



## ITIL Foundation for IT Service Management

h1846s i.00

HP Training

# Student guide

© Copyright 2005 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This is an HP copyrighted work that may not be reproduced without the written permission of HP. You may not use these materials to deliver training to any person outside of your organization without the written permission of HP.

Printed in US

**ITIL Foundation for IT Service Management**

Student guide

January 2005

---

## Contents

### Module 1 — Introduction

IT Service Management .....	1-2
Course Format.....	1-4
IT Service Management Foundation Certificate .....	1-5
IT Infrastructure Library (ITIL).....	1-7
IT Infrastructure Library (ITIL).....	1-8
ITIL Philosophy .....	1-10
Best Practice — A Working Definition.....	1-11
Where Does Best Practice Fit? .....	1-12
The Drivers for High Quality IT Services .....	1-13
The Balance between Quality and Cost.....	1-15
ITIL Objectives .....	1-16
Achieving High Quality.....	1-17
Continuous Improvement .....	1-18
Service Culture .....	1-20
Achieving a Service Culture.....	1-21
Who Is Doing This? .....	1-22
Benefits.....	1-23
What Is an IT Service? .....	1-24
Service Components.....	1-25
As Seen by the Customer/User... ..	1-26
Process Orientated Working.....	1-27
Core ITSM Components .....	1-28
Service Support Processes.....	1-30
Service Delivery Processes.....	1-31
Service Management.....	1-32

### Module 2 — Service Desk

Mission of Service Desk .....	2-2
Objectives of Service Desk .....	2-4
Common Features and Characteristics (1 of 2) .....	2-6
Common Features and Characteristics (2 of 2) .....	2-8
Staffing Options.....	2-10
Skills and Mindset .....	2-11
Service Desk Implementation.....	2-13
Local Service Desks .....	2-14
Central Service Desk .....	2-15
Virtual Service Desk .....	2-16
‘Follow the Sun’ Option.....	2-18
Information Routing .....	2-20
A Self-Service Strategy .....	2-21
Outsourcing the Service Desk — Potential Benefits .....	2-22
Outsourcing the Service Desk — Care Needed.....	2-23
Question (1 of 2).....	2-25
Question (2 of 2).....	2-26

## Contents

### Module 3 — Incident Management

Mission of Incident Management.....	3-2
Scope of Incident Management.....	3-3
Objectives of Incident Management.....	3-4
Inputs, Outputs, and Activities.....	3-5
Definition — an Incident .....	3-7
Definition — a Problem .....	3-8
Definition — a Known Error .....	3-9
Relationships among Incidents, Problems, Known Errors and Changes .....	3-10
Example Coding System for Incident/Request Classification.....	3-11
Impact + Urgency = Priority (1 of 2) .....	3-12
Impact + Urgency = Priority (2 of 2) .....	3-13
Example of a Priority Coding System .....	3-14
Incident Status — Examples .....	3-15
Escalation .....	3-16
Escalation Path .....	3-17
Functional Escalation .....	3-18
Hierarchical Escalation.....	3-19
Incident Manager Responsibilities .....	3-20
Service Desk Support Analyst Responsibilities .....	3-21
Second Line Support Staff Responsibilities .....	3-22
Question (1 of 2) .....	3-23
Question (2 of 2) .....	3-24

### Module 4 — Problem Management

Mission of Problem Management .....	4-2
Scope of Problem Management .....	4-3
Objectives of Problem Management .....	4-4
Core Elements.....	4-5
Incident Management and Problem Management .....	4-6
Problem Control .....	4-7
Error Control.....	4-8
Known Errors — Development.....	4-9
Problem Management Inputs, Activities, and Outputs .....	4-10
Previous Incident/Problem Data.....	4-11
Proactive Problem Management.....	4-12
Problem Management Techniques .....	4-13
Pain Value Analysis (1 of 2).....	4-14
Pain Value Analysis .....	4-15
Ishikawa Diagram.....	4-16
Question (1 of 2) .....	4-17
Question (2 of 2) .....	4-18

### Module 5 — Configuration Management

Mission of Configuration Management.....	5-2
Scope of Configuration Management.....	5-4
Objectives of Configuration Management .....	5-5
Core Elements of Configuration Management.....	5-6
Planning for Configuration Management.....	5-7
Identification .....	5-8
Naming Conventions .....	5-9
What Do We Need to Identify?.....	5-10

CMDB .....	5-12
Identifying CIs .....	5-13
Identifying CIs — Level of Breakdown .....	5-14
Identifying CIs .....	5-16
What Do We Need to Identify? (1 of 3).....	5-17
What Do We Need to Identify? (2 of 3).....	5-19
What Do We Need to Identify? (3 of 3).....	5-21
Configuration Management's Responsibility to License Management.....	5-22
Configuration Control (1 of 2).....	5-23
Configuration Control (2 of 2).....	5-25
Configuration Status Accounting.....	5-26
Configuration Audit and Verification .....	5-27
Managing the Support Cycle.....	5-28
Configuration and Change Management.....	5-31
Question (1 of 2).....	5-33
Question (2 of 2).....	5-34

## Module 6 — Change Management

Mission of Change Management .....	6-2
Scope of Change Management .....	6-3
Objectives of Change Management.....	6-5
Scalability.....	6-6
Core Elements .....	6-7
CAB Membership .....	6-9
Logging Changes — Normal .....	6-11
Assessing and Scheduling Normal Changes .....	6-13
Building and Implementing Normal Changes.....	6-15
Assessing and Scheduling Urgent Changes .....	6-17
Building and Implementing Urgent Changes.....	6-19
Urgent Change Review .....	6-20
Change Models (1 of 2).....	6-22
Change Models (2 of 2).....	6-23
Change and Program Management.....	6-24
Question (1 of 2).....	6-25
Question (2 of 2).....	6-26

## Module 7 — Release Management

Mission of Release Management .....	7-2
Scope of Release Management.....	7-4
Objectives of Release Management .....	7-6
Definition of a Release .....	7-7
Licensing Issues .....	7-8
Anti-Virus Controls .....	7-9
Definitive Software Library (DSL) .....	7-10
Definitive Software Library (DSL) .....	7-11
Definitive Hardware Store (DHS) .....	7-12
Release Policies.....	7-13
Release Scales .....	7-15
Full Release.....	7-17
Delta Release .....	7-18
Package Release.....	7-19
Elements.....	7-20

## Contents

Release Records.....	7-21
Release Management Activities (1 of 2).....	7-22
Release Management Activities (2 of 2).....	7-24
Question (1 of 2) .....	7-25
Question (2 of 2) .....	7-26
Service Support: Summary .....	7-27

## Module 8 — Service Level Management

Mission of Service Level Management.....	8-2
Scope of Service Level Management.....	8-4
Objectives of Service Level Management .....	8-5
The Service Level Management Process.....	8-6
Internal and External Documents .....	8-8
SLA Support Structure .....	8-9
Service-based SLA Structure .....	8-10
Customer-based SLA Structure.....	8-11
Multi-level SLAs .....	8-12
SLA Contents.....	8-13
SLA Contents.....	8-15
Example Service Catalog.....	8-16
Example SLAM/RAG Chart .....	8-17
Service Improvement Program .....	8-18
Integration with Other Disciplines .....	8-19
Question (1 of 2) .....	8-22
Question (2 of 2) .....	8-23

## Module 9 — Availability Management

Mission of Availability Management .....	9-2
Scope of Availability Management .....	9-3
Objectives of Financial Management .....	9-4
Key Concepts .....	9-5
Availability.....	9-6
Reliability.....	9-8
Maintainability, Serviceability, and Security .....	9-9
Service Agreements.....	9-11
MTBF, MTTR, and MTBSI .....	9-13
Availability Management and Incidents.....	9-14
Vital Business Function (VBF).....	9-15
Availability Components.....	9-16
Techniques and Tools .....	9-18
Example of CFIA .....	9-20
Fault Tree Analysis (FTA) .....	9-21
Resilience (1 of 2).....	9-22
Resilience (2 of 2).....	9-23
Question (1 of 2) .....	9-24
Question (2 of 2) .....	9-25

## Module 10 — Capacity Management

Mission of Capacity Management.....	10-2
Scope of Capacity Management.....	10-4
Objectives of Capacity Management.....	10-5
Capacity Management.....	10-6

Alignment of Technology and Business .....	10-7
Capacity Management Strategy .....	10-8
Areas of Responsibility .....	10-9
Capacity Management .....	10-10
Capacity Management Activities .....	10-12
Iterative Activities (1 of 2) .....	10-13
Iterative Activities (2 of 2) .....	10-15
Demand Management .....	10-16
Demand Management .....	10-17
The CDB .....	10-18
The CDB Inputs and Outputs .....	10-19
Workload Management .....	10-20
Application Sizing .....	10-22
Modeling .....	10-23
Types of Modeling .....	10-25
Capacity Planning .....	10-27
The Capacity Plan .....	10-28
Question (1 of 2) .....	10-30
Question (2 of 2) .....	10-31

## Module 11 — Financial Management

Mission of Financial Management .....	11-2
Scope of Financial Management .....	11-4
Objectives of Financial Management .....	11-5
Budgeting .....	11-6
IT Accounting .....	11-8
Major Cost Types and Cost Elements of Financial Management .....	11-9
The IT Accounting System — Cost Models .....	11-10
Cost Model .....	11-13
Investment Appraisal .....	11-14
Charging .....	11-16
When Do You Charge? .....	11-17
Benefits of Charging .....	11-18
Problems of Charging .....	11-19
Charging and Pricing Policies .....	11-20
Differential Charging .....	11-22
Billing .....	11-23
Question (1 of 2) .....	11-25
Question (2 of 2) .....	11-26

## Module 12 — IT Service Continuity Management

Mission of IT Service Continuity Management .....	12-2
Scope of IT Service Continuity Management .....	12-3
Objectives of IT Service Continuity Management .....	12-4
Business and IT Responsibilities .....	12-5
Possible Risks .....	12-7
The Process — Stages 1 and 2 .....	12-8
Business Impact Analysis .....	12-9
Risk Analysis and Management .....	12-10
Graphical Representation of Priorities .....	12-12
Service Continuity Strategy .....	12-13
The Process — Stage 3 .....	12-14

## Contents

Typical Organization Structure.....	12-15
Standby Arrangements.....	12-17
IT Service Continuity Plan.....	12-19
IT Recovery Plans.....	12-20
Test the Plan.....	12-22
The Process — Stage 4.....	12-23
Question (1 of 2) .....	12-25
Question (2 of 2) .....	12-26
Service Delivery: Summary .....	12-27
IT is the business .....	12-28



---

## **Module 1 — Introduction**

This course is for IT practitioners who are involved in the support and delivery of business-focused IT services, and who require a detailed insight into IT Service Management practices and procedures.

The course is accredited by the Information Systems Examinations Board (ISEB) and prepares delegates for the Foundation Certificate in IT Service Management examination.

## IT Service Management

### IT Service Management



- The management of IT services to support one or more business areas
- The IT Infrastructure Library (ITIL) defines “best practice” processes
- Course syllabus
  - Service Delivery
  - Service Support
- Summarized in student notes
- Pocket Guide — excellent for revision

### Student Notes

IT Service Management is the management of IT services to support one or more business areas. As organizations have become more dependent upon IT to support their core business, so the demand for high quality, cost effective IT services has also increased. IT service providers, whether in-house or external, face increasing pressure from Customers and increasing competition from other providers.

The adoption of IT Service Management disciplines and processes will facilitate a continuous improvement in the quality of IT services, aimed at achieving and maintaining best value whilst remaining in line with changing business requirements. The disciplines are described in the IT Infrastructure Library, which defines “best practice” processes and procedures.

IT Service Management comprises eleven disciplines, which are split into two core sets. These core sets are known as Service Delivery and Service Support. The IT Infrastructure Library contains manuals relating to each of the eleven disciplines.

In practice, the eleven disciplines are so closely inter-related they should not be viewed in isolation. Implementation, therefore, is best seen as a phased, project-oriented introduction of one overall topic - IT Service Management.

The Student Notes provide an excellent summary of the description of each discipline, and are designed to complement the slides.

The itSMF Pocket Guide is also a useful summary and is particularly useful for exam revision.

## Course Format

### Course Format



- Brief lectures
- Practical assignments
- Example questions, mock examinations
- Formal ISEB/EXIN examination

## Student Notes

This is a three-day course, comprising short lectures and group assignments. There is a strong emphasis on practical and group work and the course can be used as a valuable part of any organization's team-building, service culture and general IT service management awareness programs.

The start and end time for each day will normally be agreed at the start of the course. Delegates can expect to attend for approximately eight hours on the first and second days, with a slightly shorter third day. Lunch, tea and coffee breaks will be taken at appropriate times.

The course culminates in an hour long, formal examination administered by the ISEB. Although the majority of delegates sit the exam, to do so is optional. Some delegates (in agreement with their sponsor) choose not to sit the exam, and organizations may decide that there is no requirement to hold the exam at all.

## IT Service Management Foundation Certificate

### IT Service Management Foundation Certificate



- ISEB/EXIN IT Service Management Foundation Certificate
- Multiple choice examination (1 hour)
- 65% required to pass (26 from 40)
- Pre-requisite for the Practitioner and Manager's Certificates

## Student Notes

### Information Systems Examination Board (ISEB)

The syllabus for this course is based on the Office of Government Commerce's (OGC) IT Infrastructure Library (ITIL) and is accredited by the ISEB.

Originally known as the Systems Analysis Examination Board (SAEB), the ISEB was formed in 1967 with representation from the British Computer Society (BCS), Central Computer and Telecommunications Agency (CCTA), EXIN (the Dutch IS examination board) and a number of experienced representatives from the IT industry.

The board currently functions under the auspices of the British Computer Society (BCS).

### Examination for the Foundation Certificate in IT Service Management

The optional examination which normally concludes the final day, takes the form of a closed book multiple choice paper of 40 questions, and lasts for one hour. The examination is invigilated by an ISEB representative.

**Module 1**  
**Introduction**

To pass the examination, you will need to achieve 65% (or 26 correct answers). The paper will be collected and marked by the ISEB. Your result (either “Pass” or “Fail”) is usually sent to you within three weeks.

An examination entry form will be given to you by the course instructor.

Possession of the Foundation Certificate is an essential pre-requisite for those wishing to progress to the Manager’s Certificate in IT Service Management, or one of the Practitioner’s Certificates.

## IT Infrastructure Library (ITIL)

### IT Infrastructure Library (ITIL)



- Series of books giving guidance on the provision of quality IT services
- Produced by OGC, published by The Stationery Office
- Non-proprietary
- itSMF



### Student Notes

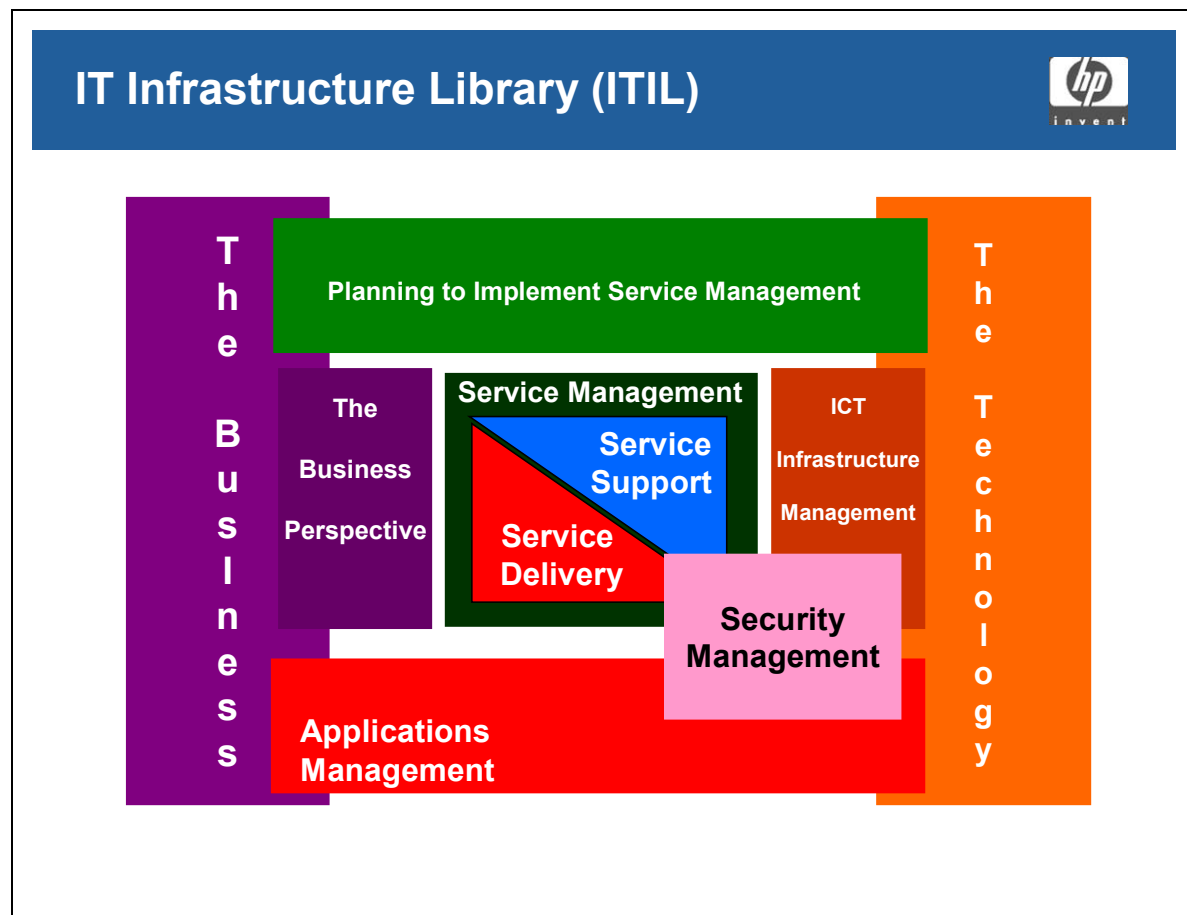
The IT Infrastructure Library was developed originally by the Central Computer and Telecommunications Agency (CCTA) as a set of comprehensive and inter-related codes of practice in achieving the efficient support and delivery of high quality, cost effective IT services.

The Office of Government Commerce (OGC) now incorporates the CCTA. The OGC maintains the library and produces updates. The Stationery Office (UK) publishes the material.

The OGC is an office of HM Treasury (UK). As such, it is independent of any commercial interests involved in ITIL (for example, software vendors or training providers). ITIL's impartiality in this area is one of its key strengths.

The itSMF (IT Service Management Forum) was set up to support and influence the IT Service Management industry. It has, through its very large membership, been influential in promoting industry best practice, and driving updates to ITIL.

## IT Infrastructure Library (ITIL)



### Student Notes

The IT Infrastructure Library (ITIL) consists of many books, of which Service Management (Service Support and Service Delivery) is a part. The other books are:

- **The Business Perspective** – describes many issues related to understanding and appreciating IT services an integrated aspect of managing a business. Sections include:
  - Business Continuity Management
  - Partnerships and outsourcing
  - Surviving changes
  - Adapting the business to radical change
- **ICT Infrastructure Management** – IT Operations management issues e.g.:
  - Network Services management
  - Operations Management
  - Managing local processors
  - Computer Installation and acceptance
  - Systems management



- Environmental Management
- **Application Management** – the software development lifecycle including:
  - Software lifecycle support
  - Testing an IT service for operational use
- **Security Management** – protecting the IT Infrastructure against unauthorized use based on SLA requirements, contractual requirements, legislation, policy and a basic level of security.
- **Planning to Implement** - planning and implementing programs to optimize IT Service Management.

## ITIL Philosophy

### ITIL Philosophy



- Capture industry “best practice”
- Organizations should adopt and adapt
- Not standards!
- Scalable — organization size and need
- Platform independent
  - Version 1 is 10+ years old — focused on UK Government and mostly centralized IT
  - Version 2 – industry wide & took into account changes in technology

### Student Notes

The ethos behind the library is the recognition that organizations are becoming increasingly dependent on IT in order to satisfy their corporate aims and meet their business needs. As codes of practice the library is intended to assist organizations handle increasing system complexity, demands from Customers and Users for flexibility and the ever present need for change.

The IT Service Management set of books was written and is constantly being revised by experienced IT professionals and seek to give ‘best practice’ advice and guidance. A recurring theme is the need to provide high quality, cost-effective IT services which meet the business needs of the Customers, Users and the organization.

The principles embodied in the IT Service Management books are not intended to be hard and fast rules which must be obeyed. It is recognized that organizations will need to adapt and adopt the processes to suit their own particular needs and objectives, but the core values will be applicable to all organizations.

The ITIL disciplines can be used by any type and size of organization. The most current books (published 2000-2001) have incorporated decentralized processing.

## Best Practice — A Working Definition

### Best Practice — A Working Definition



*Best Practice* is a set of guidelines based on the best experiences of the most qualified and experienced professionals in a particular field.

*Best Practice* is based on:

- More than one person
- More than one organization
- More than one technology
- More than one event

## Student Notes

Best Practice is a set of guidelines based on the best experiences of the most qualified and experienced professionals in a particular field.

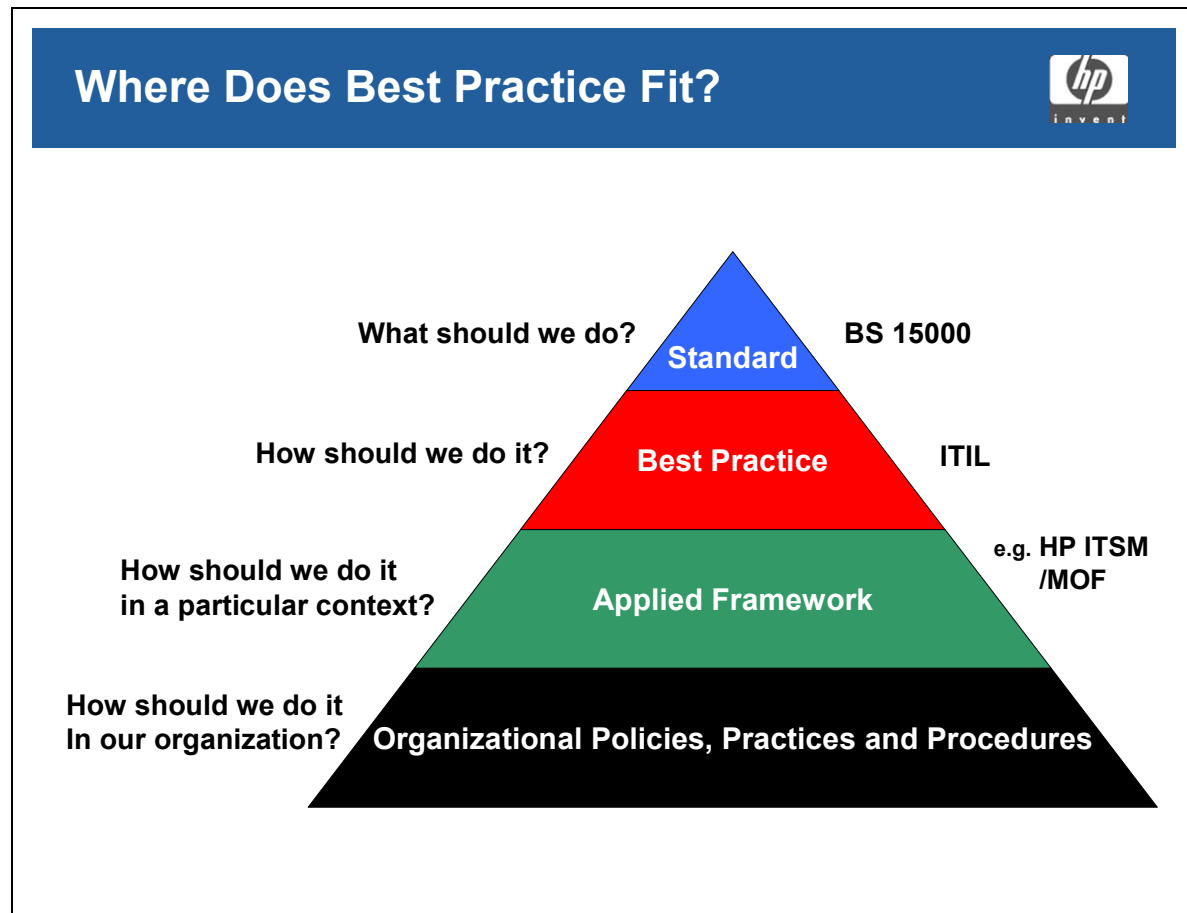
Best Practice is based on:

- More than one person
- More than one organization
- More than one technology
- More than one event

The characteristics and benefits of a best practice approach are:

- It provides a starting point, not a goal
- It presents guidelines, not regulations
- It promotes internal direction through a common vision and a common language
- It is not intended to be imposed from the outside
- It is generic
- It builds a basis for professionalism

## Where Does Best Practice Fit?



### Student Notes

Best practice describes a framework of goals, general activities, inputs and outputs of the various ITIL disciplines. The industry standards are detailed in BS15000, which gives explicit instructions on evidence to be sought in an ITIL-compliant organization.

More practically, there are many organizations offering IT Service Management solutions in given contexts, such as Hewlett-Packard's ITSM, and the Microsoft Operating Framework (MOF). These solutions are complemented by the target organization's internal policies, practices and procedures.

## The Drivers for High Quality IT Services

### The Drivers for High Quality IT Services



- Organizations increasingly dependent on IT service provision
- Higher visibility of failure
- More exacting User requirements
- Increased complexity of the infrastructure
- Charging for IT services
- Competition for Customers

### Student Notes

- **Increased dependency on IT**  
Most organizations could not function as a business without acceptable levels of IT service availability and reliability.
- **Higher visibility of service failures**  
If an organization experiences service failures, the impact on the business is more likely to be noticed quickly.
- **More exacting Customer and User demands**  
A general increase in computer literacy, particularly amongst Customers and Users, has led to a higher expectation of what is required from IT services, and a reduction in their level of tolerance of faults and failures in the IT services.
- **Increased complexity of the IT infrastructure**  
IT services are delivered by a complex mix of hardware, software, networks and people. It is essential that all these components are managed effectively and efficiently, as poor performance of any one component can seriously affect the quality of the overall IT service.

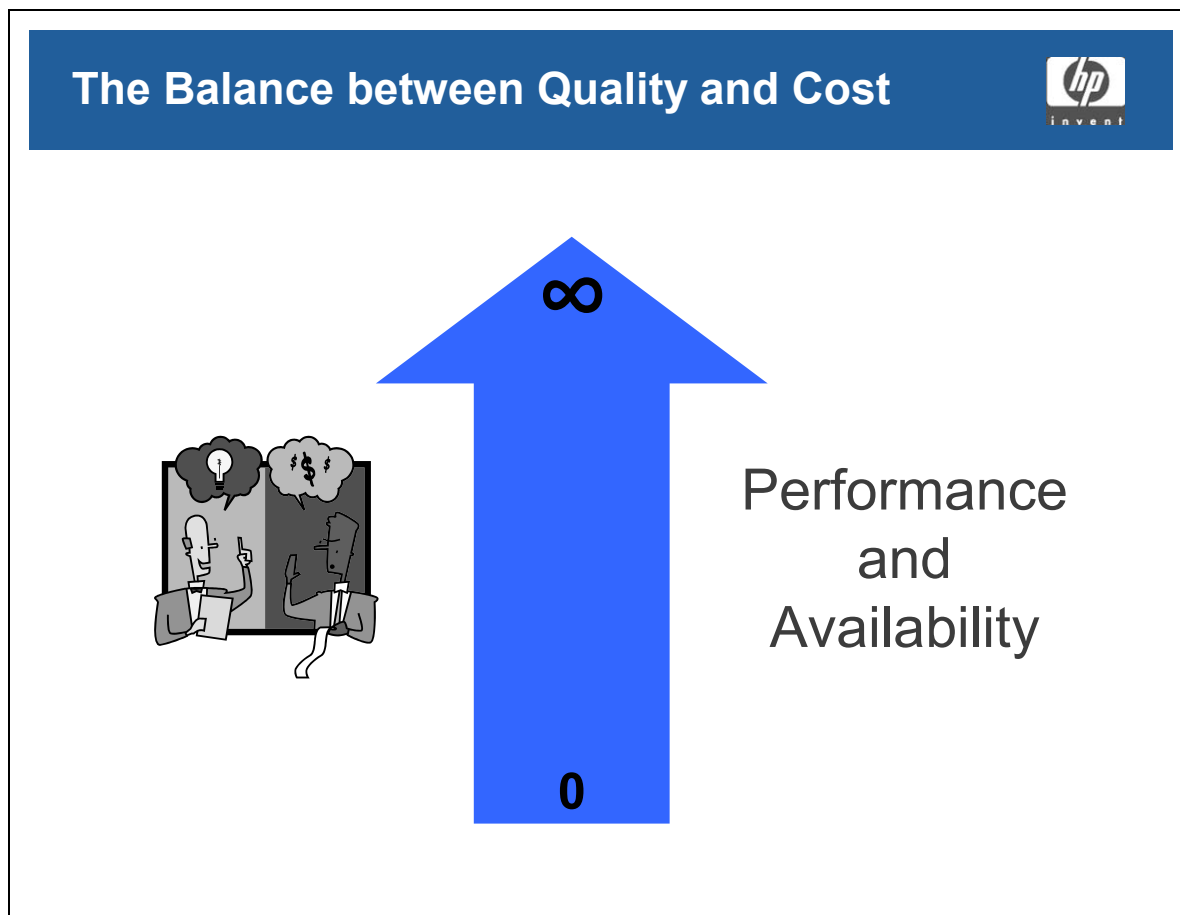
## **Module 1**

### **Introduction**

- **Charging and competition**

Today, Customers are more likely to be asked to pay for the IT services they receive, either directly or indirectly. The introduction of real or notional charging enables Customers to make comparisons, and puts IT service providers in competition with each other.

## The Balance between Quality and Cost



### Student Notes

Although ITIL promotes high quality IT services, it equally emphasizes the need for efficient use of resources, and the need to deliver services to meet the requirements of the business. Wasteful, inefficient services, or those which “over-deliver” are not the intention of ITIL.

## ITIL Objectives

### ITIL Objectives



- Reduce ***Costs***
- Improve ***Availability***
- Tune ***Capacity***
- Increase ***Throughput***
- Optimize resource ***Utilization***
- Improve ***Scalability***

### Student Notes

The objectives of ITIL are to:

- Reduce costs
- Improve availability
- Tune capacity
- Increase throughput
- Optimize resource utilization
- Improve scalability



## Achieving High Quality

### Achieving High Quality



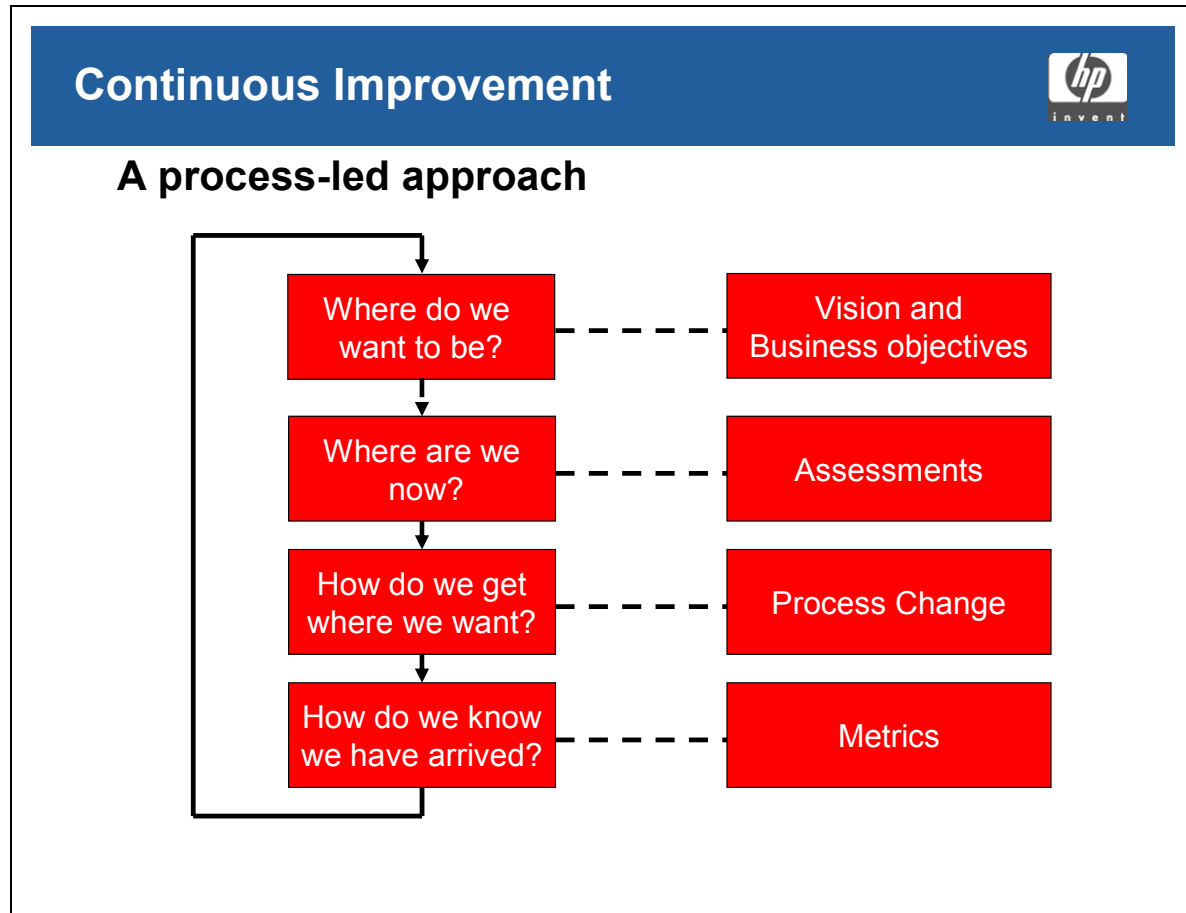
- Service Improvement Program using Project management (for example: PMI, PRINCE)
- Service Culture
- Supporting Disciplines

### Student Notes

ITIL recognizes three key facets of achieving high quality IT services. These are:

- The use of Service Improvement Programs
- The existence of a Service Culture within IT (and the rest of the organization)
- The implementation of ITIL disciplines

## Continuous Improvement



### Student Notes

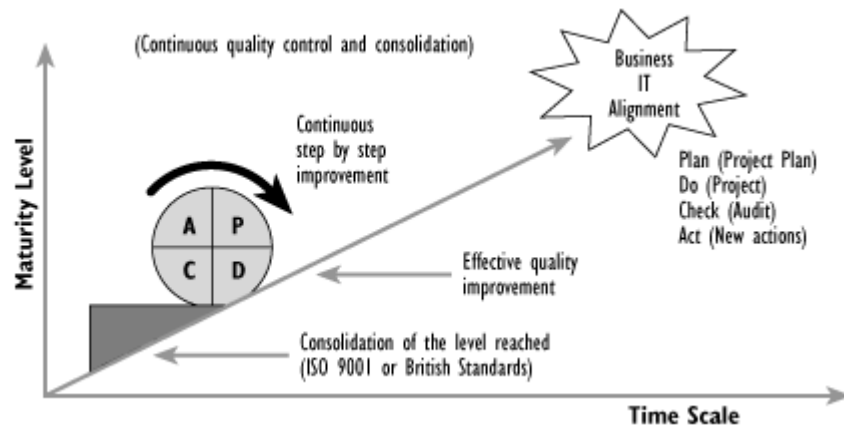
The cycle of continuous improvement begins with the establishment of an organization's (or service provider's) vision and business objectives. The level of service currently provided is then assessed. This work is completed before embarking on process change (such as ITIL implementation). Metrics should be in place to measure the success of the proposed improvements.

Quality management for IT Services is a systematic way of ensuring that all the activities necessary to design, develop and implement IT services which satisfy the requirements of the organization and of Users take place as planned and that the activities are carried out cost effectively.

For quality improvement Deming\* proposed the Deming Cycle (or Circle). The four key stages are Plan, Do, Check and Act after which a phase of consolidation prevents the 'Circle' from 'rolling down the hill' as illustrated overleaf.

\*W. Edwards Deming (1900-93) is best known for his management philosophy establishing quality, productivity, and competitive position.

Deming's Quality Circle:



As discussed above, the cycle is underpinned by a process-led approach to management, where defined processes are in place, the activities are measured for compliance with expected values, and outputs are audited to validate and improve the process.

## Service Culture

### Service Culture



- Recognition that IT only exists to underpin the business of the organization
- A corporate IT mission to deliver agreed levels of service
- A willingness to go that 'extra step' to satisfy Customer needs
- An understanding of the Customers' perspective

### Student Notes

A service culture must originate from:

- A recognition amongst IT staff that the IT division only exists in order to provide services which underpin the business of the organization. It is also important that each member of staff realizes that they have an important part to play in the delivery of those services.
- A corporate mission within the IT division to provide, as a minimum, the agreed levels of service. It is imperative that the motivation and desire to achieve high quality services emanates from senior management.
- An understanding of the Customers'/Users' perspective. IT staff, especially those in the 'front-line' such as Service Desk staff, should be encouraged to consider the Customers'/Users' view and ensure that their requirements are reflected accurately within the IT service organization.

## Achieving a Service Culture

### Achieving a Service Culture



- Senior Management support
- A good understanding of why IT Services are being provided
- An understanding of the impact on the business of poor service
- Clear targets to aim for, and from which to progress

### Student Notes

A service culture cannot be imposed upon an organization so the need for such a culture must be understood by all staff. They must understand that the IT service provider exists to further the business aims of the Customers and Users of its services.

To achieve a service culture, there must be whole-hearted support from the senior management of the organization, and all levels of management and staff must understand why the IT services are provided and the impact on the business of poor service.

An organization dedicated to achieving a service culture will have distinct service performance targets for which to aim, and a clear vision of how it will continue to achieve improving levels of service in the future.

## Who Is Doing This?

### Who Is Doing This?



- Government
- Financial services
- Insurance
- Manufacturing
- Publishing
- Outsourcing companies
- Utilities

## Student Notes

Although originally intended for use by the UK central government, ITIL has proved useful to organizations in all sectors, including:

- Government
- Financial
- Insurance
- Manufacturing
- Publishing
- Outsourcing companies
- Utilities

Today, ITIL is known and used worldwide.

## Benefits

### Benefits



#### Qualitative

- Better quality services
- Increased morale
- Improved uptime
- Better business support
- Cost and quality information and decision capability

#### Quantitative

- License / Maintenance fees
- Support Costs
- People
- Deferred expenditure

## Student Notes

The benefits of implementing ITIL can be split into those which are qualitative and others which are quantitative.

- Qualitative
  - Better quality services
  - Increased morale
  - Improved uptime
  - Better business support
  - Cost and quality information and decision capability
- Quantitative
  - License/maintenance fees
  - Support costs
  - People
  - Deferred expenditure

## What Is an IT Service?

### What Is an IT Service?



- A set of related functions provided by IT systems in support of one or more business areas
- This service can be made up of hardware, software and communication components, but is **perceived** as a self-contained, coherent entity

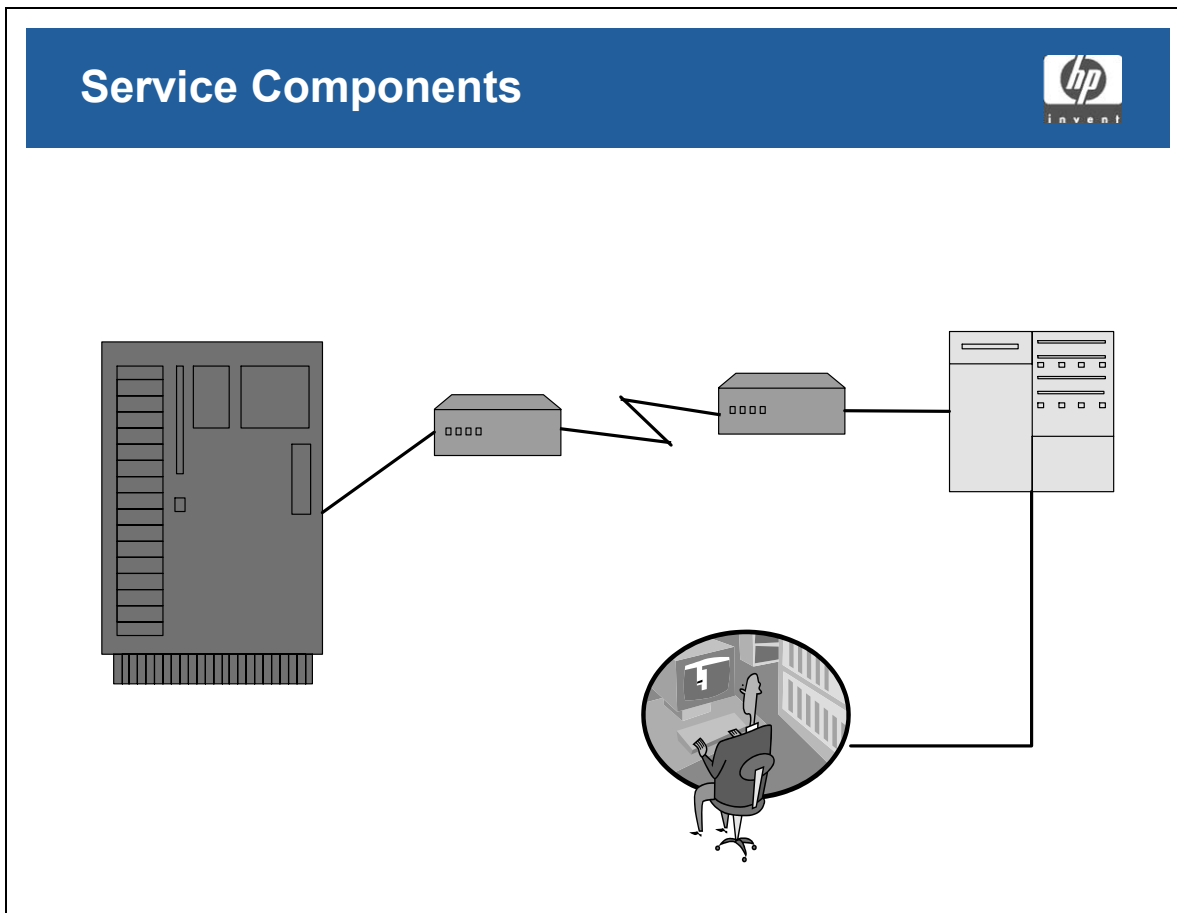
### Student Notes

IT Service Management views the IT facilities offered by an IT department as “services”.

An IT Service can be defined as “a set of related functions provided by IT systems in support of one or more business areas. This service can be made up of software, hardware and communication facilities, but the Users perceive it as being a self-contained, coherent entity.”



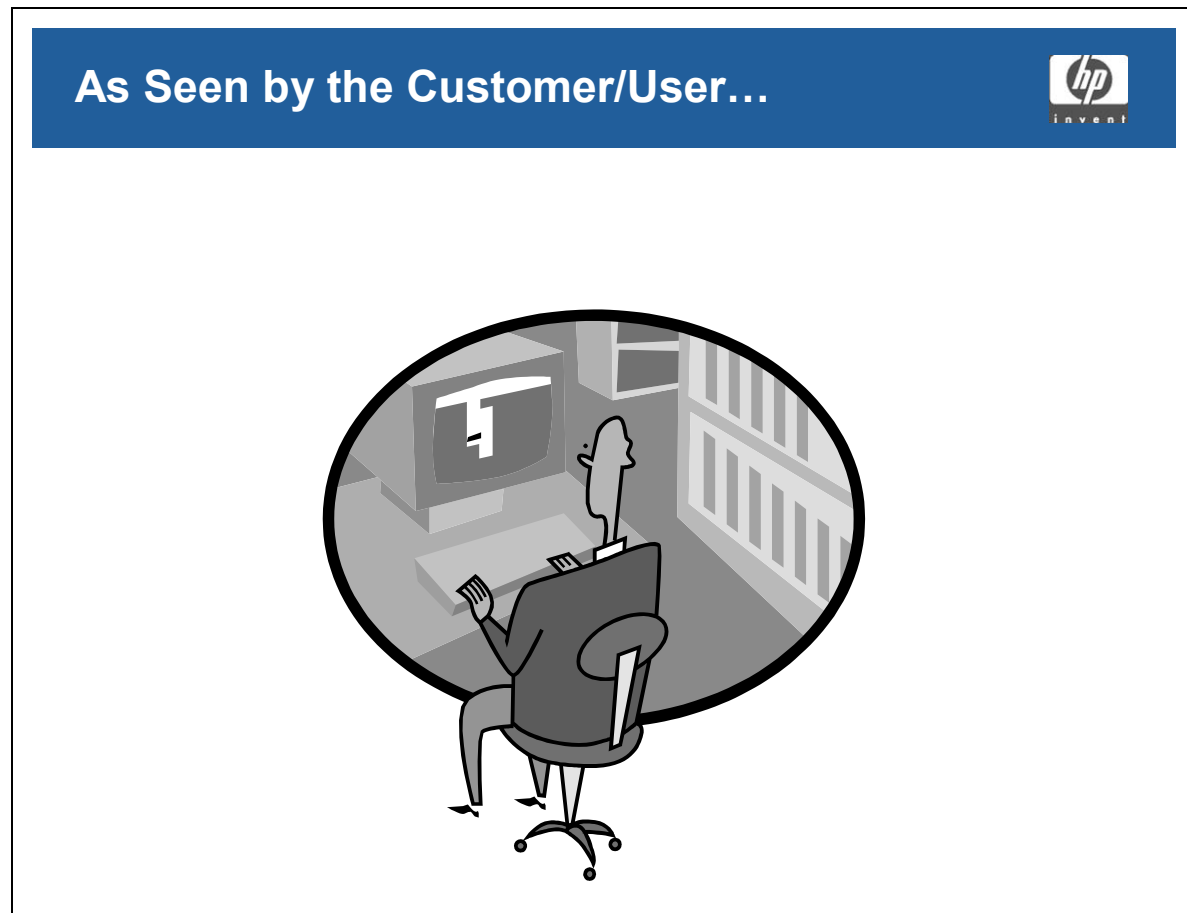
## Service Components



### Student Notes

As IT staff know, there are often many components which make up the overall service delivered to the Customer/User.

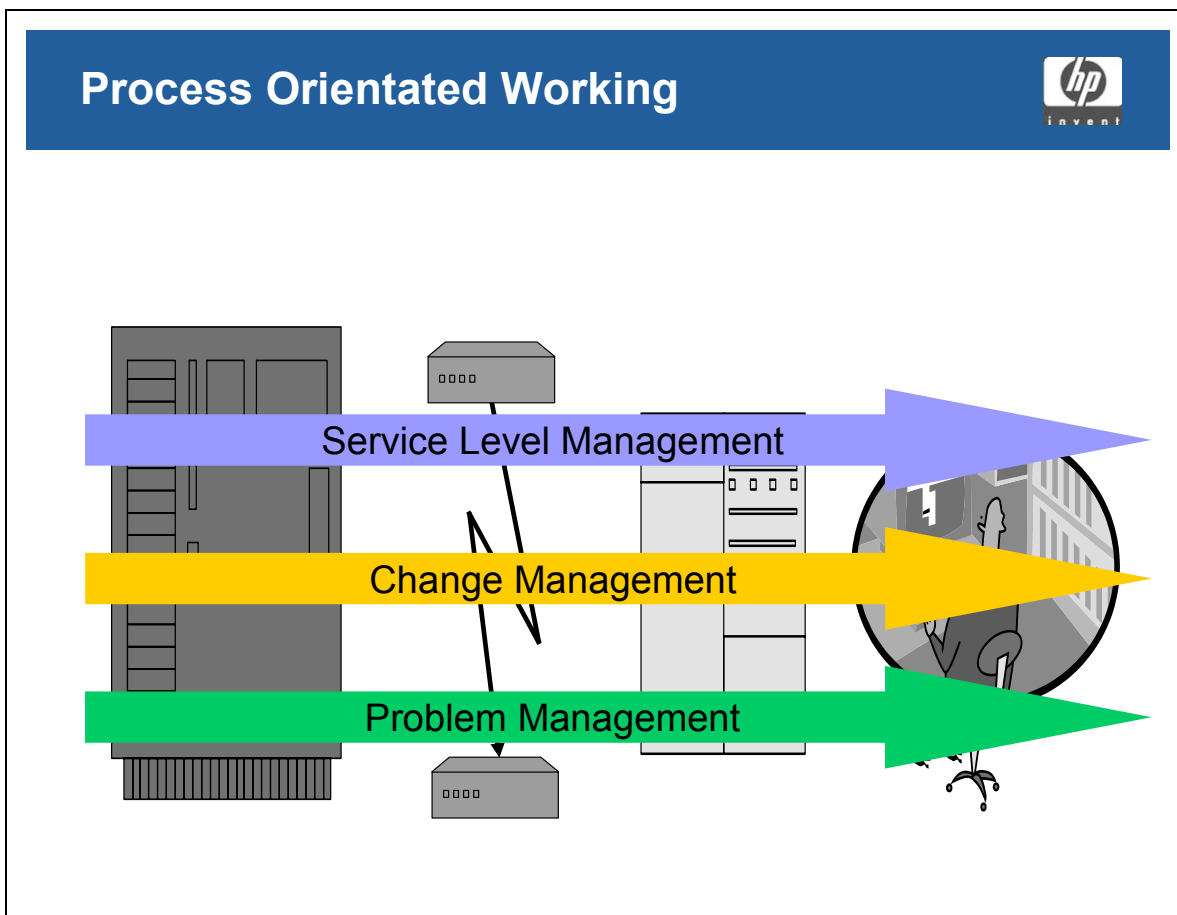
## As Seen by the Customer/User...



### Student Notes

However, the Customer's/Users only impression of the quality of the IT Services they receive, is that which is delivered to their workstation. A failure, not matter where it occurs, or how minor the component, is visible to the Customer/User if it disrupts the delivery of the end-to-end service.

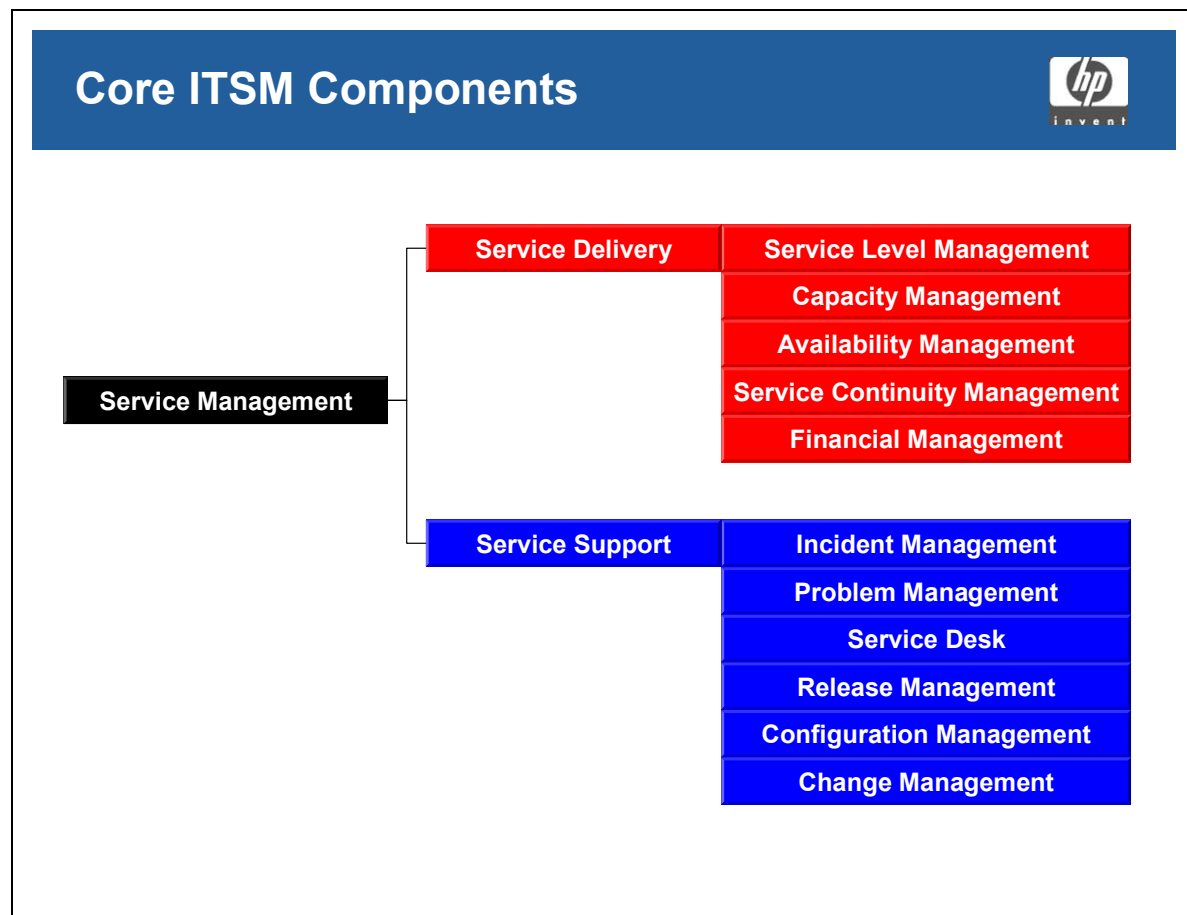
## Process Orientated Working



### Student Notes

ITIL disciplines work across all the service components to ensure high quality IT services are delivered, as perceived by the Customer/User.

## Core ITSM Components



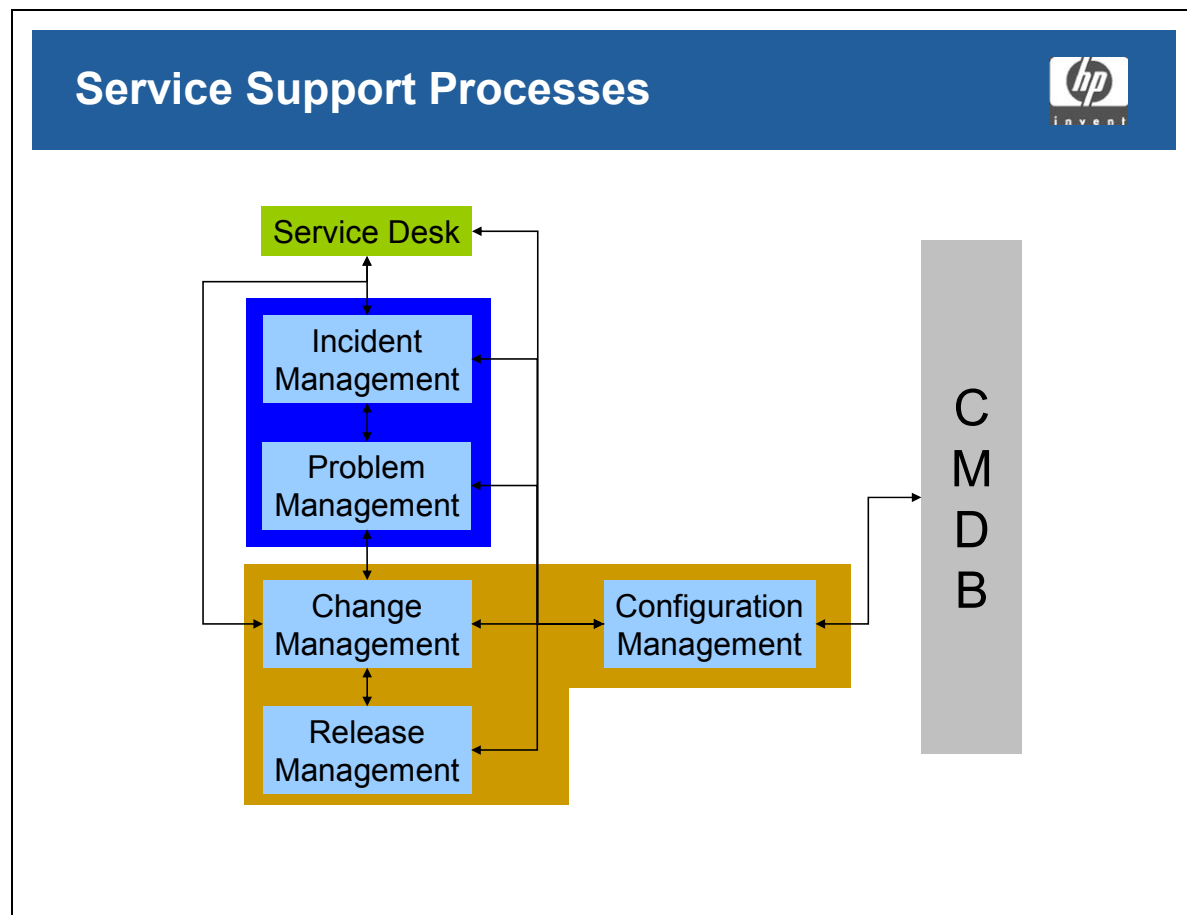
### Student Notes

IT Service Management is split into two core sections, which are further split into eleven disciplines.

- **Service Delivery (These are concerned with tactical /medium term management cycles)**
  - Service Level Management
  - Capacity Management
  - Availability Management
  - Service Continuity Management
  - Financial Management
- **Service Support (These are concerned with operational /short term management cycles)**
  - Incident Management
  - Problem Management
  - Service Desk

- Release Management
- Configuration Management
- Change Management

## Service Support Processes

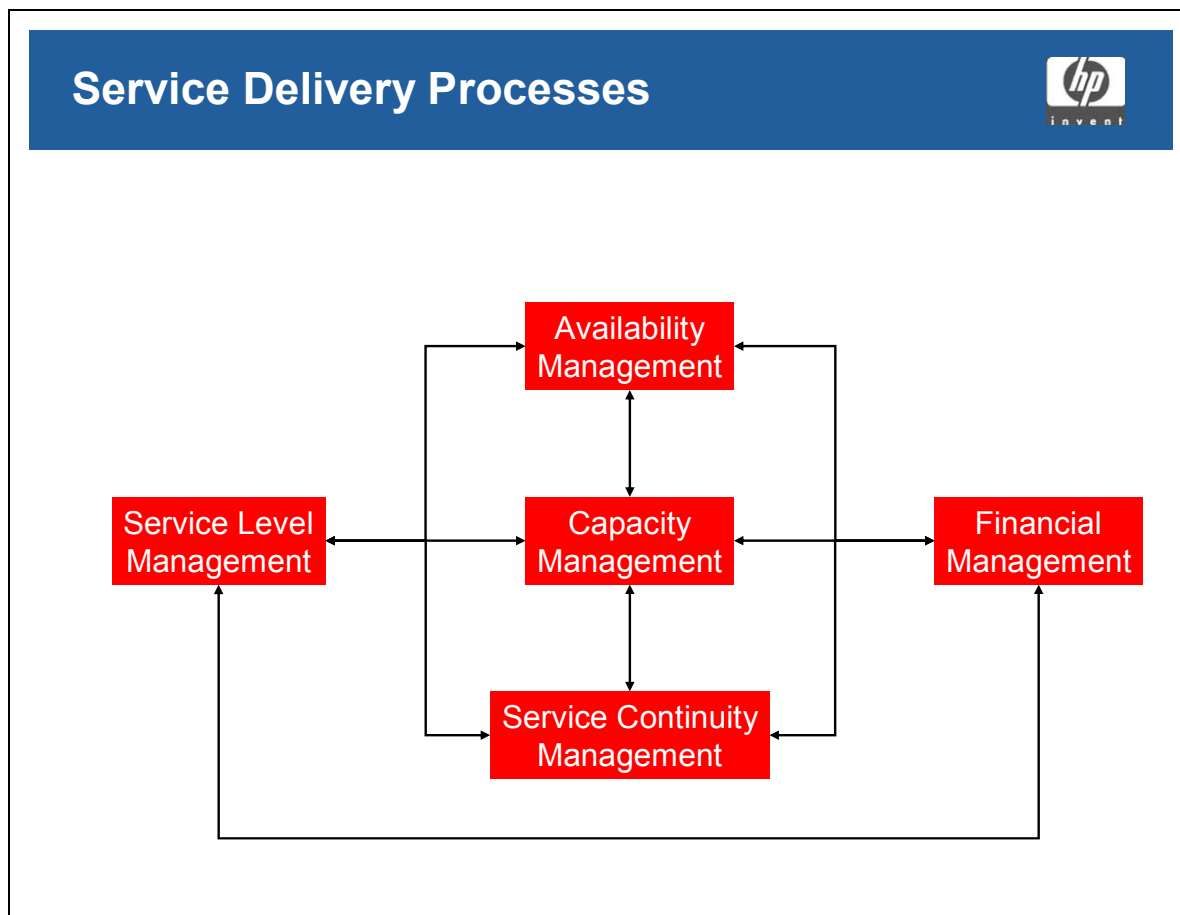


### Student Notes

Configuration Management, which is responsible for the Configuration Management Database (CMDB) is the key ITIL discipline, and underpins all other disciplines.

There is a flow through the Service Desk, Incident Management, Problem Management, Change Management and Release Management disciplines, in that order. However, there are exceptions. For example, the Service Desk may interact directly with Change Management, as the Service Desk often processes Service Requests and Requests For Change.

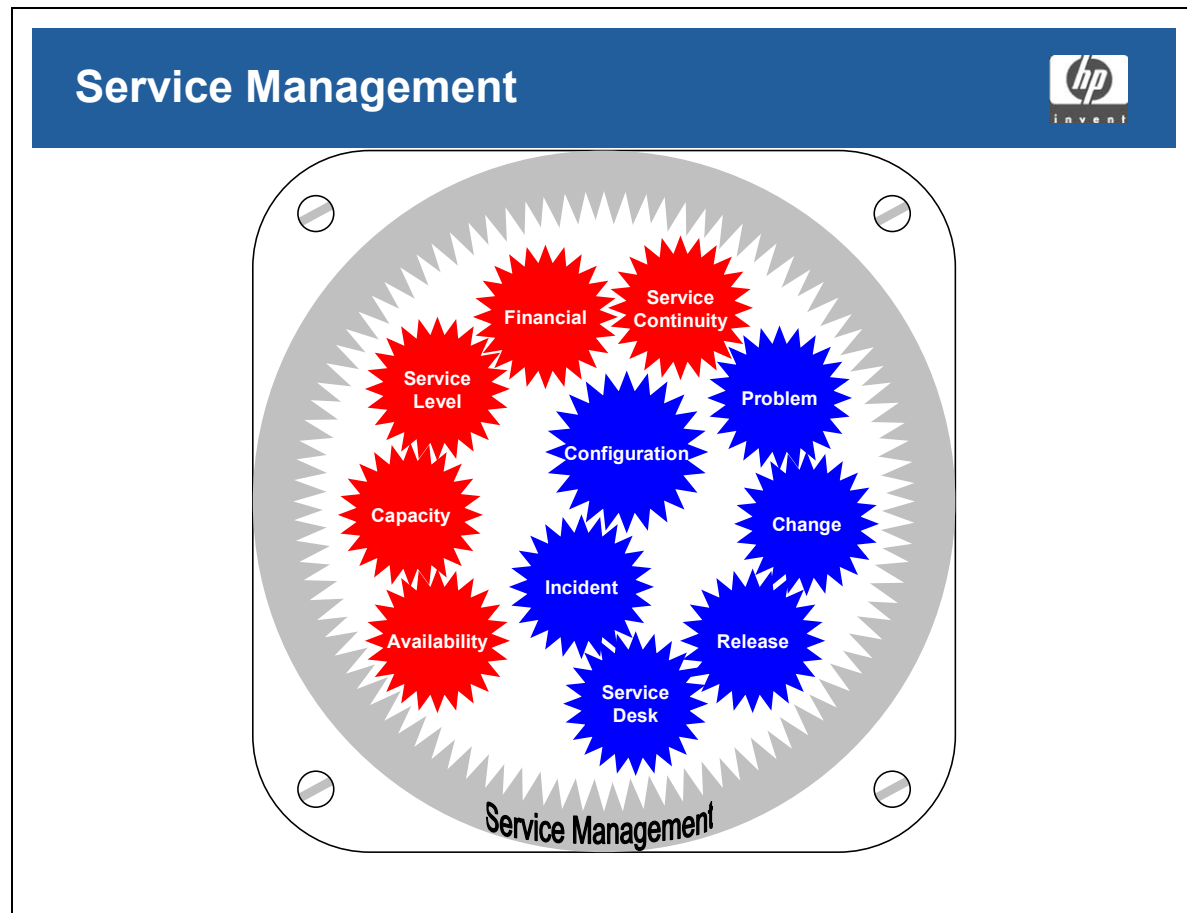
## Service Delivery Processes



### Student Notes

The Service Delivery disciplines are also closely related. For example, Service Level Agreements (SLAs) contain requirements relating to the Availability and Capacity of an IT Service; will reference the applicable IT Service Continuity plans; and will have been written with the costs of providing the service in mind (the SLA may even contain details of charges and/or penalties for the service, if Charging is in force).

## Service Management



### Student Notes

Service Management embraces all the Service Support and Service Delivery disciplines, which are not intended to work in isolation, but as an integrated framework. At the heart of this framework is Configuration Management.



---

## **Module 2 — Service Desk**

## Mission of Service Desk

### Mission of Service Desk



To minimize disruption to business through faulty IT services by detecting incidents, recording them, and coordinating the activity required to restore them, while recording information that will result in the timely resolution and future prevention of problems

## Student Notes

### Mission

*To minimize disruption to business through faulty IT services by detecting incidents, recording them, and coordinating the activity required to restore them, while recording information that will result in the timely resolution and future prevention of problems.*

Service Desk is different from all the other disciplines in that it is a FUNCTION and NOT a PROCESS.

Service Desk supports the mission statement by

- Logging the incident
- Attempting an initial resolution
- If not possible will escalate to appropriate resolver group
- Control further escalations as required
- Maintain ownership and control of all incidents making sure that none are “lost”
- Maintain information about the incident to aid current and future resolutions
- Close all incidents following Incident Management practices

In addition Service Desk has other abilities over and above incident Management. These are (as required by the organization):

- Ability to perform some standard changes e.g. Password resets
- Log Changes, Complaints, Service Requests etc.
- Act as Configuration Librarians
- Provide Management Information
- Maintain a flow of communication between the IT Department and Customers/Users

## Objectives of Service Desk

### Objectives of Service Desk



- To be the single point of contact for all IT customers/users
- To restore service whenever possible
- To maximize service availability
- To manage *all* incidents to a closure
- To be aware of business needs
- To be aware of the impact of failure upon the business
- To provide Business Systems Support

### Student Notes

The Service Desk needs to be Customer and User focused at all times

- At an operational level, its objective is to provide a SPOC (Single Point Of Contact) to provide advice, guidance and the rapid restoration of normal services to its Customers and Users.
- To make an initial diagnosis of the incident and attempt where possible to restore service, using a variety of tools and techniques (e.g. Knowledge bases, KEDB etc.)
- Maximizing Service Availability is achieved by making sure that incidents are resolved and the user is back up and working as quickly as possible, this will be achieved through monitoring, tracking and prompt escalation of incidents
- To manage ALL incidents to closure. This is the control function of the service Desk in managing, monitoring and tracking all incidents to make sure none are lost or forgotten about. It is also referring to the fact that ALL incidents are logged – no exceptions!
- Be aware of the Business need and impact of failure upon the business – this is a key difference between a service Desk and a Call Centre/Help Desk. The Service Desk need

an appreciation on what affect the incident has on the business as a whole, not just on the individual being affected by the incident. This is required to reduce any negative business impact associated with the incident. (For example, assigning appropriate severity/priority and escalation times.

- **Business System Support** - The ability (if required) to provide a contact and control point (SPOC) for critical non-IT systems e.g. ATM machines in a Bank environment

To meet both Customer and business objectives, many organizations have implemented a central point of contact for handling Customer, User and related issues. This function is known under several titles, including:

- **Call Center:** The main purpose is to handle large volumes of telephone based transactions like telesales or order processing
- **Help Desk:** The main purpose is to manage and resolve incidents quickly and effectively, and to make sure that all requests are followed up
- **Service Desk:** This function extends the range of services offered by the Help Desk, and allows business processes to be integrated into the Service Management infrastructure. In addition to handling incidents, it will provide an interface for managing changes, SLM, maintenance issues, software licensing, ITSCM, Financial, Availability and Configuration Management

All three organizations share these characteristics:

- They represent the service provider to the Customer/User
- They all aim to achieve customer satisfaction
- They use technology, people and processes to provide a service to the business

## Common Features and Characteristics (1 of 2)

### Common Features and Characteristics (1 of 2)



- A single point of contact
- A central log of all incidents, numbered and time stamped
- Diagnostic scripts and other aids
- Supported by Configuration Management tools
- An impact coding system
- Automatic escalation procedures

### Student Notes

- A single point of contact for all incidents and other day to day operational enquiries (e.g. Service Requests, Change registrations etc)
- A central log of all incidents, numbered and time stamped
- Diagnostic scripts and other aids
- Configuration Management support tools
- An impact coding system
- Automatic escalation procedures

These are usually integrated into a single “Service Management” tool such as HP Openview, Remedy, Touchpaper, Assyst etc,

They provide a single database that all incidents can be logged onto and then monitored and tracked throughout their lifecycle. They provide a central repository of information about incidents that is usually available both to the Service Desk and other Resolver groups, with

the addition of some form of “knowledge base” then diagnostic aids and scripts can be accessed. An Impact code is assigned to each individual incident so that decisions can be made on the impact on the business and urgency required for a resolution to be assessed and acted upon accordingly.

Automatic escalation procedures are usually built into the tool; these will handle both functional escalation (e.g. suggested likely resolver group) and hierarchical escalation (usually time bound and associated with an SLA and handles escalation up the management chain).

## Common Features and Characteristics (2 of 2)

### Common Features and Characteristics (2 of 2)



- Communication with support staff
- Interface to SLAs
- Regular progress reporting
- Classification of incidents at call closure
- Management summaries
- Operational systems access

### Student Notes

- Communication with support staff – monitoring of the incident, escalation between and within resolver groups and the liaison role between the user and the resolver groups as required.
- Interface to SLAs – escalation according to rules laid down within the SLA (functional and hierarchical), also monitoring and communications about breaches or potential breaches. In addition lots of Management Information to do with performance against the SLA is derived from Service Desk metrics.
- Regular progress reporting – liaison with the Users on incident resolution progress, can either be reactive or proactive.
- Classification of Incident at call closure. This is a closure category based on the “real” cause of the incident, and not just on the “suspected” cause logged at opening. This is useful information for Problem Management.



- Management summaries – Management Information derived from service desk metrics are used by nearly all the other ITIL disciplines and are used to gauge performance against targets and inform Management decision making.
- Operational systems access – password resets, and allocation etc (where applicable and appropriate).

## Staffing Options

### Staffing Options



#### Minimum qualifications

- Interpersonal skills
- Business understanding
- IT understanding

#### Skill levels

- Technically unskilled
- Technically skilled
- Expert

## Student Notes

- Minimum Qualifications – The Service Desk Agents need the three qualities as a minimum; they do not have to be experts, but do have to have good customer handling skills and an appreciation of the business in order to work effectively.
- The skill level in IT will determine the level of first time fix that is available via the service desk. This may be an important factor to you and hence a high degree of technical knowledge is required in order to promote a high first time fix. In other situations technical knowledge may not be as high a requirement as is another skill, e.g. languages.

## Skills and Mindset

### Skills and Mindset



- Teamwork
- Empathy with Users
- Professionalism
- First impressions count
- Accept ownership
- Use customer terminology
- Assume users perspective
- Active listening

### Student Notes

- Teamwork – Internally and with resolver groups
- Empathy with Users – Realizing that they are angry at the situation and not with you personally; understanding their perspective
- Professionalism – Do not get angry or loose your temper. Be assertive not aggressive.
- First impressions count – Strive to come across as professional and helpful as you take the call. Your initial tone can help to set the tone for the rest of the conversation.
- Accept ownership – Its now “Your” incident as well. Look to get it resolved quickly and efficiently
- Use customer terminology – Don’t use internal IT jargon where possible. Use the every day business language used in your organization. Don’t set out to deliberately confuse or hide behind technical explanations
- Assume users perspective – Understand what this incident means for them personally.

**Module 2**  
**Service Desk**

- Active listening – Give positive re-enforcement and feedback signals (i.e. visually = eye contact and nodding etc. Verbally = “yes”, “I see”, “Can I just re-phrase that” etc.)

## Service Desk Implementation

### Service Desk Implementation



- Staff resourcing – correct numbers, profile, skill-sets
- Target effectiveness metrics (KPIs)
- Selecting the correct structure:
  - Local Service Desk
  - Central Service Desk
  - Virtual Service Desk

### Student Notes

- Staff resourcing – having the correct people available when you need them and in the right numbers, e.g. shift patterns/requirements, numbers on each shift (more during the day and less at night), correct skills e.g. technical vs. customer vs. language skills etc. for a multinational support organization.
- Target Effectiveness Metrics – being able to tell how hard and how efficiently you are working. Different types of metrics which show the “work effort” e.g. number of calls logged, which are outside the control of the Service Desk, and effectiveness/efficiency metrics, e.g. Average Speed of Answer (ASA) which is within their control.
- Correct Structure – these are the different types of Service Desk you can have. Explained in more detail in later slides.

## Local Service Desks

### Local Service Desks



- Designed to support local business needs
- Support is usually in the same location as the business it is supporting
- Practical for smaller organizations
- Impractical for geographically widespread organizations

### Student Notes

This is fairly self-explanatory. Usually used by single site or specialist operations (which can be part of a larger organization)

## Central Service Desk

### Central Service Desk



- Designed to support multiple locations
- The desk is in a central location whilst the business is distributed
- Ideal for larger organization as:
  - Reduces operational costs
  - Consolidates management overview
  - Improves resources usage
- Could provide secondary support to local desks

### Student Notes

Can be used to support multinational operations

- Enables economies of scale to be applied, with Management overview on a central point rather than on a distributed organization.
- Small Local desks can be backed up from a Central desk (e.g. specialist application only used in that location is supported from a local desk, whereas all the other IT is supported from the Central desk)

## Virtual Service Desk

### Virtual Service Desk



- Location of SD analysts is invisible to the customers
- May include some element of 'home working'
- Common processes and procedures should exist – single incident log
- Common agreed language for data entry
- Single point of contact per customer
- On-site presence may still be needed for some functions
- 'Workload partitioning' needed

### Student Notes

Tends to be used by very large multinational companies

SD agents could work from home and their actual location would not be factor in where the incoming call is answered from (e.g. a call originating in England can be answered in Singapore). This is also true of where the support for resolution of the incident comes from (e.g. the actual resolver group may be based in America).

Because of the above everyone must have access to the same database (information) in order to resolve the incident and it must be accessed and treated in a standard way (i.e. common procedures). It is also vital that a common language for data entry is used so that everyone can follow what is happening. This does not mean that the SD analyst cannot use a local language to speak to the user / resolver group.

An on site presence is usually required to do the "hands on" work required in resolving an incident (i.e. an engineer is not going to be sent from America to fix the problem in England).

*Workload partitioning - For the Virtual Desk, the support tools in place should allow for 'workload partitioning' and authorised views. (For example, if I am the person looking after local support in, say, Amsterdam, I only want to see requests for that location.) This*



*should include other associated processes and related data, such as planned Changes, asset and configuration data. (From ITIL Service Support Book)*

## 'Follow the Sun' Option

### 'Follow the Sun' Option



- Where Service Desk support switches between two or more desks to provide 24 hr global cover.
- Telephony switching needed
- Multilingual staff usually required
- Local conditions and cultural issues need to be considered
- Clear escalation channels needed



### Student Notes

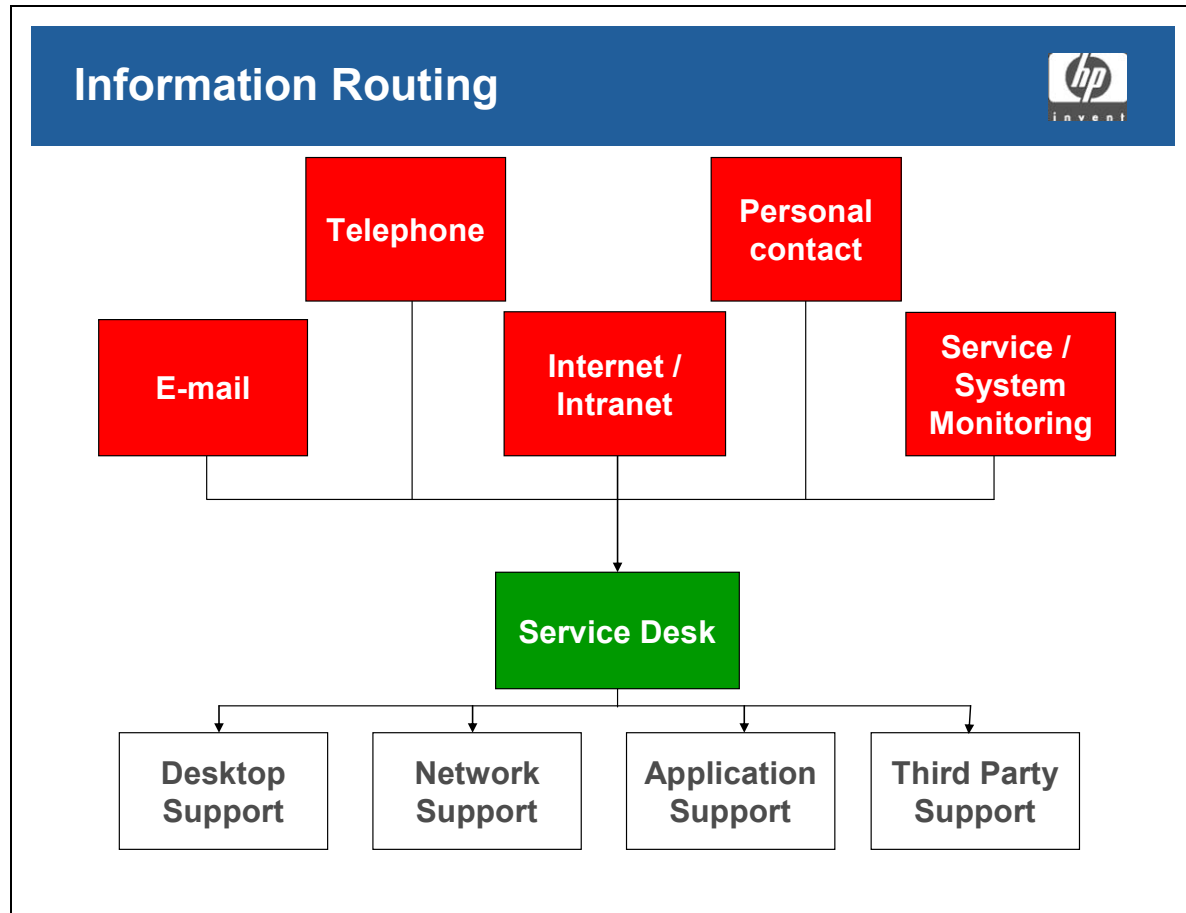
THIS IS AN OPTION AND NOT A TYPE OF SERVICE DESK!

- Usually used by multinational organizations using 3 central desks to give 24/7 global support, while the Central desks are only operational during “office hours” within their own time zone (e.g. London Desk(UK) hands off to Chicago Desk(US) , which hands off Sydney Desk (Australia)
- Telephony switching required to make sure that at 5pm UK time when the London desk shuts down then all calls are then answered by the Chicago Desk etc)
- Multi-lingual staff usually required to handle the “out of hours” support calls from different parts of the globe (E.g. Spanish speaker is useful on UK Desk to handle Spanish (in same time zone) and Latin American (out of hours) calls).
- Local conditions and cultural issues need to be considered – Cultural differences should not be taken for granted e.g. in some cultures it is not easily accepted for a Man to take orders from a Woman, In most case engineers (males) are told “what to do” by Service Desk Personnel (quite often these are women). Also don't think you always understand

what is being said to you – “America and Britain, two nations divided by a common language” etc.

- Clear escalation channels required – to whom do you escalate and where are they?

## Information Routing



### Student Notes

From the ITIL Service Support Book –

*Customer interaction is no longer restricted to the telephone and personal contact. Service can be greatly enhanced and extended to the Customer, Users and support staff by expanding the methods for registering, updating and querying requests. This can be achieved primarily using email and the Internet/Intranet for remote offices, although fax can also be a valuable tool. These methods are best exploited for activities that are not business-critical, which include registering non-urgent Incidents or requests, such as:*

- *incident product purchases*
- *application queries*
- *requests for equipment moves, installations, upgrades and enhancements*
- *requests for consumables.*

*For the support team, a number of benefits are derived, including:-*

- *support personnel are freed from unnecessary telephone interruptions*
- *workloads are better managed.*

## A Self-Service Strategy

### A Self-Service Strategy



- Gives some control to customers, optionally:
  - Log new incidents, change requests
  - Self-Help
  - Order goods or services
- Can reduce load on Service Desk
- Particularly useful 'out of hours' and for non-critical activities
- There are some inherent dangers of a self- service strategy
  - care is needed.

### Student Notes

Growth of Internet and Intranet has made this possible. Quite a few Service Management tools have a web front-end access or client.

- Can be used to do some self-help and diagnostic work by the user and log a call if this fails. Also used a lot to enable user to self-track progress rather than contacting Service Desk. Can be used to divert away from Service Desk analysts low priority or non-incident calls, giving the Analyst more time and focus on higher priority calls.
- Need to be aware of the potential to actually “double” your calls if the system fails or is not “user-friendly”. I.e. log the call to say the web front end is not working, and then log the call the user was going to log via the web!

---

## Outsourcing the Service Desk — Potential Benefits

### Outsourcing the Service Desk — Potential Benefits



- Financial savings
- Economies of scale
- Access to larger skill pool
- Improved staff and service cover
- Competitive marketplace

### Student Notes

- The major advantage in going with an Outsourcer is the financial savings to be had. This is due to the economies of scale that an Outsourcer can provide in that they have Service Desks set up to support multiple clients, which can be passed onto future clients.
- The Outsourcer can move SD Analysts between clients they support giving greater coverage and access to larger skill pools than can be achieved internally.
- The competitive marketplace means that Outsourcers are going to compete to give you the best possible deal, so again enhancing the savings and potential benefits you can gain.

## Outsourcing the Service Desk — Care Needed

### Outsourcing the Service Desk — Care Needed



- Viewing the SD as an overhead is damaging
- SD is the ‘window of service and professionalism’
- The intellectual capital should be protected
- Seek ‘vendor partnerships’ and long-term relationships

### Student Notes

- Viewing the SD as an overhead is damaging and SD is the ‘window of service and professionalism’. This is because morale on the SD will inevitably go down when it is known they are being outsourced. Most people feel unappreciated by the current employer and are therefore resentful, so do not strive to provide the best possible service under those circumstances. They are also usually apprehensive of what the new employer is going to do and so are usually not as co-operative as usual with new employer representatives. This leads to a downturn in the user perception of the Service Desk for the period prior to the handover.
- Intellectual Capital should be preserved – care should be taken in that when you outsource your Service Desk you are also giving away access to a lot of raw data about your organization and its operations, i.e. where does most of your data on how your IT department is performing come from?
- *You are buying a total solution and you should want your vendor to be a business partner. A sign of a good working relationship between yourselves and a supplying organization is that it is hard to tell the contracted staff from the full-time employees, in terms of their commitment and understanding of the Customers needs. A*

**Module 2**  
**Service Desk**

*professional vendor will seek a long-term relationship and repeat businesses in the form of additional product's upgrades, training and consultancy. (From the ITIL Service Support Book)*



---

## Question

### Service Desk Responsibilities



Which of the following activities is a responsibility of the Service Desk?

- A. Assessing the impact of changes
- B. Tracing the underlying causes of incidents
- C. Recording solutions to the problems which cause incidents
- D. Restoring the service to users as quickly as possible

## Student Notes

## Question

### Service Desk Functions



Which of the following is not a function of the Service Desk?

- A. A single point of contact between the customers/users and the IT department
- B. First-line incident management
- C. Business system support
- D. Management of the Known Error Database

## Student Notes

---

## **Module 3 — Incident Management**

## Mission of Incident Management

### Mission of Incident Management



To restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring the best possible levels of service quality

### Student Notes

Incident Management Process supports the mission statement by initially logging all incidents and then using diagnostic and escalation techniques to identify a resolution that will restore service to the affected user(s) as soon as possible. This may not be a permanent fix to the underlying cause (addressed in Problem Management), but rather a temporary workaround in order to maximize availability and hence productivity of systems.

## Scope of Incident Management

### Scope of Incident Management



The scope of incident management is very wide, and can include anything affecting customer service, for example:

- Hardware failure
- Software error
- Network faults
- Information request
- How do I...?
- Request for equipment moves
- Password re-set, changes
- New starters
- Request for consumables
- Service extension requests
- Performance issues

### Student Notes

While there is a specific definition for an “Incident” (see future slide) the actual start point for Incident Management is much wider. It is the Process that is responsible for logging all contacts to the Service desk (remember service desk is a Function not a Process). Once entered into the Incident Management Process the “incidents can be filtered to allow through into the rest of the process, true incidents and re-direct other enquiries (Service requests etc) to the correct procedure for their resolution.

## Objectives of Incident Management

### Objectives of Incident Management



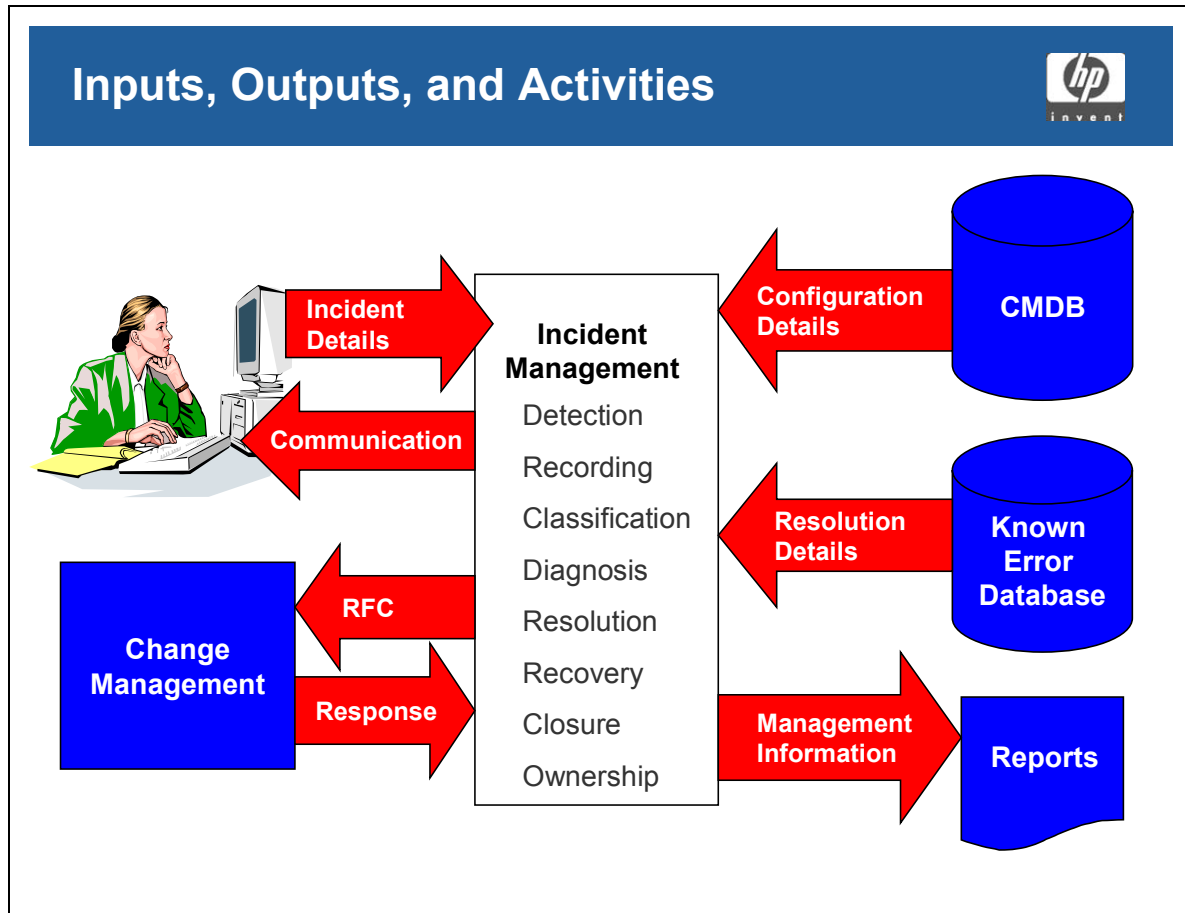
Ensure best use of resources to support the organization during service failures

- To log and track incidents
- To maintain meaningful records
- To deal with incidents consistently

### Student Notes

The Service desk will use the tools and techniques used in Incident Management (e.g. escalation) to enable the IT organization to quickly resolve the incident, without there being undue delay or the incident getting “lost”. The major benefit is that Incident Management means that you can resolve incidents in a consistent way that enables you to analyze information obtained during that resolution, in order to improve resolution times in the future.

## Inputs, Outputs, and Activities



### Student Notes

- The user in the top left hand corner is a key input into the process, being the first source of information in most cases (although automatic detection tools are becoming more common). There is a flow of information both coming from and going back to the user throughout the incident lifecycle (usually controlled through Service Desk)
- The CMDB (Configuration Management Database) (Top Right) is a primary source of information about the CI(s) (asset) involved in the incident. Also to see if there are any other current incidents that this particular incident could be related to.
- The KEDB (Known Error Database, actually part of the CMDB) (Middle Right), is used by Incident Management to look for any potential workarounds currently available for this type of incident.
- Change Management process (Bottom Left) is the process used to permanently resolve an incident. So the Output from the Incident Management Process (in some cases) is a Request For Change. This will, when actioned by the Change Management Process, lead to a permanent resolution

### Module 3

#### Incident Management

- The Central column shows the stages/phases that are gone through during the Incident Resolution Process.
  - Detection – actually identifying that an incident is taking place, this can either be by a user(s) or from automatic detection tools (e.g. BMC Patrol etc)
  - Recording – the actual logging of the incident
  - Classification – assigning a “type” to the incident to aid with both the functional escalation (i.e. deciding who to send the incident to in the first place if it cannot be resolved at first line), and for later Problem Management analysis.
  - Diagnosis – finding out the cause of the problem and identifying a resolution/workaround.
  - Resolution – applying the resolution/workaround
  - Recovery – bringing the CI back to operational status and restoring it to the user (i.e. reloading data, applications etc)
  - Closure – closing the incident (done by SD Analysts) , usually after a confirming contact with the user to make sure they are now back up and working OK
  - Ownership – This is in effect all the way through the lifecycle and ensures that the incident is not lost, unduly delayed, forgotten about etc.
- Usually a good point to bring up D2R3 (Detect, Diagnose, Repair, Recover, Restore).



---

## Definition — an Incident

### Definition — an Incident



“An *incident* is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service”

### Student Notes

The ITIL Book definition of an incident

## Definition — a Problem

### Definition — a Problem



“A *problem* is the unknown underlying cause of one or more incidents”

### Student Notes

The ITIL Book definition of a Problem

**Note** Problems are the responsibility of Problem Management not Incident Management. The reason we discuss it here is due to the relationship between Problems and Incidents.

## Definition — a Known Error

### Definition — a Known Error



“A *known error* is an incident or problem for which the root cause is known and for which a temporary workaround or permanent alternative has been identified.

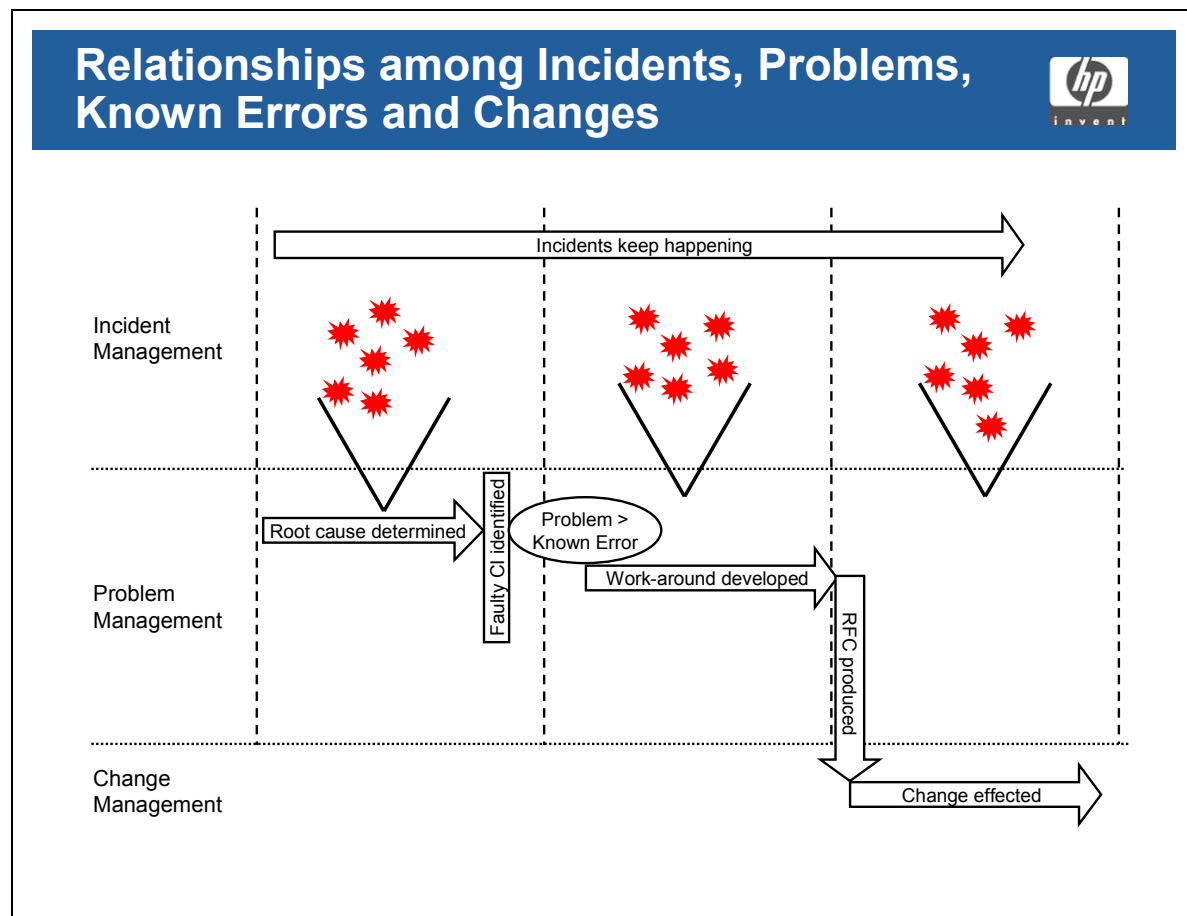
If a business case exists, a Request For Change (RFC) will be raised, but, in any event it remains a known error unless it is permanently fixed by a change.”

## Student Notes

The ITIL Book definition of a Known Error

**Note** Known Errors are the responsibility of Problem Management not Incident Management. The reason we discuss it here is due to the relationship between Known Errors and Incidents especially with regard to work arounds.

## Relationships among Incidents, Problems, Known Errors and Changes




### Student Notes

**NOTE:** An incident never “evolves” into a problem etc. It always remains an incident, problem or know error in its own right – there is only ever a relationship between an incident, problem etc !!!!

This slide shows the relationship between incidents and problems etc. Incidents NEVER become problems, they remain as incidents. The reason for this is that you may have 15 reported incidents that people cannot access e-mail, which upon investigation 14 are related to the identified Problem that the server is down, the 15th is that Outlook is corrupted !

The slide shows that incidents will keep happening and will be handled by the Incident Management process, while Problem Management and Change Management identify the route cause and establish a permanent fix for the problem (which continues to generate the other associated incidents)

## Example Coding System for Incident/Request Classification

Example Coding System for Incident/Request Classification			
			
<i>Type of Incident</i>	<i>Main Category</i>	<i>Sub-Category</i>	<i>Indication Priority</i>
<b>Failure</b>	<b>Software</b>	<b>Word processing</b>	<b>2</b>
		<b>Spreadsheet</b>	<b>2</b>
		<b>Business Application</b>	<b>1</b>
	<b>Hardware</b>	<b>Mainframe</b>	<b>1</b>
		<b>Work Station</b>	<b>2</b>
	<b>Etc.....</b>		
<b>Service Request</b>	<b>Password Reset</b>		<b>1</b>
	<b>Change Toner</b>		<b>3</b>
	<b>Help User</b>	<b>Office Software</b>	<b>3</b>
	<b>Etc.....</b>	<b>Business Application</b>	<b>2</b>

### Student Notes

Taken from the ITIL book.

This is an example of the type of classification that should be given to each incident. Most organizations will take this down 4 or 5 levels to help correct escalation and future analysis

E.g. Incident > Hardware > Laptop > Compaq > NC6000  
Incident > Software > E-Mail > MS Outlook > Non Delivery

## Impact + Urgency = Priority

### Impact + Urgency = Priority



#### Impact

- Affect on the business
- Defined in the SLA
- Based on user, service or number of items
- Same codes used in all disciplines
- Use tools to determine

#### Urgency

- Speed needed to resolve incident
- Extent it can bear delay

### Student Notes

This describes how the priority of an incident is decided upon, based on its Impact on the Business and the Urgency for which a resolution is required.

## Impact + Urgency = Priority

### Impact + Urgency = Priority



#### Priority

- Sequence of dealing with events
- Determined by impact, urgency and effort
- Not assigned by the user
- Decided outside the Service Desk


### Student Notes

This describes how the priority of an incident is decided upon based on its Impact on the Business and the Urgency for which a resolution is required.

Further explanation is required for the last statement on this slide

- **Decided outside the Service Desk** – The Service Desk DO assign Priorities to incidents. What this statement means is that the generic priority list and descriptions (e.g. the 1 – 5 that most organizations have and what they stand for) is decided by others rather than the Service Desk. (Usually jointly between the Customers and the IT provider (SLM/Problem Mgmt/Incident Mgmt etc.))

## Example of a Priority Coding System

Example of a Priority Coding System				
<i>Urgency</i>	<i>Impact</i>			
		High	Medium	Low
	High	1	2	3
	Medium	2	3	4
	Low	3	4	5
Priority Code	Description	Target Resolution Time		
1	Critical	1 hour		
2	High	8 hours		
3	Medium	24 hours		
4	Low	48 hours		
5	Planning	As planned		

### Student Notes

Taken from the ITIL Book



## Incident Status — Examples

### Incident Status — Examples



- New
- Accepted
- Scheduled
- Assigned / dispatched to specialist
- Work in progress (WIP)
- On hold
- Resolved
- Closed

### Student Notes

Each incident has a “lifecycle” – the status assigned to it is just a way of tracking it through that lifecycle. This helps Incident Management with tracking and escalation where required. This is an example of one but should be reasonably familiar to most Service Desk staff , as it is reasonably generic.

## Escalation

### Escalation



- Right number and level of resources
- To resolve incidents within the agreed time
- Defined in Problem Management
- Executed by the Service Desk
- Inform the user of the status
- Automatic

### Student Notes

Escalation is used to make sure that the incident is resolved in the quickest and most efficient way, and is not subject to undue delay in resolution.

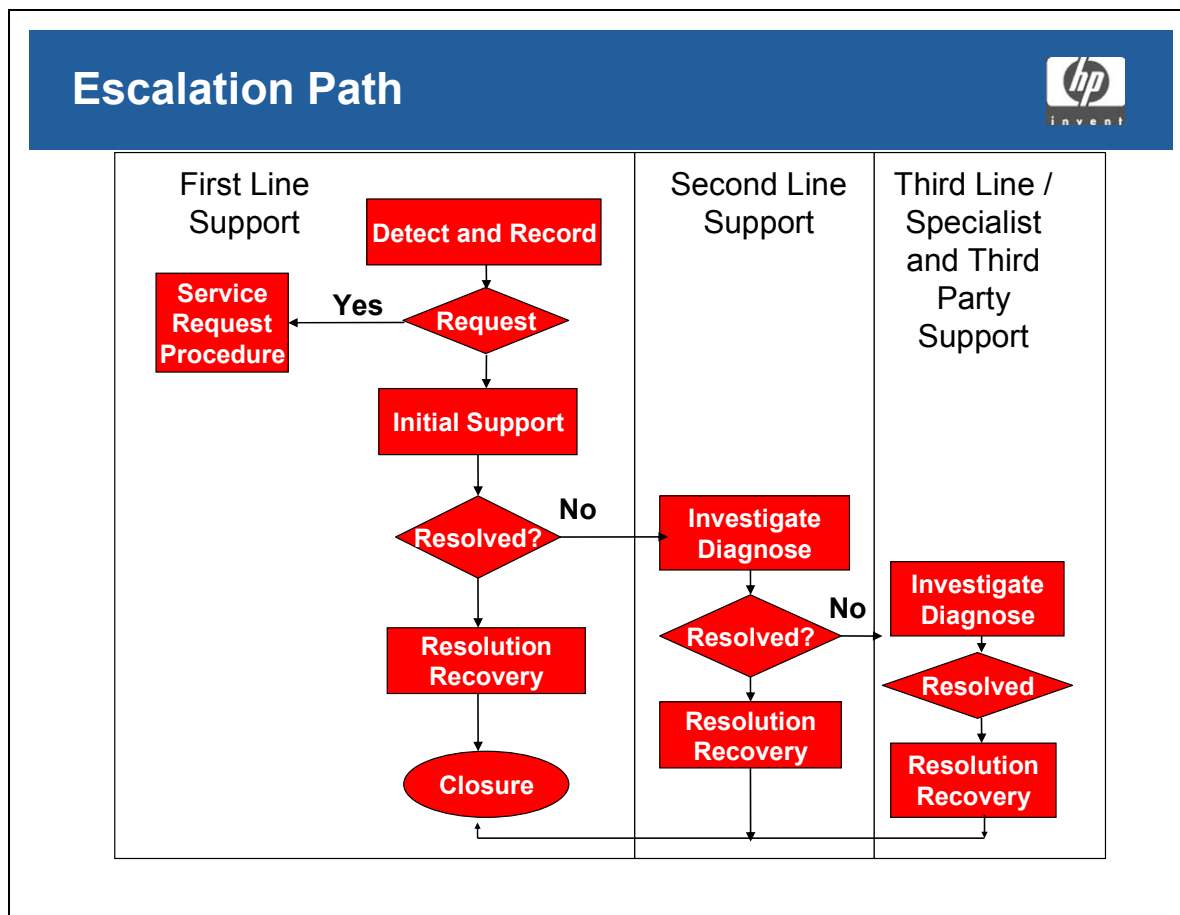
---

*NOTE:* Escalation paths are not solely defined by Problem Management but actually in conjunction with Incident and Service Level Management.

---

Escalation should be as automated as possible particularly where the trigger point is time based. Most Service Management tools these days allow you to do this.

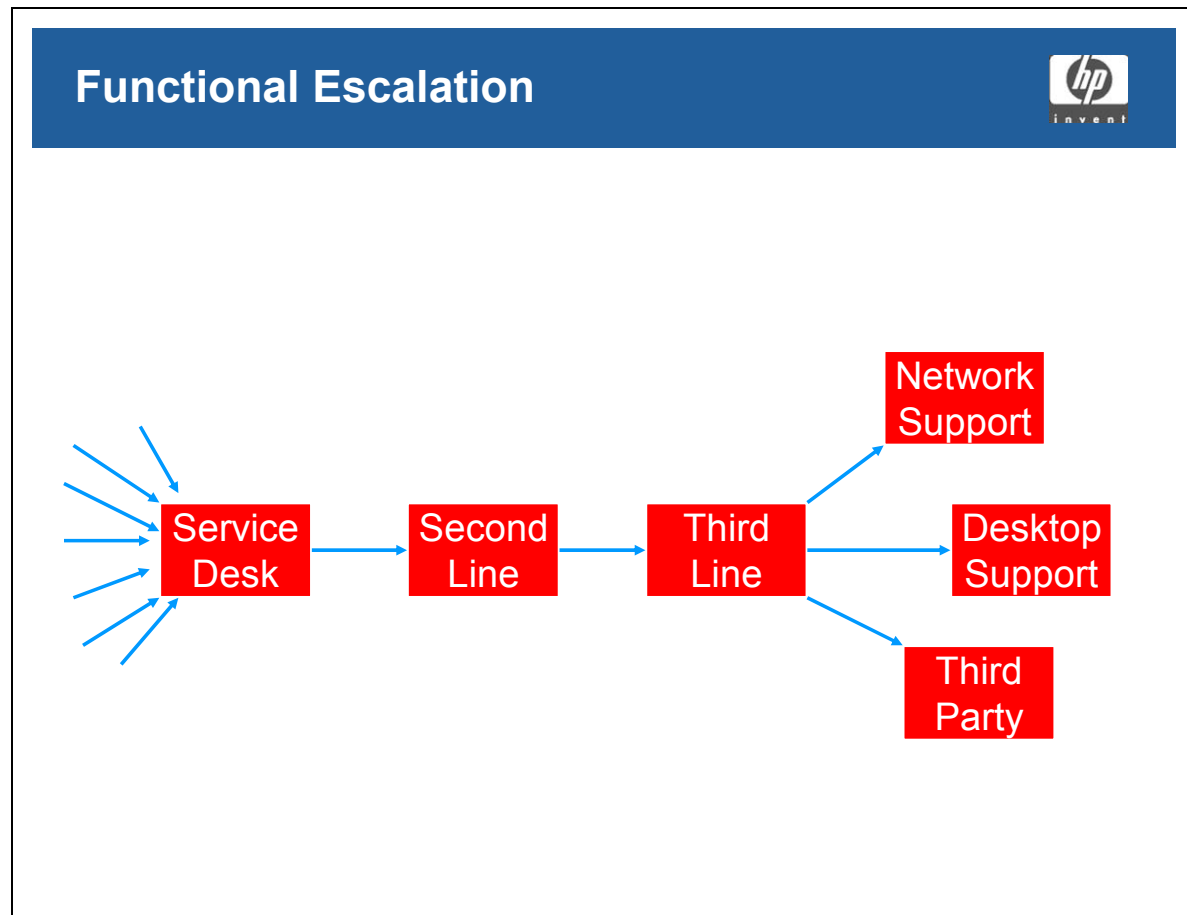
## Escalation Path



## Student Notes

This diagram shows the “functional” (explained in a future slide) escalation route for a typical incident. The call is received and logged by SD, determined to be an incident and First Line (e.g. SD themselves) initially attempts to resolve the incident. If they are not successful, they will escalate to second line support etc.

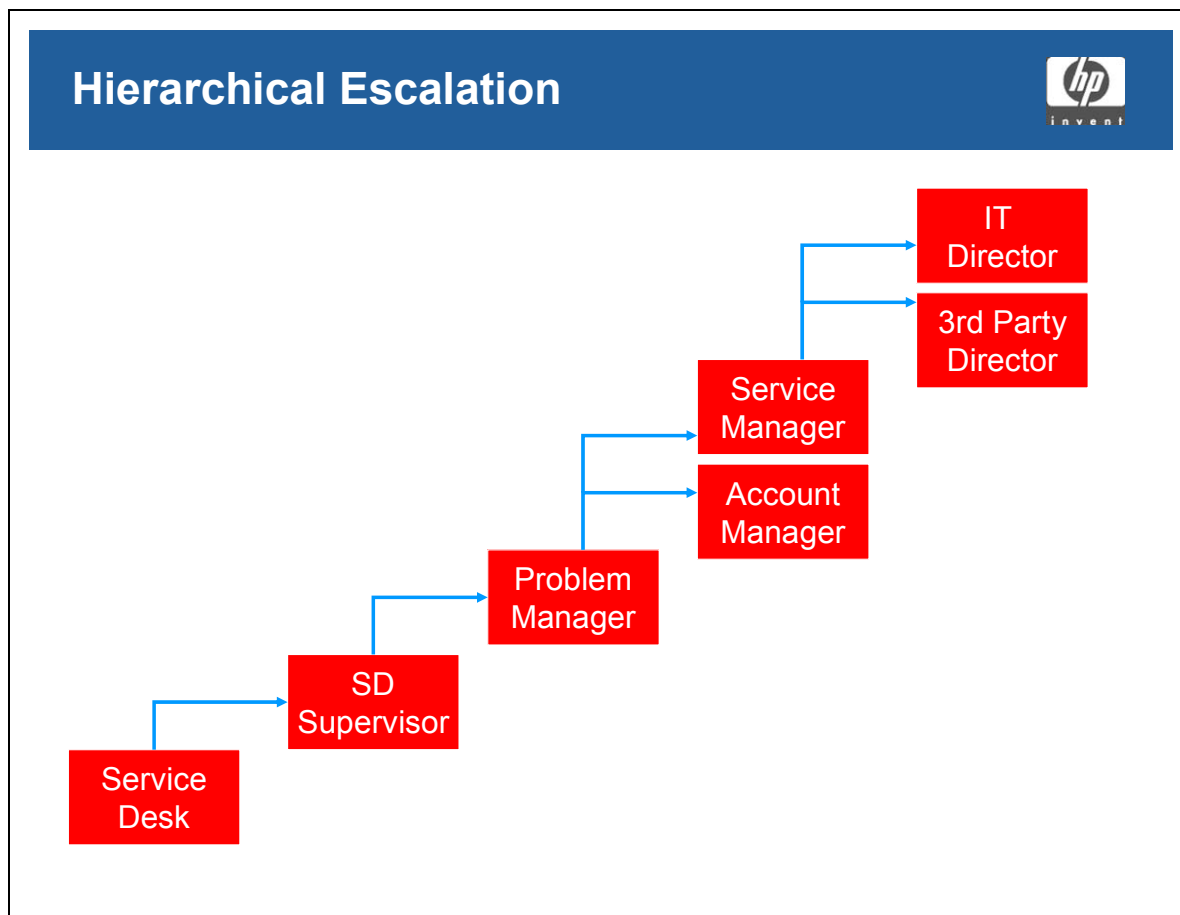
## Functional Escalation



### Student Notes

Example of a Functional Escalation route (i.e. down the technical expertise path)

## Hierarchical Escalation



### Student Notes

This is an example of a Hierarchical escalation path.

(NB this is an example and should not be taken to imply that the Problem Manager is ALWAYS in the escalation chain).

---

## Incident Manager Responsibilities

### Incident Manager Responsibilities



- Drive and monitor the efficiency and effectiveness of the Incident Management process
- Recommend and implement improvements
- Develop and maintain the Incident Management support tools
- Schedule and manage the work of Incident support staff (first-and second-line)

In many organizations, the role of Incident Manager is assigned to the Service Desk Supervisor.

### Student Notes

This is fairly self-explanatory. The only real point to make is that while someone is working on an incident then he is working directly for the Incident Manager (Matrix Management), and not necessarily for his direct Line Manager.

## Service Desk Support Analyst Responsibilities

### Service Desk Support Analyst Responsibilities



- Incident registration
- Initial support and classification
- Resolution and recovery of incidents if possible
- Escalation of incidents to support groups if necessary
- Ownership, monitoring, tracking and communication
- Review and closure of incidents

### Student Notes

These are the responsibilities of the Service Desk staff when using the Incident Management Process.

## Second Line Support Staff Responsibilities

### Second Line Support Staff Responsibilities



- Handling escalated incidents and service requests
- Incident investigation and diagnosis
- The resolution and recovery of assigned Incidents.
- Further escalation if needed
- Detection of possible Problems and the assignment of them to the Problem Management team

### Student Notes

These are the responsibilities of the Second (and Third) line staff when using the Incident Management Process.



## Question

### Service Desk Incident Logging



1. The Service Desk must record the impact of each incident so that the priority and escalation criteria can be established.
2. The Service Desk need not log an incident if a similar incident has already been recorded and is being investigated.

Which of the above statements is true?

- |                    |            |
|--------------------|------------|
| A. Only the first  | C. Neither |
| B. Only the second | D. Both    |

## Student Notes

## Question

### Incident Management Elements



Which of the following is least likely to be used in the Incident Management process?

- A. The incident impact code
- B. The cost of the faulty item
- C. The incident category
- D. The make/model of the faulty item

## Student Notes

---

## **Module 4 — Problem Management**

## Mission of Problem Management

### Mission of Problem Management



To minimize the disruption of IT services by organizing IT resources to resolve problems according to business needs, preventing them from recurring and recording information that will improve the way in which IT deals with problems, resulting in higher levels of availability and productivity

### Student Notes

Problem Management Process supports the mission statement by identifying the underlying causes of incidents and problems, finding a workaround and creating a Known Error and propagating that workaround (usually via the Known Error Database), and then raising a Request For Change (where appropriate) for a permanent resolution.

## Scope of Problem Management

### Scope of Problem Management



- IT problems that affect IT services
- Recurring Incidents/Problems
- Pro-active Problem Management
- Major incidents, if required
- Entry to ITSCM
- Vendor liaison

### Student Notes

- IT problems that affect IT services, usually as a result of one or more incidents
- Recurring Incidents/Problems
- Pro-active Problem Management – actually trying to find and alleviate problems either before they occur or at least in the early stages of a wide outbreak, and proactively applying the workaround to prevent the problem occurring elsewhere.
- Major incidents (extremely high impact on the business), if required. The Problem Manager is a likely candidate to become involved in Major/High priority incidents at an early stage due to the tools and techniques he can bring to bear on the incident.
- Entry to ITSCM (IT Service Continuity) – this is one possible entry route (although a likely one for technically driven invocations of the IT Service Continuity Plan)
- Vendor liaison – During the resolution of a Problem involving 3rd party equipment or technicians, the Problem Manager is responsible for the management of those people and liaison with the 3rd party vendor organization.

## Objectives of Problem Management

### Objectives of Problem Management



- To ensure that problems are identified and resolved
- To prevent problem occurrence and recurrence
- To reduce the overall number of IT incidents
- To minimize the impact of problems and incidents
- To ensure that the right level and number of resources are resolving specific problems
- To ensure that vendors comply with their contracts

### Student Notes

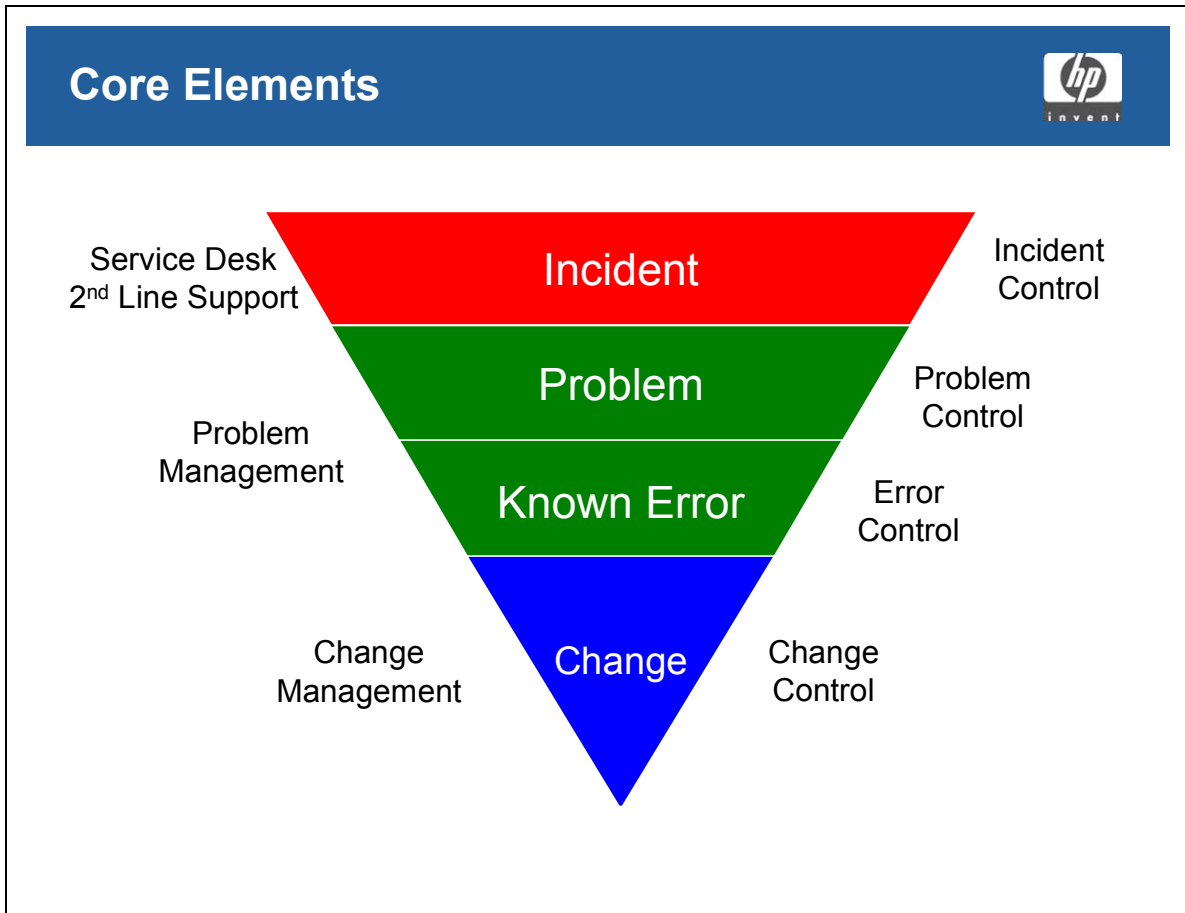
These are standard Problem Management objectives

---

*NOTE:* To ensure that vendors comply with their contracts –Here we are talking specifically about where a vendor's non-compliance is causing problems to occur in the IT infrastructure. This is generally a Service Level Management Issue from a day to day/operational point of view.

---

## Core Elements



## Student Notes

This diagram shows the relationship between the Incident, Problem and Change Management processes, and where the relevant control activities take place and who controls them.

---

## Incident Management and Problem Management

### Incident Management and Problem Management



#### Incident Management

- Restores agreed levels of services
- Uses workarounds

#### Problem Management

- Diagnoses the root cause of incidents
- Identifies a permanent solution
- May take longer than Incident Management

### Student Notes

This slide shows the basic difference between the Problem Management and the Incident Management Process.

- Could be a good point to bring up the fact that ITIL recommends that you do not make your Incident Manager your Problem Manager as well due to the potential inherent conflict between the two roles.



## Problem Control

### Problem Control



- Identify and record problem
- Classify problem
- Investigate and diagnose problem
- Root cause analysis

### Student Notes

This slide shows the stages that are present during Problem Control

- Identify and record problem – analogous to detecting and logging an incident. Here we make sure that there is a potential problem and not just an incident.
- Classify problem – usually using the classification used in logging the incident in the first place but here the category is verified and confirmed.
- Investigate and diagnose problem – finding the symptoms and clues to enable the investigation to decide the actual fault
- Root cause analysis – determining the unknown underlying cause of the problem

## Error Control

### Error Control



- Identify and record errors
- Assess error
- Record error resolution
- Monitor resolution
- Close error

### Student Notes

This slide shows the stages that are present during (Known) Error Control

- Identify and record errors – make sure that a problem being handed over from Problem Control, has a known cause and a workaround before it can be accepted and logged in the Known Error database. .
- Assess error - Most organizations do a “sanity” check on the root cause and workaround at this stage, and look to update the workaround with any enhancements that have come to light since original investigation.
- Record error resolution – Make sure that the error is recorded and propagated out to the appropriate support organizations. Also this is the point at which the RFC will be raised for a permanent resolution
- Monitor resolution – liaise with Change Management to ensure the problem is permanently resolved
- Close error – close and remove the Known Error.

## Known Errors — Development

### Known Errors — Development



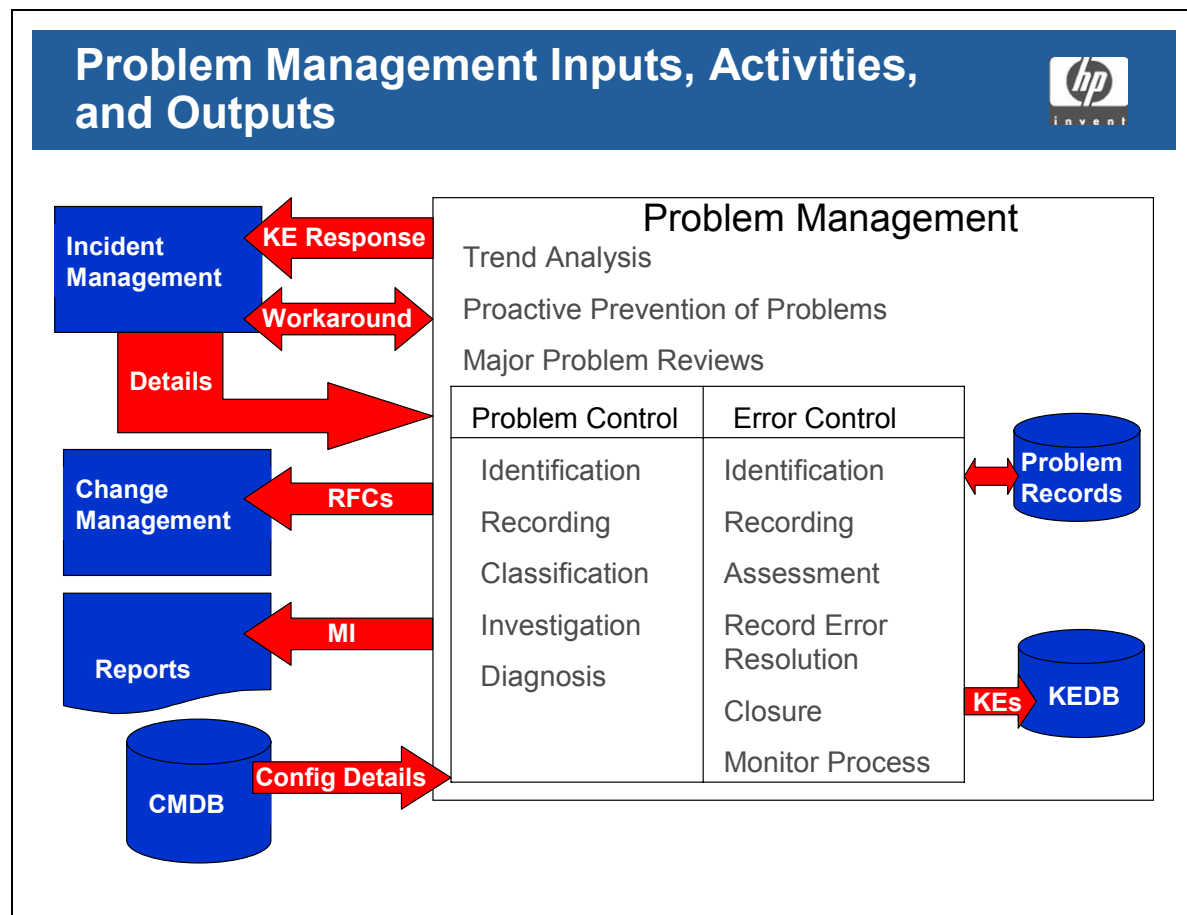
Sometimes a system might be allowed to be released into the live environment even though known errors have been detected during testing.

Problem Management needs to ensure any such known errors, and any resolutions, are recorded in the Known Error Database.

### Student Notes

Known Errors are best picked up from the Application Developers prior to any new system “going live”. In most cases the Application Developers will know the known bugs a system is being released with and the workarounds associated with those bugs, as they will have found them and worked on them during the pre-release testing phase. These should be collected and made available in the KEDB prior to going live.

## Problem Management Inputs, Activities, and Outputs



### Student Notes

Diagrammatical representation of the previous four slides

## Previous Incident/Problem Data

### Previous Incident/Problem Data



Problem Manager must ensure:

- Data is properly recorded
- Data is regularly inspected and maintained
- Known Errors are recorded in a suitable Database
- Support staff are educated to capture and record high-quality data

### Student Notes

This slide shows the responsibilities Problem Management has for the collection and maintenance of data (mainly from Incident Management/Service Desk), to ensure that they have the correct/sufficient data on which to work.

---

## Proactive Problem Management

### Proactive Problem Management



Proactive Problem Management covers the activities aimed at identifying and resolving Problems before Incidents occur. These activities are:

- Trend analysis
- Targeting support action
  - Internal and external
- Targeting preventative action
- Feed-back of information to the relevant people

### Student Notes

- Trend Analysis is the ability to analyze data to spot a series of linked events or consequences and act upon that “trend”
- Targeting support action is supplying a workaround or avoidance instructions to users/support organisations/3rd parties to prevent further and/or future incidents from occurring.

## Problem Management Techniques

### Problem Management Techniques



- Pain Value Analysis
- Ishikawa Diagrams
- Kepner and Tregoe Analysis (see notes)
- Major Problem Reviews (see notes)

### Student Notes

These are the names of 4 problem management techniques. PVA and Ishikawa are explained on the next few slides.

- Kepner & Tregoe - Charles Kepner and Benjamin Tregoe developed a useful method to analyze Problems. They distinguish the following five phases for Problem analysis:
  1. Defining the Problem
  2. Describing the Problem with regard to identity, location, time and size
  3. Establishing possible causes
  4. Testing the most probable cause
  5. Verifying the true cause.
- Major Problem Review - when a Major Problem has been resolved, a review should be held. The appropriate people involved in the resolution should be called to the review to determine:
  - What was done right?
  - What was done wrong?
  - What lessons can be learned?
  - How to prevent the Problem from happening again?

## Pain Value Analysis

### Pain Value Analysis



Calculate pain value:

Pain value = No. of incidents x duration x severity x weighting factor

Address in order of pain value

Diminishing scale of return

- The eighty-twenty rule (80% of benefits in first 20% of effort)

### Student Notes

This is a snapshot technique to show what is causing the most “pain” to an organization at that point in time.

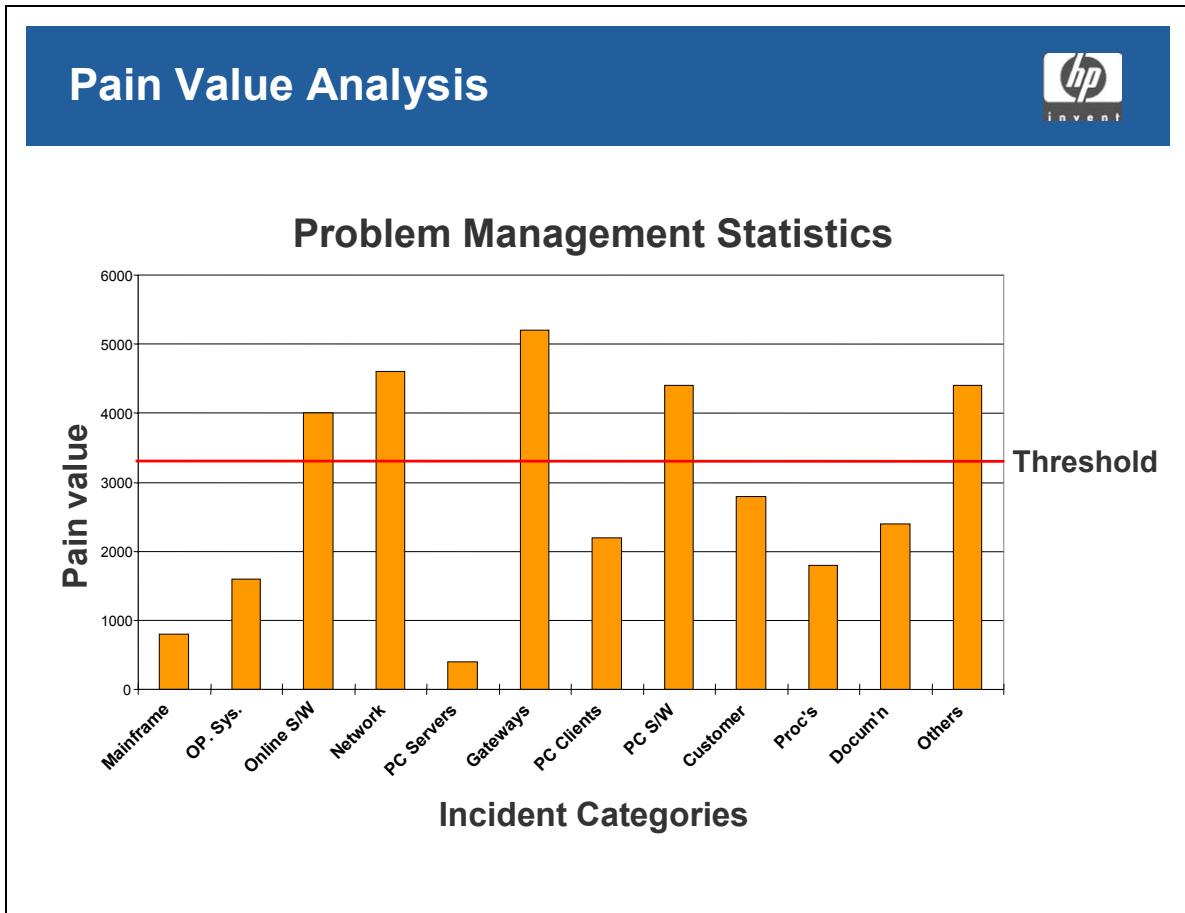
The calculation is made as shown (for severity read priority and in most cases you will need to reverse this e.g. if you have a priority scale of 1-5 with 1 being the most severe impact then you will need to multiply these incidents by 5, low impact incidents i.e. severity 5 will need to be multiplied by 1).

Something like the graph on the next slide will result.

Diminishing scale of return – use this rule to decide how much of each “bar” to tackle, i.e. it is unlikely that the gateway problems in the graph on the next slide are all down to one incident type. Handle the most common cause first and don’t try to eliminate all the problems (hence 80/20 rule)

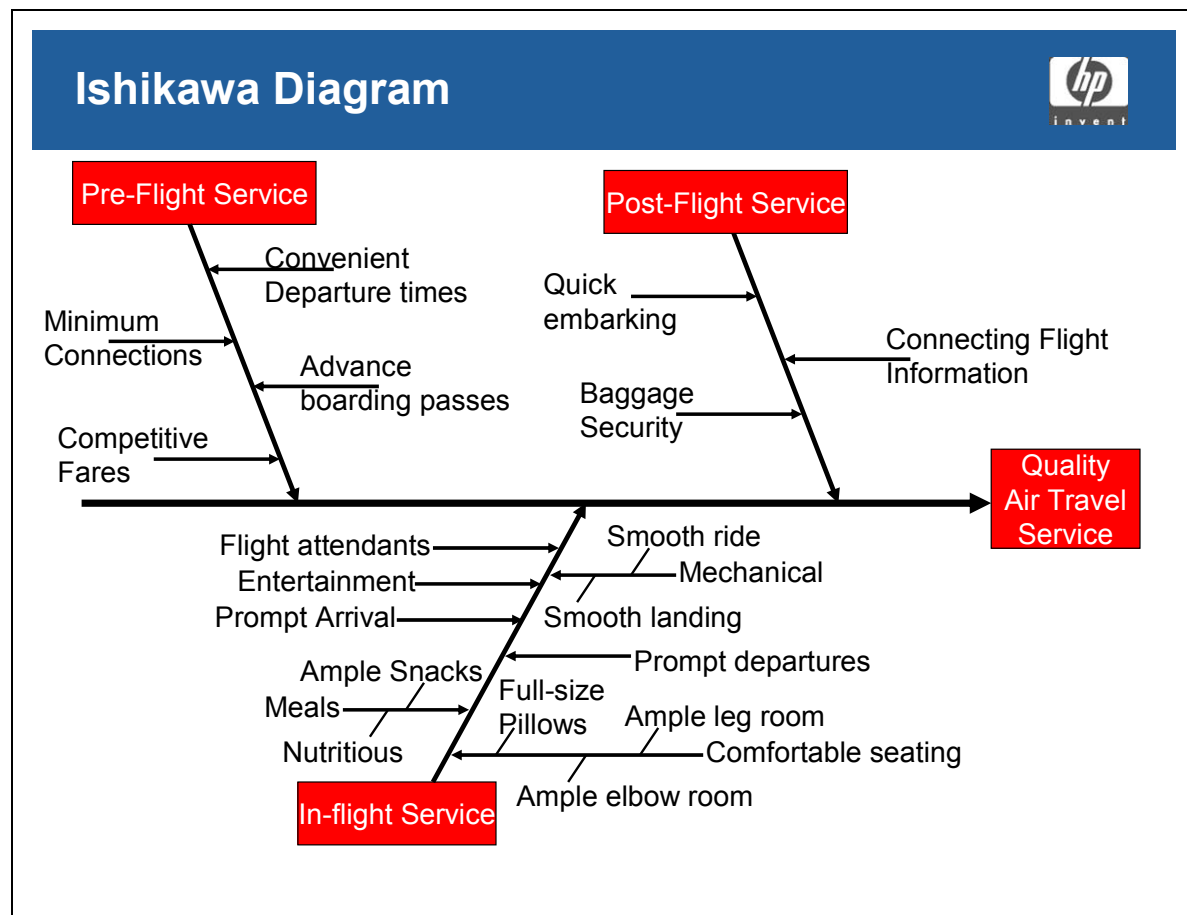


## Pain Value Analysis



## Student Notes

## Ishikawa Diagram



### Student Notes

Also known as "Fishbone" Diagrams, this is a way of taking a large complex problem and breaking it down bit by bit into manageable portions. The actual diagram is a real one based on one produced by SAS (Scandinavian Airline Services) and shows how the large problem of "providing what is considered to be a Quality Airline Service" can be broken down to relatively small and easily solvable problems (i.e. providing ample snacks)

## Question

### Logging Responsibility



A user calls the Service Desk to report that their PC locks-up every time a certain application is used.

Which discipline has overall responsibility for ensuring that the underlying cause is traced and recorded?

- A. The Service Desk
- B. The desktop support team
- C. Problem Management
- D. Application development

## Student Notes

## Question

### Terminology



Which two terms best describe the cause and the diagnosis of a fault?

- A. Incident and problem
- B. Problem and change request
- C. Problem and known error
- D. Configuration item and attribute

## Student Notes

---

## **Module 5 — Configuration Management**

## Mission of Configuration Management

### Mission of Configuration Management



To identify, control and audit the information required to manage IT services by defining and maintaining a database of controlled items, their status, lifecycles and relationships and any information needed to manage the quality of IT services cost effectively

## Student Notes

### Mission

*To identify, control and audit the information required to manage IT services by defining and maintaining a database of controlled items, their status, lifecycles and relationships, and any information needed to manage the quality of IT services cost effectively.*

Configuration Management supports this mission through:

- Identification
- Control
- Status
- Audit and verification

of all the items that comprise the IT infrastructure AND which are under the control of Configuration Management.

A database of these items — the Configuration Management database (CMDB) — is updated after every change to the IT infrastructure. By so doing, Configuration Management ensures that complete and accurate information about the IT infrastructure can be given to the rest of the IT organization, thereby supporting their activities in the ITIL areas of Service Support and Service Delivery.

The Configuration Management process provides a sound foundation for the Change Management and Release Management processes

## Scope of Configuration Management

### Scope of Configuration Management



#### Configuration Management

- All information to manage IT components

#### Asset Management

- Accountancy process
- Items above a certain value
- Financial information

## Student Notes

**Configuration Management** covers the identification, recording and reporting of all controlled IT components e.g. HW, SW, documents etc., together with their status and relationships.

The 'Scope' of Configuration Management is defined by two elements:

- The range of responsibility of Configuration Management, and
- The breadth of the Configuration Management Database.

Correctly setting the 'Scope' of Configuration Management is one of the critical management decisions when establishing the ITIL processes. Too narrow a scope can result in other processes failing to achieve their goals (through lack of necessary information). Too broad a scope can result in the process becoming unmanageable and can lead to failure of the ITIL implementation through the withdrawal of management support.

**Asset Management** is specifically an accountancy process that focuses on assets above a certain value, together with details about their business unit, financial history and location. Configuration Management enables Asset Management by recording the information needed as part of the Configuration Management Database (CMDB).



## Objectives of Configuration Management

### Objectives of Configuration Management



- Identify and record infrastructure information
- Control information in the CMDB
- Leads to improved service quality (indirectly)
- Supports license management
- Ensure infrastructure information is up to date
- A basis for Service Management processes
- Information about the status of the infrastructure
- Management information

### Student Notes

- To identify and record information about the IT assets and configurations required to manage IT services
- To control the information in the database
- Indirectly leads to improved service quality by enabling the IT organization to provide the optimal service to its customers at costs it can justify to them and itself
- Supports license management
- To ensure that infrastructure information is up to date, and accurately reflects the actual infrastructure
- To provide a basis for the management of IT Service Management processes
- To provide information about the status of infrastructure components
- To provide a source for management information related to IT Infrastructure management

## Core Elements of Configuration Management

### Core Elements of Configuration Management



- P Planning
- I Identification
- C Control
- S Status Accounting
- V Verification

### Student Notes

## Planning for Configuration Management

### Planning for Configuration Management



- Analyze current configurations
- Assess the organizational context
- Assess the policies of related processes
- Define the key interfaces
- Agree key structures, roles and operation
- Identifying library and database locations
- The Configuration Management Plan

### Student Notes

Steps in the planning process include:

- Analyzing current configurations and assets
- Assessing the organizational context within which Configuration Management will be implemented
- Assessing the policies of related processes
- Identifying key project, supplier, development and support groups
- Agreeing the key structures, roles and operation of the Configuration Management process itself
- Identifying the location of the various libraries and databases used in Configuration Management

One output is a Configuration Policy and Strategy, which outlines the objectives and critical success factors of Configuration Management. The Configuration Management Plan will include the Policy and Strategy and the project milestones.

## Identification

### Identification



#### Logical

- What items need to be recorded?
- What do we need to know about them?

#### Physical

- Marking items that are under Configuration Management control

## Student Notes

This addresses the selection and identification of the configuration structures for all the Configuration Items in the IT infrastructure. It also covers the selection and identification of the owners of those items, the relationships between items and the configuration documentation associated with those items.

### Physical and Logical Identification

Identification has two aspects:

- **Logical:** This means identifying what items need to be recorded and what information is recorded about them.
- **Physical:** This means marking items to identify which items are under Configuration Management control. This could be a bar code or colored sticker.

## Naming Conventions

### Naming Conventions



- Unique
- Clearly visible
- Consistent with the organization
- Copy and version numbers
- Plan for growth

### Student Notes

Most of the work done in Configuration Management has to do with logical identification. Some basic principles are:

- CIs must be uniquely identified
- The identification must be prominent and clearly visible
- Be consistent with naming conventions used by the organization and its vendors
- Copy and version numbers must be provided for
- Plan for growth

## What Do We Need to Identify?

### What Do We Need to Identify?



#### **Configuration**

- Anything that needs to be controlled

#### **Configuration Item (CI)**

- A component within a configuration
- A configuration in its own right

#### **CI Type**

- e.g. software products, business systems, system software, etc.

#### **Attribute**

- Describes a CI

## Student Notes

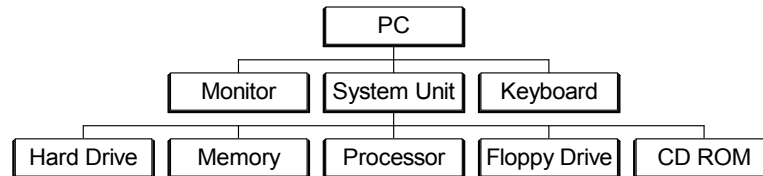
### **Configuration**

A configuration is anything that needs to be controlled, and could include:

- Hardware
- Software
- Documentation
- Networks
- People
- Changes, incidents, problems
- Procedures
- Anything else that needs to be controlled

## **Configuration Item**

This is a component within a configuration. What can be confusing is that a CI could also be a configuration in its own right. The following diagram shows how a CI could also be seen as a configuration:



In this diagram, the System Unit is a CI and a configuration. To overcome this confusion, ITIL refers to all controlled items as Configuration Items.

A key decision is how far a configuration is broken down into CIs. There are three principles that help to define this:

- CIs should only be broken down to their lowest level of independent change
- The level of breakdown, and the type of information kept, will depend on who needs the information and how they will be using it
- The value of the information must exceed the cost of collecting it

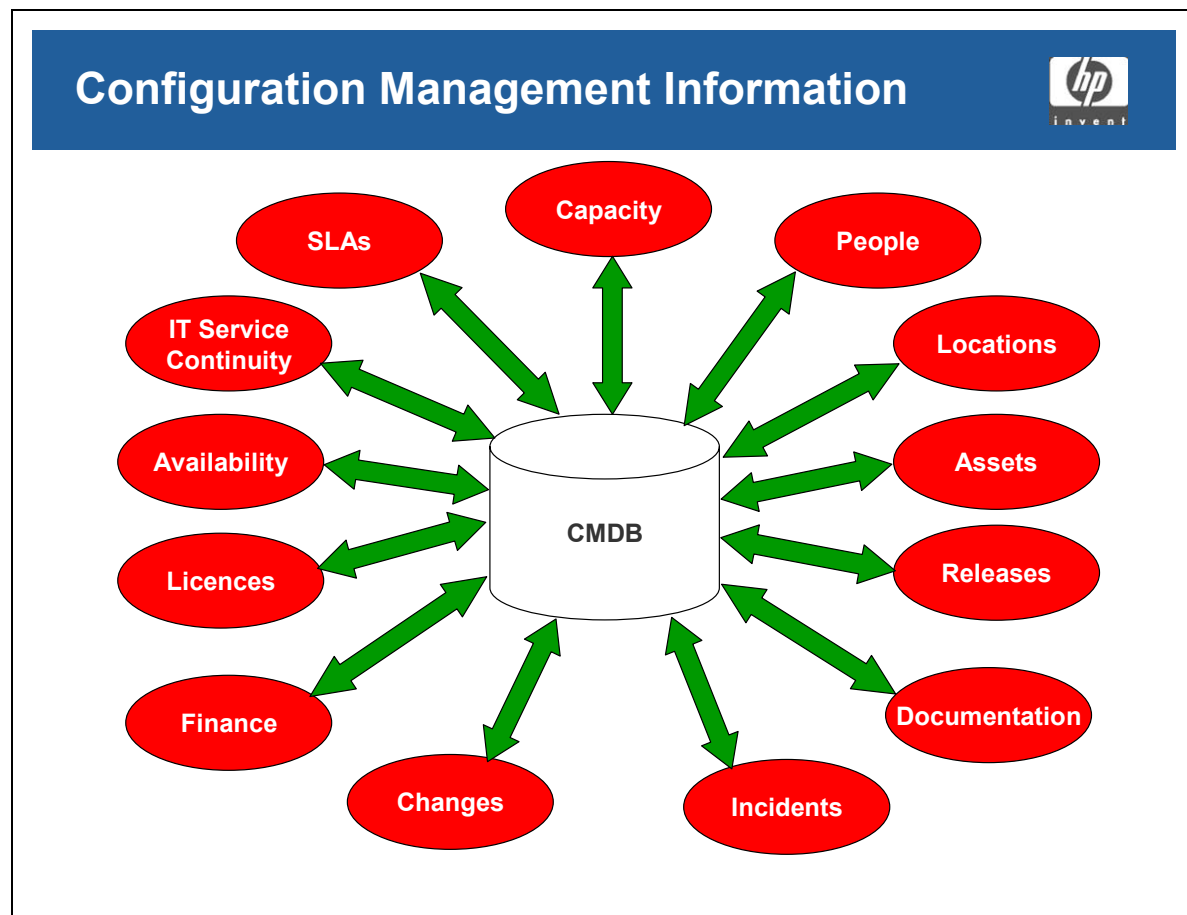
## **CI Types**

Components should be classified into CI types because this helps to identify and document what is in use, the status of the items and where they are located. Typical CI types are: software products, business systems, system software, servers, mainframes, workstations, laptops, routers and hubs

## **Attribute**

An attribute is simply a piece of information that can be recorded to describe a CI.

## CMDB

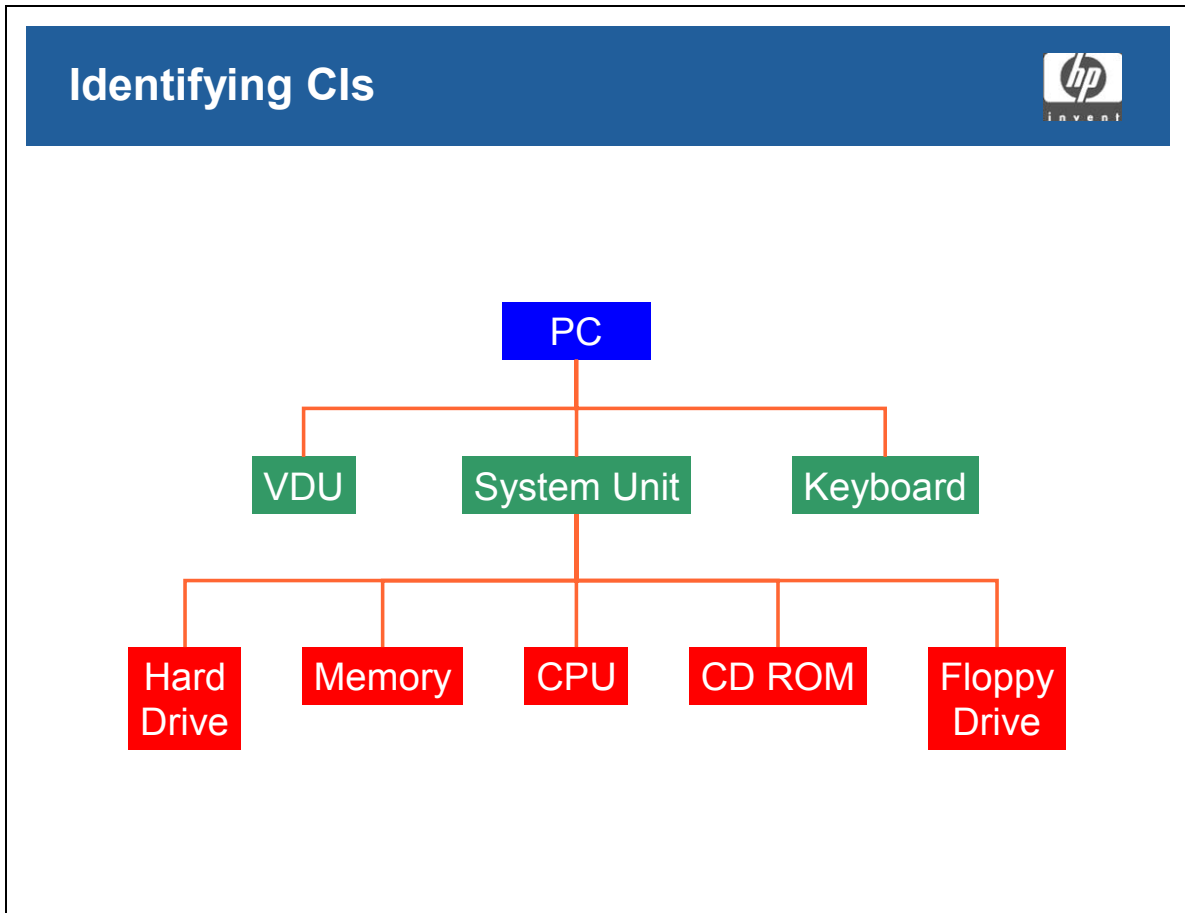


### Student Notes

Please note that not all those items shown above are CIs. The purpose of the diagram is to demonstrate the kind of information found in a CMDB.



## Identifying CIs



## Student Notes

## Identifying CIs — Level of Breakdown

### Identifying CIs — Level of Breakdown



- Lowest level of independent change
- Who are you and what are you doing?
- Information value

### Student Notes

**Remember:** A key decision is how far a configuration is broken down into CIs. There are three principles that help to define this:

- CIs should only be broken down to their lowest level of independent change
- The level of breakdown, and the type of information kept, will depend on who needs the information and how they will be using it
- The value of the information must exceed the cost of collecting it (including the amount of database space and maintenance required)

Choosing the correct level of breakdown is a balance between:

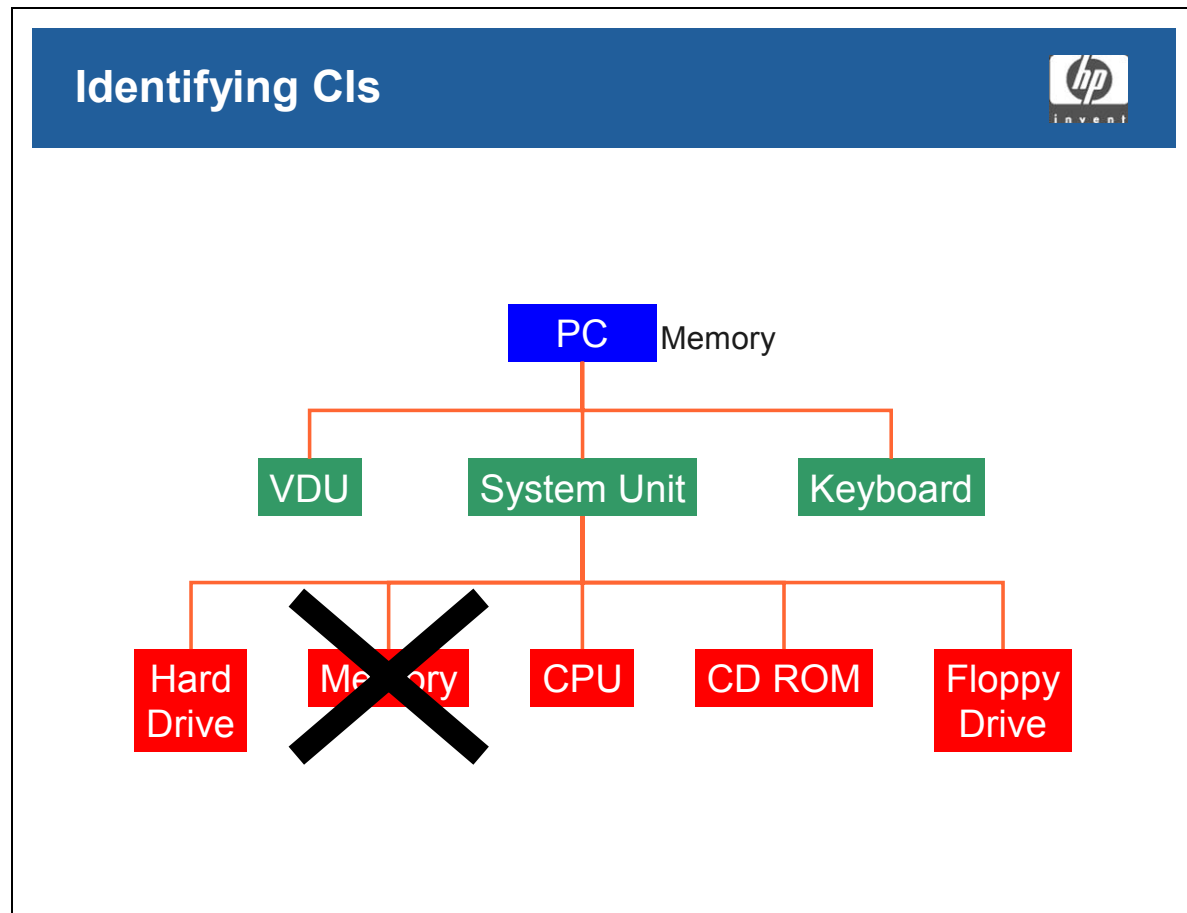
- What information is available?
- What level of control is appropriate?
- Which resources and what level of effort are required to support it?

In some cases, further breakdown is not possible, e.g. where the configuration is owned and managed by another organization. Here it is important to identify the relationships with the configuration so that any dependencies can be included in the SLM process. Any performance specifications, contractual obligations or other deliverables should be included as attributes of the configuration.

The breakdown level should be reviewed regularly. This will ensure:

- No unnecessary data is being stored and maintained, resulting in higher costs
- Any additional data requirements are accommodated in a controlled way

## Identifying CIs



## Student Notes

## What Do We Need to Identify? (1 of 3)

### What Do We Need to Identify? (1 of 3)



#### Relationship

- Primary
  - Parent/child (part of)
- Secondary
  - Connected to
  - User of

#### Baseline

- Snapshot of a CI at a time or stage
- What did a CI look like before a change?
- Reverting to a previous version of a CI
- Simplify data capture
- Simplify database design

## Student Notes

### Relationship

A relationship is a link or association that exists between one CI and other CIs. Relationships can be primary (hierarchical) or secondary (temporary or “used by”).

The relationships between CIs should be stored so as to provide dependency information. For example:

- a CI is a part of another CI (e.g. a software module is part of a program, a server is part of a site infrastructure) - this is a 'parent/child' relationship

a CI is connected to another CI (e.g. a desktop computer is connected to a LAN)

a CI uses another CI (e.g. a program uses a module from another program, a business service uses an infrastructure server).

## **Module 5**

### **Configuration Management**

There may be many more types of relationships, but all of these relationships are held in the CMDB - this is one of the major differences between what is recorded in a CMDB and what is held in an asset register.

### **Baseline**

A baseline is a snapshot of a CI at a specific time or stage in its lifecycle. It can also be seen as a "Standard CI". Baselines can be used to:

- Identify what a CI looked like before a change
- Revert to a previous version of a CI
- Simplify the capture of information about CIs
- Simplify database design

## What Do We Need to Identify? (2 of 3)

### What Do We Need to Identify? (2 of 3)



#### Variant

- A baseline with minor differences

#### Lifecycle

- Stages in the life of a CI
- Allow CIs to be moved, tracked and checked for
  - Cost, time and specification
  - Authorization
  - Completion
- Allows checking for
  - Responsibility
  - Progress
  - Problems

## Student Notes

### Variant

A variant is a baseline with some minor differences. For example a baseline could be a PC with an English or German keyboard.

### Lifecycle

A lifecycle refers to the stages that occur during the life of a CI. Each CI has its own lifecycle, and CIs of the same type will share the same lifecycle.

By defining lifecycles, Configuration Management allows CIs to be moved and tracked from stage to stage in a controlled manner. CIs can then be checked to see whether they are:

- To cost
- On time
- Complete
- To specification
- Authorized

## **Module 5**

### **Configuration Management**

Specifying lifecycles also allows checking during a stage for:

- Responsibility
- Progress
- Problems



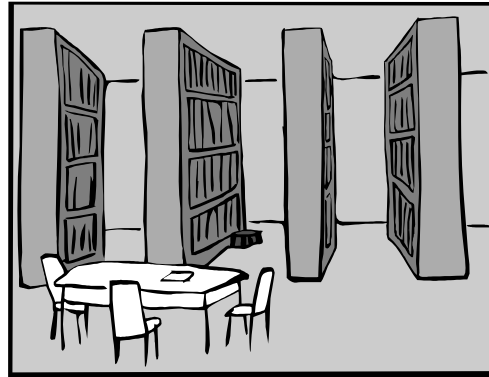
## What Do We Need to Identify? (3 of 3)

### What Do We Need to Identify? (3 of 3)



#### Software and document libraries

- Contents, location and medium
- Conditions for entering an item
- Protection and recovery
- Conditions of use
- Access controls



## Student Notes

### Software and Document Libraries

A controlled library is a collection of software or document CIs of a known type and status. Access to items in a controlled library should be restricted. Libraries should be identified with the following information:

- Contents, location and medium
- Conditions for entering an item
- How to protect and recover libraries
- Conditions of use and access controls

---

## Configuration Management's Responsibility to License Management

### Configuration Management's Responsibility to License Management



- Ensure legality of software environment
- Configuration Management audit enables software license monitoring and control
- Enable Release Management software control responsibilities

## Student Notes

### License Management

Company directors, senior managers, and others are liable for ensuring that their organization complies with the law. Ignorance is not an acceptable defense and does not absolve the company from legal proceedings.

Configuration Management auditing enables an enterprise to monitor and control software licenses throughout their lifecycle. Software license structures, corporate and multi-licensing schemes, need to be understood and communicated to service-provider staff and Customers. Therefore Configuration Management needs to link software license control to these corporate guidelines as well as to disciplinary procedures detailed within the organization's Security Policy.

License Management also enables Release Management to meet its responsibilities when it comes to software rollouts as one of their tasks is to ensure that all purchased or otherwise obtained software complies with legal obligations or restrictions.

## Configuration Control

### Configuration Control



#### Information in the CMDB

- Access
- Changes
- Adding new items

#### Examples of controls

- Registering new CIs
- New software
- Versions of CIs from Release Management
- License control
- Decommissioned CIs

## Student Notes

### Controlling Information in the CMDB

Control is concerned with the information held in the CMDB:

- Access to it
- Changes to it
- Adding new items

Control over the CMDB is critical to the efficient and effective working of Configuration Management and the ITIL processes that depend on it. 'Control' ensures that no CI is added, modified or deleted without the appropriate permissions and controlling documentation (eg. approved change request, updated specification).

## **Module 5**

### **Configuration Management**

Configuration Management ensures that only authorized and identifiable CIs are recorded in the CMDB. Examples of these controls are:

- Registration of new CIs
- New software, either developed in house or purchased
- Versions of CIs from Release Management
- License control
- Updating decommissioned CIs

## Configuration Control

### Configuration Control



- ITSM processes exercise physical control
- Configuration Management makes it possible by exercising control of the information
- To achieve control
  - Agree and freeze CI specification
  - Only allow changes through Change Management

### Student Notes

Other IT Service Management processes can assist in these tasks, but Configuration Management is responsible for the data in the database, and will have to define strict controls to manage access.

Control requires:

- The specification of CIs is frozen and agreed.
- Only changes that have been authorized by Change Management procedures will be allowed.

## Configuration Status Accounting

### Configuration Status Accounting



- Uses lifecycles and attributes
- Records and reports on
  - Current data
  - Historical data
- Can be predefined or *ad hoc*

## Student Notes

### Tracking the Status of CIs

Status accounting uses the lifecycles and attributes to track and update the status of CIs.

Status accounting is responsible for the recording and reporting of all current and historical data for all CIs. These reports can be produced to pre-defined criteria or they can be taken from the CMDB when required.

Examples of useful reports could be:

- The number of incidents for a CI during a period
- A history of the changes to one CI during a period
- The total amount spent with a supplier during the year
- How many PCs have a specific version of operating system

## Configuration Audit and Verification

### Configuration Audit and Verification



- Does the CMDB reflect reality?
- Accuracy is improved by
  - Active rather than passive CMDB
  - Automatic updating
  - Integration with other processes
  - Automatic checks

## Student Notes

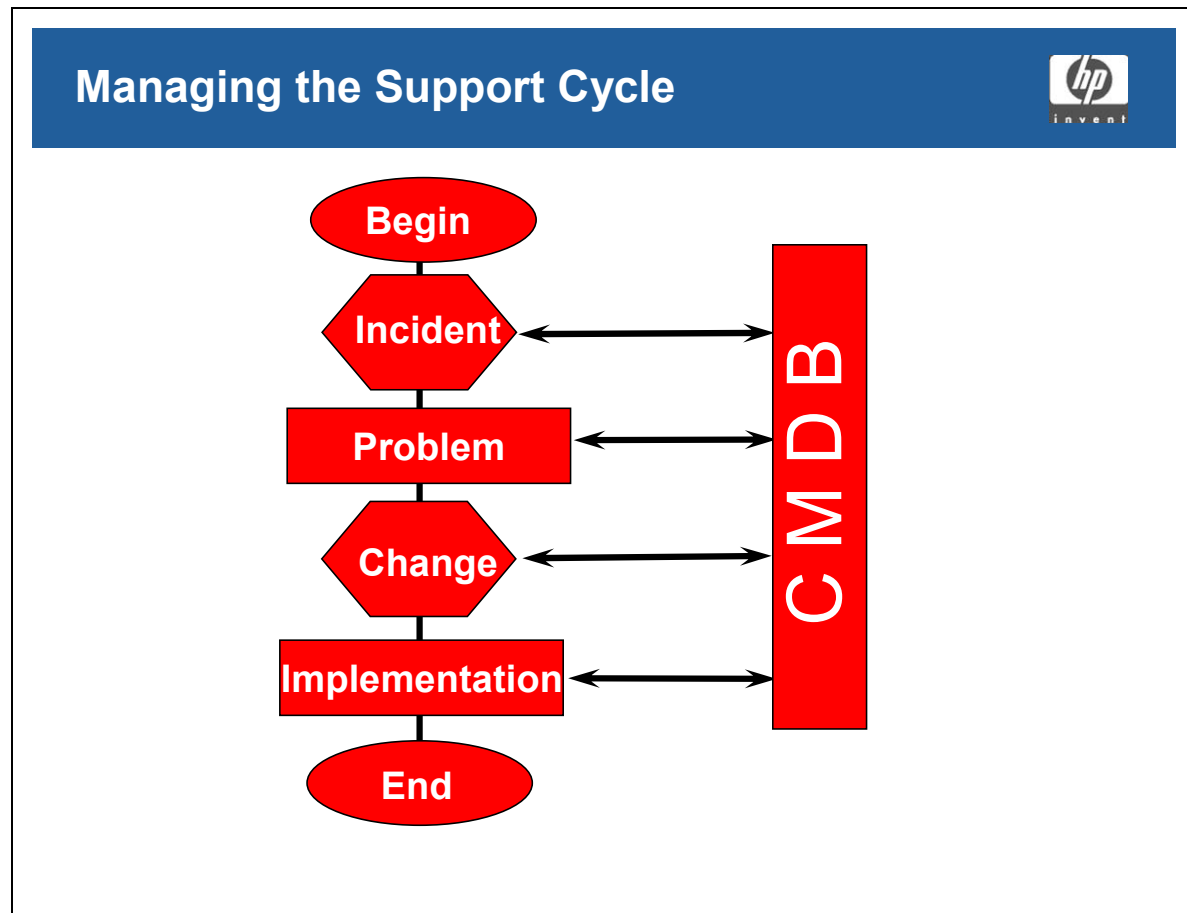
### Does the CMDB Reflect Reality?

Configuration Management should audit the CMDB to ensure that it accurately reflects the reality of the IT infrastructure. There is a natural tendency of recorded data to 'degrade' over time. This is sometimes called the 'morbidity' of data. A process of 'Verification and Audit' greatly assists in mitigating the effects of morbidity by checking and verifying database records against actuality, and vice versa. The physical existence of recorded items is verified, and the recording of a physical entity is also verified. The Configuration Management staff should do this, but other disciplines can help by making operational checks during their normal work.

### The accuracy of the CMDB will be easier to control if:

- The CMDB is active rather than passive
- The CMDB is updated automatically where possible
- Configuration Management activities are integrated into other procedures
- Automatic audits/checks are built into the system

## Managing the Support Cycle



### Student Notes

#### Managing the Support Cycle

Problems and changes are often linked. The diagram on the slide shows how an incident is diagnosed as a problem. To overcome the problem a change is proposed and implemented. Often the problem is not managed properly, or the change is not tested or assessed for impact. In these cases, when the change is implemented further incidents often result. In some cases these incidents are more serious than those that the change was supposed to correct. This is even more likely to occur if these actions are carried out in a hurry. A Configuration Management system can assist the organization to manage problems and changes efficiently and effectively, and thereby break this vicious circle.



### **At the Service Desk**

By answering a few simple questions the Service Desk staff will have access to the following information:

- Equipment held
- Software accessible
- Diagnostic aids
- Problem History
- Change History
- Service Level Agreement
- Training/experience record
- Personal information

If the CMDB is connected to other Service Management tools it will be constantly up to date and updated in real-time.

### **In Problem Management**

Configuration management will assist the Problem Manager by:

- Automatic escalation
- Problem logging
- Highlighting trends and Problem matching
- Listing known errors and outstanding problems
- Relationship identification
- Listing recent changes
- Outlining responsibilities
- Impact assessment
- Allowing the cost of a fix to be compared with the cost if not fixing the problem

### **In Change Management**

The CMDB can help in the following ways:

- The pre-change status is known
- Identification of affected CIs and owners
- Cross reference to incidents/problems and other changes
- Improves resource assessment - reference to past records
- Speeds up the change management process
- Risk assessment

## **Module 5**

### **Configuration Management**

#### **In Release Management**

The CMDB can help with:

- Recording location of software and hardware
- Code control
- Release building
- Identifying who needs new releases
- Implementation
- Software and hardware recovery
- Corruption or loss of data

## Configuration and Change Management

### Configuration and Change Management



- Change Management ensures CI control
- Changes to the CMDB initiated through Change Management
  - Introducing new CIs, deleting old CIs
  - Change to status, owner or location of CIs
  - Changed relationships between CIs
  - Exceptions
- CMDB is used to assess RFC impacts
- Change Management keeps CMDB up to date

## Student Notes

### The Relationship between Configuration and Change Management

There can be no control over the CIs in an organization if they are not subject to change control. At the same time, there can be no meaningful change control if there is no idea of what CIs are in an organization and what their functions are.

Configuration Management can be prompted to update the CMDB in a number of ways. Many of these are part of Change Management:

- When new CIs are added to the IT infrastructure.
- When the status of CIs change.
- When the owners of CIs change.
- When the location of CIs change.
- When relationships affecting CIs change.
- When old CIs are removed.
- When an unregistered CI is found or information regarding a CI is inaccurate.

## **Module 5**

### **Configuration Management**

- When a change is requested, Change Management should use the CMDB to assess that change's impact on the business and other CIs.

Changes are requested using a Request for Change (RFC), which is recorded in the CMDB. This enables the tracking of progress and tracing of problems in the IT infrastructure back to previous changes.

Change Management enables the CMDB to reflect the current status of specific CIs in the organization.

If changes fail, the CMDB could be used to indicate what state of the CI should be reverted to. If that is out of date, time will be wasted trying to remember what the CI looked like before work started.

## Question

### Components Recorded in the CMDB



The computer equipment and the system and applications software should be recorded in the CMDB.

Which other components should be recorded in the CMDB?

1. Data communications equipment
2. Documentation
3. Personnel

- |            |                |
|------------|----------------|
| A. 1 and 2 | B. 1 and 3     |
| C. 2 and 3 | D. 1, 2, and 3 |

## Student Notes

## Question

### Configuration Items



Which of the examples below is *not* an example of a configuration item?

- A. A PC comms card
- B. A user manual
- C. A company's organization chart
- D. A unique identification number

## Student Notes

---

## **Module 6 — Change Management**

## Mission of Change Management

### Mission of Change Management



To manage all changes that could impact on IT's ability to deliver services through a single, centralized process of approval, scheduling and control to ensure that the IT Infrastructure stays aligned to business requirements

### Student Notes

*To manage all changes that could impact on IT's ability to deliver services through a formal, centralized process of approval, scheduling and control to ensure that the IT Infrastructure stays aligned to business requirements with a minimum of risk*

To achieve this mission requires a careful and considered approach to assessing risk, the potential impact of change(s), the resource requirements, and the process for approving changes. This is essential to balance the need for a change against the impact it may have on the service and possibly on the business.

It should be noted from a reporting perspective, that a large number of changes measured over a period of week and longer does not necessarily indicate that there is any major problem (or problems). Rather it may reflect a volatile system, adapting to changes in the business. In this situation, it may be inadvisable to attempt to moderate the number of changes, as to do so might adversely impact the business.

Nevertheless, in general, overall quality of service will be improved if the number of changes is minimized, especially those relating to Incidents. An efficient Change Management function should effect a reduction in change-related incidents, and to be measured as effective must show such a reduction from before it was implemented.



## Scope of Change Management

### Scope of Change Management



Covers areas including:

- Hardware
- Environment and facilities
- Software
  - Live
  - Under development
- Documentation and procedures
- Organization and people

### Student Notes

Change Management must be a formal, centralized process. It is responsible for managing changes to:

- Hardware
- Environmental equipment and facilities
- Software
  - Live
  - Under development
- All documentation, plans and procedures relevant to the running, support and maintenance of live systems
- Organization and people

Change Management will usually exclude changes to CIs under the control of a development project.

## **Module 6**

### **Change Management**

**Configuration Management** is responsible for identifying affected CIs and for updating the CMDB with changes. **Release Management** is responsible for releasing changed CIs.

## Objectives of Change Management

### Objectives of Change Management



- Manage the process of:
  - Requesting changes
  - Assessing changes
  - Authorizing changes
  - Implementing changes
- Prevent unauthorized changes
- Minimize disruption
- Ensure proper research and relevant input
- Coordinate build, test and implementation

### Student Notes

The overriding objective of Change Management is to ensure proper control over the IT infrastructure. It achieves this by:

- Managing the process of:
  - Requesting changes
  - Assessing changes
  - Authorizing changes
  - Implementing changes
- Ensuring that no unauthorized changes are implemented
- Minimizing the risk and disruption caused by changes
- Ensuring that changes are properly researched and that all relevant parties have input into the assessment of changes
- Coordinating the effort involved in building, testing and implementing changes

## Scalability

### Scalability



The Change Management process must be scaleable for:

- Different types
- Large or Small
- High or low Cost
- Major or minor impact
- Changes in a required timeframe
- Urgent changes

### Student Notes

The size and dynamics of an organization should be considered when implementing Change Management. It is the most politically sensitive of all the ITIL processes and needs to be handled carefully if it is not to be seen as too bureaucratic. The process should be flexible and adaptable to ensure it can be scaled to suit each situation.

Considerations are:

- Different types of change
- Size of change
  - Large
  - Small
- The cost of the change whether it is high or low
- The impact of the change major or minor
- The timeframe the change must be delivered in
- A separate procedure for urgent changes

## Core Elements

### Core Elements



- Request for Change (RFC)
- Change Advisory Board (CAB)
- CAB Emergency Committee (CAB/EC)
- Forward Schedule of Changes (FSC)
- Projected Service Availability (PSA)
- Change Model
- Standard Change

## Student Notes

### Request for Change (RFC)

The RFC is the only mechanism in ITIL for requesting changes to the infrastructure. RFCs must contain all the information necessary for a change to be assessed, approved and built.

### Change Advisory Board (CAB)

The CAB is responsible for assessing the impact of requested changes and estimating the resource requirements. They will advise the Change Manager on whether changes should be approved and will assist in scheduling changes.

CAB membership will depend on the change being requested, but could consist of anyone who is potentially impacted by the change.

To prevent large, unmanageable meetings, the RFCs are managed electronically and attendance at the meetings is optional.

### **Change Advisory Board / Emergency Committee (CAB/EC)**

It may not always be possible for the CAB to meet for very urgent changes. The Change Manager will probably need to consult with some key managers before approving urgent changes.

The CAB/EC consists of one to three key staff. These can be predefined but may not necessarily be so as their selection will depend on the nature of the change. This may just require a telephone conference, and members must be prepared to be available after hours.

### **Forward Schedule of Changes (FSC) and Projected Service Availability (PSA)**

The FSC contains details of all approved changes and their implementation dates for an agreed period. The FSC is used so that all groups affected by a change can plan for its release.

The FSC could have detailed short-term schedules, with less detailed schedules for longer-term planning.

Change Management uses the Projected Service Availability (PSA) to determine the best time for a change to be implemented.

Both the FSC and the PSA are agreed with the customers, SLM the Service Desk and Availability Management. The Service Desk will communicate any planned downtime to the users/customers. A copy could be maintained on the Intranet.

### **Change Model**

This is a predefined way (or procedure) of dealing with changes of a known type or complexity. The aim of a change model is to facilitate the accurate and timely assessment of changes by the appropriate groups of people.

Change Models are discussed in more detail later in this module.

### **Standard Change**

This is one of the most common forms of Change Model, and refers to simpler or small-scale changes.

A standard change is a change that is well known, follows a predefined path and is the accepted response to a specified set of circumstances.

Standard changes are well-known and proven tasks that are pre-authorized and often initiated by the Service Desk. They also have a predefined budget limit usually within the approval of the requestor.

## CAB Membership

### CAB Membership



- Change Manager (Chair) — only permanent member
- Customer/user representatives
- Applications developers/maintainers
- IT Service Management representatives
- Other IT staff
- Office Services
- Suppliers

### Student Notes

CAB membership will depend on the change being requested, but could consist of anyone who is capable of ensuring that the change is assessed adequately from a business and technical viewpoint. This could include:

- Change Manager (Chair) — only permanent member of CAB
- Customers or User managers and user group representatives
- Applications developers/maintainers
- Representatives from all other ITSM processes
- Other IT staff, including technical staff and consultants
- Office services staff
- Contractors or 3rd party representatives

## **Module 6**

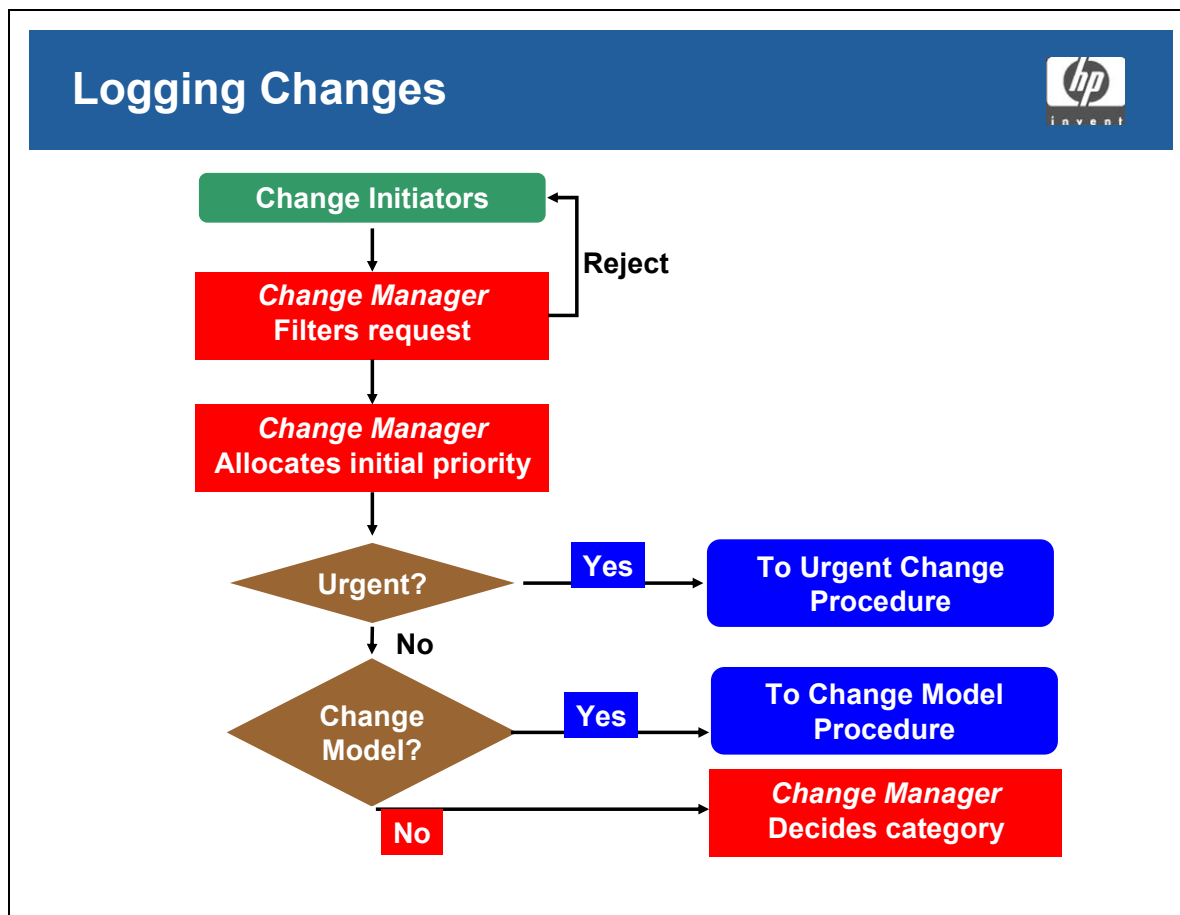
### **Change Management**

To prevent large, unmanageable meetings, the RFCs are distributed to all members for comments, and attendance at the meetings is optional. Support tools or e-mails should handle most changes, and only more complex, high-risk or high-impact changes will require a physical meeting.

CAB meetings should be scheduled at least once every 6 months and when major projects are due to deliver products. The meeting will then be used to sign-off approved changes, review outstanding changes and to assess future changes.



## Logging Changes — Normal



### Student Notes

#### Change Initiation

Technical staff should be allowed to log changes directly, while user change requests should be filtered by a line manager or user liaison structure.

This is to prevent duplication and impractical changes, while also ensuring a broader base of support for the change.

#### Initial Logging and Filtering

All requests for change should be logged using an RFC form. Each RFC should be given a unique number and, if the change is being made to resolve a problem, the incident number should be reflected.

The Change Manager should briefly filter requests and reject any that are obviously impractical, undesirable or repetitive

An appeal process should be available where the initiator is unable to accept the Change Manager's verdict.

### **Initial Priority**

The Change Manager then allocates an initial priority to indicate the urgency of the required change. This can be done in consultation with the initiator.

If the change is urgent, it will be dealt with through the urgent change management procedures.

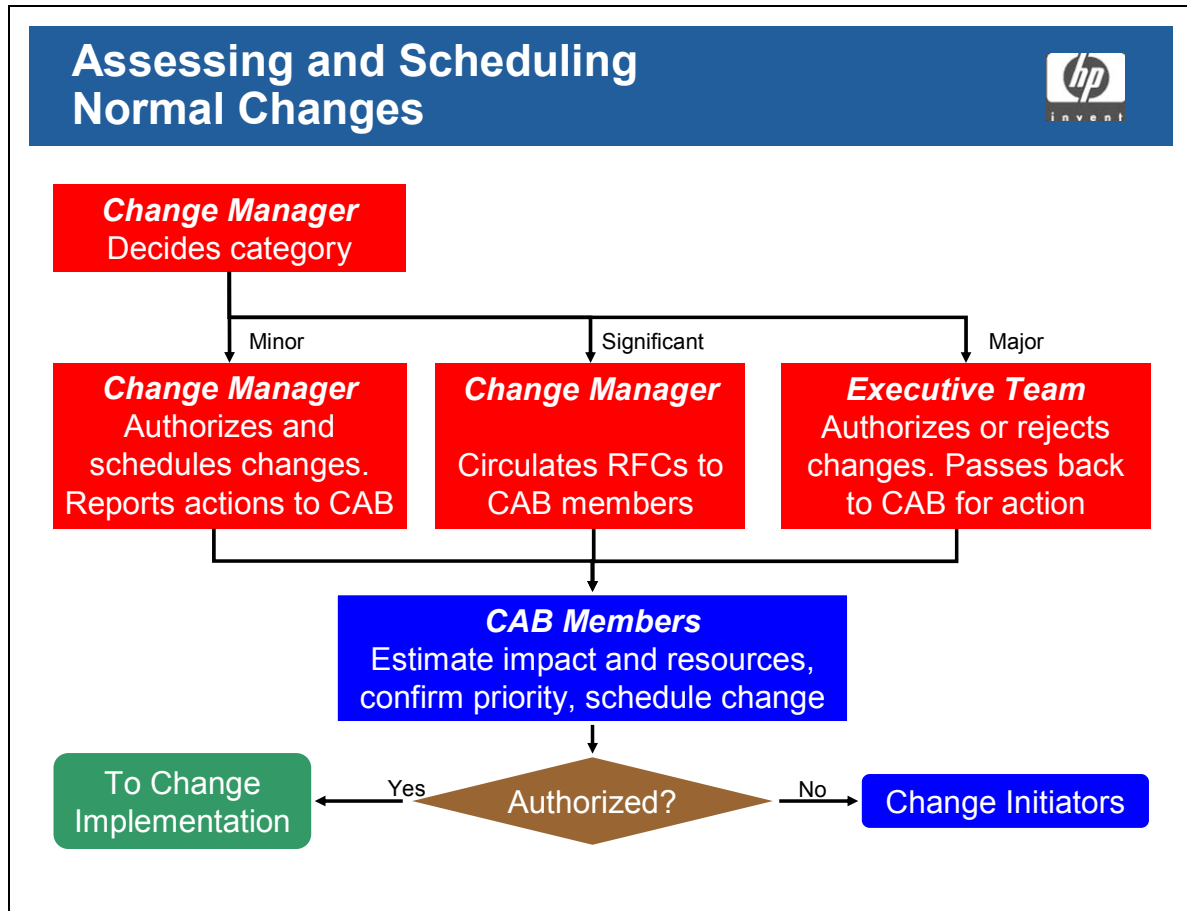
If the change is not urgent the next step is to check whether there is a Change Model for this type of Change. If there is the Change Manager will follow the steps for initiating that procedure, if not it will continue on to the categorization step in the normal procedure.

### **Change Categorization**

The change is then categorized in two ways:

- To indicate the type of change. This is used for reporting and tracking, and is not discussed in this course.
- To indicate how to deal with the change. This category is determined by:
  - The impact of the change
  - The cost of the change
  - The number of people needed to build the change
  - The time it will take to build

## Assessing and Scheduling Normal Changes



### Student Notes

#### Assessing and Scheduling Normal Changes

ITIL identifies 3 basic categories:

- **Category 1:** Minor impact and few additional resources required
- **Category 2:** Moderate impact or moderate resources required
- **Category 3:** Major impact or major resources required

## **Change Assessment and Approval**

### **Category 1 — Minor**

The Change Manager has delegated authority to approve and schedule changes although these should be reported to the CAB. If there are any doubts about authorizing the change, it can be referred to the CAB or CAB/EC.

### **Category 2 — Significant**

The RFC must be discussed at the next CAB meeting. RFCs are circulated to CAB members before the meeting, and to an even wider audience if necessary, for impact and resource assessment.

### **Category 3 — Major**

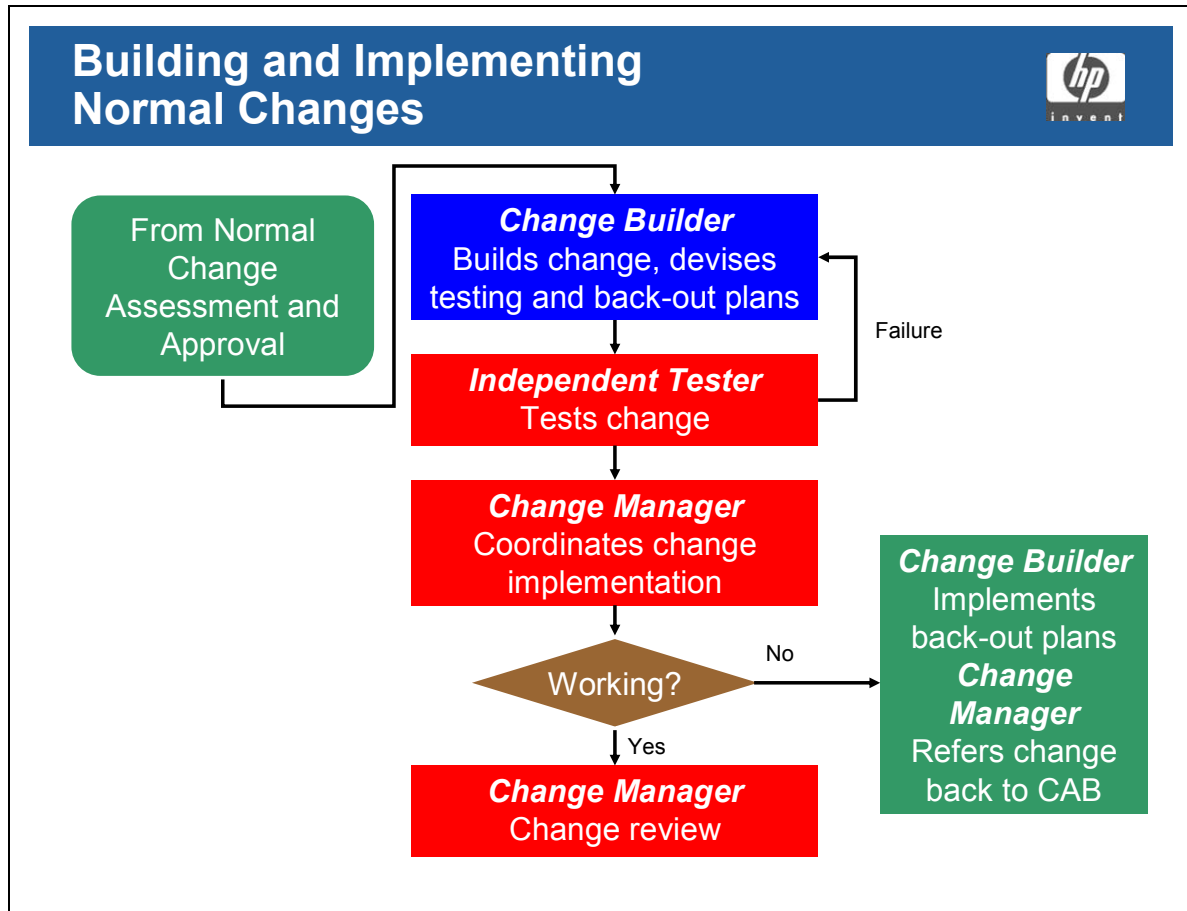
The CIO or senior IT manager must refer the request upwards. Approved changes must be passed back to the CAB for scheduling and implementation.

## **Change Scheduling**

Some changes are simple and can be implemented one at a time, but many are complex and involve several changes under the same RFC.

These changes should be combined into releases and implemented through Release Management, according to the FSC.

## Building and Implementing Normal Changes



### Student Notes

#### Change Building

Once the change is authorized, the appropriate technical person or team will:

- Prepare and build the change
- Devise testing plans
- Produce a back-out plan to enable the implementation team to revert to a known, trusted state if there are any problems

Change Management will coordinate the build, supported by Release Management and the appropriate line managers.

### **Change Testing**

An independent testing authority should test the change and the back out plans. Progress will only be allowed once the test has been completed successfully. The following aspects should also be tested:

- Performance
- Security
- Maintainability
- Supportability
- Reliability and availability
- Functionality

Progress will only be allowed once the test has been completed successfully.

### **Implementation**

The Change Manager will co-ordinate the implementation of the change. All relevant staff should be advised in advance of the planned implementation (perhaps through the Service Desk). If things go wrong the back-out plans must be implemented and the change will normally be removed.

### **Change Review**

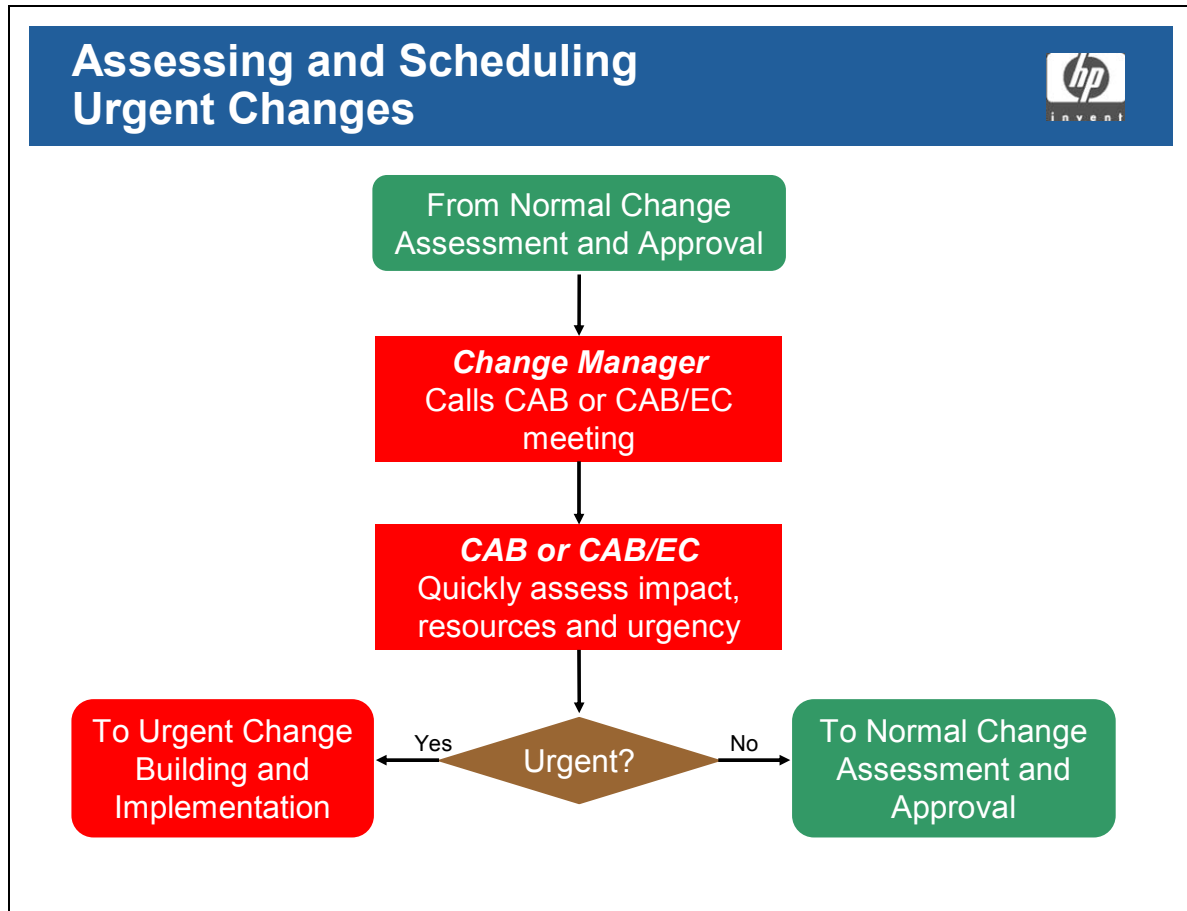
All changes should be reviewed after a pre-defined period to ensure that the desired effect has been achieved and to assess whether resource estimates have been accurate. This process should also improve future estimating.

### **Documentation**

The Change Manager should ensure that all documentation has been brought up to date. This will include:

- The RFC
- User and technical manuals
- Process documentation
- The information in the CMDB (through Configuration Management)

## Assessing and Scheduling Urgent Changes



### Student Notes

#### When are Urgent Changes Allowed?

Urgent changes should be kept to a minimum because they are more disruptive and error prone. Where urgent changes are necessary, the following principles apply:

- Normal management controls should still be applied
- Incident Management staff and technical support staff should be delegated authority to implement certain types of change as workarounds or problem resolutions
- Circumventions to fix incidents should be limited to actions that do not change the specification of the CI and do not attempt to fix software errors
- Changes must be reviewed as normal

### **Urgent Change Assessment and Approval**

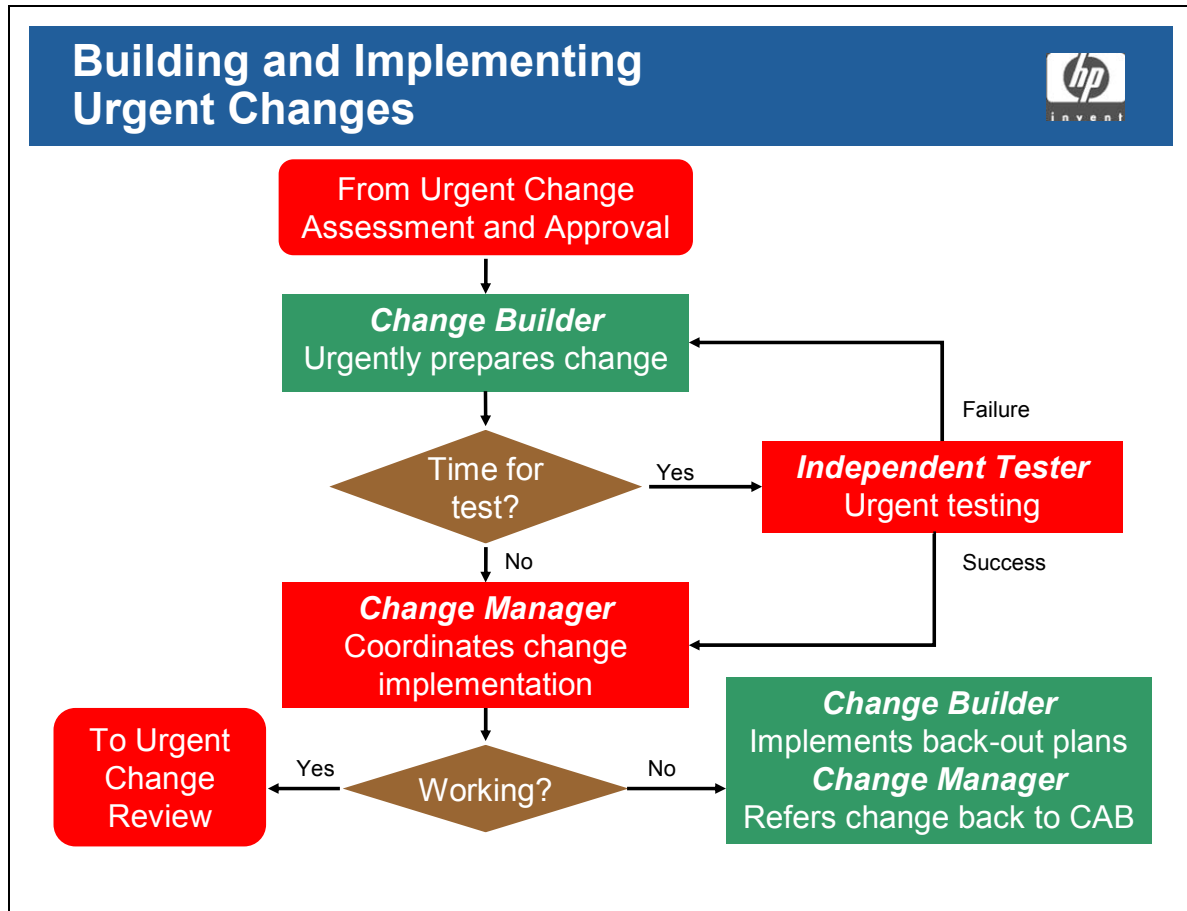
The Change Manager will call the appropriate CAB/EC who will quickly assess the change for impact and urgency. They should have the appropriate experience and skill necessary for determining the risk and impact of the change and whether it is truly urgent. If not it should be rejected with the recommendation it be submitted via the Normal Change Procedure.

### **Urgent Change Scheduling**

It is essential the CAB/EC have access to information on current changes taking place and the FSC if they are to make a sound judgment as to when and whether the Urgent change can be implemented. Many of these could be severely impacted as a result of implementing the Urgent change or need to be rescheduled at a later date.



## Building and Implementing Urgent Changes



### Student Notes

#### Urgent Change Building

Procedures and OLAs should be in place to specify how technical staff are allocated and called out to build urgent changes. The cost of emergency call-outs should be pre-approved in the IT budget. Back-out and testing plans should still be devised.

#### Urgent Change Testing

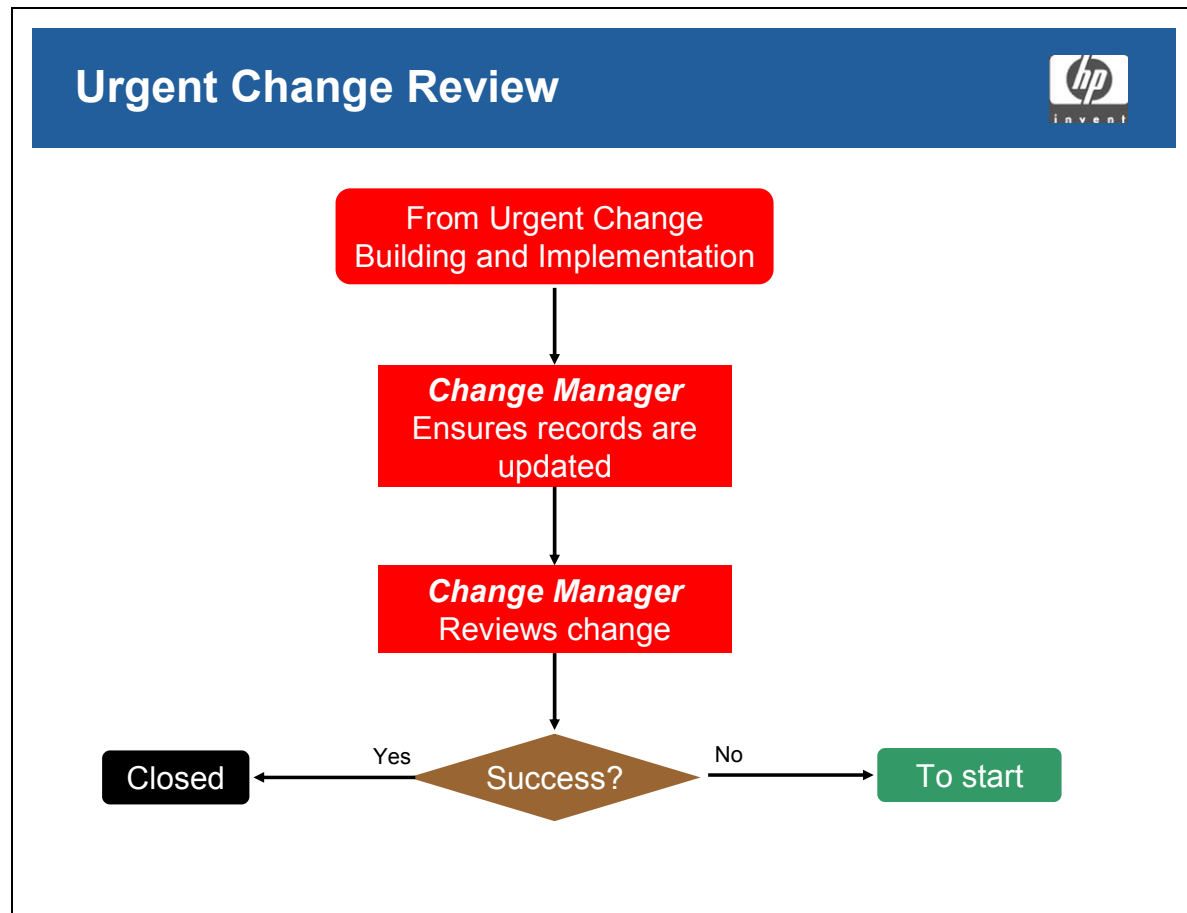
Testing should be carried out as far as possible. Untested changes should not be implemented if at all possible. The cost of reworking a change that failed is usually greater than the cost of testing the change in the first place.

#### Urgent Change Implementation

As much advance warning as possible should be given before the actual implementation of the change. The Service Desk can do this.

Even more so than during a normal implementation, technical support staff should be present during an urgent change implementation.

## Urgent Change Review



## Student Notes

### Urgent Change Review

Unlike Normal changes, all Urgent changes should be reviewed immediately after implementation to ensure they were successful and that there have been no undesirable side-effects to functionality, availability, capacity, performance, security, maintainability etc. This process should also improve future Urgent change assessment, scheduling, building, testing and implementing – see the section titled “What Happens if an Urgent Change Fails?” below.

### Documentation of Urgent Changes

Although formal documentation will probably not be completed while the change is being made, manual records should be kept and the permanent records updated as soon as possible after the change.

This will be checked at the change review

### **What Happens if an Urgent Change Fails?**

An urgent change may need several iterations before it succeeds. If this is the case, the following principles apply:

- Change Management needs to ensure that business needs remain the primary concern
- Each iteration needs to be controlled and logged
- Abortive changes should be properly backed out and assessed
- If the situation goes on for too long, Change Management should consider making a partial service available

## Change Models

### Change Models



- A Change Model is a template applied to regular changes ensuring that they are managed, to a proven, predefined process.
- Pre-defined models must be agreed, defining the:
  - actions needed to implement the change
  - responsibilities
  - authorization
  - timescales
- The Change Model will define the categorization, based upon type, impact, risk, resources, and so on

### Student Notes

A Change Model basically a template for a change that follows a pre-defined path that has been defined by Change Management and agreed with the organization. A model may be specific to type, to severity or impact, or any other variable that is relevant to an organization.

A pre-defined change model can be used to represent complex changes so that various groups can identify:

- The potential impact of the change
- Actions needed to implement the change
- Authorization
- Timescales

This will also enable them to define the categorization based on these criteria.

Service Delivery disciplines could assist in defining these models to ensure that all aspects of the change are properly assessed and scheduled.

## Change Models

### Change Models

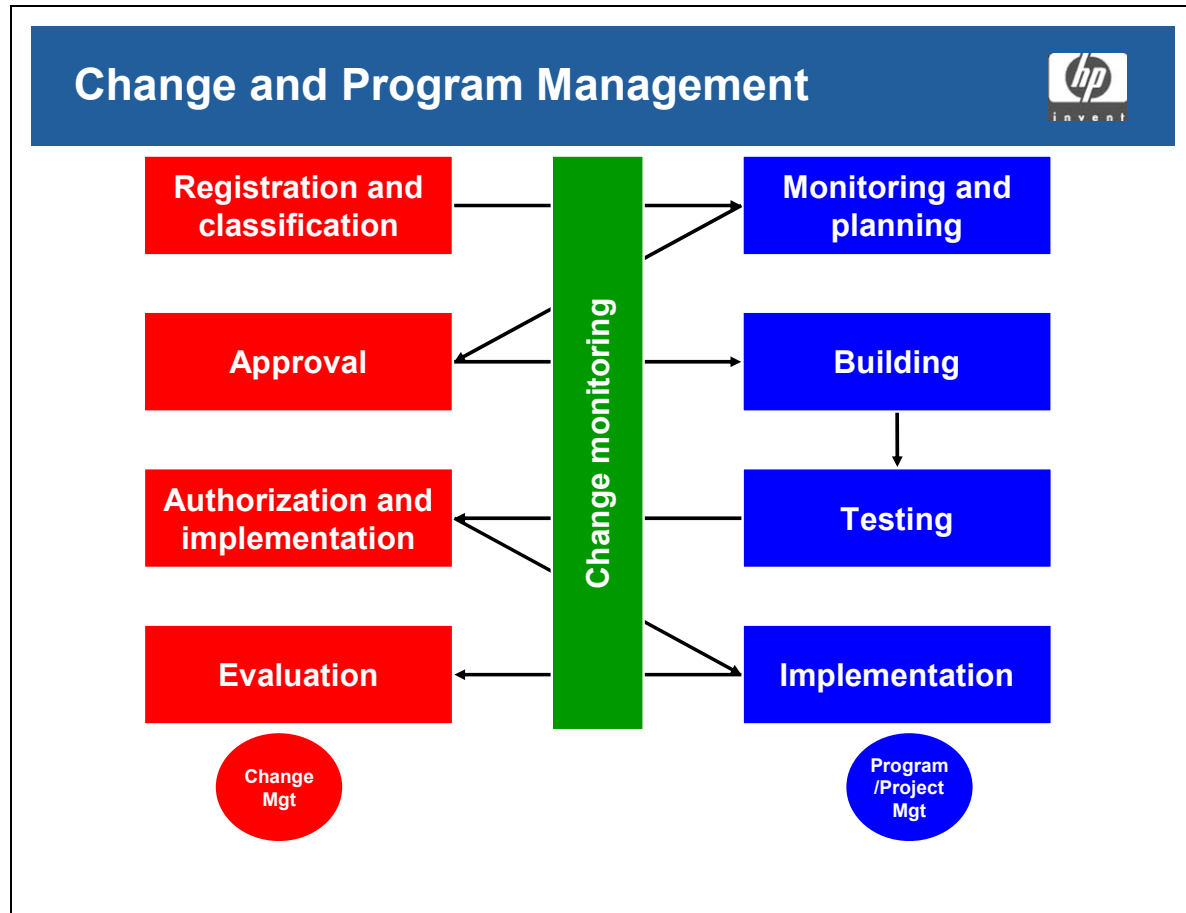


- Models should be predefined and automated so far as possible
- It should be possible to easily create a new model, or variation of an existing model
- Ability to use and easily amend models should be a significant criteria in tool selection

### Student Notes

- Models should be predefined and automated so far as possible
- It should be possible to easily create a new model, or variation of an existing model
- Ability to use and easily amend models should be a significant criteria in tool selection

## Change and Program Management



### Student Notes

Since many changes and new services are complex, Change Management should also be integrated with processes used to control projects and programs within the operational environment.

For example, there will be times when a proposed infrastructure Change will potentially have a wider impact upon other parts of the organization (e.g. applications development projects, or business operations), or vice versa. Such changes will come under ***Program/Project Change Management*** procedures but the regular Change Management team will be expected to liaise closely with them to mitigate possible negative impacts from either direction.

Consequently, it is imperative that the infrastructure and other Change Management systems are appropriately interfaced.

## Question

### Controlling Changes to IT Infrastructure



Which consecutive steps have to be taken to carry out controlled changes to the IT infrastructure?

- A. Logging and filtering -> prioritization -> categorization -> assessment -> approval -> scheduling -> building and testing -> implementation -> review -> closure
- B. Acceptance -> categorization -> determination of impact and urgency -> logging -> testing -> closure
- C. Identification -> registration -> allocation -> investigation -> testing -> implementation -> reporting -> closure
- D. Registration -> diagnosis -> detection -> classification -> acceptance -> implementation -> closure

## Student Notes

## Question

### Accessing the Impact of Change



Which of the following should be consulted when assessing the impact of a change to the network configuration?

1. The Release Manager
2. The Change Advisory Board
3. The CMDB
4. The Executive board

A. 1 and 4

B. 2 and 3

C. 2 and 4

D. 1, 3, and 4

## Student Notes



---

## **Module 7 — Release Management**

## Mission of Release Management

### Mission of Release Management



To manage the effective use of new and changed services throughout the organization by planning, designing, building, testing and releasing the hardware and software components to ensure the deployment of compatible, licensed and appropriate releases and to minimize the use of releases that do not contribute to organizational objectives

### Student Notes

*To manage the effective use of new and changed services throughout the organization by planning, designing, building, testing and releasing the hardware and software components to the live environment to ensure the deployment of compatible, licensed and appropriate releases and to minimize the use of releases that do not contribute to business objectives*

Many service providers and suppliers are naturally involved in the release of software and hardware items into an environment. Effective planning and management are essential both to package and distribute successfully such releases to the customer.

Release Management takes a holistic view of a change to an IT service and should ensure that all aspects of a release (technical and non-technical) are considered together.

Release Management is responsible for the protection and integrity of the live environment. It uses Change Management and Configuration Management to achieve this.

Release Management stands between the development and the live environments. It ensures that the standards for delivering a service are maintained consistently between the two environments.

Major activities include:

- Release policy and planning
- Release design, build and configuration
- Release acceptance
- rollout planning
- extensive testing to predefined acceptance criteria
- sign-off of the Release for implementation
- communication, preparation and training
- audits of hardware and software prior to and following the implementation of Changes
- installation of new or upgraded hardware
- storage of controlled software in both centralized and distributed systems
- Release, distribution and the installation of software.

## Scope of Release Management

Scope of Release Management	
<b>Software</b> <ul style="list-style-type: none"><li>• In-house applications</li><li>• Packaged software</li><li>• Bespoke software</li><li>• Compilers, interpreters, assemblers</li><li>• Operating systems</li><li>• Utility Software</li></ul>	<b>Hardware</b> <b>Licenses</b> <b>Documentation</b> <ul style="list-style-type: none"><li>• Technical specifications</li><li>• User manuals</li><li>• Procedures</li></ul>

### Student Notes

Release Management includes:

- Software:
  - In-house developed applications
  - Packaged software
  - Bespoke software (custom built)
  - Externally developed software
  - Compilers, interpreters, assemblers
  - Operating systems
  - Utility software
- Hardware and hardware specifications
- Licenses

- Documentation:
  - Technical specifications
  - User manuals
  - Procedures

## Objectives of Release Management

### Objectives of Release Management



- Rollout of software and related hardware
- Communicate changes in CIs to Configuration Management
- Distribution and installation of changes
- Ensuring only correctly released, tested and authorized Configuration Items are used
- Agreeing release content and plans
- Physical storage of master software

### Student Notes

- To plan and manage the rollout of software and related hardware
- Communicate changes in CIs to Configuration Management
- To design and implement procedures for the distribution and installation of changes to IT systems
- Ensuring only correctly released, tested and authorized versions of CIs are in use
- To agree the exact content and plan for each release
- To ensure the physical storage and protection of master copies of all software

## Definition of a Release

### Definition of a Release



- A collection of authorized Changes to an IT service
- A Release is defined by the RFCs that it implements

### Student Notes

The term 'Release' is used to describe a collection of authorized Changes to an IT service. A Release is defined by the RFCs that it implements. The Release will typically consist of a number of Problem fixes and enhancements to the service. A Release consists of the new or changed software required and any new or changed hardware needed to implement the approved Changes.

## Licensing Issues

### Licensing Issues



- Ensure that all licenses are in order
- Ensure that no illegal software is in use
- Ensure that software being paid for is in use, and no unnecessary costs are incurred
- Policy statements must be made
- Enforcement Agencies

### Student Notes

*See also License Management in the Configuration Module*

While Configuration Management is responsible for License Management, Release Management is responsible for ensuring that during a release:

- All licenses are in order
- No illegal software is in use
- That software being paid for is in use, and no unnecessary costs are incurred
- Policy statements are be made
- Enforcement agencies are in place e.g. FAST (Federation Against Software Theft) in the UK, BSA (Business Software Alliance) in USA



## Anti-Virus Controls

### Anti-Virus Controls



Release Manager has responsibility for ensuring that an Organization's Anti-Virus measures are kept up to date, in conjunction with organizational security policies

### Student Notes

A Release Manager has responsibility for ensuring that and organization's Anti-Virus measures are kept to date, in conjunction with organization security policies.

## Definitive Software Library (DSL)

### Definitive Software Library (DSL)



- The library in which the original, definitive authorized versions of all software CIs and source code are stored and protected.
- Physical, secure library or storage repository where master copies of software versions are placed.
- Logical versus physical software libraries
- The DSL may also include a physical store to hold master copies of bought-in software, such as a fireproof safe.
- Several locations

## Student Notes

### Definitive Software Library (DSL)

The Definitive Software Library (DSL) is the term used for a library in which the definitive authorized versions of all software CIs are stored and protected.

It is a physical library or storage repository where master copies of software version are placed. This one logical storage area may in reality consist of one or more physical software libraries or filestores.

The DSL may also include a physical store to hold master copies of bought-in software, e.g. a fireproof safe. Only authorized software should be accepted into the DSL, strictly controlled by Change and Release Management.

## Definitive Software Library (DSL)

### Definitive Software Library (DSL)



#### Quality Assurance

- Change Management authorization
- No malicious additions
- Development quality review
- No additional changes
- CMDB updated

## Student Notes

### Quality Assurance

Before software is added to the DSL it has to go through Quality Assurance to check that:

- All items have been authorized through Change Management
- There are no malicious additions
- All software has passed a quality review in development
- There are no additional changes
- All items have been updated in the CMDB

---

## Definitive Hardware Store (DHS)

### Definitive Hardware Store



- The Definitive Hardware Store (DHS) is a secure area holding spare definitive hardware CIs.
- These are maintained at the same level as the comparative systems within the live environment.
- Details of these components should be recorded in the CMDB.
- These can then be used in a controlled manner when needed in live or test environments.
- Such items should be returned or replaced.

### Student Notes

This is an area set aside for the storage of all definitive hardware spares. These are spare components and assemblies that are maintained at the same level as the comparative systems in the live environment, and can be used for additional systems or for recovery from major incidents.

Details of these components and their respective should be recorded in the CMDB so they can then be used in a controlled manner when needed in live or test environments.

If they were used as temporary fixes, they can be returned to the DHS when they are no longer needed or when replacements have been obtained.

## Release Policies

### Release Policies



- Release Units
- Release types
  - Full release
  - $\Delta$  (Delta) release
  - Package release
  - Urgent
- Release identification

## Student Notes

### Release Policies

Release Management is responsible for defining the frequency, content, type and method of release. The release policy also defines the roles and responsibilities for Release Management as well as:

- The numbering of Releases
- The frequency of Releases
- The level in the IT infrastructure that will be controlled by definable Releases

The Release Policy identifies **Release Units**, or the level of software to be released. The lower the release unit, the smaller and more frequent the release.

## **Release Types**

The Release Policy also identifies what type of software release will be made. There are four main types of release:

- **Full** — all components of the Release Unit are built, tested, distributed and implemented together which reduces the temptation to short-cut the testing of 'unchanged' CIs.

Any problems are therefore more likely to be detected and rectified before the build is released into the live environment. The amount of time, effort and computing resources needed to build, test, distribute and implement the release will increase, and this can be seen as a major disadvantage.

As part of implementing a Full Release, the associated regression testing allows a large number of infrastructure components to be retested to minimize degradation in system function, behavior or performance.

- **Delta** — a partial release, usually to fix a problem or release some functionality earlier than scheduled. A release of only the CIs that have changed.

Where a Full Release cannot be justified, a Delta Release may be appropriate. The Change Advisory Board (CAB) should make a recommendation in each case, taking into account factors such as: the completeness of impact analysis information available to make an *informed and objective* decision; the size of the proposed Delta Release against that of a Full Release; the urgency of the Change occasioning the Release; the risk to the business if compatibility errors are found in the Release; the number of CIs (below the Release unit level) that have changed since the last full Release; and the resources available for building, testing, distributing and implementing the Delta Release.

- **Package** — including at least two Releases (eg. Delta, Full). A Package Release is intended to offer longer period of stability by reducing the frequency of Releases.

Where appropriate and where larger amount of Change can be confidently handled without problems, individual Releases (Full Releases, Delta Releases or both) are grouped together to form Package Releases. For example, changes to one system often require changes to be made to another(s); if these have to be made at the same time they should be included in the same Package Release.

The use of Package Releases can reduce the likelihood of old or incompatible software being inappropriately continued in use. It can encourage organizations to ensure concurrency of all Changes that should be made concurrently.

- **Urgent** — not recommended in ITIL

This is a release that is required to correct a small number of Known Problems

## **Release Identification**

Each release will be identified by a release number, which is assigned in the Release Management process.

## Release Scales

### Release Scales



- Major Releases
  - normally containing large areas of new functionality
- Minor Releases
  - normally containing small enhancements and fixes
- Emergency fixes or patches
  - normally containing the corrections to a small number of known Problems

## Student Notes

### Release Scales

A release is a collection of authorized changes to an IT service. Releases could contain several problem fixes and enhancements that have been defined in Requests for Change (RFC). Releases consist of any new or changed software or hardware.

Releases are often divided into:

- Major software releases and hardware upgrades
  - Normally containing a lot of new functionality, some of which will replace temporary problem fixes
- Minor software releases and hardware upgrades
  - Normally containing small enhancements or fixes, some of which have already been issued as fixes and emergency fixes
- Emergency fixes or patches
  - Normally containing corrections to a small number of known problems

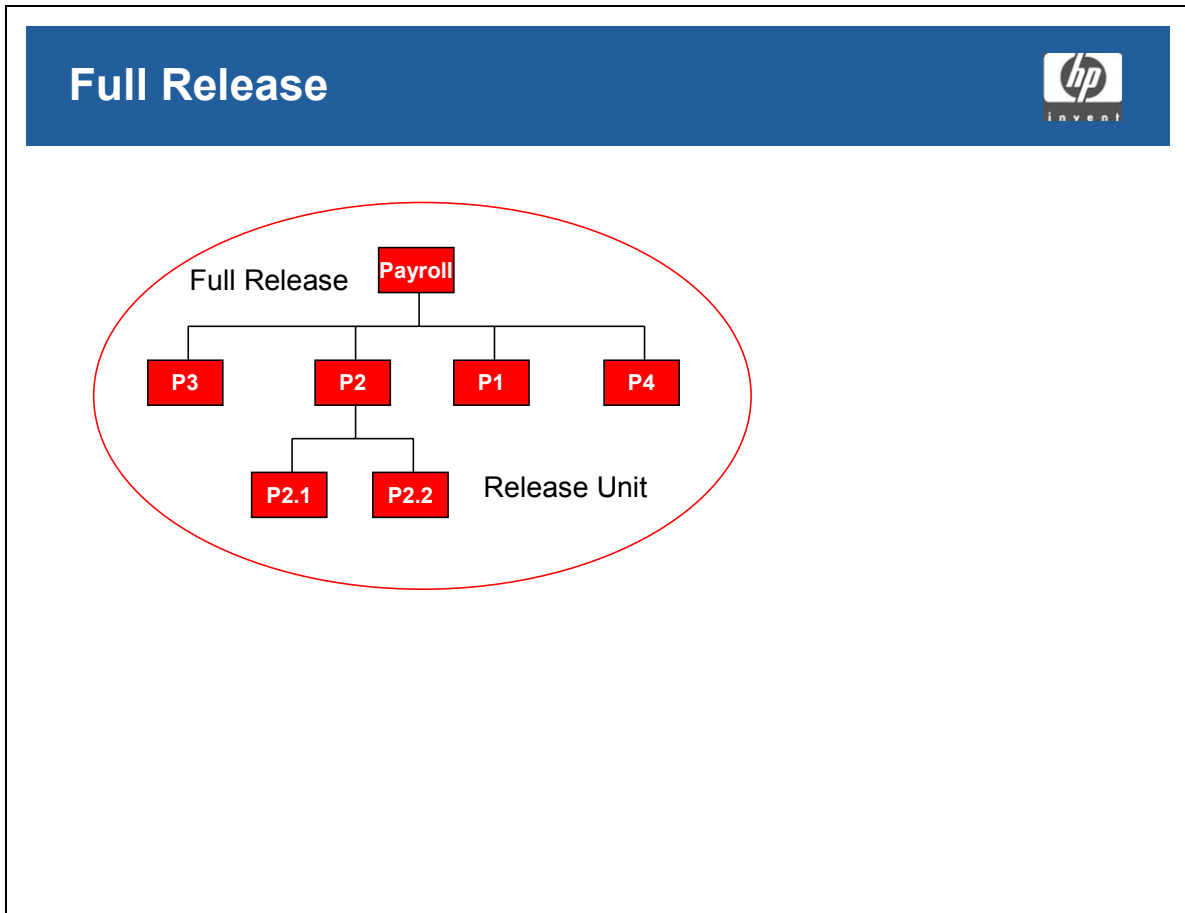
## **Module 7**

### **Release Management**

Since there are often dependencies between a software release and the hardware that supports it, a release could consist of hardware and software together.

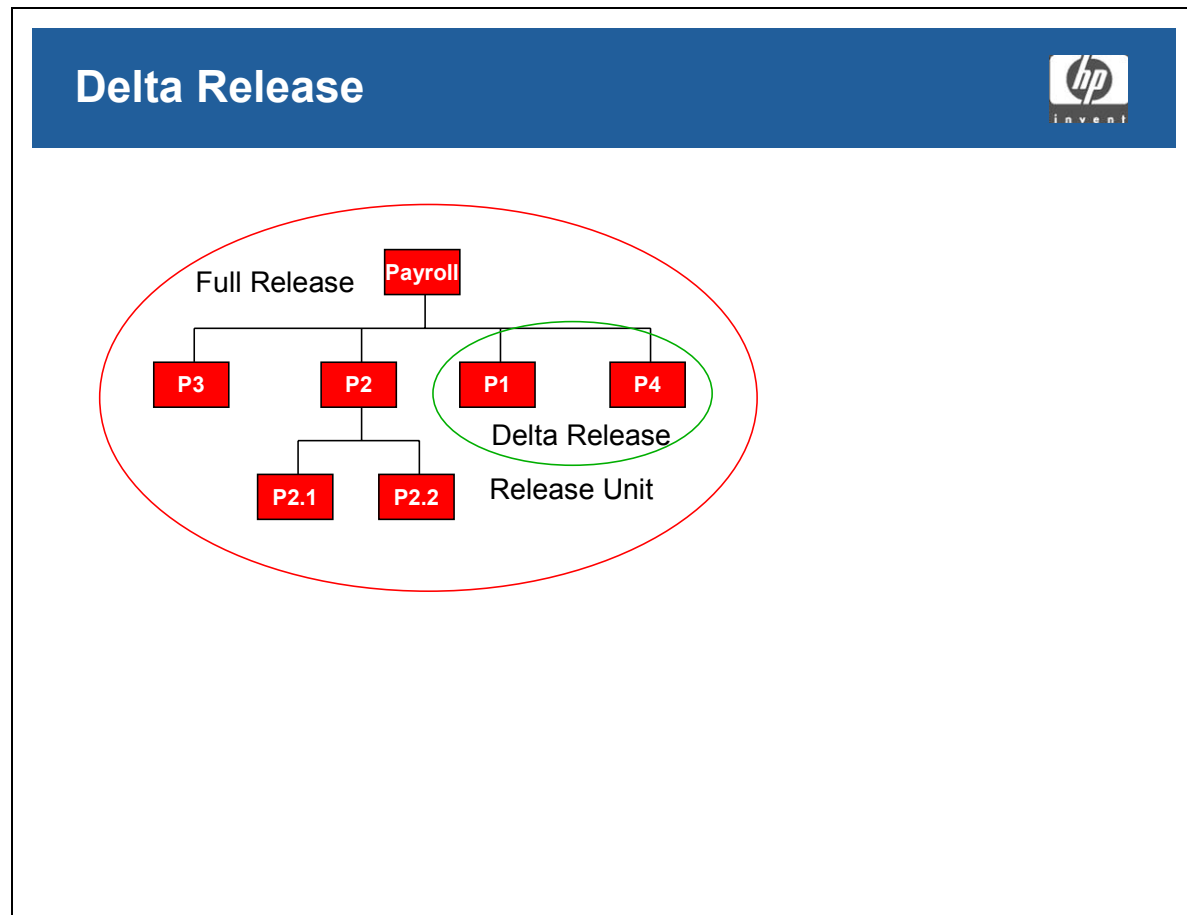


## Full Release



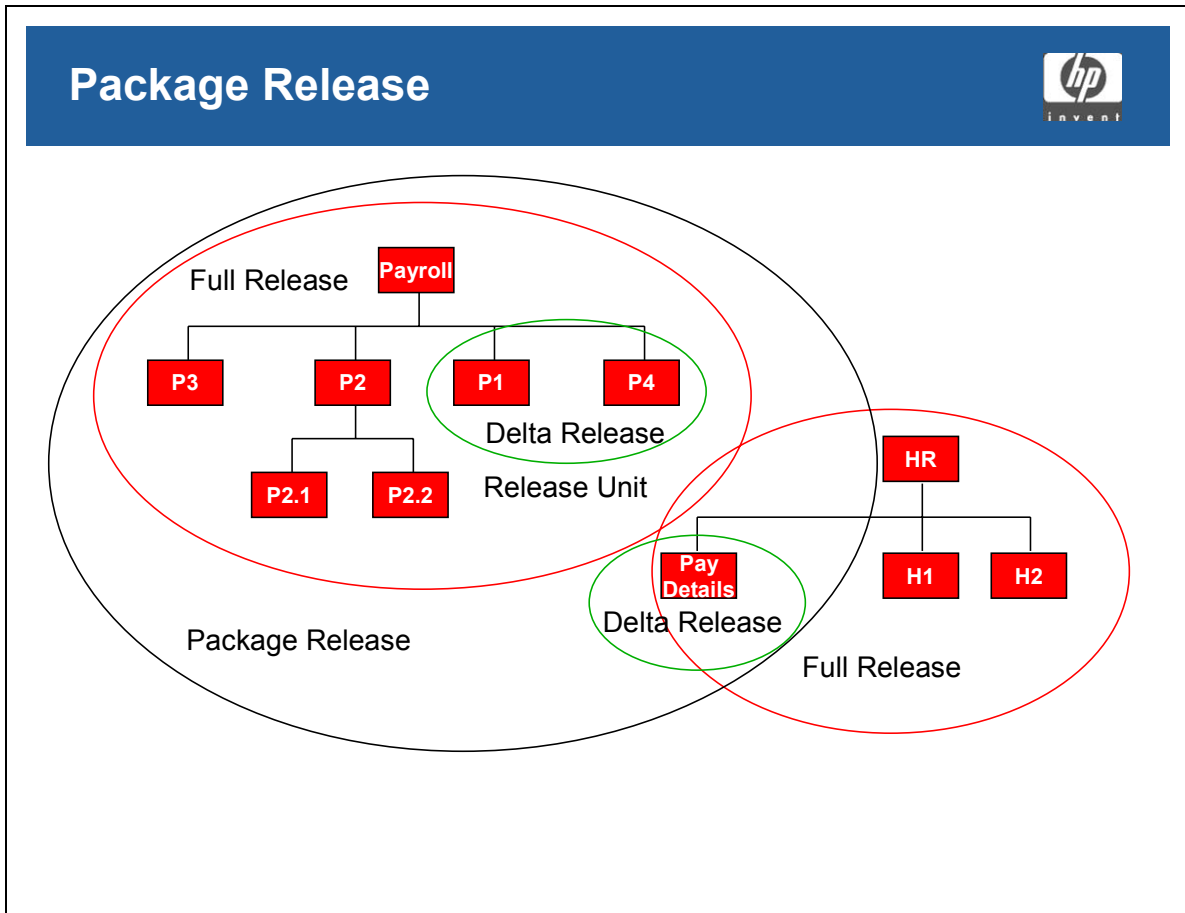
## Student Notes

## Delta Release



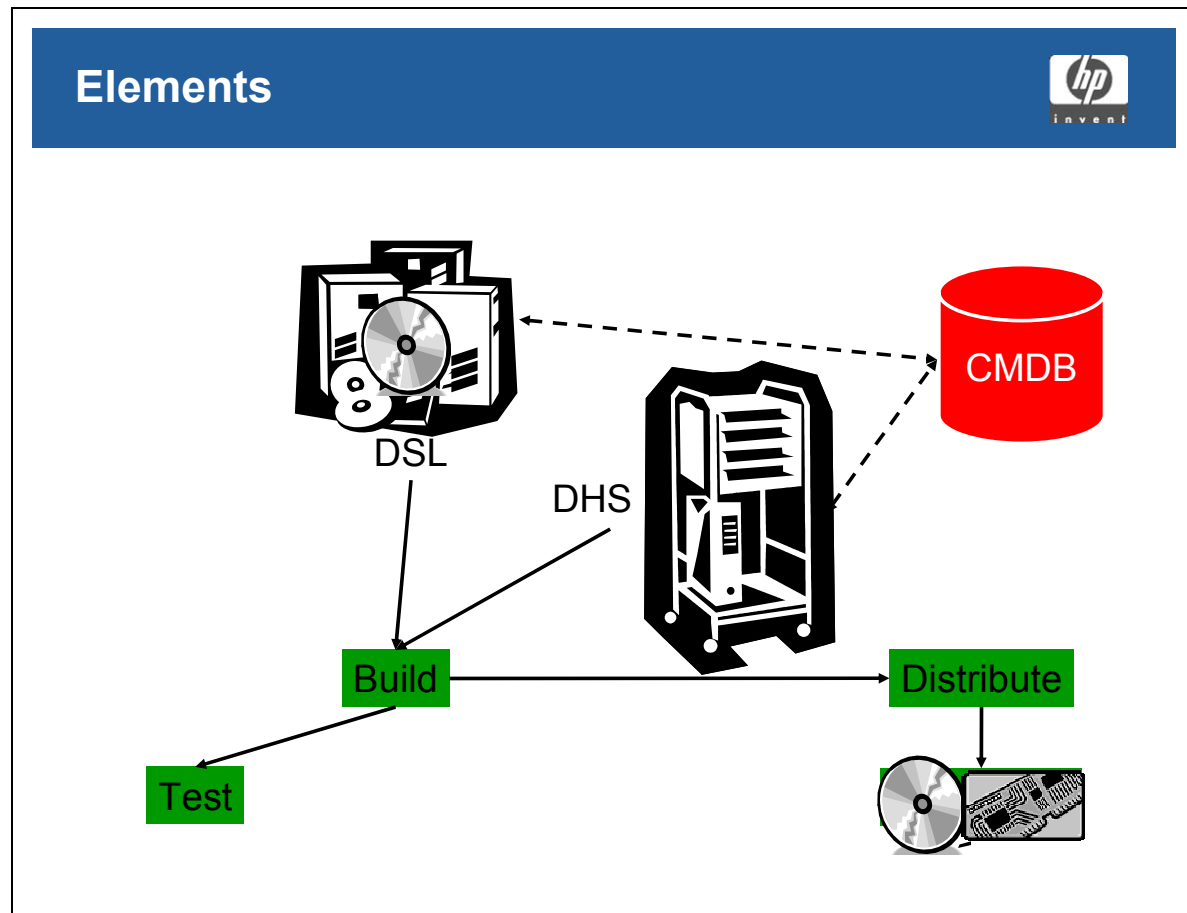
## Student Notes

## Package Release



## Student Notes

## Elements



## Student Notes

## Release Records

### Release Records



- Release Records are held in the CMDB
- Release Records contain
  - Details of constituent CIs
  - Links to RFCs
  - Target destinations
  - Schedule of implementation
  - Back-out plans
  - Dependencies
  - Responsibilities
- CMDB will maintain records of the CIs impacted by planned and past Releases

### Student Notes

Release records are held in the CMDB. They contain:

- Details of constituent CIs
- Links to RFCs
- Target destinations
- Schedule of implementation
- Back-out plans
- Dependencies
- Responsibilities

The CMDB will main records of the CIs impacted by planned and past Releases.

## Release Management Activities

### Release Management Activities



#### Release Planning

- Developing a plan for each release
- Agree and schedule with Change Manager

#### Designing, Building and Configuring Releases

- Process for assembling CIs for release
- CIs are under Configuration Management control

#### Testing and Release Acceptance

- Installation procedures
- System functionality

## Student Notes

### Release Planning

This activity is aimed at developing a plan for each release that is made into the operational environment. Planning a release involves agreeing the content of the release with Change Management and producing a schedule.

### Designing, Building and Configuring a Release

The hardware and software components of a release should be assembled in a controlled, reproducible process.

All software, hardware, parameters, test data, etc. required for the release should be under Configuration Management control. A complete record of the build will be kept in the CMDB.

### **Testing and Release Acceptance**

Testing and user acceptance is performed on the installation procedures and final system functionality before hardware or software is deployed in the live environment. This should include:

- Functional testing
- Operational testing
- Performance testing
- Integration testing
- Testing of the back-out plan

## Release Management Activities

### Release Management Activities



#### Rollout Planning

- Builds onto the release plan
- Exact implementation actions

#### Communication, Preparation, and Training

- When and how releases will be rolled out
- How they will be affected
- Progress of changes

#### Distribution and installation

- Moving the release to the target environment
- Deploying the release

## Student Notes

### Rollout Planning

Rollout planning builds onto the Release Plan with information about the exact installation process that will be used during deployment of the release.

### Communication, Preparation and Training

Customer liaison and support staff, as well as customers need to know what releases are due, what mechanism will be used, and how they are going to be affected. They should also be informed about the progress of changes to fix incidents and problems.

### Distribution and Installation

The rollout of releases consists of a distribution phase where the release is moved to the target locations and an installation phase where the release is actually deployed.



## Question

### Definitive Software Library



Which of the following best describes the Definitive Software Library?

- A. A secure work area where changes to software can be made
- B. A library containing back-up copies of all software used in the organization
- C. A secure library where all accepted software versions are kept in their quality controlled form
- D. A secure library in which all the latest software versions are stored

## Student Notes

## Question

### Benefits of a Release Management Process



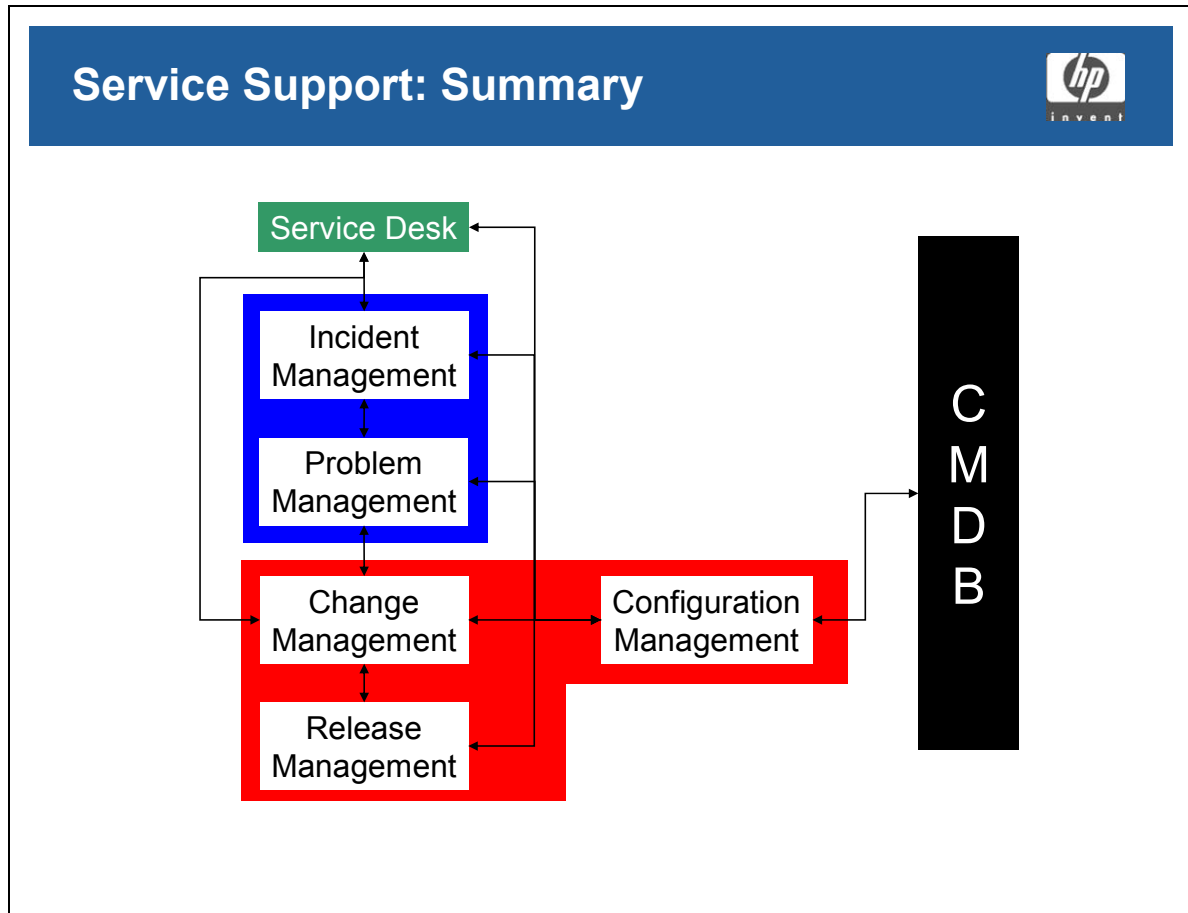
The benefits of introducing an effective Release Management process include:

1. Software is released into the live environment in a way that minimizes the chance of error
2. Only one version of a particular software application will be in use at any one time
3. The risk of illegal software being introduced is minimized

- |                        |                      |
|------------------------|----------------------|
| A. 1 and 2 are correct | B. Only 1 is correct |
| C. 1 and 3 are correct | D. All are correct   |

## Student Notes

## Service Support: Summary



## Student Notes

**Module 7**  
**Release Management**

---

## **Module 8 — Service Level Management**

---

## Mission of Service Level Management

### Mission of Service Level Management



To maintain and improve IT service quality through a cycle of negotiating, defining and managing the level of IT services and instigating actions to eliminate poor service

### Student Notes

*To maintain and improve IT service quality through a cycle of negotiating, defining and managing the level of IT services and instigating actions to eliminate poor service.*

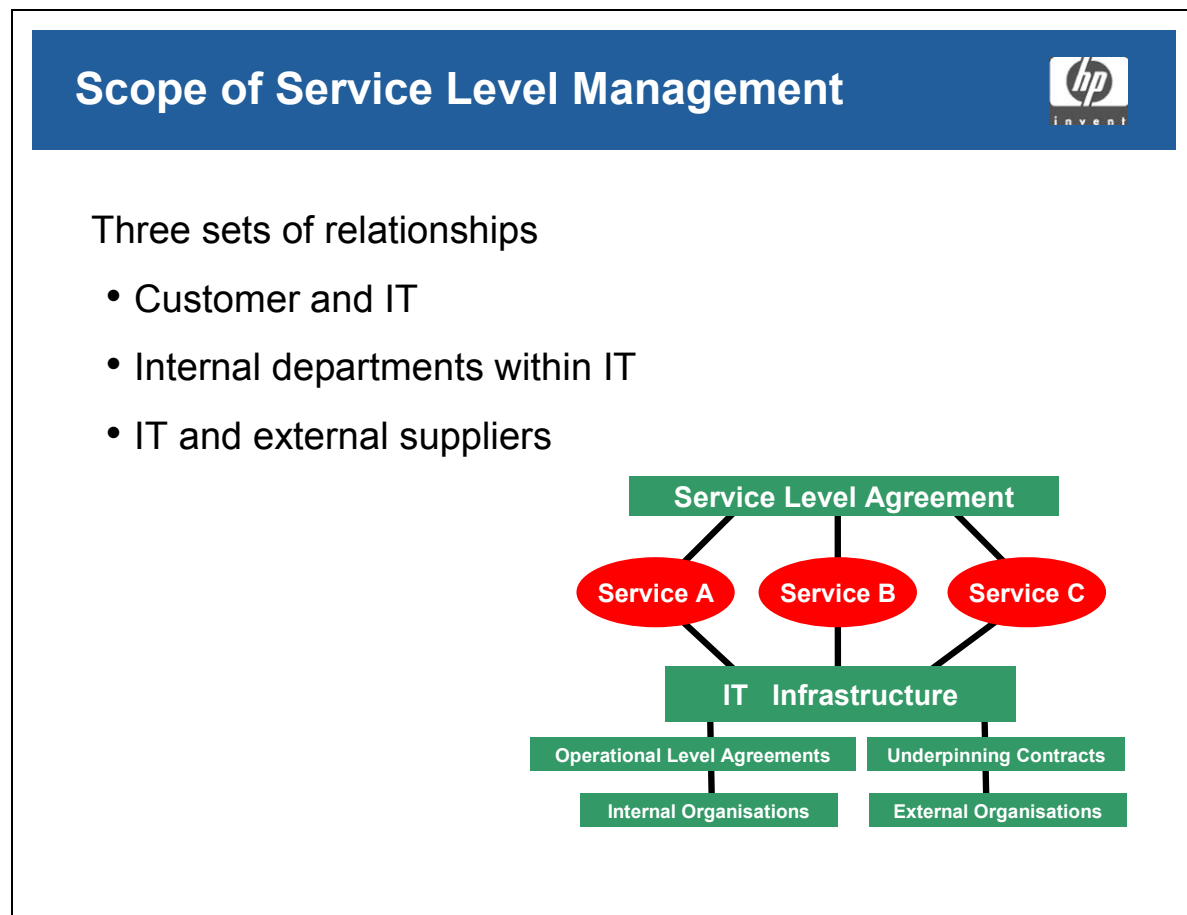
Service Level Management (SLM) in itself is not a guarantee of good service. It only really works if a number of other disciplines have been implemented and are working properly. At the same time, good service is not possible unless there is a formal program to determine and maintain a consistent level of service.

In many companies the quality of service is arbitrary. Few people can specify exactly what is meant by a quality service. This results in people judging the quality of service based on subjective criteria, usually based on short-term measurement. This is why customers can be satisfied with a service in one month, and demanding the resignation of IT personnel the following month.

Please note:

- Services are defined by the way in which the customer perceives them
- The services must be justified by the business
- SLM must quantify the services in terms that both IT and the business can measure
- This is used to set and manage the level of expectation

## Scope of Service Level Management



### Student Notes

The scope of the SLM process involves the management of IT services between:

- The customer organization and the IT services organization
- The IT services organization and its external suppliers
- The IT services organization and its internal departments



## Objectives of Service Level Management

### Objectives of Service Level Management



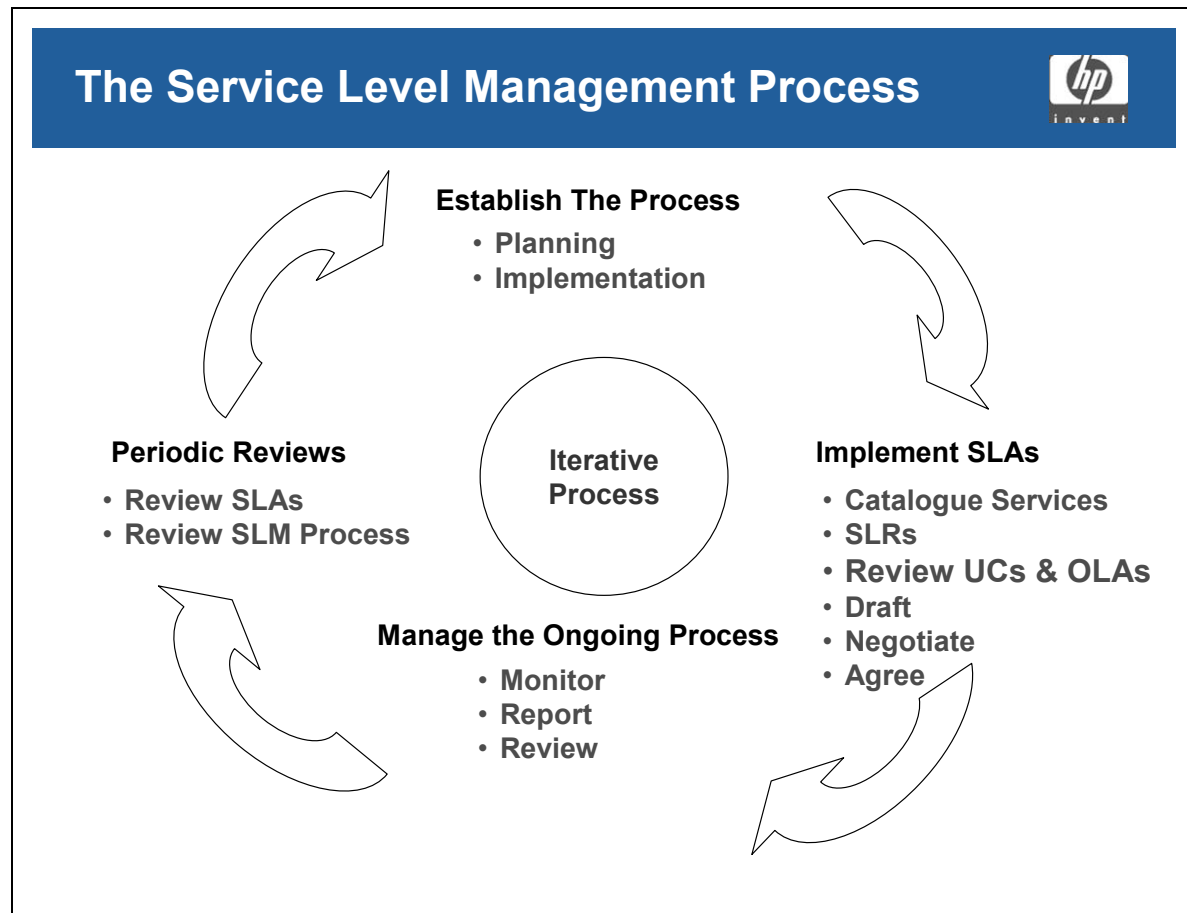
- To catalog IT services
- To quantify IT services
- To define internal and external service targets
- To achieve agreed service targets
- Ongoing improvement of service levels
- To review agreements and contracts

### Student Notes

When defining the objectives of the SLM process, the deliverables should be specified in quantifiable terms, for example:

- IT services are cataloged
- IT services are quantified in terms that both customer and IT provider can relate to
- Internal and external targets of IT services are defined and agreed
- Achievement of agreed service targets
- Ongoing improvement of service levels through a Service Improvement Program (SIP)
- Reviewing agreements and contracts to meet changing business needs

## The Service Level Management Process



### Student Notes

The Service Level Management Process creates a management framework which disciplines both the service provider and the customer. SLM encourages the customers to consider, document and define their real needs. SLM generally makes the service provider more focused and accountable.

#### Establish the Process

This is the introduction of SLM to an organization. The basic activities are:

- Establishing a project and appointing a project manager and team
- Defining the SLM documents to be used
- Specifying SLM tools
- Determine measurement capability
- Establish initial perceptions of service
- Determine what is currently being offered in terms of existing agreements or contracts

## Implement SLAs

This phase consists of:

- **Cataloging IT services:** This includes understanding what services are being used currently, as well as the level of customer expectation
- **SLRs:** This is where the SLM negotiates and agrees the service requirements and expected service characteristics with the Customer
- **Drafting SLAs:** Here the structures of the SLA are drawn up and services are mapped to customers
- **Negotiation:** This is the beginning of a reiterative process of setting actual levels of service that will be included in the SLAs
- **Review underpinning contracts and OLAs:** SLM has to be sure that they can deliver the required level of service before any agreement is signed. This is done together with the internal IT departments and the external IT suppliers
- **Agree:** The SLAs are finalized and signed by all parties

## Manage the Ongoing Process


- **Monitor:** Once an agreement is in place, it is continuously monitored to ensure compliance with the SLA, and also to identify areas for improvement
- **Report:** SLM reports are communicated regularly to different parties of the agreements to ensure ongoing awareness and improvement
- **Review:** Service reviews are held as part of a Service Improvement Program

## Periodic Reviews

Periodic audits are held in addition to the regular review cycle to ensure that the SLM function is working properly. These reviews include:

- SLAs
- The SLM process

## Internal and External Documents

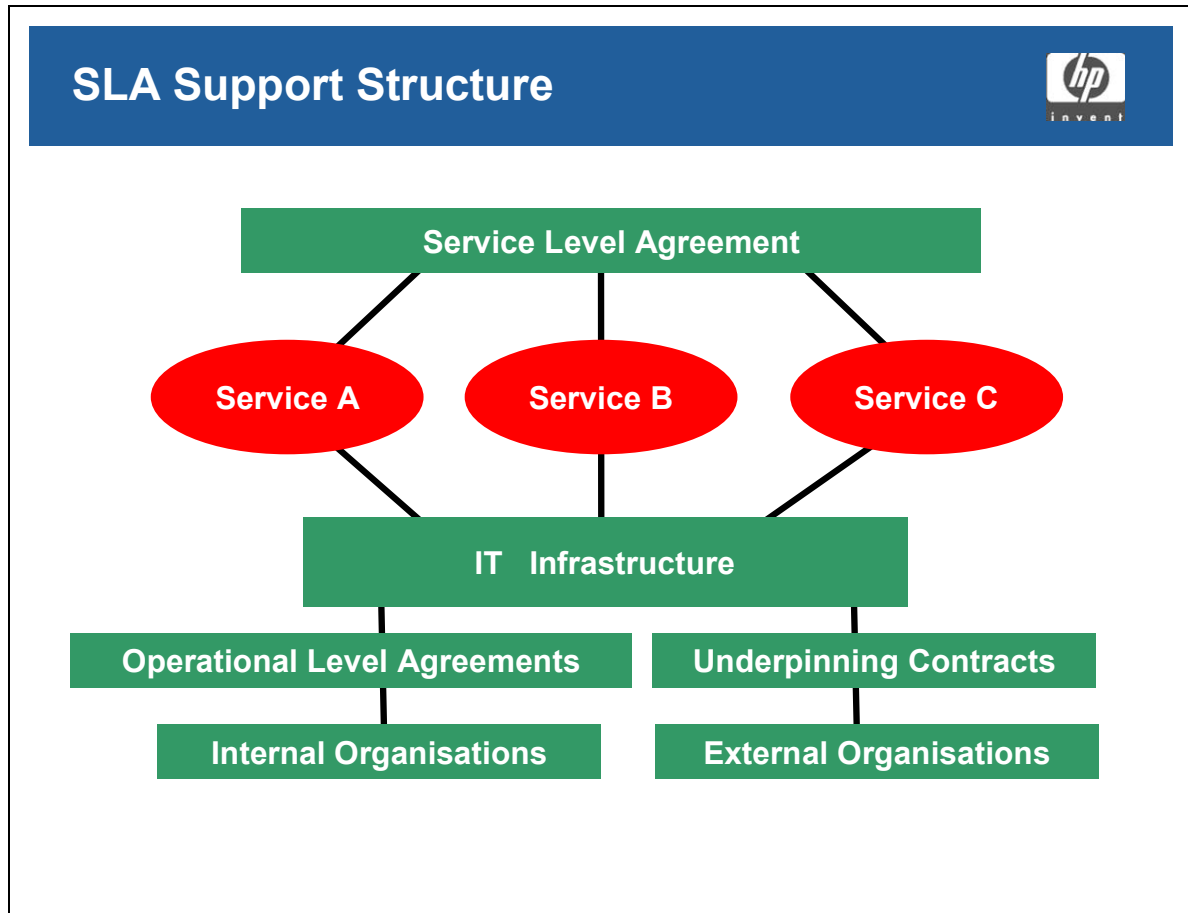
Internal and External Documents	
	
External Documents	Internal Documents
Refer to targets agreed with the customer	Refer to targets within the IT organization
Provide the input for the internal documents	Are defined from the stated customer requirements

### Student Notes

When specifying IT Services, documents for internal use should be separated from documents for external use.

Dividing these two types of document means that SLM does not have to bother customers with unnecessary technical detail, while still maintaining documentation for both business and IT staff.

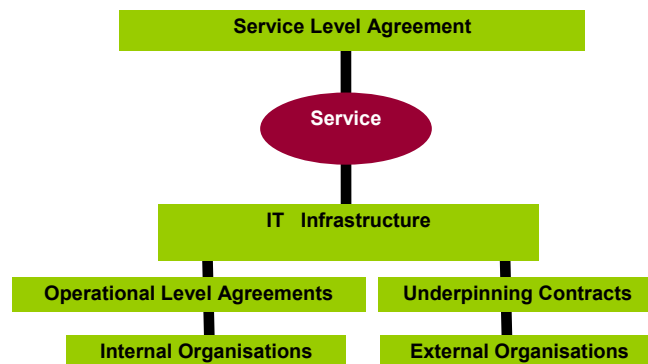
## SLA Support Structure



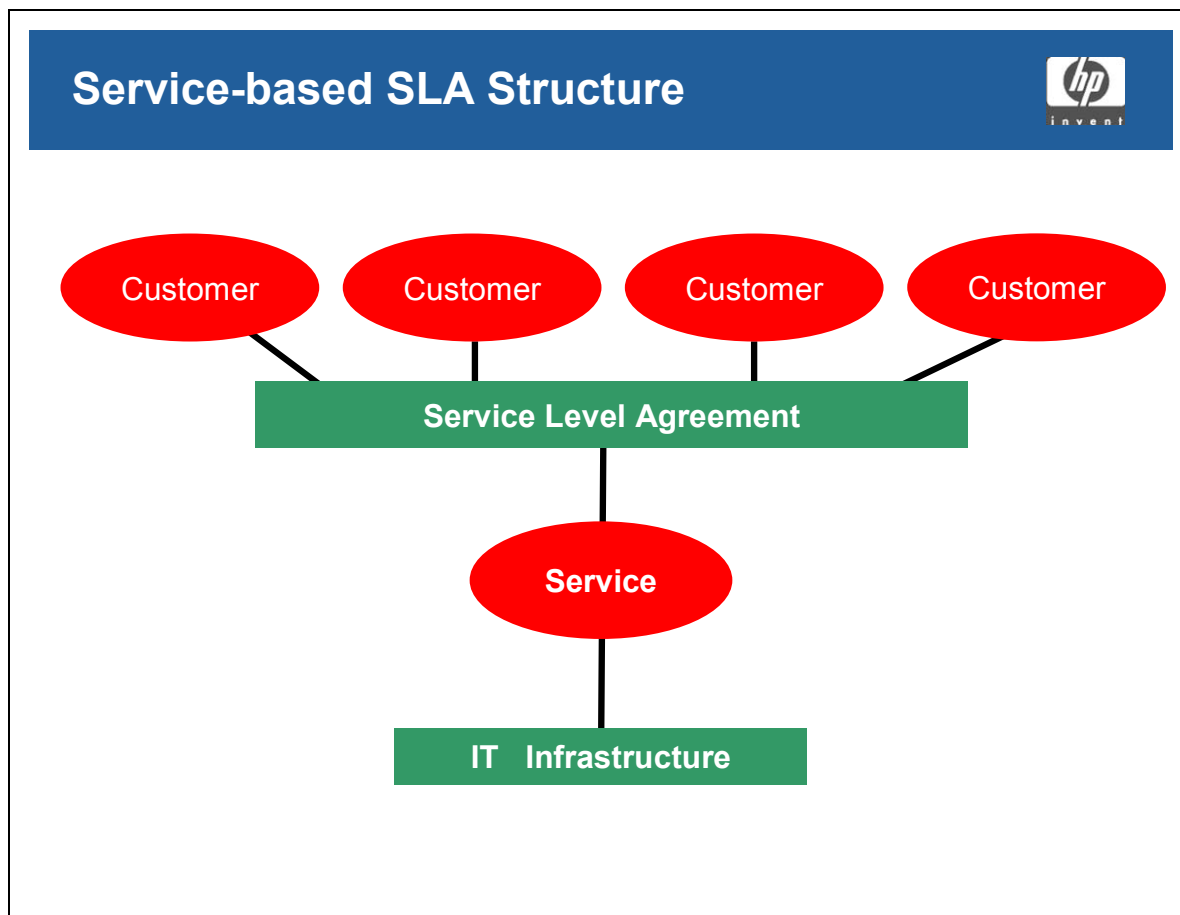
### Student Notes

SLAs are the formal agreements between IT and its customers. They are based on the specsheets. The content and structure of an SLA will depend on a number of factors including the physical, cultural and business aspects of the organization.

A simple SLA of one service to one customer could look like this:

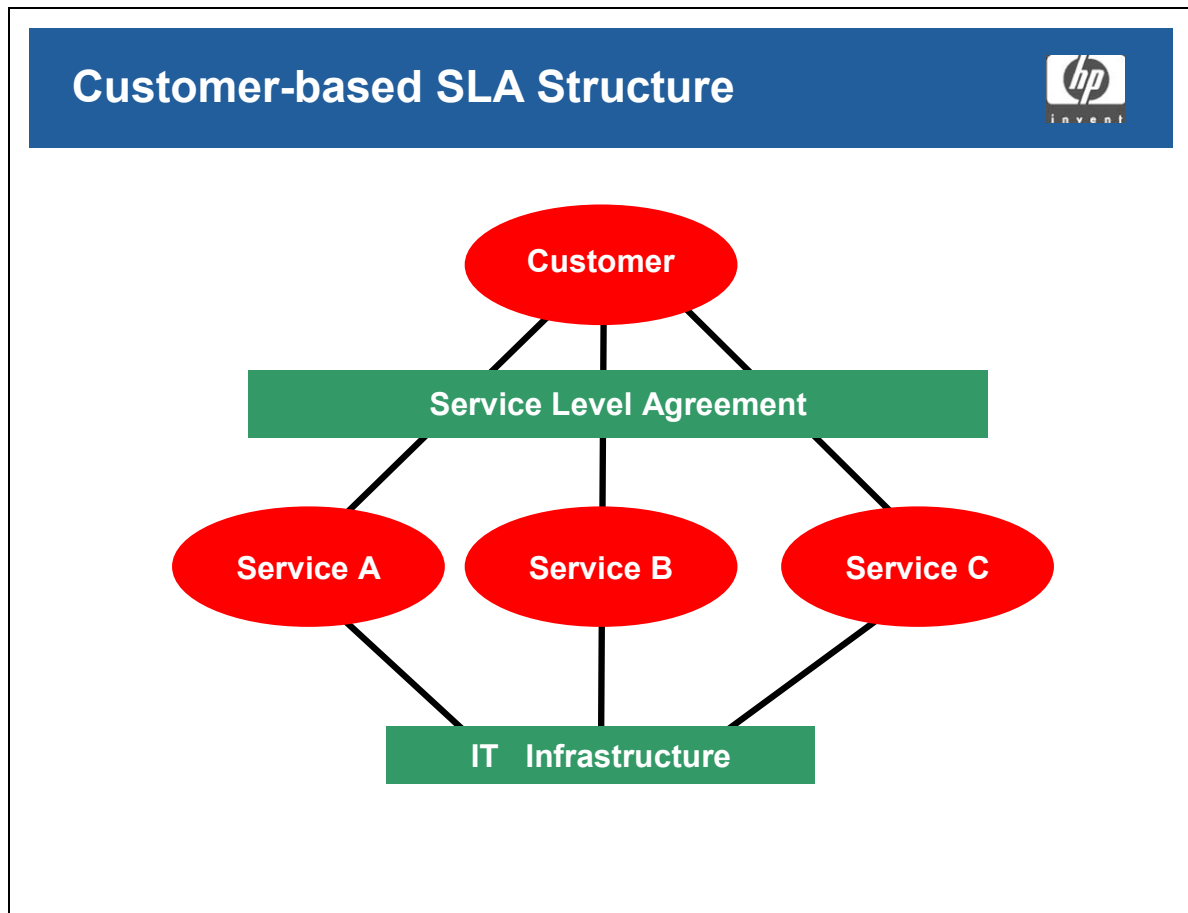


## Service-based SLA Structure



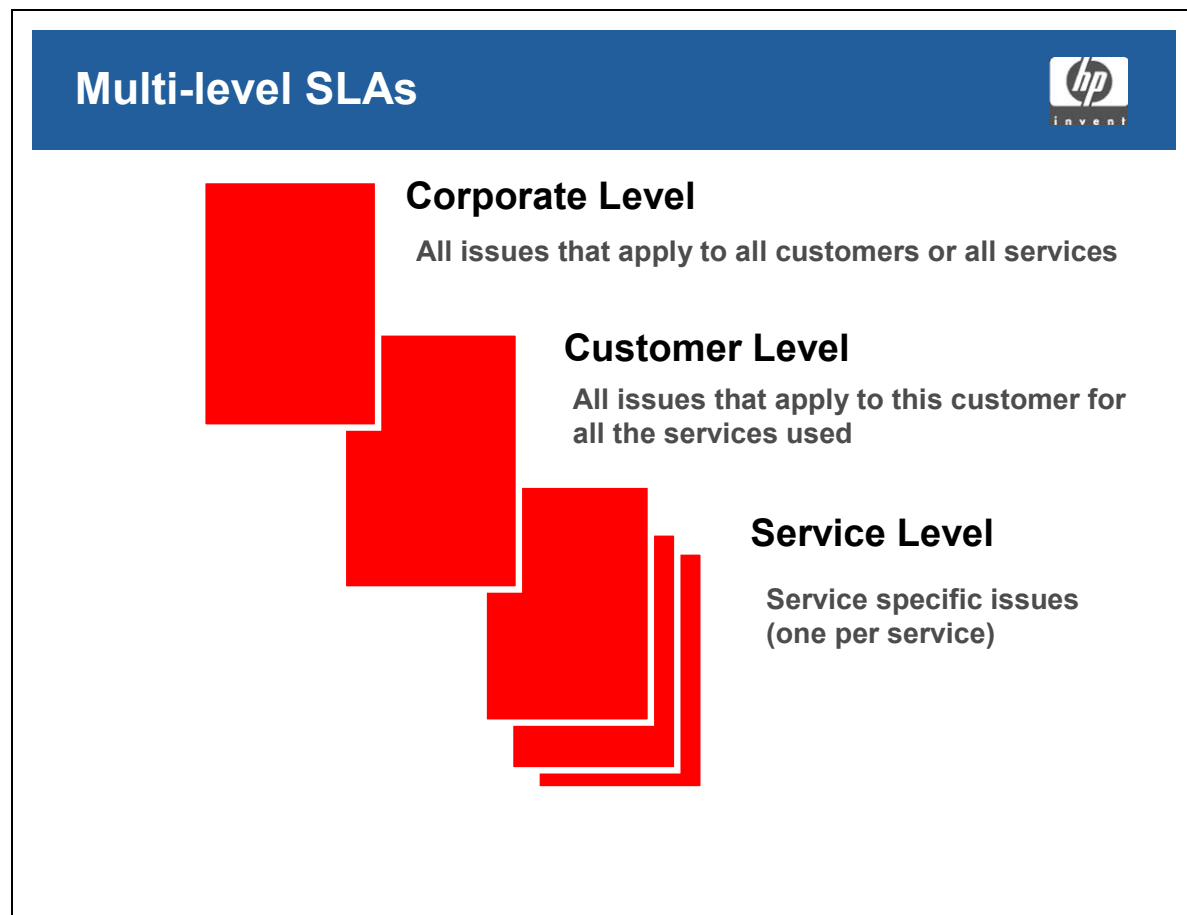
## Student Notes

## Customer-based SLA Structure



## Student Notes

## Multi-level SLAs



### Student Notes

ITIL makes allowance for multi-level SLAs to accommodate services offered at different levels within the organization.



## SLA Contents

### SLA Contents



- Service scope and description
- Service hours
- Measures of availability and reliability
- Support details – who to contact, when, how
- Respond and fix times
- Deliverables and time scales
- Change approval and implementation

## Student Notes

The contents of and SLA should include:

- Scope of the agreement and a description of the service
- Service Hours
  - The hours during which the service will be available
  - Extensions to the service hours
  - Special days (e.g. holidays)
- Measures of Availability and Reliability
  - Availability — this is measured as the percentage of agreed time that the customer could actually access the service. Availability should always be measured from the customer's perspective, although there should also be internal measures of individual component or system availability

## **Module 8**

### **Service Level Management**

- Service Reliability — this should not be confused with the reliability of components, which the customer will never see. Service reliability is measured as the Mean Time Between Failure (MTBF) of the service or Mean Time Between System Incidents (MTBSI)
- Support Details
  - Support hours
  - Service Desk contact details
  - Extension to support hours
- Respond and Fix Times
  - Target time to respond
  - Target time to resolve incidents
- Deliverables and Time Scales
- Change Approval and Implementation
  - Targets for responding to RFCs

## SLA Contents

### SLA Contents




- Reference to IT Service Continuity plan
- Signatories
- Responsibilities of both parties
- Reporting
- Review process
- Glossary of terms

## Student Notes

- Service Continuity
  - A brief summary of the Service Continuity plans that have been prepared
- Signatories
- Responsibilities of both parties
- Service Reporting and review
  - The content, frequency and distribution list of all periodic reports
  - Schedule of review meetings
- Glossary of terms

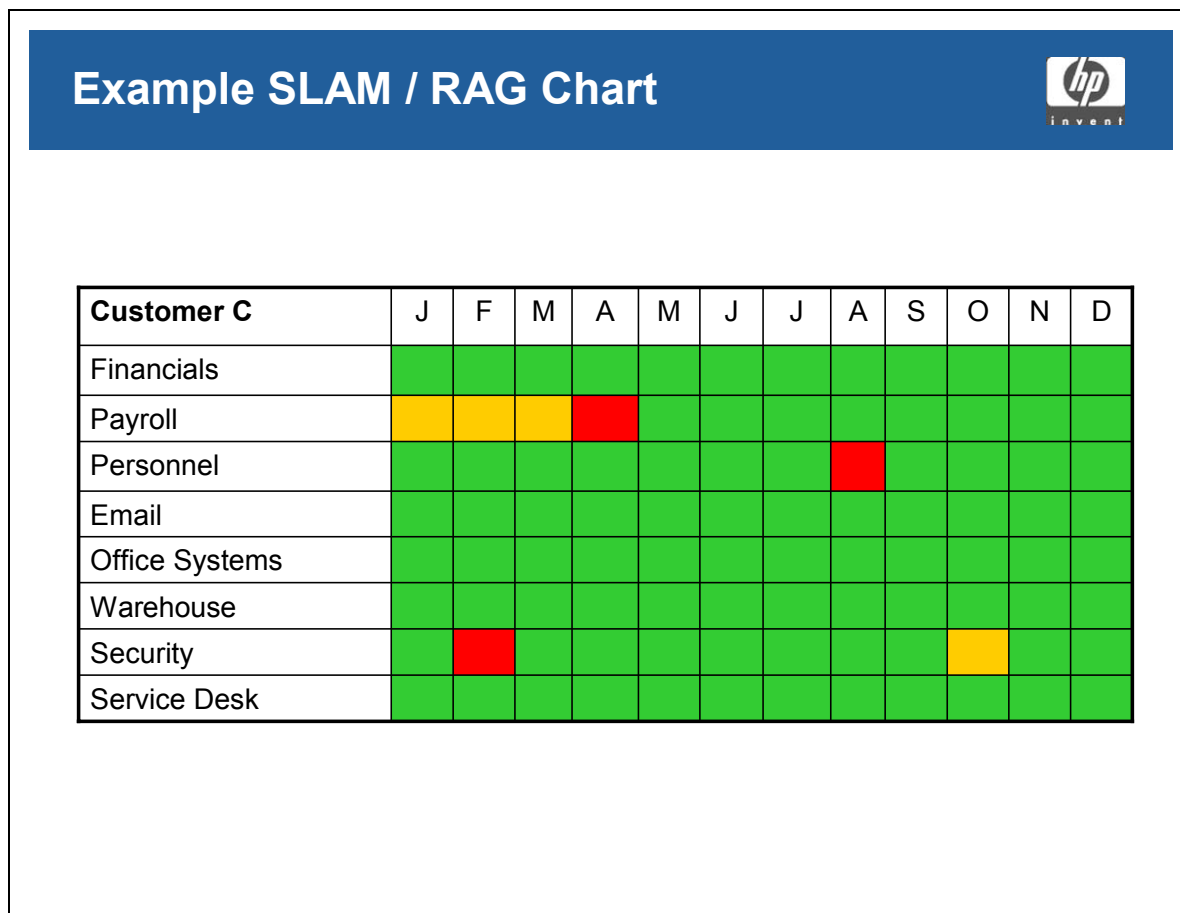
## Example Service Catalog

Example Service Catalog 										
Service /Customer	Accounts	HR	Wages	Warehouse	Transport	Admin	Sales	Marketing	Security	Factory
Financials	✓	✓	✓		✓	✓	✓	✓		✓
Payroll	✓	✓	✓							
Personnel		✓	✓							
Logistics				✓	✓	✓			✓	✓
Stock Control	✓				✓	✓	✓	✓		✓
CAD/CAM										✓
Production					✓	✓	✓			✓
CRM	✓					✓	✓	✓		
Email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Office Systems	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

## Student Notes

A service catalog should list all of the services being provided, a summary of their characteristics and details of the Customers and maintainers of each. A degree of 'detective work' may be needed to compile this list and agree it with the Customers (sifting through old documentation, searching program libraries, talking with IT staff and Customers, looking at procurement records and talking with suppliers and contractors etc). If a CMDB or any sort of Asset database exists, these may be a valuable source of information

## Example SLAM / RAG Chart



## Student Notes

A Service Level Agreement Management (SLAM) chart which can be used to give an 'at a glance' overview of how achievements have measured up against targets. These are most effective if color coded (Red-Amber-Green, and sometimes referred to as RAG charts as a result).

## Service Improvement Program

### Service Improvement Program



- Long term, formal process
- Aimed at improving service defined in SLAs
- Three components:
  - ITSM processes
  - Service culture
  - Management commitment

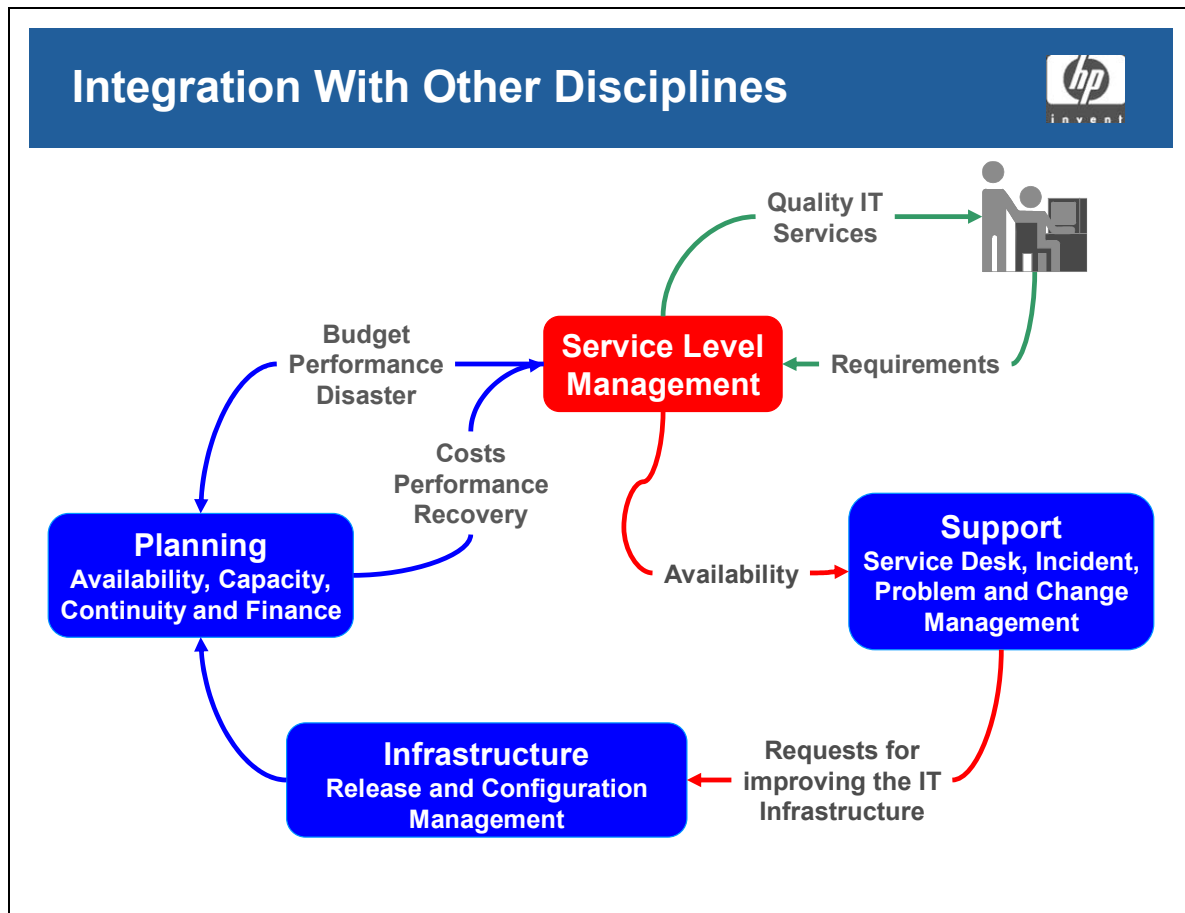
### Student Notes

The SIP is a long term, formal and planned process of improving the levels of service defined in the SLAs.

It requires at least three components:

- Formal, integrated ITSM processes
- A service culture
- Management commitment

## Integration with Other Disciplines



### Student Notes

Service Level Management does not operate in isolation. To be really effective, it needs to be integrated with the other Service Management disciplines.

#### Availability Management

Availability Management is responsible for the overall availability of the services provided by the IT infrastructure. This may involve the negotiation of underpinning contracts with external suppliers and may also involve setting targets to shorten service repair and restoration times.

Availability Management also provides management information to SLM in the form of availability statistics, which can be used as service achievement reports.

#### Capacity Management

The Capacity Plan is important in assessing IT's capability to meet internal targets, because it relates to current and expected usage levels of systems. Capacity Management also delivers reports for performance, resource and workload management that support the SLM monitoring activities.

## **Module 8**

### **Service Level Management**

SLM provides critical information about the business environment to Capacity Management to enable more accurate and relevant forecasting.

#### **Incident and Problem Management**

The Service Desk can detect service level deviations. It can also assist the SLM process through correct allocation of severity and the co-ordination of technical support teams to ensure timely resolution of problems.

Escalation times are agreed between the Service Level Manager and the Business Manager and it is up to the Problem Management team to implement the appropriate procedures.

The statistics provided by the Service Desk are an invaluable source of service performance information for the SLM process.

#### **Change Management**

Changes to existing IT services or IT infrastructure could affect service achievements. Change management verifies requests for change against the Service Catalogue and SLAs. Changes to any SLM documents should also be managed under strict change control.

#### **Configuration Management**

Configuration management is responsible for the registration of all components of the IT services. As such, this process will also register the Service Catalogue, SLAs, underpinning contracts, Service Quality Plan, customer organizations and suppliers.

#### **Financial Management**

Financial Management registers and maintains the cost accounts concerning IT service usage. It can supply statistics and reports to assist the SLM process in assessing the right balance between service cost and delivery. Cost aspects in the Service Catalog and SLAs are agreed between the Financial Manager and SLM.

#### **Service Continuity Management**

It is essential that IT services can quickly be recovered and delivered to the agreed quality in a contingency. Service Continuity Management aims to reduce the impact of major incidents, emergencies or disasters. It also advises SLM concerning continuity plans and test results.

Service Continuity Management provisions should be part of the SLA and should also include reference to the organization's business continuity management, which aims to protect all aspects of the organization's business.

The Service Level Manager therefore needs to work with any existing Business Continuity Management (BCM) plans and with those devising and maintaining them.



### **Security Management**

Attempted security violations must be reported to the Service Level Manager. Security requirements may well impose constraints on the SLM process including:

- Restricted access to business information
- System access security requirements that prevent an organization-wide access approach
- Physical security requirements that restrict maintenance and support access to some users and equipment
- Allocation of particular staff to specific customer areas.

### **Application Development**

Service Level requirements of new or revised software should be specified at the design stage. The SLM staff should work with the customers to determine the required service levels.

## Question

### Service Level Agreement Purpose



Consider the following statements:

- A Service Level Agreement is a document in which measurable levels of service are defined
- A Service Level Agreement gives customers guarantees that the most important applications will always be available

Which is correct?

- |                   |                    |
|-------------------|--------------------|
| A. Only the first | B. Only the second |
| C. Both           | D. Neither         |

## Student Notes

## Question

### Service Level Manager Responsibility



Which of the following is *not* the responsibility of the Service Level Manager?

- A. Drawing up a service catalogue
- B. Negotiating agreements with customers as to the levels of service they can expect to receive
- C. Making changes to services to ensure levels of service are maintained
- D. Reviewing actual levels of service against agreed levels of service

## Student Notes

**Module 8**  
**Service Level Management**

---

## **Module 9 — Availability Management**

## Mission of Availability Management

### Mission of Availability Management



To ensure the delivery of IT services where, when and to whom they are required, by planning and building a reliable and maintainable infrastructure and maintaining key support and supply relationships according to service requirements

### Student Notes

*To ensure the delivery of IT services where, when and to whom they are required, by planning and building a reliable and maintainable infrastructure and maintaining key support and supply relationships according to service requirements.*

This mission is achieved by determining the availability requirements of the business and matching these to the capability of the IT infrastructure, services and supporting organization to deliver a cost-effective and sustained level of availability enabling the business to meet their objectives.

Availability Management also deals with a number of security issues not otherwise addressed by Security Management.

## Scope of Availability Management

### Scope of Availability Management



- All new services
- Existing services where SLAs are in place
- IT Suppliers
- All infrastructure issues that can affect availability
- Not Service Continuity Management

### Student Notes

Availability Management should be applied to:

- All new IT services and
- Existing services where SLAs have been agreed
- IT suppliers (internal and external)
- All aspects of the IT infrastructure which may impact availability

Availability Management is not responsible for Service Continuity Management

## Objectives of Availability Management

### Objectives of Availability Management



- Designing IT services for availability
- Measuring and monitoring the key areas
- Optimize the availability of the infrastructure
- Reducing incident frequency and duration
- Corrective action for downtime
- The Availability Plan
- Balancing Availability and Cost

### Student Notes

- To ensure IT services are designed to deliver the agreed levels of availability
- To measure and monitor Availability, Reliability and Maintainability on an ongoing basis
- To optimize the availability of the IT infrastructure according to business objectives
- To work at reducing the frequency and duration of incidents
- To ensure corrective actions for downtime are identified and progressed
- To create and maintain an Availability Plan

Availability Management also has a responsibility to ensure that the cost of high availability does not exceed its value.

Availability Management will look for the best compromise between the cost of the availability solution and the costs of unavailability.



## Key Concepts

### Key Concepts



- Availability (%)
- Reliability (Time)
- Maintainability
- Serviceability
- Security

## Student Notes

Availability (%) — this is the ability of an IT service or infrastructure component to perform its required function at a stated moment or over a stated elapsed period of time.

Reliability (Time) — is defined as the freedom (of a component) from operational failure.

Maintainability — is the ability of an IT infrastructure component to be retained in, or restored to its operational condition

Serviceability — this describes the contractual arrangements made to assure the Availability, Reliability and Maintainability of infrastructure components and IT services.

Security — is defined in terms of Confidentiality, Integrity and Availability (CIA).

## Availability

### Availability



- Proportion of agreed service hours a customer can access a service
- Measured from the customers' perspective
- Expressed as a percentage

$$\text{Availability} = \frac{(\text{AST} - \text{DT})}{\text{AST}} \times 100$$

### Student Notes

Availability is the proportion of time that a customer is able to access a particular service. Availability is measured from the customer's point of view and is recorded in the SLA.

#### Basic Availability calculation

To determine the basic Availability of a given IT Service or component as an Availability percentage (%) the following basic formula can be used:

$$\text{Availability} = \frac{(\text{AST} - \text{DT})}{\text{AST}} \times 100 = \text{Service or Component Availability (\%)}$$

Where: - **AST** = Agreed service time & **DT** = Actual downtime during agreed service time

Example calculation overleaf

### Example

A 24x7 IT Service requires a weekly 2-hour planned downtime period for application maintenance. Following the completion of the weekly maintenance an application software error occurs which results in 3 hours of unplanned downtime.

The weekly Availability for the IT Service in this reporting period is therefore based on the following:

The **AST** should recognize that the planned 2 hr weekly downtime is scheduled.

The **DT** is the 3 hrs of unplanned outage following the application maintenance.

The **AST** value is therefore 24hrs x 7days - 2 hrs planned maintenance = 166 hrs/week.

The **DT** value is therefore the 3 hrs unplanned downtime.

The Availability calculation is: -

$$A = 166 - 3 / 166 \times 100 = 98.78\%$$

## Reliability

### Reliability



- Freedom from operational failure
- Ability to perform
  - a required function
  - under stated conditions
  - for a stated time
- MTBF/MTBSI

### Student Notes

Reliability of a service is determined by the amount of freedom from operational failure.

Reliability can further be defined as the ability of components to perform a required function under stated conditions for a stated period of time.

Measurements of reliability include:

- Mean Time Between Failures (MTBF)
- Mean Time Between System Incidents (MTBSI)
- Number of breaks in a period

Reliability depends on:

- The resilience built into the service
- The preventative maintenance applied

## Maintainability, Serviceability, and Security

### Maintainability, Serviceability, and Security



#### Maintainability

- Preventative maintenance
- Restoration and repair times, Mean Time To Repair (MTTR)

#### Security

- Confidentiality, Integrity and Availability to authorized personnel only

#### Serviceability

- The support for which external suppliers can be contracted to provide parts of the IT infrastructure

## Student Notes

### Maintainability

This is the ability of an IT service to be maintained in or restored to a satisfactory operational state.

Maintenance or restoration of a service can be divided into 5 separate stages:

- Anticipating failures
- Detecting failures
- Diagnosing failures
- Resolving failures
- Recovering from failures
- Restoring the data and IT Service
- Applying preventive maintenance to prevent failures occurring

## **Security**

Availability Management is concerned with the Availability of all IT Service components, including data. Availability Management is therefore closely connected with Security Management. As a result, there is potential for confusion between the process owners for Security Management and Availability Management with regard to security requirements for new IT Services. Here is a tip to help clarify this:

Security Management can be viewed as *accountable* for ensuring compliance to IT security policy for the implementation of new IT Services. Availability Management is *responsible* for ensuring security requirements are defined and incorporated within the overall Availability design.

Security Management, in the context of this course, is the process of protecting and maintaining the **C**onfidentiality, **I**ntegrity and **A**vailability (CIA) of data.

A number of security issues have to be covered by Availability Management:

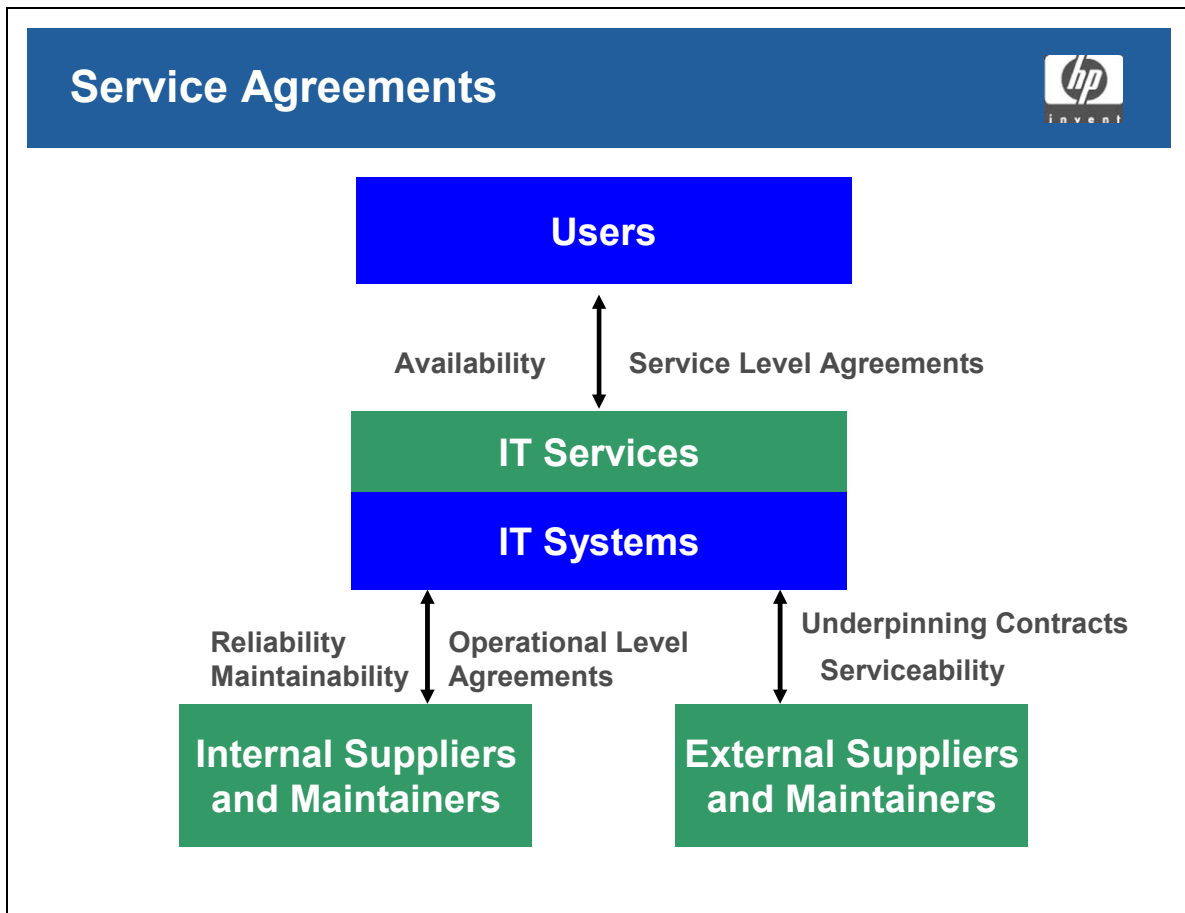
- Services must only be available to authorized staff
- Data must be available only to authorized staff and only at agreed times
- Services must be recoverable within the agreed confidentiality and integrity parameters
- Services must be designed and operated within IT security policies
- Access for contractors to hardware or software

## **Serviceability**

This is the ability of external suppliers to meet the contractual conditions regarding reliability, maintainability and maintenance support of components.

In an outsourced environment, availability and serviceability are the same thing.

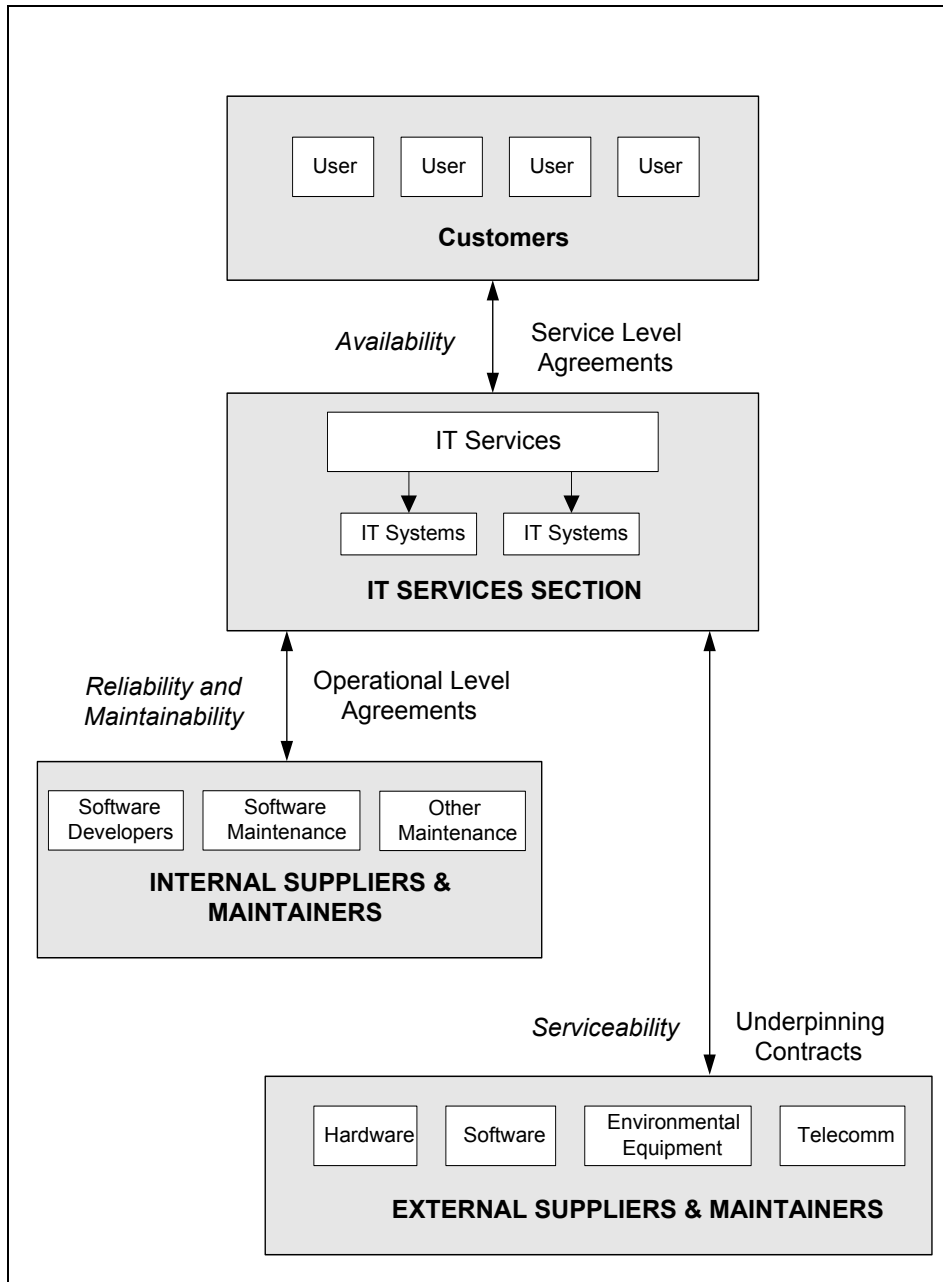
## Service Agreements



## Student Notes

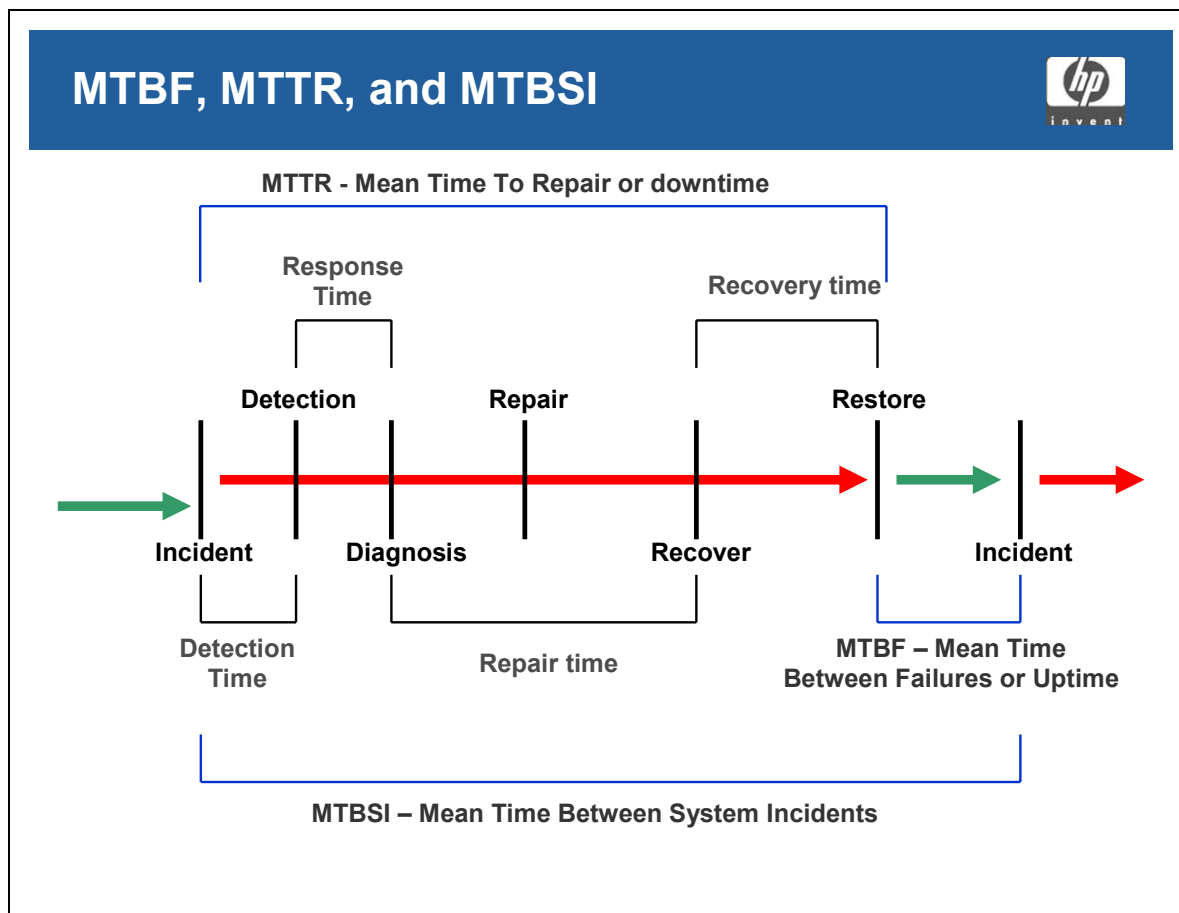
## Module 9 Availability Management

### Relationships with suppliers and maintainers





## MTBF, MTTR, and MTBSI



### Student Notes

This diagram (the Expanded Incident Lifecycle) illustrates the relationship between Availability Management and the Incident lifecycle.

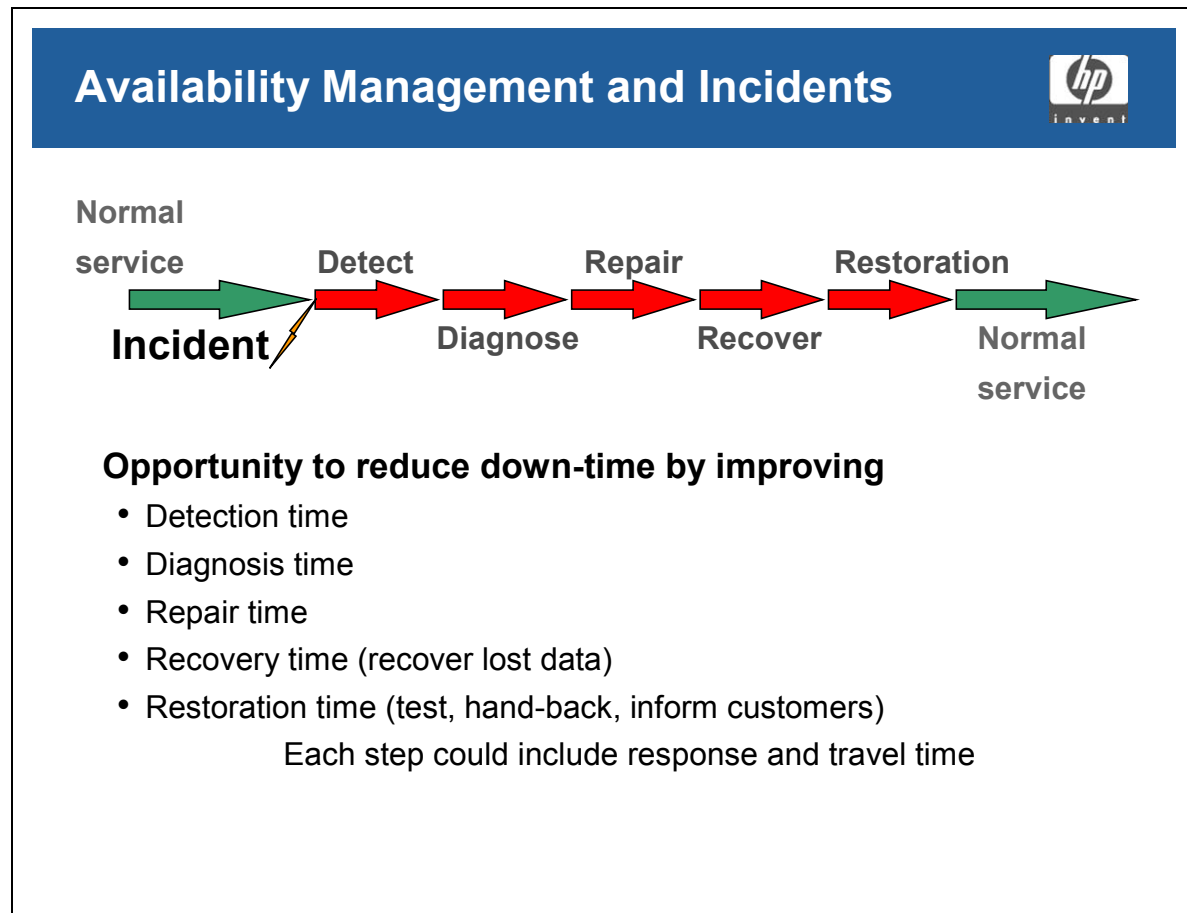
The role of Availability Management in this scenario is to find ways of shortening the elements of downtime, and lengthening uptime. This will be done together with Problem, Change and Capacity Management.

**The Mean Time Between Failure (MTBF)** for a given component is defined as that period between the restoration of service using that component — following a ‘failure’ (incident) of the component — and the next failure of the component.

**The Mean Time To Repair (MTTR)** — also known as ‘Downtime’ — for a given component is defined as that period of time between the detection of the ‘failure’ (incident) of the component and the restoration of service using that component.

**The Mean Time Between System Incidents (MTBSI)** is that period of time between the detection of one incident and the detection of another incident on the same component.

## Availability Management and Incidents



### Student Notes

Opportunity to reduce down-time by improving

- Detection time
- Diagnosis time
- Repair time
- Recovery time (recover lost data)
- Restoration time (test, hand-back, inform customers)
- Each step could include response and travel time

## Vital Business Function (VBF)

### Vital Business Function (VBF)



The business critical functions of the organization, supported by an IT service

### Student Notes

The Vital Business Function(s) are those business functions identified as business critical through a formalized process — typically a risk or Business Impact Assessment (see IT Service Continuity Management) — that are supported by an IT service.

An IT Service may support a number of business functions that are less critical. For example an ATM service **VBF** would be the dispensing of cash. However the ability to obtain a mini statement print from an ATM may not be considered as vital. This distinction is important and should influence Availability design and associated costs.

## Availability Components

### Availability Components



- Design
  - Availability and Recovery
- Availability Plan
  - Continuous Improvement
- Measurement
  - Metrics
  - Monitoring
  - Reporting

## Student Notes

### Designing for availability and recovery

- Should be designed from the start of development
- Identify Single Points of Failure (SPOF)
- Risk Analysis
- Define measurements and instrumentation for new services
- Testing

## **Availability Plan**

Availability improvement is a long term, dedicated plan for improving availability levels within budget constraints. The major output of this function is the Availability Plan.

The Availability plan should be a long-term plan for the improvement of IT availability within the agreed cost.

The plan should have goals, objectives and deliverables and should consider the wider issues of people, process, tools and techniques as well as having a technology focus.

## **Availability Measurement and Reporting**

- **Metrics:**  
The availability of infrastructure components and supported IT services must be monitored. From the figures gained, trend analysis of availability, reliability and maintainability can be conducted. This can lead to improvements in maintenance procedures, timing and costs and refinement of the resilience built into the infrastructure.
- **Monitor maintenance obligations:**  
The serviceability should be monitored by examining the performance of the maintenance organizations/functions in regard to the components, systems and services they support. The baseline metrics are the targets set for availability, reliability and maintainability of the infrastructure components.
- **Produce management information:**  
Appropriate management information should be collected and disseminated.

## Techniques and Tools

### Techniques and Tools



- Component Failure Impact Analysis (CFIA)
- Fault Tree Analysis (FTA)
- CCTA Risk Analysis and Management Method (CRAMM)
- Service Outage Analysis (SOA)
- Expanded Incident Lifecycle
- Technical Observation Post (TOP)

## Student Notes

### Component Failure Impact Analysis (CFIA)

CFIA is a technique developed by IBM and used to identify the impact on specific service if a specific system or component should be unavailable.

### Fault Tree Analysis (FTA)

This technique is used to analyze the chain of events that led to an instance of downtime. The following types of events are investigated and linked until the root cause of the failure is found.

- Basic events, which do not require further investigation
- Resulting events, which are caused by a another event
- Conditional events, which occur under specific conditions
- Trigger events, which initiate another event, such as an alarm

### **The CCTA Risk Analysis and Management Method (CRAMM)**

Identifying risks and identifying activities to mitigate them are important activities in Availability Design and Service Continuity.

CRAMM exists as a software tool as well as a methodology used to identify risks and countermeasures. The components of this methodology are discussed in the section on IT Service Continuity Management

### **Service Outage Analysis (SOA)**

This technique is used to analyze downtime and to identify opportunities to improve end-to-end service uptime. Once an opportunity has been identified, the following steps are taken:

- Scope and plan the assignment
- Build hypotheses (possible cause and effect relationships)
- Analyze data
- Interview key personnel
- Produce the findings and recommendations in a report
- Build and validate the solution

### **The Expanded Incident Lifecycle**

Discussed earlier in the chapter under MTBF, MTTR and MTBSI

### **Technical Observation Post (TOP)**

A TOP is a prearranged meeting of specialist technical support staff from within the IT support organization brought together to focus on specific aspects of IT availability.

The TOP will monitor real time events so that they can identify improvements or bottlenecks.

The TOP is also a means of identifying areas for ongoing improvement.

## Example of CFIA

### Example CFIA



Component	Gateway 12	Application Server 1	File Server 1	Printer 104
Accounting	-	X	B	A
Human Resources	-	X	-	-
E-Mail	F	-	-	-
Stock Control	-	-	B	A

X – Failure of component causes total loss of service to the workload

A – There is an Alternative device

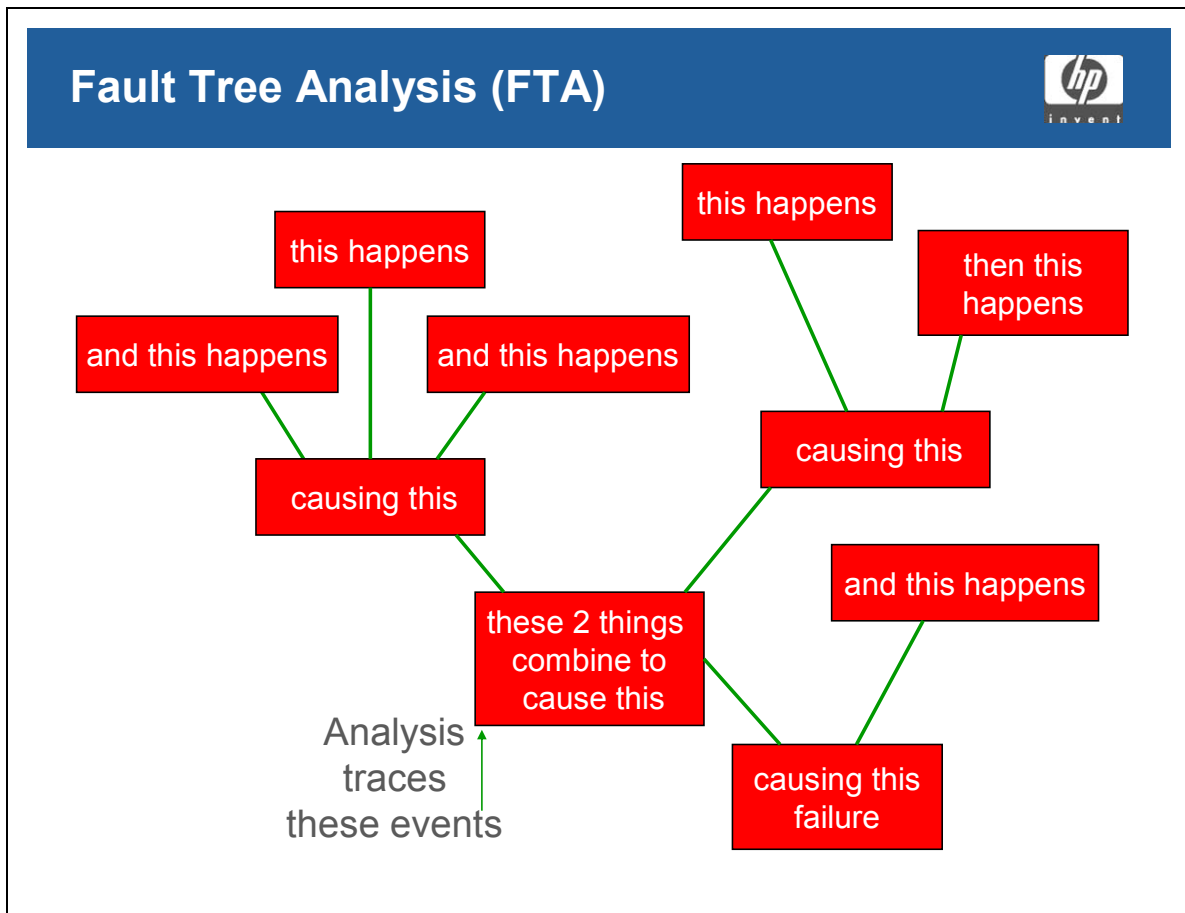
B – There is a backup device

F – There is an alternative path

## Student Notes

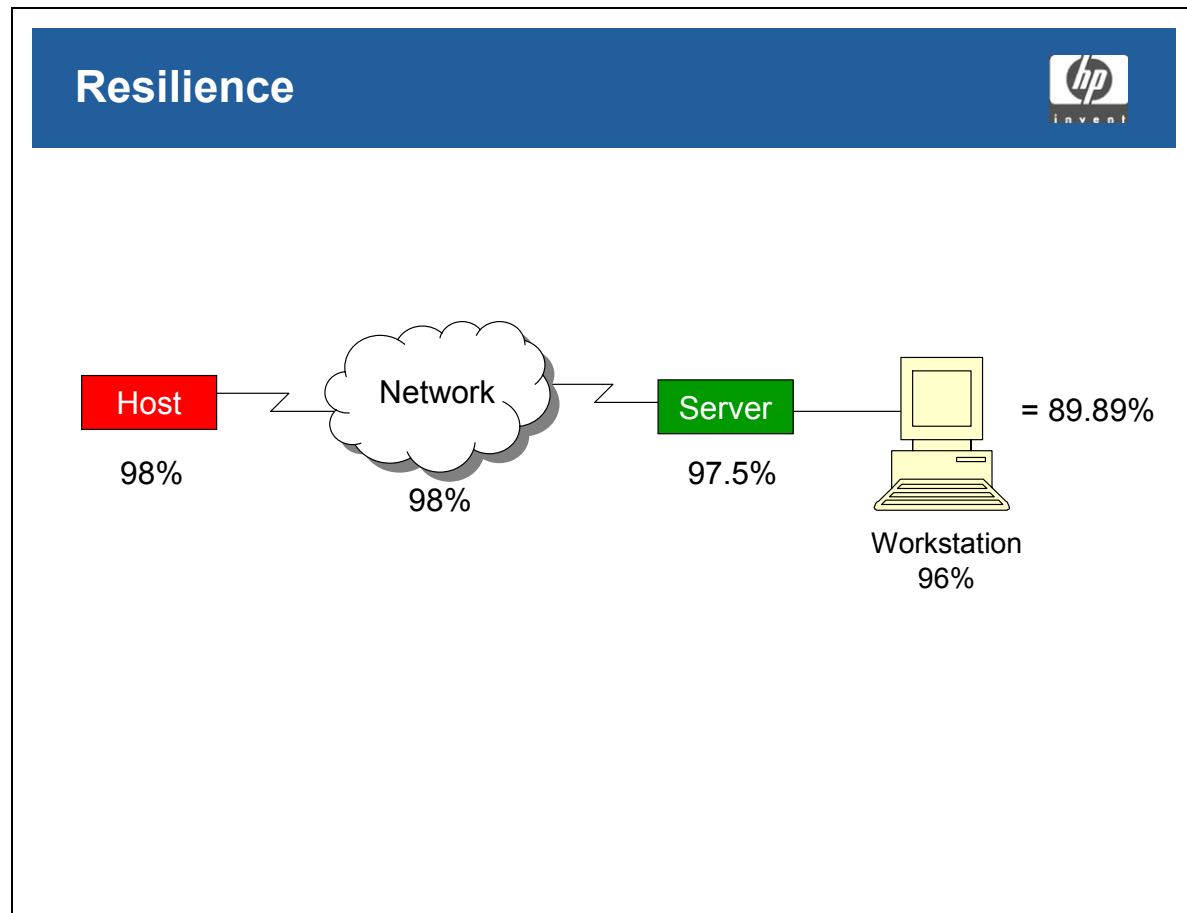


## Fault Tree Analysis (FTA)



## Student Notes

## Resilience



### Student Notes

Definition of Resilience – the capability of a set of CIs to continue to provide a required function when one or more CIs in the set have suffered a failure.

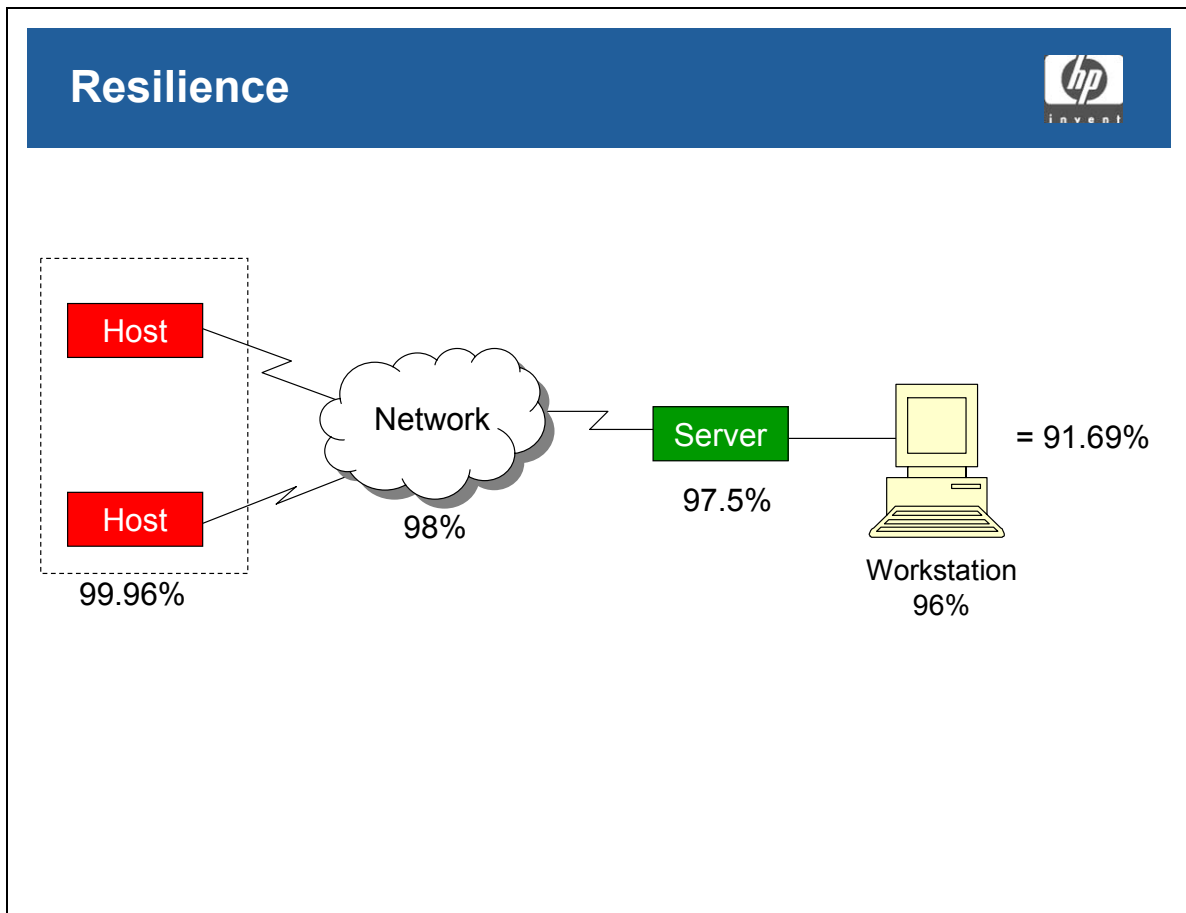
The aim of resilience is to build robust components, using redundancy or multiple fallback options so that, even if the component is threatened, it will not be compromised.

Because of its focus on maintaining up time, resilience “belongs” to Availability Management, although it is often implemented as a result of the Service Continuity Management process.

Resilience (or “*bouncebackability*”) is usually implemented in the following areas:

- Physical environment
- Computer environment (hardware and software)
- Network environments

## Resilience



## Student Notes

## Question

### Risk Analysis and Management Techniques



Risk Analysis and Management techniques are essential components of which of the following disciplines?

1. Configuration Management
  2. Availability Management
  3. IT Service Continuity Management
  4. Capacity Management
- A. 1 and 2
  - B. 2 and 4
  - C. 2 and 3
  - D. 3 and 4

## Student Notes

## Question

### Continuous Operation



A Network Server operates continuously for an average period of 2000 hours. This figure is a measure of:

- A. Availability
- B. Reliability
- C. Maintainability
- D. Security

## Student Notes



---

## **Module 10 — Capacity Management**

## Mission of Capacity Management

### Mission of Capacity Management



To ensure best use of the appropriate IT Infrastructure to cost effectively meet business needs by understanding how IT services will be used and matching IT resources to deliver these services at the agreed levels currently and in the future

### Student Notes

*To ensure the best use of the appropriate IT Infrastructure to cost-effectively meet business needs by understanding how IT services will be used and matching IT resources to deliver these services at the agreed levels of service currently and in the future*

There are two major elements to Capacity management, firstly the maintenance of a balance between cost and capacity, and secondly the maintenance of a balance between supply and demand.

#### Cost against Capacity

Capacity Management should ensure that the capacity (of the IT infrastructure – processing power, disk storage, printing, etc.) can be cost-justified in terms of the stated business need and also provides the most efficient use of the resources available.

#### Supply against Demand

Capacity Management must make sure that the IT infrastructure (processing power, disk storage, printing, etc.) available for use meets the current demands of the business and can address the future needs of the business.



To achieve this, Capacity Management may use a number of strategies, including differential charging (eg. charging different rates for the use of a resource depending on the time of day).

Capacity management needs to understand the business's requirements for service delivery and the IT infrastructure. It must also understand how the business is organized and operates. It must also understand the potential for service delivery and any new technologies that could be used to deliver the service more cost-effectively.

The rate of change in new technology and business development is unlikely to slow down. Capacity Management must keep abreast of all such developments.

## Scope of Capacity Management

### Scope of Capacity Management



- Hardware
- Software
- Networking equipment
- Peripherals
- Human Resources

### Student Notes

Capacity Management will include planning for:

- Hardware
- Software
- Networking equipment
- Peripherals
- Human resources, but only where a lack of human resources could result in a delay in end-to-end response time

## Objectives of Capacity Management

### Objectives of Capacity Management



- Optimal performance of the current infrastructure
- Understanding how the infrastructure is being used and how it will be used
- Building capacity for new services
- Forecasting and planning infrastructure requirements for ongoing IT Service Delivery

### Student Notes

The key objectives are:

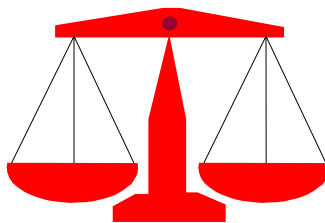
- To ensure that the existing infrastructure is performing optimally in terms of the agreed levels of service
- To understand the way in which the infrastructure is currently being used and will be used in future
- To build capacity for new services so that existing services are not impacted
- To forecast and plan infrastructure requirements to ensure the ongoing delivery of agreed IT services

## Capacity Management

### Capacity Management



Capacity Management is concerned with having the appropriate IT capacity and making the best use of it.



Under capacity causes  
performance problems

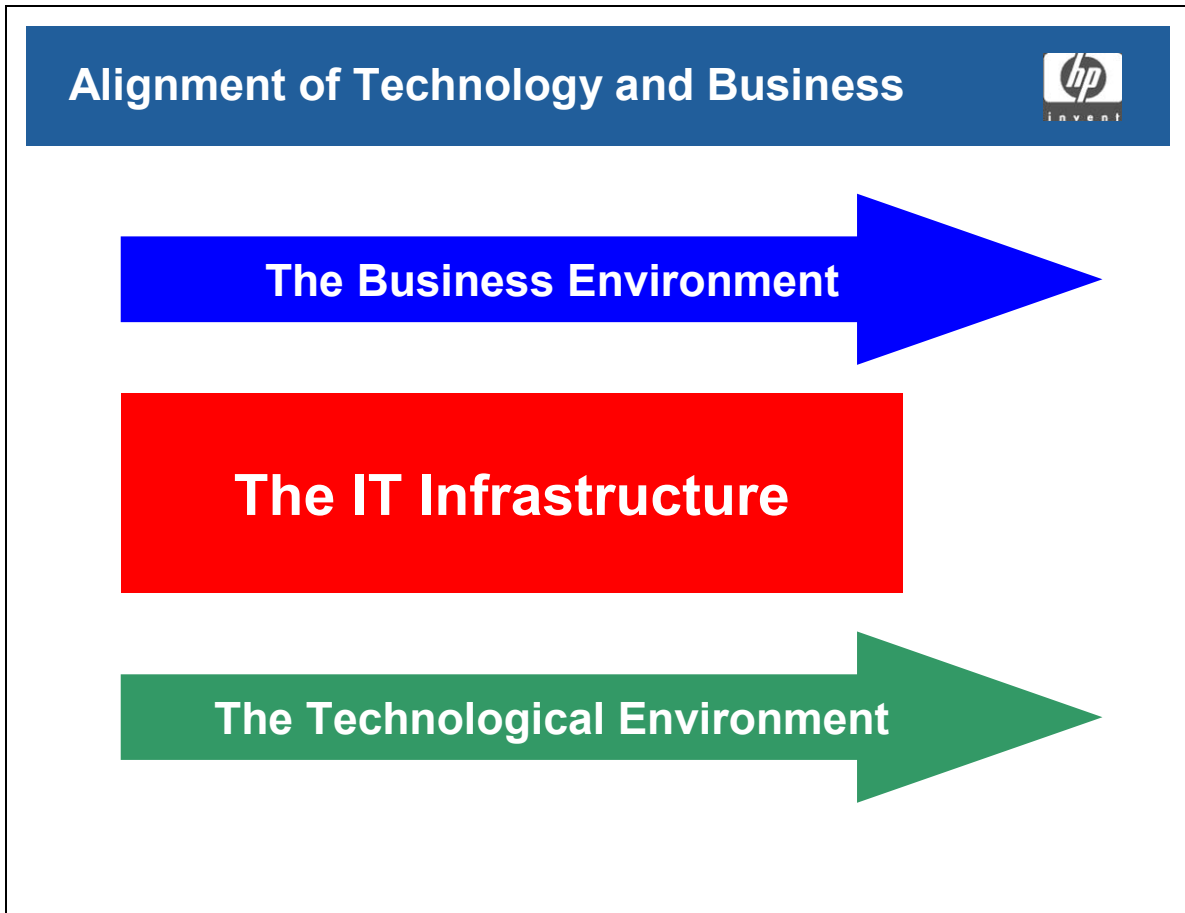
Over capacity is expensive and  
increases the cost of services

### Student Notes

Capacity Management is responsible for ensuring that the capacity of the IT infrastructure matches the evolving demands of the business in the most cost-effective and timely manner. That 'cost-effectively' is a most important phrase:

- Under capacity causes performance problems which can affect availability hence impacting business productivity and consequently revenue
- Over capacity is expensive and increases the cost of services thereby not offering the business value for money

## Alignment of Technology and Business



### Student Notes

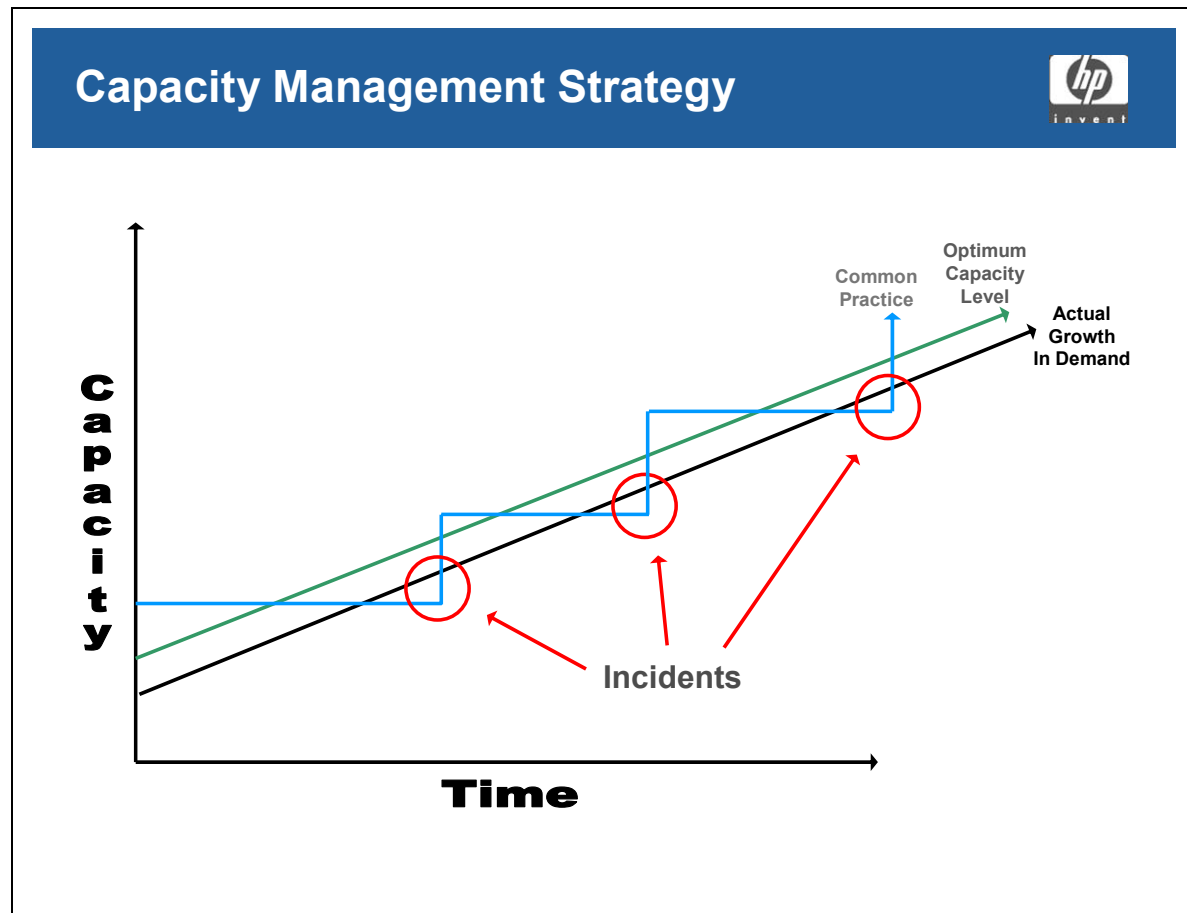
One of the major inputs for Capacity Management is change, which comes from two primary sources — the business and the industry.

Nothing remains constant in business. The amount, type and method of work changes constantly as the organization strives to maintain competitive advantage. IT services must be constantly evaluated to ensure that they stay in line with organizational changes.

On the other hand, technology is developing faster than anyone could have imagined. New innovations bring new opportunities and for our business. How can we best make use of them? Will they really save us money? Are they going to make us more productive?

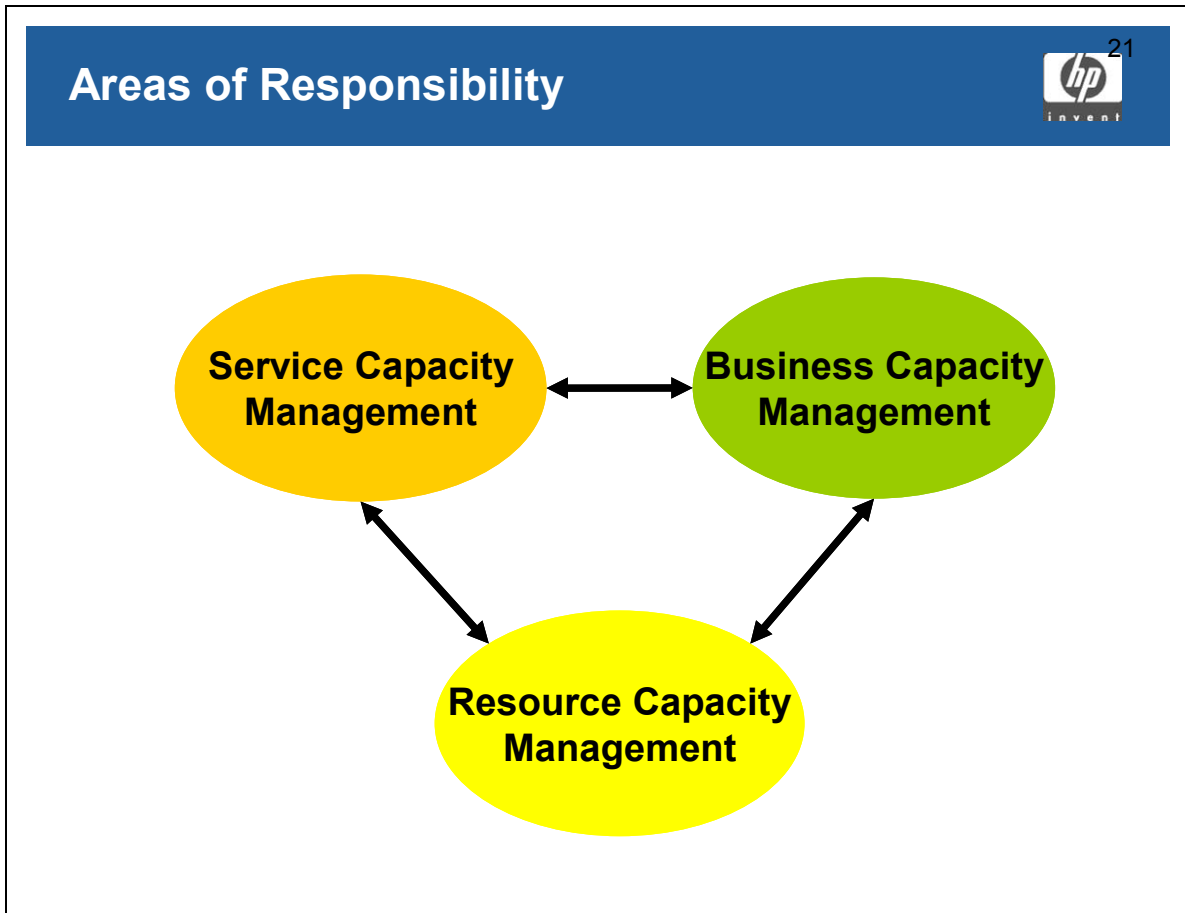
These are questions that the Capacity Manager has to help find the answers to. This is only possible if we know how systems have performed in the past under known variables and can compare these figures with current and projected variables.

## Capacity Management Strategy



### Student Notes

## Areas of Responsibility



### Student Notes

The three primary sub-processes of Capacity Management individually address the areas of:

- Business Capacity Management
- Service Capacity Management
- Resource Capacity Management

## Capacity Management

### Capacity Management



#### **Business Capacity Management**

- understand future business needs
- plan and implement sufficient capacity to support services

#### **Service Capacity Management**

- understand IT services, resource usage and variations
- ensure that SLA targets can be met

#### **Resource Capacity Management**

- understand the utilization of all component parts of the IT infrastructure
- optimize use of the current hardware and software resources

## Student Notes

### **Business Capacity Management**

A prime objective of the Business Capacity Management sub-process is to ensure that future business requirements for IT services are understood and taken into account, that there is planning for sufficient capacity to support (new) services, and that this capacity is implemented at an appropriate time.

There may be a variety of sources of information with which Capacity Management needs to engage. Some will lie within the business (functions), others may arise within the Change Management process and within Capacity Management itself.



Inputs into this area include:

- Existing SLAs
- Future service level requirements
- The business plans
- The capacity plan
- Modeling
- Application sizing

It is important to recognize that Capacity Management is an essential aspect of good IT management and must not be left until the last moment.

### **Service Capacity Management**

A prime objective of the Service Capacity Management sub-process is to identify and understand the IT services provided, how the resources are utilized, what (and when) peaks and troughs occur, and what patterns of working exist or become established. This leads to assurance that the IT services can and do meet the targets set for them in SLAs. This last provides the focus for Service Capacity Management — that of managing service performance as set out in the SLAs.

By monitoring performance and comparison with the targets, Service Capacity management can advise Service Level Management of service breaches or any 'close calls'.

Inputs include:

- SLAs
- Systems and service throughput and performance
- Monitoring, measurement, analysis, tuning and demand management

### **Resource Capacity Management**

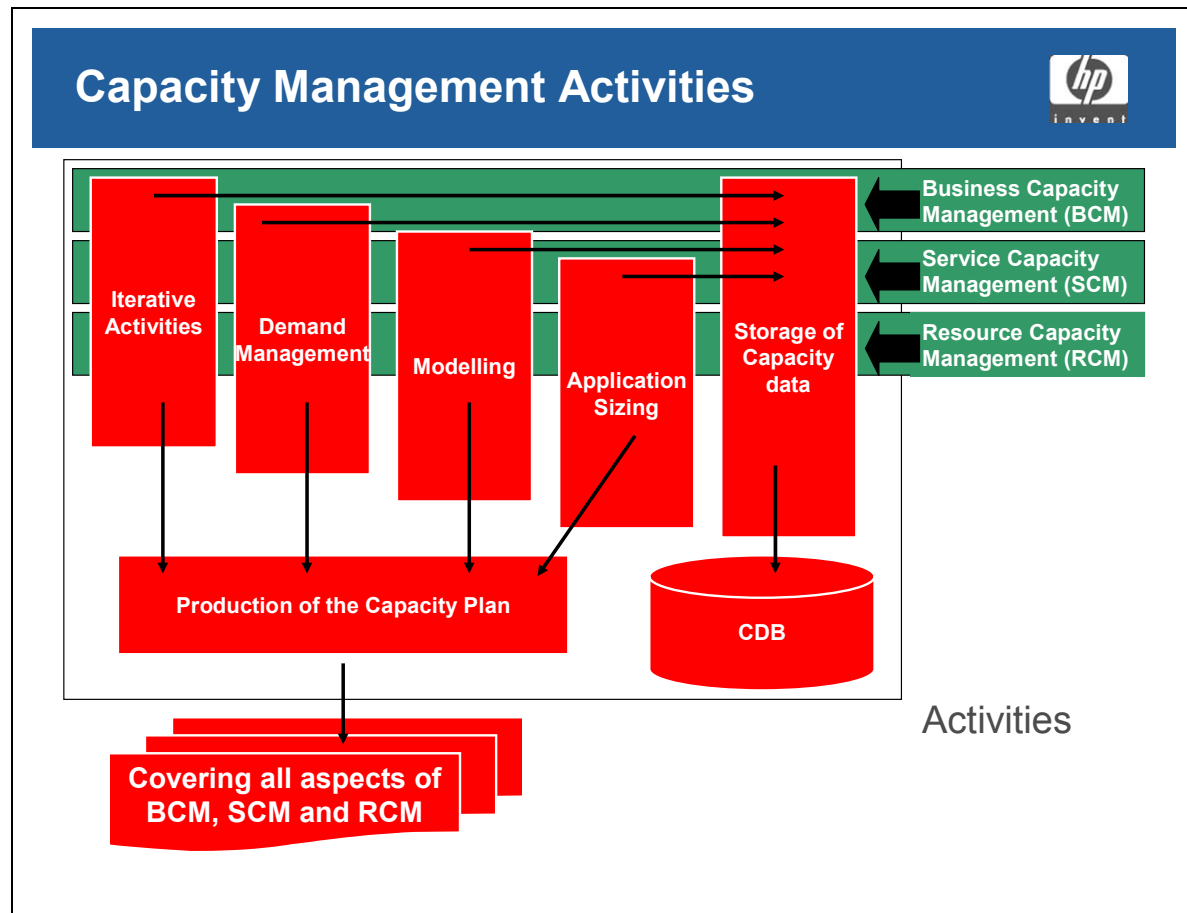
A prime objective of the Resource Capacity Management sub-process is to identify and understand the capacity and utilization of each of the elements (component parts) of the IT infrastructure. The sub-process also maintains awareness of new technologies and developments therein.

The aim of this sub-process is to ensure the optimum use of current hardware and software.

Inputs include:

- Current technology and its utilization
- Future or alternative technology
- Resilience of systems and services

## Capacity Management Activities



### Student Notes

The activities in Capacity Management are carried out as follows:

Iterative activities	ongoing
Demand Management	ongoing
Data storage in the CDB	ongoing
Application sizing	ad hoc
Modeling	ad hoc
Production of the Capacity Plan	regularly

## Iterative Activities

### Iterative Activities



- Also called “Performance Management”
- Focus on meeting agreed service levels
- Ensure optimum performance of resources
- Learn to prevent problems
- Main activities:
  - Monitor
  - Analyze
  - Identify tuning measures
  - Implement tuning measures

## Student Notes

In ITIL v2 the term “**Iterative Activities**” is also used for Performance Management.

Performance Management is the day-to-day management of IT systems to ensure that they are performing optimally and to prevent any performance problems. It also ensures that systems are able to support the levels of performance required to meet the SLAs.

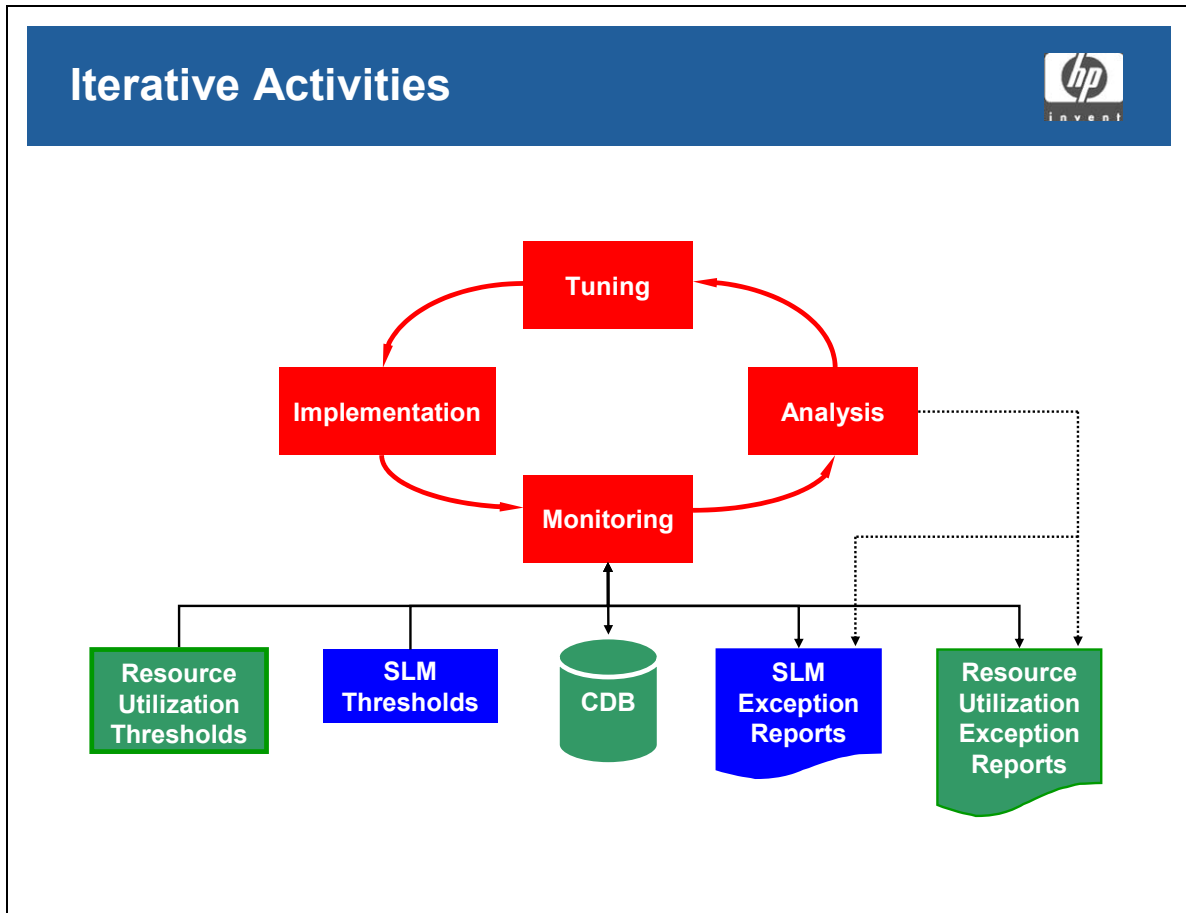
There are four major activities in Performance Management:

- **Monitoring** is aimed at ensuring that resources and services perform as required to meet the terms of the SLAs. It includes items regarding capacity (e.g. throughput) and performance (e.g. response time). Monitoring is performed on the basis of thresholds set by technical specifications and Service Level Management.
- **Analysis** is used to identify trends of utilization and service level so that a normal or baseline can be determined. Regular monitoring and comparison with this baseline can identify exception conditions or near misses in the SLAs. Analysis can be used to predict future resource usage, or to monitor actual growth against predicted growth.

**Module 10**  
**Capacity Management**

- **Tuning** is used to identify measures to improve either utilization or performance levels for a specific device or service.
- **Implementation** of the tuning measures must be conducted through Change Management to minimize disruption and reduce negative impact on the service.

## Iterative Activities



## Student Notes

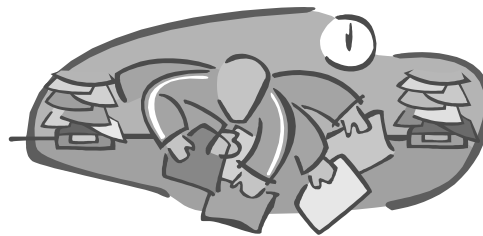
Note: SLM = Service Level Management

## Demand Management

### Demand Management



- Reactive and Proactive Capacity Management
- Managing demand where capacity is limited
- Resources allocated by business priority



### Student Notes

This is the most reactive part of Capacity Management and its prime objective is to influence the demand for computing resource and the use of that resource.

**In the short term**, Demand Management is used when there has been a partial failure to a component used to provide services.

**In the longer term**, Demand Management is used when an identified upgrade is too expensive or impractical.

In both cases customer demand for IT is managed by assigning resources according to business priority. This is not a popular role, since it imposes regulation and could result in certain services being unavailable at certain times.

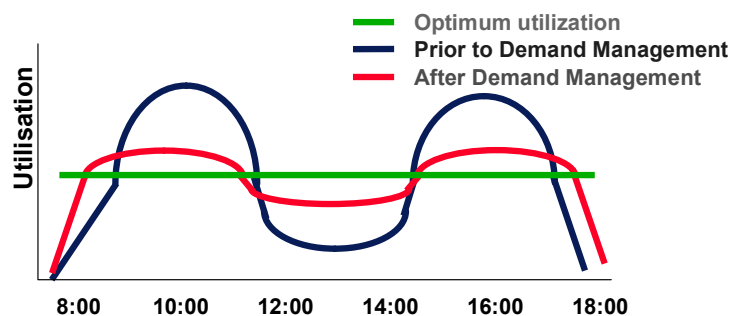
Demand Management is, however, the most cost-effective form of Capacity Management in the shorter term.

## Demand Management

### Demand Management



- Influence user behavior
- Increased or reduced charges for specific resources or times
- May require specific restrictions or concurrency levels



### Student Notes

To better control the workload, the demand for the resources needed can be controlled by a number of processes. Prime among these is to control demand by pricing, differential charging is sometimes used to encourage utilization during off-peak times.

At times of traditionally high demand the cost of the resources is increased, and conversely it is reduced when demand is traditionally low.

To be able to affect this kind of control Demand Management needs to know which services use which resources, to what extent and when. It also needs to know the schedule of activity in the IT infrastructure. Based on this knowledge, Demand Management can assist decisions regarding the potential to influence demand and the means of influencing it.

## The CDB

### The CDB



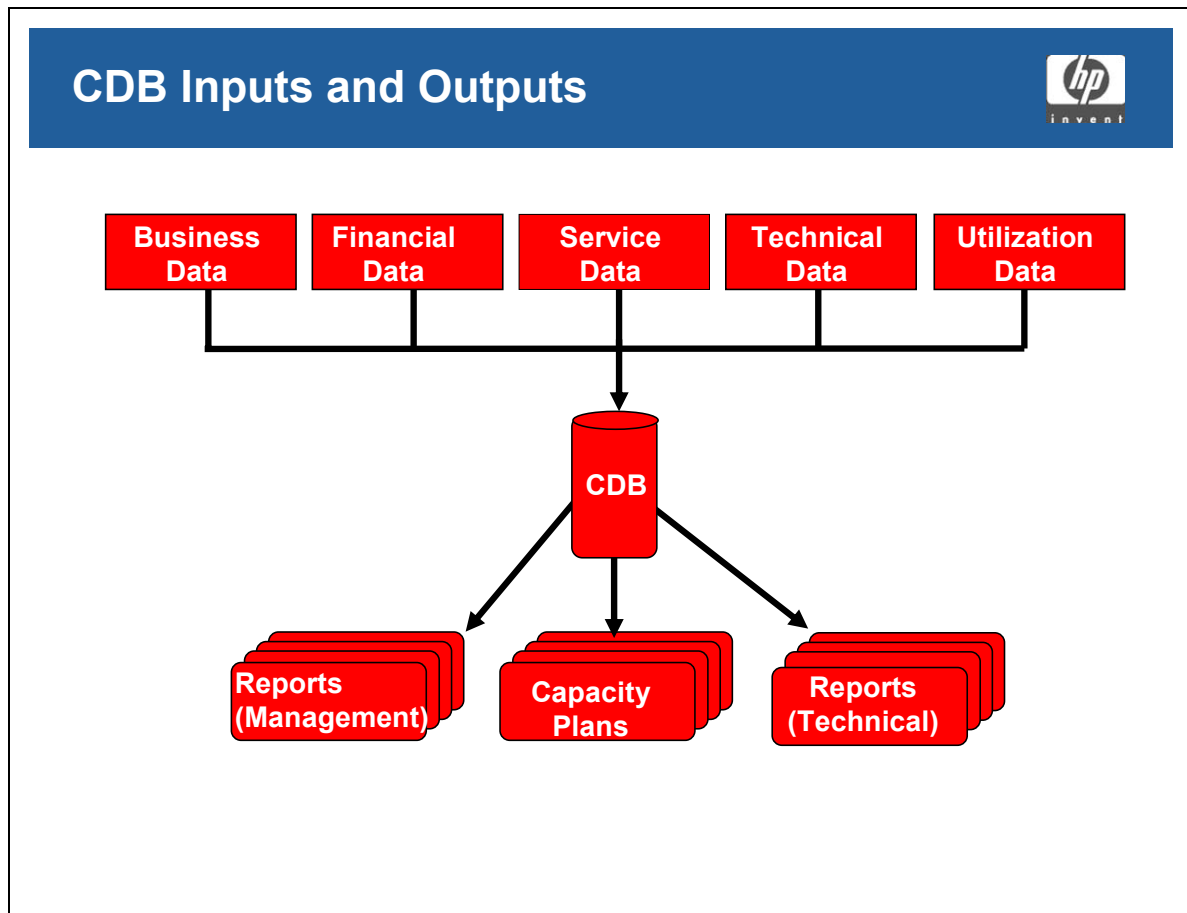
- Data relevant to Capacity Management
  - Technical
  - Business
  - Service
  - Financial
  - Utilization
- Produces technical and management reports
  - Service and Components
  - Exceptions
  - Capacity forecasts
- Part of the CMDB

### Student Notes

All the areas in Capacity Management use this tool. It is conceptually a single database and would form part of the total Configuration Management Database (CMDB) discussed in the Configuration Management section of these notes.



## The CDB Inputs and Outputs



### Student Notes

Inputs to the CDB:

- Business data
- Financial data
- Service data
- Technical data
- Utilization data

The CDB is used to produce:

- Management reports
- Capacity Plans
- Technical reports

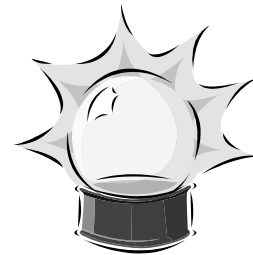
Different platforms require different data and the CDB will consist of a number of data sources.

## Workload Management

### Workload Management



- No longer separate in ITIL v 2
- Still seen as separate by Availability and Financial Management
- Amount of work processed by users
- Forecasts demand on services and systems



### Student Notes

Although this is not listed as a separate activity in the Capacity Management section of ITIL v2, it is often referred to in the Financial Management and Availability Management sections. These notes therefore contain a brief overview of the activity.

The workload of a device or system is the amount of processing or traffic initiated by a user. It excludes system overheads or tasks.

Workload Management identifies and forecasts how this throughput is going to change during the planning period. This provides input to Resource Management and Application Sizing.

The main activities include:

- Defining the actual workloads. These will typically be tasks that the user performs on a regular basis, such as standard transactions or the transmission of a specific document
- Defining and cataloging a workload profile for each workload
- Defining the business activities that initiate each workload

- Trending their past use and using business information to estimate their future use
- Producing a workload forecast

## Application Sizing

### Application Sizing



- For new applications, to predict:
  - Service Level
  - Resources
  - Cost implications
  - Affect on existing applications
- At the beginning and at key points in development projects

### Student Notes

The objective of application sizing is to predict the service level, resource and cost implications of any new application or any major addition to existing applications.

Application Sizing must be done from the early stages of a project, where costing and business impact implications are assessed.

## Modeling

### Modeling



The ability to predict the behavior of the IT infrastructure under any given volume and variety of work

### Student Notes

Modeling enables the Capacity Management team to predict the performance of a specified system under a given volume and variety of work.

Modeling techniques are used to conduct feasibility studies of capacity plans during the planning stages, to optimize capacity and detail the division of capacity on an appropriate basis. Modeling is used to answer “What if?” questions for:

- Specific configurations
- Specific workloads
- Combinations of workloads

## **Module 10**

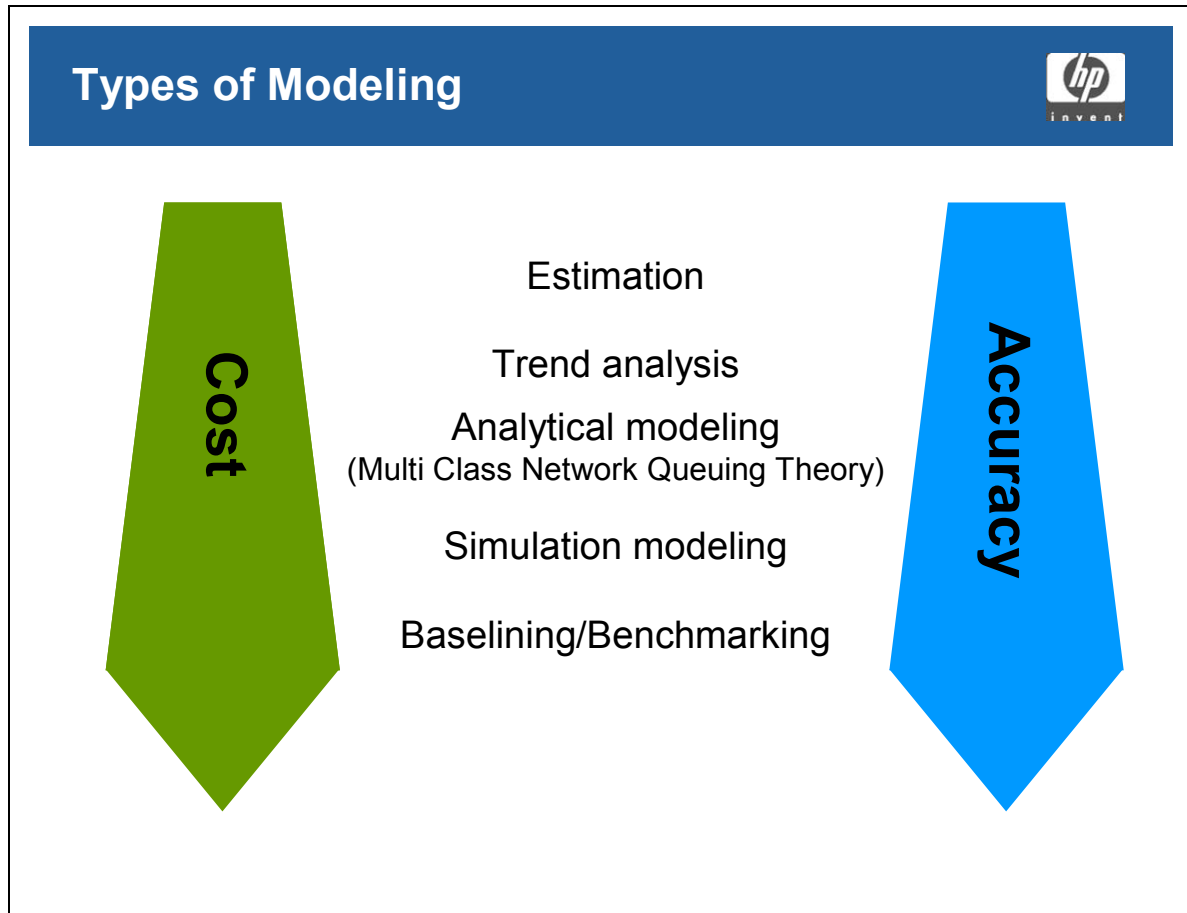
### **Capacity Management**

Modeling is a technique, which is used by all the components of Capacity Management.

The main activities are:

- Define the current performance as a baseline in the model
- Verify the accuracy of the results and tune the model until the results are within an acceptable tolerance
- Predict the outcome of the planned scenarios

## Modeling



### Student Notes

There are five different types of modeling shown here in increasing order of cost and accuracy:

- **Estimation** is a cheap and easy method of predicting performance based on previous experience and current knowledge. It is not accurate enough to be valuable for anything other than small, day-to-day issues.
- **Trend analysis** is done using the resource utilization and performance data, which is measured over time and represented in a graph. These are really only sophisticated estimates, though and cannot be used to determine accurate response times.
- **Analytical Modeling** is done using more sophisticated tools, which are created using mathematical models. These tools are usually designed for specific systems, networks or applications and do not give an end-to-end view of the service. These tools need to be kept up to date, but are usually cheaper and take less time than simulation modeling.
- **Simulation Modeling** is used to model discrete events against a specific configuration. This is usually done in a dedicated environment such as a laboratory. Simulation tools that simulate transactions or network traffic are also available.

**Module 10**  
**Capacity Management**

- **Benchmarking** is an extreme form of simulation modeling where the entire operational environment is replicated or simulated. Workloads are produced to replicate the live environment. The variables are then manipulated or introduced and the actual effect measured.



## Capacity Planning

### Capacity Planning



- Planning capacity requirements:
  - Forecast saturation point
  - Identify action to prevent
- Two year period
- Revised every three months
- Uses scenarios

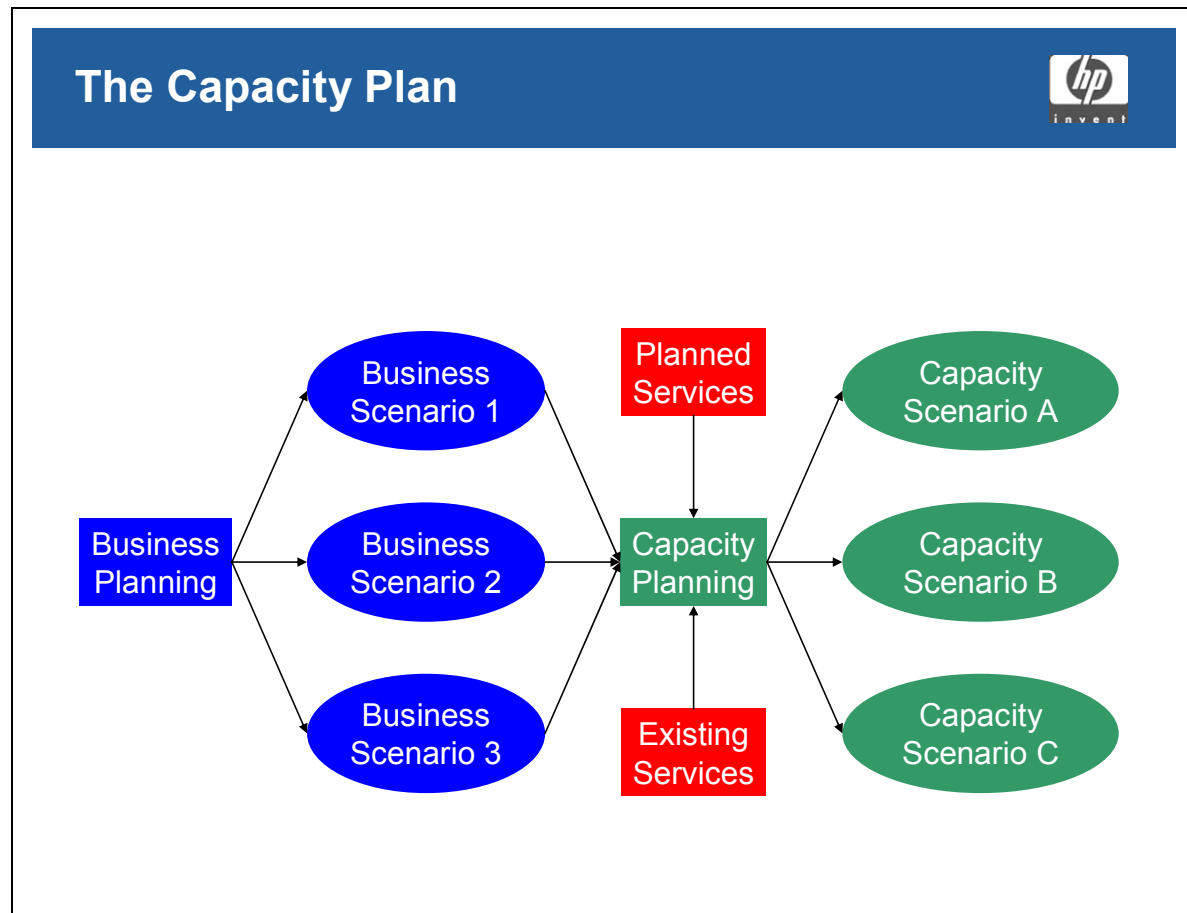
### Student Notes

The Capacity Plan documents the current levels of resource utilization and service performance, and after consideration of the business strategy and plans, forecasts the future requirements for resources to support the IT services that underpin the business activities.

In short, the capacity plan predicts when the system is going to reach saturation point and then identifies what action should be taken to prevent it.

Planning is done for a two-year cycle and is reviewed every 3 months. The planning process uses scenarios to increase accuracy.

## The Capacity Plan



### Student Notes

Using the current workloads as a base, the Capacity Manager will use the input from the business planning scenarios, as well as planned changes and application sizing, to produce a set of capacity planning scenarios.

These are discussed with the business and IT managers and the most likely scenario is selected for the planning period.

Once a scenario has been agreed, the Capacity Management team can begin to model the different alternatives with various ranges of usage levels. This should use the workload forecasts for at least the next 2-year period.

It will normally be sufficient to model each quarter, but it may be necessary to model each month in extreme cases - perhaps where a number of significant changes are likely to occur over a relatively short space of time.

For the selected scenario(s) it will be necessary to calculate and report on expected resource utilization (and proposed upgrades) based upon anticipated workloads.

These should be documented in a draft plan, which should be discussed with senior IT management and, following any necessary amendments, should be published.

## Question

### Information Needed for Capacity Management



In order to carry out effective Capacity Management, which of the following sources of information are required?

1. Financial data
2. Business data
3. Technical data
4. Service data

A. 1 and 2

B. 2 and 4

C. 2, 3, and 4

D. All of them

## Student Notes

## Question

### Capacity Management Benefits



Which of the following statements is *not* true?

1. The true cost of an upgrade cannot be established without effective Capacity Management
2. The likely effect of an upgrade on response times cannot be predicted without Capacity Management
3. Capacity Management ensures that upgrades can be planned before response times suffer.

- |                    |                   |
|--------------------|-------------------|
| A. Only the first  | C. Only the third |
| B. Only the second | D. None of them   |

## Student Notes



---

## **Module 11 — Financial Management**

## Mission of Financial Management

### Mission of Financial Management



To manage IT Infrastructure costs and to provide a sound financial basis for business decisions relating to IT by identifying and accounting for the costs of delivering services, and where appropriate by recovering costs in an equitable manner

### Student Notes

*To manage IT Infrastructure costs and to provide a sound financial basis for business decisions relating to IT by identifying and accounting for the costs of delivering services, and where feasible by recovering costs in an equitable manner.*

To achieve this goal, Financial Management for IT Services should include within its capabilities:

- The ability to account fully for all spend relating to the provision of IT services
- The ability to attribute all spend to specific and general services delivered to individual customers
- The ability to assist management in decision-making on IT investment by providing financial information in support of business cases made.



The services provided by the IT department are usually considered to be critical to the business. Increases in the number of users, coupled with demands for the implementation of new technologies and the growing complexities of the IT systems (e.g. client-server) has caused IT costs to grow faster than other business costs. Consequently, IT services are often viewed as high-cost and/or inflexible.

The complexity of accounting for IT usage often means that it is rare for the actual running costs to be easily and properly identified. This can lead to user dissatisfaction with the perceived 'value for money' of those services.

The answer to many of these sort of charges leveled against IT is often, "We're doing the best that we can with the money that we have!"

The IT department has to understand the true cost of providing their services and manage those costs professionally. This is the only effective way to demonstrate that is doing the best that it can. Thus, IT accounting and budgeting processes are introduced and many organizations also implement processes for charging for the services delivered.

When dealing with accounting matters, organizations are recommended to contact an appropriately qualified accountant.

## Scope of Financial Management

### Scope of Financial Management



- Budgeting (mandatory)
  - Forecasting, control and monitoring of expenditure
- IT Accounting (mandatory)
  - Enables IT to account for where money is spent on running the department and providing services
- Charging (optional)
  - Billing customers for services

### Student Notes

The scope of IT Financial Management is IT budgeting, accounting and charging, although many of the activities involved are often managed by the Financial division within an organization.

#### Budgeting

Forecasting, control and monitoring of expenditure

#### IT Accounting

Enables IT to account for where money is spent on running the department and providing services

#### Charging

Billing customers for services

## Objectives of Financial Management

### Objectives of Financial Management



- To account for running IT
- To facilitate accurate budgeting
- As a basis for business decisions
- Balancing cost, capacity and SLRs
- To recover costs where required (Charging)

### Student Notes

The objectives reflected in this mission statement are:

- To account for the cost of running the IT department and providing IT services
- To facilitate accurate budgeting
- To provide information about the cost of IT services, which will enable the business to make better decisions
- To build a basis for determining the Return on Investment (ROI) of IT
- To create the basis for balancing cost, capacity and service level requirements
- Where required, to build a fair framework for recovering costs (charging)

## Budgeting

### Budgeting



The process of predicting and controlling the spending of money within the enterprise — consists of a periodic negotiation cycle to set budgets, usually annual, and the day-to-day monitoring of the current budgets.

### Student Notes

**Budgeting** is the process of predicting and controlling how money is spent, and consists of a periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of current budgets. Budgeting in IT forms part of the overall budgeting cycle set by the business.

The final budget agreed for an IT department may include financial disciplines imposed by the enterprise, including:

- Limits on capital expenditure
- Limits on operational expenditure
- Limits on variance between actual and predicted spend
- Guidelines on how the budget must be used
- An agreed workload and set of services to be delivered.
- Limits on expenditure outside the organization
- Agreements on how to cope with exceptions

Budgets are set by forecasting the costs of specific categories of expenditure. Where these are not known, they are estimated according to business forecasts, Capacity Management forecasts and Service Level Management.

## IT Accounting

### IT Accounting



The set of processes that enable the IT organization to fully account for the way its money is spent, particularly the ability to identify costs by customer, by service or by activity. It usually involves ledgers and should be overseen by someone trained in accountancy.

### Student Notes

**IT Accounting** is the set of processes that enable the IT organization to fully account for the way its money is spent. It usually involves ledgers and should be overseen by someone trained in accountancy.

An accounting system is a set of interrelated activities, policies and tools, which is used to budget, track and charge for IT services. The aims of the system are to:

- Track actual costs against budget
- Support the development of a sound investment strategy
- Provide cost targets for performance and service delivery
- Prioritize resource usage
- Make day-to-day decisions with full understanding of the cost implications and hence the minimum of risk
- Support the introduction, if required, of charging for IT service

## Major Cost Types and Cost Elements of Financial Management

### Cost Elements



Major type	Cost Elements
Hardware	Servers, storage, workstations, laptops, PDAs, printers, networks
Software	Operating systems, applications software, utilities
People	Recruitment, employment costs, benefits, cars, relocation costs, expenses, training
Accommodation	Offices, power, lighting, water, storage, secure areas
Transfer	Internal charges from other cost centres within the organisation
External Services	Security services, IT Service Continuity services, outsourcing services

### Student Notes

Cost types are categories that make it easier to identify where money is being spent or where it is going to be spent. Cost Elements are subcategories within the high level Cost Types.

## The IT Accounting System — Cost Models

### The IT Accounting System — Cost Models



- Cost Classification
  - Capital and Operational (Revenue expenditure)
  - Direct and Indirect (absorbed and unabsorbed overheads)
  - Fixed and variable
  - Depreciation
- Cost Units
- Cost Centers
- Monitoring

### Student Notes

A cost model is a framework in which all known costs are identified and allocated to specific customers or services. The first step in defining a cost model is to categorize how the costs are actually incurred; the cost types and elements discussed earlier are the first part of this categorization. The next step is to classify them.

#### Cost Classification

Within each Cost Element there are different types of cost that will behave in different ways. There are 7 broad categories:

- Capital — For an accountant's definition of 'capital costs', please refer to a qualified accountant. For the purposes of this Workbook, 'capital costs' can be taken generally to include:
  - computer equipment
  - building and plant
  - software packages



- Operational (Revenue expenditure) — For an accountant's definition of 'revenue costs', please refer to a qualified accountant. For the purposes of this Workbook, 'revenue costs' can be taken generally to include:
  - staff costs;
  - maintenance of computer hardware and software
  - consultancy services, rental fees for equipment
  - software license fees
  - accommodation costs
  - administration expenditures
  - electricity, water, gas, rates
  - disaster recovery
  - consumables
- Direct— Those costs that are clearly attributable to a single Customer, e.g. Manufacturing systems used only by the Manufacturing division
- Indirect — Those costs that are incurred on behalf of all, or a number of, Customers e.g. the network or the technical support department, which have to be apportioned to all, or a number of, Customers in a fair manner.

Any Indirect Costs, which cannot be apportioned to a set of Customers (sometimes called Unabsorbed Overheads), have then to be recovered from all Customers in as fair a way as is possible, usually by uplifting the costs calculated so far by a set amount. This ensures that the sum of all of the costs attributed to each Customer still equals the total costs incurred by the IT organization

- Fixed — Costs that do not vary even when resource usage varies are referred to as Fixed Costs (e.g. a maintenance contract for a piece of hardware, or a corporate software license).
- Variable — Variable Costs are those that vary with some factor, such as usage or time. They are likely to be used for cost elements which cannot be easily predicted (eg. out-of-hours cover, major equipment re-location, and the production of additional quarterly reports).
- Depreciation — This is an accounting entry, which allows the organization to reduce the value of assets based on the time they have been in use, or their amount of usage.

## **Cost Units**

A cost unit is the basic unit of service that a customer will use or be charged for. Cost units need to be items that can easily be measured or seen by the customer.

The different types of cost will be calculated and allocated or apportioned to cost units. A simple calculation will include the following steps:

- Identify the direct costs of the service
- Apportion the indirect costs
- Add the two figures together
- Divide by the projected number times that service will be used (e.g. number of transactions)
- Add any variable cost

## **Cost Centers**

There are 3 types of accounting organization in ITIL:

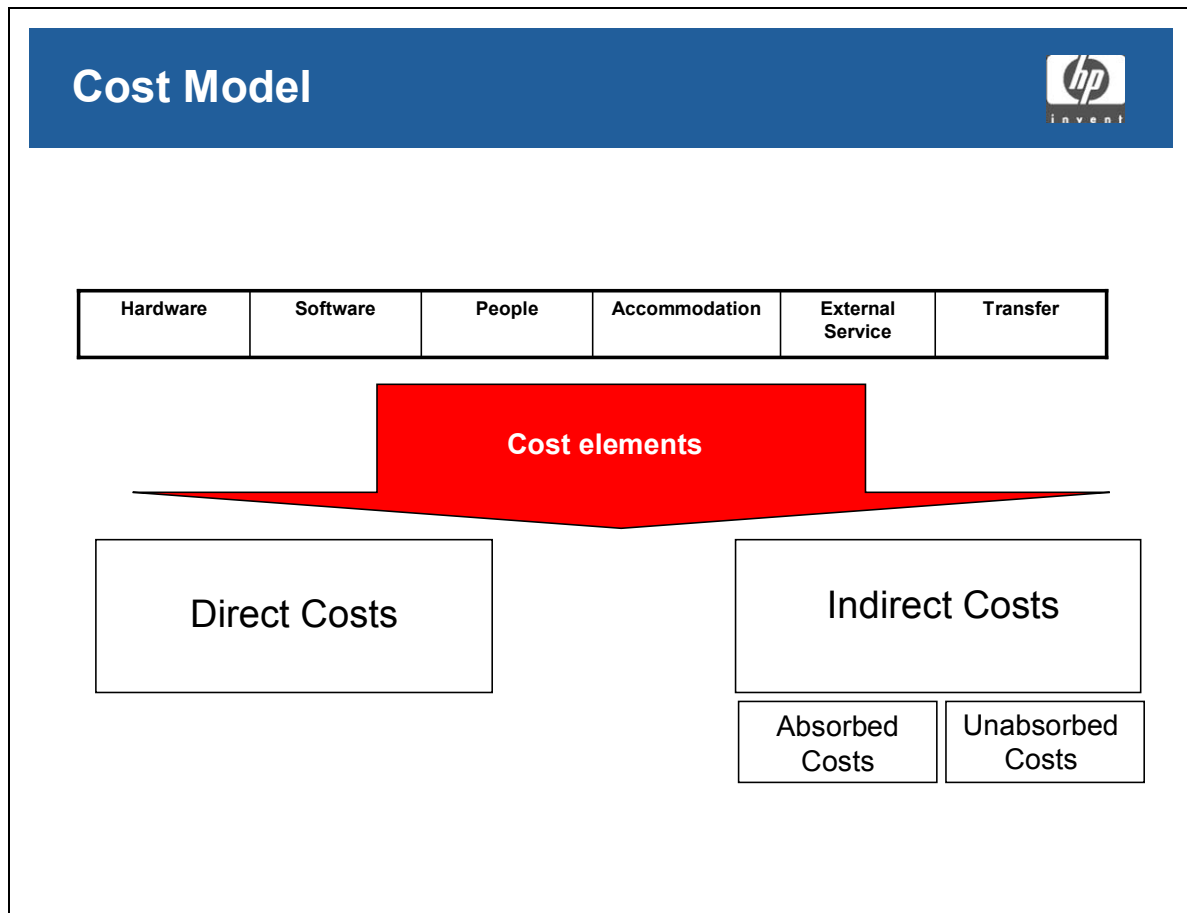
- Accounting Center — This type of organization simply identifies the costs of providing service, and may do some budgeting. The focus is on measuring performance and conducting investment assessment.
- Recovery Center — This is where the organization analyses its full expenditure and investments so that they can be recovered from the customers – usually in some form of charging. The main focus is on making customers aware of the true costs of using services.
- Profit Center — This is where the IT department acts as a business in its own right, although its objectives are set by the organization as a whole. This does not always imply that the department has to make a profit.

## **Monitoring**

All identified costs and cost units must be continuously measured to detect variance, which could cause deviations in budget or charges.

Where necessary recalculation should be done and budgets and charges re-aligned

## Cost Model



## Student Notes

## Investment Appraisal

### Investment Appraisal



Evaluation of the financial benefits of alternative IT solutions

- Return on Investment (ROI)
- Return on Capital Employed (ROCE)
- Total Cost of Ownership (TCO)

### Student Notes

Investment Appraisal is the process of determining whether the business will benefit from changes to IT service quantity and quality. Systematic appraisal entails:

- Being clear about objectives
- Thinking about different ways of meeting them
- Estimating and presenting the costs and benefits of each potentially worthwhile option

There are several types of IA, including:

- Return on Investment (ROI), which calculates the effect of an investment on the organization's profitability.

$$\text{ROI} = \frac{\text{Average increase in Profits}}{\text{Investment}}$$

- Return on Capital Employed (ROCE), a commonly used ratio used by analysts to determine how effective an organization is.

$$\text{ROCE} = \frac{\text{Net Profit Before Interest and Tax}}{\text{Total Assets - Liabilities}}$$

- Total Cost of Ownership (TCO), devised by the Gartner Group, which consolidates all of the investments and expenses for specific CIs throughout its lifecycle into one investment amount.

## Charging

### Charging



The set of processes required to bill a customer for the services supplied to them. To achieve this requires good IT Accounting, to a level of detail determined by the requirements of the analysis, billing and reporting processes.

### Student Notes

**Charging** is the set of processes required to bill Customers for the services supplied to them. To achieve this requires that sound IT Accounting processes are implemented, to a level of detail determined by the requirements of the analysis, billing and reporting processes.

Its main aims are to:

- Determine the most suitable Charging policies for an organization
- Recover fairly and accurately, the agreed costs of providing IT services
- Shape customer behavior to ensure optimal return on IT investment by the enterprise

## When Do You Charge?

### When Do You Charge?



- Budgetary control by users
- Charging exists for other resources
- Freedom of Choice
- Commercial flexibility
- Adequate monitoring capabilities

### Student Notes

ITIL suggests the ideal charging environment is where:

- Budgetary control by users exists
- Charging exists for other resources
- Freedom of choice
- Commercial flexibility
- There are adequate monitoring capabilities

## Benefits of Charging

### Benefits of Charging



- Improved cost consciousness
- Better utilization of resources
- Allows comparisons
- Demand management
- Recover IT costs in an equitable manner, according to IT demands
- Allowing users to influence usage/charges
- Raise revenue

### Student Notes

- Improved cost consciousness
- Better utilization of resources
- Allows comparisons
- Demand management (differential charging)
- Recover IT costs in an equitable manner according to IT demands
- Allowing users to influence usage/charges
- Raise revenue



## Problems of Charging

### Problems of Charging



- Cost of implementing and running charging system
- Allocation of running costs to customers
- Negative reaction to IT costs and charges due to increased visibility
- Perception of poor value for money
- Failure to differentiate between internal and external money
- Failure to make equivalent comparisons

### Student Notes

- Cost of implementing and running charging system
- Allocation of running costs to customers
- Negative reaction to IT costs and charges due to increased visibility
- Perception of poor value for money
- Failure to differentiate between internal and external money
- Failure to make equivalent comparisons

## Charging and Pricing Policies

### Charging and Pricing Policies



- Determine Charging Policy
- Chargeable Items
- Pricing Policy
- Pricing Methods:
  - Cost
  - Cost Plus
  - Going Rate (Internal)
  - Market Rate (External)
  - Fixed Price

### Student Notes

#### Determine Charging Policy

The type and configuration of a charging system will be determined by four main factors:

- Level of recovery required
- The need to influence user behavior
- Ability to measure usage
- Level of control of the internal market

#### Chargeable Items

This is the process of identifying exactly what the customers will be charged for. The user should see these items as a unit. Both fixed and variable costs should be identified for each Chargeable Item.

## Pricing Policy

This is the process of identifying exactly how much money the Charging process should recover.

Since the level of pricing has a direct impact on the demand for the service, these factors should be taken into account:

- What is the pricing objective?
- What is the true demand for the service?
- Accurate determination of direct and indirect costs
- The level of control of the internal market
- What services are available externally if customers have a choice
- What are the legal, regulatory and tax issues
- Are the customers “tied” or “untied”?

In many IT organizations, Customers are “tied” to using the internal IT Services. In an “untied” situation charging becomes particularly important because it enables Customers to choose between using the in-house IT Services organization or outside suppliers, based on the relative quality and price of services offered

## Pricing Methods

Cost

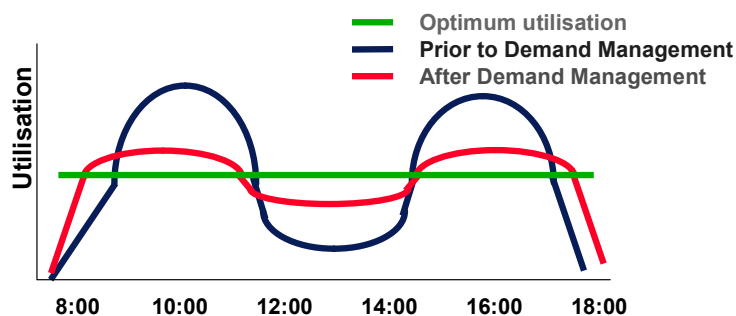
Cost-plus	The mark-up could be set as a fixed percentage or as a target return on investment
Going rate	This is where the cost is similar to other internal departments or to similar organizations
Market price	This is the price quoted by an external supplier, which could be lower than the internal IT department because of economies of scale
Fixed price	IT and the customers agree on a price for the planning period, regardless of the cost.

## Differential Charging

### Differential Charging



- Setting different charges during specific periods
  - For example applying higher charges at peak times, lower charges off-peak
- Used to influence demand



### Student Notes

Charging business customers different rates during specific periods for the same work, typically to dampen demand or to generate revenue for spare capacity. This can also be used to encourage off-peak or night time running e.g. applying higher charges during peak times and lower charges off-peak.

## Billing

### Billing



Bills must be:

- Simple
- Understandable
- Justifiable

Options:

- Information only
- Notional
- Full/Hard charging

## Student Notes

Billing is the process of producing an invoice and recovering the funds from the customer. Billing cycles must be aligned to the business financial cycles to ensure that there is no negative impact on cash flow.

There are three objectives billing:

- Bills must be simple, clear and matched to the ability to pay
- Chargeable Items must be understood by the user
- IT accounting data must be available to back up the bills

## Module 11

### Financial Management

There are three basic types of billing identified in ITIL:

- Information only — The total cost of providing a service are calculated and circulated to the customer but no actual charging takes place
- Notional charging — In addition to the total cost, the bill contains itemized details about how the costs would be charged, but no actual cost recovery takes place based on the bills
- Full or hard charging — Payment takes place as a result of the bill—

Notional charging is often used when introducing charging, to get users used to the idea that services are not “free”. It should not be used for longer terms, since the value reduces if no money changes hands.

## Question

### Financial Management Objectives



Which of the following is *not* an objective of the Financial Management process?

- A. To influence user behavior by providing incentives to use resources at off-peak times
- B. To make users aware of the cost of IT services
- C. To provide the correct level of IT resources to support existing and new applications
- D. To motivate the IT department to provide an economical service

## Student Notes

## Question

### When to Set Charging



Consider the following statements:

- It is impractical to introduce an effective charging regime without knowing the true cost of providing IT services
- Charging for IT services is a pre-requisite, or mandatory, for introducing service level agreements

Which is correct?

- |                   |                    |
|-------------------|--------------------|
| A. Only the first | B. Only the second |
| C. Both           | D. Neither         |

## Student Notes



---

## **Module 12 — IT Service Continuity Management**

## Mission of IT Service Continuity Management

### Mission of IT Service Continuity Management



To manage the risks of key IT services failing by avoiding identified risks and by planning to recover key IT services in a contingency, to support the continued functioning of the business to a specified level within a stated set of circumstances

### Student Notes


~~To manage the risks of key IT services failing by reducing and avoiding identified risks and by planning to recover key IT services in a contingency, to support the continued functioning of the business to a specified level within a stated set of circumstances.~~

The goal of IT Service Continuity Management (ITSCM) is to ensure that the required IT technical and services facilities can be recovered within required and agreed timescales. IT Service Continuity Planning is a systematic approach to the creation of a plan and procedures — which are regularly tested and updated — to prevent, cope with, and recover from the loss of critical services for extended periods.

## Scope of IT Service Continuity Management

### Scope of IT Service Continuity Management



- IT services that support critical business processes
- Identifying and minimizing impact
- Agree the minimum level of business operation following a service disruption 
- Does not directly cover longer-term risks
- Does not cover minor disruptions and faults

### Student Notes

ITSCM focuses on all IT services that are needed to keep critical business processes functioning. It is also responsible for identifying and minimizing any impact on those business processes.

ITSCM should agree the minimum level of business operation following a service disruption.

ITSCM does not directly cover longer-term risks such as those from changes in business direction, restructuring, etc. It also does not cover risks of minor disruptions and faults.

## Objectives of IT Service Continuity Management

### Objectives of IT Service Continuity Management



- Reduce the vulnerability of the organization
- Reduce identified risks
- Plan for recovery of business processes
- To involve 3<sup>rd</sup> parties to mitigate risk
- Reduce the threat of potential disasters
- To prevent loss of Investor confidence

### Student Notes

- To reduce the vulnerability of the organization by maintaining or preserving IT services
- To reduce or avoid identified risks
- To plan for the recovery of key IT services that support critical business processes
- To transfer all or part of the risk to a third party (e.g. insurance or outsourcing)
- To reduce the impact of potential disasters
- To prevent the organization from losing investor confidence

## Business and IT Responsibilities

Business and IT Responsibilities	
<b>Business</b>	<b>IT</b>
<ul style="list-style-type: none"><li>• Business Processes</li><li>• Facilities</li><li>• Business Staff</li><li>• Strategy for Business Continuity</li></ul>	<ul style="list-style-type: none"><li>• IT Services</li><li>• Systems</li><li>• Technical Staff</li><li>• Strategy for IT Continuity</li></ul>

### Student Notes

The dependencies between business processes and technology are now so inter-twined that Business Continuity Management (BCM) incorporates both a business element (Business Continuity Planning — BCP) and a technology element (IT Service Continuity Management Planning — ITSCM). Their dependencies on each other determine that one is a sub-set of the other, depending on the nature of the business and the extent to which technology has pervaded the organization. Therefore it is often understood that business continuity is the main driver and that IT Service Continuity Management is a sub-set of the Business Continuity Management process.

### Business Responsibilities

The Business is responsible for managing business continuity risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur as a result of a risk.

Business Continuity Management is concerned with the management of Business Continuity that incorporates all services upon which the business depends, one of which is IT.

## **Module 12**

### **IT Service Continuity Management**

The minimum business requirements must be determined and agreed between the business and the IT service providers (internal or external) prior to the definition of the scope of ITSCM. It is vital that the prerequisites for recovering services are fully understood, defined and agreed by the business.

- Business Processes
- Facilities
- Business Staff
- Strategy for Business Continuity

## **IT**

ITSCM is a part of the overall Business Continuity Management process and is dependent upon information derived through this process.

The purpose of IT Service Continuity Management is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required, and agreed, business timescales.

- IT Services
- Systems
- Technical Staff
- Strategy for IT Continuity

## Possible Risks

### Possible Risks



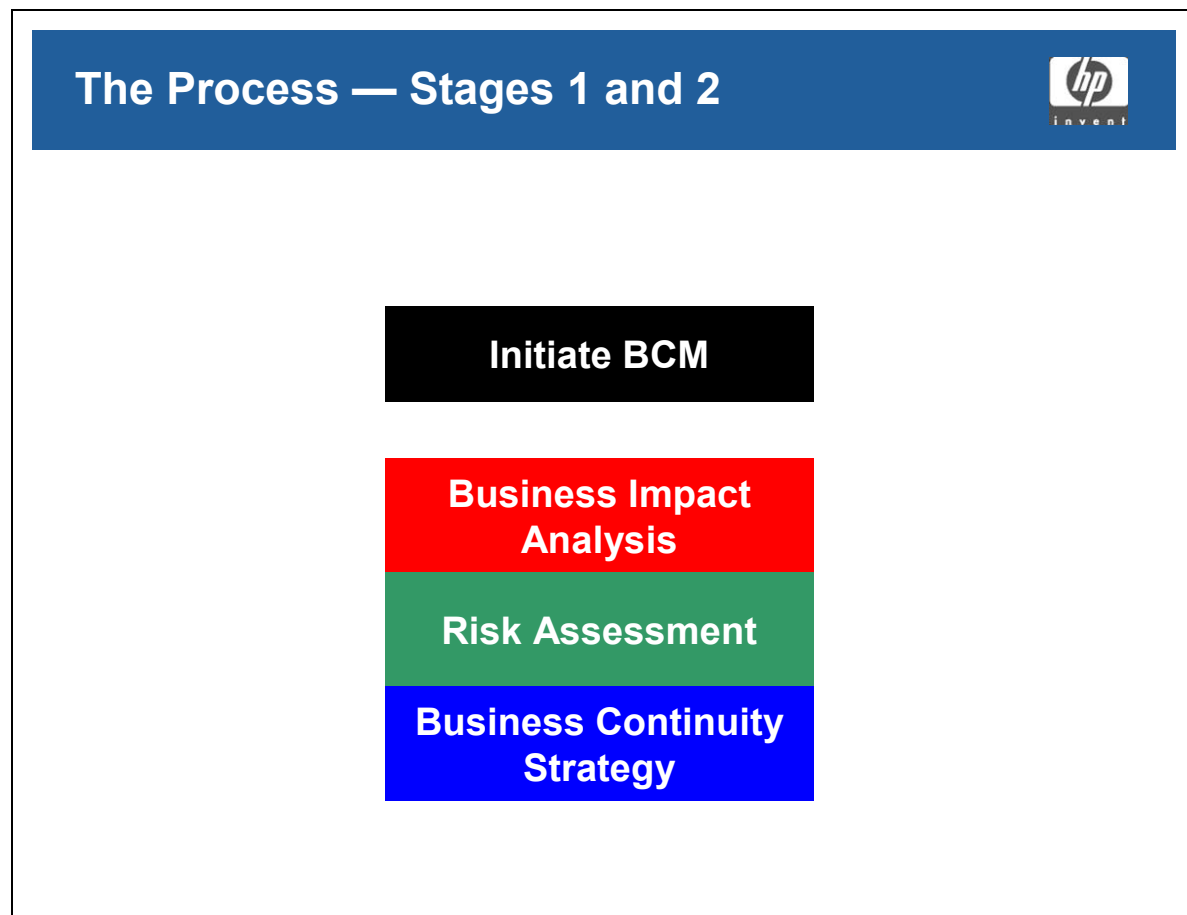
- Damage and denial of access
- Loss of critical support services
- Failure of critical suppliers
- Human error
- Technical error
- Fraud, sabotage, extortion, espionage
- Viruses or other security breaches
- Industrial action
- Natural disasters

## Student Notes

The risks to be addressed are those that could result in a sudden and serious disruption to the business:

- Damage or denial of access to premises (terrorism, fire, flood or other physical disasters)
- Loss of critical support services such as telecomm and power
- Failure or non-performance of critical suppliers
- Human error
- Technical error or environmental unit breakdown
- Fraud, sabotage, extortion or commercial espionage
- Infiltration of IT systems by viruses
- Other security breaches
- Industrial action or other unavailability of key staff

## The Process — Stages 1 and 2



### Student Notes

Note that Stage 1, Initiate BCM, is a joint project between the Business and IT.



## Business Impact Analysis

### Business Impact Analysis



Purpose:

- Identify key IT services
- Determine the effect of unavailability
- Investigate the time before the effects are felt
- Assess minimum recovery requirements
- Document with the business

Impact scenarios

### Student Notes

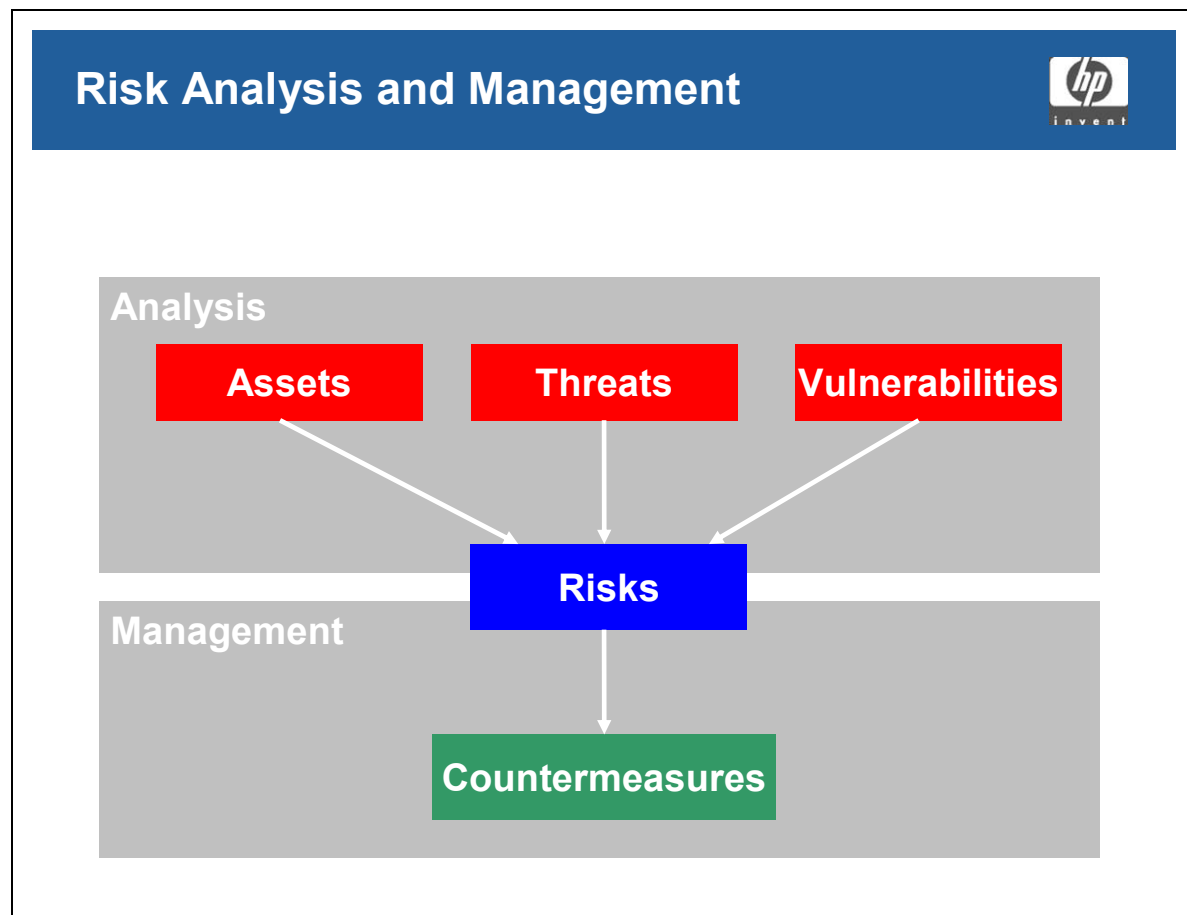
The **purpose** of a business impact analysis is to identify:

- Which IT services support critical business processes
- The damage or loss for the organization if they were unavailable
- The time before those impacts would be felt

This is done using **impact scenarios**, which identify different combinations of service unavailability, and assess the effect of each on the business. This also helps to identify:

- The form that the damage or loss may take
- How the damage or loss could escalate after an incident
- The minimum staffing, facilities and services necessary for business processes to operate at a minimum acceptable level
- The time within which these should be recovered
- The time within which business processes and all supporting staff, facilities and services should be fully recovered

## Risk Analysis and Management



### Student Notes

ITSCM can now assess just how likely it is that a disaster (or partial disaster) could affect the critical services. This can be done using a tool or methodology such as CRAMM (the CCTA's Risk Analysis and Management Method) to take the following steps.

- Identify the assets that support the key IT services
- Assess the threat
- Assess the vulnerability
- Assess the probability of the risk

### Definitions

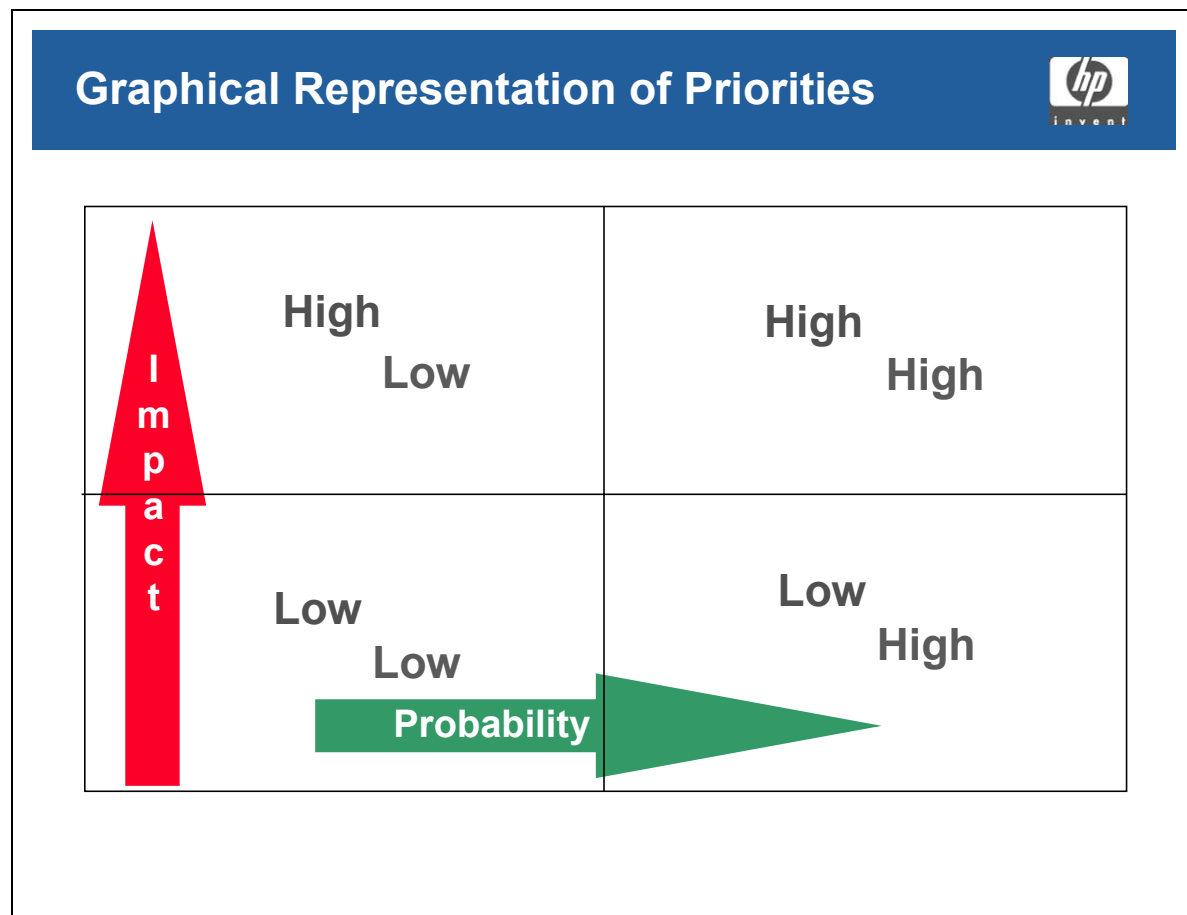
**Risk** - A measure of the exposure to which an organisation may be subjected. This is a combination of the likelihood of a business disruption occurring and the possible loss that may result from such business disruption.

**Threat** - The possible causes of disruption that might prevent the delivery of services. Threats act upon the assets of an organization or service.

**Vulnerability** - A weakness of a service and its constituent CIs(assets) which could be exploited by threats.

**Countermeasure** - An action taken to reduce risk. It may reduce the 'value' of the asset, the threats facing the asset or the vulnerability of that asset to those threats.

## Graphical Representation of Priorities



### Student Notes

Using an approach like CRAMM requires confidence that:

- All risks and countermeasures have been identified
- All threats and vulnerabilities have been identified and their levels accurately assessed
- All results are consistent across the broad spectrum of the IT infrastructure reviewed
- All expenditure on selected countermeasures can be justified

## Service Continuity Strategy

### Service Continuity Strategy



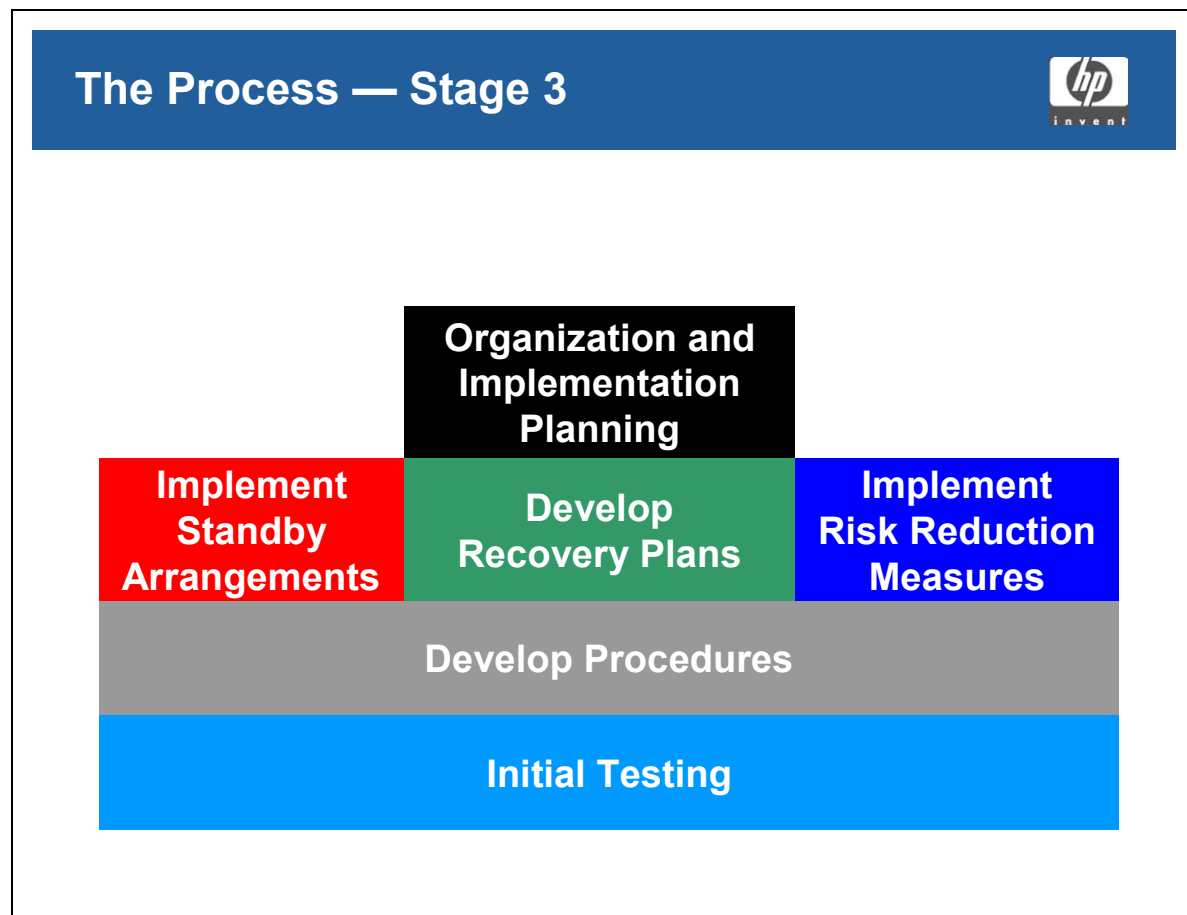
- Which services will we plan for?
- What recovery and preventative options are available?
- What are the costs of each?
- Which services take priority in recovery?

### Student Notes

The strategy will outline:

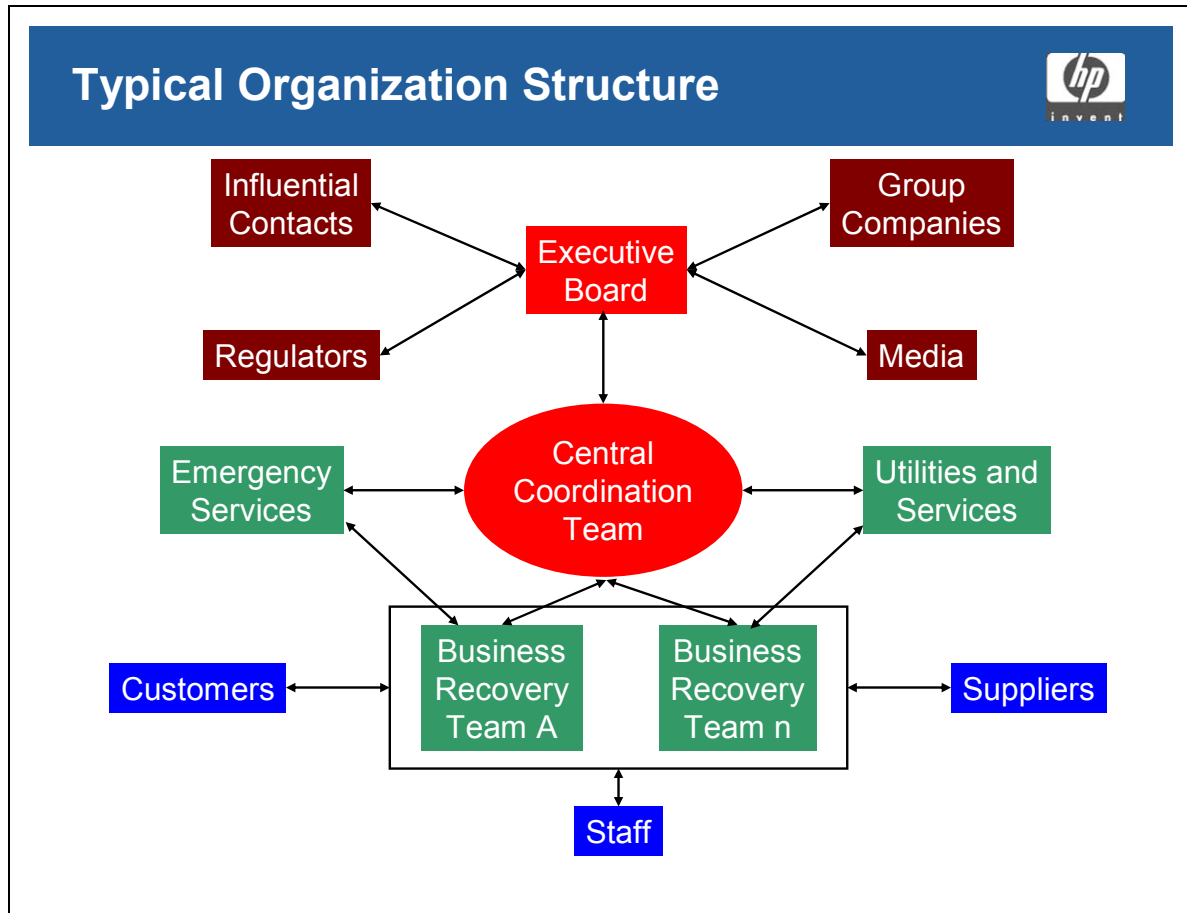
- The services to be included in the Continuity Plan
- What recovery and prevention alternatives will be chosen for each
- The costs of the alternatives
- The priorities for recovery

## The Process — Stage 3



## Student Notes

## Typical Organization Structure



### Student Notes

The organization for ITSCM must include:

- **Executive Board:** retain overall authority and control within the organization and will also be responsible for:
  - Crisis management
  - Public relations
  - Liaison with other departments or group companies, the media, regulators, influential contacts, etc.
  - Executive decisions
- **A central coordination team:** consists of people one level below the executive board. They have a good overall understanding of the business processes and priorities, and have operational control over the groups that will invoke stand-by arrangements and recover the business.
  - Overall Recovery Manager, who manages the central coordination team
  - Critical business process or function coordinators
  - Key support function coordinators (including IT)

**Module 12**  
**IT Service Continuity Management**

- Coordinators for any other critical activities
- **Business Recovery teams:** are responsible for implementing the business recovery plans for their own areas and for day-to-day liaison with staff, customers and suppliers. A business recovery team may support each coordinator on the central coordination team.

Please note that the planning process must create the appropriate authority for each team or individual to make decisions and take action during a contingency. This authority must be clearly designated in the continuity plans.



## Standby Arrangements

### Standby Arrangement



#### Options

- Do nothing
- Manual workarounds
- Reciprocal arrangements
- Immediate recovery – hot standby (<24 hrs)
- Intermediate recovery – warm standby (24-72 hrs)
- Gradual recovery – cold standby (>72 hrs)
- Fortress Approach
- Dormant contracts
- Insurance

### Student Notes

The steps involved in implementing stand-by arrangements include:

- Negotiating and agreeing on the terms for third party recovery facilities
- Preparing and equipping the stand-by site
- Purchasing and installing stand-by equipment
- Ensuring that the recovery contractor is covered by Continuity plans

There are a number of options for Recovery Planning. These include:

- **Do Nothing** — for non-critical or transitional services
- **Manual Workarounds** — users do some of the work manually as an interim measure. This usually requires temporary staff. Most business critical applications are difficult to reproduce manually. Also, in many cases, the data has to be available before the work can be done

## Module 12

### IT Service Continuity Management

- **Reciprocal Arrangements** — this is an agreement between organizations to use one another's facilities in a disaster. This may work for batch jobs or storage, is not really feasible in complex and distributed environments. There are also capacity, maintenance and security issues to consider
- **Immediate Recovery (Hot Standby)** — this is **an alternative site**, already running critical systems, to be used when the main site is inaccessible or unusable. The recovery time is usually less than 24 hours and generally within 24 hours. Business critical systems are mirrored on the alternative site.
  - **Internal** — within the organization, although not usually in the same building.
  - **External** — provided by a third party supplier and shared by several customers
  - **Mobile** — specific facilities in a truck, which can be transported to the main or alternative site
- **Intermediate recovery (Warm Standby)** — **this is similar to Immediate Recovery** except that critical systems need to be recovered and run. This usually takes between 24 and 72 hours. There are 3 types of warm standby facility:
  - **Internal:** This is a spare site maintained internal to the organization. It is very expensive, and therefore often used for testing or development. If this is the case, further alternatives may need to be planned
  - **External:** Third parties normally provide these sites for an annual fee, which reduces the cost and shares the risk, but they are often located remotely. Also there is a greater chance of multiple hits. If the site is invoked, there is an additional daily fee, which usually increases the longer it is used. Most commercial sites limit their cover to between 6 and 12 weeks. This is to reduce the risk of multiple hits.
  - **Mobile:** Computer facilities in a truck or trailer, which is driven to an agreed site for a call-out fee. The amount of equipment is limited by the size of the truck. Special licenses may have to be obtained for parking and running the facility
- **Gradual Recovery (Cold Standby)** — an empty facility, with utilities, support staff and telecommunications equipment, that is ready to accommodate new computer equipment. This is used if the new equipment has been delivered but the base site is not ready to receive it. There are two types of cold standby:
  - **Fixed** — usually provided as a remote facility by a third party, or as a permanent site owned or rented and maintained by the organization itself
  - **Portable** — normally a prefabricated building erected at a site predetermined in the contract
- **Fortress Approach** — An approach to IT Service Continuity where the entire IT site is made as disaster-proof as possible
- **Dormant Contracts** — suppliers agree to keep stock of certain items, which will be available at a fixed price through the year.
- **Insurance** — This is an important element, regardless of which option is chosen, but it is not a replacement for proper stand-by options

## The IT Service Continuity Plan

### The IT Service Continuity Plan




- A working document detailing *all* processes and procedures
- Under stringent Change Management
- Detailing individual and team responsibilities
- Off-site storage essential

### Student Notes

- A working document detailing ALL processes and procedures
- Under stringent Change Management
- Detailing individual and team responsibilities
- Off-site storage essential

## Recovery Plans

### Recovery Plans



#### Phases

- Alert Phase
- Invocation and recovery phases
- Return to normal phase

#### Key areas

- Roles and responsibilities
- Action lists
- Reference data

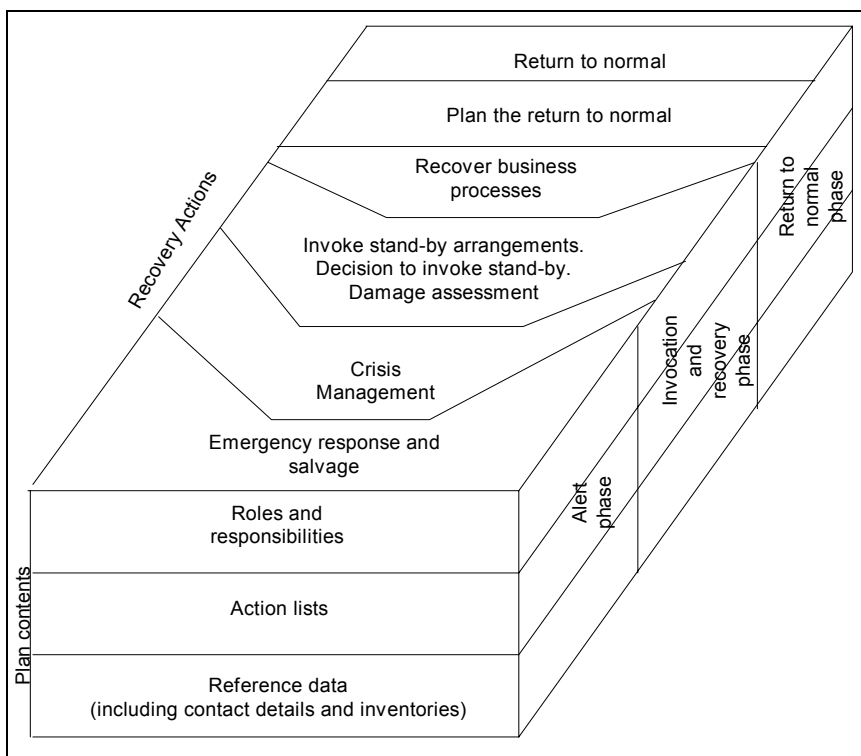
## Student Notes

Recovery Plans must plan for:

- An **Alert phase** during which an incident is reported, an initial damage assessment is completed and a decision is taken on whether or move to the Invocation and Recovery phase
- An **Invocation and Recovery phase** during which stand-by arrangements are invoked and business processes are recovered
- A **Return to normal phase** during which the return to normal is planned, facilities and assets are refurbished, repaired or replaced, and operations are transferred from the stand-by arrangements to permanent arrangements

## Key Areas

- Roles and responsibilities
- Action lists
- Reference data



## Test the Plan

### Test the Plan

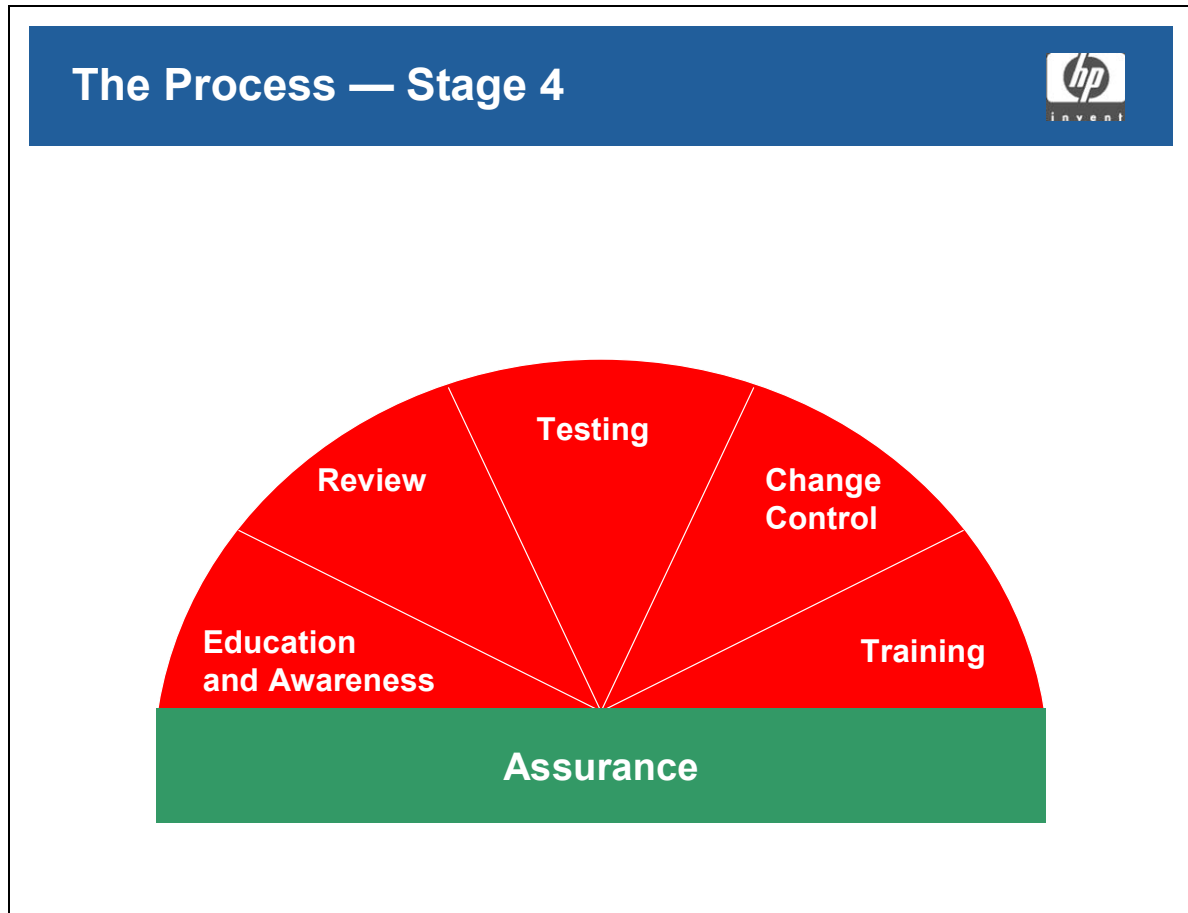


- Sit down and talk through plan – line by line
- Intermediate Recovery
  - Recommended
- Gradual Recovery
  - *Not* recommended
  - Suppliers will *not* generally allow this
- Crisis and scenario testing
- Frequency of testing
  - initially
  - every 6–12 months
  - after every major change to the Plan

## Student Notes

- Sit down and talk through plan — line-by-line
- Intermediate Recovery — Recommended
- Gradual Recovery — *not* recommended — suppliers will *not* generally allow this
- Crisis and scenario testing
- Frequency of testing
  - initially
  - every 6–12 months
  - after every major change to the Plan

## The Process — Stage 4



### Student Notes

#### Education and Awareness

It is important that the business community understands what continuity plans exist for their services and what their role will be in the event of a disaster.

Their expectations must be realistic, and the priority of their specific service must be clearly communicated before any disaster, probably as part of an SLA.

#### Training

The recovery teams must know exactly what to do in a disaster. Having a plan is one thing. Being able to implement it is another.

Training could be done as part of the testing schedule. There should be regular training to ensure that staff are familiar with any changes to the continuity plans.

## **Testing**

Regular testing is needed to:

- Ensure that the continuity plans are workable
- Ensure that the plans are current
- Train IT staff
- Ensure that users understand what will be available

## **Change Management**

Change Management is needed for 2 areas:

- Changes to infrastructure items or services that are covered in the continuity plans
- Changes to the plans themselves

## **Review**

The review will focus on:

- Whether the Service Continuity Management process was followed
- Whether the plans are adequate and scoped correctly
- The results of testing (are the plans workable?)



## Question

### Testing a Continuity Plan



An Intermediate IT Service Continuity plan should be tested:

- A. Regularly, at least every year
- B. Initially, then at least annually and after making any significant changes
- C. As soon as it is completed
- D. Whenever a disaster occurs

## Student Notes

## Question

### Defining an Intermediate Recovery Site

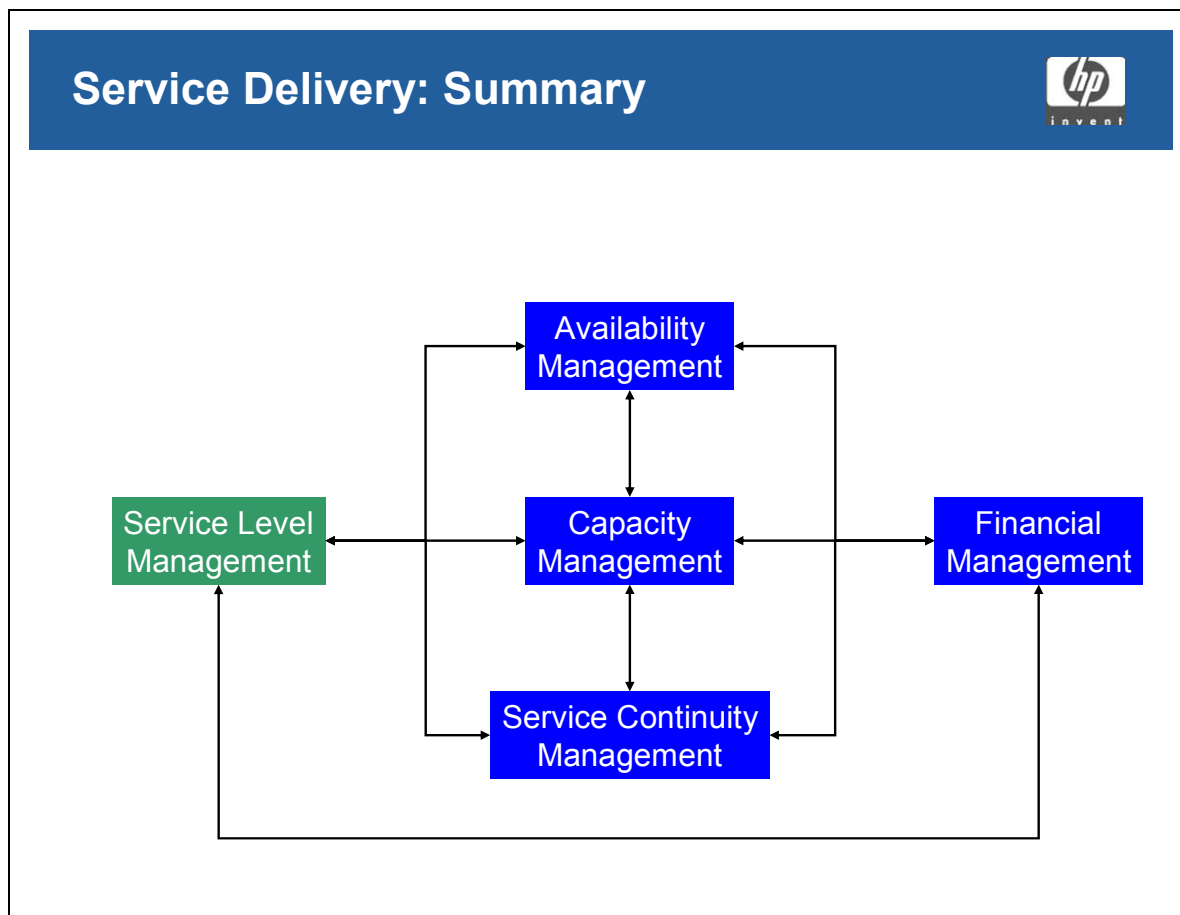


An Intermediate Recovery site provides:

- A. A remote computer *room*, which can be used following a disaster
- B. A back-up computer room, together with replacement computer equipment
- C. Replacement computer equipment which allows immediate recovery without loss of service
- D. A mobile computer *room*

## Student Notes

## Service Delivery: Summary



## Student Notes

## IT is the business.....

IT is the business.....



“IT is the business”  
and  
“The business is IT”

### Student Notes

It is no longer possible to separate The IT department from the process of delivering the "End Product" of the business as the IT is now truly "customer facing" in most organizations. It is also fair to say that the Business cannot ignore or underestimate the importance of IT to its own survival. The relationship is now a true symbiosis where both sides have to work as one to survive and prosper.