Design phase. Although in many cases it is a process that is typically coordinated by the Service Desk, it can involve many different internal and external groups responsible for Service Operations.

9.8.1 Goal and objectives

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.

9.8.2 Scope

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.

9.8.3 Benefits

Access Management provides the following value:

- Controlled access to services ensures that the organization is able to maintain more effectively the confidentiality of its information;
- Employees have the right level of access to execute their jobs effectively;
- Less likelihood of errors in data entry or in the use of critical service by an unskilled user;
- Ability to audit use of services and to trace the abuse of services;
- Ability to easily modify and revoke access rights when needed – an important security consideration; and
- Provides ability to meet various regulatory/compliance requirements.
9.8.4 Basic concepts of Access Management

Access Management should be utilized for providing/modifying and removing access rights to agreed services documented within the Service Catalogue. The following definitions describe the major concepts involved with the process:

- **Access**: refers to the level and extent of a service’s functionality or data that a user is entitled to use.

- **Identity**: refers to the information about them that distinguishes them as an individual and which verifies their status within the organization. By definition, the identity of the user is unique to that user.

- **Rights**: (also called privileges) refer to the actual settings whereby a user is provided access to a service or group of services. Typical rights, or levels of access, include read, write, execute, change, delete.

- **Services or service groups**: instead of providing access to each service for each user separately, it is more efficient to be able to grant each user access to a whole set of services that they are entitled to use at the same time.

- **Directory of services**: refers to a specific type of tool that is used to manage access and rights.

9.8.5 Activities of Access Management

![Figure 9.23: Activities of Access Management](image-url)
1. Requesting access

Requests for access can be generated from many sources within an organization, as well as from any external suppliers and customers that require controlled access to services, systems and information. Typical interfaces that generate requests include:

- Requests generated by normal Human Resources (HR) processes. This occurs when staff are hired, promoted, moved, transferred or when they leave the organization;
- A Request for Change (which requires modifications to access rights);
- A service request submitted to the Service Desk, or those submitted via automated and self-help mechanisms; and
- Management requests for special circumstances (e.g. technical specialist needs access to a specific service or system).

2. Verification

When a request for access is received, defined procedures should control how the request is verified to check:

1. That the user requesting access is who they say they are
   For verifying this, an identification check is typically performed, requiring the user to confirm such details as usernames, enquiry passwords, date-of-birth, full name. For systems with high security level requirements, mechanisms such as RSA keys, security certificates, swipe cards or biometric scans (e.g. finger print) may be used.

2. They have a legitimate business reason for accessing the service, system or information
   Depending on the access being requested, this may involve parties other than the user to verify. This can include:
   - notification from HR;
   - authorization from an appropriate line manager;
   - approved RFC; or
   - policies stating that the user may have access to an optional service if they need it.

To improve efficiency, interfaces with systems and tools used by any Human Resource department or business process should be developed to allow independent and automated verification of access requests.
3. Providing rights

If the access request has been appropriately verified, Access Management then uses defined procedures and mechanisms to provide, modify or remove the access rights stipulated. Where possible, these mechanisms should be automated, particularly in large organizations with dynamic and specialized HR requirements.

As discussed in Basic Concepts of Access Management, the use of roles and groups are an effective way of providing users with multiple access levels appropriate to a type of need (e.g. teachers, students, administrators, contractors etc). These groups should be defined in such a way that they are neither too narrow nor too broad in their scope.

A potential issue that occurs when providing group and user access rights is that of Role Conflict. This is caused by conflicting rights that have been provided to a user or group of users. When users are allocated to multiple groups (each with different levels of rights), care needs to be taken that these permissions are applied in the correct order. For example, if a user is a member of both the USER and ADMINISTRATOR groups, the procedures and mechanisms utilized should ensure that the rights associated with the USER group don’t override those of the ADMINISTRATOR group. Most directory services safeguard against Role Conflict, however there is still potential for these conflicts to be otherwise missed by the tool.

Over time, reviews should be performed to ensure that roles and groups are still appropriate for the end-user and staff population, with any obsolete or unwanted groups/roles being removed.

4. Monitoring identity status

To ensure that the confidentiality and integrity of systems and information is continually protected, constant monitoring needs to be deployed to ensure consistency between user roles/status and the access levels being provided. In any organization there will be frequent changes in staffing that need to be identified, including:

- Transfers;
- Acting and temporary roles;
- Job changes;
- Promotions or demotions;
- Retirement;
- Resignation;
- Death;
- Disciplinary action; or
- Dismissals.
When implementing Access Management, interfaces with existing HR processes should be developed so that audits for consistency of access levels can be automated.
5. **Logging and tracking access**

So that Access Management can ensure that provided access levels are used responsibly, access monitoring and control should be deployed and included in normal monitoring activities performed by Service Operation teams. Interfaces with Event Management can also be developed for any access events that are considered significant to the IT organization. In some cases, records for access events may need to be kept for a defined period of time for compliance, security or safety reasons.

Any exceptions that are detected should be raised as incidents, using Incident Models designed specifically with security and access rights.

6. **Removing or restricting rights**

Like the work performed for **3. Providing rights**, when needs arise for access rights to be removed or restricted, procedures and guidelines provided by Information Security Management should be followed. Confirmation that the modification/removal has occurred should also be communicated to HR for reporting purposes.

Restriction of rights can often occur under circumstances such as:

- A user has been demoted, or no longer requires the same level of access;
- A user is under investigation, but still requires access to basic services such as email; or
- A user is away from work temporarily and will not require access during that time.

### 1.1.6 Triggers and Interfaces

The execution of Access Management activities is normally triggered by:

- Service Requests, taken by the Service Desk or submitted using automated and self-help mechanisms;
- Requests from Human Resources personnel;
- Direct requests from department managers;
- Request for Changes (RFCs) involving modification of access rights; and
- Requests for enabling restricted access to contractors and external suppliers.

Some of the key interfaces that need to be maintained within the Service Lifecycle are:

- **Service Design**
  - Information Security Management, in the development and renewal of security policies, guidelines and procedures, which are then executed by Access Management; and
- Availability Management, in the design of security systems and infrastructure.

**Service Transition**
- Change Management, which should coordinate changes to processes and any groups and roles defined for Access Management; and
- Configuration Management, which can be used to record relationships between users and systems they can access.

### 1.1.7 Key Performance Indicators (KPIs) for Access Management

Metrics that can be used to measure the effectiveness and efficiency of the Access Management process are:

- Number of exceptions found when auditing access rights;
- Number of requests for access (e.g. Service Requests, RFCs);
- Instances of access granted, by service, user and department etc;
- Instances of access granted by department or individual granting rights;
- Number of incidents requiring a rest of access rights;
- Percentage of requests grouped by method of submission (e.g. using self-help, via the Service Desk, direct requests from management etc); and
- The average time taken to provide, restrict and remove access rights.
10 ITIL Functions

The term function in ITIL refers to the logical grouping of roles and automated measures that execute a defined process, an activity or combination of both. The functions involved with Service Operation are required to enable the effective and efficient delivery and support of IT services. The functions are designed in such a way that aligned roles are grouped together to allow optimal application of resources, skills and knowledge of available staff. When using functions in this way, clear definition of roles and responsibilities is essential for developing a high performing and coordinated approach to Service Operation.

“Know your role, do your job”

Team motto describing the goal for every player, coach and general staff member of the Kansas City Chiefs.

Figure 10.1: 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.

## 10.1 The Service Desk

A Service Desk is a functional unit that acts as the primary point (first line) of contact for the end-user community for all incidents, requests and general communication that arise. It plays an essential and valuable role for any organization, contributing significantly to the satisfaction of users and the overall impression of the IT organization. Depending on the type of business, services and technology supported, the exact size and physical organization of the Service Desk will vary from a small centralized team to a diverse range of teams in multiple locations and time zones.

![Figure 10.2: The Service Desk acting as a ‘Single Point of Contact’ for the end-user community](image)

*Figure 10.2: The Service Desk acting as a ‘Single Point of Contact’ for the end-user community*
10.1.1 Goal and objectives

The primary goal of the Service Desk is to support the agreed IT service provision by ensuring the accessibility and availability of the IT organization and by performing various supporting activities. Other objectives include:

- To act as a single point of contact for all user incidents, requests and general communication;
- To restore ‘normal service operation’ as quickly as possible in the case of disruption;
- To improve user awareness of IT issues and to promote appropriate use of IT services and resources; and
- To assist other the other IT functions by managing user communication and escalating incidents and requests using defined procedures.

10.1.2 Benefits

While many organizations have already seen the justification for the creation of a Service Desk team(s), in many cases the business case for the improvement fail to gain support from various levels of management. As discussed earlier, the needs and requirements will vary significantly for each organization, however the typical benefits gained through the implementation/improvement of a Service Desk function include:

- Improved customer service perception, and satisfaction;
- Increased accessibility through the use of a single point of contact;
- Better quality and speedier turnaround of requests;
- Improved teamwork and communication;
- Better managed infrastructure and control; and
- Improved usage of IT resources.

10.1.3 Service Desk organizational structures

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

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

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

![The local Service Desk structure](image)

**Figure 10.3 – The local Service Desk structure**

<table>
<thead>
<tr>
<th>Benefits of a Local Service Desk structure</th>
<th>Disadvantages of a Local Service Desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Local and specific user knowledge.</td>
<td>• Higher costs for replicated infrastructure and more staff involved.</td>
</tr>
<tr>
<td>• Ability to effectively communicate with multiple languages.</td>
<td>• Less knowledge transfer, each Service Desk may spend time rediscovering knowledge.</td>
</tr>
<tr>
<td>• Appropriate cultural knowledge.</td>
<td>• Inconsistency in service levels and reporting.</td>
</tr>
<tr>
<td>• Visible (and physical) presence of the Service Desk.</td>
<td>• Service Desks may be focused on local issues.</td>
</tr>
</tbody>
</table>
Centralized Service Desk

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

![Figure 10.4: The centralized Service Desk structure](image)

<table>
<thead>
<tr>
<th>Benefits of a centralized Service Desk structure</th>
<th>Disadvantages of a centralized Service Desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced operational costs.</td>
<td>• Potentially higher costs and challenges in handling 24x7 environment or different time zone.</td>
</tr>
<tr>
<td>• Improved usage of available resources.</td>
<td>• Lack of local knowledge.</td>
</tr>
<tr>
<td>• Consistency of call handling.</td>
<td>• Possible gaps in language and culture.</td>
</tr>
<tr>
<td>• Improved ability for knowledge sharing.</td>
<td>• Higher risk (single point of failure), in case of power loss or other physical threat.</td>
</tr>
<tr>
<td>• Simplicity for users (call one number) to contact the Service Desk.</td>
<td></td>
</tr>
</tbody>
</table>
**Virtual Service Desk**

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

![Figure 10.5 – A virtual Service Desk structure](image)

<table>
<thead>
<tr>
<th>Benefits of a virtual Service Desk structure</th>
<th>Disadvantages of a virtual Service Desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Support for global organizations.</td>
<td>• Initial cost of implementation, requiring</td>
</tr>
<tr>
<td>• 24x7 support in multiple time zones.</td>
<td>diverse and effective voice technology.</td>
</tr>
<tr>
<td>• Reduced operational costs.</td>
<td>• Lack in the consistency of service and</td>
</tr>
<tr>
<td>• Improved usage of available resources.</td>
<td>reporting.</td>
</tr>
<tr>
<td>• Effective matching of appropriate staff for different types of calls.</td>
<td>• Less effective for monitoring actions of staff.</td>
</tr>
<tr>
<td></td>
<td>• Staff may feel disconnected from other</td>
</tr>
<tr>
<td></td>
<td>Service Desk staff.</td>
</tr>
</tbody>
</table>
**Follow the Sun**

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

![Follow the Sun Service Desk structure](image)

*Figure 10.6 – A ‘Follow the Sun’ Service Desk structure*

<table>
<thead>
<tr>
<th>Benefits of a ‘Follow the Sun’ Service Desk structure</th>
<th>Disadvantages of a ‘Follow the Sun’ Service Desk structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Support for global organizations.</td>
<td>• Typically higher operating costs.</td>
</tr>
<tr>
<td>• 24x7 support in multiple time zones.</td>
<td>• Cost of required technology.</td>
</tr>
<tr>
<td>• Improved quality of service.</td>
<td>• Challenges in using single language for multiple regions when recording knowledge, workarounds, Known Errors etc.</td>
</tr>
<tr>
<td>• Improved customer/user satisfaction.</td>
<td></td>
</tr>
<tr>
<td>• Effective knowledge sharing and high level visibility of distributed infrastructure.</td>
<td></td>
</tr>
</tbody>
</table>
10.1.4 Service Desk Types (skill levels)

Depending on the requirements defined for the Service Desk, organizations will need to consider what skill level is appropriate for the Service Desk and the support it will offer. This skill level can be defined in many ways, but most often is associated with the first time resolution achieved for calls, incidents and requests made to the Service Desk by users.

The 3 types of Service Desks are:

- **Call Centre**: Responsible for handling/logging of large volumes of calls;
- **Help Desk**: Responsible for managing and co-ordinate incidents; and
- **Service Desk**: Responsible for managing incidents and requests, and also provides a wide variety supporting services (e.g. supporting Human Resources).

*Figure 10.7: Relationship between Service Desk types, costs and first-time resolution*
10.1.5 Service Desk staffing

One of the most challenging issues facing a Service Desk Manager is that of staffing, with many organizations finding it increasingly difficult to acquire and retain quality employees. Additionally, determining appropriate staff levels can be difficult, with call rates being very volatile and dynamic. The following section will describe some of the issues involved with staffing a Service Desk.

Hiring Service Desk staff

Most Service Desk Managers will have a list of key competencies or selection criteria that is used when hiring new staff members. Depending on the type of Service Desk that has been implemented and what types of technologies are being supported these criteria will vary, however typical skills required include:

- Communication skills;
- Technical knowledge;
- Business understanding;
- Diagnosis and analysis skills;
- Understanding of the role/value of processes and procedures; and
- Typing skills.

Communication skills are ultimately the most important as they will need to be able to deal effectively with a wide range of people and stressful situations.

Service Desk staffing levels

The number of staff employed on the Service Desk is dependent on the needs of the business, the objectives/goals defined and a range of other important criteria including:

- Business budget;
- Customer service expectations;
- Size, maturity, design, complexity of the IT Infrastructure and service catalogue;
- The number of customers and users to support;
- The volume of requests, incidents and general communication required;
- Period of support cover required;
- Workload pattern of requests;
- SLA definitions in place;
- Level of training required; and
- Support technologies available.
**Super Users**

Super Users are useful positions to be appointed across an organization to act as liaison points with the IT organization and the Service Desk in particular. Super Users can be used in a number of ways such as:

- To assist in general communication between the Service Desk and users;
- To filter requests and issues raised by the user community; and
- To assist in user training.

While Super Users can be a valuable resource if they are properly coordinated, the following rules should be in place:

- Roles and responsibilities are clearly defined;
- Escalation channels are defined;
- Standard support processes defined and used; and
- All requests recorded and maintained consistently.

**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; and
- 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).
10.1.6 Key Performance Indicators (KPIs) for the Service Desk

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

Some of the typical metrics reviewed when monitoring the performance of the Service Desk include:
- The number of calls to Service Desk (broken down by type, time of day and day of the week);
- First-line resolution rate;
- Average Service Desk cost of handling any incident or request;
- Number of knowledgebase articles created;
- Number or percentage of SLA breaches;
- Call resolution time;
- Customer satisfaction (surveys); and
- Use of self-help (where exists).

10.1.7 Outsourcing the Service Desk

Although fairly common, there are potential risks that can be introduced when outsourcing an organization’s Service Desk. When reviewing the potential for this to occur, Service Managers should consider the following items when developing contracts to reduce these risks:
- Use of your own Service Management tool, not theirs;
- Retain ownership of data;
- Ability to maintain required staffing levels;
- Agreements on reporting and monitoring needs;
- Proven up-to-date procedures;
- Agreed and understood support needs; and
- Engage contract specialists for assistance.
10.2 Technical Management

To enable regular Service Operation, one or more technical support teams or departments will be required 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 departments are also responsible for the daily operation of a subset of the IT Infrastructure.

Technical Management plays an important role within Service Operation by:

- Being the custodian of technical knowledge and expertise related to managing the IT Infrastructure;
- Providing detailed technical skills and resources needed to support the ongoing operation of the IT Infrastructure;
- Providing the actual resources to support the IT Service Management lifecycle; and
- Ensuring resources are effectively trained and deployed to design, build, transition, operate and improve the technology to deliver and support IT Services.

Technical Management is usually organized into teams or departments dealing with technology areas such as:

- Mainframes;
- Servers;
- Storage devices;
- Networks;
- Desktops and Standard Operating Environments;
- Databases;
- Middleware;
- Directory Services;
- Messaging; and
- Telecommunications (including VOIP).

10.2.1 Goal and Objectives

The Technical Management function’s primary goal is to plan, implement and maintain a stable technical infrastructure that supports the organization’s business processes.

This is achieved through:

- Well designed, highly resilient, cost effective technical architectures;
- The use of adequate technical skills to maintain the technical infrastructure in optimum condition; and
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.
To enable quality knowledge sharing and continual improvement of services, technology, processes and other capabilities, Technical Management staff should develop effective communication channels and meet regularly to discuss issues or potential ideas. History demonstrates that quality design requires involvement from those who will be supporting the product/service, as does quality support require involvement from the designers in turn.

### 10.2.2 Key Performance Indicators (KPIs) for Technical Management

The metrics chosen to evaluate the performance of Technology Management will largely depend on which technology is being managed, however some generic metrics areas include:

- **Measurement of agreed outputs:**
  - Contribution in support/enhancement of business processes;
  - Knowledge transferred to other teams and functions;
  - Training provided;
  - Availability of key infrastructure provided;
  - Transaction rates supported; and
  - Installation and configuration of CIs under their control.

- **Process metrics:**
  - Number of events captured and managed (grouped by type);
  - Resolution timeframes for escalated incidents and problems;
  - Number of changes implemented and backed out;
  - Costs incurred against those budgeted;
  - Security issues detected and resolved; and
  - SLA compliance/exceptions.
• Technology performance:
  o Capacity provided;
  o Utilization rates;
  o Availability of services and systems; and
  o Individual CI performance rates.
• Mean time between failures of specified equipment:
  o Per cent of purchased components that remain in place for length of time as expected.
• Measurement of maintenance activity.
• Training and skills development.
10.3 IT Operations Management

IT Operations Management is the function that provides capabilities for performing the daily operational activities required to maintain a stable production (live) environment. In many ways, the function performs many of the logistical activities required for the effective and efficient delivery and support of services (e.g. Event Management).

It is shown in the figure below with an overlap to the Technical Management and Application Management functions, as many of the activities performed will involve elements of the technical infrastructure or applications being supported. In some organizations this means that many of the IT Operations Management activities are performed by the other functions themselves, but in larger organizations it is more common that a centralized group of staff will be designated with responsibility. Good practice generally recommends that Technical and Application Management areas should manage new and unstable systems and applications, and transfer them to IT Operations Management when they have matured.

![Figure 10.9: IT Operations Management](image)

10.3.1 Goal and objectives

The primary goal of IT Operations Management is to perform the IT organization’s day-to-day operational activities using repeatable and consistent actions. Some of the objectives include:

- 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; and
• Swift application of operational skills to diagnose and resolve any IT operations failures that occur.

10.3.2 Operations Control

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

• Monitoring and Control;
• Console Management;
• Job Scheduling;
• Backup and restores; and
• Print and Output Management.

See section 8. Common Service Operation Activities for more information about these activities.

10.3.3 Facilities Management

Facilities Management refers to the role responsible for management of all physical IT environments, usually data centers, computer rooms and recovery sites. In some organizations many physical components have been outsourced and Facilities Management may include the management of the outsourcing contracts. For any organization this is a very important element of IT Service Management, and will contribute to the ability to provide a safe working environment. Facilities Management should be involved in any large scale and project planning to provide advice regarding any physical accommodation of staff or infrastructure required.

1.1.8 Key Performance Indicators (KPIs) for IT Operations Management

IT Operations are measured in terms of its effective execution of specified activities and procedures, as well as its execution of process activities. Some typical metrics areas that are evaluated include:

• Successful completion of scheduled jobs;
• Number of exceptions to scheduled activities and jobs;
• Number of data or systems restores required;
• Equipment installation statistics;
• Process metrics; and
• Maintenance activities.
**Application Management**

The Application Management function (much like the Technical Management function) is responsible for managing applications throughout their lifecycle. This scope can include any staff developing, testing, supporting and improving applications, including those in project roles. In smaller organizations, Applications Management will typically be responsible for performing the daily operations required for applications under their control. Application Management also plays roles such as:

- Supporting and maintaining operational applications, and so plays an important role in design, testing and improvement of applications that form part of IT Services;
- Supporting the organization’s business processes by helping to identify functional and manageability requirements for application software;
- Assisting in the design and deployment of those applications;
- Providing ongoing support and improvement of those applications; and
- Identifying skills required to support the applications.

Application Management will usually be organized into teams or departments dealing with specific applications under their control. This is because each application or set of applications has a different set of management and operational requirements, influenced by:

- Application Purpose;
- Functionality;
- Platform; and
- Brand of technology.

### 10.3.4 Goal and objectives

Application Management’s primary goal is to develop, maintain and support quality applications that enhance the organization’s business processes. This goal is achieved through:

- Applications that are well designed, interface with existing architectures, are resilient and cost-effective;
- Ensuring the functionality and performance requirements of the business are delivered in optimal fashion;
- The use of technical skills to maintain availability of applications; and
- Swift response to diagnose and resolve any disruptions that occur.
10.3.5 Build or Buy?

One of the key decisions that Application Management is faced with is whether to:

*Buy an application that supports the required functionality*

**OR**

*Build the application specifically for the organization’s requirements.*

In most cases the final decision will be made by a Chief Technical Officer (CTO) or IT Steering Group, but to do so they require information from a number of sources. Application Management will assist in the decision making process by providing:

- Application sizing and forecasting workloads and demand cycles;
- Specification of manageability requirements;
- Identification of ongoing operational costs;
- Data access requirements for reporting or integration into other applications;
- Analysis of whether functionality can be met by existing tools – and how much customization will be required to achieve this;
- Estimating the cost of customization;
- Identification of what skills will be required to support the solution;
- Administration requirements; and
- Security requirements.

If the decision is made to build the application, a further decision needs to be made on whether the development will be outsourced or built by employees. Most decisions will be made during the Service Strategy and Design phases, but there are some important considerations for Service Operation, including:

- How will manageability requirements be specified and agreed?
- What are the Acceptance Criteria for operational performance?
- How and where will the solution be tested and who will perform the tests?
- Who will own and manage the Definitive Library for that application?
- Who will design and maintain the operational management and administration scripts for these applications?
- Who is responsible for environment set-up and owning and maintaining the different infrastructure components?
- How will the solution be instrumented so that it is capable of generating the required events?
10.3.6 Application Management Lifecycle

Application Development processes should be implemented as part a coordinated approach to IT Service Management, although in many cases this fails to happen. When the development of applications is not integrated with the rest of ITSM it often leads to a breakdown in communication channels between developers and support staff, and ultimately released applications that are not optimal in supporting business processes.

Application Development and Operations are part of the same overall lifecycle and both should be involved at all stages, although their level of involvement will vary depending on the stage of the lifecycle.

Figure 10.10: The Application Management Lifecycle

© Crown Copyright 2007 Reproduced under license from OGC

1. Requirements

This phase is where the requirements for the new/modified application are gathered through consultation with the business and customers who will be using it. Primarily driven by the Service Design and Service Strategy phases of the ITSM Service Lifecycle, it encompasses the tasks that go into determining the needs or conditions to meet for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders, such as customers, users or the IT organization.
When gathering the requirements for any application, they are usually grouped into six main categories:

1. **Functional requirements** are developed to specify particular behaviors of a system to support a particular business function.
2. **Manageability requirements** are identified from the perspective of the IT organization, addressing the need for a responsible, available and secure service. They also seek to ensure that the application can be built, deployed and supported by Service Operation.
3. **Usability requirements** address the needs of the end-user, evaluating the accessibility of the application and what training may be required to facilitate its effective use.
4. **Architectural requirements** evaluates how the application will integrate within existing architectures, or whether any modifications are required.
5. **Interface requirements** to see where there may be dependencies between existing applications or tools and the new application.
6. **Service Level Requirements** which should specify the performance requirements, the quality of its output and any other qualitative measures that are identified from the customer or user perspective.

**2. Design**

In the Design phase of the Application Management Lifecycle, the requirements are translated into specifications by the system architects and other developers. This enables the design of the application itself, the architecture to be used and the supporting environment for its operation.

Where the application is being purchased from an external supplier, this phase may involve consultation to ensure compatibility for its introduction and to facilitate any modifications or plug-ins that are required for its use. Consideration as to the level of customization of purchased software will often affect the decision whether to build or buy an application.

**3. Build**

During the Build phase, the application is configured and made ready for deployment. Typically this will integrate with the processes of Release and Deployment and Service Validation and Testing, so any application components are coded, integrated and tested effectively.

Using techniques such as the Service V model (see Figure 9.10) for testing provides a framework to help organize the levels of Configuration Items that are needed and the associated testing and validation activities within and across stages of the development of
an application. The left hand side represents the specification of the service requirements down to the detailed Service Design. The right hand side focuses on the validation and test activities that are performed against the specifications defined on the left hand side, and there is direct involvement by the equivalent party on the right hand side.

It shows that service validation and acceptance test planning should start with the definition of the high level requirements. It also describes that the person/group or sign off on the requirements on the left side should be involved on the right side to accept that the requirements have been met.

**Figure 10.11: The Service V Model**

© Crown Copyright 2007 Reproduced under license from OGC

**The Service V Model** is a concept of establishing acceptance requirements against the various levels of requirements that apply in order to justify release to the customer for trial and assessment.

The actual tests required at each level should reflect the approach to risk and level of confidence that is required for the service change being transitioned. There are many
frameworks and sources of guidance focused specifically on testing *e.g.* Test Management Approach (TMAP) that provide more details about the specific types of testing activities that can be performed. These normally include:

- Usability testing;
- Process and procedure testing;
- Knowledge transfer and capability testing;
- Performance, capacity and resilience testing;
- Volume, stress, load and scalability testing;
- Availability, security backup and recovery testing;
- Logistics, deployment and migration testing;
- Build, packaging and distribution testing; and
- Operability and maintainability testing.

4. **Deploy**

The Deploy phase provides a controlled mechanism for the deployment of the application and associated operational model (using Release and Deployment Management). The quality of transition to Service Operation is a crucial element to the success of the overall deployment that is being implemented. Rather than simply hand off support post-deployment, the application development teams should assist provide *Early Life Support,* managing any calls, incidents and problems that are detected in the early of the new or modified service. This enables more stability in this vulnerable period, increased customer and user satisfaction, enhanced learning and better momentum for continual improvement. The resource allocation from these teams will then be gradually reduced while Service Operation takes on more responsibility for support.

5. **Operate**

In the Operate phase, Service Operation delivers and supports the application as required by the business and customers. The techniques described earlier in this book will be used to monitor, control and respond to any disruptions or questions that arise in the use of the application. It is important to note however, that the application is but one component making up an IT Service, and so and end-to-end view of the service should be maintained for effective Service Operation.

6. **Optimize**

The Optimize phase is primarily driven by Continual Service Improvement, where the measurements taken during Service Operation are analyzed and acted upon. Improvement actions may seek to make functionality, usability, performance or any other range of improvement actions that are desired. Internally, ways in which the Application Management Lifecycle itself is utilized may be improved to develop quality applications with less cost/effort.
10.3.7 Key Performance Indicators (KPIs) for Application Management

Some typical metric areas utilized to evaluate the performance of the Application Management function include:

- Measurement of agreed outputs:
  - Accessibility of deployed applications;
  - Recorded Known Errors and workarounds; and
  - User measures of the quality of outputs as defined in SLAs.

- Process metrics:
  - Time taken to build, test and deploy applications;
  - Response times to incidents and problems;
  - Resolution times for incidents and problems;
  - Number of changes implemented and backed out;
  - Defined budgets compared against actual costs incurred; and
  - Utilization levels of application compared to estimates.

- Application Performance:
  - Response times (actual and synthetic transactions); and
  - Application availability, Mean Time between System Incidents, Mean Time to Restore Service etc.

- Measurement of Maintenance activity:
  - Exceptions to agreed maintenance or deployment schedules; and
  - Number of fixes and updates applied.

- Projects:
  - Time and costs spent on projects.

- Training and skills development:
  - User training facilitated;
  - Service Desk training; and
  - Knowledge transfers.
11 Continual Service Improvement

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.

The main areas of focus for Continual Service Improvement to usually address are:

- The overall health of ITSM as a discipline;
- Continual alignment of the portfolio of IT services with the current and future business needs; and
- Maturity of the enabling IT processes for each service in a continual service lifecycle model.

To implement Continual Service Improvement (CSI) successfully it is important to understand the different activities that can be applied to CSI. The following activities can be used to support a continual process improvement plan:

- Reviewing management information and trends to ensure that services are meeting agreed service levels and that the output of the enabling ITSM processes are achieving the desired results;
- Periodically conducting maturity assessments against the process activities and roles associated with the process activities to demonstrate areas of improvement or, conversely areas of concern;
- Periodically conducting internal audits verifying employee and process compliance;
- Reviewing existing deliverables for relevance;
- Making ad hoc recommendations for approval;
- Conducting periodic customer satisfaction surveys; and
- Conducting external and internal service reviews to identify CSI opportunities.

These activities must be planned and scheduled on an ongoing basis. By default, ‘improvement’ becomes a process and mindset within IT with defined activities, inputs, outputs, roles and reporting. CSI must ensure that ITSM processes are developed and deployed in support of an end-to-end service management approach to business customers.
Typically the implementation of IT Service Management comes from an identified need for formalized practices for delivering and supporting services in a controlled and efficient manner. There can be many types of approaches used for implementing these processes, including those using project management methodologies, or those described in the volume of Continual Service Improvement. Even the practices from the Service Strategy in Service Design lifecycle phases themselves are useful guidance to consider when implementing these processes in an effective way.

### 11.1 The Continual Service Improvement Model

The CSI Model provides the basis by which improvements to IT Service Management processes can be made. They are questions to ask in order to ensure all the required elements are identified to achieve the improvements desired.

![Figure 11.2: Continual Service Improvement Model.](image)

© Crown Copyright 2007 Reproduced under license from OGC

The Continual Service Improvement Model summarizes the constant cycle for improvement. While there may be a focus on a particular lifecycle phase, the questions require close interactions with all the other ITIL® processes in order to achieve Continual Service Improvement.
Example improvement initiative for Service Operation:

- **What is the Vision?** Defining what wants to be achieved by improving Service Operation. Is the focus on Service Quality, compliance, security, costs or customer satisfaction? What is the broad approach that we should take?
- **Where are we now?** Baselines taken by performing maturity assessments and by identifying what practices are currently being used (including informal and ad-hoc processes). What information can be provided by the Service Portfolio regarding strengths, weaknesses, risks and priorities of the Service Provider?
- **Where do we want to be?** Defining key goals and objectives that wish to be achieved by the formalization of Service Operation processes, including both short-term and long-term targets.
- **How do we get there?** Perform a gap analysis between the current practices and defined targets to begin developing plans to overcome these gaps. Typically the process owners and Service Operation manager will oversee the design/improvement of the processes, making sure they are fit for purpose and interface as needed with other Service Management processes.
- **Did we get there?** At agreed time schedules, checks should be made as to how the improvement initiatives have progressed. Which objectives have been achieved? Which haven’t? What went well and what went wrong?
- **How do we keep the momentum going?** Now that the targets and objectives have been met, what is the next course of improvements that can be made? This should feed back into re-examining the vision and following the CSI model steps again.

Since Continual Service Improvement involves ongoing change, it is important to develop an effective communication strategy to support CSI activities and ensure people remain appropriately informed. This communication must include aspects of:

- What the service implications are;
- What the impact on personnel will be; and
- Approach/process used to reach the objective.

If this communication does not exist, staff will fill the gaps with their own perceptions. Proper reporting should assist in addressing any misconceptions about improvements.

To aid understanding the differences in perception between the service provider and the customer a Service Gap model can be used. This identifies the most obvious potential gaps in the service lifecycle from both a business and IT perspective.

SLM will produce Service Improvement Plans (SIPs) to meet the identified gaps.
11.2 Managing Cultural Change

Formalizing processes and procedures will require the delivery and management of cultural changes. History has shown that initiatives surrounding IT Service Management, especially for the Service Transition and Operation lifecycle phases, tend to create some resistance in the IT staff, customers and end-users involved or affected. This is largely due to the perception of bottlenecks and bureaucracy being created, or taking away power and authority that the staff members may previously have had.

Those responsible or accountable for implementing or changing Service Management practice should consider the various stakeholders that will be involved or affected, and how best their support can be gained. This typically will involve holding awareness sessions, team meetings and face-to-face discussions, so that all those involved understand the reasons for the changes, the benefits that are being created and how their role contributes or has changed as a result.

The goal of a Communication Plan is to build and maintain awareness, understanding, enthusiasm and support among key influential stakeholder for the CSI program. The plan should incorporate the ability to deal with responses and feedback from the targeted audiences.
11.3 The Deming Cycle

W. Edwards Deming in the 1950s proposed that business processes should be analyzed and measured to identify sources of variations that cause products to deviate from customer requirements. He recommended that business processes be placed in a continuous feedback loop so that managers and supporting staff can identify and change the parts of the process that need improvements. As a theorist, Deming created a simplified model to illustrate this continuous process, commonly known as the PDCA cycle for Plan, Do, Check, Act:

- **Plan**: Design or revise business process components to improve results.
- **Do**: Implement the plan and measure its performance.
- **Check**: Assess the measurements and report the results to decision makers.
- **Act**: Decide on changes needed to improve the process.

![Figure 11.4: The Deming Cycle of Continual Improvement.](image)

Too often organizations are looking for a big-bang approach to improvements. It is important to understand that a succession or series of small, planned increments of improvements will not stress the infrastructure as much and will eventually amount to a large amount of improvement over time.

So in relation to Continual Service Improvement, the PDCA model can be applied with the following steps.
1. Plan – scope, establishing goals, objectives and requirements, interfaces, process activities, framework of roles and responsibilities, appropriate tools, methods and techniques for measuring, assessing, analyzing and reporting.

2. Do (Implement) – funding and budgets, documenting and allocating roles and responsibilities, documentation and maintaining CSI policies, plans and procedures, communication and training, ensuring monitoring, analysis and trend evaluating and reporting tools is in place, integration with the other lifecycle phases.

3. Check (monitor, measure, review) – reporting against plans, documentation review, conducting process assessments and audits. The key here is identifying and recommending CSI process improvement opportunities.

4. Act – implementing actual CSI enhancements (e.g. updating CSI policies, procedures, roles and responsibilities).

11.4 SWOT Analysis

A SWOT analysis is a useful technique that can be used as part of Continual Service Improvement, involving the review and analysis of the internal Strengths and Weaknesses, and the external Opportunities and Threats. Once this analysis has been performed, plans should be made to:

- Develop, exploit and capitalize on the organization’s strengths;
- Reduce, minimize or remove weaknesses;
- Take maximum advantages of opportunities; and
- Manage, mitigate and eliminate threats.

SWOT analyses can be performed at multiple levels or from different perspectives to provide appropriate coverage of the organization as a whole. As a result, the output of a SWOT analysis will feed into the various elements of the Continual Service Improvement phase, and executed by means of the Seven Step (Continual Service) Improvement Process or using a PDCA cycle.

As some suggested guidance for the use of a SWOT analysis:

- Be realistic about the strengths and weaknesses of your organization when conducting SWOT analysis;
- A SWOT analysis should distinguish between where your organization is today, and where it could be in the future;
- SWOT should always be specific, so try to avoid generalizations;
- Where possible, perform a SWOT in relation to your competition, i.e. better than or worse than your competition;
- Keep your SWOT short and simple, so avoid excess complexity and over analysis; and
- SWOTs are subjective, so be sure to include a range of perspectives and levels for analysis.
11.5 Implementing Continual Service Improvement (CSI) processes

Implementing and formalizing CSI will have a major impact on both the customers and IT organization, with changes being made to processes, people, technology and management controls. Unfortunately many project management structures and frameworks fail to appropriately account for the softer aspects involved in organizational change such as resistance, gaining commitment, empowering, motivating and communicating. Especially in the case of CSI programs, success is dependent on the buy-in of all stakeholders, so gaining their support and keeping it will help to ensure their participation and acceptance of the developed solutions. Those responsible for the CSI program should consider these softer issues during the organizational transformation being attempted.

The following describes the main eight reasons why transformation efforts fail (investigated and developed by John P. Kotter from the Harvard Business School), which equally applies to ITSM and CSI implementation programs.

1. Creating a sense of urgency

Unless a sense of urgency is created many stakeholders won't accept that the change is actually required. The sense of urgency should be concerned with answering the question ‘What will happen if we do nothing?’ By answering this question at all levels of the organization it can help to gain stakeholder support and provide input into the business case for implementing CSI. Such consequences of doing nothing could include:

- The business will lose money and productivity due to disruptions to critical IT services, systems and applications; and
- Users will lose confidence in the quality of IT services and revert to manual methods and techniques.

Discussions should be held with the range of involved stakeholders to create awareness and commitment that the current situation is no longer acceptable.

2. Forming a guiding coalition

The next step requires the gathering of a group with enough power to lead the change effort. The guiding coalition team does not need to be comprised of only senior managers, but should include a range of members with the ability to inspire and motivate the organization to change. Over time the group should grow to include a wider range of people and functions. Where necessary, it may be necessary for the group to work together as a team outside of the normal hierarchy.

3. Creating a vision

The guiding coalition should be responsible for ensuring that a vision is produced describing the aim and purpose of CSI. A good vision statement can serve four important purposes:
- To clarify the direction of the program;
- Motivate and inspire people to take action in the right direction;
- Coordinate the actions of many different people; and
- Outline the aims of senior management.

The goals defined as part of the vision should also be SMART (specific, measurable, achievable, realistic and time-bounded).

4. Communicating the vision

The sense of urgency and vision should form the basis of communication to the stakeholders involved in a CSI initiative. For effective communication, all types of communication channels should be used to convey these messages. Another important part of this communication from those responsible should be the demonstration by example (walking the talk).

5. Empowering others to act on the vision

In the empowering phase plans should be directed towards providing the people being affected with the tools, training, direction required in order to contribute to the initiative. When this occurs, the previous energy and enthusiasm developed can be used to assist in the development and implementation of the initiative.

6. Planning for and creating short-term wins

Most initiatives to implement or improve service management practices are a lengthy program of change. So that the enthusiasm and motivation of staff and stakeholders can be maintained a number of short-term wins should be targeted and achieved. They may also help to:

- Convince change skeptics of the benefits;
- Retain support of influential stakeholders; and
- Build confidence to tackle even more complex issues and process integration.

7. Consolidating improvements and producing more change

To ensure that motivation is retained, changes are accepted and the program stays on track to reach the desired long-term goals, those responsible for the CSI program should plan for and target a range of goals, including short-term, medium-term and long-term wins.

8. Institutionalizing the change

Before the CSI initiative and team is finalized, checks should be made to assess whether the changes have been institutionalized. This is a critical step as too often does the organization and staff fall back to their old ways and methods of work. Some signs that the changes have been institutionalized include:

- Monitoring and reporting shows the procedures are being followed;
• People defend the new practices in a positive manner;
• People make suggestions to refine and improve the processes; and
• Service and process owners are proud of their achievements.

11.6 Service Measurement and Reporting

11.6.1 Types of metrics

There are three main types of metrics that an organization will need to collect to support CSI activities as well as other lifecycle process activities:

Technology Metrics: These are often associated with component and application-based metrics such as performance, availability and capacity etc. In most cases it is the system design staff from the Technology and Application Management functions that are responsible for defining, monitoring and reporting against technology metrics.

Process Metrics: The metrics are captured in the form of key performance indicators (KPIs) and activity metrics for the service management processes. They help to determine the overall health, performance and contribution 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. Process owners and managers are typically responsible for defining, monitoring and reporting against process metrics.

Service Metrics: The metrics represent the health, quality and performance of the end-to-end service. Technology and other component metrics are used to calculate the service metrics, which together along with elements of customer/user satisfaction help to understand the customer perspective of services. Service Level Managers and Service Owners are normally responsible for defining, monitoring and reporting against Service Metrics.

11.6.2 Tension Metrics

All service providers are faced with the challenge with a balancing act of three main elements:

• Resources – people, IT infrastructure, consumables and money;
• Features - the product or service and its quality; and
• Time schedule – the timeframes within which various stages and the final delivery of a service or product are required to be achieved.

The delivered product or service therefore represents a balanced trade-off between these three elements. Tension metrics can help create that balance by preventing teams from focusing on just one element. If an initiative is being driven primarily towards satisfying a business driver of on-time delivery to the exclusion of other factors, the manager will achieve this aim by flexing the resources and service features in order to meet the delivery
schedule. This unbalanced focus will either lead to budget increase or lower product quality. Tension metrics help create a balance between shared goals and delivering a product or service according to the business requirements within time and budget.
12 Roles and Responsibilities

12.1 Generic Roles

Process Owner:

The person/role that is responsible for ensuring that all activities defined within the process are undertaken, and is responsible for:

- Defining the process strategy and approach;
- Ensuring the process is designed appropriately for the organization’s needs;
- Ensuring documentation is produced for the process;
- Defining appropriate policies and standards;
- Auditing the process to ensure compliance;
- Review the process, making changes and improvements where necessary;
- Communication process information to key stakeholders;
- Ensuring that staff involved have adequate training, skills and knowledge;
- Addressing issues with the process; and
- Providing input into Continual Service Improvement.

Service Owner:

The person/role that is responsible to the customer for the initiation, transition and ongoing improvement of a particular service, with key responsibilities being:

- To act as the primary customer contact for all service-related enquiries and issues;
- To maintain service quality that meets agreed customer requirements;
- To identify opportunities for improvement;
- To represent the service for CAB meetings;
- To monitor and report data and statistics in order to provide visibility and insight into service quality and performance; and
- To be accountable to the IT director for the delivery of the service.

12.2 Roles within Service Transition

To ensure the quality execution of Service Transition and handover to Service Operations, there should be clear definition of the roles and responsibilities involved. This includes interfaces to Service Design and Project Management, as both require Service Transition in order to deliver one or more service changes.
The roles required for managing the transition of service changes that will be described are:

1. Service Transition Manager.
2. Change Manager.
3. Release and Deployment Manager.
4. Service Test Manager.
5. Service Asset and Configuration Management roles.
6. Knowledge Management process owner.

Depending on the relative size and complexity of the organizations, and requirements for service management, there may be the need to formally define extra roles responsible for specific elements of the Service Transition processes. In other organizations, these roles may be combined and performed by one individual. Regardless of size, all organizations should ensure that testing is managed and performed by resources independent of other functions and processes.
1. Service Transition Manager

Has responsibility for the day-to-day management and control of all the resources, processes and activities being utilized for Service Transition. Their prime responsibilities include:

- Overall planning and management of Service Transition delivery;
- Managing and coordination the Service Transition functions and resources;
- Budgeting and accounting for the team activities and resources involved;
- Acting as the main interface with senior management;
- Ensuring all policies and procedures are followed within transitions;
- Ensuring the transition meets the agreed requirements; and
- Making a final recommendation regarding the decisions for deploying a release in the live environment.

2. The Change Manager

The main responsibilities (including those which may be delegated) include:

- Maintaining oversight of the Change Management process;
- Documenting and communicating agendas for CAB meetings;
- Choosing appropriate CAB members;
- Chairing CAB and ECAB meetings;
- Authorizing or rejecting changes based on evaluation decisions;
- Issuing Change Schedules to be communicated by the Service Desk;
- Reviewing changes for completion of objectives;
- Auditing the process for compliance;
- Reviewing the process for potential inputs to Continual Service Improvement; and
- Producing regular management reports.

3. Release and Deployment Manager

Has overall responsibility for the planning, design, build, configuration, testing and deployment of all software and hardware required for service changes. The main responsibilities include:

- Managing all aspects of the end-to-end release;
- Coordinating the resources required for release and deployment activities;
- Defining an appropriate release policy;
- Assisting in release and deployment planning;
- Overseeing communication, preparation and training; and
- Overseeing any audits of hardware and software in the DML and Definitive Spares.

The Release and Deployment Manager may be supported by other defined roles including:

- Packaging and build managers;
- Deployment managers;
• Early life support; and
• Build, test, deployment environment managers.

4. Service Test Manager

The Service Test Manager should be an independent (not shared) role within Service Transition, with typical responsibilities including:
• Documenting the appropriate test strategy;
• Designing test models;
• Allocating and coordinating test resources;
• Providing management reports on test results, issues and risks;
• Overseeing test execution;
• Managing test environments;
• Verifying tests conducted by Release and Deployment teams; and
• Assisting in the evaluation of service changes based on test results.

5. Service Asset and Configuration Management roles

As the scope of implementations for the process can vary greatly, there may be one, or many roles defined to ensure process objectives are met. The key roles normally defined are:
• Configuration Manager:
  o Responsible for designing and implementing the Configuration Management process, and appropriate policies and standards to be used;
  o Determines appropriate scope and CI recording level for Configuration Management;
  o Develops awareness campaigns to gain support;
  o Assists in evaluating and choosing appropriate systems and tools for the Configuration Management Systems;
  o Oversees the management of the CMS; and
  o Provides management reports.
• Configuration administrator/librarian:
  o Has the operational responsibility for managing the CMS and master copies of software, assets and documentation CIs;
  o Responsible for controlling updates and retrievals of information in the CMS;
  o Provides status reports on CIs;
  o Administers the control activity, including the authorization of ownership rights for CIs;
  o Produces Configuration reports and baselines;
  o CMS/tools administrator;
  o Evaluates off-the-shelf CMS and interfacing tools that meet the organization’s budget, resource and technical requirements;
Manages any tools required for Service Asset and Configuration Management; Liaises with suppliers for customizations and support; and Oversees in-house developed solutions.

Service Asset Manager:
- Has responsibility for the overall management of the service assets used by a service provider;
- Agrees the scope and strategy of the process;
- Designs the process, including interfaces with other processes such as procurement and HR;
- Audits the process for compliance and to detect exceptions; and
- Provide management reports such as audit outcomes and asset reports.

6. Knowledge Management process owner

Has responsibility for the design and maintenance of the Knowledge Management strategy, process and procedures. Key responsibilities include:
- Interfacing designs with the organizational policies and processes;
- Identifying information and knowledge sources, and providing capabilities for capturing using electronic means;
- Maintaining the controlled knowledge items to ensure current validity and usefulness;
- Ensuring accessibility of relevant knowledge bases;
- Advising the business and IT staff members on Knowledge Management concepts and procedures; and
- Providing management reports on the use and value of Knowledge Management.
13 Technology Considerations

Technology is a significant factor in the quality and success of IT Service Management for the modern service provider. There are two main ways in which delivery and support of services is supported by technology:

- Enterprise-wide tools that support the broader systems and processes within which services and service portfolios are developed and managed; and
- Tools targeted more specifically at supporting specific IT Service Management processes or capabilities.

The following systems support the wider scope for enterprise requirements, providing automated support for some elements of Service Management:

- **IT Service Management systems:**
  - Enterprise frameworks;
  - System, network and applications management tools; and
  - Service dashboards and reporting tools.

- **Specific ITSM technology and tools that cover:**
  - SKMS (Service Knowledge Management Systems);
  - Collaborative, content management, workflow tools;
  - Data mining tools;
  - Extract, load and transform data tools;
  - Measurement and reporting systems;
  - Test Management and testing tools;
  - Database and test data management tools;
  - Copying and publishing tools;
  - Release and deployment technology; and
  - Deployment and logistics systems and tools.

With particular focus on the Service Strategy and Service Design processes, tools and systems that can be utilized include:

- Financial Management tools and systems, utilized for charging, accounting and budgeting;
- Web publishing systems utilized for easy communication of the Service Catalogues;
- Monitoring tools for measuring utilization of services, used by Demand Management for predicting and analyzing PBAs and their affect on demand; and
- Document Management Systems, used to manage SLAs, OLAs, Underpinning Contracts and other controlled documents.
For Service Transition processes, tools and systems that can be utilized include:

- Configuration Management Systems (CMS) and tools;
- Version control tools;
- Distribution and installation tools;
- Discovery tools;
- Virtualization for simulating multiple environments; and
- Detection and recovery tools.

For Service Operation, tools and systems that can be utilized include:

- Configuration Management Systems (CMS) and tools;
- Monitoring Agents and Event Correlation Engines;
- Databases for the storage of Incident, Problem and Known Error Records;
- Discovery tools;
- Virtualization for simulating multiple environments;
- Detection and recovery tools; and
- Backup and recovery tools.

13.1 Selecting ITSM tools and supporting technology

While the needs for supporting technology will be influenced by a large number of factors, an integrated suite of ITSM tools and systems should generally include the following functionality:

- Self-help;
- Workflow or process engine;
- Integrated CMS;
- Discovery/Deployment/Licensing technology;
- Remote control;
- Diagnostic utilities;
- Reporting;
- Dashboards; and
- Integration with Business Service Management.
Typical items to consider when evaluating various products for the most appropriate selection include:

- Data structure;
- Integration;
- Conformity;
- Flexibility;
- Usability;
- Support for monitoring service levels;
- Conversion requirements;
- Support options;
- Scalability;
- Tool and Vendor credibility;
- Training needs;
- Customization; and
- What level of adaptation is needed to implement the product successfully.

### 13.2 Knowledge Management Tools

Knowledge Management tools should be utilized to address an organization’s needs for processing information, and enabling and distributing knowledge to enhance the quality of IT Service Management processes. These needs are typically categorized into the following areas:

- **Document Management:**
  - Defines the set of capabilities to support the storage, protection, archiving, classification and retirement of documents and information; and
o Is used to manage documentation CIs such as Service Level Agreements, Underpinning Contracts, User and support documents etc.

- Records Management:
  o Defines the set of capabilities to support the storage protection, archiving, classification and retirement of records; and
  o Includes the management of Incident, Problem and CI records during Service Transition and Service Operation.

- Content Management:
  o Defines the capability that manages the storage, maintenance and retrieval of documents and information of a system or website. The result is often a knowledge asset represented in written words, figures, graphics and other forms of knowledge presentation; and
  o Includes user- and customer-generated information, captured and disseminated using one or more IT Services such as a website or email system.

13.2.1 Communities

Communities are rapidly becoming the communication method of choice for groups of people spread across time zones and country boundaries to collaborate and share knowledge.

Examples of services and functions provided within the typical online community are:

- Community portals;
- Email alias management;
- Wikis and forum groups;
- Focus groups;
- Intellectual property, best practice, work examples and template repository; and
- Online events and net shows.

Successful communities often implement reward schemes for their members to acknowledge and reward the contribution of valuable knowledge assets. It is also recommended that senior management actively participates in these communities to foster a culture and environment that rewards knowledge-sharing and collaboration.

13.2.2 Collaboration

Collaboration is the process of sharing tacit knowledge and working together to accomplish stated goals and objectives. Knowledge services, when properly implemented,
can significantly improve the productivity of people by streamlining and improving the way they collaborate.

Examples of knowledge services, widely available today:

- Shared calendars and tasks;
- Threaded discussions;
- Instant messaging;
- White-boarding;
- Video or teleconferencing; and
- Email.

### 13.2.3 Workflow Management

Workflow Management is another broad area of knowledge services that provides systematic support for managing knowledge assets through a predefined workflow or process. Many knowledge assets today go through a workflow process that creates, modifies, augments, informs, or approves aspects of the asset.

Workflow applications provide the infrastructure and support necessary to implement a highly efficient process to accomplish these types of tasks. Typical workflow services provided within this services category include:

- Workflow design;
- Routing objects;
- Event services;
- Gate keeping at authorization checkpoints; and
- State transition services.
14 Review Questions

The ITIL V3 Intermediate exams are comprised of 8 scenario-based multiple-choice questions (though not all exam questions contain a scenario followed by a question). The following practice exam contains 8 questions for you to complete. In the official exam, all scenarios are provided first, then the questions. To make it easier to follow due to the number of questions, we have set it out with a scenario followed by two associated questions.

Scenario 1

One of the largest auto rental companies in the United States has decided to enter a new market space. Their success in the auto rental has enabled them to invest and diversify into new markets. Based on their market assessments, they have decided to breach into sales of used autos, primarily using the stock of their auto rental fleet. They currently have offices in every city in the US that has a population of 60,000 people or more.

For the new markets, an assessment was performed to determine organization readiness. It was executive internally with consultation from a third party marketing firm and took 9 months to complete. The results of the assessment determined that the current IT infrastructure could not support the new markets and the service levels required. Additionally current business operational capabilities and resources may not be enough to support the expected growth in sales staff.

Financial Management has set a budget for the new services to address the new markets. The board of directors and all major stakeholders are excited about the new markets and the positive response from the customer base for the new services.

Question 1

You are the IT Service Manager. Based on the findings of the organizational readiness assessment, the CEO has asked you to identify the key Service Management challenges that must be understood and addressed.

Which of the following options best identifies the key Service Management challenges?

a) Understanding the initial auto sales market related to current capabilities and resources that can be used to guide sales staff, technology requirements, as well as training for sales staff.

b) Understanding the timelines, milestones, and stages required to rollout to all target locations, alternate support designs, and designs risks in regards to the capabilities of a
third party doing the IT and Business assessment.

c) Understanding the Service Level requirements related to the new auto sales program, warranty of services offered, and the governance requirements related to compliance and audit processes and legal requirements.

d) Understanding the end-to-end scope of transitioning IT support of auto sales with a concentration on organizational transition and the current IT maturity and budget expenditure required to support the new service.

Question 2

Since the majority of stock used by the sales force will come from the stock on hand for auto rentals, a technical solution has been suggested to connect the rental management system to the sales inventory system.

As the project manager assigned to manage the development and transition of this system interface, what is the most appropriate approach to handle the situation successfully?

a) • Analyze the requirements for both the rental and sales business services on the IT solution;
   • Design an appropriate interface between the two systems; and
   • Create a transition schedule that will allow for testing and piloting the interface in cities that have a low risk potential.

b) • Analyze the IT infrastructure, data, and application against the business requirements for supporting the rental and sales business services to determine the gaps in successfully supporting both services;
   • Identify the policies and criteria that must be in place to manage the data flow between the two systems; and
   • Evaluate technical alternatives to identify the most cost effective solution for bridging the two systems.

c) • Design a closed loop system which ensures that data from the rental management is successfully pulled into the sales system with associated activities for transferring assets to the sales force;
   • Implement measurements in the system to track the number of transfers made from system to system as well as the quality of the information as an impact on auto sales; and
   • Monitor the performance of the interface and implement improvements through change control when necessary.

d) • Create a well-defined communication plan identifying the requirements for gathering and distributing information, the audience, and frequency of the communication;
   • Analyze the current business and IT strategies against the requirements for the technical interface to validate the value to the business; and
   • Monitor the development and implementation of the new interface against the
strategic direction for IT to maintain proper integration of the new service.

**Scenario 2**

A new strategic direction has been communicated by the executive team of a large retailer detailing the opening of 100 new stores per year for the next 10 years, expansion of the product line, and the creation of an Internet marketplace.

The retailer currently has 600 stores and over 5000 employees. They only have 100 people working within their IT Department. They have determined that to fulfil their strategy, the IT Department will double in size in the first year with a 5% increase every year after that.

They have hired a new IT Director to manage the growth and demand on IT. A major criterion for choosing the right candidate was knowledge and proven track record in implementing ITIL.

**Question 3**

As the new IT Director, you have decided to review and update the IT strategy to align with the business's new focus and to incorporate the ITIL framework.

What is the best approach for determining the new IT strategy?

a) Determine the IT requirements necessary to support the business within the market spaces they are currently residing and planning to create a presence in. Review the Service Portfolio to determine whether the current IT services meet those requirements, noting any gaps in support that may be identified. Determine the critical success factors in supporting the new business growth and the creation of an Internet presence. Perform a competitive analysis to evaluate the company's current position in the market space and what actions need to be taken to improve the business's competitive edge. Create a plan for creating or modifying services to support the business based on the results of the analysis.

b) Review the current IT strategy against the updated business strategy to identify changes to vision, direction, and requirements. Evaluate the current IT solution to determine gaps in providing services under the new requirements, with special focus on the organization's ability to support an Internet marketplace with its current capabilities. Identify the risks associated with the new direction for the business and the identified gaps. Work with the IT departments to determine the best approach to eliminate or mitigate these risks and incorporate these solutions into the growth plan for IT.

c) Review the updated business strategy and associated plans with key members of the business and IT organization to clearly understand the vision and direction of the business and aligning the IT vision with the business. To ensure competitiveness in the marketplace and properly support the vast number of locations in the company, identify a small number of critical services required by the business to focus on and bring under control. Create a general plan to review each service against business requirements and evaluate or determine the technical solutions available to meet those requirements. Monitor the performance of these services against business outcomes and make adjustments as business requirements change.
d) Perform an analysis of the business activities supported by the current IT solution, specifically noting the frequency and volume of those business activities which will be supported in the new market spaces. Work with the application developers to determine the impact of business growth on the availability and capacity requirements to support the business outcomes expected by the customer. Identify the services and services assets most likely to be impacted by the business growth and prioritize them according to complexity, impact, and cost to update the service. Create a plan that effectively supports the business in their growth while maintaining the same level of support they currently have.

Question 4

The company is planning initiatives to run the business more efficiently. They are currently reviewing different delivery model choices for their Service Desk. They are considering outsourcing this function to reduce cost.

What is the best service provider strategy they should consider during the Service Design phase to manage quality.

a) You recommend the following:
   - Consult with Supplier Manager to identify possible candidates for delivering on business requirements;
   - Business Process Outsourcing to the sourcing organization that is best equipped to handle BPO design and implementation; and
   - Create Service Acceptance Criteria for the Business Process Outsourcer.

b) You recommend the following:
   - Review the service level requirements with potential service providers provided by the Supplier Manager and assess their capabilities to address all SLR’s;
   - Co-source with the service provider that has the best value-to-cost ratio; and
   - Create Service Acceptance Criteria for the External Service Provider

c) You recommend the following:
   - Consult with Supplier Manager to identify possible candidate for delivering on business requirements;
   - Knowledge Process Outsource to the service provider that is best equipped to handle the data; and
   - Create the Organizational Readiness Assessment in the Service Design Package for the Knowledge Process Outsourcer.

d) You recommend the following:
   - Review service warranty expectations with the Service Desk staff;
   - Identify the best Type III provider based on its commitment and maturity to ITIL and lowest cost option; and
   - Create the Service Lifecycle Plan in the Service Design Package for the Type III provider.
Scenario 3

The Wichita State Bank has 475 bank branches in MidWest United States serving over 75,000 customers. It has headquarters in Wichita, Kansas and three data centers located in Sioux Falls, Kansas City, and Oklahoma City. Customers can call to make transactions and inquiries against their accounts or report a problem. The company's normal working hours are 8am to 6pm in each time zone.

The company also has a self-service website that has been experiencing problems with performance because of an issue with server capacity related to the number of transactions that can be handled simultaneously. This has resulted in more customers calling directly to the Service Desk to perform normal banking activities. Changes have been made to the message that customers receive indicating increased wait times because of issues with the web services.

The company has 3800 employees including 450 IT professionals reporting to the IT Operations Director. There are 77 people assigned to a Virtual Service Desk. Of the remaining 368 employees, 5% are assigned to IT Operations Control, 55% to Infrastructure Operations, 18% to Application Support and 22% to Facilities Management.

There is a current project in transition to outsource the Service Desk function. The issues with capacity were not expected during this transition period.

The outsourced service provider has decided to hire 63% of the current Service Desk staff and layoff the remaining staff. Staff morale at the Service Desk is decreasing.

Question 5

As the IT Director, what is the most appropriate approach to handle the performance issue related to server capacity?

a) Review the performance reports against the service commitments detailed in the SLAs to identify gaps between actual performance and desired performance. Prioritize the gaps based on difficulty and cost to implement. Create a plan based on that list that creates a sufficient business case for each improvement opportunity. Monitor the effectiveness of the improvements through changes in performance.

b) Review Service Level Agreements with the appropriate support teams to isolate any contributing sources to the issues and identify any potential solutions to ensure that performance levels match those required by the SLA. Prioritize the improvement opportunities based on level of difficulty to implement, level of impact to problem, and cost. Implement improvements using the change process and monitor those improvements against SLA to validate objectives have been met and identify next steps.

c) Meet with the appropriate support teams to review the services commitment to the business, specifically in the area of performance. Request options for solutions that would resolve the problem with associated timeframes and costs. Authorize the solutions that can be implemented within a reasonable timeframe and will have a low cost of implementation.

d) Perform a risk assessment on the performance issues to identify the impact on the business. Identify appropriate solutions to eliminate or mitigate the risk to business operations and create plans to implement those solutions based on cost and expected time
to completion. Monitor service performance to identify and validate service improvements.

**Question 6**

The insurance company needs to mitigate risk with the Service Desk service provider. What is the best assessment approach in order to mitigate risk?

a) You recommend the following:

- Determine the metrics to measure performance for the end-to-end operations of an outsourced Service Desk; and
- Assess the need for an incentive addresses at the retention of the 65% of the Service Desk staff expected to be hired by the service provider.

b) You recommend the following:

- Assess the need for training the Service Desk pertaining to the outsourcing commitment, the benefits to the organization and the future growth of the Service Desk and company; and
- Utilize organizational metrics so that the organizational model and be updated to closely align with the service provider.

c) You recommend the following:

- Measure and assess the metrics required to monitor end-to-end operation of the outsourced Service Desk; and
- Assess the maturity of the Service Desk process and the Utilization of Technology that will be used by the service provider and identify the gaps.

d) You recommend the following:

- Perform tension metrics against the 77 Service Desk staff, the budget for the outsourced Service Desk and the timeline for the Service Desk transition; and
- Assess service metrics for the end-to-end operation of the Service Desk provider.
Scenario 4

An IT organization is running some business critical services. An assessment identified the following:

- Some areas are well covered with personnel, especially within operations. There is a lack of competence to manage some of the storage needs.
- Due to perceived management pressures, steps are bypassed when implementing changes.
- IT Service Management processes are not well established, but incidents are handled effectively after they occur.
- The cooling system in the service room is of poor quality. Performance has degraded over time.

The organization has an immediate need to improve the following:

- Integration with capacity management; and
- IT audits and overall project management.

As an IT Service Management consultant you are asked to provide guidance to the IT organization on how to best address this situation, considering the above information. ITIL is well received but the organization is also looking for guidance on how to apply best practices to complement their current ITIL practice.

Question 7

The IT organization wants to know which other complementary guidance and established best practice techniques can best help them improve based on their assessment results and on the immediate needs listed in the scenario.

a) You recommend the following:

- Perform a CMMI process review of change and capacity to define a baseline and identify gaps;
- Conduct an ISO20000 certification review of the gaps discovered in CMMI; and
- Apply PMI standards for all on-going and future project management.

b) You recommend the following:

- Apply PRINCE2 standards for managing current and future projects;
- Establish a COBIT review process to identify audit gaps in service processes, specifically capacity; and
- Perform a CMMI process review of Change and Release to establish a baseline and identify gaps for improvement.

c) You recommend the following:

- Establish a Capacity Planning and Management structure using the OSI methodology;
- Perform a CMMI process review of Change Management to define a baseline and identify gaps; and
- Apply Six Sigma to the change process using the CMMI gaps to guide improvements.

d) You recommend the following:

- Perform a CMMI process review of change and capacity to define a baseline and identify gaps;
- Apply PMI standards for all on-going and future project management; and
- Utilize the Monitor and Evaluate process to the gaps identified in CMMI.

Questions 8

The cooling system is problem that shouldn't be ignored. As the IT Service Management Consultant, what is the best approach to address this concern?

a) Perform a risk assessment of the problem and identify possible solutions for reducing the strain on the current cooling system while maintaining the same or better level of support to the business. Make recommendations based on the least difficulty and lowest cost to implement.

b) Review the current Service Level Agreements impacted by the performance issues against the current server capabilities. Analyze the situation to determine the degree of degradation in the current capabilities due to the poor cooling. Working with the IT teams, identify the cooling specifications required to optimize the performance of the current infrastructure. Review the findings with the IT Director.

c) Work with Financial Management and the IT Director to find current opportunities to fund a replacement of the current cooling system. Monitor the progress to ensure that the new system meets the minimum requirements necessary to prevent disruptions in service.

d) Perform a Business Impact Analysis to determine the risk and impact of not resolving the problem immediately against the potential loss of revenue and customer satisfaction. Create a business case presenting the results of the BIA compared to the cost of upgrading or replacing the current cooling system.
16 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.

**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/CIs under control of external suppliers.

**SIP:** Service Improvement Plan.

**SKMS:** Service Knowledge Management System.

**SLA:** Service Level Agreement.

**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.

**Tuning:** Used to identify areas of the IT infrastructure that could be better utilized.
**UC:** Underpinning Contract.

**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.
17 Certification

17.1 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 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.

For more information on certification and available programs please visit our website http://www.artofservice.com.au
17.2 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 in 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 understand and master the standard itself and issues relating to earning actual standards compliance.

For more information on certification and available programs please visit our website http://www.artofservice.com.au
18 Answers to Review Questions

The way the exams are scored are on a 5/3/1/0 point scale. The following answer guide will help you to identify the most correct answer, and why it is more correct than the next answer.

**Question 1**

<table>
<thead>
<tr>
<th>Question Rationale</th>
<th>The question focuses on organizational challenges faced during transformations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Correct</td>
<td>D The answer handles the end-to-end concerns of transitioning support, especially handling cost and process maturity as components to be monitored.</td>
</tr>
<tr>
<td>Second Best</td>
<td>C Does not focus on all components of the transition, just those related to and impacting service levels.</td>
</tr>
<tr>
<td>Third Best</td>
<td>B Focuses on project specific components and low priority items such as alternative solutions and third-party providers. Not all the components of transition can be perceived from these options.</td>
</tr>
<tr>
<td>Distracter</td>
<td>A This answer is simply useless because it is a redundant effort to analysis the market space which has already been done and used to decide on the transition.</td>
</tr>
</tbody>
</table>

**Question 2**

<table>
<thead>
<tr>
<th>Question Rationale</th>
<th>The question focuses on the project management and transition approaches to developing and implementing a technical enhancement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Correct</td>
<td>B Proper design creates proper execution; the focus of this approach clearly understands the requirements and options for creating the interface between the two systems. The information gathered in these steps can be used to assist in the transitional and operational controls for the interface in the future.</td>
</tr>
<tr>
<td>Second Best</td>
<td>C The closed loop system design provides a specific and useful model for ensuring the intentions of integrating the two systems are met. The answer also focuses on the requirements of the services after implementing the solution.</td>
</tr>
<tr>
<td>Third Best</td>
<td>A A workable plan that would get the work done, but the level of success has to focus solely on the proper development and implementation of the interface with almost no input from the business or current capabilities in the IT organization.</td>
</tr>
<tr>
<td>Distracter</td>
<td>D By themselves, these options do not provide any assistance in understanding and designing the interface required, but focuses on its impact on the business.</td>
</tr>
</tbody>
</table>

**Question 3**

<table>
<thead>
<tr>
<th>Question Rationale</th>
<th>The question focuses on aligning the strategies of IT and the business.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Correct</td>
<td>C This answer is the only one that covers all entry points into Service Strategy, perspective, position, plan, and pattern. The approach also directly involves the business.</td>
</tr>
</tbody>
</table>
| Second Best        | A The approach is a reasonable set of activities to create a suitable strategy, but does not provide a well-rounded approach. Focuses specifically on critical success factors in the strategy which concentrates on strategic
<table>
<thead>
<tr>
<th>Question 4</th>
<th>The question focuses on the outsourcing of the Service Desk.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question Rationale</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Most Correct</strong></td>
<td>B</td>
</tr>
<tr>
<td><strong>Second Best</strong></td>
<td>A</td>
</tr>
<tr>
<td><strong>Third Best</strong></td>
<td>D</td>
</tr>
<tr>
<td><strong>Distracter</strong></td>
<td>C</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 5</th>
<th>The question focuses on continual improvement options during Service Operation.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question Rationale</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Most Correct</strong></td>
<td>B</td>
</tr>
<tr>
<td><strong>Second Best</strong></td>
<td>A</td>
</tr>
<tr>
<td><strong>Third Best</strong></td>
<td>D</td>
</tr>
<tr>
<td><strong>Distracter</strong></td>
<td>C</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 6</th>
<th>The question focuses on assessments and mitigating risk.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question Rationale</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Most Correct</strong></td>
<td>D</td>
</tr>
<tr>
<td><strong>Second Best</strong></td>
<td>C</td>
</tr>
<tr>
<td><strong>Third Best</strong></td>
<td>A</td>
</tr>
<tr>
<td><strong>Distracter</strong></td>
<td>B</td>
</tr>
</tbody>
</table>
### Question 7

<table>
<thead>
<tr>
<th>Question Rationale</th>
<th>This question focuses on complementary guidelines, frameworks, and best practices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Correct</td>
<td>B COBIT will handle the improvement of IT audit, PRINCE2 for project management, and CMMI will handle additional issues found in the assessment.</td>
</tr>
<tr>
<td>Second Best</td>
<td>A ISO20000 provides additional support for ITIL, but doesn't provide much additional support in improving IT audits.</td>
</tr>
<tr>
<td>Third Best</td>
<td>D Similar problems as A, and the Monitor and Evaluate process only provides a small amount of additional support.</td>
</tr>
<tr>
<td>Distracter</td>
<td>C Six Sigma is not needed in the scenario described.</td>
</tr>
</tbody>
</table>

### Question 8

<table>
<thead>
<tr>
<th>Question Rationale</th>
<th>This question focuses and identifying and mitigating risk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most Correct</td>
<td>D A BIA provides the greatest insight into the risks related to service disruptions. The creation of a business case provides a comprehensive perspective into the problem and solution from all views.</td>
</tr>
<tr>
<td>Second Best</td>
<td>B Not the best solution but at least attempts to gauge the impact on the business from the perspective of SLA achievement, as well as engaging input from IT.</td>
</tr>
<tr>
<td>Third Best</td>
<td>A A straightforward approach to assessing the risk, the mitigation actions do not consider all options, including the possible replacement of the cooling system.</td>
</tr>
<tr>
<td>Distracter</td>
<td>C There is no rationale behind the steps to replace the cooling system created, and thus no means to justify the new cooling system.</td>
</tr>
</tbody>
</table>
19 References


Websites

www.artofservice.com.au (Company website)
www.theartofservice.org (Online Learning)
www.theartofservice.com (Products and Books)
INDEX

A
acceptance criteria 204, 210-11, 227, 229, 338
access 109, 167, 208, 234, 274, 314-16, 319-20
controlled 314, 316
access rights 207, 316-17, 319-20
accounting 70, 72, 75, 95, 114, 118, 242, 357, 360
Activities of Access Management 315, 319
Activity-based Demand Management 78-9, 81, 85
agents 3, 37-8
Agreed Service Time 129
agreements 83, 97-9, 103, 116-17, 121, 123, 156, 167, 290
alerts 150, 268-9, 273-4
alignment 3, 10-11, 119
Application Management 4, 337-8, 343
Application Management Lifecycle 339-40, 342
application sizing 151-2, 374
approval, financial 190, 310
arrangements 118-19
assemblies 199, 239
    organizational readiness 365, 368
Asset Management 230, 267
    intangible 85
associated business processes 141, 279
attributes 3, 8, 25-6, 44, 66, 232-4, 238-40
audits 114, 164, 169, 234, 240, 242, 244, 253, 318, 350, 357, 359, 372, 382
authorization 62, 64, 114, 182, 186, 189-90, 303, 308, 358
automated business processes 143
automated processes 80, 276
automation 85, 200, 202, 234, 244
availability 9, 14, 18, 25, 44, 77, 125-34, 139-40, 144-5, 151, 166, 193, 245-6, 259, 261-2, 268 [9]
availability levels 27, 125, 128, 132-3, 138, 145, 150, 304
Availability Management process 140
Availability Plan 125, 127, 140

B
backup job 273-4
balance 35, 53, 60, 64, 73, 77, 83, 126, 132, 142, 161-2, 179, 182, 258-64, 266-8, 353-4 [4]
bang 201-2
Banking 198, 240
baselines 68, 151, 153, 189, 208, 221, 230, 239, 347, 358, 372-4
BCM 156-7, 161
BCP (Business Continuity Plans) 162-4
behavior, proactive 266-7
benefits 9-10, 43, 55, 66, 73-4, 97, 110, 117, 197, 224-5, 231, 245-6, 252, 255, 282, 294 [28]
    centralized Service Desk structure 325
    local Service Desk structure 324
    virtual Service Desk structure 326
Benefits of Service Design 90
BENEFITS of SERVICE DESIGN 3
Benefits of Service Operation 255
BENEFITS of SERVICE OPERATION 4
Benefits of Service Strategy 43
BENEFITS of SERVICE STRATEGY 3
Benefits of Service Transition 173
BENEFITS of SERVICE TRANSITION 3
Business Units and Service Units 23, 35-6
business units/processes 68
business users 254
business value 43, 54, 81, 91, 114

C
CAB (Change Advisory Board) 182, 186, 188-9, 192-3, 303
CAB meetings 193, 355, 357
capabilities 7, 24, 31, 35, 39-40, 45-6, 58, 93, 133, 142, 150, 260, 268, 359-60, 362-3, 374-5 [37]
current 206, 365, 367, 373, 380
organization’s 42, 196
self-help 114
excess 77-9, 81, 148
server 370
Capacity and Availability Management 102, 276
Capacity Management 3, 11, 77, 107, 146-50, 152, 154, 281, 304-5, 372
Capacity Management Activities 148
capacity management process 154
Capacity Plan 75, 146, 154, 189
capacity problems 267
capital 68-9, 206
capture 49, 57, 246, 249-50, 252
catalogue information, □ Updating Service 114
cent reduction 107
centralized Service Desk structure 325
certification 4, 378-9
Certification Pathway 4, 378-9
CFIA (Component Failure Impact Analysis) 133-5, 150
challenges 3, 5, 22, 62, 82-3, 145, 154, 171, 178, 194, 246, 255, 258, 292, 325
key Service Management 365
Change Advisory Board, see CAB
Change and Incident Management processes 275
change authority 186, 189
Change Management 3, 112, 114, 154, 179-82, 184-6, 188, 190-6, 200, 204, 212, 224-9, 237, 305, 308, 310-11 [3]
control of 62, 114, 163, 234
organization’s 122
Change Management Activities 186
Change Management and Service Validation 79
Change Management process 106, 164, 181, 183, 185, 193, 294, 357
Change Manager 182, 189-90, 192-3, 356-7
Change Models 182, 186, 188, 191, 309
change proposal 186, 188
change requests 83, 148, 185, 188
changed services 89, 91, 106, 172, 176, 192, 197, 201-2, 206, 212, 214, 224, 232, 246, 252
choice 26-7, 88, 119, 363
clearance 32, 36, 65, 67, 73, 96-7, 110
classification 33, 70, 169, 186, 188, 362-3
closed-loop control system 39-41
closed-loop systems 39
closure 222, 276, 289, 311
CMDB (Configuration Management Databases) 175, 199, 234, 248, 374
CMMI process review 372-3
CMMI process review of Change and Release 372
CMMI process review of Change Management 372
CMS data 243

collaboration 84, 363

communication services 80

communities 363

compny 367-8, 370-1

competition 25, 27, 56, 350

complaints 106, 266, 308

compliance 90, 93, 143, 157, 167, 192, 231-2, 234, 275, 310, 319, 347, 353, 355, 357, 359 [1]

compliments 101, 106

component availability 126-7, 129, 139

Component Capacity Management 148-9, 152, 154

Component Capacity Management sub-process 149

Component Failure Impact Analysis, see CFIA

component failures 130, 134, 161

components 9, 22, 27, 51, 112-13, 126-30, 132-5, 137, 145-6, 149-52, 198-9, 233-4, 246, 258-9,
304, 380-1 [20]

behavioral 30

constituent 92

required 207

service/release 210

sub-service 70

value-added 68

concepts 3, 8, 10, 14, 16-17, 21-4, 40, 67, 72, 116, 128, 130, 202, 214, 219, 248-9 [2]

conditions 39, 44, 52, 63-4, 118, 150-1, 211, 272-3, 310, 339

Conduct service reviews 101, 105

confidence 65, 87, 137, 141, 214-15, 219-21, 223, 341, 352, 381

confidentiality 166, 314, 317

configuration 93, 218, 221, 230, 233, 237, 243, 249, 311, 333, 341, 357-9, 374

Configuration Control 241

Configuration Item, see CI

Configuration Items, see CIs

Configuration Management 4, 93, 113, 185, 194-5, 230-2, 236-9, 242-4, 291, 306, 320

Configuration Management Activities 236

Configuration Management Databases, see CMDB

configuration management roles 356, 358

Configuration Management System, see CMS

Configuration Models 232, 239

conjunction 38, 64, 113, 131, 134, 150, 167, 181, 196-7

consistency of service 201, 326

constraints 24, 26, 31, 50, 88, 106, 214, 216-17

contact 101, 282, 291, 307, 322, 325

context 36, 48, 64, 69, 80, 84, 87, 96, 112, 140, 148, 150, 156, 245, 247, 305 [1]

Continual Service Improvement 4, 13, 17-19, 44-5, 94-5, 131, 139, 169, 175, 212, 223-4, 256, 296,
342, 345-7, 349-50 [3]

CONTINUOUS IMPROVEMENT (CSI) 4, 13, 17-19, 44-5, 79, 94-5, 127, 131, 139, 169, 175, 212,

Continual Service Improvement Model 4, 346

contract reviews 122-3

contracts 98, 103, 116-17, 119, 122-4, 130, 155, 167, 218, 256, 341, 360

Contracts Database 121, 375

contractual commitments 87


control processes 39

cook 22

cooperation 83-4

coordinate, business unit”s capabilities 35

core infrastructure 260, 262

Core Service Package 26-7, 81

correlation 231, 274-5, 278

costs 35-6, 38-40, 42-4, 69-71, 73-4, 84-5, 90-2, 139-40, 144-5, 161-2, 178-9, 231-3, 255, 263-4,
302-4, 370 [37]

actual 68, 71, 73-4, 140, 172, 178, 343

hidden 62, 84-5

©The Art of Service
intangible 140
  □ Average Service Desk 331
Costs of Services and Charging models 114
Creating Service Value 68, 261
criteria, selection 239, 329, 362
Critical Success Factors (CSFs) 3, 46-7, 83, 206, 367, 380
CSFs, see Critical Success Factors
CSI, see CONTINUAL SERVICE IMPROVEMENT
CSI program 348, 351-2
culture, organizational 42, 72-3
customer assets 39-40, 44
Customer/Business Requirements 218, 341
Customer Portfolios 46-7
customization 338, 340, 359

D
damage 141, 158, 164, 170
Data, Information, Knowledge, Wisdom (DIKW) 247
databases 54, 122, 153, 238, 248-9, 276, 285, 360
Definitive Media Library, see DML
Demand Management 3, 38, 68, 75, 77-82, 125, 146, 148, 262
departments 5, 32, 37, 52, 70, 116, 232, 259-60, 267, 308-10, 320, 322, 332, 337, 367
dependencies 109-10, 113-14, 119, 131, 134-5, 281, 340
deploy 35, 93, 196-7, 342
deployment 54, 64, 92-3, 109, 178, 184, 191, 196-7, 199-200, 202-4, 206-14, 219, 224, 311, 340, 342 [7]
deployment activities 203, 206, 209, 213-14, 357
Deployment Management 4, 190-1, 196, 342
Deployment Manager 356-7
deployment of software 213, 310-11
deployment plans 178, 196, 200, 203-4, 209-10, 222
deployment process 200, 203-5
design 8, 14, 16, 18, 30, 38-9, 42, 87, 89-91, 113-14, 130, 148, 221-2, 254-5, 337-8, 340, 359 [23]
design processes 93
design processes 93
Design Service Release 218, 341
Design Service Solution 218, 341
Developing Service Operation 260, 262
devices 39-40, 272-3, 276
diagnose 213, 288, 294, 299, 336-7
diagnosis 125, 142-3, 146, 252, 278, 284, 288, 297, 299, 302-3, 305
diagram 156-7, 186, 249-50, 300
differentiation 24, 26, 47, 81
DIKW (Data, Information, Knowledge, Wisdom) 247
direction 44, 48, 50, 89, 137, 191, 352, 367
directional 52, 54-5, 71, 367, 381
director 193, 355, 365, 367, 370, 373
disadvantages 37, 73, 324-7
disaster 155-6, 162-4, 242, 267
disruptions 123, 125, 128-9, 131-3, 135-6, 139-42, 147, 149, 155, 159-60, 162, 164, 176, 179, 279-80, 299 [11]
disruptions business/organizational 303
Distracter 380-2
distribute 166, 196-7
DML (Definitive Media Library) 199, 311, 374

E
Early Life Support 174, 204, 210-11, 213, 252, 342, 358
ECAB (Emergency CAB) 186, 189, 193, 303
effect
positive 24, 26
unintended 224, 226-7
effectiveness 47, 51, 84, 112, 144, 176, 179, 183, 193, 222-3, 230, 244, 253-4, 260, 278, 291 [4]
elements, critical 130-1, 191, 273
Emergency CAB, see ECAB
emergency changes 183, 193, 261, 267
employees 37-8, 48, 50, 78-9, 182, 249, 338, 367, 370
Encapsulation 3, 38
end-users 21, 23, 97, 114, 190, 194, 196, 214, 226, 268, 284, 291, 294, 304, 311, 317 [3]
environments 19, 32, 92, 126, 151, 157, 174, 180, 197, 205, 208, 222-3, 237, 242, 256, 335-6 [4]
errors 179, 202, 221, 223, 246, 252, 294, 297, 303, 305, 314
problems/Known 305-6
escalation 98, 127, 260, 266, 281, 287-8, 290-1, 297
evaluation 44, 47-8, 58, 72, 93, 148, 181, 184, 186, 191, 193, 204, 212, 214, 224-9, 256 [2]
evaluation report 184, 186, 228
Event and Incident Management 281
event correlation 272, 274, 279
event detection 272-3
event filtering 272-3
Event Management 4, 127, 142, 150, 268-9, 271, 273, 275-6, 278-9, 284, 292, 297, 319, 335
Event Management process 270
Event notification 272-3
events 18, 33, 39, 46, 58, 72, 116, 132-3, 136, 142, 190, 267-9, 272-6, 278-9, 289, 302 [10]
ignoring 273
exceptions 39, 68, 114, 221-2, 242, 244, 262, 269-70, 273-5, 279, 319, 343, 359
exchanges 38, 45-6
External Service Providers 37, 368

F
Facilities Management 336, 370
failures 46, 87, 123, 129-30, 134-5, 138-9, 142-3, 162, 165-6, 176, 183, 194, 276, 284, 299, 374 [1]
Fault Tree Analysis (FTA) 136
field 135, 284-5
filtering 273
Financial Management 3, 11, 64-70, 74, 78, 81, 114, 237, 242, 305, 360, 365, 373
financial resources 66, 69, 85
fit 16-17, 24, 29, 84, 93, 148, 214, 217, 262, 347, 375
focus 6, 10, 14, 22, 36, 40-1, 45, 49-50, 59, 208-9, 260, 262-3, 282, 345-7, 367, 380 [16]
external 259-60
focus of ITIL 10, 14
Formal Problem Management and Incident Management processes 267
formal review 122, 212
formulas 25, 129, 286, 302
frequency 104, 137, 139, 208, 215, 298, 366, 368
FTA (Fault Tree Analysis) 136
FTE (full-time employee) 265
Fulfillment 310
full-time employee (FTE) 265
functionality 89, 91, 138, 255, 261, 304, 337-8, 342, 361, 376
functions 16-17, 19, 32-3, 80, 83, 118, 129-30, 164, 196, 255-6, 321, 323, 333, 335, 351, 356 [3]
funding 72-3, 75, 82, 96, 221, 255, 279, 350
funding models 72-4
funds 72-3, 255, 261, 263-4, 373

G
gaps 75, 347, 366-7, 370-3
generation 104, 269, 275-6
Mean Time  129, 343
Mean Time Between Failures, see MTBF
Mean Time Between Service Incidents, see MTBSI
Mean Time to Restore (MTTR)  129, 278, 375
Mean Time to Restore Service, see MTRS
mechanisms  103, 106, 108-9, 123, 133, 140, 153, 171, 182, 193, 205, 208, 215-16, 250, 310, 316-17
  [4]
  automated  221, 241, 284, 290, 310
meeting  10, 49-50, 105, 128, 132, 197, 290-1, 345
  service level management review  192
minutes, service scope review meeting  107
model  40, 44, 58, 72-3, 75, 218-19, 225, 254, 281, 340-1, 380
  chargeback  54, 73-5, 81
  □ Capacity/Resource  174, 256
modifications  87, 112, 114, 151, 180, 199, 287, 316, 319, 340
modified services  8, 87, 91-3, 150-1, 172, 200, 210, 213-14, 216, 223, 261, 272, 306, 342
Monitor Control Loops  40
monitor service performance  371
monitoring  3, 5, 39-40, 93, 97-8, 102, 104, 132-3, 137, 140, 149-50, 152, 269, 275-6, 331, 353 [6]
monitoring service performance  101, 103
Most Correct  380-2
MTBF (Mean Time Between Failures)  129-30, 135, 145, 334, 374
MTBSI (Mean Time Between Service Incidents)  129-30, 374
MTRS (Mean Time to Restore Service)  129-30, 145, 343, 375
MTTR (Mean Time to Restore)  129, 278, 375

N
new technologies  47, 138, 150, 154, 262, 265
normal changes  182, 186, 192, 256, 308
normal processes  275, 287
notifications  268-9, 272-3
number  10, 105, 115, 124, 129, 134-6, 139-40, 145, 178-9, 229-31, 274, 278, 307, 325-6, 329-31, 365-7 [33]

O
objectives  10-11, 54, 77-8, 96-7, 109-10, 116, 125-6, 146, 155, 166, 168, 176, 196, 230-1, 323, 346-7 [34]
Objectives of Service Design  89
OBJECTIVES of SERVICE DESIGN  3
Objectives of Service Operation  254
OBJECTIVES of SERVICE OPERATION  4
Objectives of Service Strategy  42
OBJECTIVES of SERVICE STRATEGY  3
Objectives of Service Transition  172
OBJECTIVES of SERVICE TRANSITION  3
OLAs (Operational Level Agreements)  18, 95, 101-3, 105, 107, 113-14, 145, 168-9, 175, 200, 256, 281, 360, 375
open-loop systems  39
Operational Level Agreements, see OLAs
Operational Suppliers  120
operations  60, 72, 87, 92, 126, 133, 148, 156, 159, 163, 167, 172, 179, 201, 254-5, 339-40 [5]
Operations Control  336, 370
Operations Management  4, 335-6
Option Space  58-9, 63
organization/business  302
organizational capabilities  7
  specialized  7
organizational changes  5, 31, 209, 249, 351
organizational learning  225, 294
organizational objectives  7
organizational structure  32, 168, 322-3
  suggested  32, 322
potential risks 53, 56, 59-60, 90, 193, 331
price 24, 84, 86, 108
prioritization matrix 286-7
Proactive Problem Management 296, 304-5
problem analysis 299
problem categorization 297-8
problem detection 297
problem investigation 297, 299
problem logging 297
Problem Management 4, 114, 127, 142, 144, 149, 181, 244, 268, 275-6, 282, 290-1, 293-4, 296-300, 302-3, 305-7
activities of 293, 296
problem management processes 139, 303, 307
problem prioritization 298, 303
problem records 275, 291, 297, 303, 305
problem resolution 297, 299, 303
cooperation 83
process activities 336, 345, 350
process compliance 169, 345
process input 39
process integration 149, 352
process interfaces 114
process managers 29, 104
Process metric 114, 175, 353
Process metrics and KPIs 45, 95
process owners 29, 347, 353, 355, 375
knowledge management 356, 359
processes/staff, associated 110
product/service 122, 333
production environment 90, 93, 104, 143, 151, 154, 261, 299, 304
products 7, 11, 92, 103, 121, 132, 146, 168, 196, 300, 309, 349, 353-4, 362, 376, 381 [1]
program 6, 74, 164, 177, 352, 378-9
project management 177, 184, 191, 237, 355, 372-3, 380, 382
Projected Service Outage, see PSO
providers 24-5, 36, 49, 51, 68, 70, 72, 78, 88, 98, 162, 214, 368, 371
business/service 222
PSO (Projected Service Outage) 138, 184, 190

Q
quality, perceived 22
quality management processes 300
quality service management 179, 184

R
RACI 32-3
RACI Model 32-3
Rationale 380-2
RCI 33
recommendations 144, 154, 226-7, 373, 381
recovery 129, 132-4, 142-3, 159, 161-3, 199, 219, 250, 267, 274, 284, 289, 342, 375, 381
recovery facilities 162
recovery mechanisms 155, 305
recovery plans 134, 155, 163-4
recovery tools 361
recurrence 105, 142, 303-4
Reduced operational costs 325-6
Reduced time 145, 213, 252
reduction 68, 88, 124, 145, 165, 167, 169, 374
redundancy 38, 44, 126, 132, 134
rejection 62, 186, 188, 190
Release & Deployment 181, 306
Release & Deployment Management 213, 294
Release and Deployment 191, 196-7, 199, 203, 207, 213, 239, 311
Release and Deployment Activities 203
Release and Deployment and Service Validation 340
Release and Deployment Management 190, 196
Release and Deployment Manager 356-7
Release and Deployment process 200, 203
release packages 175, 196, 198, 203, 208
Release Policy 198, 201, 203, 215
release teams 202, 207
release units 197-8, 200
repair 142-3
Request for Changes, see RFCs
Request Fulfillment 4, 280, 308-13
scope of 308
resolution 117, 125, 143, 146, 282, 284, 286-90, 294, 303, 305-6, 343
resource requirements 9, 93-4, 151, 158, 188, 190, 204, 249, 278
resources 31, 35, 38-9, 54-8, 72, 84-5, 90-1, 114, 130-2, 139-40, 146-7, 156-7, 176, 189-90, 197-8, 356-8 [38]
business/customer 221
response 43, 58, 104, 143, 161, 242, 269, 273-6, 281-2, 286, 288, 290, 298-9, 343, 348, 375
service provider’s 50, 54
responsibilities 4, 7, 9, 32-3, 74, 80-1, 102-3, 114, 164-6, 181-2, 190-2, 210, 237-8, 350, 355, 357-9 [24]
responsiveness 261-2
restaurant 22, 108
retail business processes 99
retirement 52, 114, 204, 210, 362-3
Return on Investment, see ROI review 47, 101-2, 104-5, 114, 121-3, 169-70, 186, 191-3, 204, 212, 242, 303-5, 350, 367, 370, 373 [12]
rewards 61, 64, 83, 120, 363
RFCs (Request for Changes) 18, 44, 106, 114, 174, 177, 182, 184, 186, 188, 192-4, 222, 226, 233, 256, 319-20 [5]
rights 315, 317, 319-20
Risk Analysis and Management 136-7
risk management 86, 137, 160, 225, 228, 381
risk reduction 159, 161
longer-term business 155
low 64, 182, 308, 366
mitigate 371
mitigating 381-2
operational 87-8
service provider manages 215
unacceptable 227
RISKS of SERVICE MANAGEMENT 3
ROI (Return on Investment) 35, 64, 91, 255
S
sales business services 366
sales staff 365
scalability 85, 87-8, 219, 342
SCD (Supplier and Contract Database) 116, 121-2, 375
scenarios 5, 156, 158, 201, 267, 365, 367, 372, 382
scope 13, 54, 72, 108-9, 126, 155-7, 178, 180-1, 189, 196-7, 230-1, 234, 236, 269, 293-4, 358-60
Service Desk Managers 287, 329-30
service desk process 371
service desk staffing 329
service desk staffing levels 329
service desk types 328
service disruptions 129, 133, 142, 190, 262, 382
service downtime 131
Service Evaluation 4, 222, 224-6, 229
service failure 133, 214
Service Failure Analysis, see SFA
service groups 189, 315
Service Improvement Plan, see SIPs
Service Improvement Plans 18, 101, 105, 347, 375
Service Incidents 374
service interfaces 38
service interruptions 144
service investments 58, 60, 64
Service Knowledge Management System, see SKMS
Service Level Agreement, see SLAs
Service Level Agreements 98, 108, 132, 233, 279, 363, 373, 375
Service Level Management, see SLM
Service Level Management process 97
Service Level Managers 94, 375
Service Level Packages 26-7, 81, 148
Service Level Requirements, see SLRs
service levels 49, 87, 105, 113, 148, 150, 153, 156, 173, 202, 254, 260, 324, 345, 365
SERVICE LIFECYCLE PHASES 3-4, 16, 18, 55, 174, 177, 255-6
service lifecycle processes 136, 184
service lifecycle work 3, 18
service management 3, 5, 7, 10, 13, 15, 31, 35, 38-42, 45, 50, 52, 57, 83-4, 87, 281-2 [22]
context of 37, 39
service management activities 18, 112, 166
Service Management implementations 196
service management plans 78
service management practices 9, 352
service management principles 3, 35
Service Management processes 43, 167, 181, 230-1, 244, 250, 276, 346-7, 353, 362, 379
service management systems 91
service management tools 241, 281, 285, 287, 291, 297-8, 310
Service Managers 5, 193, 331, 365
Service Measurement 4, 353
service metrics 353, 371, 381
Service Model 45, 85, 189, 218, 341
Service Offerings & Agreements 9, 82, 96, 116-17
Service Operation 13, 18-19, 32, 44-5, 94-5, 131-3, 149-50, 174-5, 210, 254-6, 258, 260-1, 267-8, 321, 342, 347 [18]
SERVICE OPERATION 4, 43, 126, 143, 196, 276
Service Operation, effective 268, 342
SERVICE OPERATION, normal 129, 163, 268, 279
Service Operation, role of 267, 296
Service Operation and Continual Service Improvement 127, 267
Service Operation processes 127, 255, 262, 275, 347
Service Operational Criteria/Plan 218, 341
Service Operational Readiness Test 218, 341
service operations 176, 196, 224, 227, 252, 254-6, 261, 304-5, 314, 355
service operations key roles 254
Service Operation’s key roles 258
service organization 7, 10, 52
Service Owners 355, 375
Service Package Example 26-7
Service Packages 24, 26-7, 80-1, 218, 222, 341
Service Packages and Service Level Packages 26-7, 114
service performance 18, 120, 122, 146, 213
Service Portfolio and Service Catalogue 102, 112
Service Portfolio Management 3, 52-4, 57, 63-4, 108, 113-14
Service Portfolio Management and Change Management 155
Service Portfolio Management Methods 57, 64
Service processes 372
service provider 14-15, 24-5, 27, 36-9, 45-50, 54-5, 60-1, 65-6, 77-8, 80, 83-8, 98, 116-18, 139-43, 223-4, 371 [27]
service provider interfaces 211, 222
service provider risks 87
service provider staff 245
service provider’s ability 148, 173
service provision 9, 82, 114, 117, 155, 230, 323
service provisioning models 67, 71
service recording 70, 230
Service Release 174
Service Release Package Test 218, 341
Service Release Test Criteria 218, 341
service reports 101, 104, 107
service requests 18, 78, 80, 117, 182, 280, 308-11, 313, 316, 320
service requirements 91, 98, 218-19, 341
Service Review Criteria/Plan 218, 341
service review meetings 104-6, 122, 304
service reviews 107, 123, 345
service scope 9, 63, 101-2, 122
service solution 89, 91, 218, 341
service strategies 42, 47, 50, 83
SERVICE STRATEGY 3, 46, 48
Service Strategy and Service Design processes 360
SERVICE STRATEGY INTERFACES 3
service strategy processes 80
service systems 85
service targets 94, 97, 146
service teams 176, 197
Service Test Manager 220, 356, 358
Service Transition 13, 18-19, 44-5, 64, 87, 93, 95, 131, 172-5, 177-9, 212, 215, 245-6, 251-2, 355, 357-8 [6]
SERVICE TRANSITION 3-4, 177
Service Transition, close 204, 212
service transition activities 176-7
Service Transition Manager 229, 356-7
Service transition plan 95, 176, 204
service transition processes 177, 197, 243, 356, 361
service units 3, 23, 35-6, 39, 87
Service Utility 24-5, 261
Service Validation 4, 204, 207-8, 213-14, 216, 218-19, 222-3, 341
Service Validation and Testing activities 220
Service Validation and Testing process 220, 222-3
service valuation 67, 69-70, 75
service value 24-5, 43, 54, 69, 71, 79, 81
potential 71
Service Value Potential 68
Service Value Test Strategy 217
service warranty 24-5, 261, 366
Serviceability 130, 375
services
common 62, 308, 310
core 26, 81
cost of 245, 263
decommissioned 54, 174
Supplier and Contracts Database 121, 375
Supplier Categorization 119-20
Supplier Management 3, 102-3, 114, 116-17, 122-3, 167, 184, 237
supplier management process 123
Supplier Manager 124, 368
support business processes 68, 97
support organization 43, 138, 144
support services 14, 252, 254
support staff 196, 209, 246, 253, 339
support teams 103, 107, 113, 370
SWOT analysis 350
symptoms 293
system boundaries 62
    cooling 372-3, 382
T
targets
    back-to-back 103
contractual 124
TCO (Total Cost of Ownership) 69, 200
TCU (Total Cost of Utilization) 84, 88
teams 83, 210, 259, 270, 282, 322, 332-3, 337, 342, 351-2, 373-4
technical infrastructure 332, 335
Technical Management 4, 32, 322, 332-3
Technical Service Catalogue 112-13
tension metrics 353-4, 371, 381
test 154, 163-4, 172, 184, 190, 196-8, 202, 204, 206-8, 213-14, 217-19, 221-2, 338, 341, 343, 381 [1]
test environments 189, 208, 221, 299
Test Management 220, 360
Test Management Approach (TMAP) 219, 342
test models 217-18, 221-2
testing activities 163, 219-20, 222, 342
Testing and Service Asset and Configuration Management 213
Testing and Validation Results 175
Third Best 380-2
threats 160, 228, 350
time
    average 307, 320
    repair 143
time zones 322, 325, 363, 370
    multiple 326-7
timeframes 83, 142-3, 172, 178, 288, 290-2, 353, 370
timelines 286-7, 302, 365, 371
Timely incorporation of business plans 154
timescales 90, 162, 281-2, 286
TMAP (Test Management Approach) 219, 342
tools 5, 8, 29, 32, 39, 45, 58, 89, 91, 142, 177, 248, 254-5, 315-17, 350, 358-61 [12]
Total Cost of Ownership (TCO) 69, 200
Total Cost of Utilization (TCU) 84, 88
transactions 46, 85, 108, 145, 153, 274, 370
Transfer of risks 86-7
transition 5, 8, 64, 92, 118, 123, 177, 184, 197, 212-13, 246, 252, 272, 332, 355-7, 380 [2]
Transition Planning and Support  
transition processes, surrounding Service  
TSO  
types  
U  
UCs (Underpinning Contracts)  
unavailability  
Underpinning Contracts, see UCs  
urgency  
users  
utility  
validation  
validation results  
value  
Value networks  
value proposition  
variations  
VBFs (Vital Business Function)  
Vendor Contracts Information  
VIP users  
Virtual Service Desk  
virtual Service Desk structure  
vision  
Vital Business Function, see VBFs  
Vital Business Functions  
vn  
W  
warranty  
websites  
weeds  
Work orders  
workarounds  
Workflow Management  
www.artofservice.com.au