Cloud Computing Best Practices

for Managing and Measuring Processes for On-demand Computing, Applications and Data centers in the Cloud with SLAs

Haley Beard

Foreword

The evolution of managing Cloud Computing Services in principles and practices provided by t he best pr actices I T Service M anagement framework provides the m ore holistic guidance needed for an industry that continues to mature and develop at a rapid pace.

Many organizations and individuals who had previously struggled with their adoption and implementation of Cloud C omputing solutions will co ntinue t o f ind c hallenges in implementing a m anagement framework as part of their approach for governance of their Cloud Computing initiatives. In light of this, the primary goal of this book is to provide the support m aterials needed t o enable t he un derstanding and a pplication o f t he S ervice Management framework in a Cloud Computing Solution.

This comprehensive book is designed as an easy reference that will walk you through the 5 Li fecycle cr itical st eps you n eed t o t ake t o cr eate a su ccessful portfolio o f managed Cloud C omputing IT Services. I n addi tion y ou w ill learn how t o m anage an d r efine y our Cloud Computing service portfolio as your company's business evolves.

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

Contents

1 Introduction

The term IT Service Management (ITSM) is used in many ways by different management frameworks and or ganizations seeking g overnance a nd i ncreased m aturity o f t heir I T organization. Standard elements for most definitions of ITSM include:

- Description o f t he **processes** required t o del iver and su pport I T S ervices for customers.
- The pur pose pr imarily being to del iver and su pport the **technology or pr oducts** needed by the business to meet key organizational objectives or goals.
- Definition o f r oles and r esponsibilities for t he **people** involved i ncluding I T st aff, customers and other stakeholders involved.
- The m anagement of **external su ppliers (partners)** involved i n t he del ivery 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 del iver and su pport q uality I T S ervices that m eet sp ecific business needs and requirements.

The official ITIL® definition of IT Service Management is found within the Service Design book on page 11, describing ITSM as *"A set of specialized organizational capabilities for providing value to customers in the form of services".*

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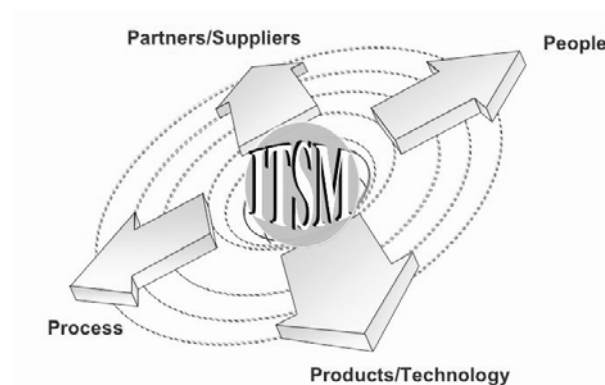
Figure 1.A – Four Perspectives (Attributes) of ITSM

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: IT staff, customers and other stakeholders. E.g. Do staff have the correct skills and knowledge to perform their roles?
- **Products/Technology Perspective:**
Takes into account IT services, hardware & software, budgets, tools.
- **Process Perspective:**
Relates the end to end delivery of service based on process flows.

Quality IT Service Management ensures that all of these four perspectives are taken into account as part of the continual improvement of the IT organization.

1.2 Benefits of ITSM

While the benefits of applying IT Service Management practices vary depending on the organization's needs, some typical benefits include:
- improved quality service provision
- cost justifiable service quality
- services that meet business, Customer and User demands
- integrated centralized processes
- everyone knows their role and knows their responsibilities in service provision
- learning from previous experience
- demonstrable performance indicators

1.3 Business and IT Alignment

A central concept to keep in mind when discussing the benefits of IT Service Management is the goal of business and IT alignment. When staff members of an IT organization have an internal focus on the technology being delivered and supported, they lose sight of the actual purpose and benefit that their efforts deliver to the business. A way in which to communicate how IT supports the business is using the following Figure demonstrating business and IT alignment.

Figure 1. B bel ow di vides an or ganization i nto a nu mber o f su pporting l ayers t hat w ork towards meeting a number of organizational goals. These layers are communicated by the following:

1. **Organization** (What are the key goals for the organization?)
2. **CORE Bu siness Processes** (These b usiness processes enable t he o bjectives above to be met)
3. **IT Service Organization** (What IT Services are required to enable the effective and efficient execution of the business processes above?)
4. **IT S ervice M anagement** (The focus here i s on t he I TIL® pr ocesses required f or quality delivery and support of the IT Services above)
5. **IT T echnical Activities** (The actual t echnical act ivities required as part of t he execution of the ITIL® processes above. These are technology specific and as such not the focus of ITIL® or this document.
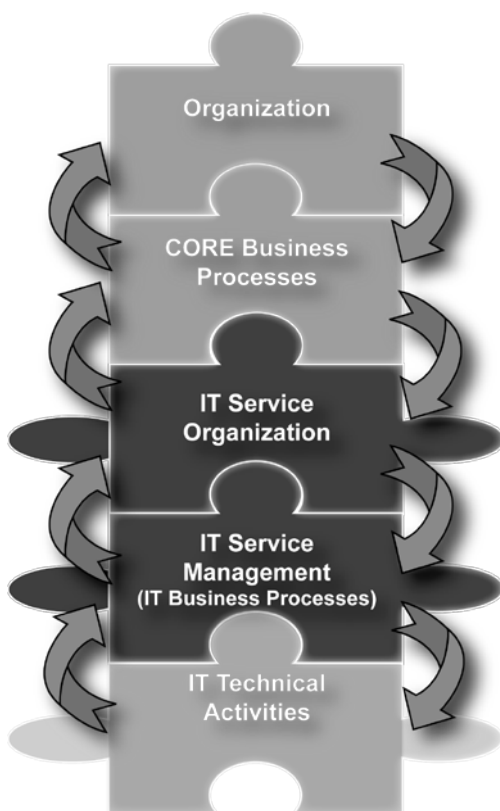
Figure 1.B – Business and IT Alignment

Example to illustrate business and IT alignment:
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 MGT, Incident MGT etc.)
Provisioned cost-effectively (Financial MGT, Service Level MGT)

If we don't manage the IT Services appropriately we cannot rely on these services to be available when we need. If this occurs we cannot adequately support our business processes effectively and efficiently. And therefore we cannot meet or support our overall organization's objectives!!!

1.4 What is ITIL®?

ITIL® st ands for t he I nformation T echnology I nfrastructure Library. I TIL® i s the international d e facto m anagement framework describing "best pr actices" f or I T S ervice Management. The ITIL® framework evolved from the UK government's efforts during the 1980s to doc ument h ow su ccessful or ganizations approached s ervice m anagement. B y the e arly 1990s they had produced a l arge co llection of books documenting t he "best practices" for I T S ervice M anagement. T his library was eventually ent itled t he IT Infrastructure Li brary. T he O ffice o f G overnment C ommerce i n t he U K c ontinues to operate as the trademark owner of ITIL®.

ITL has gone through several evolutions and was most recently refreshed with the release of v ersion 3 i n 2 007. Through t hese ev olutions the sco pe o f pr actices documented h as 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.

ITL is only one of many sources for best practices, including those documented by:
*   **Public frameworks** (ITIL®, COBIT, CMMI etc.)
*   **Standards** (ISO 20 000, BS 15 000)
*   **Proprietary knowledge of organizations and individuals**

Generally best pr actices are t hose formalized as a r esult o f bei ng **successful in w ideindustry use.**
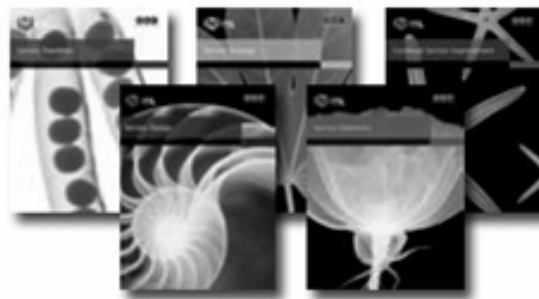
Five volumes make up the IT Infrastructure Library (Version 3).
*   Service Strategy
*   Service Design
*   Service Transition
*   Service Operation
*   Continual Service Improvement

2 Common Terminology

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

Terminology	Explanations
IT Service Management:	A set of specialized organizational capabilities for providing value to customers in the form of services.
Capabilities:	The ability of an organization, person, process, application, CI or IT service to carry out an activity. • The functions and processes utilized to manage services. • Capabilities are intangible assets of an organization and cannot be purchased, but must be developed and matured over time. • *The ITSM set of organizational capabilities aims to enable the effective and efficient delivery of services to customers.*
Resources:	A generic term that includes IT Infrastructure, people, money or anything else that might help to deliver an IT service. Resources are also considered to be tangible assets of an organization.
Process:	A set of *coordinated activities* combining and implementing resources and capabilities in order to produce an outcome and *provide value to customers or stakeholders.* • Processes are *strategic assets* when they create competitive advantage and market differentiation. • Processes *may* define roles, responsibilities, tools, management controls, policies, standards, guidelines, activities and work instructions if they are needed.

Functions: A team or group of *people* and the tools they use to carry out one or more Processes or Activities. Functions provide units of organization responsible for specific outcomes. *ITIL® Functions covered include:*
- Service Desk
- Technical Management
- Application Management
- IT Operations Management

RACI Model: A technique used to define roles and responsibilities of people or groups in relation to processes and activities.
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).
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). **Refer to Figure 2.A*

Service: A means of delivering value to Customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks

Process Owner: The person responsible for ensuring that the process is fit for the desired purpose and is accountable for the outputs of that process.
Example: The owner for the Availability Management Process

Service Owner: The person who is accountable for the delivery of a specific IT Service. They are responsible for continual improvement and management of change affecting Services under their care.
Example: The owner of the Payroll Service

Process Manager: The person responsible for the operational management of a process. There may be several Managers for the one process. They report to the Process Owner.

Internal Service Providers: An internal service provider that is embedded within a business unit. E.g. one IT organization within each of the business units. The key factor is that the *IT Services provide a source of competitive advantage* in the market space the business exists in.

Shared Service Providers:	An internal service provider that provides shared IT service to more than 1 business unit e.g.: one IT organization to service all businesses in an umbrella organization. IT Services typically don't provide a source of competitive advantage, but instead *support effective and efficient business processes.*
External Service Providers:	Service provider that provides IT services to external customers. i.e. outsourcing
Business Case	A decision support and planning tool that projects the likely consequences of a business action. It provides justification for a significant item of expenditure. Includes information about costs, benefits, options, issues, risks and possible problems.

RACI Model

	Service Desk	Desktop	Applications	Operations Manager
Logging	**RA**CI	-	-	CI
Classification	**RA**CI	**R**CI	-	CI
Investigation	**A**CI	**R**CI	**R**CI	CI

Figure 2.A – 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:
Only 1 "A" per Row (ensures accountability, more than one "A" would confuse this)
At least 1 "R" per Row (shows that actions are taking place)

3 The Service Lifecycle
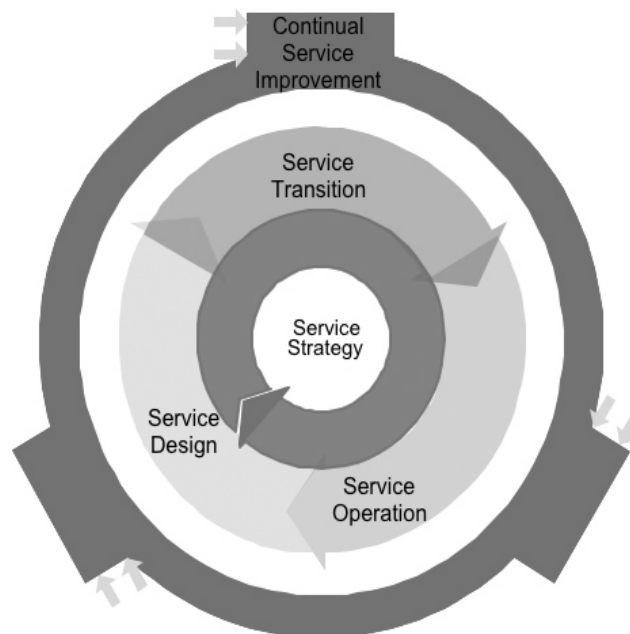
Figure 3.A – ITIL® Service Lifecycle Model

(Acknowledgement – OGC)

Lifecycle: *The nat ural pr ocess of st ages t hat an or ganism or i nanimate obj ect go es through as it matures. For example, human stages are birth, infant, toddler, kid, pre-teen, teenager, young adult, 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 r esult o f t his previous focus on pr ocesses, V ersion 2 o f t he I TIL® F ramework 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 m aintains a h olistic view co vering t he ent ire l ifecycle of a se rvice, 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 maximum value to customers and stakeholders.

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

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

3.1 Mapping the Concepts of ITIL® to the Service Lifecycle

There has been much debate as to exactly how many processes exist within Version 3 of ITIL®. Questions asked include:
- What exactly constitutes a process?
- Shouldn't some processes be defined as functions?
- Why has x process been left out?

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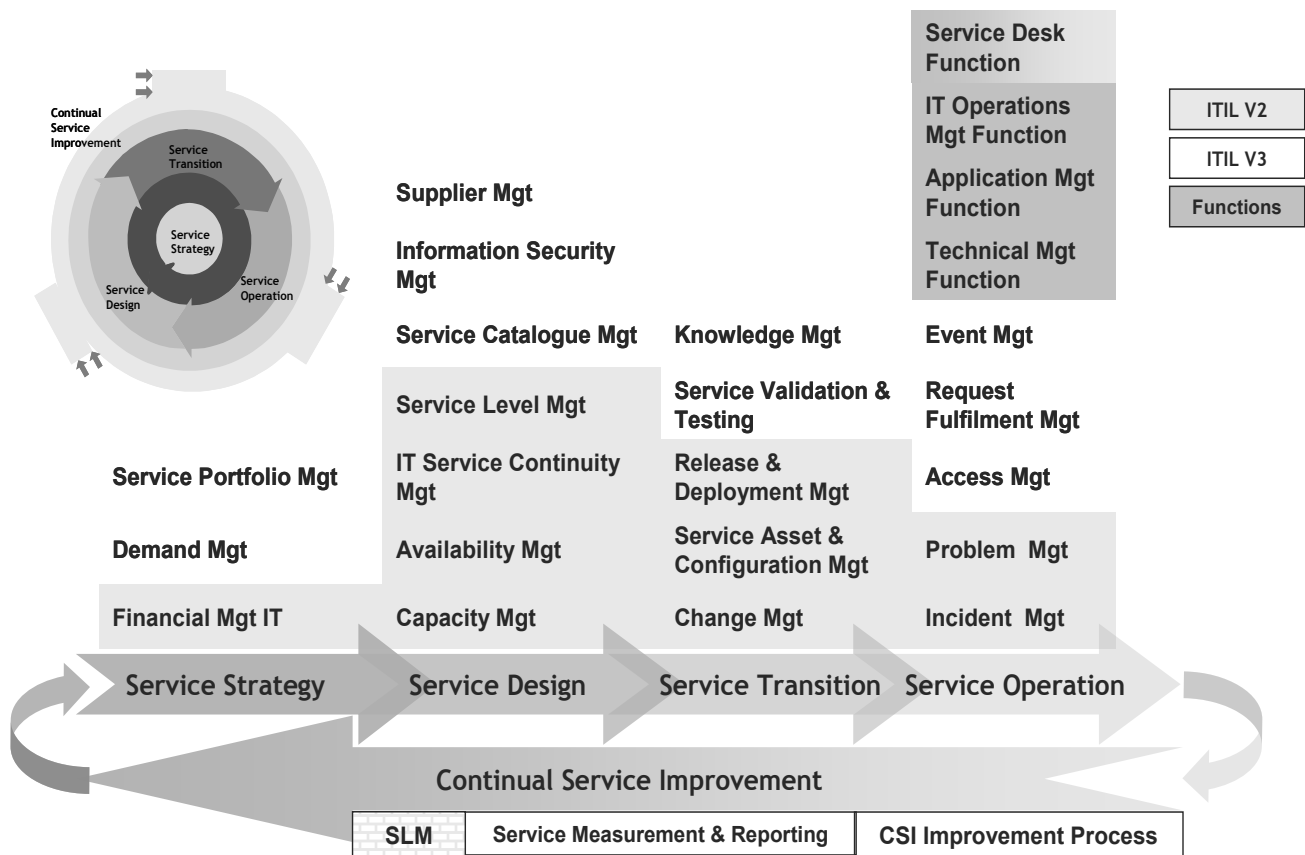
Figure 3.B – The Major Concepts of ITIL®

NOTES:
- The Service Lifecycle phases (and ITIL® books) are shown through the arrows at the bottom.
- The concepts in light shading are the V2 ITIL® concepts.
- The concepts not shaded are the new ITIL® V3 concepts.
- The concepts in dark shading are Functions.
- Although Service Level Management officially sits in the Service Design book, it plays a very important role in the Continual Service Improvement phase, and therefore could also fit in the CSI book as a process.

3.2 How does the Service Lifecycle work?

Although there are 5 phases throughout the Lifecycle, they are not separate, nor are the phases necessarily ca rried o ut i n a par ticular or der. The w hole et hos o f t he S ervice Lifecycle approach is that each phase will affect the other, creating a continuous cycle. For this to w ork successfully, t he C ontinuous Service I mprovement (CSI) p hase i s incorporated throughout al l of t he ot her pha ses. F igure 3. C dem onstrates some t he key outputs from each of the Service Lifecycle Phases.
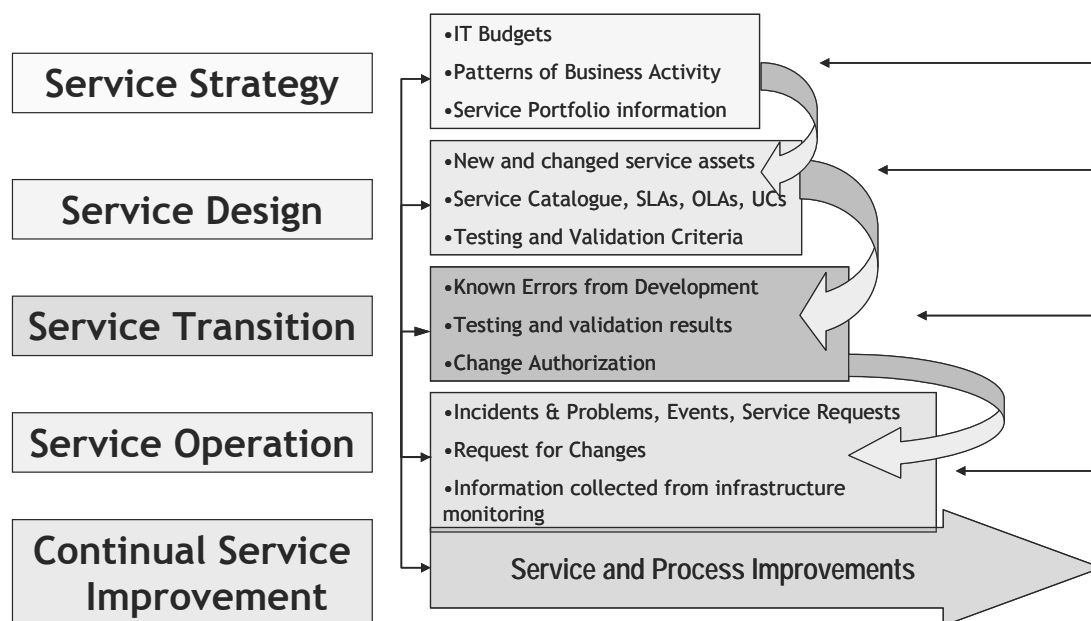
Figure 3.C – How does the Service Lifecycle Work?

It is important to note that most of the processes defined do not get executed within only one l ifecycle phase . A s an ex ample w e w ill l ook at t he pr ocess of **Availability Management** and where some activities will get executed throughout Service Lifecycle.

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.

4 Service Strategy
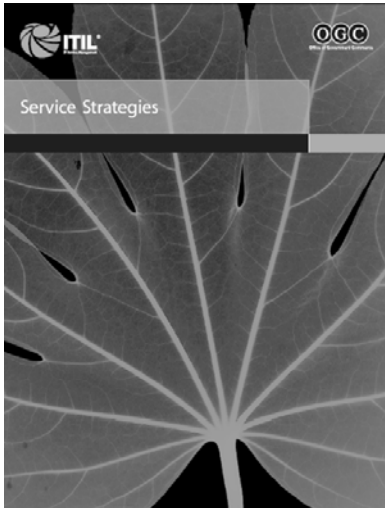
What is strategy?

The term strategy was traditionally used in the military world, where strategy defined the distribution and application of military resources in order to meet the objectives of a plan.

Strategy in the context of Service Management is used by Service Providers to:

- **Attain Market focus** – deciding where and how to compete
- **Distinguish capabilities** – develop service assets that the business appreciates

The processes found within the Service Strategy lifecycle phase are:

- Financial Management for IT Services
- Service Portfolio Management
- Demand Management

4.1 Objectives

The primary objectives of Service Strategy are to:

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

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

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

4.2 Major Concepts

4.2.1 Creating Service Value

One of the major concepts developed within the Service Strategy phase is determining how to create Service value. This ensures that before rushing out to determine how to design a Service, we stop and ask two important questions:

* Why does the customer need this Service?
* Why should the customer purchase it from us?

To answer these questions we will look at the two factors that combine to create value in IT Services.
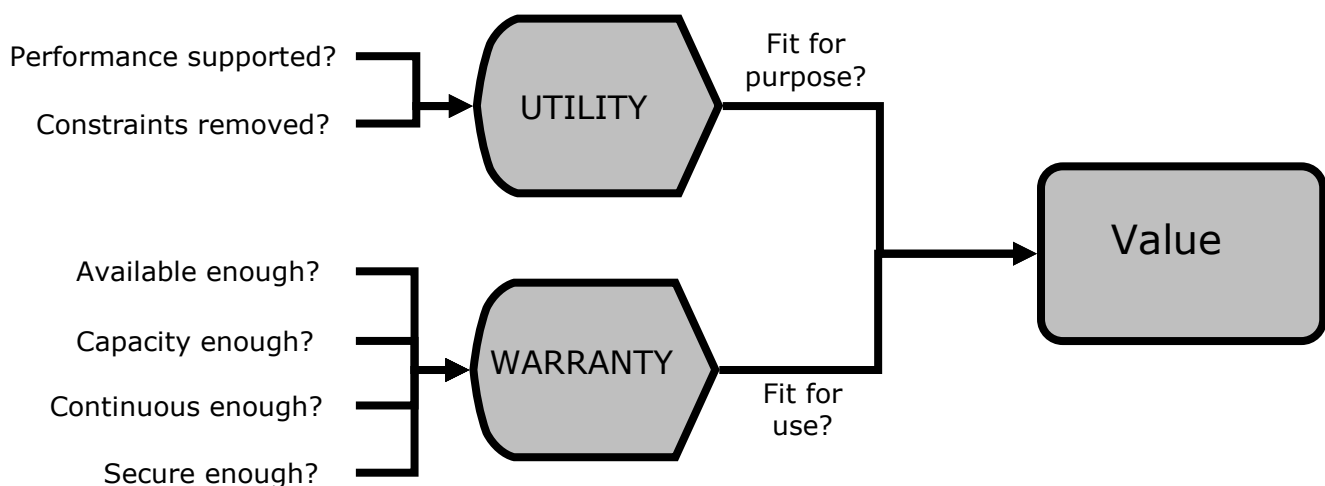
Figure 4.A – Creating Service Value

Service Warranty + Service Utility = Service Value

Service Utility defines the functionality of an IT Service from the customer's perspective (i.e.: what the service does)

Service Warranty for a service provides the customer a level of reassurance and guarantee to meet agreed requirements. (Example attributes: Availability, capacity, continuity, security etc)

These two factors will be communicated via the Service Package produced by the IT organization for use by customers. By doing this it clearly communicates the value offered so that customers can make an informed decision whether to acquire the Service for use.

4.2.2 Service Packages and Service Level Packages

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

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

Service Packages:
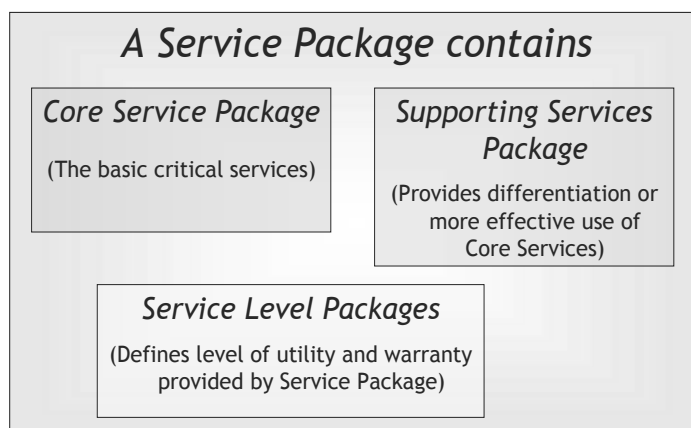
A **Service Package** provides a detailed description of a service available to be delivered to Customers. The contents of a Service Package includes:
- The core services provided
- Any supporting services provided (often the excitement factors)
- The Service Level Package (see next page)

Service Level Packages:
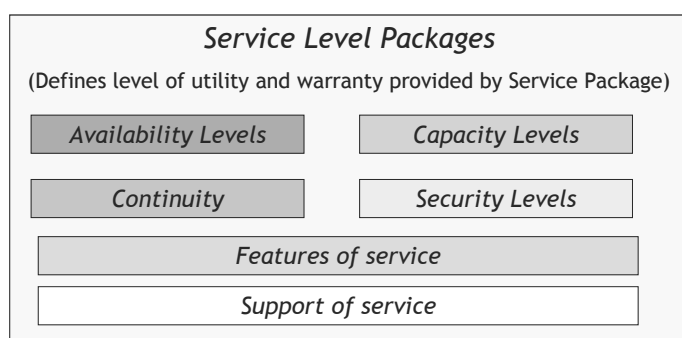
Service Level Packages are effective in developing service packages with levels of utility and warranty appropriate to the customer's needs and in a cost-effective way.
- Availability Levels
- Continuity (e.g. Disaster Recovery)
- Capacity Levels (inc. performance)
- Security Levels

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

Figure 4.B – Service Package Example (ISP)

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 – 24 000kbs (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.

4.3   Service Strategy Processes

The processes included in the Service Strategy lifecycle phase are:
- Financial Management for IT Services
- Service Portfolio Management
- Demand Management

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

4.3.1   Financial Management for IT Services

GOAL: To provide cost effective stewardship of the IT assets and the financial resources used in providing IT services. This enables an organization to account fully for the spend on IT Services and to attribute these costs to the services delivered to the organization's customers.
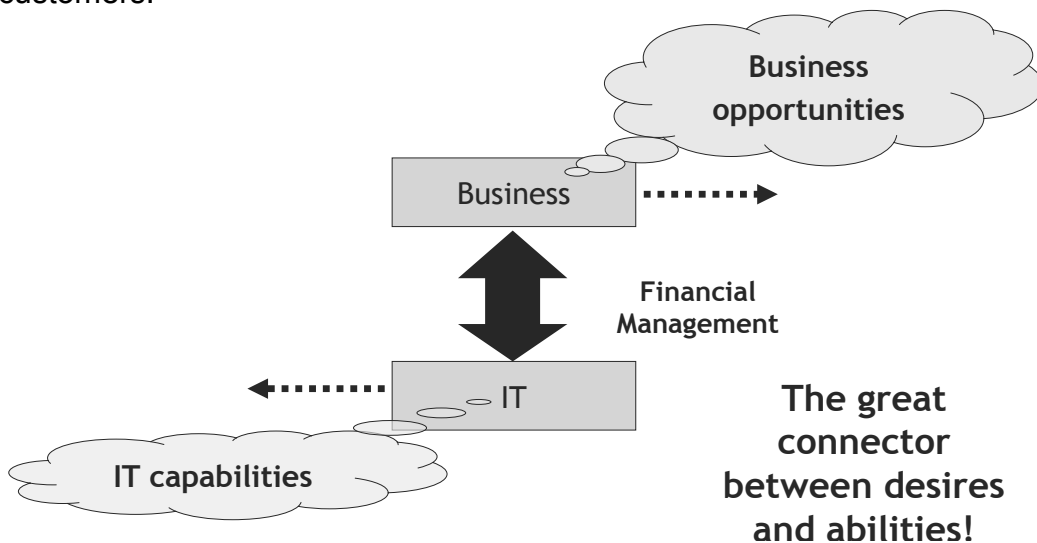
Figure 4.C – Financial Management for IT Services

Using Financial Management for IT (FMIT) to provide services with cost transparency (e.g. via service catalogue) clearly understood by the business and then rolled into the planning process for demand modeling and funding is a powerful benefit for the organization. It enables the best balance to be struck between the opportunities available for the business against the capabilities levels of the IT organization.

Activities

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

1. Budgeting
2. IT Accounting
3. Charging.

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

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

3. **Charging: (optional activity)** Charging customers for their use of IT Services. Charging can be implemented in a number of ways in order to encourage more efficient use of IT resources. Notional charging is one option, in which the costs of providing Services to customers are communicated but no actual payment is required.

Other Terminology (Not Examined at a Foundation Level)

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

FMIT assists in the task of Service Valuation, which is used to help the business and the IT S ervice Provider, agree on t he v alue of t he I T Service. I t determines the bal ance demonstrating the total cost of providing an IT Service against the total value offered to the business by the Service.

Service V alue for s ervices is created by t he co mbination o f S ervice U tility and S ervice Warranty.

4.3.2 Service Portfolio Management

GOAL: To assist the IT organization in managing investments in service management across the enterprise and maximizing them for value.

A **Service Portfolio** describes provider's services in terms of business value. They include the complete set of services managed by a Service Provider. These portfolios are 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.

- Includes the complete set of services managed by a service Provider.
- Provides the information required to manage the entire lifecycle of all services.

3 Categories of services defined in Service Portfolio

- Service Pipeline (proposed or in development)
- Service Catalogue (Live or available for deployment)
- Retired Services (Decommissioned services)

Service Portfolio

Requirements
Description
Value proposition
Business cases
Priorities
Risks
Offerings and packages
Cost and pricing

Service Pipeline

Service Catalogue
•Service Description
•Functional Spec's
•Business English
•Options
•Gold, Silver, Bronze
•customizations
Availability times
•(Price list)

Retired Services
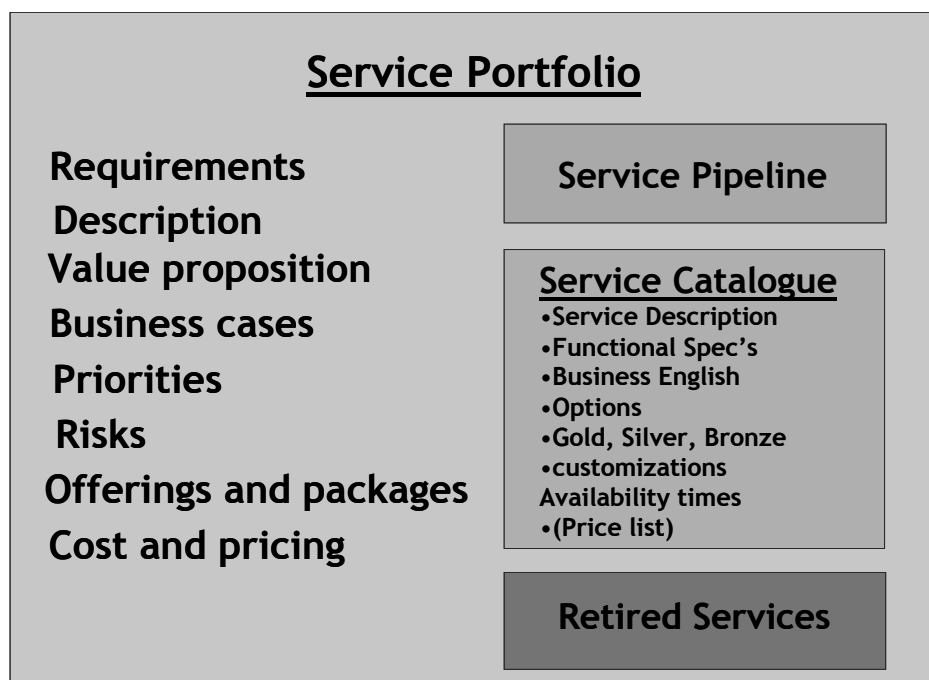
Figure 4.D – A Service Portfolio

Service Portfolios have a much larger scope than Service Catalogues, and is used to manage the lifecycle of all services in order to maximize the value of IT Service Management to the business.

The Portfolio should have the right mix of services in the pipeline and catalogue to secure the financial viability of the service provider. Just like a Financial Portfolio, we need to ensure the balance between risk and benefit provided by the Service Portfolio.

The Service Portfolio uses the above information to provide informed responses to the following strategic questions:
1. Why should a customer buy these services?
2. Why should they buy these services from us?
3. What are the pricing or chargeback models?
4. What are our strengths and weaknesses, priorities and risk?
5. How are resources and capabilities to be allocated?

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

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

Analyze: Maximize portfolio value, align and prioritize and balance supply and demand. This is where strategic intent is created. Questions asked here include:
- What are the long term goals of the service org?
- What services are required to meet those goals?
- What capabilities and resources are required to deliver and support those services?
- How will we get there?

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

Charter: Plans and tracks the progress of service investments across the portfolio and allocate the required resources. Used to schedule and manage the design, transition, change and retirement of services.
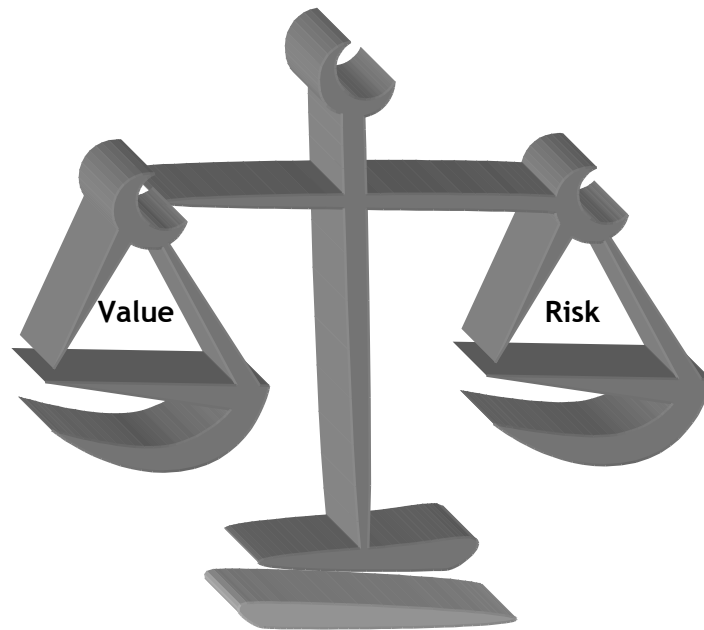
Figure 4.E – Balancing a Service Portfolio

Understanding t heir opt ions helps senior ex ecutives to m ake i nformed i nvestment decisions in s ervice initiatives with appr opriate l evels of r isks and r ewards. These initiatives may cr oss business functions and may sp an sh ort, medium a nd l onger t ime frames.

Investment categories & Budget Allocations
Service Investments are split among 3 strategic categories:

Transform t he B usiness (TTB): TTB i nvestments are m oves into new market spaces

Grow the business (GTB): GTB i nvestments ar e i ntended t o g row the organization's scope of services.

Run the business (RTB): RTB i nvestments are ce ntered o n maintaining service operations
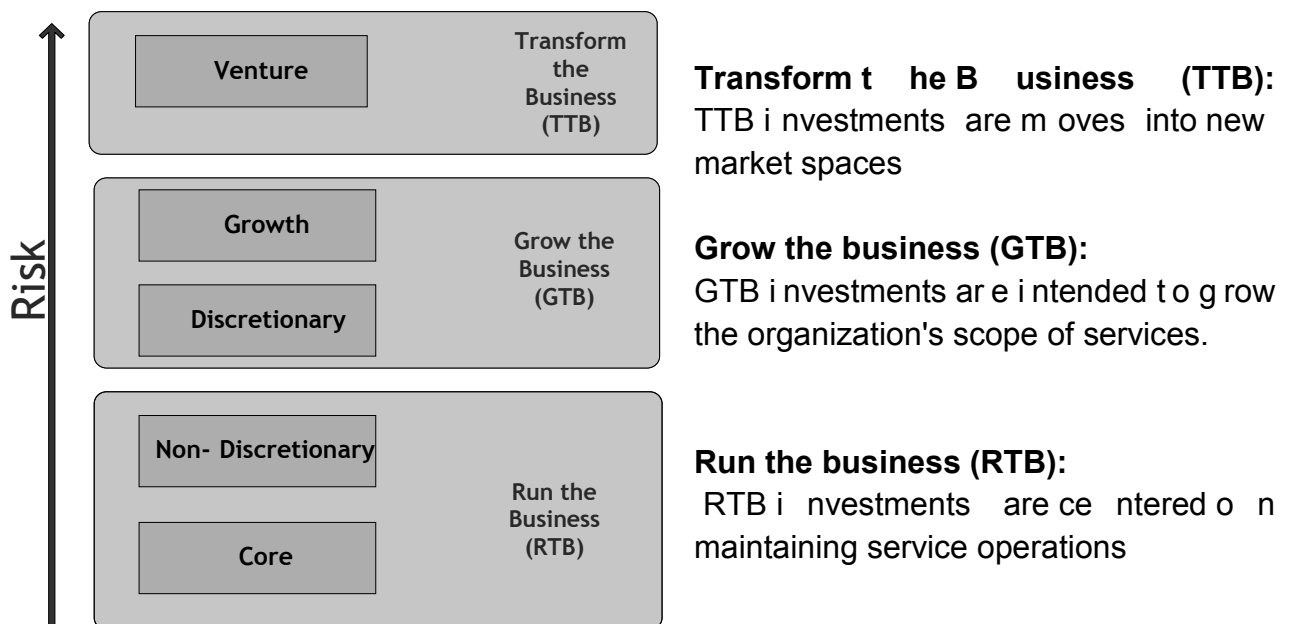
The outcomes for existing services fall into 6 categories:

RENEW: These services meet functional fitness criteria, but fail technical fitness.

REPLACE: These services have unclear and overlapping business functionality.

RETAIN: Largely se lf co ntained, w ith well def ined asset, pr ocess and s ystem boundaries. These s ervices are al igned with an d ar e r elevant t o t he organization's strategy

REFACTOR: Often se rvices that meet t he t echnical and functional cr iteria of t he organization di splay fuzzy pr ocess or sy stem boundaries. I n t hese cases, t he s ervice ca n o ften be r efactored t o i nclude only t he core functionality, with common services used to provide the remainder.

RETIRE: Retire se rvices that do no t m eet minimum l evels of t echnical an d functional fitness.

RATIONALIZE: Used to address portfolios that offer services which in fact are composed of multiple releases of the same operating system, service or application etc.

Service Retirement
An often ov er l ooked i nvestment, t his is potentially one o f t he l argest hi dden co sts in a service providers organization, particularly in a large organization with a long history. Few providers have a clear plan for retiring increasingly redundant services. This is often due to a number of reasons, including a lack of visibility of what services are actually offered, and the fear that retiring a service may impact other services being offered.

Refreshing the Portfolio
As conditions and markets change, some services may no longer be required.
- The C IO m ust m onitor, m easure, r eassess and make c hanges as business needs change
- By or ganizing an e fficient portfolio w ith opt imal l evels of R eturn on I nvestment (ROI) and risk, the organization maximizes the value realization on its resources and capabilities.

4.3.3   Demand Management

GOAL: To assist the IT Service Provider in understanding and influencing Customer demand for Services and the provision of Capacity to meet these demands.

Demand Management was previously an activity found within Capacity Management, and now within Version 3 of ITIL® it has been made a separate process found within the Service Strategy phase. The reasoning behind this is that before we decide how to design for capacity, decisions must be made regarding why demand should be managed in a particular way. Such questions asked here include:
- Why does the business need this capacity?
- Does the benefit of providing the required capacity outweigh the costs?
- Why should the demand for services be managed to align with the IT strategic objectives?

Demand Management is responsible for understanding and strategically responding to business demands for services by:
- Analysing patterns of activity and user profiles.
- Provisioning capacity in line with strategic objectives.

Two ways to influence or manage demand:
1. Physical/Technical constraints
    (E.g. restrict number of connections, users, running times)
2. Financial constraints
    (E.g. using expensive charging for services near full capacity or over capacity quotas)
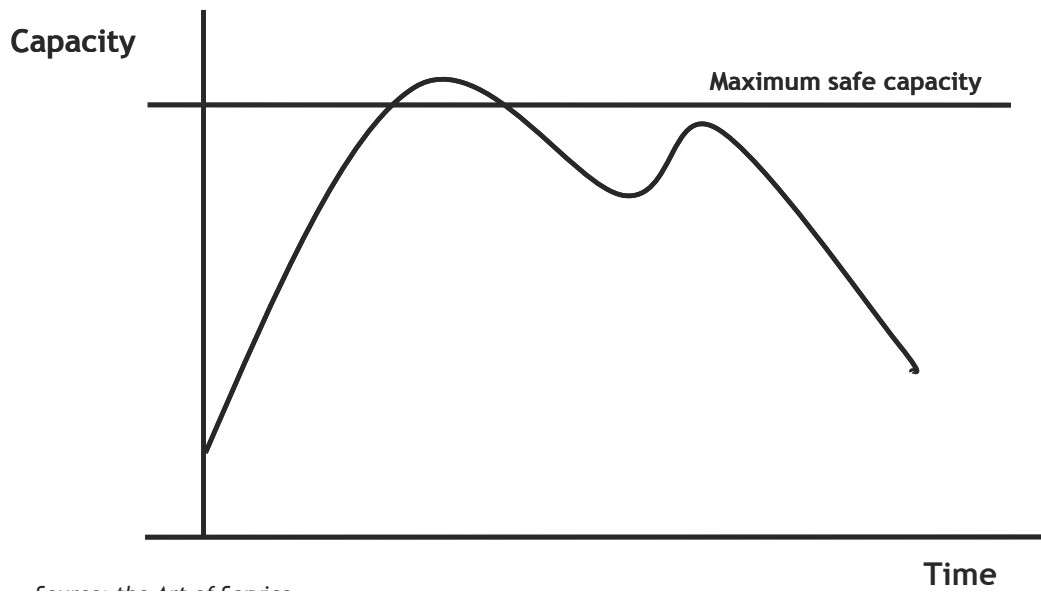
Figure 4.F – Using Demand Management to Optimize IT Capacity

Example responses:

- Staggering work start times
- Prioritizing reports and batch jobs
- Running no n-time-critical r eports and ba tch j obs at ni ght or outside t ypical w ork hours
- Restricting any non-critical activities during peak periods.

Analyzing Patterns of Business Activity (PBA)

Business p rocesses ar e t he p rimary so urce o f d emand f or services. Patterns of business a ctivity (PBA) i nfluence t he d emand p atterns seen b y the ser vice providers.

It is very important to study the customer's business to identify, analyze and co dify such patterns to provide sufficient basis for capacity management.
- Analyzing and t racking t he act ivity patterns of t he busi ness process make i t possible to predict demand for services in the catalogue that support the process.
- Every additional unit of demand generated by business activity is allocated to a unit of service capacity.
- Activity-Based D emand M anagement c an l ink the de mand p atterns to ensu re that the customer's business plans are sy nchronized w ith t he se rvice management plans of the service provider.
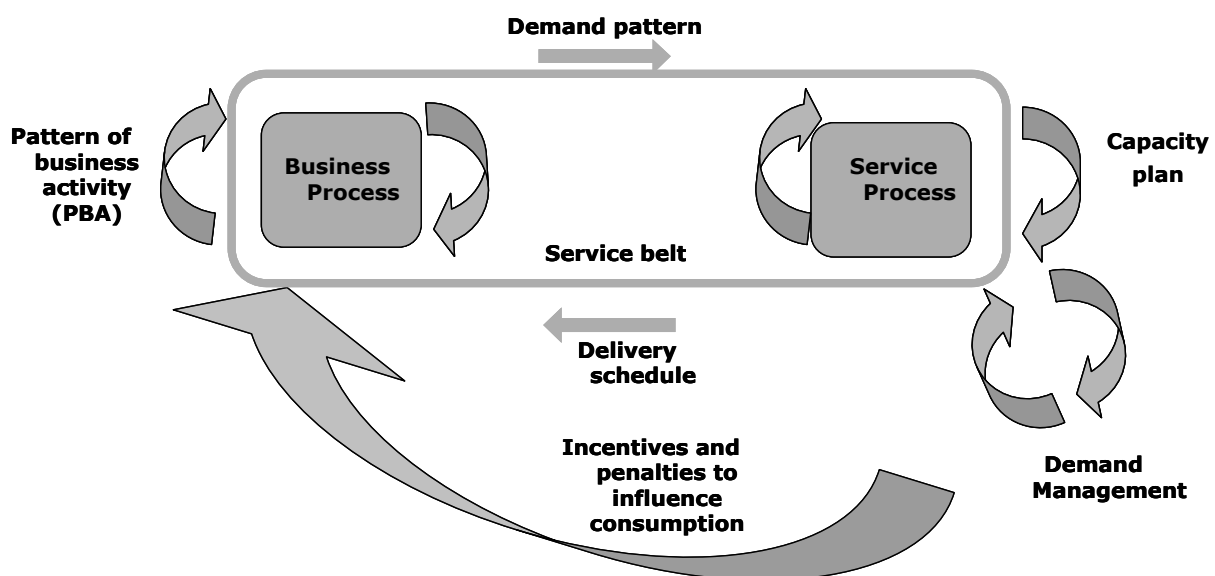
Figure 4.G – Patterns of Business Activity

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 w ay in which Demand M anagement i s utilized will vary greatly between eac h organization. Two examples showing these differences are:

1. **Health O rganizations:** When pr oviding I T S ervices that su pport cr itical services being o ffered t o t he public, i t would be unl ikely t hat a ny de mand management techniques would be utilized, as the impact of these restrictions could lead to tragic implications for patients being treated.

2. **Commercial C onfectionery O rganizations**: Typically a co nfectionery company will ha ve ex tremely busy per iods around t raditional hol idays (E.G Christmas). D emand Management t echniques would be ut ilized t o pr omote more cost-effective use of I T during the non-peak periods, however l eading up to these holidays it would be unlikely for any restrictions to be used.

4.3.4   Implementation

Strategic positions are converted into plans with goals and objectives for execution through the Service Lifecycle. *Figure A* outlines the process whereby positions are driven by the need to service specific customers and market spaces and are influenced by strategic perspectives as a service provider.

Plans are the means of achieving those positions. They include the Service Catalogue, Service Pipeline, Contract Portfolio, financial budgets, delivery schedules, and improvement programs. Plans will ensure that each phase in the Service Lifecycle has the capabilities and resources necessary to reach strategic positions. Clarity and context for the development of these is provided by the Service Lifecycle.

The intent of strategy into action through Service Design, Service Transition, Service Operation and Service Improvement is translated through plans. Service Strategy provides input to each phase of the Service Lifecycle and continual Service Improvement provides the feedback and learning mechanism by which the execution of strategy is controlled.

Figure A

Customer
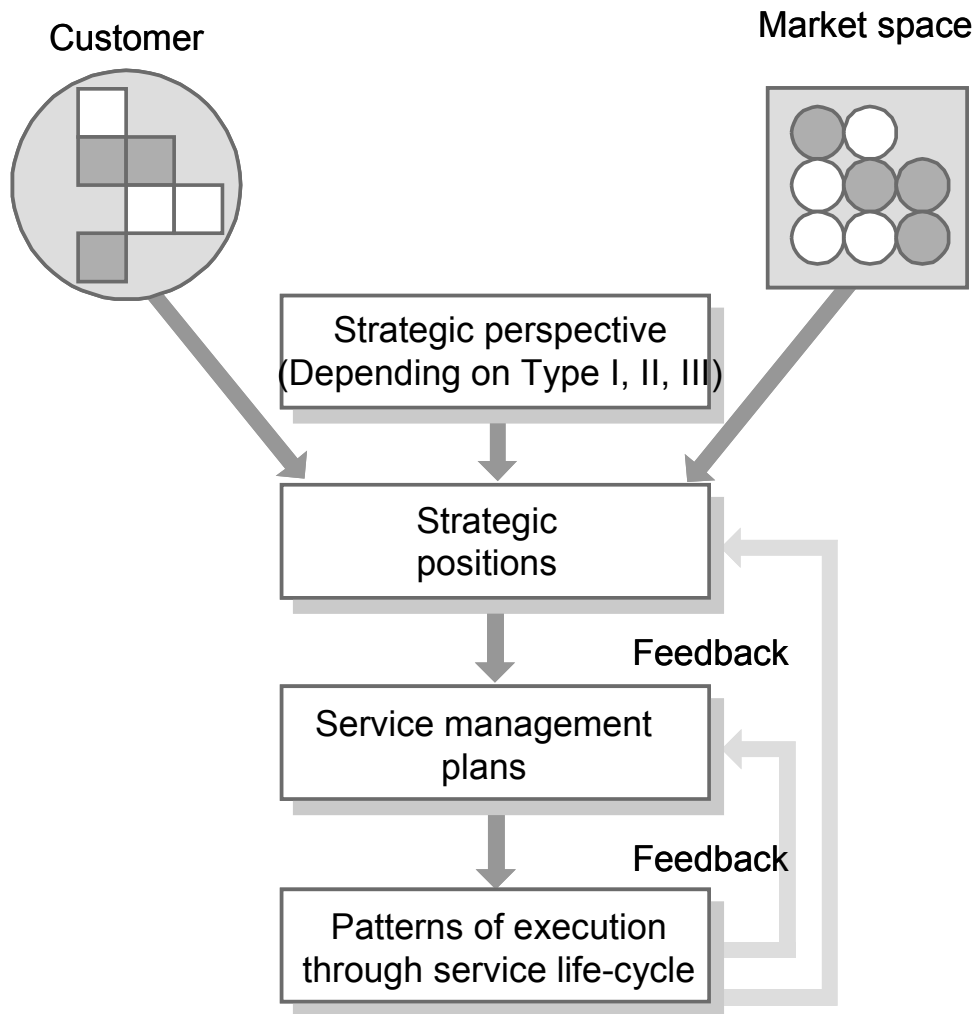
Market space

Top Down

Within any given market space, Service Strategy defines the portfolio of services to be offered and the customers to be supported (see *Figure B*). This in turn determines the Contract Portfolio that needs to be supported with design, transition and operation capabilities. The systems, processes, knowledge, skills and experience required at each phase define the lifecycle capabilities. Interactions between service management capabilities are clearly defined and managed for an integrated and systematic approach to service management. The type of transition capabilities required is determined by Service Desk and Operation capabilities. They also determine the portfolio of service design and the operating range of the service provider in terms of models and capacities.

Figure B

Transition capabilities determine the costs and risks managed by a service provider. The capabilities of the service transition phase determine how quickly a service is transitioned from design to operations. Transition capabilities reduce the costs and risks for customers and service providers throughout the lifecycle by maintaining visibility and control over all service management systems and processes. Not only acting as filters, transition capabilities act as amplifiers that increase the effectiveness of design and operation. Transition capabilities interact with service designs to provide new and improved service models. They also interact with operation models and capacity to increase the operational effectiveness of plans and schedules. The net effect is the service levels delivered to customers in fulfilment of contracts.

Service providers and customers each face strategic risks from uncertainties. It is impossible to either control or predict all the factors in a business environment. The risks may translate into opportunities or challenges depending on the alignment between service management capabilities and the emergent needs of customers. Continual Service Improvement is required for Service Strategy to drive feedback through the Lifecycle elements to ensure that challenges and opportunities are not mismanaged (*Figure C*).

Figure C

New strategic positions are adopted based on patterns that emerge from executing the Service Lifecycle. In order to form a closed-loop planning and control system for service strategies, bottom-up development of Service Strategy is combined with the traditional top-down approach (*Figure D*). Such feedback and learning is critical to the success factor for service management to drive changes and innovation.

Figure D
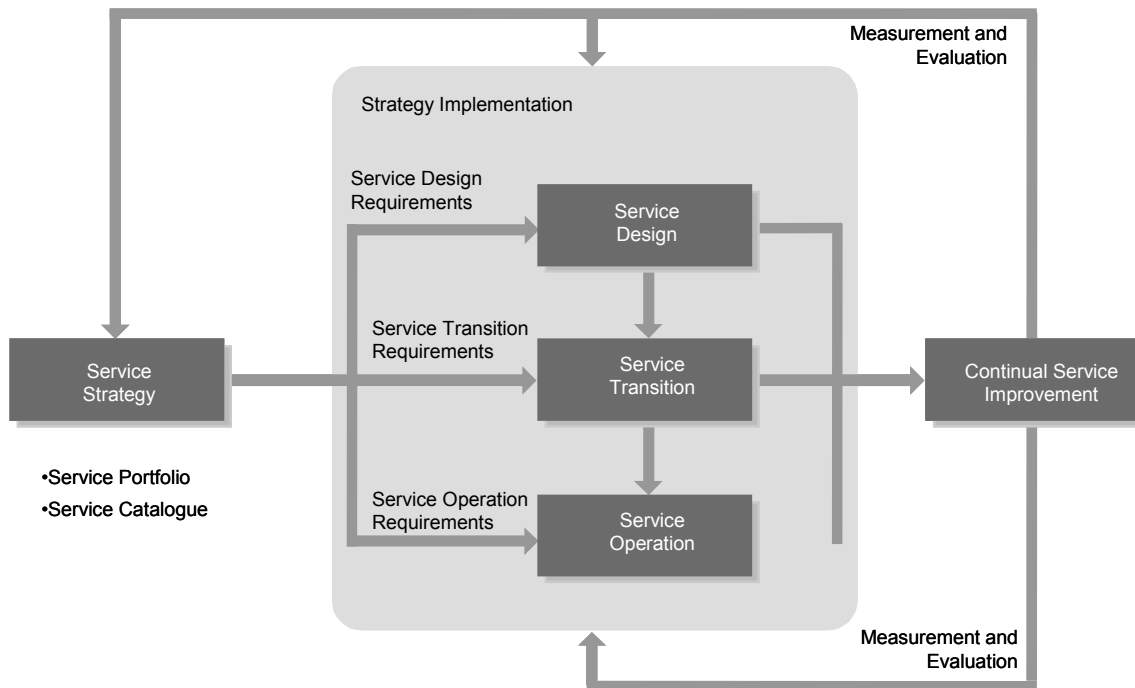
4.4 Service Strategy Summary

The Service Strategy phase enables the organization to ensure that the organizational objectives for IT are defined and that Services and Service Portfolios are maximized for value. Other benefits delivered include:

- Enhanced ability to predict the resources required to fund IT.
- Clearer visibility of the costs for providing IT Services.
- Quality information to support investment decisions in IT.
- Understanding of the use and demand for IT Services, with the ability to influence positive and cost-effective use of IT.
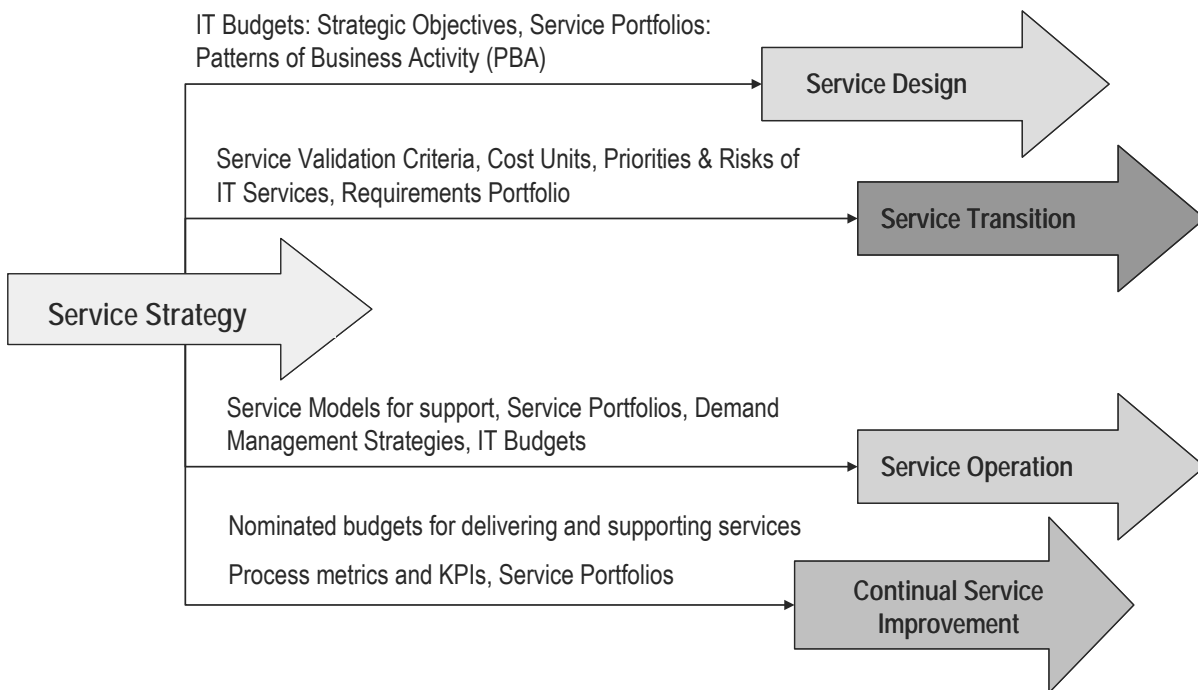
Figure 4.H – Some outputs to other lifecycle phases.

4.5   Service Strategy Service Scenario

To assist with your learning and understanding of how the phases and processes work together, the following scenario will be used throughout this book.

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

The business has requested that they would like to be able to use the internet for instant messaging with international offices. They are also interested in VOIP and video conferencing. (We shall call this new service HYPE!)

Overall Service Strategy

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

Service Portfolio Management

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

FMIT

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

Demand Management

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

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

5 Service Design

Service Design's ultimate concern is the design of new or modified se rvices for i ntroduction i nto a pr oduction (live) environment. I t i s also co ncerned w ith t he desi gn of new and m odified processes required t o deliver and su pport these services.

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

5.1 Objectives

There are three main objectives of the Service Design lifecycle phase:
- To co nvert t he st rategic objectives defined dur ing S ervice S trategy i nto S ervices and Service Portfolios.
- To use a holistic approach for desi gn t o e nsure i ntegrated en d-to-end busi ness related functionality and quality.
- To ensure consistent design standards and conventions are followed.

5.2 Major Concepts

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

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

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

Service Design Packages
The information contained within a Service Design Package including all aspects of the service and its requirements is used to provide guidance and structure through all of the subsequent stages of its lifecycle. A Service Design Package is produced for each new IT Service, major Change, or IT Service Retirement.

Service Design Packages	
• Business Requirements	• Organizational Readiness Assessment
• Service Applicability	• User Acceptance Test Criteria
• Service Contacts	• Service Program
• Service Functional Requirements	• Service Transition Plan
• Service Level Requirements	• Service Operational Plan
• Service Design & Topology	• Service Acceptance Criteria

5.3   Service Design Processes

The processes included with the Service Design lifecycle phase are:
* Service Level Management (Design)
* Capacity Management
* Availability Management
* IT Service Continuity Management
* Information Security Management
* Supplier Management
* Service Catalogue Management

It is important to note that many of the activities from these processes will occur in other lifecycle ph ases, especially S ervice O peration. A dditionally, Service Lev el M anagement also plays an important role in Continual Service Improvement.

5.3.1 Service Level Management

GOAL: To ensure that the levels of IT service delivery are achieved, both for existing services and new services in accordance with the agreed targets.

During the Service Design lifecycle phase, Service Level Management:
• Designs and plans the SLM process and Service Level Agreement (SLA) Structure.
• Determines the Service Level Requirements (SLR's)
• Negotiates and Agrees upon the relevant Service Level targets with customers to produce Service Level Agreements

Negotiates and agrees upon the support elements required by the internal IT groups and External Suppliers to produce Operational Level Agreements (internal) and Underpinning Contracts (external).

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

Figure 5.A – SLAs, OLAs and UCs

Negotiating and Agreeing upon the SLAs and OLAs is the responsibility of Service Level Management. Supplier Management is responsible for negotiation and agreeing upon Underpinning Contracts with external suppliers. These two processes must communicate to ensure that the Underpinning Contracts do align with and support the SLAs in place.

What are the roles of OLAs and UCs?
They are agreements with the internal IT departments and external suppliers on how they support the IT organization in meeting the Service Level Agreements with customers.

Figure 5.B – How it all fits together

The Service Catalogue

Figure 5. C bel ow demonstrates t he B usiness Service C atalogue an d Technical Service Catalogues and t he di fferent v iews they represent. S ervice Lev el Management su pports Service C atalogue M anagement i n t he cr eation o f a c ustomer facing B usiness Service Catalogue, ensuring that all current (live) services are represented here.

Figure 5.C – The Service Catalogue

Service Level Agreement Structures

There ar e a number o f ways in w hich S ervice Lev el A greements can be st ructured. The important factors to consider when choosing the SLA structure are:

- Will t he S LA al low flexibility i n t he l evels of se rvice t o be del ivered for v arious customers?
- Will the SLA structure require a lot of duplication of effort?
- Who will sign the SLAs?

Three t ypes of S LAs st ructures that ar e di scussed w ithin I TIL® ar e S ervice-based, Customer-based and Multi-level or Hierarchical SLAs.

Customer-based and Service-based SLAs

Multi-level SLAs

Figure 5.D – SLA structures

Many di fferent factors w ill need t o be c onsidered w hen d eciding which S LA st ructure i s most appropriate for an organization to use.

Typical Multi-level SLA Structure components:
1. **Corporate l evel:** All generic issues are c overed, w hich ar e t he same for t he e ntire organization.

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

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

Example: *Security r equirements of o ne or more depar tments within t he or ganization a re higher: E.g. The financial department needs higher security measures.*

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

Example: *The em ail services for a par ticular depar tment nee ds encryption a nd se cure backups.*

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

The Contents of Service Level Agreements:
- Introduction
- Service hours
- Availability targets
- Reliability
- Support arrangements

- Transaction response times
- Disaster Recovery
- Reporting requirements
- Incentives and Penalties

See t he C ontinual S ervice I mprovement Chapter f or t he asp ects o f S ervice L evel Management t hat f ocus on i mproving t he l evel of qua lity being de livered f or IT Services.

5.3.2   Capacity Management

GOAL: To ens ure the current an d f uture capacity and performance de mands of t he customer regarding IT service provision are delivered against justifiable costs.

Capacity Management is the process that manages:
- the right capacity,
- at the right location,
- at the right moment,
- for the right customer,
- against the right costs

Capacity M anagement p rovides the p redictive and o ngoing ca pacity indicators needed to align ca pacity t o de mand. I t i s about finding t he r ight bal ance between r esources and capabilities, and demand.

- Too many resources & capabilities = ↑ $$$$

- Too little resources & capabilities = ↓ performance

Figure 5.E - The Consequences of Reactive Behaviour

This gr aph r epresents t he c onsequences of r eactive be haviour i n m anaging capacity.
- Diagonal so lid l ine r epresents t he t ypical c apacity ne eds of an o rganization ov er time.
- The do tted l ine r epresents the I deal m anagement of ca pacity t o m eet t he organization's needs.
- The H orizontal l ines depicts the r eactive appr oach, w hereby $ $ ar e p ut i nto resolving capacity issues, only when it becomes an issue. This goes well until the next m ajor i ncident, and more reactive $$ are injected to try and " fix" the capacity issues, rather than addressing the issue in a proactive manner.
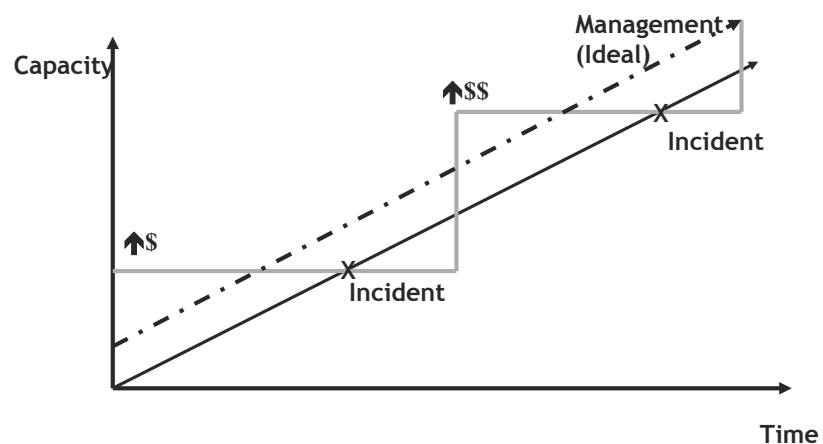
Sub-Processes of Capacity Management:

Business Capacity Management:
- Manage Capacity to meet future business requirements for IT services
- Plan and implement sufficient capacity in an appropriate timescale
- Should be included in Change Management and Project management activities

Service Capacity Management
- Focus on managing ongoing service performance as detailed in SLA or SLR
- Establish baselines and profiles of use of Services

Component Capacity Management
Identify and manage each of the components of the IT Infrastructure
- E.g. CPU, memory, disks, network bandwidth
- Evaluates NEW technology
- Load balances across resources

All 3 components collate their data and report to Service Level Management and Financial Management for IT Services.

Activities
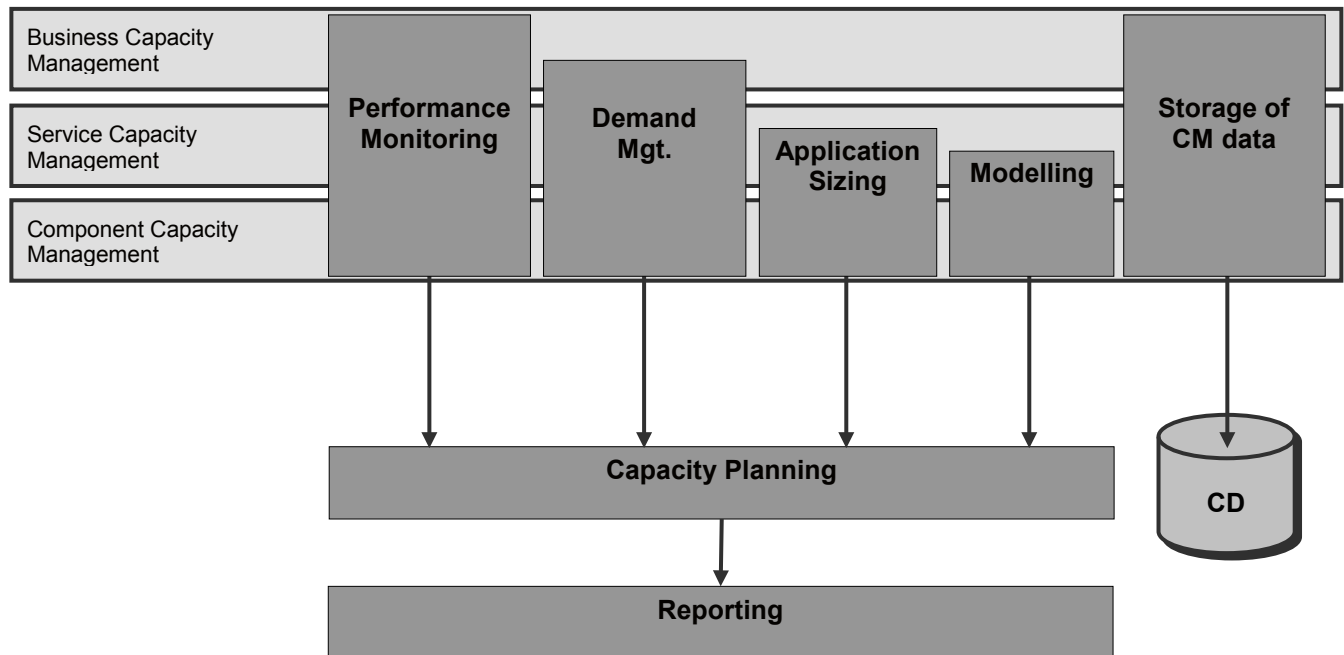
Figure 5.F – Activities of Capacity Management

Capacity Management has 6 main activities:

1. **Performance Monitoring -** Measuring, monitoring, and tuning the performance of *IT Infrastructure components.*
2. **Demand M anagement -** Short t erm r eactive i mplementation o f st rategies considered in Service Strategy to manage current demand
3. **Application Sizing -** Determining the hardware or network capacity to support new or modified applications and the predicted workload.
4. *Modelling* - Used t o f orecast t he be haviour o f t he i nfrastructure *under ce rtain conditions.*
5. Storage of Capacity Management Data
6. Capacity Planning
7. Reporting

Roles and Responsibilities for Capacity Management:

Capacity Manager:
<u>Role</u>
To ensure adequate performance and capacity for all IT services.

<u>Responsibilities:</u>
Capacity Plan (development and management)
Oversee Performance and Capacity monitoring & alerting
Report provision and advice

<u>Skills:</u>
Strategic business awareness, technical, analytical, consultancy

Capacity M anagement i s critical f or e nsuring ef fective and efficient c apacity an d performance I T S ervices and I T co mponents in l ine w ith busi ness requirements and overall IT st rategic objectives. It is essential that the Capacity Manager ensu res that the process utilizes information from an d pr ovides information t o all phase s of t he S ervice Lifecycle.

INPUTS	SUB-PROCESS	OUTPUTS
·Technology ·SLA, SLR, SC ·Business Plan and strategy ·IS/IT plans ·Business requirements ·Operational Schedules ·Deployment and development plans ·FSC ·Incidents and problems ·SLA breaches ·Service Reviews ·Financial Plans ·Budgets	**Business Capacity Management** ·Trend, Forecast, Model, Prototype, Size and document future business requirements **Service Capacity Management** ·Monitor, Analyse, Tune and report on Service Performance, establish baselines and profiles of use of services, manage demand for service. **Component Capacity Management** ·Monitor, Analyse, Run and report on Component Performance, establish baselines and profiles of use of components	·Capacity Plan ·CDB ·Baselines and profiles ·Thresholds and alarms ·Capacity Reports ·SLA and SLR recommendations ·Costing and Charging recommendations ·Proactive changes and service improvements ·Revised operational schedule ·Effectiveness reviews ·Audit reports

Figure 5.G – Capacity Management relationships with the rest of ITIL®

5.3.3 Availability Management

GOAL: To optimize the capability of the IT infrastructure and supporting the organization to deliver a co st effective and su stained level of availability that enables the business to satisfy its objectives.

Other Availability objectives are:
* Reduction in the frequency and duration of Availability related incidents.
* Maintain a forward looking Availability plan.

30 min outage
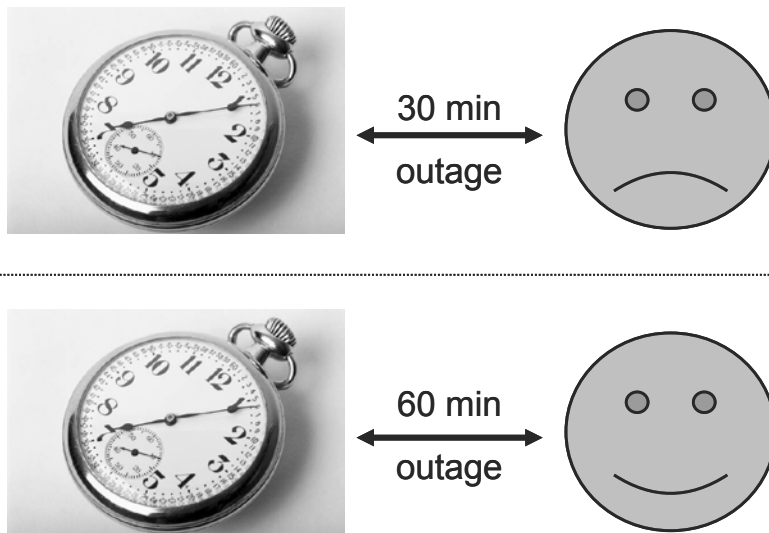
60 min outage

Figure 5.H – The Perception of Availability

Question?
Why c ould us ers be ha ppy w ith a 6 0 m inute out age a nd unha ppy with 3 0 m inute outage?

A1: 30min outage during peak time, overtime being paid to staff, urgent report required.
A2: 60min outage on weekend, holiday, off peak, when service not required.
A3: 30min outage on critical IT Service, 60min outage on non-critical IT Service.
A4: 30mins unplanned outage, 60min planned outage (e.g. maintenance).

For a consumer/user of an I T Service, its Availability and R eliability can directly influence both the perception and satisfaction of the overall IT Service provision.

Proactive and Reactive Elements of Availability Management:

Proactive activities:
Involves the proactive planning, design and improvement of availability. These activities are principally involved within design and planning roles.
(Service Design Phase)

Reactive activities:
Involves the monitoring, measuring, analysis and management of all events, incidents and problems regarding availability.

(Service Operation Phase)

Terminology	Explanation
Availability:	The ability of an IT Service or component to perform its *required function* at a stated instant or over a *stated period* of time.
Security:	Information Security Management *determines requirements*, Availability Management *implements measures*
Reliability:	*Freedom* from operational failure.
Resilience:	The ability to **withstand failure.**
Maintainability: (internal)	The ability of an IT component to be retained in or restored to, an operational state. Based on skills, knowledge, technology, backups, availability of IT staff.
Serviceability: (external)	The contractual obligation / arrangements made with 3rd party external suppliers. Measured by Availability, Reliability and Maintainability of IT Service and components under control of the external suppliers. Managed by Supplier Management through Underpinning Contracts.
Vital Business Function (VBF):	The **business critical elements** of the business process supported by an IT Service.

Activities
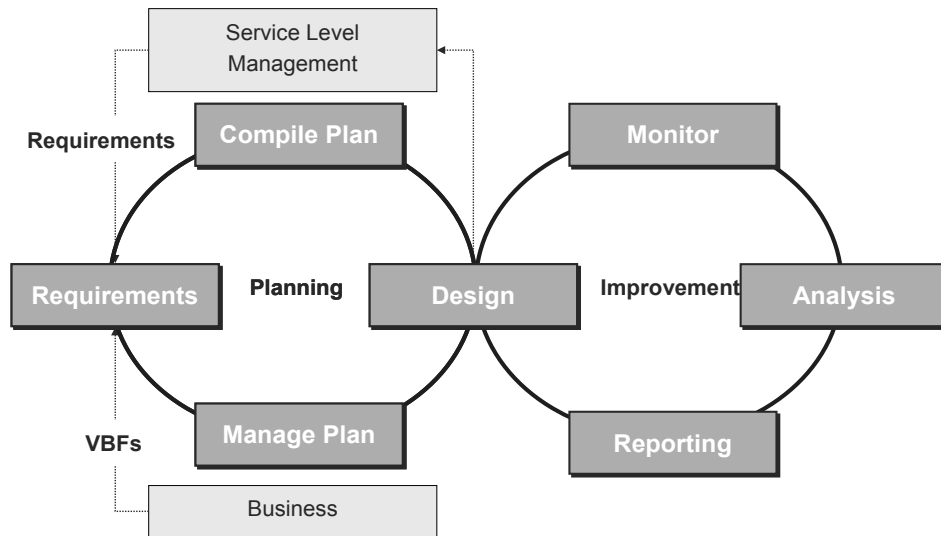
Figure 5.I – Availability Activities

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

Availability Management and Incident Management:

An aim of Availability Management is to ensure the duration and impact from Incidents impacting IT Services are minimised, to enable business operations to resume as quickly as possible.

The expanded Incident lifecycle enables the total IT Service downtime for any given Incident to be broken down and mapped against the major stages that all Incidents go through.
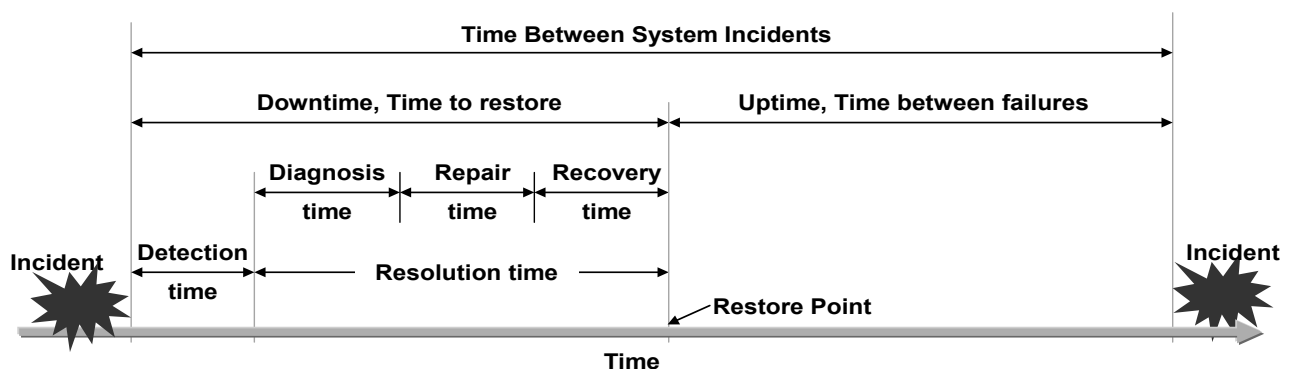
Figure 5.J – The Expanded Incident Lifecycle

Lifecycle of an Incident. (Availability Management Metrics)

Mean time between Failures (MTBF) or *uptime*
- Average time between the recovery from one incident and the occurrence of the next incident, relates to the reliability of the service

Mean time to Restore Service (MTRS) or *downtime*
- Average time taken to restore a CI or IT service after a failure.
- Measured from when CI or IT service fails until it is fully restored and delivering its normal functionality.

Mean time between System Incidents (MTBSI):
- Average time between the occurrence of two consecutive incidents.
- Sum of the MTRS and MTBF.

Relationships:
- high ratio of MTBF/MTBSI indicates there are many minor faults
- low ratio of MTBF/MTBSI indicates there are few major faults

Detection Time: Time for the service provider to be **informed** of the fault. **(Reported)**

Diagnosis Time: Time for the service provider to respond after **diagnosis** completed

Repair Time:
Time the service provider restores the components that caused the fault.
Calculated from **diagnosis** to **recovery** time

Restoration Time: (MTRS)
The **agreed** level of service is restored to the user.
Calculated from **detection** to **restore point.**

Restore Point:
The point where the agreed level of service has been restored

Roles and Responsibilities

Availability Manager:

<u>Role:</u>
To ensure adequate availability of all IT services.

<u>Responsibilities:</u>
Availability Plan (development and management)
Availability monitoring & alerting
Report provision and advice

<u>Skills:</u>
Awareness of how IT supports the business,
Technical, analytical, consultancy,
Seeks continuous improvement

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

5.3.4 IT Service Continuity Management

GOAL: To su pport t he ov erall B usiness Continuity M anagement by ensu ring t hat t he required I T i nfrastructure an d t he I T s ervice pr ovision ca n be r ecovered w ithin r equired and agreed business time scales. ** Often referred to as Disaster Recovery planning. **

Terminology	*Explanation*
Disaster:	NOT p art o f *daily o perational a ctivities* and r equires a *separate system*. (Not necessarily a f lood, fire et c. may be due to a bl ackout or power pr oblem a nd the S LAs are i n danger of being breached).
Business Continuity Management: (BCM)	Strategies and ac tions to t ake pl ace t o co ntinue B usiness Processes in t he ca se of a di saster. It i s essential t hat t he ITSCM st rategy i s integrated i nto a nd a su bset o f t he B CM strategy.
Business Impact Analysis: (BIA)	Quantifies the i mpact loss of I T se rvice would hav e on t he business.
Risk Assessment:	Evaluate *Assets*, *threats* and *vulnerabilities*.
Scope:	The sco pe o f I T S ervice C ontinuity M anagement co nsiders all i dentified cr itical b usiness processes and I T se rvice(s) that u nderpin t hem. This may i nclude har dware, so ftware, essential services and utilities, critical paper r ecords, courier services, voice se rvices & phy sical l ocation ar eas e.g. offices, data centres etc.
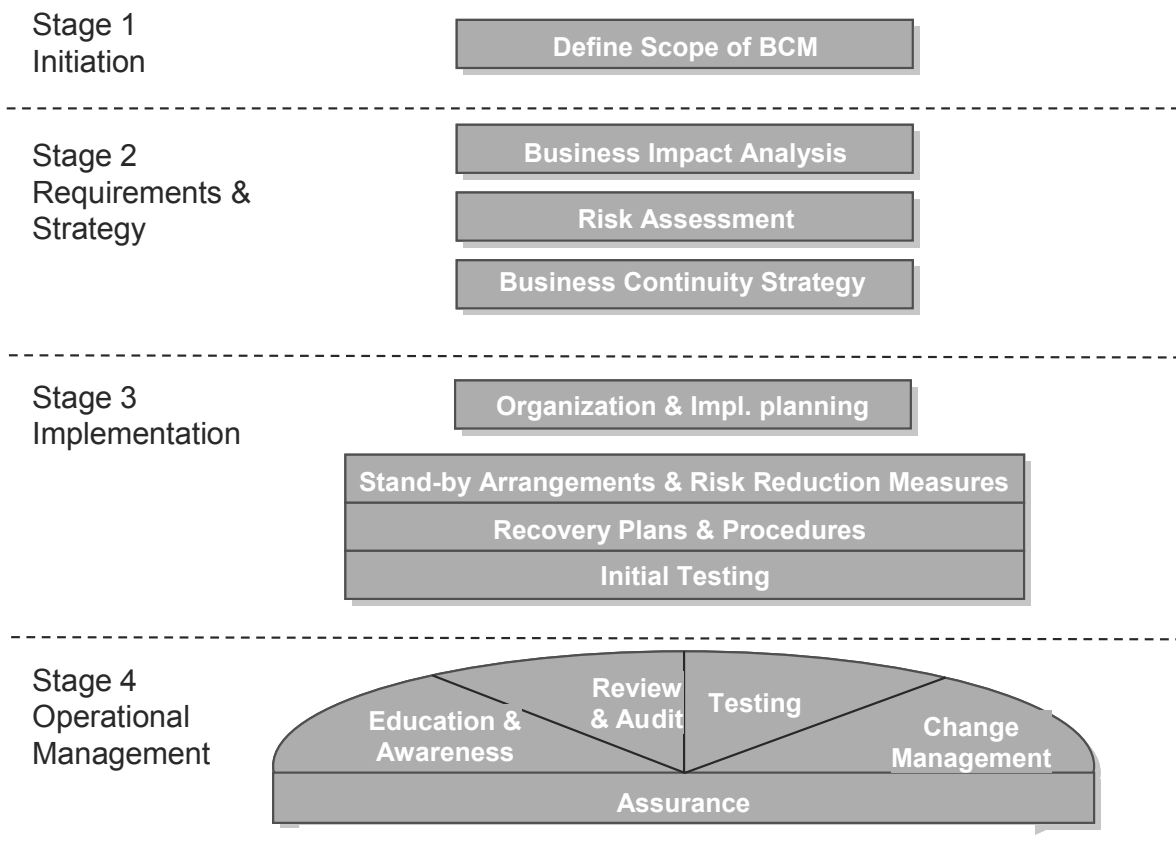
Figure 5.K – Activities of IT Service Continuity Management

Key Activities of IT Service Continuity Management:

Performing a Business Impact Analysis (BIA) identifies:
- Critical business processes & Vital Business Functions
- Potential damage or loss caused by disruption
- Possible escalations caused by damage or loss
- Necessary resources required to enable continuity of critical business processes
- Time constraints for minimum recovery of facilities and services
- Time constraints for complete recovery of facilities and services

Risk Assessment:
- Gather information on assets (IT infrastructure components),
- Threats from both Internal & external sources (the likelihood of occurring)
- Vulnerabilities (the extent of impact or effect on organization)

Developing Countermeasures (Recovery and Risk Reduction Measures):

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

Operational Management:
- Education & awareness
- Training
- Reviews
- Ongoing testing
  - At least annually
  - Following major changes
- Audits of r ecovery pr ocedures, r isk-reduction m easures and for co mpliance t o procedures.

Roles and Responsibilities:

Role	Responsibilities and Skills
Board	Crisis Management Corporate/Business decisions External affairs
Senior Management	Co-ordination Direction and arbitration Resource authorization
Management	Invocation of continuity or recovery Team Leadership Site Management Liaison & Reporting
Supervisors and Staff	Task execution Team membership Team and Site liaison

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

Skill requirements for ITSCM Manager and staff:

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

5.3.5   Information Security Management

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

Information S ecurity M anagement e nsures t hat t he ***confidentiality***, ***integrity*** and ***availability*** of a n or ganization's assets, i nformation, data a nd I T se rvices is maintained. Information Security Management must consider the following four perspectives:

- Organizational
- Procedural
- Physical
- Technical

Terminology	Explanation
Confidentiality:	Protecting information against unauthorized access and use. Examples: *Passwords, swipe cards, firewalls*
Integrity:	Accuracy, completeness and timeliness of the information. Examples: *Rollback mechanisms, test procedures, audits.*
Availability:	The i nformation s hould be acce ssible at a ny ag reed t ime. This depends on t he continuity pr ovided by t he i nformation processing systems. Examples: *UPS, resilient systems, Service desk hours*
Security Baseline:	The security level adopted by the IT organization for its own security and f rom the point o f view of good 'due di ligence'. Possible to have multiple baselines Examples: *Security access based employee rank/title*
Security Incident:	Any i ncident t hat m ay i nterfere w ith ach ieving t he S LA security requirements; materialisation of a threat Examples: *Security Breach or potential weakness*
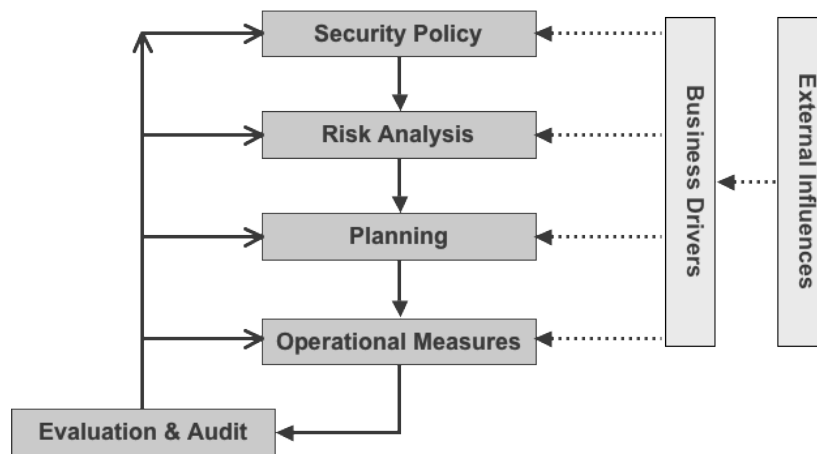
Figure 5.L – Factors influencing Information Security Management

Information S ecurity M anagement (ISM) needs to b e co nsidered w ithin t he ov erall corporate g overnance f ramework. T his provides the **_strategic_** direction f or security activities and ensu res obj ectives are ach ieved. I t f urther ensu res that t he i nformation security risks are appropriately managed and that the enterprise information resources are used responsibly.

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

Activities
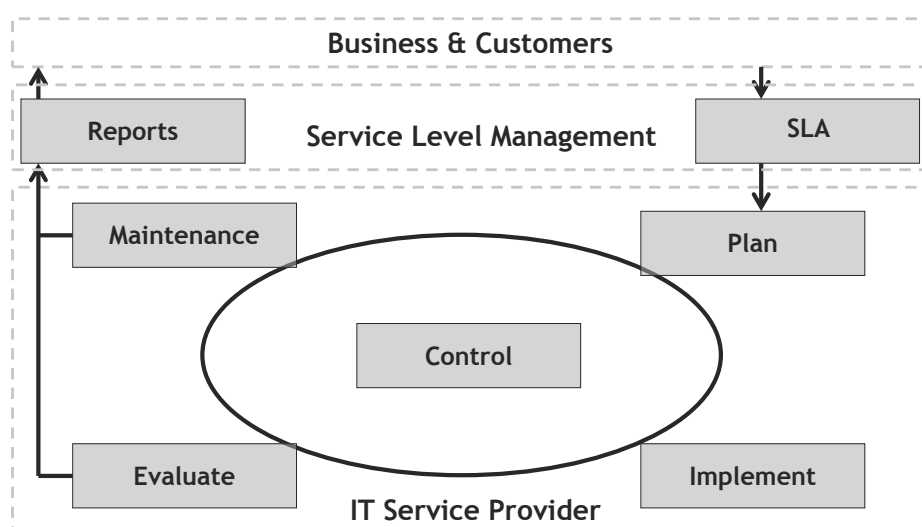
Figure 5.M – Activities of Information Security Management

Control:

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

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

Roles and Responsibilities

Information Security Manager

Responsibilities:

- Manage entire security process,
- Consult with senior management

Skills:

- Strategic Sense of PR, tactical.

Security Officer

Responsibilities:

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

Skills:

- Analytical, eye for detail, consultancy

Perspectives

	Organizational	Procedural	Technical	Physical
Prevention Reduction				
Detection				
Repression				
Correction				
Evaluation				

Measures

Figure 5.N – Activities of Information Security Management

The I nformation S ecurity M easure M atrix i s a us eful t ool in pe rforming a ga p analysis:
- Ensures there is a balance in measures
- Avoids a concentration of measures in either a ce rtain perspective (e.g. technical) or of a certain measure (e.g. detection).

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

5.3.6 Supplier Management

GOAL: 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.

Terminology	*Explanation*
Supplier service improvement plans: (SSIP)	Used to record all improvement actions and plans agreed between suppliers and service providers.
Supplier Survey Reports:	Feedback gathered from all individuals that deal directly with suppliers throughout their day to day role. Results are collated and reviewed by Supplier Management, to ensure consistency in quality of service provided by suppliers in all areas.
Supplier & Contract performance reports:	Used as input for the Supplier & Contract review meetings to manage the quality of the service provided by suppliers and partners. This should include information on shared risk, when appropriate.
Types of Supplier Arrangements:	
Co-sourcing:	An informal combination of insourcing and outsourcing, using a number of outsourcing organizations working together to co-source key elements within the lifecycle.
Partnership or multi-sourcing:	Formal arrangements between two or more organizations to work together to design, develop transition, maintain, operate, and/or support IT service(s). The focus here tends to be on strategic partnerships that leverage critical expertise or market opportunities.
Business Process Outsourcing:	Formal arrangements where an external organization provides and manages the other organization's entire business process (es) or functions(s) in a low cost location. Common examples are accounting, payroll and call centre operations.

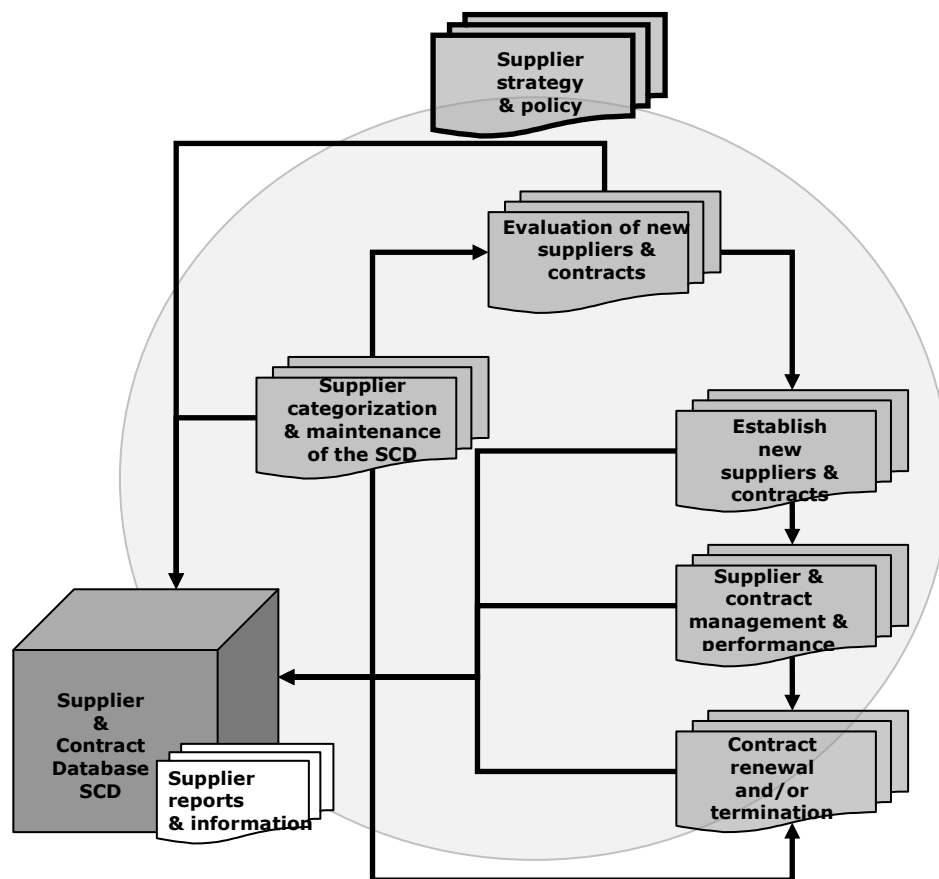|	
Knowledge Process Outsourcing:	This is a **new enhancement** of Business Process Outsourcing, where ex ternal or ganizations provide do main bas ed processes and business expertise r ather t han j ust pr ocess expertise a nd requires advanced anal ytical and sp ecialized ski lls f rom t he outsourcing organization.
Application Service Provision:	Where ex ternal organizations provide sh ared co mputer b ased services to cu stomer or ganizations over a net work. T he complexities and costs of such shared software can be reduced and provided to organizations that could otherwise not justify the investment.

Supplier and Contact Database (SCD):

Figure 5.O – The Supplier & Contract Database

All Supplier Management process activity should be driven by supplier strategy and policy. In order to achieve consistency and effectiveness in the implementation of the policy, a Supplier and Contract Database (SCD) should be established.

Ideally t he S CD sh ould form an i ntegrated el ement of a co mprehensive CMS(Configuration M anagement S ystem) or S KMS(Service K nowledge M anagement System), r ecording al l su pplier an d co ntract det ails, t ogether w ith t he t ypes of s ervice, products etc provided by each supplier, and all the other information and relationships with other associated CIs(Configuration Items).
This will also so contribute to the information held in the Service Portfolio and Catalogue.

Relationships with other Lifecycle Phases:

The information within the SCD will provide a complete set of reference information for all Supplier M anagement pr ocedures and ac tivities needed acr oss the S ervice Li fecycle. Such activities include:

Lifecycle Phase	Activities
Service Design	• Supplier categorization and maintenance of the SCD • Evaluation and set-up of new suppliers and contracts
Service Design	• Assessing the transition to new suppliers • Establishing new suppliers
Service Operation	• Supplier and Contract Management and performance • Contract renewal and termination
Continual Service Improvement	• Identifying improvement actions involving suppliers. • Collating measurements gather on supplier arrangements.

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

5.3.7 Service Catalogue Management

GOAL: To ensure that a Service Catalogue is produced, maintained and contains accurate information on all operational services and those ready for deployment.

The Service Catalogue has two aspects:
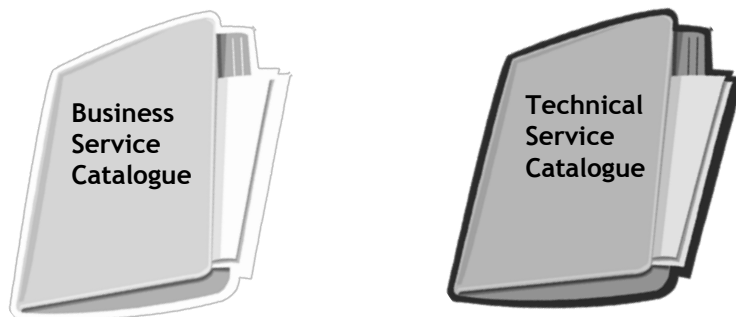
Business Service Catalogue: contains details of all the IT service delivered to the customer, together with relationships to the business units and the business process that rely on the IT services. This is the customer view of the Service Catalogue.

Technical Service Catalogue: contains details of all the IT service delivered to the customer, together with relationships to the supporting services, shared services, components and Configuration Items necessary to support the provision of the service to the business. This should underpin the Business Service Catalogue and *not form part of the customer view.*

5.3.8 Implementation

This section considers the task of implementing the Service Design processes and covers issues such as:

- Where do we start?
- How do we improve?
- How do we know we are making progress?

The activities of implementing and improving Service Design need to be focused on the needs and requirements of the customer and the business. These activities should be prioritized by:
- Business needs and business impacts
- Risks to the services and processes.
The activities will be dictated by the requirements documented in the Service Level Requirements and the Service Level Agreements.

Business Impact Analysis

The BIA is an ongoing source of valuable input when trying to establish business needs, impacts and risks. It is an essential tool used by the overall Business Continuity process and will dictate the strategy for risk reduction and disaster recovery. The BIA will show which parts of the organization will be effected by a major incident and what effect that will have on the company as a whole. This in turn identifies the most critical business functions on which the company's survival depends. In addition, data from the BIA can provide valuable input in to a number of other areas as well and enables a greater understanding of the service that would have otherwise been available.

The BIA can be divided in to two areas:

- Business Management; which has to investigate the impact of the loss of a business process or a business function. This would also include the knowledge of manual workarounds and the associated costs.
- Service Management; it is essential to break down the effects of service loss to the business. This element of the BIA shows the impact of service disruption to the business. The services can be managed and influenced by Service Management. Other aspects also covered in 'Business BIA' can not be influenced by Service Management.

As part of the design phase of a new or changed service, a BIA should be conducted to help define the business continuity strategy and to enable a greater understanding about the function and importance of the service. This will enable the organization to define:

- Which are the critical services, what constitutes a major incident on these services, and the subsequent impact and disruption caused to the business – important in deciding when and how to implement changes
- Acceptable levels and times of service outage levels – also important in the consideration of change and implementation schedules
- Critical business and service periods – important periods to avoid
- Cost of loss of service – important for Financial Management
- Potential security implications of a loss of service – important consideration in the management of risk.

Service Level Requirements (SLR's)

SLR's for all services will be identified and the ability to deliver against these requirements assessed and finally agreed in a formal Service Level Agreement. For new services, the requirements must be identified at the beginning of the development process, not after completion. Building a service with the SLR's leading the way is an essential factor from a Service Design perspective.

Risks to the Service and Processes

When implementing the Service Design phase and ITSM processes, business as usual practices must not be adversely affected. This aspect must be

considered during the production and selection of the preferred solution to ensure that disruption to operational services is minimized. The assessment of risk should then be considered in detail during the Service Transition phase activities as part of the implementation process.

Implementing Service Design

The process, policy and architecture for the design of services outlined in this publication will need to be documented and utilized to ensure the appropriate innovative IT services can be designed and implemented to meet current and future agreed business requirements.

The question often asked is 'which process do I implement first?' The most correct answer is all of them, as the true value of implementing all of the Service Management processes is far greater than the sum of the individual processes. All of the processes are interrelated, and in some cases are totally dependent on others. What is ultimately required is a single, integrated set of processes, providing management control of a set of IT services throughout their entire lifecycle.

However, in reality it is unlikely that organizations can do everything at once. In this situation it is recommended that the areas of greatest need are addressed first. A detailed assessment needs to be undertaken to ascertain the strengths and weaknesses of IT service provision. This should be undertaken by performing customer satisfaction surveys, talking to customers, talking to IT staff and analyzing the processes in action. From this assessment, short to medium and long term strategies can be developed.

It may be that 'quick wins' need to be implemented in the short term to improve the current situation, but these improved processes may have to be discarded or amended as part of the medium to long term strategies. I 'quick wins' are implemented, it is important that they are not done at the expense of the long-term objectives, so these must be considered at all times. However, every organization will have to start somewhere, and the starting point will be wherever the organization is now in terms of IT Service Management maturity.

Implementation priorities should be set against the goals of a Service Improvement Plan (SIP). Throughout the implementation process, key players must be involved in the decision making process. There can be a tendency, when analyzing the areas of greatest need, to go straight for tools to improve the situation. Workshops or focus groups will be beneficial in understanding the requirements and the most suitable process for implementation that will include people, processes, products and partners.

Step one is to establish a formal process, method of implementation and improvement of Service Design, with the appropriate governance in place. This formal process should be based around the six stage process of the Continual Service Improvement cycle (found in section 8.2).

It is important that when implementing or improving processes a structured Project Management method is used. The improvement process can be summarized as understanding the vision by ascertaining the high-level business objectives. The 'vision-setting' should set and align business and IT strategies and assess the current situation to identify strengths that can be built on weaknesses that need to be addressed.

The following are key elements for successful alignment of IT with business objectives:

- Vision and leadership is setting and maintaining strategic direction, clear goals, and measurement of goal realization in terms of strategic direction
- Acceptance of innovation and new ways of working
- Thorough understanding of the business, its stakeholders and its environment
- IT staff understanding the needs of the business
- The business understanding the potential
- Informational and communication available and accessible to everyone who needs it
- Separately allocated time to familiarize with the material
- Continuous tracking of technologies to identify opportunities for the business.

The implementation/improvement cycle is useful in checking the alignment between the business and IT (see section 8.2).

Measurement of Service Design

The success of the Service Design phase and the success of the improvement to the processes around Service Design must be measured; the data must be analyzed and reported on. Where the design or process does not meet the requirements of the business as a whole, changes to the process may be required and the results of the changes must also be measured. Continuous measurement, analysis and reporting are mandatory requirements for both the Service Design process and the ITSM processes.

There are measurement methods available that enable the analysis of service improvement. The Balanced Scorecard is a method developed by Robert Kaplan and David Norton as a concept for measuring company activities in terms or its vision and strategies. It gives a comprehensive view of the performance of the business. The system forces managers to focus on the important performance metrics that drive success. It balances a financial perspective with customer, internal process and learning and growth perspectives.
More information can be found on the Balanced Scorecard at www.scorecardsupport.com

Six Sigma is a methodology developed by Bill Smith at Motorola Inc. in 1986, and was originally designed to manage process variations that cause defects, defined as unacceptable deviation from the mean or target, and to

systematically work towards managing variation to eliminate those defects. Six Sigma has now grown beyond defect control and is often used to measure improvement in IT process execution. More information can be found on Six Sigma at http://www.isixsigma.com

Six Sigma (**DMADV**) is an improvement system used to develop new processes at Six Sigma quality levels and is defined as:

Define – formally define the goals of the design activity that are consistent with customer demands and organization strategy.
Measure – identify Critical Success Factors, capabilities, process capability and risk assessment
Analyze – develop and design alternatives, create high level design and evaluate capability to select the best design
Design – develop detailed design, optimize design and plan for design verification
Verify – set up pilot runs, implement production process and hand over to process owners.

This process is an improvement system for existing processes falling below specification and looking for incremental improvement.
Prerequisites for Success

There are several prerequisites needed for the Service Design phase and the successful introduction of new or revised processes. Often these prerequisites for success are elements of one process required by another. For example, fully completed and up-to-date Business Service Catalogue and Technical Service Catalogue are required before Service Level Management can design the SLA and supporting agreement structure, and before SLM can set up and agree the SLA's. Problem Management will depend on a mature Incident Management process. The prerequisites for success can be much wider than just ITSM process interdependencies. For example, the design of availability and capacity for a new service can not be achieved without details of the business plan for the utilization of the new service. The design of service will be impossible without the Service Portfolio and Service Transition pack. There are more examples of these prerequisites for success that need to be considered and planned before high process maturity levels can be achieved. Low maturity in one process will mean that high levels of maturity will not be achievable in other processes.

5.3.9 Service Design Summary

Good Service Design means it is possible to deliver quality, cost effective services and to ensure that the business requirements are being met. It also delivers:
- Improved Quality of Service
- Improved Consistency of Service
- Improved Service Alignments
- Standards and Conventions to be followed

- More Effective Service Performance

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

Service Transition

Service Design

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
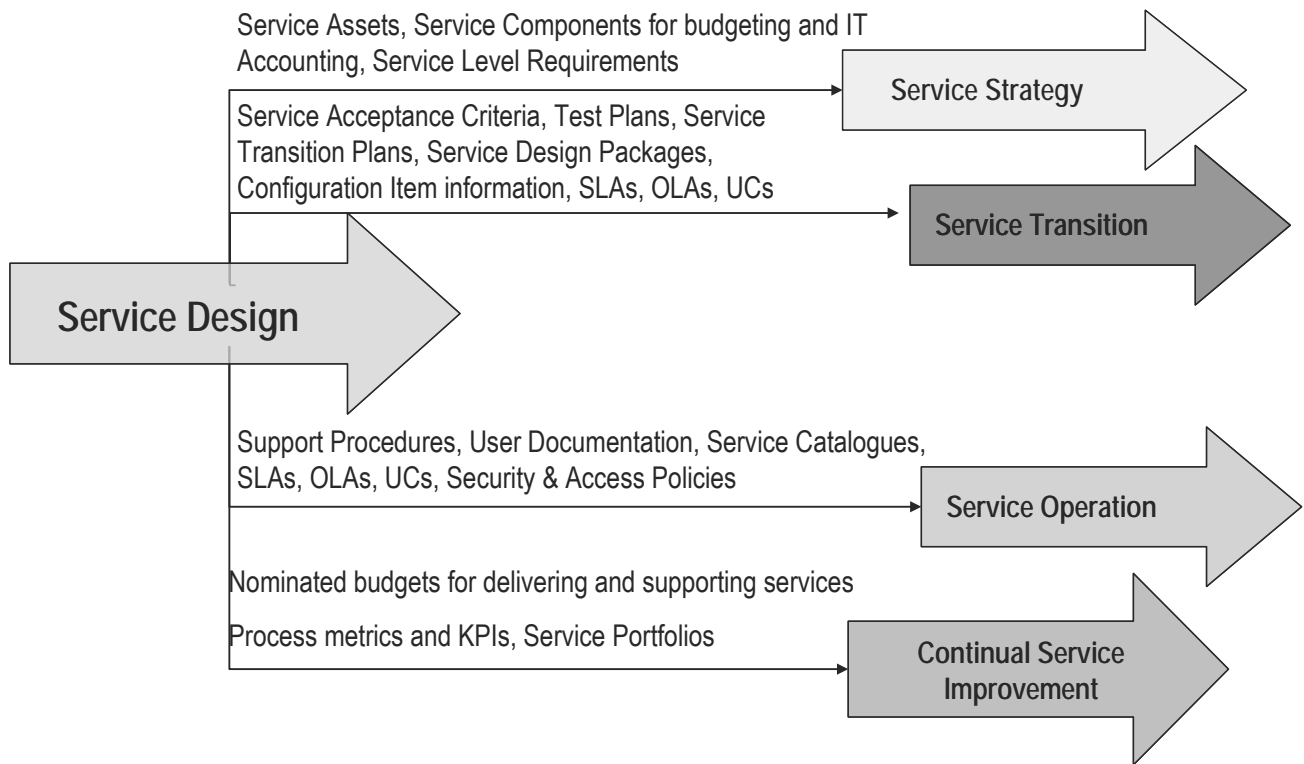
Continual Service Improvement

Figure 5.M – Some outputs to other lifecycle phases.

5.4 Service Design Scenario

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

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

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

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

Service Catalogue Management

- Business Service Catalogue – will describe HYPE service as business understands it, including levels of service
- Technical S ervices Catalogue – will cl early list t echnical an d su pporting se rvice information, e.g. ISP bandwidth, server requirements etc…

ITSCM

- The busi ness has decided t hat t his is a B CP, so st andby a rrangements are negotiated with business ($$)
- Decided t hat t he t elephone l ine an d/or e mail will be possi ble r ecovery m easures until service is restored – included in ITSCM plan
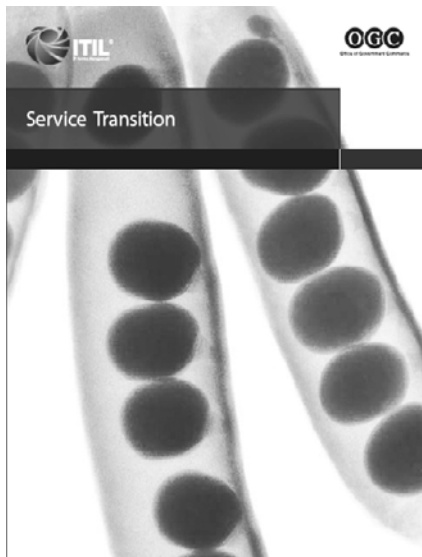
Supplier Management

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

The Service Design processes will ensure that HYPE meets the customer needs and can continue to be supported during the Service Operation phase.

6 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 an d t echnical er rors not found during t his phase will result in significantly higher impact levels to the busi ness and/or IT infrastructure and w ill usually cost much more to fix once the Service is in operation.

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

6.1 Objectives

The d evelopment and i mprovement o f c apabilities for t ransitioning new and ch anged 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.

6.2   Major Concepts

Components, Tools and Databases

The ex ecution of any I T S ervice M anagement pr ocess usually r equires access t o, or storage o f, r elevant sets of d ata and i nformation. As the Service T ransition ph ase incorporates the processes of Knowledge Management and Service Asset & Configuration Management, w hich a re he avily f ocussed on t he management of dat a, i nformation an d knowledge, the components, tools and databases needed to do this are discussed during this chapter.
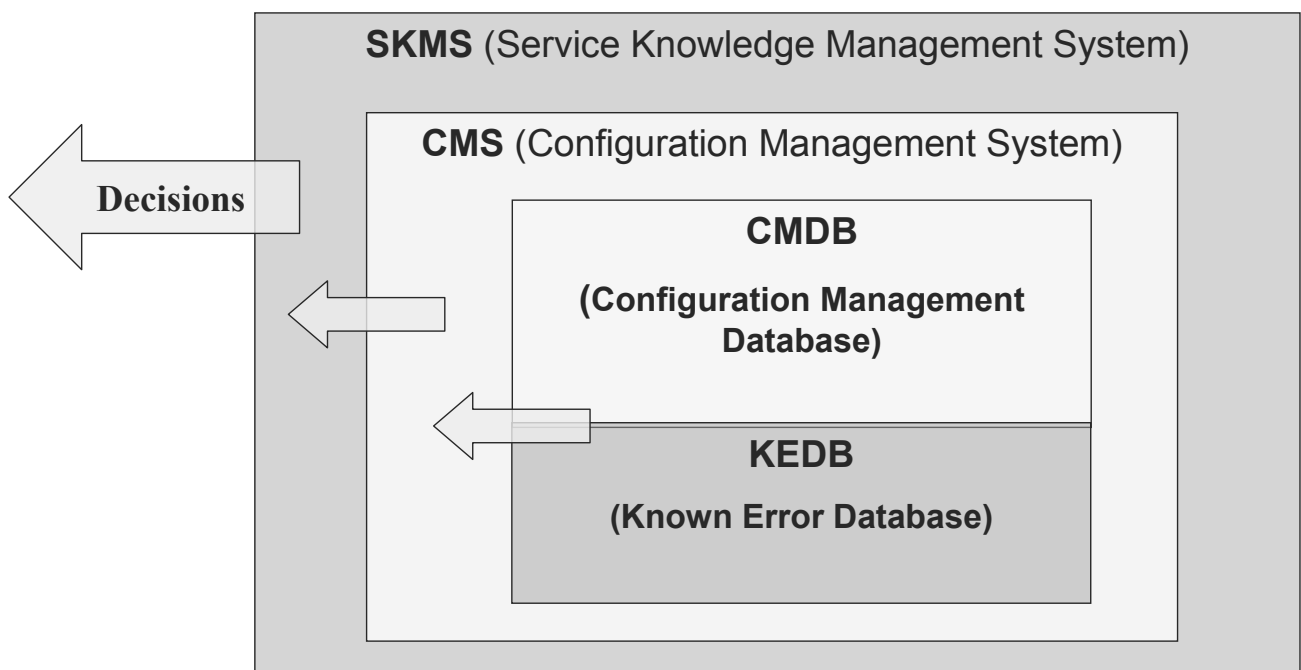

Figure 6.A – Components making up the Service Knowledge Management System

SKMS: Service Knowledge Management System (SKMS):
The co mplete s et of t ools and da tabases t hat ar e used t o m anage k nowledge an d information. The SKMS includes the Configuration Management System as well as other tools and da tabases. The S KMS st ores, m anages, up dates and p resents all i nformation that a n I T s ervice pr ovider needs to m anage t he full l ifecycle of i ts services. T he m ain purpose of the SKMS is to provide quality information so that informed decisions can be made by the IT service provider.

CMS: Configuration Management System:

A se t of t ools and d atabases that are us ed t o manage an I T se rvice pr ovider's configuration data. The CMS also includes information about incidents, problems, known er rors, ch anges and r eleases; a nd m ay co ntain d ata a bout e mployees, suppliers' locations, business units, customers and users. The CMS is maintained by S ervice A sset & C onfiguration M anagement an d i s used by al l I T S ervice Management processes. Two major components are the:

- **CMDB: Configuration Management Database**

- **KEDB: Known Error Database.** This database is created by Problem Management and used by Incident and Problem Management.

6.3   Service Transition Processes

6.3.1   Knowledge Management

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

The pr imary pur pose i s to i mprove e fficiency by r educing t he ne ed t o r ediscover knowledge. T his requires accessible, q uality and r elevant d ata and i nformation t o be available to staff.

Benefits t hat a su ccessful K nowledge M anagement S ystem would d eliver t o t he business and IT organization:
  •   We can stop having to continually reinvent the wheel
  •   More efficient use of resources (including people)
  •   Enables the organization to continually mature and develop.

Challenges   you   would s ee i n i mplementing a nd op erating a   K nowledge Management System:
  •   Getting staff to use the systems.
  •   Having the extra time required to record relevant information and knowledge after actions are made.
  •   Managing i nformation and k nowledge t hat i s no l onger co rrect or relevant f or t he organization.
  •   Designing a system that can scale well as an organization grows.

One of the more difficult components of Knowledge Management is ensuring that we do more than simply capture discrete facts about various elements of the organization and IT infrastructure. What t his requires is an under standing o f t he di fferent co mponents and processes required to develop and mature knowledge and wisdom.
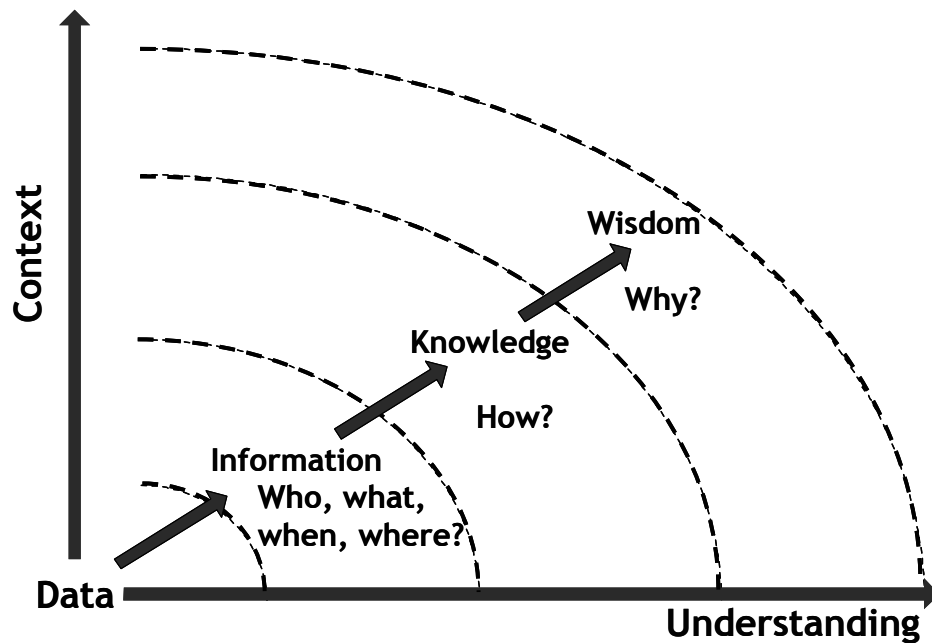
Figure 6.B – Moving from data to wisdom

Data:

Data i s a se t o f di screte facts. M ost organizations capture si gnificant amounts of d ata every day.

Information:

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

Knowledge:

Knowledge i s composed o f t he ex periences, i deas, i nsights and j udgments from individuals. This usually requires the analysis of information, and is applied in such a way to facilitate decision making.

Wisdom:

Gives the ultimate discernment of the material and hav ing the application and contextual awareness to pr ovide a st rong common se nse j udgment. The us e o f w isdom ul timately enables an organization to direct its strategy and growth in competitive market spaces.

We can us e t ools and d atabases to ca pture D ata, I nformation an d K nowledge, but Wisdom cannot be captured this way, as Wisdom is a concept relating to abilities to use knowledge to make correct judgments and decisions.

6.3.2   Service Asset and Configuration Management

GOAL: To su pport t he ag reed I T se rvice pr ovision by managing, st oring and pr oviding information about Configuration Items (CI's) and Service Assets throughout their life cycle.

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

Terminology	*Explanations*
Configuration Item (CI):	***ANY*** component that supports an IT service (except people). *Example: IT components or associated items such as Request for Changes, Incident Records, Service Level Agreements.*
Attribute:	***Specific*** information about CI's. *Example: Size of RAM, hard drive, bandwidth*
CI Level:	Recording and reporting of CI's at the level that the ***business requires*** without being overly complex. It's a trade-off balancing the value that the information will provide versus the effort and cost to manage the information over time.
Status Accounting:	Reporting of all ***current and historical*** data about each CI throughout its lifecycle. *Example: Status = Under Development, being tested, live, withdrawn etc*
Configuration Baseline:	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)

The Configuration Management Database (CDMB):
The C MDB i s a se t of o ne or m ore co nnected da tabases and i nformation so urces that provide a l ogical model of the IT infrastructure. It captures Configuration Items (CIs) and the r elationships that exist bet ween t hem. Figure 6. B dem onstrates the el ements of a CMDB.
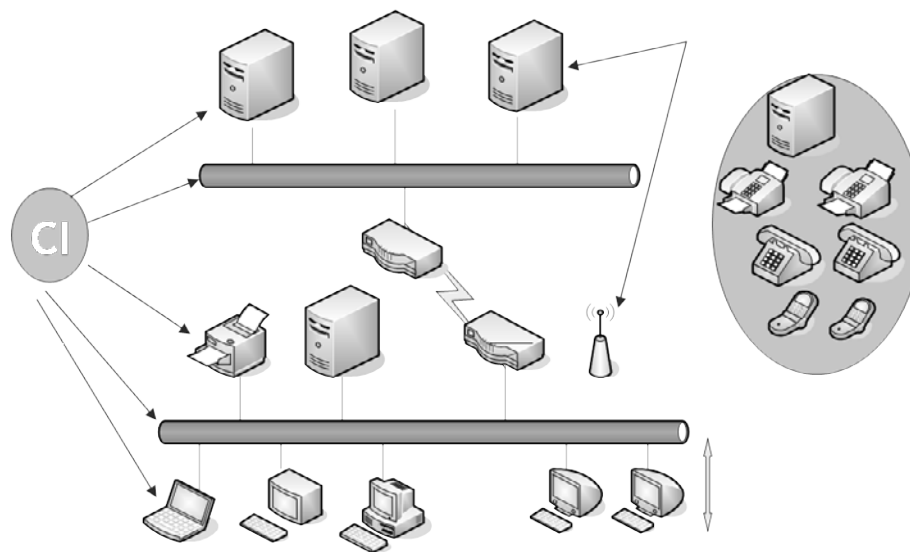
Figure 6.B – The Configuration Management Database (CMDB)

As shown, i t i s important t o de termine what l evel t o w hich the CM DB w ill r ecord information about the IT infrastructure and to decide what is not covered within the scope of t he C MDB. C omponents out o f sco pe are t hose t ypically not un der t he co ntrol of Change Management (e.g. telecommunication equipment)

Activities

Figure 6.C – Configuration Management Activities

Notice how MANAGEMENT & PLANNING are the central activities. Good, sound Service Asset & C onfiguration M anagement r equires thorough pl anning for t he op eration o f t he process to work.

Planning:
- Defining the strategy, policy, scope, objectives, processes and procedures.
- Roles and responsibilities of involved staff and stakeholders.
- Location of storage areas and libraries used to hold hardware, software and documentation.
- CMDB Design.
- CI naming conventions.
- Housekeeping including license management and archiving of CI's.

Identification:

The selection, identification, labelling 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
- Documentation

Control:

Ensures that only authorized and identifiable CIs are recorded from receipt to disposal in order to protect the integrity of the CMDB. Control occurs anytime the CMDB is altered, including:
- Registration of all new CIs and versions
- Update of CI records and licence control
- Updates in connection with RFCs and Change Management
- Update the CMDB after periodic checking of physical items

Status Accounting:

The reporting of all current and historical data concerned with each CI throughout its lifecycle. Provides information on:
- Configuration baselines
- Latest software item versions
- The person responsible for status change
- CI change/incident/problem history

Verification and Audit:

Reviews and audits verify the existence of CIs, checking that they are correctly recorded in the CMDB and that there is conformity between the documented baselines and the actual environment to which they refer.

Configuration Audits should occur at the following times:
- Before and after major changes to the IT infrastructure
- Following recovery from disaster
- In response to the detection of an unauthorized CI
- At regular intervals

The benefits of the CMDB (not necessarily one physical database):
- One tool and not several tools -> reduce costs
- Consistent and visible information about the IT infrastructure available to all staff.
- One team and not several support teams -> reduce costs, improve consistency in CI management
- On stop shop for Configuration queries
- The data about CIs and methods of controlling CIs is consolidated -> reduces auditing effort.
- Opens opportunities for consolidation in CIs to support services.

Roles and Responsibilities

Service Asset Management:

The management of service assets across the whole lifecycle including:
- Full lifecycle management of IT and service assets from acquisitions to disposal
- Maintenance of the asset inventory.

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

The actual roles related to Service Asset and Configuration Management includes:
- Service Asset Manager
- Configuration Manager
- Configuration Analyst
- Configuration Administrator/Librarian
- CMS/Tools Administrator
- Change Manager (all Changes to CIs must be authorized by Change Management)

6.3.3 Change Management

GOAL: To ensure that **standardized methods and procedures** are used for controlled, efficient and prompt handling of all Changes, in order to **minimize the impact** of Change-related Incidents upon se rvice q uality, and co nsequently t o i mprove t he d ay-to-day operations of the organization.

"Remember: N ot ever y ch ange i s an i mprovement, b ut ever y i mprovement i s a change!"
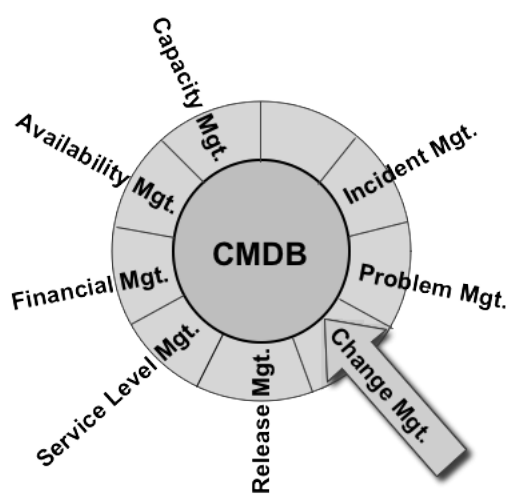
Change M anagement act s as the g reatest contributor t o t he C MDB, as Changes to C MDB must b e asse ssed and a uthorized by Change Management first.

To work effectively, Change Management needs to remain impartial to the needs of any one particular IT g roup or cu stomer, i n or der t o m ake e ffective decisions that best su pport t he ov erall organizational objectives.

Terminology	Explanations
Change:	ANY alteration in the state of a Configuration Item. This includes the addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.
Change Models:	Defines how various categories of changes are assessed & authorized, with different mechanisms and activities used to process and deliver changes based on the change type.
NORMAL Change:	A change that follows all of the steps of the change process. It is assessed by either a Change Manager or Change Advisory Board.
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.***
EMERGENCY Change:	A change that must be introduced as soon as possible. E.g. to resolve a major incident or implement a security patch. The change management process will normally have a specific procedure for handling Emergency Changes.
Request for Change: **(RFC)**	Standard form to capture and process ALL Changes to any CI
Forward Schedule of Changes (FSC):	Schedule of Approved Changes and proposed implementation dates. The Service Desk should communicate this to the users.
Projected Service Outage (PSO):	Details of Changes to agreed SLAs and service availability because of the Forward Schedule of Change in addition to planned downtime from other causes such as planned maintenance and data backups.
Change Advisory Board: **(CAB)**	A group that provides expert advice to the Change Manager. Involves representatives from various IT and business areas as well as other involved stakeholders including external suppliers. Chaired by the Change Manager
Emergency CAB: **(ECAB)**	Subgroup of CAB to provide expert advice on urgent Change matters.

Activities:
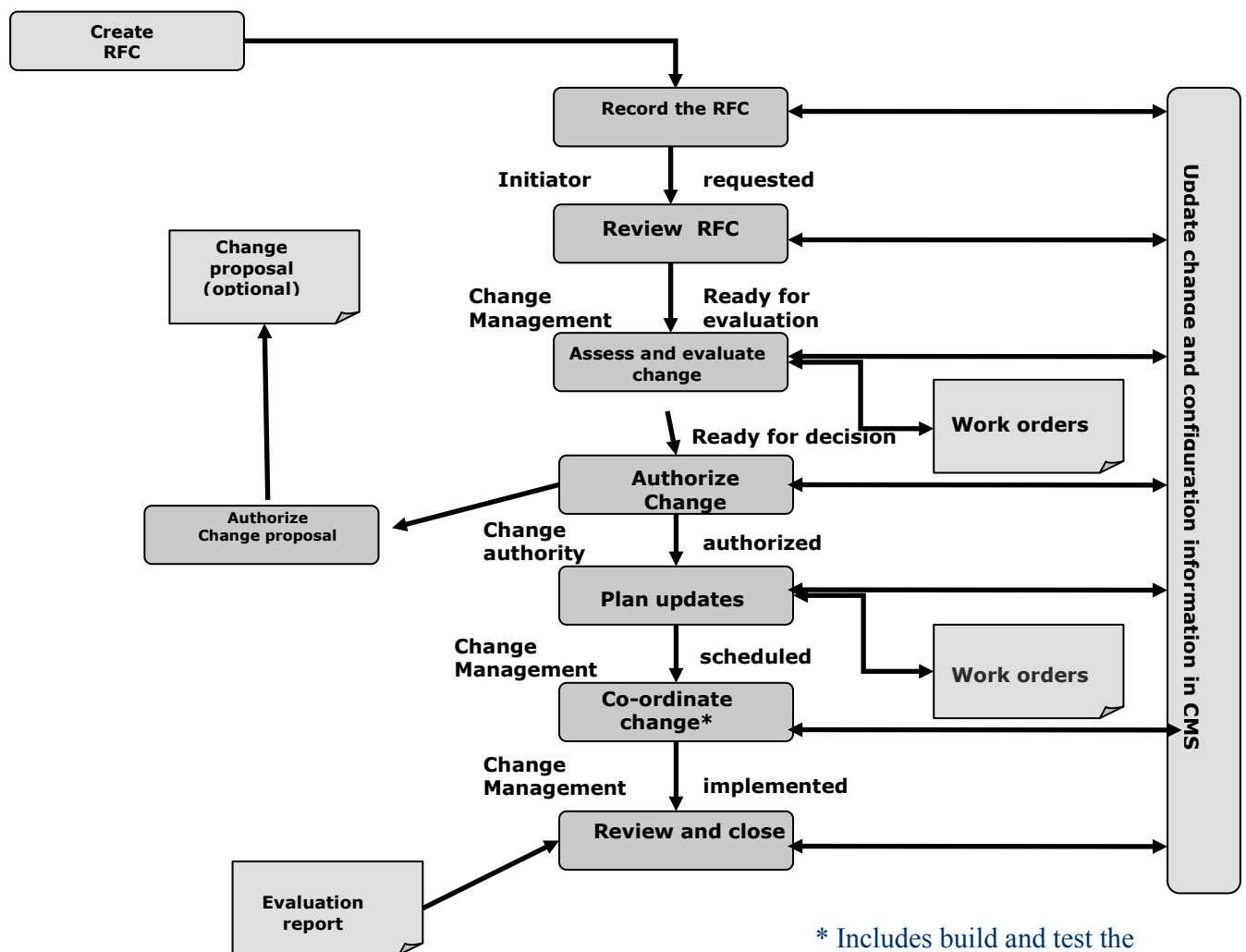
Figure 6.C– The Activities of Change Management

Important Steps:
1. The RFC is logged:
2. An initial review is performed (filter RFCs)
3. The RFCs are assessed – may require involvement of CAB or ECAB.
4. This is authorized by the Change Manager
5. Work orders are issued for the build of the Change (carried out by other groups)
6. Change Management coordinates the work performed.
7. The Change is reviewed.
8. The Change is closed.

Where can RFCs be initiated?
Anywhere (Other ITIL® processes, customers, end-users etc.)

Who does the actual build/test/implement?
- Technical areas
- Project Teams
- Release and Deployment Management

Assessing and Evaluating Changes

To e nsure that t he C hange M anagement process does no t b ecome a bottleneck, i t i s important to define w hat C hange M odels will be use d t o e nsure e ffective an d e fficient control and implementation of RFCs.

Impact:	Escalation Level:
- Standard	Executed using a pre-defined form/template

Normal Changes
- Minor	Change Manager (CM)
- Significant	Change Advisory Board (CAB)
- Major	IT Management Board

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

The 7Rs of Change Management:

When asse ssing C hanges, i t i s important t o hav e answ ers to t he following se ven questions:
- Who RAISED the change?
- What is the REASON for the change?
- What is the RETURN required from the change?
- What are the RISKS involved in the change?
- What RESOURCES are required to deliver the change?
- Who is RESPONSIBLE for the build, test and implementation of the change?
- What is the RELATIONSHIP between this change and other changes?

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

Authorization of Changes:

While the responsibility for authorization for Changes lies with the Change Manager, they in turn will ensure they have the approval of three main areas.
- Financial Approval - What's it going to cost? And what's the cost of not doing it?
- Business Approval - What are the consequences to the business? And not doing it?
- Technology Approval - What are the consequences to the infrastructure? And not doing it?

Key Points:
- Consider the implications of performing the Change, as well as the impacts of NOT implementing the Change.
- Importance of empowering Change Manager as their primary role is to protect the integrity of the IT infrastructure.
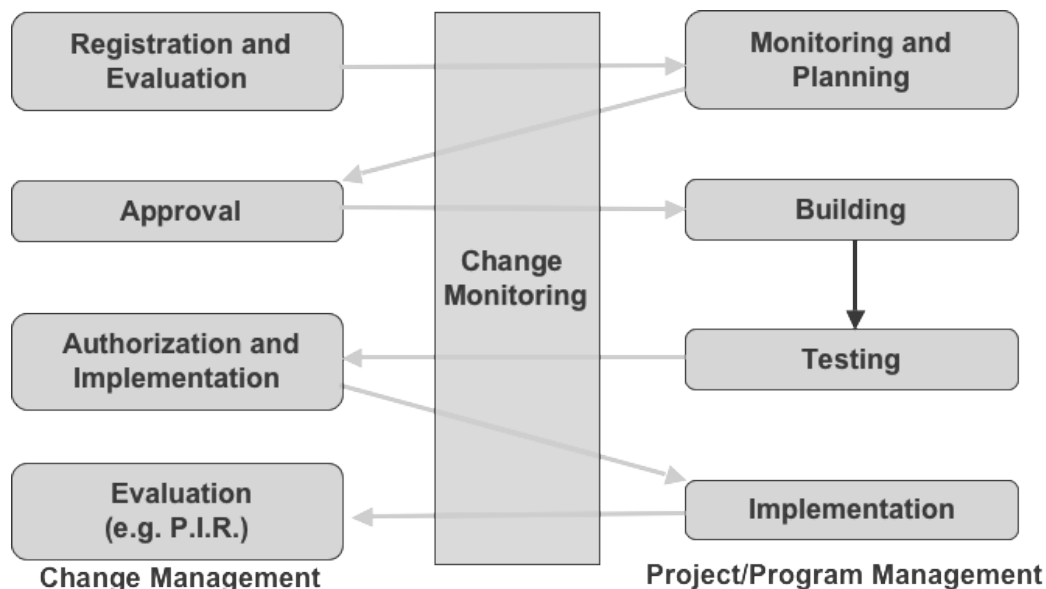
Relationship with Project Management:

Figure 6.D Relationship with Project Management

How does Change Management work with Project Management?
- Change Management authorizes, controls, coordinates
- ***Does not*** plan, build, test or implement.
- Change Management is concerned with Remediation Planning to ensure that each RFC has a fallback / rollback plan.

Roles and Responsibilities

Change Manager
- Administration of all RFCs.
- Prepare RFCs for CAB meetings, FSC for Service Desk.
- Authorize (or reject) changes.

CAB
- Advises Change Manager on authorization issues for RFCs with significant or major impact.

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

Technical specialists
- Build and test the actual change.

Key Performance Indicators (KPIs) of Change Management

It is important that a balanced view of metrics is used when assessing the effectiveness and efficiency of the Change Management process. These metrics include:
- Number of RFCs (Accepted/Rejected)
- Number and % of successful Changes
- Emergency Changes
- Number of Changes awaiting implementation
- Number of implemented Changes
- Change backlogs and bottle-necks
- Business impact of changes
- Frequency of Change to CIs

Challenges affecting Change Management

- Change in culture - 1 central process comes into place that influences everyone's activities
- Bypassing - projects ducking the Change Management planning
- Optimal link with Configuration Management - to execute a controlled change all data MUST be reliable
- Commitment of the supplier(s) to the process
- Commitment of management.

6.3.4 Release and Deployment Management

GOAL: To deploy r eleases into pr oduction and est ablish e ffective use o f t he se rvice i n order to deliver value to the customer and be able to handover to Service Operation.

| *Terminology*	*Explanations*
Release:	A collection of **authorized** Changes to an IT Service.
Release Unit:	A R elease U nit d escribes the por tion o f a s ervice of I T infrastructure t hat i s normally r eleased t ogether acc ording t o t he organization's release pol icy. The u nit may v ary depen ding o n type(s) or item(s) of s ervice asse t or se rvice co mponent su ch as hardware or software.
Definitive Media Library (DML): *(previously known as the DSL)*	The se cure l ibrary i n which the definitive authorized versions of all media C Is are st ored an d pr otected. The D ML sh ould i nclude definitive co pies o f pur chased s oftware (along w ith l icense documents or information) as well as software developed on site.
Definitive Spares (DS): *(previously known as DHS)*	Physical st orage of a ll ***spare I T co mponents an d assem blies maintained at t he same l evel a s w ithin t he l ive environment***. New I T asse mblies are st ored h ere un til r eady f or use , a nd additional c omponents can be us ed w hen ne eded for a dditional systems or in the recovery from Incidents. • Details recorded i n t he C MDB, co ntrolled b y R elease a nd Deployment Management.
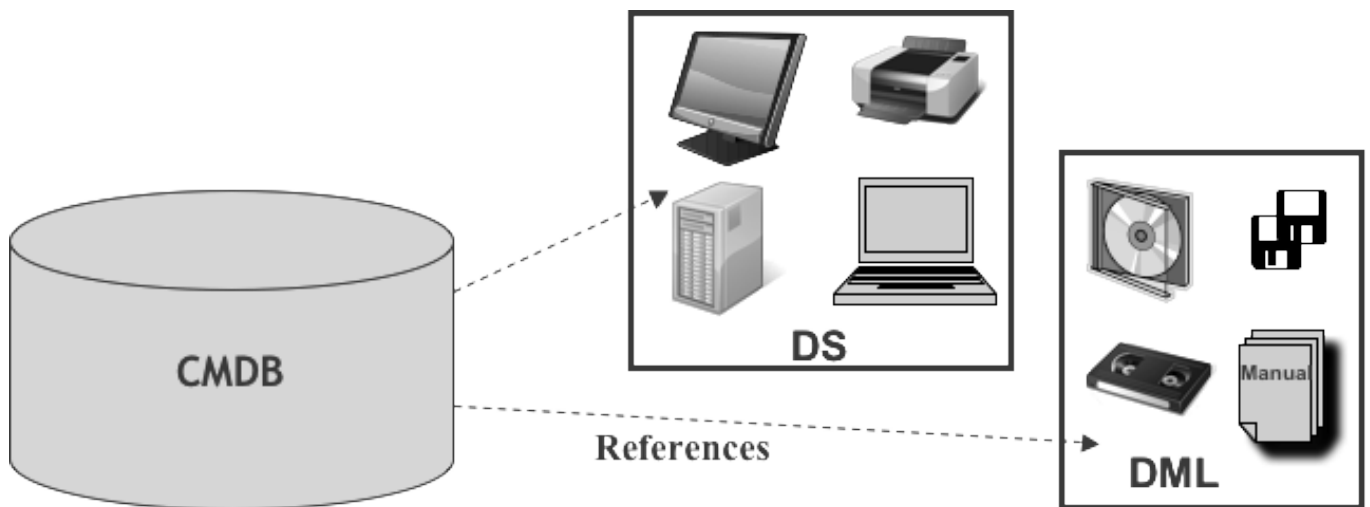
Figure 6.E – The Definitive Media Library and Definitive Spares

Remember – the el ements f ound w ithin the D ML a nd D S a re r eferenced b y t he CMDB as CIs.

Release and Deployment Management also works closely with Change Management and the S ervice D esk to i nform use rs of sch eduled ch anges/deployments. Tools used t o do this can include:
- email notification
- sms notification,
- verbal communication.

Options for Releases

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

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

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

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

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

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

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

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

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

Activities

Release policy & planning
Design & develop or order & purchase Build & configure release Release testing & acceptance
Deployment planning Communication, preparation & training
Logistics, Delivery & installation

Key Points:

The R elease P olicy i s the overarching st rategy f or Releases and w as derived from the Service Design phase of the Service Lifecycle.

The R elease Plan i s the operational implementation for each release.

The Ro llout P lan is the documented approach f or distributing a single Release.

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

Design & Te st: (Coordinates with ot her S ervice D esign an d S ervice T ransition Processes):
- Produce Release assembly & build instructions
- Create Installation scripts
- Run Test plans
- Develop Back-out procedures
- Produce tested installation procedures

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

Logistics, Distribution & Installation:
- Implement the release strategy
- CMDB updated where necessary after installation
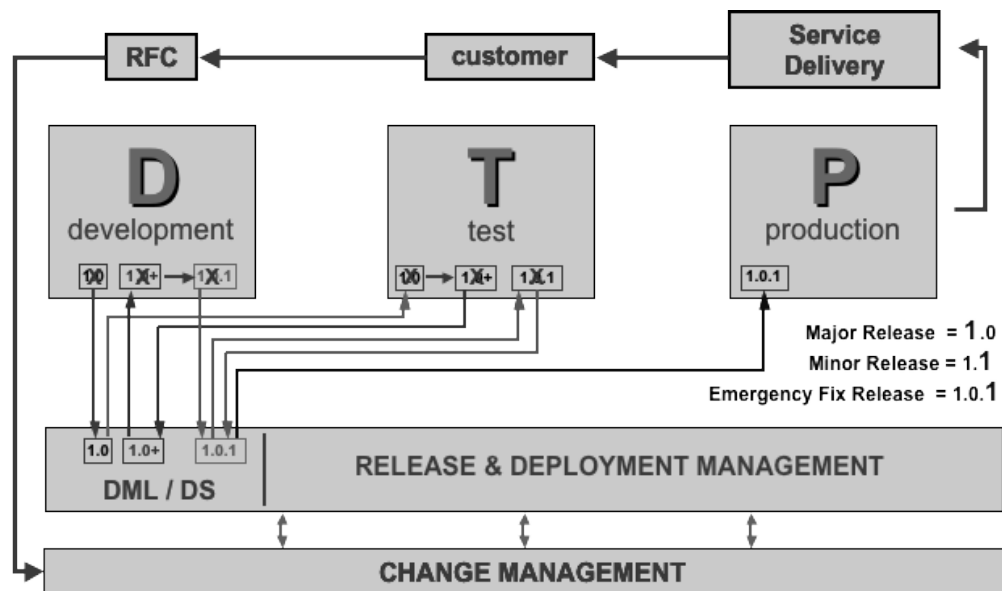- Service Desk is updated about any issues to manage the transition.

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

Note h ow C hange, R elease & D eployment, S ervice V alidation & T esting an d S ervice Asset & C onfiguration M anagement w ork together for the t ransition of n ew or m odified Services.

Roles and Responsibilities

Release & Deployment Manager
- Drive effectiveness & efficiency of process
- Manage release management team
- Liaise w ith C hange & C onfiguration Management, I T pl atform m anagers, Application Developers etc.

Skills: technical & coordination skills, project manager.

Release & Deployment Management Team
- Manage the DML & DS
- Design, build, test & deploy releases.
- Manage software management/distribution tools.

6.3.5 Service Validation and Testing

GOAL: To ensure that new or changed IT Services match the design specification and will meet the needs of the business.

The un derlying co ncept t o w hich S ervice Validation co ntributes i s quality assu rance – establishing that the service design and release will deliver a new or changed service or service offering that is fit for the purpose and fit for use.

Testing i s a vi tal ar ea w ithin S ervice M anagement an d has often be en t he uns een underlying cause of what was taken to be inefficient Service Management processes. If services are not tested sufficiently then their introduction into the operational environment will bring rise in:

- **Incidents** – failures in service elements and mismatches between what was wanted and what was delivered impact on business support
- **Service Desk calls for assistance** – services that are not functioning as intended are inherently less intuitive causing higher support requirements
- **Problems and errors** – that are harder to diagnose in the live environment.
- **Costs**, since errors are more expensive to fix in production than if found in testing.
- **Services that are not used effectively** by the users to deliver the desired value.

The S ervice V alidation and Testing pr ocess closely co llaborates with ot her S ervice Transition processes as well as others from across the Service Lifecycle.
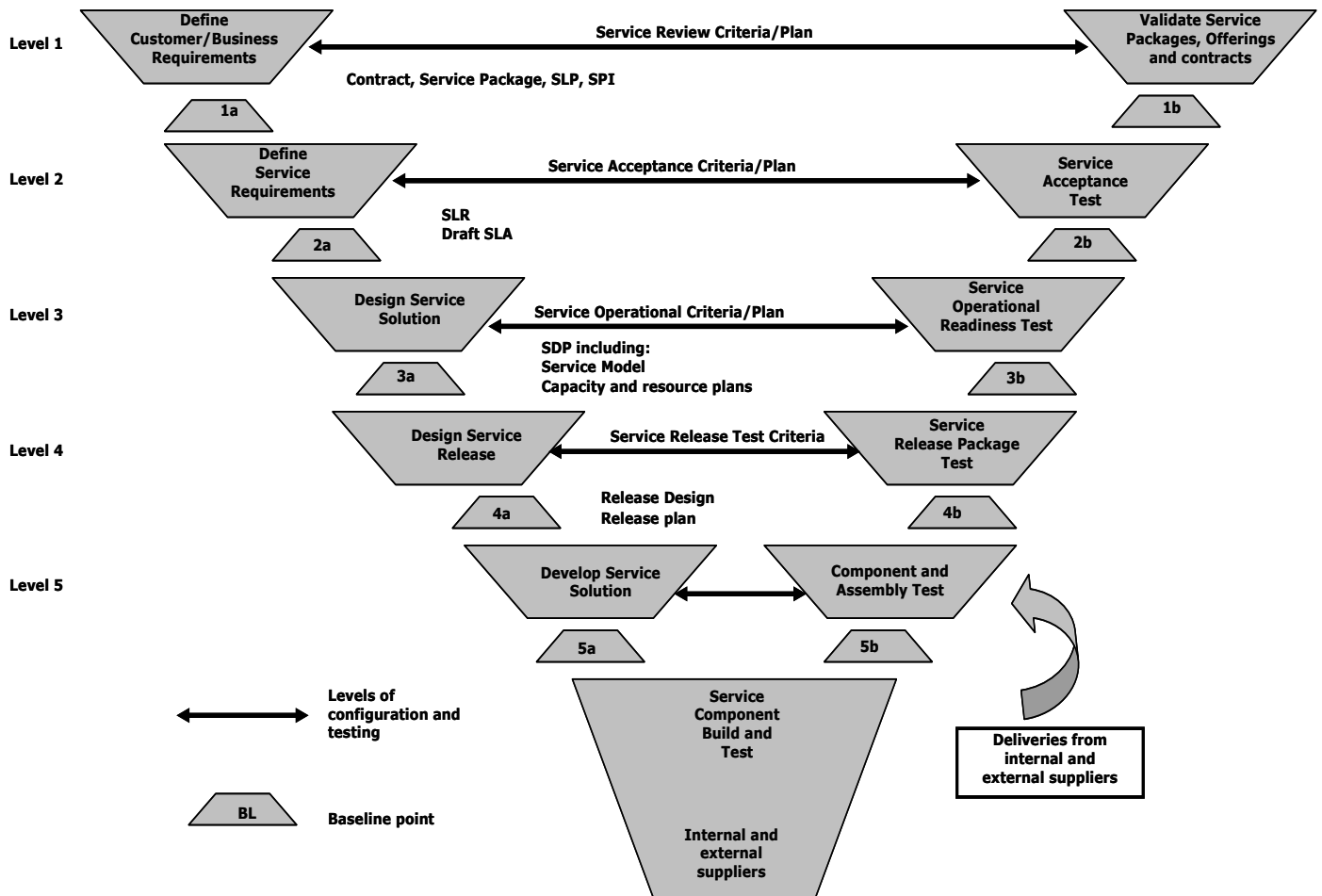
Figure 6.F – The Service V Model

The S ervice V M odel is a co ncept o f establishing acce ptance r equirements against various levels of requirements that apply in order to **justify release to the customer for trial and assessment.**

The **left hand s ide** represents the specification of the service requirements down to the detailed Service Design.

The **right ha nd s ide** focuses on t he v alidation and t est act ivities that ar e per formed against the specifications defined on the left hand side, and there is direct involvement by the equivalent party on the right hand side.

It sh ows that se rvice v alidation and acce ptance t est pl anning sh ould st art w ith t he definition o f se rvice r equirements. E .G cu stomers who sig n of f t he ag reed se rvice requirements will also sign off the service Acceptance Criteria and test plan if successful.

6.3.6   Implementation

Implementing S ervice T ransition i n an organization w hen t his has not ex isted be fore i s only l ikely i f a new se rvice pr ovider i s being est ablished. Therefore, t he t ask for most service provider organizations will be on e of se rvice i mprovement, a m atter of assessing their cu rrent ap proach t o the Service Transition processes and est ablishing t he m ost effective and efficient improvements to make, prioritized according to the business benefit that can be achieved.

Implementing new or i mproved S ervice Transition processes will be a si gnificant organizational change and a n introduction of improved se rvices delivered by t he se rvice provider. From that context, much of the guidance in this publication on delivering new or changed services is directly applicable to introducing Service Transition itself. In doing so, is in itself, a Service Transition exercise, since it is changing the services delivered by the service provider.

Stages of Introducing Service Transition

These st ages will m atch t hose of other se rvices, r equiring a j ustification for t he introduction, designing of the Service Transition components and then their introduction to the organization (transitioning) before they can run in normal mode.

Justifying Service Transition

Service T ransition i s a ke y co ntributor t o t he s ervice pr ovider's ability t o d eliver q uality services to the bu siness. It is the delivery mechanism b etween the work of d esign, and the day-to-day care delivered by operations. H owever, Service T ransition p rocesses are not al ways visible t o customers, a nd this can m ake financial j ustification difficult. When setting up S ervice T ransition, at tention needs to b e p aid t o w ays of q uantifying an d measuring the benefits, typically as a balance between impact to the business (negative and positive) and co st) in terms of money/staff resources) and in terms of what would be prevented by appl ying r esource t o a ny sp ecific transition, su ch as delivering st aff resources or delaying implementation.

Gathering of evidence on the cost of current inadequate Service Transition is a valid and useful exercise, addressing issues such as:
• Cost of failed changes
• Extra cost of actual transition compared with budgeted costs
• Errors found in live running that could have been detected during test transition.

Designing Service Transition

Useful factors to consider when designing Service Transition are:

Applicable standards and policies

Consider h ow ag reed pol icies, st andards and l egislation w ill c onstrain the design of Service Transition. C onsiderations might i nclude requirements for i ndependence an d visible accountability.

Relationships

Other internal su pport se rvices: t here ar e m any si tuations when S ervice T ransition m ust work together with other areas that are transitioning other elements of a business change, such as HR, facilities m anagement, production control, e ducation a nd t raining. The processes will be desi gned to facilitate these relationships. T he aim should be to ensure that ow nership for e ach c omponent o f t he ov erall se rvice pa ckage i s defined and subsequently management responsibility is clear.

Program and project management

Major t ransition may be managed as pr ograms or pr ojects, an d Service T ransition w ill deliver t heir r ole w ithin t he appropriate u mbrella. T o ensure a ppropriate transition is delivered, st aff w ill b e i nvolved i n ag reeing ke y pr ogram and project milestones and timelines and Service Transition should be set up to adopt this role.

To be effective, S ervice Transition needs to take a br oader v iew acr oss projects, combining transitions and releases to make the best use of available resources.

Internal development teams and external suppliers

Communication channels will need to deal with defects, risks and issues discovered during the transition process. Channels to both internal teams and external suppliers will need to be identified and maintained.

Customers/user

Communication w ith customers and users i s important to ensure t hat t he transitioned service will remain focused on current business requirements. The requirements at actual transition may ev olve f rom t he needs identified at d esign st age an d co mmunication channels with t he c ustomer w ill be t he so urce o f i dentifying t hose ch anges. E ffective communication will benefit f rom an agreed st rategic stakeholder co ntact map. In m any circumstances this communication will be r outed through service or account management or Service Level Management, but these channels need to be identified and designed into the Service Transition processes also.

Other stakeholders

Other st akeholders will need t o i nterface w ith S ervice T ransition and t hese sh ould b e identified for all foreseeable ci rcumstances, including in di saster r ecovery sce narios, and so liaison with ITSCM should be created for. Other possible considerations might include:
- IT, e.g. networks, IT security, data management
- Outside of I T but w ithin the or ganization, e. g. facilities management, HR p hysical security

- Outside of the organization, e.g. landlords, police and regulatory bodies.

Budget and resources

Funding approach

A m echanism for co ntrolling t he funding of t he t ransition i nfrastructure n eeds to b e established, this will need to include:
- Testing environments
- SCM and Service Knowledge Management Systems

The costing of transition objectives needs to be an essential inclusion of design. Often the transition options will be costed and a business risk-based decision reached.

Resources

Similar to the issues and options identified in the funding area, supply and control of other resources will need to be addressed within the Service Transition such as:
- Staff
- Central Infrastructure

Test environment management is a major item of expenditure and a significant resource element i n m any or ganizations. U nder funding/resourcing ca n cause v ery e xpensive errors and problems in supporting live services, and have severe detrimental effects on an organization's overall business capability.

Risk & Value

As with all transitions, decisions around transitioning the transition service should not be made without adequate understanding of the expected risks and benefits. Risks may include:
- Alienation of support staff
- Excessive costs to the business
- Unacceptable delays to business benefits.

The risks and beneficial values require a baseline of the current situation, if the changes are to be measureable. Measures of the added value from Service Transition might include:
- Customer and user satisfaction
- Reduced incident and failure rates for transitioned services
- Reduced cost of transitioning.

6.4   Service Transition Summary

Effective S ervice T ransition ca n si gnificantly improve a S ervice pr ovider's ability t o effectively handle high volumes of change and releases across its Customer base. Other benefits delivered include:

- Increased success rate of Changes and Releases
- More accurate estimations of Service Levels and Warranties
- Less variation of costs against those estimated in budgets
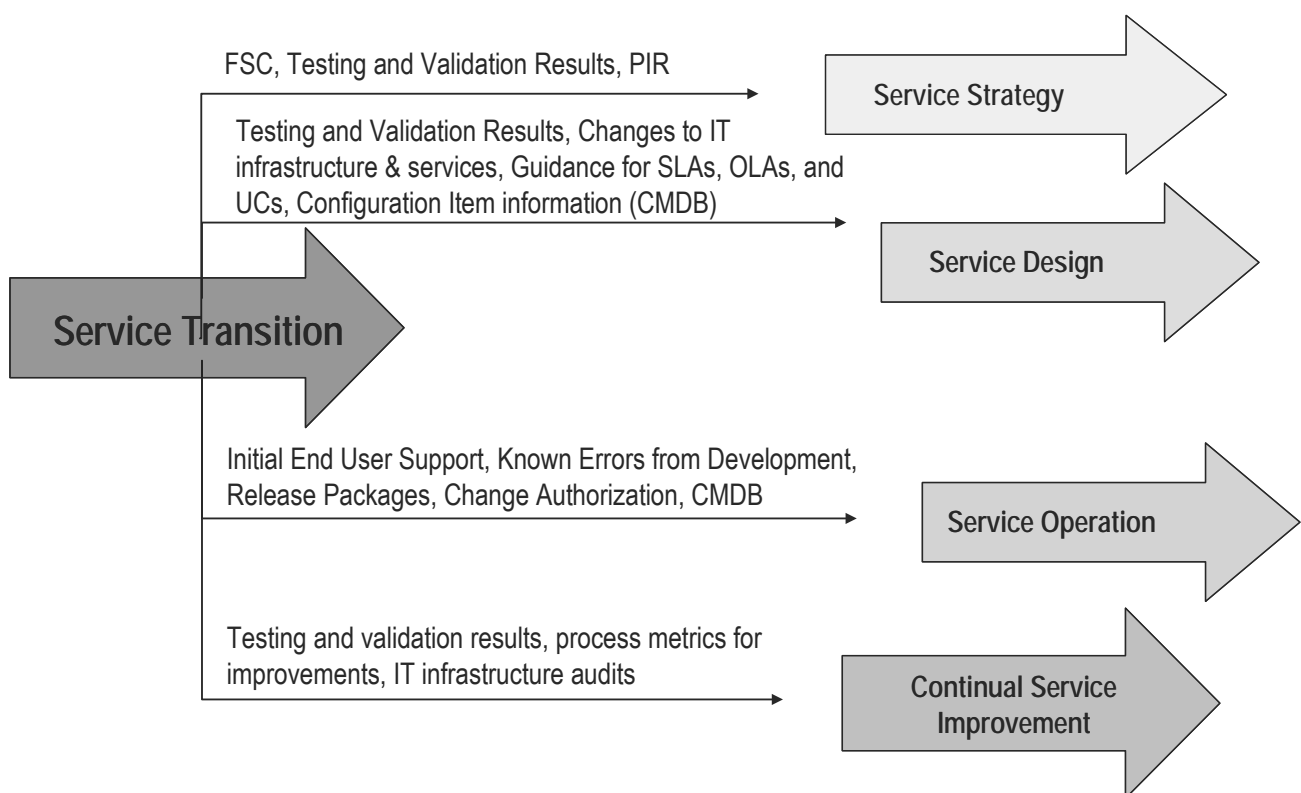- Less variation from resources plans.

FSC, Testing and Validation Results, PIR

Service Strategy

Testing and Validation Results, Changes to IT infrastructure & services, Guidance for SLAs, OLAs, and UCs, Configuration Item information (CMDB)

Service Design

Service Transition

Initial End User Support, Known Errors from Development, Release Packages, Change Authorization, CMDB

Service Operation

Testing and validation results, process metrics for improvements, IT infrastructure audits

Continual Service Improvement

Figure 6.G – Some outputs to other lifecycle phases.

6.5 Service Transition Scenario

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

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

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

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

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

7 Service Operation
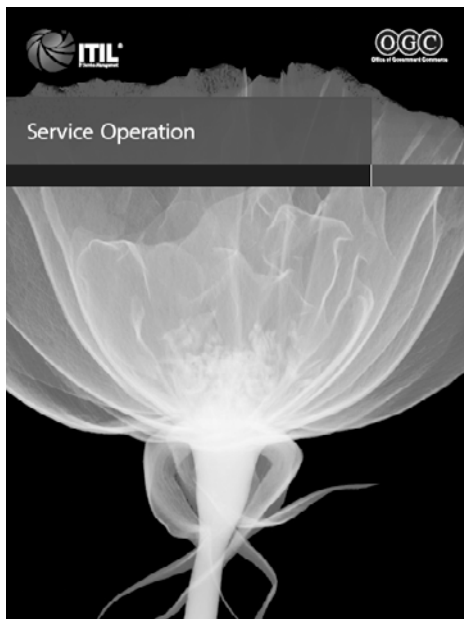
From a customer viewpoint, Service Operation (SO) is where actual value is seen.

This is because it is the execution of strategies, designs and plans and improvements from the Service Lifecycle phases.

Functions	Processes
Service Desk	Incident Management
Technical Management	Problem Management
Application Management	Event Management
IT Operations Management	Request Fulfillment
	Access Management

The Service Operation phase is also concerned with the operational activities that need to be performed for the processes found in the other lifecycle phases.

7.1 Objectives

To enable effectiveness and efficiency in delivery and support of IT services.

Other objectives include:
- Delivering cost-effective stability in the IT infrastructure
- Providing effective and efficient mechanisms to deal with Service Requests, Events, Incidents and Problems.

7.2   Major Concepts

Achieving the Balance

Service Operation is more than just a repetitive execution of a standard set of procedures or activities. S O works in an ev er changing environment. This forms a conflict between maintaining the status quo and adapting to changes in the business and technological environments.

One of Service Operation's key roles is to deal with this conflict and to achieve a balance between conflicting sets of priorities.
Error!

Achieving the Balance

Internal IT View:		External Business View:
Focuses on t he way i n which I T components and sy stems are managed t o deliver the services.		Focuses on t he w ay i n which services are experienced by its users and customers.
An organization here i s out of balance and is in dang er o f n ot m eeting busi ness requirements.	**VS**	An organization has business focus, but t ends to un der-deliver on promises to the business.
Stability:		**Responsiveness:**
No m atter how g ood t he functionality i s of an I T se rvice or ho w well i t has been designed, i t will be w orth f ar l ess if t he service components are not av ailable or i f they per form i nconsistently. S ervice Operation has to e nsure t hat t he I T infrastructure i s stable an d av ailable as required.	**VS**	Service O peration must r ecognize that t he busi ness and I T requirements change.

When t here i s an ex treme focus on responsiveness IT may t end t o overspend on change and al so decrease t he st ability of t he infrastructure. |
| However an ex treme focus on st ability means that I T i s in danger o f ignoring changing business requirements | | |

Cost of Service:		Quality of Service:
An organization with an extreme focus on cost is out of balance and is in danger of losing service quality because of heavy cost cutting. The loss of service quality leads to a loss of customers, which in turn leads to further cost cutting as the negative cycle continues.	VS	An organization with an extreme focus on quality has happy customers but may tend to overspend to deliver higher levels of service than are strictly necessary, resulting in higher costs and effort required.

The goal should be to consistently to deliver the agreed level of IT service to its customer and users, while at the same time keeping costs and resource utilization at an optimal level. |
| **Reactive:** | | **Proactive:** |
| An organization that is extremely reactive is not able to effectively support the business strategy. Unfortunately a lot of organizations focus on reactive management as the sole means to ensure services are highly consistent and stable, actively discouraging proactive behavior from staff. The worst aspect of this approach is that discouraging effort investment in proactive Service Management can ultimately increase the effort and cost of reactive activities and further risk stability and consistency in services. | VS | An extremely proactive organization tends to fix services that are not broken, or introduce services that are not yet needed, resulting in higher levels of change, costs and effort.

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

7.3 Service Operation Functions

"Know your role, do your job"

Team motto describing the goal for every player, coach and general staff member of the Kansas City Chiefs.

Functions refer to the people 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 ha ve a sp ecific role t o pl ay i n t he ove rall t eam st rategy, I T F unctions define t he different roles and responsibilities required for the overall Service Delivery and Support of IT Services.
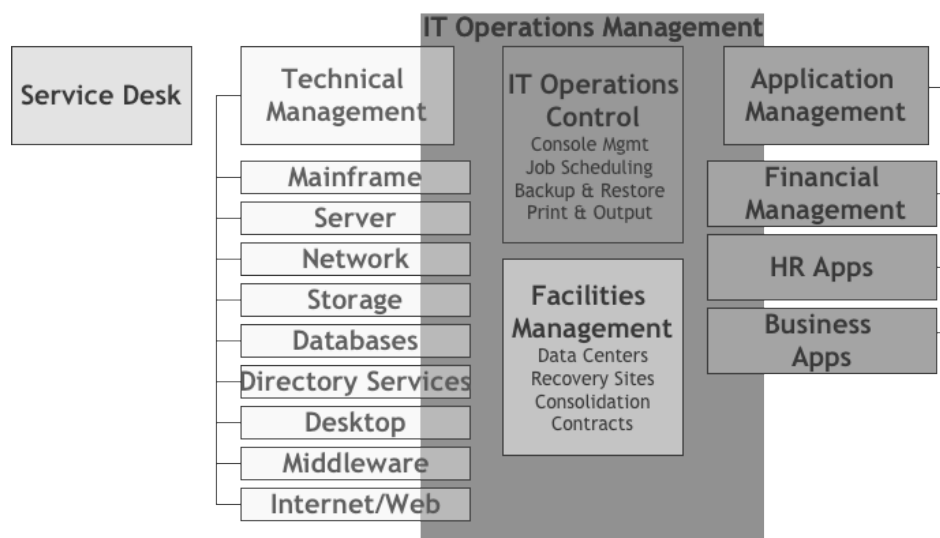
Figure 7.A – The ITIL® Functions from Service Operation

NOTE: These ar e l ogical f unctions and d o not n ecessarily hav e t o be performed by equivalent or ganizational st ructure. This means that Technical and A pplication Management c an b e or ganized i n any combination an d i nto any num ber of departments. The lower groupings (e.g. Mainframe, Server) are examples of activities performed by Technical Management and are not a suggested organizational structure.

7.3.1   The Service Desk

GOAL: To support t he ag reed I T s ervice pr ovision by ensu ring t he accessibility a nd availability of the IT organization and by performing various supporting activities.

| Terminology	Explanation
Service Desk Types:	• *Relates to the skill level and first-time resolution rate for service calls.*
Call Centre:	• *Handling/logging of large volumes of calls. Low first-time resolution rate for calls and requests.*
Help Desk:	• *Manage and co-ordinate incidents. Medium first-time resolution rate for calls and requests.*
Service Desk:	• *A wide variety of services offered. High first-time resolution rate for calls and requests.*
Service Desk Structure:	• *Relates to the physical organization of the service desk.*
Local	• *The Service Desk is situated in the same physical location (or time zone for international organizations) as the user groups that it serves.*
Central	• *A centralized Service Desk serves multiple user groups from different physical locations.*
Virtual	• *A Service Desk that has no physical structure, but instead relies on technology to coordinate call resolution across disparate Service Desk staff and to provide a centralized Knowledgebase.*
Follow-the-Sun	• *Utilizing multiple Service Desks across different time-zones in order to provide 24x7 availability of the Service Desk. Typically there will still be a centrally managed Knowledgebase to enhance the quality of support delivered.*
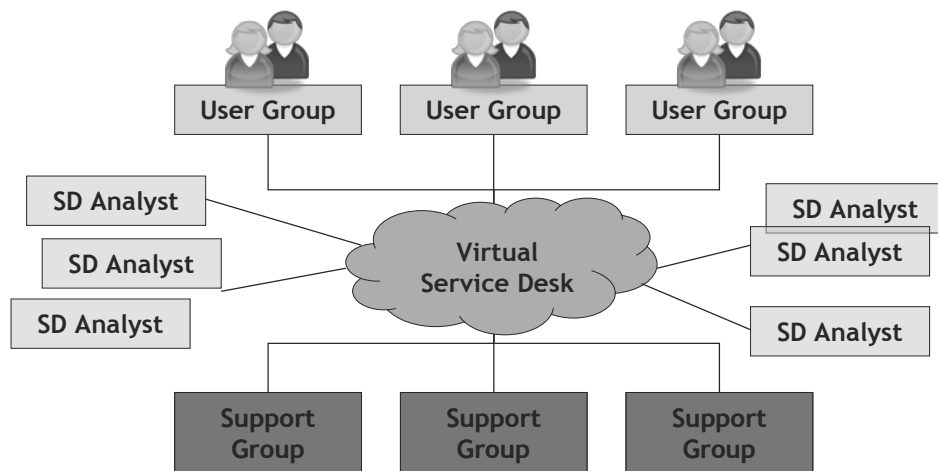
Figure 7.B – A Virtual Service Desk structure

Skills

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

- Communication Skills
- Technical Skills
- Business Understanding

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

Self-Help

Many organizations find it beneficial to offer "Self Help" capabilities to their users. The technology should therefore support this capability with some form of web front-end allowing web pages to be defined offering a menu-driven range of self help and service requests – with a direct interface into the back-end process-handling software. This reduces the amount of calls into the Service Desk and is often used as a source for improvements to efficiency. An example of this is the ability for a customer to track online the status of their parcels when shipped through a major courier company.

Aside from this, the Service D esk will use m any di fferent tools, sy stems and ot her technology components in order to provide effective and efficient support to end-user calls and requests. To enable this, typical technology components utilized include:

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

Key Performance Indicators for the Service Desk:
It i s important t o use a ba lanced r ange o f metrics for measuring t he e ffectiveness and efficiency of the Service Desk. Typical metrics include:

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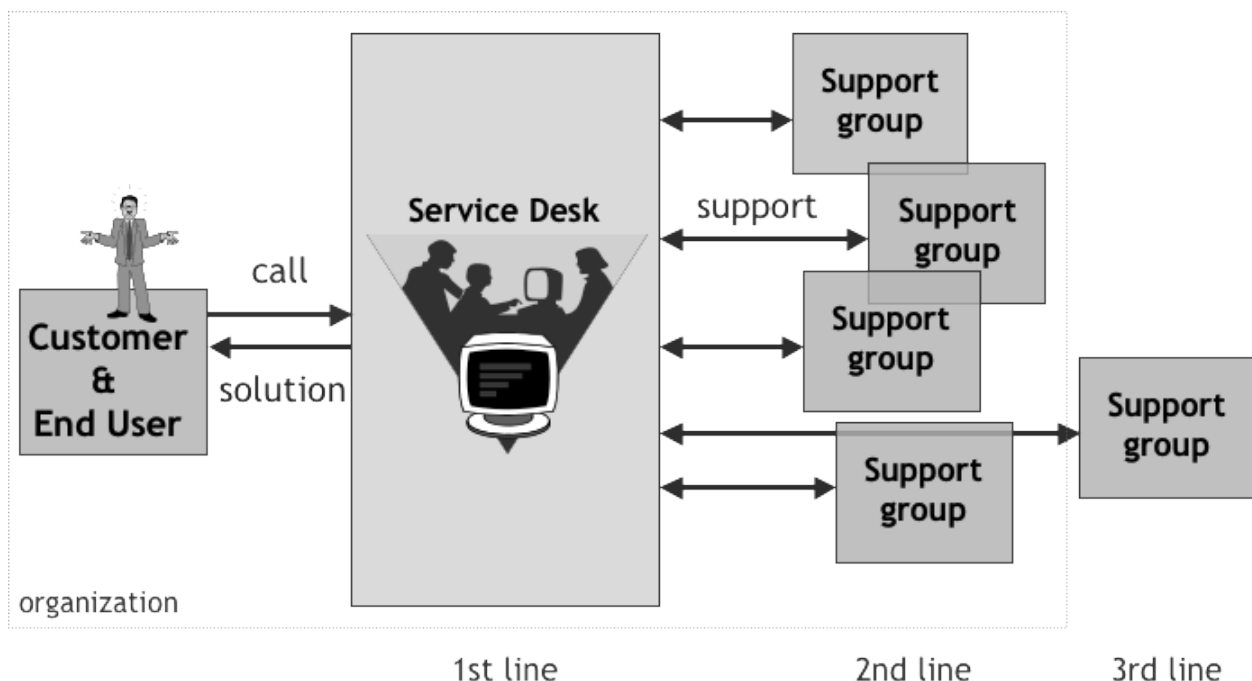- Use of self help (where exists)

**Figure 7.C – The Service Desk managing all end-user communication**

7.3.2 Technical Management

Goal: To help plan, implement and maintain a stable technical infrastructure to support the organization's business processes through:

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

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

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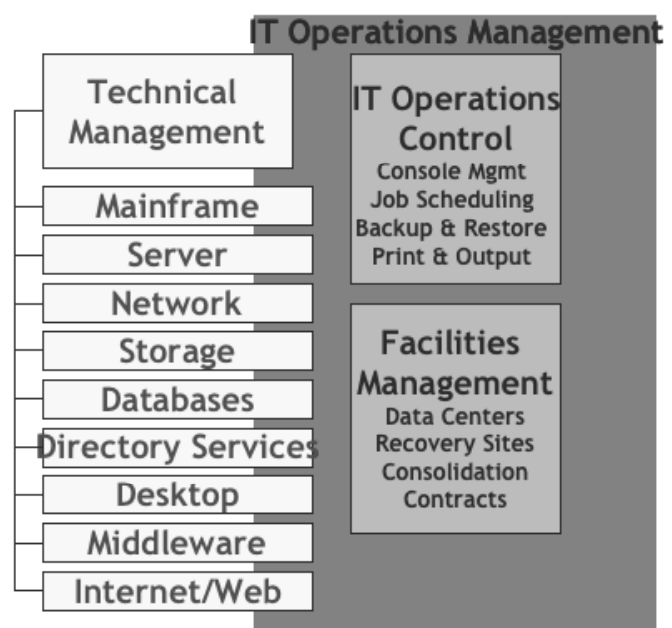
In many organizations, the actual role played by IT Operations Management is carried out by either Technical or Application Management.

Roles and Responsibilities:

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

Specialist Technical Architects & Designers

Specialist Maintenance & Support Staff

(Primarily involved in Service Operation)

Technical Management

Figure 7.D – Staff making up the Technical Management Function

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

7.3.3   IT Operations Management

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

In m any se nses, t he function per forms many of t he l ogistical act ivities required f or t he effective and efficient delivery and support of services (e.g. Event Management).

In some or ganizations this is a single, centralized de partment. While i n others some activities and st aff ar e centralized a nd s ome are p rovided by distributed and sp ecialized departments.

In m any ca ses, t he r ole o f I T Operations Management i s act ually performed by t he T echnical a nd Application Management f unctions where required.
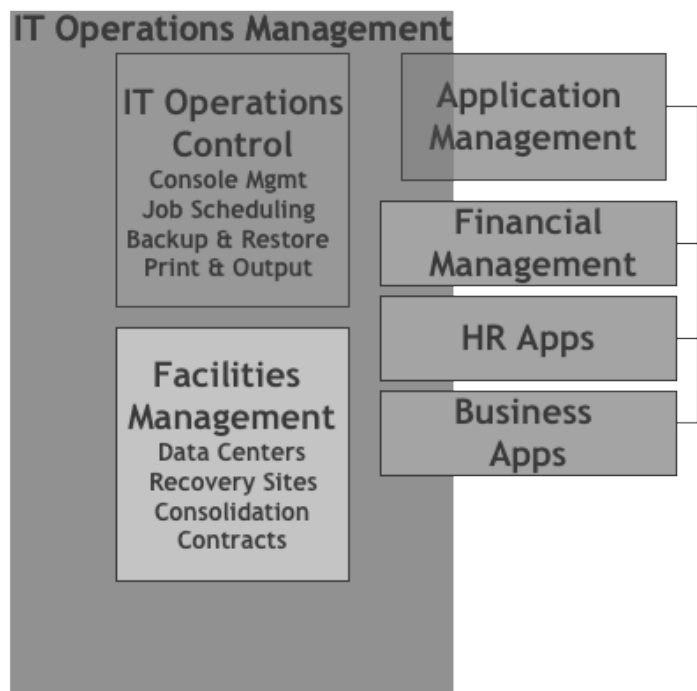
Roles and Responsibilities:
- Maintenance of the 'status quo' to achieve stability of the organization's day to day processes and activities.
- Regular scrutiny and improvements to achieve improved service at reduced costs, whilst maintaining stability.
- Swift appl ication o f o perational ski lls to di agnose and r esolve any I T oper ations failures that occur.

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

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

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

| IT Operations Control	Facilities Management
Event Mgmt Console Mgmt Job Scheduling Backup & Restore Print & Output	Data Centers Recovery Sites Consolidation Contracts

7.3.4 Application Management

Goal: To hel p de sign, i mplement and maintain st able ap plications to su pport t he organization's business processes.

Application M anagement i s usually di vided i nto departments based on t he ap plication portfolio o f t he organization al lowing easi er sp ecialization and m ore focused support.

Roles and Responsibilities:
- Managing Applications throughout their lifecycle.
- Supports and maintains operational ap plications, and pl ays an i mportant r ole i n d esign, t esting and improvement o f appl ications that f orm par t of IT Services.
- Support t he organization's business processes by helping t o i dentify f unctional an d m anageability requirements for application software.
- Assist i n t he d esign and/ or de ployment o f t hose applications.
- Provide ongoing support and i mprovement of those applications.
- Identify skills required to support the applications
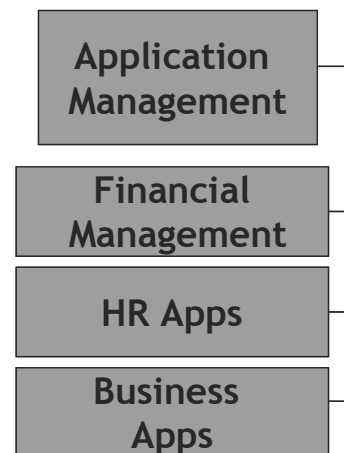
7.4   Service Operation Processes

The g oal of S ervice O peration as previously mentioned i s to en able e ffectiveness and efficiency in delivery and support of IT services. The processes that support this goal are:

- Event Management
- Incident Management
- Problem Management
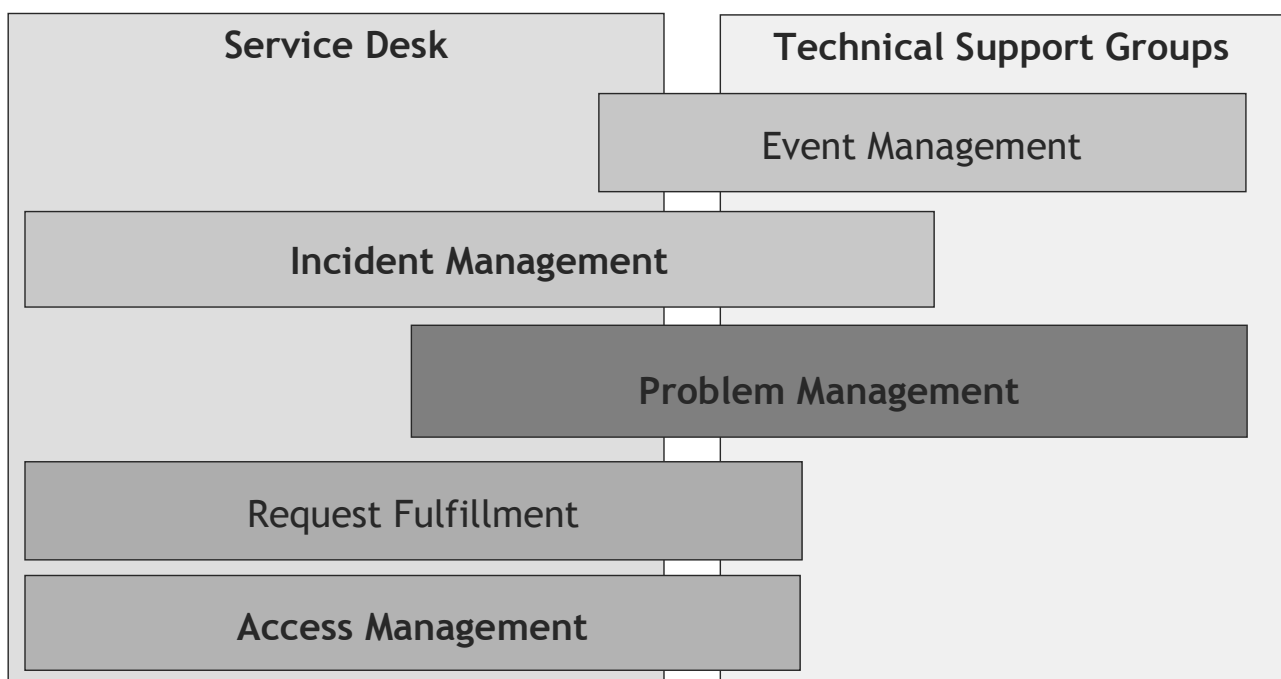- Request Fulfillment
- Access Management

Service Desk

Technical Support Groups

Event Management

Incident Management

Problem Management

Request Fulfillment

Access Management

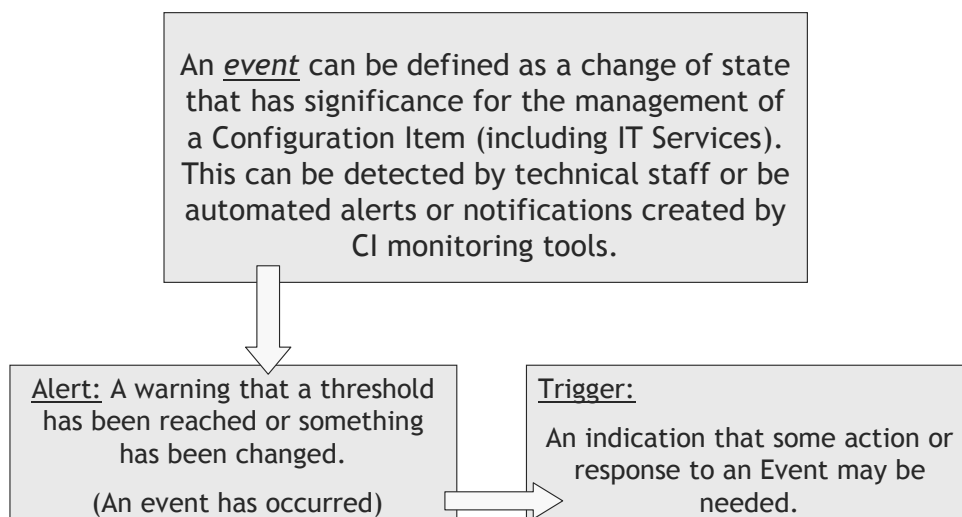**Figure 7.E – Where the Service Operation Processes get carried out**

The figure ab ove de monstrates how m uch r esponsibility t he S ervice D esk and t he Technical S upport G roups (Technical, I T O perations and A pplication M anagement functions) hav e i n t he S ervice O peration Processes. Incident Management, R equest Fulfillment a nd A ccess Management ar e pr imarily ca rried out by t he S ervice D esk, with Event Management and Problem Management as primarily 'back-of-house' processes.

7.4.1   Event Management

Goal: To enable stability in IT Services Delivery and Support by monitoring all events that occur throughout the IT infrastructure to allow for normal service operation and to detect and escalate exceptions.

Event Management also:
- Provides the entry point for the execution of many Service Operation processes and activities (e.g. Incident Management)
- Provides a way of comparing actual performance and behaviour against design standards and Service Level Agreements.
- Provides a basis for Service Assurance and Reporting and Service Improvement in the Continual Service Improvement phase.

An *event* can be defined as a change of state that has significance for the management of a Configuration Item (including IT Services). This can be detected by technical staff or be automated alerts or notifications created by CI monitoring tools.

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

(An event has occurred)

Trigger:

An indication that some action or response to an Event may be needed.

There are many different types of events, for example:

- Events that signify regular operation: *(e.g. A scheduled backup occurred successfully)*

- Events that signify an exception: *(e.g. A scheduled backup failed)*

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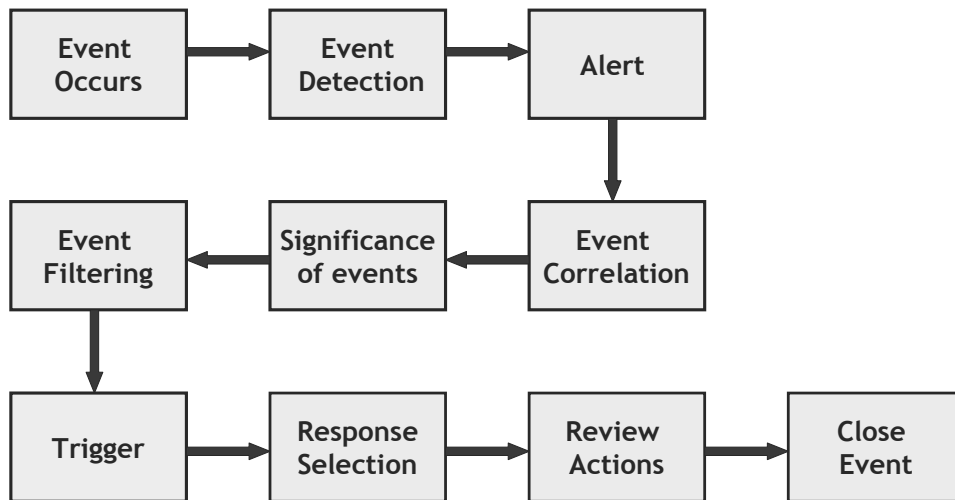
Activities

Figure 7.F – Activities of Event Management

NOTE: In most organization's IT i nfrastructure t here w ould be a si gnificant a mount of events occurring every day, which may impact on the way in which events are correlated and provide triggers indicating a response is needed.

7.4.2   Incident Management

Goal: To r estore normal s ervice oper ation *as q uickly a s p ossible* and m inimize the adverse i mpact o n bu siness operations, t hus ensuring that t he b est possi ble l evels of service quality and availability are maintained.

What is the difference between Incident Management and Problem Management?

Incident Management is not concerned with the root cause, only addresses the symptoms as quickly as possible.

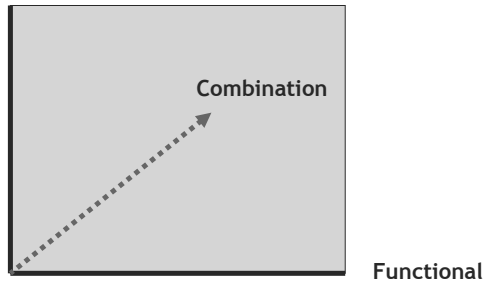# Major Concepts:

Escalation:

Hierarchical

Figure 7.G – Escalation Graph

Escalation i s the **human e lement of Incident Prioritization**. It helps us identify incidents that m ay need t o be moved u p or dow n t he pr iority l ist du e t o ch anging factors or pr iorities. E scalations can al so be combined.

Functional:
- Based on *knowledge or expertise*
- Also known as "Horizontal Escalation"

Hierarchical:
- For corrective actions by authorized *line management*
- Also known as "Vertical Escalation"
- When resolution of an incident will not be in time or satisfactory.

Categorization:

Figure 7.H – Priority Grid

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

IMPACT + URGENCY = PRIORITY
- **Impact:** Degree to which the **user/business** is affected
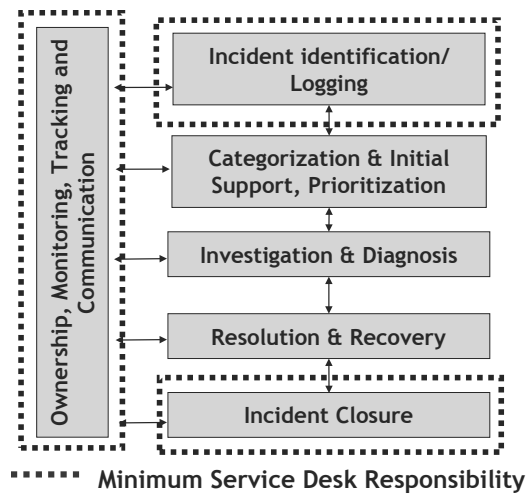- **Urgency:** Degree to which **resolution** can be delayed

Activities:

Figure 7.I – Activities of Incident Management

Ownership, Monitoring, Tracking & Communication
- Service Desk OWNS/accountable for ALL Incidents
- Monitor progress, escalation of Incidents
- Advise user and IT management

Incident identification and Logging
- Update/confirm Incident and user details

Categorization, Initial Support, Prioritization (Most critical activity)
- Categorize so the exact type of call is recorded e. g. Incident (E.g. Desktop, Network, Email)
- Assess urgency and impact to assign priority
- Match against existing Problems/Known Errors
- Match multiple Incidents and create new Problem record.
- Prioritization: taking into account the impact and urgency (how quickly to incident needs a resolution).

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

Resolution and Recovery
- Resolve the Incident or raise a RFC

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

Major Incidents

The hi ghest c ategory or i mpact de fined for an i ncident. A major i ncident r esults in significant disruption to the business.

A se parate pr ocedure, w ith sh orter t imescales and g reater ur gency, m ust be use d for 'major' i ncidents. A d efinition of w hat co nstitutes a major i ncident m ust b e ag reed and ideally mapped on to the overall incident prioritization system – such that they will be dealt with t hrough t he major i ncident process. T his often l eads directly i nto P roblem Management, t o e nsure t hat t he r oot-cause o f t he I ncident i s removed and t he i ncident never occurs again.

Roles and Responsibilities

Incident Manager:
- Drive effectiveness & efficiency of process
- Manage incident management team
- Ensure SLA targets for Incident resolution are met.

   Skills: analytical, t echnical, business u nderstanding, co mmunication, ca lm u nder pressure.

Service Desk:
- Log/record Incidents
- Incident classification and categorization
- Provide initial support
- Match to existing Incident or Problem records
- Manage communication with end-users

1st, 2 nd, 3 rd l ine s upport gr oups (including Te chnical a nd Application Management):
- Incident classification
- Investigation and resolution of Incidents

Key Performance Indicators for Incident Management

Just l ike any ot her I TIL® process, a   balanced r ange of metrics must b e us ed to demonstrate effectiveness and efficiency of the Incident Management process, including:

- Total number of incidents
- Percentage o f I ncidents handled w ithin ag reed r esponse t ime (Incident r esponse-time targets may be specified in SLAs, for example, by impact code)
- Average cost per Incident
- Percentage o f I ncidents closed by t he S ervice D esk without r eference t o other levels of support
- Number and percentage of Incidents resolved remotely, without the need for a visit.

Challenges affecting Incident Management:

- Are all calls registered? Under a unique number?
- Which priority codes do we use and how is the priority determined?
- Organization of the 1st line
- Organization of the 2nd line
- What % "closed on first call" is possible through Incident Management?

7.4.3 Problem Management

Goal: To minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT infrastructure, and to prevent the recurrence of Incidents related to these errors.

Defined as two major processes:
Reactive Problem Management
Proactive Problem Management **

** (initiated in Service Operation but generally driven as part of Continual Service Improvement)

Terminology	Explanations
Problem:	**Unknown** underlying cause of one or more Incidents (The investigation)
Known Error:	**Known** underlying cause. Successful diagnosis of the root cause of a Problem, and workaround or permanent solution has been identified
KEDB:	Known Error Database, where Known Errors and their documented workarounds are maintained. This database is owned by Problem Management.
Workaround:	The documented technique in which to provide the user with the required functionality, by either alternate means or by carrying out some action required to restore service.

Relationship with other Processes:
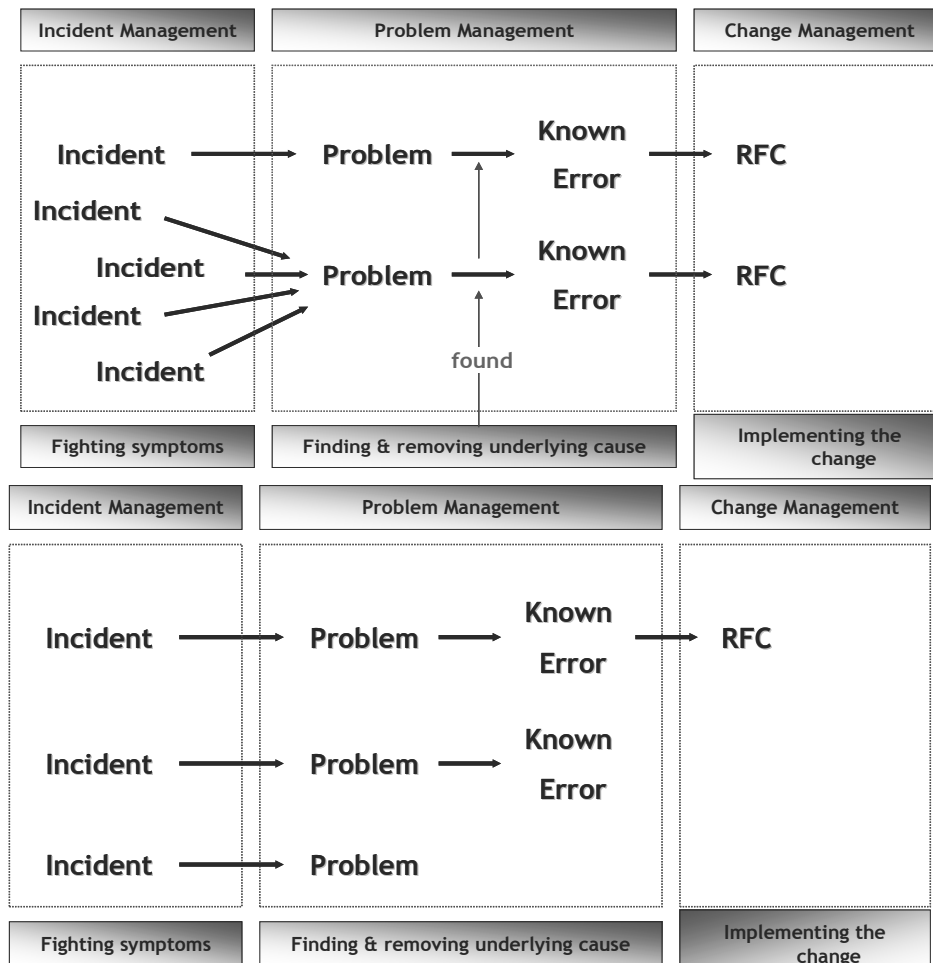
As shown above, the way in which Problems identified and corrected occur in multiple ways. For most organizations, the primary benefit of Problem Management is demonstrated in the "Many to One" relationship between Incidents and Problems. This enables an IT Service Provider to resolve many Incidents in an efficient manner by correcting the underlying root-cause.

Why do some Problems not get diagnosed?
- Because the root cause is not always found.

Why do some Known Errors not get fixed?
- Because we may decide that the costs exceed the benefits of fixing the error or
- Because it may be fixed in an upcoming patch from a Supplier, e.g. Windows patch or update.
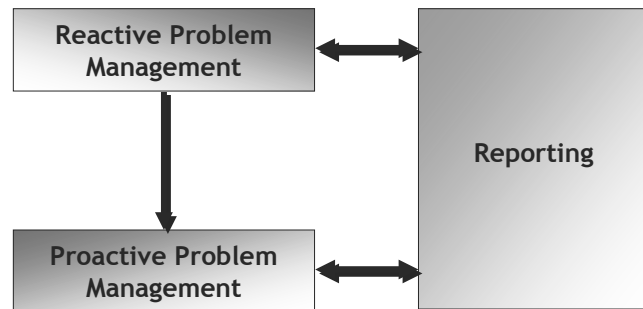
Two Sub-Processes of Problem Management

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

The activities of Problem Management are carried out within the Proactive and Reactive Problem Management. The main goal of Proactive Problem Management is to identify errors that might otherwise be missed. Proactive Problem Management analyses Incident Records, an d use s data co llected by ot her I T S ervice Management pr ocesses and external sources to identify trends or significant problems.
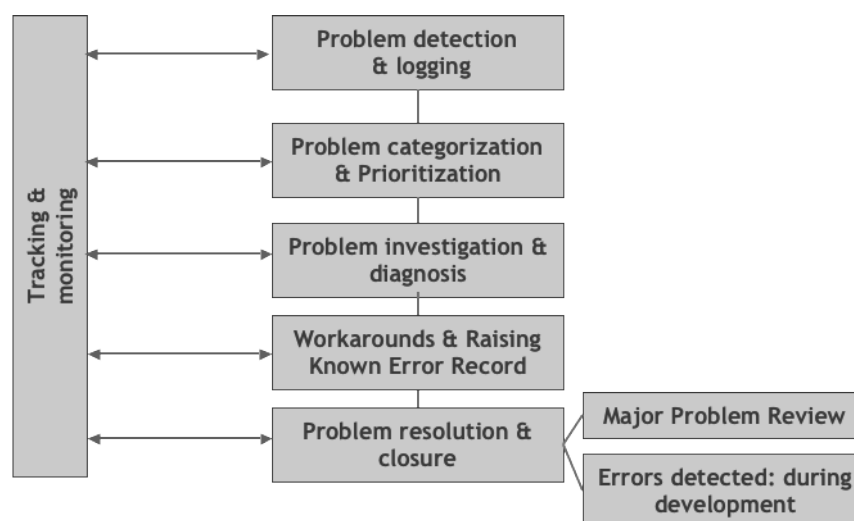
Reactive Problem Management

Figure 7.K – The activities of Reactive Problem Management

The act ivities of R eactive P roblem M anagement ar e si milar t o t hose o f I ncident Management for t he l ogging, ca tegorization and cl assification f or P roblems. The subsequent activities are di fferent as this is where t he act ual r oot-cause a nalysis is performed and the Known Error corrected.

Major Problem Review

After every major problem, while memories are still fresh a review should be conducted to learn any lessons for the future. Specifically the review should examine:

- Those things that were done correctly
- Those things that were done wrong
- What could be done better in the future?
- How to prevent recurrence
- Whether there has been any third-party responsibility and whether follow-up actions are needed.

Such r eviews can b e use d as par t o f t raining and awareness activities for st aff – any lessons learned sh ould be d ocumented i n appropriate pr ocedures, w orking i nstructions, diagnostic scripts or Known Error Records.

Proactive Problem Management

The two main activities of Proactive Problem Management are:

- **Performing a Trend Analysis**
  - o Review reports from other processes (e.g. Incident, Availability Management)
  - o Identify recurring Problems or training opportunities.
- **Targeting Preventative Action**
  - o Perform a cost - benefit analysis of all costs associated with prevention
  - o Target specific areas taking up the most support attention

Roles and Responsibilities

Problem Manager

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

Skills:

- Business knowledge,
- Lateral thinker, coordination skills.

Problem M anagement Te am (including Application a nd Te chnical M anagement functions)

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

Skills:

- Analytical, technical, business knowledge

7.4.4   Request Fulfillment

Goal: To pr ovide an effective and e fficient ch annel f or us ers to m ake r equests, g ain information and obtain standard Services.

A Service Request is:
- A request for information or advice
- A request for a *standard* change
- A request for access to an IT Service

Standard Change: E.g. User asking for a password reset or for the provision of standard IT services. These are usually handled by the Service Desk and do get implemented via the normal steps of Change Management.

Roles and Responsibilities:
Request F ulfilment i s pr imarily ca rried out by t he S ervice D esk F unction, but i s also assisted by other teams within the IT organization.

Just like Change Management, to assist with Request Fulfilment many organizations will wish to create pre-defined Request Models. These would typically include some form of pre-approval by Change Management.

7.4.5   Access Management

Goal: To *grant* authorized users the right to use a Service while *preventing* access to non-authorized use rs in order t o pr otect t he c onfidentiality, i ntegrity and av ailability (CIA) of information and infrastructure.

Relationship with other Processes

Access Management i s the ex ecution o f pol icies and act ions de fined i n I nformation Security and Availability Management.
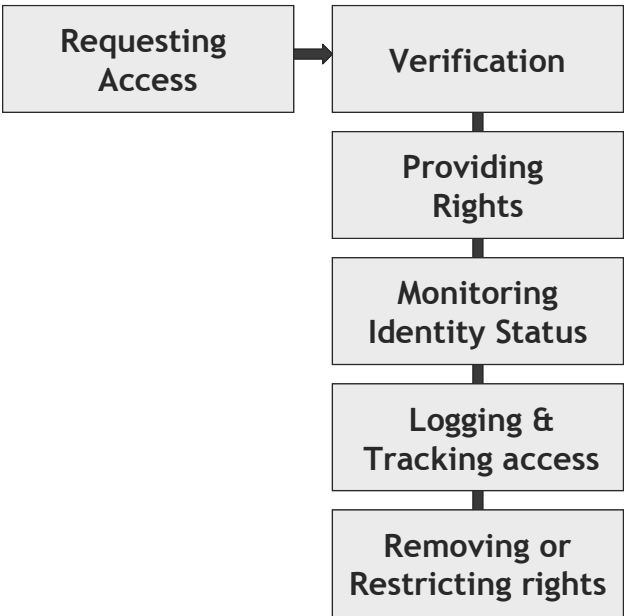

Figure 7.L – Access Management Activities

Figure 7. L dem onstrates the l ifecycle f or m anaging acce ss to se rvices, i nformation and facilities.

7.4.6   Implementation

This section focuses on generic implementation guidance for Service Operation as a whole.

Managing Change in Service Operation

The purpose of Service Operation is to achieve stability. Service Operation staff must ensure that changes are absorbed without adverse impact upon the stability of the IT services.

Change Triggers

There are many things that can trigger a change in the Service Operation environment. They include:

- New or upgraded hardware or network components
- New or upgraded applications software
- New or upgraded system software (operating system, utilities, middleware etc. including patches and bug fixes)
- Legislative, conformance or governance changes
- Obsolescence – some components may become obsolete and require replacement or cease to be supported by the supplier/maintainer
- Business imperative – you have to be flexible to work in ITSM, particularly during Service Operation, and there will be many occasions when the business needs IT changes to meet dynamic business requirements
- Enhancements to processes, procedures and/or underpinning tools to improve IT delivery or reduce financial costs
- Changes of management or personnel (ranging from loss or transfer of individuals right through to major take-over's or acquisitions)
- Change of service levels or in service provision – outsourcing, in-sourcing, partnerships, etc.

Change Assessment

In order to ensure that operational issues are taken into account, Service Operation staff must be involved in the assessment of all changes. This involvement should commence as soon as possible to ensure that they have influence over fundamental decisions. The Change Manager must inform all affected parties of the change being assessed in order for input to be prepared and available prior to Change Advisory Board meetings.

It is important that Service Operation staff are involved in the latter stages of the process, as they may be involved in the implementation and wish to ensure that careful scheduling takes place to avoid potential contentions or particularly sensitive periods.

Measurement of Successful Change

The ultimate measure of the success of changes made to Service Operation is that customers and users do not experience any variation or outage of service. The effects of change should be invisible where possible, aside from

any enhanced functionality, quality or financial savings resulting from the change.

Service Operation and Project Management

Service Operation is often viewed as 'business as usual' and focused on executing defined procedures in a standard way. Because of this, there is a tendency not to use Project Management processes when they would be appropriate. For example, major infrastructure upgrades, or the deployment of new or changed procedures, are significant tasks that should utilize formal Project Management to improve control and manage costs/resources.

Using Project Management to manage these types of activity would have the following benefits:

- The project benefits are clearly stated and agreed
- There is more visibility of what is being done and how it is being managed, which makes it easier for other IT groups and the business to quantify the contributions made by operational teams
- This in turn makes it easier to obtain funding for projects that have traditionally been difficult to cost justify
- Greater consistency and improved quality
- Achievement of objectives results in higher credibility for operational groups.

Assessing and Managing Risk in Service Operation

There are a number of occasions where it is imperative that risk assessment to Service Operation is undertaken and acted upon quickly.

Assessing the risk of potential changes or Known Errors is the most obvious area. Service Operation staff may also need to be involved in assessing the risk and impact of:

- Failures, or potential failures – either reported by Event Management or Incident/Problem Management, or warnings raised by manufacturers, suppliers or contractors
- New projects that will ultimately results in delivery into the live environment
- Environmental risk (encompassing IT Service Continuity-type risks to the physical environment and locale as well as political, commercial or industrial-relations related risks)
- Suppliers, particularly where new suppliers are involved or where key service components are under the control of third parties

- Security risks – both theoretical or actual arising from security related incidents or events
- New customers/services to be supported.

Operational Staff in Service Design and Transition

All IT groups will be involved during Service Design and Service Transition to ensure that new components or service are designed, tested and implemented to provide the correct levels of functionality, usability, availability, capacity, etc.

During the early stages of Service Design and Service Transition, Service Operation staff must be involved to ensure that when new services reach the live environment, they are fit for purpose and are 'supportable' in the future.

In this context, 'supportable' means:

- Capable of being supported from a technical and operational viewpoint from within existing, or pre-agreed additional resources and skills levels
- Without adverse impact on other existing technical or operational working practices, processes or schedules
- Without any unexpected operational costs or ongoing or escalating support expenditure
- Without any unexpected contractual or legal complications
- No complex support paths between multiple support departments of third-party organizations.

Note: Change is not just about technology. It also requires training, awareness, cultural change, motivational issues and more.

Planning and Implementing Service Management Technologies

In order to plan for in readiness for, and during deployment and implementation of, ITSM support tools, organizations need to consider the following factors.

Licences

The overall cost of ITSM tools is usually determined by the number and type of user licences required.

Often sold in modular format, the exact functionality of each module needs to be well understood. Initial sizing must be conducted to determine the number and type of users that will need to access each module.

Licences are often available in the following types:
Dedicated Licences

Staff that require frequent and prolonged use of the module will use dedicated licences. For example, Service Desk staff will need a dedicated licence to use an Incident Management module.

Shared Licences

For staff that make fairly regular use of the module, but not on a day-to-day basis, a shared licence will usually suffice. For example, third-line support staff may need regular access to an Incident Management module, but only when an incident record is being updated. It is important to estimate the ratio of required licences depending on the number of potential users, the length of periods of use and the expected frequency between usages.

The cost of a shared licence is usually more expensive than that of a dedicated licence. However, due to the nature of a shared licence, fewer are required and therefore the cost will be less.

Web Licences

Web licences allow some form of 'light interface' via web access to the tool capabilities. They are usually suitable for staff requiring remote access, occasional access or usage of just a small subset of functionality. For example, engineering staff may wish to log details of actions taken on incidents.

The cost of a web licence is usually a lot less than other licences, as the ratio of use is often much lower.

It is important to note that some staff may require access to multiple licences. For example, support staff may require a dedicated or shared licence during the day, but may require a web licence for out of hours support.

Service on Demand

There is a trend within the IT industry for suppliers to offer IT applications 'on demand', where access is given to the application for a period of demand and then severed when it is no longer required. This may be useful either for smaller organizations or if the tools in question are very specialized and used infrequently.

Alternately, the use of a tool can be offered as part of a specific consultancy assignment. For example, a specialist Capacity management consultancy may offer a regular but relatively infrequent Capacity Planning consultancy package and provide use of the tools for the duration of the assignment. Licence fees are likely to be included as part of, or as an addendum to, the consultancy fee.

A further variation is where software is licensed and charged on an agent/activity basis. An example of this is interrogation/monitoring and/or simulation software. For example, agent software that can simulate pre-defined customer paths through an organization's website to assess and report upon performance and availability. This type of software is typically charged based on the number of agents, their location and/or the amount of activity generated.

Full investigations of the licensing structure must be investigated and well understood before the tools are deployed.

Deployment

Before many ITSM tools can be used, particularly Discovery and Event Monitoring tools, they require some client/agent software deploying to all target locations. This needs careful planning and execution, and should be handled through formal Release and Deployment Management.

Careful scheduling and testing is needed even where network deployment is possible. Records must be maintained throughout the rollout so that support staff have knowledge of who has been upgraded and who has not. Interim Change Management may be necessary and the CMS should be updated as the rollout progresses.

The reboot of the devices for the client software to be recognized is often necessary and needs to be arranged in advance. Long delays can occur if staff do not generally switch off their desktops overnights. Further arrangements may also be necessary for staff to log on and receive new software.

Capacity Checks

In order to ensure that all of the target locations have sufficient storage and processing capacity to host and run the new software, Capacity Management may be needed in advance. Those that cannot will need upgrading or renewal and lead times for this must be included in the plans.

The capacity of the network should also be checked to establish whether it can handle the transmission of management information, log files and the distribution of clients and possibly software and configuration files.

Timing of Technology Department

Care is needed in order to ensure that tools are deployed at the appropriate time in relation to the organization's level of ITSM sophistication and knowledge. It may be seen as an immediate panacea if tools are deployed too soon and any necessary action to change processes, working practices or attitudes may be hindered or overlooked.

The organization must first examine the processes that the tool is seeking to address and also ensure that staff are 'brought in' to the new processes and way of working and have adopted a 'service culture'.

However, tools are tangible and can, and often do, make things a reality for many people. Technical staff can immediately see how the new processes can work and the benefits they may provide.

Without adequate tooling, some processes simply cannot be done. There must be a careful balance to ensure that tools are introduced when they are needed and not before.

Care is also needed to ensure that training in any tools is provided at the correct point. If the training is too early, knowledge will be diminished or be lost. However, staff will need to be formally trained and fully familiarized with the operations of the tools well in advance of live deployment. Additional training should be planned as needed once the tools go live.

Type of Introduction

A decision is needed on what type of introduction is needed – whether to go for a 'Big Bang' introduction or some sort of phased approach. A phased approach is more likely to be necessary as most organizations will not start from a 'green field' situation and will have live services to keep running during the introduction.

In most cases, a new tool will be replacing an older, less sophisticated tool. Therefore the changeover between the two must be considered. This often involves deciding what data needs to be carried forward from the old to the new tool and may require significant reformatting to achieve the required results. Ideally this transfer should be done electronically. However, a small amount of re-keying of live data may be inevitable and should be factored into the plans. Older tools generally rely on more manual entry and maintenance of data. For this reason, an audit should be performed to verify data quality when electronic data migration is being used.

Where data transfer is complicated or time consuming to achieve, an alternative might be to allow a period of parallel running. This involves the old tool being available for an initial period alongside the new one. It is advised that the old tool be made 'read-only' in order to ensure that no mistakes can be made logging new data into the old tool.

7.5   Service Operation Summary

From a cu stomer v iewpoint, S ervice O peration i s where act ual v alue i s seen. This is because it is the execution of strategies, designs and plans and improvements from the Service Lifecycle phases.

Key benefits delivered as a result of Service Operation are:
- Effectiveness and efficiency in IT Service delivery and support
- Increased return on investment

Other benefits can be defined as:
1. **Long t erm:**   Over a period o f t ime t he S ervice O peration p rocesses, f unctions performance a nd output are ev aluated. These r eports will be anal yzed an d decisions made a bout w hether t he i mprovement i s needed, an d how best t o implement it through Service Design and Transition. E.g. deployment of new tools, changes to process designs, reconfiguration of the infrastructure.

2. **Short t erm:** improvement o f w orking pr actices within t he S ervice O perations processes, functions and t   echnology itself. G enerally t hey   involve sm aller improvements that do not mean changes to the fundamental nature of a process or technology. E.g. tuning, training, personnel redeployment etc.
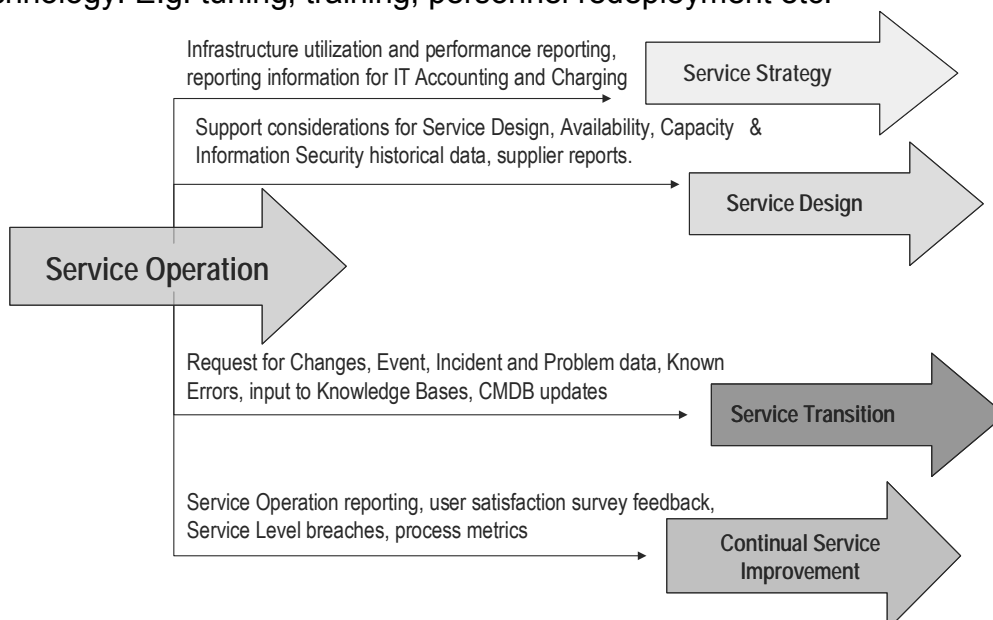

Figure 7.M – Some outputs to other lifecycle phases.

7.6 Service Operation Scenario

Functions

Service Desk
- Service desk has been trained in HYPE and can support users.
- Has access to known errors and workarounds to resolve incidents

Technical Management
- Designed, built, tested and rolled HYPE out into live environment
- Supports HYPE service

Application Management
- Made modifications to HYPE application to ensure effectively interfaced with XY app.
- Provided training on HYPE to users and Service Desk

IT Operations Management
- creates backups of logs, monitors component events

Processes

Event Management
- sends alerts to IT Ops when HYPE logs backups pass/fail
- monitors thresholds for triggers on bandwidth (set up in Availability Management)
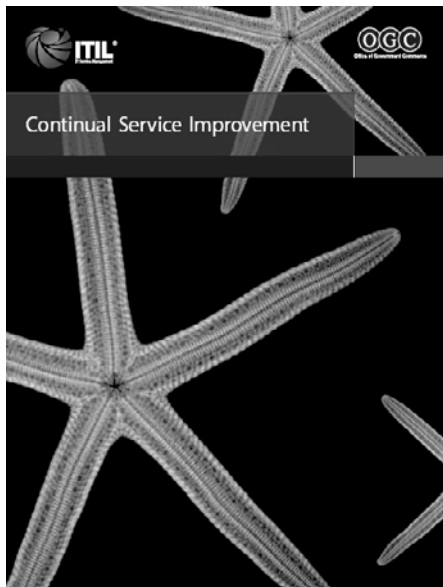
Request Fulfillment Management
- users use this process to request copy of logs

Access Management
- password reset of HYPE account – provide authorized users access

Incident Management and Problem Management will not be discussed in this example.

8 Continual Service Improvement

Processes:
- Service Level Management*
- Service Measurement & Reporting
- CSI Improvement Process

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

8.1 Objectives

To ensure continual improvements to IT Service Management Processes and IT Services.

Continual Service Improvement is the phase that binds all the other elements of the Service Lifecycle together and ensures that both the service and the IT Service Provider continually improves and matures.

8.2   Major Concepts

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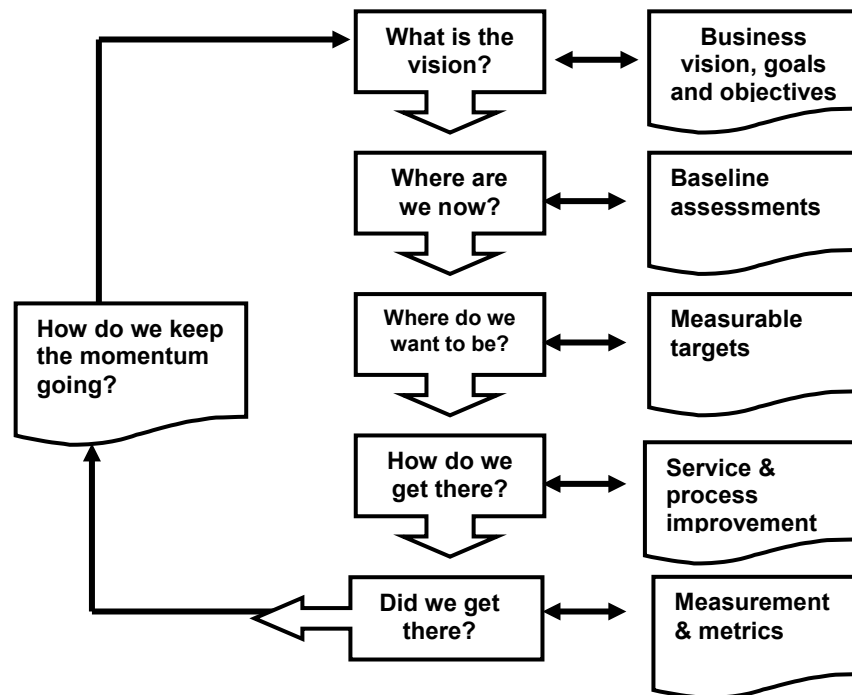

Figure 8.A – Continual Service Improvement Model.

The C ontinual S ervice I mprovement M odel su mmarizes the co nstant cy cle f or improvement. The questions require close interactions with all the other ITIL® processes in order to achieve Continual Service Improvement.

Relationships within the Service Lifecycle:
- **What is the Vision?** Service Strategy, Service Portfolio
- **Where ar e we n ow?** Baselines t aken using S ervice P ortfolios, S ervice Lev el Management, and Financial Management for IT etc.
- **Where do we want to be?** Service Portfolio, Service Measurement and Reporting.
- **How do we get there?** CSI and all ITIL® processes!
- **Did we get there?** Service Measurement and Reporting
- **How do we keep the momentum going?** Continual Service Improvement.

8.3 Continual Service Improvement Processes

8.3.1 Service Level Management

GOAL: To ensure that that the levels of IT service delivery are achieved, both for existing services and new services in accordance with the agreed targets.

Service Level Management is a critical element of Continual Service Improvement. Why embark on any se rvice i mprovement i nitiative i f t he cu stomers and the business are satisfied with the levels of service received? Because business requirements change!
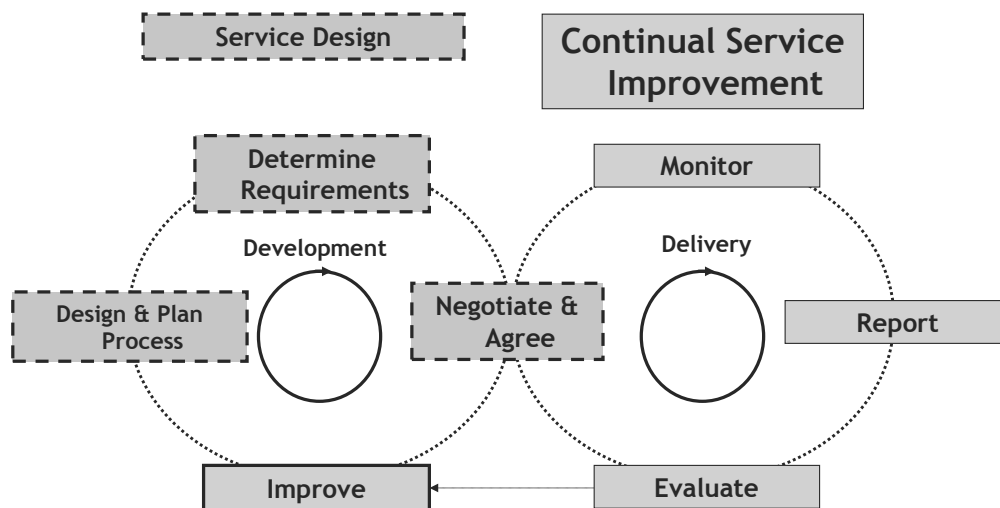
Activities

Figure 8.B – The Activities of Service Level Management

Service Level Management (SLM) is a process that is found within two Service Lifecycle phases.

Within Service Design, Service Level Management is concerned with:
- Design and plan the process
- Determining Service Level Requirements (SLR's)
- Negotiating and Agreeing upon SLAs, OLAs and UCs.

Within C ontinual S ervice I mprovement, S ervice Level M anagement i s co ncerned with improving services and processes through constant:
- Monitoring (executed within Service Operation)
- Reporting
- Evaluating
- Improving

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

Service Improvement Plans

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

The identified improvements may come from:
- breaches of Service Level Agreements
- identification of user training and documentation issues
- weak system testing
- identified weak areas within internal and external support groups.

Roles and Responsibilities

Service Level Manager:
- Must be se nior en ough t o r epresent or ganization; w ith *authority* to do w hat i s necessary
- Manages Service Catalogue, SLAs, UCs, OLAs
- Identifies and manages improvements to services and processes
- Analyses and reports on SL Achievements

Skills:
- Relationship Management
- Patience, tolerance and resilience
- Understanding of the Customer's business and how IT contributes to the delivery of that product or service

Challenges Affecting Service Level Management:

- Monitoring of pre-SLA achievements
- Targets that are achievable
- SLAs based on desire and not achievable targets
- Insufficient focus, resources and time
- Inadequate seniority of SLM staff
- Underpinning contracts ignored
- SLAs too long, not customer focused
- Improvement actions not adhered to

Key Performance Indicators of Service Level Management

Statistics:

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

Yes/Why Questions:

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

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

If the answer is no:

If the answer is "No" to any of these questions, the very next question that should be asked is "Why?"

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

8.3.2   Service Measurement and Reporting

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

There are four main reasons to monitor and measure:

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

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

Types of Metrics:

There are 3 types of metrics that an organization will need to collect to support CSI activities as well as other process activities:

- **Technology Metrics:** often associated with component and application-based metrics such as performance, availability etc

- **Process Metrics:** Captured in the form of KPIs and activity metrics for the service management processes. They help to determine the overall health of a process. 4 key questions KPIs can help answer are centered around quality, performance, value and compliance. CSI uses these metrics to identify improvement opportunities for each process.

- **Service Metrics:** The results of the end-to-end service. Component metrics are used to calculate the service metrics.

Baselines:

A benchmark used as a reference point for later comparison.

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

Examples

1. A Service Level Achievement Baseline can be used a starting point to measure the effect of a Service Improvement Plan.
2. A performance Baseline can be used to measure changes in performance over the lifetime of an IT service.
3. A Configuration Management baseline can be used to enable the IT infrastructure to be restored to a known configuration if a change or release fails.

8.3.3 CSI (7 Step) Improvement Process

GOAL: To coordinate a st ructured approach for improvements to IT services and ITSM processes

The Deming Cycle: A foundation for continual improvement:
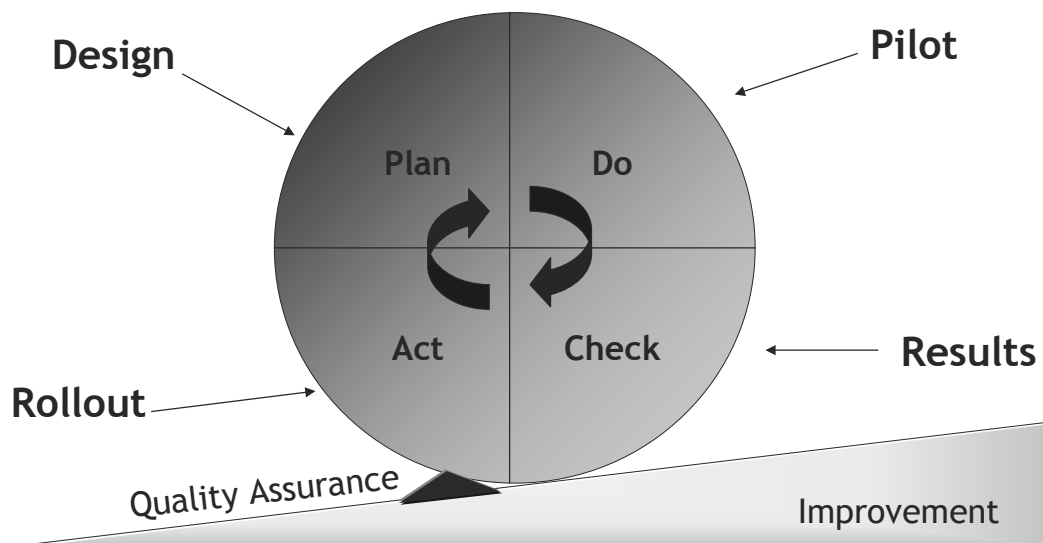
Source: Deming

Figure 8.C – The Deming Cycle

Continuous improvement i s a p art o f ev ery pr ocess in I TIL®. The C SI I mprovement Process is based on the Deming Cycle of Continual Improvement (Plan, Do, Check, Act)

Implementing I TIL®/ITSM i s an ong oing act ivity, where y ou i mprove q uality t hrough incremental steps. These four steps are carried out in the exact order, as many times as necessary in order to achieve the improvement desired.

Some of the items that occur during each of the 4 phases:
- **Plan:**   Scope, requirements, objectives, Roles and Responsibilities
- **Do:**   Funds, Policies, reports, managing, changing
- **Check:**   Monitor against plans, survey, report
- **Act:**   Policy on improvement, assess, implement (if appropriate)

Notes on William Edwards Deming:

An American statistician best known for his work in Japan in the post-WWII period. There, from 1950 onward he taught top management how to improve design (and thus service), product q uality, t esting and sa les (the l ast t hrough g lobal markets). D eming m ade a significant contribution to Japan's later renown for innovative high-quality products and its economic power.
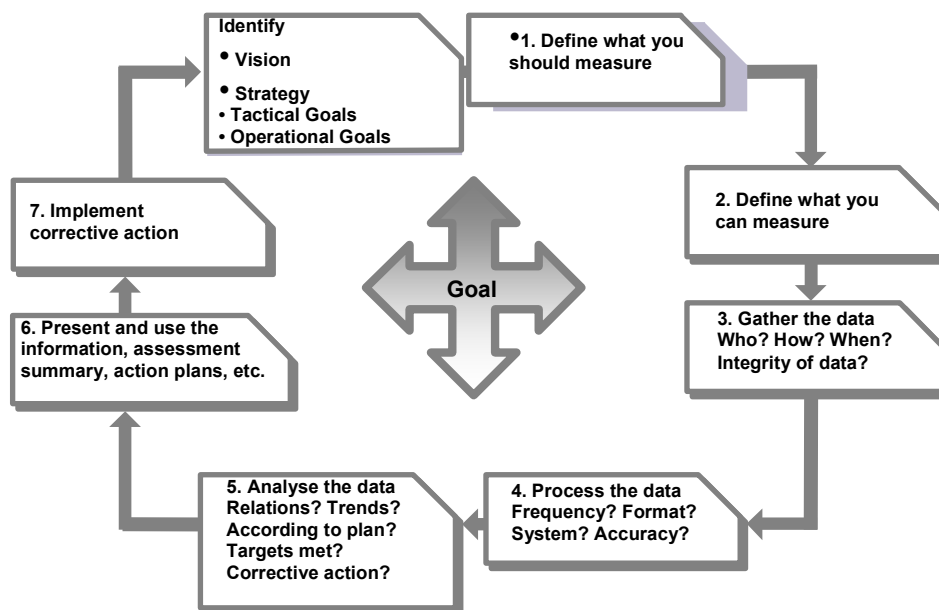

Figure 8.D – The CSI (7 Step) Improvement Process

The Deming Cycle is transformed into more detailed steps and actions to be taken for the improvement o f I T se rvices and I T S ervice M anagement pr ocesses. Li ke t he D eming Cycle, these steps need to be taken in sequential order, as many times as necessary to drive the improvement desired.

8.3.4   Methods & Techniques

An effective choice of methods and techniques for the analysis, presentation and use of the measurement information is highly dependent on the particular circumstances in which these tasks are performed and can generally not be documented in advance.

A goal oriented attitude and professional expertise and education of the individuals are required.

Effort Cost

CSI improvement activities can require a considerable amount of effort and money for larger-scale improvement projects versus minimal time and effort for some more incremental improvements.
It is up to the business and IT to decide if the costs and effort is worth it.

Costs associated with implementing and operating a measurement framework would include:
• Labour costs
• Tooling costs
• Training costs
• Expertise costs

When deciding whether the measurement framework is worth the effort, consider the budget for:

Implementation of the measurement framework, initially and if it changes – in practice these types of costs can be reliably estimated and controlled by using a project-oriented approach.

Operation - the level of costs associated with the operation of the measurement framework is largely fixed as a result of the way it is designed and equipped.

Maintenance – The level of these types of costs depends mainly on the expected rate at which the measurement framework will require adaption to changing circumstances and on the quality of its implementation.

Implementation review and evaluation
Implementation review and evaluation is key to determining the effectiveness of a CSI improvement program.

Some common areas for review include:
• Did we correctly assess the current situation and define the problem statement?
• Did we commit to the right goals?
• Did we make the right decisions when developing the strategy for improving IT services?
• Did we implement the strategy correctly?
• Have we improved the IT service provision?
• What lessons did we learn, where are we now?

Review and evaluation of a CSI initiative fall within two main categories:
• Issues closely tied to the original problem situation with respect to the IT service provision to the business and ensuring business aims and the improvement strategy for the improvement
• Issues in relation to the planning, implementation and proceedings of the IT improvement program itself and associated projects such as measurements, problems, actions and changes.

Assessments
Formal mechanisms for comparing the operational process environment to the performance standards for the purpose of measuring improved process capability and/or identify potential shortcomings that could be addressed.

The benefit of assessments is that they provide the opportunity to sample specific elements of a process which impacts the efficiency and effectiveness of the process.

Assessments can be conducted at any time. A way to think about assessment timing is in line with the improvement lifecycle:

- **Plan** – Assess the targeted processes at the interception of process introduction to form the basis for a process improvement project.
- **Plan** – A check during process implementation or improvement activities serves as validation that process project objectives are being met and provide tangible evidence that benefits are being achieved from the investment of time, talent and resources to process initiatives.
- **Do/Check** – During conclusion of the process project, it is important to validate the maturation of the process though the efforts of the project team. In addition, scheduling periodic reassessments can support the overall organization integration and quality efforts.

Assessment scope

The assessment's scope is one of they key decisions. Scope should be based on the assessments' objective and the expected future use of process assessments and assessment reports.

There are 3 potential scope levels:

Process only –assessment only of process attributes based on general principles and guidelines of the process framework which defines the subject process.

People, process and technology – extends the process assessment to include the assessment of skills, roles and talents of the mangers and practitioners of the process as well as the ability of the process enabling technology deployed to support the objectives and transaction state of the process.

Full assessment – Extends to include an assessment of the culture of acceptance within the organization, the ability of the organization to articulate a process strategy, the definition of a vision for the process environment as an 'end state', the structure and function of the process organization, the ability of process governance to assure the process objectives and goals are met, the effectiveness of process reporting/metrics and the capacity and capability of decision-making practices to improve process over time.

All these factors are compared to the maturity attributes of the selected maturity model.

Advantages and disadvantages of assessment:

Advantages:
- Provide objective perspective
- Compare to standard maturity model and process framework
- Accurate determination of process gaps
- Recommend actions and plan solutions
- Repeatable process

Disadvantages:
- Only provides a snapshot
- Does not reflect current business or cultural dynamics and process operational issues
- If the assessment process is outsourced can be vendor or framework dependent
- If this is the case, it is difficult to compare to industry standards
- Subject to the opinion of assessors

## Value of processes vs. maturity of processes
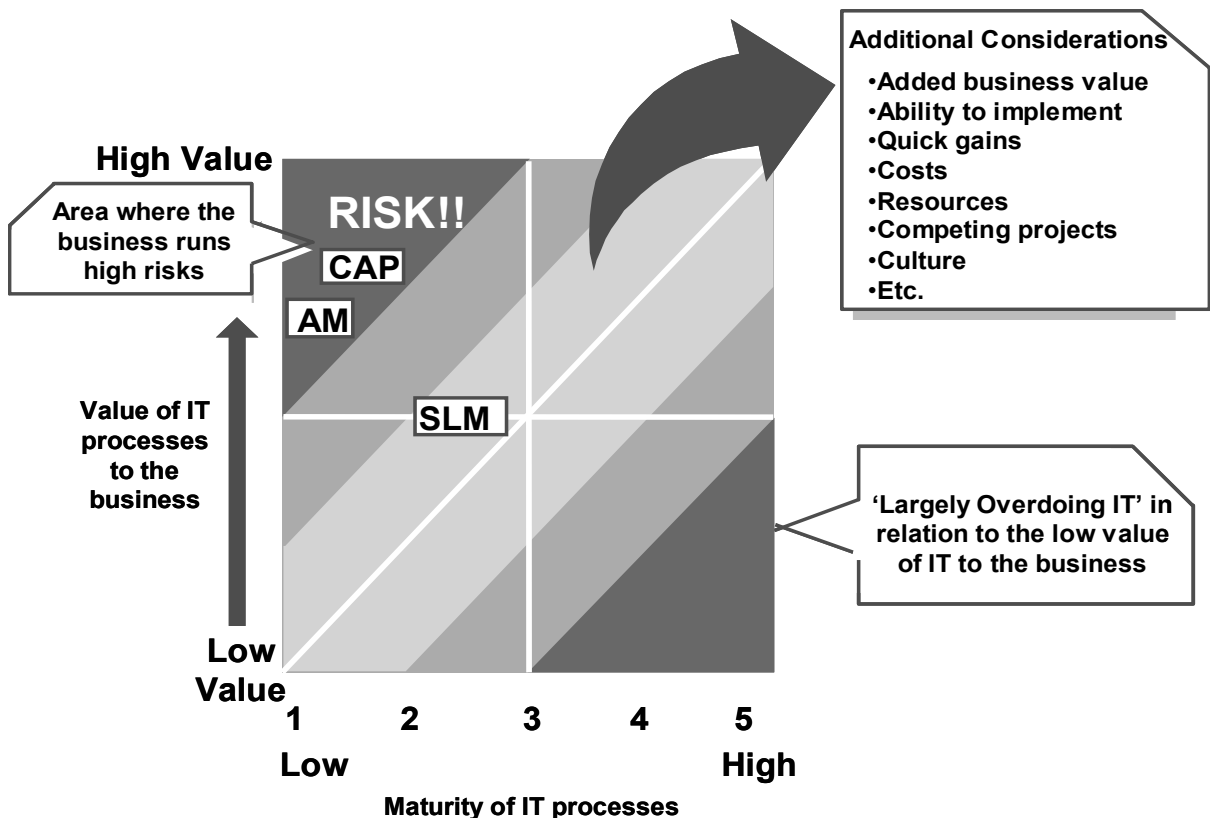
This diagram shows the value process in comparison to its maturity. For service management process improvement projects one of the many questions asked should be around how mature we need our process to be. The answer refers back to the business.

In this example the organization has completed an assessment and found 3 processes (Service Level Management, Capacity Management and Availability Management) are not very mature. This organization is changing their strategy concerning how they sell and deliver their products and services to a web-based strategy. Because of the vital parts both Capacity and Availability Management will play the organization has to implement an improvement plan for increasing the maturity. Without these initiatives the organization is leaving itself open to risk.

Having a low SLM process maturity also will create some issues for CSI activities.

The maturity of a process should ideally fall in the 'safe' areas.

Gap Analysis
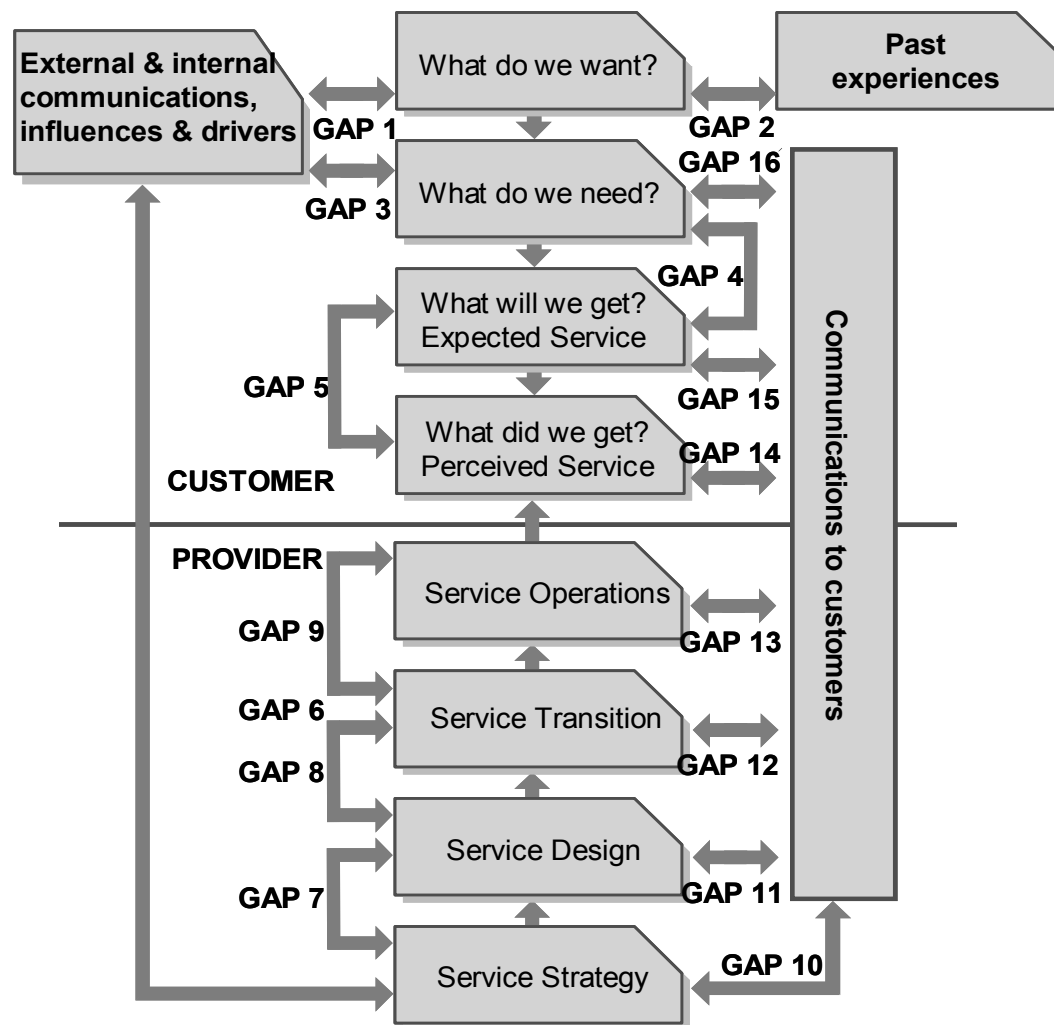
The Gap analysis process involves determining, documenting and approving the variance between business requirements and current capabilities. Gap analysis naturally flows from benchmarking or other assessments such as service or process maturity assessments'. Once the general expectation of performance is understood then it is possible to compare that expectation with the level of performance at which the company currently functions. This comparison becomes the gap analysis and can be conducted from different perspectives such as:

- Organization
- Business Direction
- Business Process
- Information Technology.

Gap analysis provides a foundation for how much effort in terms of time, money and human resources, is required to have a particular goal achieved.

Challenges

Each organization will have its own challenges, as with initiating any type of change one of the major challenges will be managing the behavioural changes that are required.

In addition, CSI will require adequate tools for managing the data, resources will need to be allocated and understand their roles and responsibilities as well as having the correct skills to execute the CSI activities.

Some common challenges that may be encountered are:
- Lack of management commitment
- Inadequate resources, budget and time
- Lack of mature processes
- Lack of information, monitoring and measurement
- Lack of Knowledge Management
- Resistance to planning and a reluctance to be proved wrong
- Lack of corporate objectives, strategies, policies and business direction
- Lack of IT objectives, strategies and policies
- Lack of knowledge and appreciation of business impacts and priorities
- Diverse and disparate technologies and applications
- Resistance to change and cultural change
- Poor relationships, cooperation and communication between business and IT
- Lack of tools, standards and skills
- Tools to complex and costly to implement and maintain
- Over commitment of resources with n associated inability to deliver
- Poor supplier management/poor supplier performance.

Critical Success Factor's
- Appointment of a CSI Manager
- Adoption of CSI within the organization
- Management commitment
- Defining clear criteria for prioritizing improvement projects
- Adoption of the service lifecycle approach
- Sufficient and ongoing funding for CSI activities
- Resource allocation
- Technology to support the CSI activities
- Adoption of processes

Risks
- Being over ambitious and unrealistic
- Not discussing improvement opportunities with the business
- Not focusing on improving both services and service management processes
- Not prioritizing improvement projects
- Implementing CSI with little or no technology
- Implementing a CSI initiative with no resources
- Implementing CSI without knowledge transfer and training
- Not performing all steps of the 7 Step Improvement Process
- Lack of management taking action
- Lack of communication/ awareness campaign
- Removing testing (or only partially testing) before implementation

Summary

Implementing CSI is a challenge; it requires a change in management and staff attitudes and values to ensure that all parties recognize CSI needs to be proactive and not reactive.

It is critical to identifying risks and challenges before implementing CSI.

Knowing the CSF's before undertaking the implementation of CSI helps to manage the risks and challenges.

One step at a time…..

8.3.5   Implementation

Critical consideration for implementing CSI

Before implementing CSI it is important to have identified and filled the critical roles that are required within this phase, such as CSI Manager, Service Owner and Reporting Analyst. A Service Level Manager is also needed to be the liaison between IT and the business.

Where to start?
One approach is to start looking at the handoff of output from the different lifecycle domains. The Service Design phase needs to monitor and report on their activities and by using trend analysis, identify relevant improvement opportunities. This needs to be done during every phase of the service lifecycle, especially during Service Design, Transition and Operation. The Continual Service Improvement phase is engaged in this activity.

Communication strategy and plan
Timely and effective communication forms an important part of any service improvement project. In an effort to transform an organization from performing CSI activities on an ad hoc basis to a more formal and ongoing CSI activities, it is crucial that staff, users and stakeholders are kept up to date of all changes to the processes, activities, roles and responsibilities.

The goal of the communications plan is to build and maintain awareness, understanding, enthusiasm and support among key influential stakeholders for the CSI program. When developing a communication plan, it is important to note that effective communication is not just based on a one-way flow of information, and it is more than just meetings. A communications plan must incorporate the ability to deal with responses and feedback from the targeted audiences.
The plan should include a role to:
  • Design and deliver communications to the different CSI roles, stakeholders such as other ITSM process roles and identified target audiences
  • Identify forums for customer and user feedback
  • Receive and deliver responses and feedback to the project manager and/or process team members.

Key activities for the communication plan include:
*   Identifying stakeholders and target audiences
*   Developing communication strategies and tactics
*   Identifying communication methods and techniques
*   Developing the communications plan
*   Identifying the project milestones and related communications requirements.

When developing the communication plan it is important to take into consideration the culture around communication within the business. In some organizations there are strict guidelines on who can communicate with the business. Often times this is through the Service Level Management and Business Relationship Management processes. No matter what the method, communicating with the business should be the key communication activity.

CSI & Organizational Change
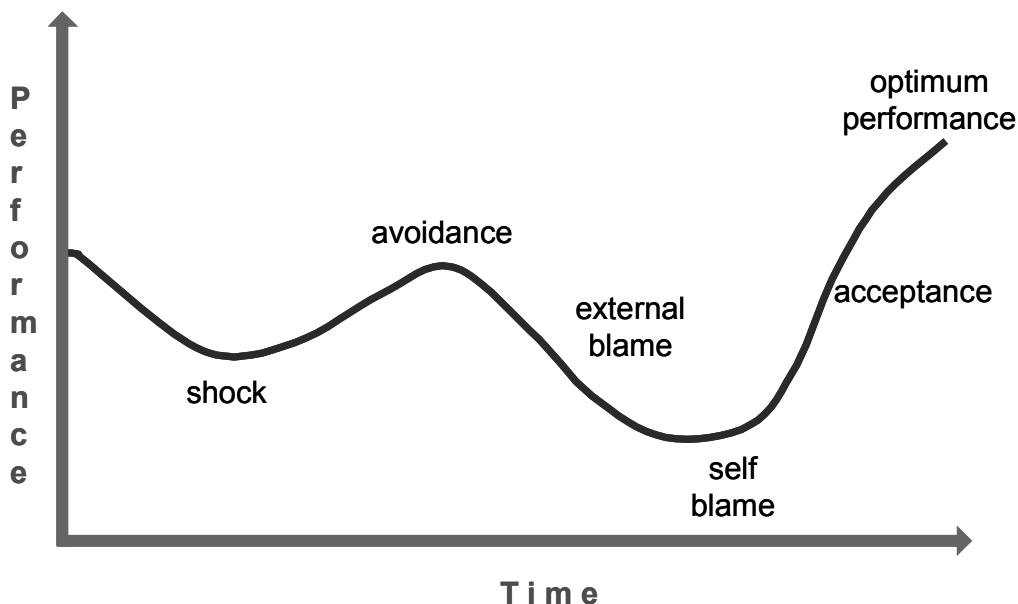
Many organizational change programs fail to achieve the desired results. People generally do not like change, so it is essential that benefits are explained to all parties to obtain and retain support as the change occurs. Communication is key to ensuring a smooth transition from old working practices to new ones. Those responsible for managing and steering the CSI program should consciously address these softer issues. Using an approach such as John P. Kotter's Eight Steps to Transforming your Organization, together with formalized project management skills and practices, will significantly increase the chance of success.

Kotter, Professor of Leadership at Harvard Business School, investigated more than 100 businesses that were involved with or had attempted a complete change program. From this research he identified the 'Eight

main reasons why transformation efforts fail' these reasons apply equally to ITSM implementation programs.

1. Create a sense of urgency
Half of all transformations fail to realize their goals due to the lack of adequate attention to this step. Not enough people buy into the fact that change is a must. It is essential that all parties understand the repercussions of not making the change as this will help to gain commitment and provide input to a business justification for investing in CSI.

2. Forming a guiding coalition
Experience shows a need for assembling a group with sufficient power to lead the change effort and work together as a team. Power means more than simply formal authority but also experience, respect, trust and credibility. This team is the guiding coalition for the CSI phase.

3. Creating a vision
This guiding coalition should be responsible for ensuring that a vision is produced describing the aim and purpose of CSI. A good vision statement can service four essential purposes:
   • Clarify the direction of the program
   • Motivate people to take action in the right direction
   • Coordinate the actions of many different people
   • Outline the aims of senior management.

4. Communicating the vision
Although the vision provides a powerful tool in helping guide and coordinate change, the real power is unleashed when the vision is effectively communicated to the stakeholders. Every stakeholder should understand the vision.

5. Empowering other to act on the vision
Establishing urgency, creating a guiding coalition, creating and communicating a vision are all aimed at creating and communicating a vision are all aimed at creating energy, enthusiasm, buy-in and commitment to enable successful change. In the empowering phase, two important aspects need to be stressed: enabling and removing barriers.

6. Planning for and creating short-term wins
Implementing service management improvements can be a lengthy program of change. It is important that during the program, short term wins are realized and are communicated. Short-term wins help to keep a change effort on track and help keep the energy and commitment levels high. Real transformation takes time. Without short-term wins, too many people give up or join the ranks of those opposed to change.

7. Consolidating improvements and producing more change
The success of short-term wins keeps the momentum going and creates more change. In CSI it is important to recognize short to medium and long term wins. Changes

should sink deeply into the new culture or the new approaches will be fragile and subject to regression:

- **Short-term wins** – have the characteristics of convincing, motivating and showing immediate benefits and gains
- **Medium-term wins** – have the characteristics of confidence and capability, and having a set of working processes in place.
- **Long-term wins** – have the characteristics of self learning and expertise, and fully integrated processes that have self-learning and improvement built into them.

8. Institutionalizing the change

Change needs to be institutionalized within the organization. Many changes fail because they are not consolidated into everyday practices. Institutionalizing change means showing how new working practices have produced real gain and benefits, and ensuring that the improvements are embedded in all organizational practices.
Often the CSI team is disbanded before the working practices are institutionalized; there is danger that people may revert to old working practices, but this can not be allowed to happen. CSI must be a way of life not e reaction to a failure of some description.

8.4 Continual Service Improvement Summary

There is great value to the business when service improvement takes a holistic approach throughout the ent ire lifecycle. C ontinual S ervice I mprovement enabl es this holistic approach to be taken.

Some key benefits of the Continual Service Improvement phase:
- Increased growth
- Competitive Advantage
- Increased Return On Investment
- Increased Value On Investment

ROI: Return on i nvestment – Difference between the benefit (saving) achieved and the amount expended to achieve that benefit, expressed as percentage. Log ically we would like to spend a little to save a lot.

VOI: Value on investment – Extra value created by establishment of benefits that include non-monetary or long term outcomes. ROI is a subcomponent of VOI.
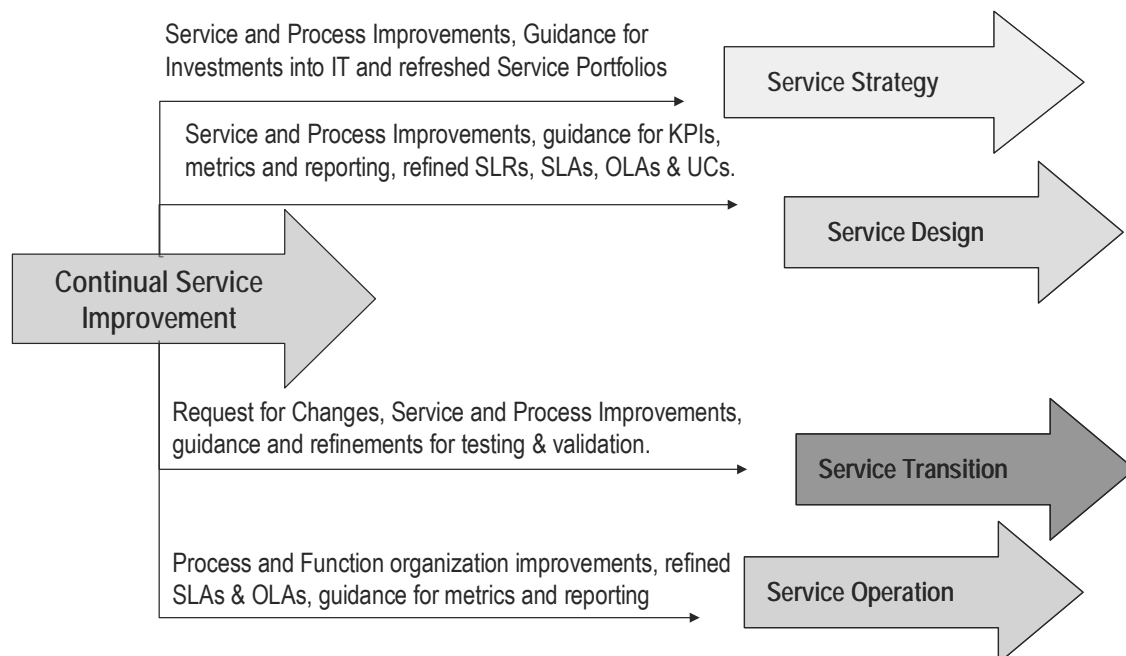
Figure 8.E – Some outputs to other lifecycle phases.

8.5   Continual Service Improvement Scenario

Service Level Management

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

Service Measurement and Reporting

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

CSI Process

The CSI improvement model was used as a roadmap for this SIP. As the business needs changed, so too has their perceived value of HYPE. HYPE had become an integral part of the business communication plan. As a result, new business plans/goals were established and new targets set, with an action plan for improvement… at a cost of course.
This will identify:
- Technology improvements
- Process improvements
- Document improvements
- Training etc

 And so it continues!

9   Glossary

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

Asset: Any resource or capability.

Application S izing: Determines the h ardware or net work capacity t o su pport n ew 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 t eam or group of p eople an d t he t ools they use t o 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 m easure of h ow q uickly and e ffectively a C I or I T se rvice ca n be restored to normal after a failure.

Modelling: A technique used to predict the future behaviour 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/CI's 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.

.

10 Certification

10.1 ITIL® Certification Pathways

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.
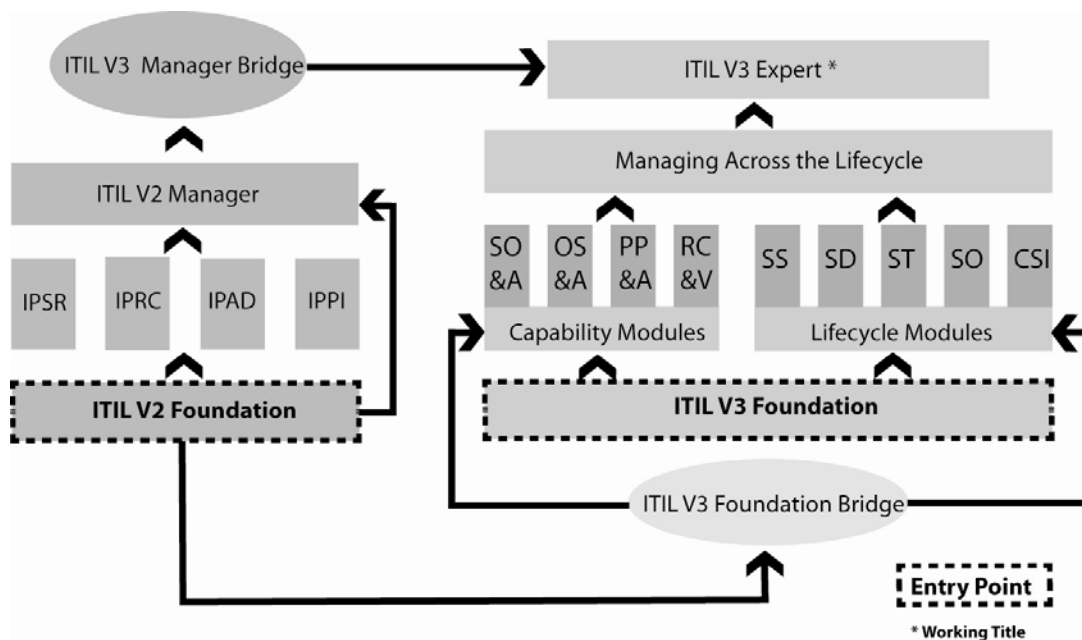

Figure 12.A – ITIL® Certification Pathway

10.2 ISO/IEC 20000 Pathways

ISO/IEC 20000 Standard is becoming a basic requirement for IT Service providers and is fast becoming the most recognized symbol of quality regarding IT Service Management processes. Once you have acquired your ITIL® Foundation Certification, you are eligible to pursue the ISO/IEC 20000 certification pathways. ISO/IEC 20000 programs aim to assist IT professionals master and understand the standard itself and issues relating to earning actual standards compliance.
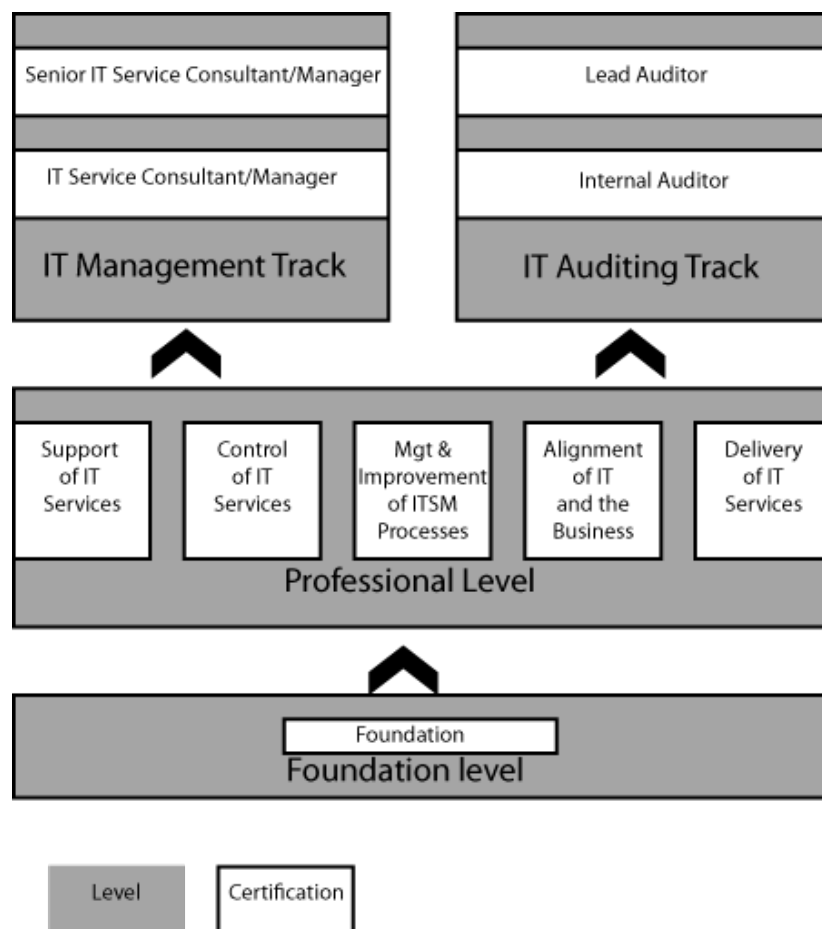

Figure 12.B – ISO/IEC 20000 Certification Pathway