



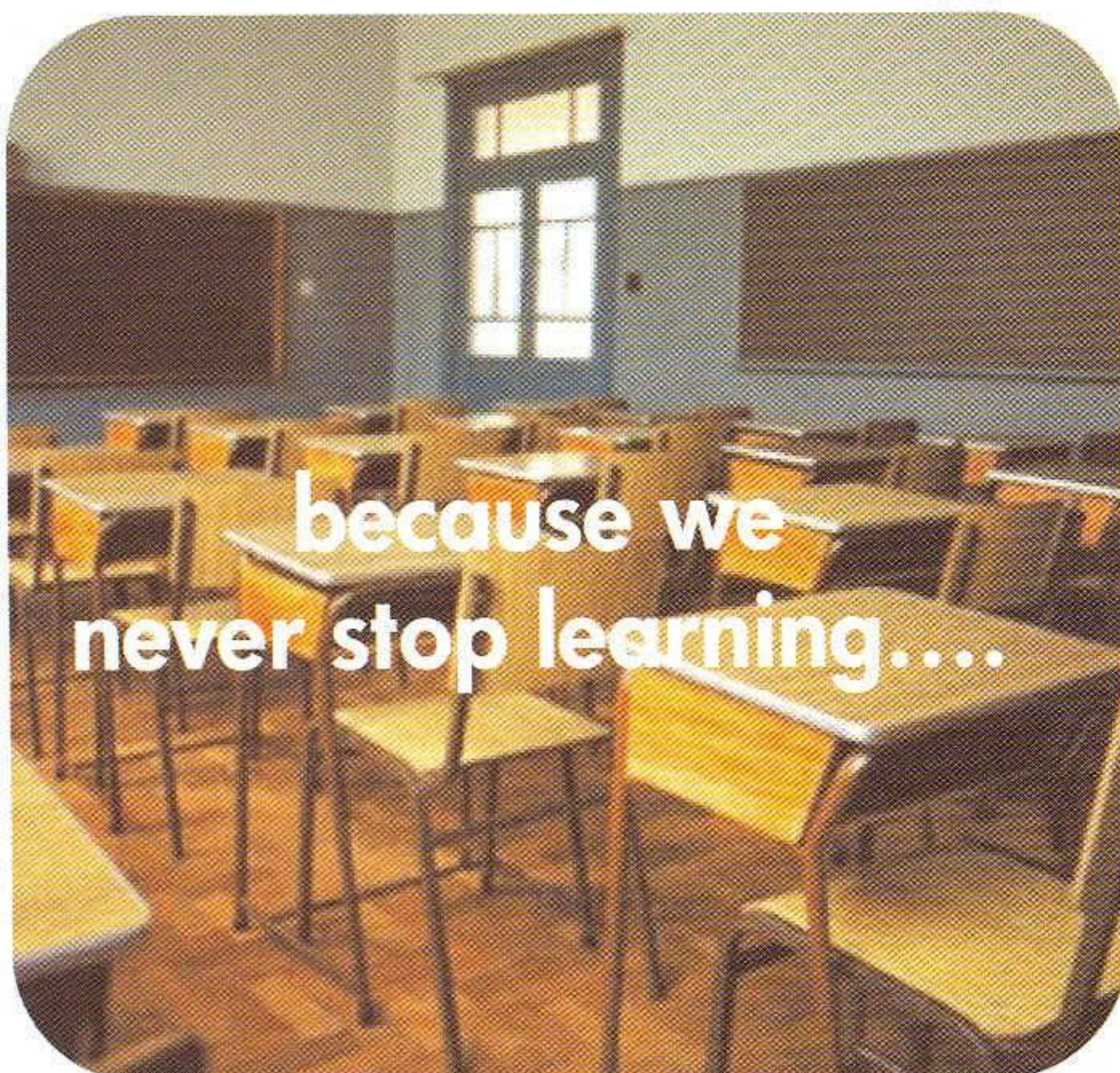
education services
www.education.hp.com

ITIL Essentials for IT Service Management

Student Workbook

Version D.00-1

Course No. H1846S





hp education services
education.hp.com

ITIL Essentials for IT Service Management

Student Workbook

Version D.00 -1
Course no. H18461

Notice

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD PROVIDES THIS MATERIAL "AS IS" AND MAKES NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HEWLETT-PACKARD SHALL NOT BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS IN CONNECTION WITH THE FURNISHING, PERFORMANCE OR USE OF THIS MATERIAL WHETHER BASED ON WARRANTY, CONTRACT, OR OTHER LEGAL THEORY).

Some states do not allow the exclusion of implied warranties or the limitations or exclusion of liability for incidental or consequential damages, so the above limitations and exclusion may not apply to you. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

This document contains proprietary information which is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior consent of Hewlett-Packard Company.

UNIX® UNIX is a registered trademark of the Open Group.

**HP Education Services
Professional Services Organization
100 Mayfield Avenue
Mountain View, CA 94043 U.S.A.**

© Copyright 2001 by the Hewlett-Packard Company and Quint Wellington Redwood

Contents

Overview

Course Description.....	1
Course Goals	1
Student Performance Objectives	1
Student Profile and Prerequisites	2
Curriculum Path.....	2

Module 1 — Introduction to IT Service Management

What Will This Course Give Me?.....	1-4
The Philosophy of IT Service Management	1-6
The Three Ps.....	1-8
Service Management — General.....	1-10
Customer and Users	1-12
Challenges to the IT organization	1-14
The Support Problem	1-16
Why Implement Service Management?	1-18
The Objectives of ITSM.....	1-20
IT Process	1-22
Quality	1-26
ITIL.....	1-28
IT Service Management Courses.....	1-30
Model (According to ITIL)	1-32
HP Reference Model.....	1-34
HP Reference Model.....	1-36
High-level Linkages.....	1-38
HP Reference Model.....	1-40

Module 2 — Configuration Management

Configuration Management	2-2
Configuration Management — Goals	2-4
Configuration Management — Responsibilities	2-6
Configuration Item (CI)	2-8
CIs — Scope and Detail	2-10
Naming and Attributes	2-12
Impact of Relationship	2-14
Status of CIs.....	2-16
Baseline.....	2-18
Assets versus Configuration Management.....	2-20
Essentials	2-22
Management Reporting.....	2-24

Module 3 — Service Desk

Service Desk	3-2
Service Desk — Goals.....	3-4
Service Desk — Responsibilities	3-6
Different Desks	3-8
Inputs and Outputs	3-10
Structures: Local Service Desk	3-12

Contents

Structures: Centralized Service Desk	3-14
Structures: Virtual Service Desk.....	3-16
Considerations.....	3-18
Essentials	3-20
Module 4 — Incident Management	
Incident Management	4-2
Incident Management — Goals	4-4
Incident Management — Responsibilities.....	4-6
Terminology	4-8
The Incident Life Cycle.....	4-10
Classification — Prioritization	4-14
Classification — Categorization	4-16
Classification — Matching	4-18
Routing Incidents	4-20
Escalation and Referral	4-22
Essentials	4-24
Management Reporting	4-26
Module 5 — Problem Management	
Problem Management	5-2
Problem Management — Goals	5-4
Problem Management — Responsibilities	5-6
Terminology	5-8
Problem Control	5-10
Error Control	5-12
Proactive Problem Management (Proactive Prevention).....	5-14
Incidents versus Problems	5-16
Processing Known Errors from the Development Environment	5-18
Reactive — Proactive	5-20
Essentials	5-22
Management Reporting	5-24
Module 6 — Change Management	
Change Management.....	6-2
Change Management — Goal.....	6-4
Change Management — Responsibilities	6-6
Terminology	6-8
Change Management Process.....	6-10
Request for Change (RFC) — Scope.....	6-12
Priority Setting.....	6-14
Impact of a Change	6-16
The Change Advisory Board (CAB)	6-18
Some Relationships.....	6-20
Essentials	6-22
Management Reporting	6-24
Module 7 — Release Management	
Release Management	7-2
Release Management — Goals	7-4
Release Management — Responsibilities.....	7-6
Release and Distribution Process	7-8

Definitive Software Library (DSL).....	7-10
Definitive Hardware Store (DHS).....	7-12
Releases	7-14
Software Roll-out and Distribution.....	7-16
Essentials	7-18
Management Reporting.....	7-20
Module 8 — Capacity Management	
Capacity Management.....	8-2
Capacity Management — Goal.....	8-4
Capacity Management — Responsibilities	8-6
The Capacity Management Process.....	8-10
Sizing and Modeling.....	8-12
Essentials	8-14
Module 9 — Availability Management	
Availability Management.....	9-2
Availability Management — Goals.....	9-4
Availability Management — Responsibilities	9-6
Terminology	9-8
Security	9-10
Risk Analysis	9-14
The Unavailability Life-cycle.....	9-16
When Is a Service Available?.....	9-18
Availability Formula.....	9-20
Essentials	9-22
Module 10 — IT Service Continuity Management	
IT Service Continuity Management	10-2
Continuity Management	10-4
The Process (1)	10-6
Business Impact Analysis	10-8
The Process (2): Operational Management	10-12
The Options	10-14
The Seven Sections of the Plan.....	10-16
Roles in Normal Operation and in a Crisis	10-18
Extensive Testing and Reviewing.....	10-20
Essentials	10-22
Module 11 — Financial Management for IT Services (Cost Management)	
Financial Management	11-2
Financial Management	11-4
Budgeting.....	11-6
IT Accounting.....	11-8
Different Cost Units.....	11-10
Categorization of Cost Units	11-12
Charging.....	11-14
Charging and Pricing Options	11-16
Essentials	11-18

Contents

Module 12 — Service Level Management

Service Level Management.....	12-2
Service Level Management.....	12-4
Service Level Management — Goals.....	12-6
Service Level Management — Responsibilities.....	12-8
Service Level Management Process.....	12-10
Agreements and Contracts.....	12-12
Service Quality Plan.....	12-14
Service Improvement Programme.....	12-16
Elements of a Service Level Agreement.....	12-18
Management Reports.....	12-20
Essentials.....	12-22
Essentials (2).....	12-24

Appendix A — The Milord Group Case Study

Appendix B — General Questions

Appendix C — Glossary by Alphabet

Appendix D — Glossary by Process

Appendix E — Sample Examination

Appendix F — Foundation Certification in IT Service Management

Overview

Course Description

IT Service Management Essentials introduces the concept of IT Service Management (ITSM) and a framework for identifying and interrelating the various activities involved in developing a framework for delivering, measuring, and improving IT services to the user communities. The origins of the course can be found in what is known as the Information Technology Infrastructure Library (ITIL), a set of documents describing best practices in a number of IT service areas, including but not limited to Change Management, Configuration Management, Release Management, Service Desk and Incident Management. ITIL identifies approximately 40 such topics, all of which are mentioned in the introductory portion of this course.

ITIL was first developed in the U.K. with the involvement of numerous industry and government organizations. Its popularity as a driving force behind effective IT management has resulted in the establishment of a certification program. The first level of certification is known as ITIL Foundation Certification, the purpose of which is to establish that an individual has a solid understanding of ITIL and has gained some field experience in implementing one or more ITIL best practices. This course, combined with additional experience, contributes to the students' capacity to achieve ITIL Foundation Certification.

Course Goals:

This course has several important goals:

- Introduce the concepts underlying IT Service Management.
- Introduce the best practices documented in ITIL.
- Understand the roles, processes, and components that are part of certain key ITSM areas: Service Desk, Incident Management, Problem Management, Change Management, Configuration Management, Release Management, IT Service Continuity Management, Availability Management, Capacity Management, Financial Management for IT Services and Service Level Management.
- Be aware of the implications in implementing one or more of the best practices.
- Increase the student's capacity to achieve ITIL Foundation Certification.

Student Performance Objectives

- Understand ITIL's history, purpose, and structure.
- Understand the objectives of the ITIL practices and be able to identify which of those practices could add value if implemented in one's own IT environment.
- Understand the main elements in a reference model diagram.
- Know where to go for additional information.
- Understand options for next steps.

Overview

Student Profile and Prerequisites

Students should have at least some experience with the specification, development, installation, and/or management of information technology. This course will benefit those IT Professionals and Executives who are responsible for the delivery of IT services required by their company or business, such as system and network administrators, IT managers, business analysts, business process specialists, systems analysts, IT architects, and CIO's of small companies.

Curriculum Path

No specific courses are required prior to attending this course. Upon completion of this course, various opportunities are available for the students to participate in additional education that probes more deeply into ITSM topics in an intense lecture/workshop setting.

Module 1 — Introduction to IT Service Management

Many public and private organizations contributed their knowledge and experience, in one form or another, to the development of ITIL. Furthermore, as businesses continually increase their investments in their IT operations, and as the complexity of those operations continues to increase, businesses have been searching for a strong framework that facilitates:

- The descriptions and objectives of the various services in an IT environment.
- A representation of how those services are interrelated.
- Some guidance on implementing those services successfully.

The combination of ITIL, which provides service descriptions and objectives, represents that framework.

Module 1
Introduction to IT Service Management

Welcome to . . .

**ITIL Essentials for
IT Service Management**

Student Notes

What Will This Course Give Me?

The purpose of this course is for students to learn about Service Management and ITIL. It covers the two main areas of Service Management, Service Support and Service Delivery, and their application to the complete service lifecycle.

The topics covered are:

- The 10 key ITIL processes and 1 ITIL Function which go to make up these areas:
 - Configuration Management.
 - Service Desk (a function not a process).
 - Incident Management.
 - Problem Management.
 - Change Management.
 - Release Management.
 - Capacity Management.
 - Availability Management.
 - IT Service Continuity Management.
 - Financial Management for IT Services.
 - Service Level Management.
- The purpose of the different processes, how they relate to one another and clarification of roles and responsibilities in each of them.
- The importance of using a standardized vocabulary to describe Service Management processes.
- An understanding of the relevance of Service Management to the student's own organization.

On completion of the course students will be fully prepared to take the Foundation Certificate in IT Service Management.

— What Will This Course Give Me?

- *Familiarity with the key processes and organizational issues relating to IT Service Management*
- *A standardized vocabulary to describe Service Management processes*
- *An understanding of the relevance of Service Management to your organization*
- *Preparation for the examination — ISEB/EXIN Foundation Certificate in IT Service Management*

Student Notes

The Philosophy of IT Service Management

The advance of technology has meant that businesses these days are totally dependant upon IT. It is essential IT departments recognize that this means the quality, quantity and availability of the infrastructure directly affects the quality, quantity and availability the business is then able to deliver.

The ITIL philosophy adopts a process driven approach which is scaleable to fit both large and small IT organizations. It considers IT Service Management to consist of a number of closely related and highly integrated processes. To realize the key objectives of IT Service Management these processes must use the three P's (people, processes and products) effectively, efficiently and economically. Only then can IT organizations be sure of delivering high quality, innovative IT services that are aligned to the business processes.

**The Philosophy of IT Service
Management**

**IT is the business
And
The business is IT**

Student Notes

The Three P's

The key objectives of IT Service Management can only be realized by the best utilization of the three P's, people, processes and products:

People

Users, Customers, IT Staff and managers all come under this heading. Communication, training and clear definitions of roles and responsibilities for all parties involved are essential if this valuable asset is to be utilized fully.

Processes

This is where ITIL comes in. Service Management processes are the heart of ITIL and are considered as two core areas:

<i>Service Support</i>	<i>Service Delivery</i>
Service Desk*	Service Level Management
Incident Management	Financial Management for IT Services
Problem Management	Capacity Management
Configuration Management	IT Service Continuity Management
Change Management	Availability Management
Release Management	

*This is a function and not a procedure.

Service Support concentrates on the day to day running and support of IT Services whilst Service Delivery concentrates on long term planning and improvement of the same.

This course serves to explain at an introductory level each of the above areas and how they relate to each other.

Products

Tools and technology have come a long way since the evolution of ITIL. There are now a number of tools available to IT organizations that are considered as being "ITIL Compliant". This basically means that they have been developed to compliment IT Service Management procedures. They should be regarded as their name suggests a tool that can assist in the implementation and running of IT service provisions. It would be a mistake to think that simply by using one of these tools you would be working to ITIL standards. "A Fool with a Tool is Still a Fool" (Hewlett Packard White Paper - <http://www.itilalumni.com/members/feature/feature.html>)

— The Three P's

This is all about the efficient, effective and economical use of:

- *People*
 - Customers, Users & IT Staff
- *Processes*
 - ITSM / ITIL
- *Products*
 - Tools and technology

Student Notes

Service Management – General

One of the biggest issues in an organization is that roles & responsibilities are not defined. IT staff often have an enormous variety of tasks they need to carry out such as handling incidents, problems and changes. This can lead to confusion when there is no clear demarcation of responsibility or good processes and procedures to be followed.

A benefit of introducing good Service Management practices is that situations like this can be controlled. For each of the processes covered by this course, one or more roles are identified for carrying out the functions and activities required. Organizations may allocate more than one role to an individual within the organization or as more often happens, allocate more than one individual to a role. The purpose of the role is to locate responsibility rather than to create an organizational structure.

— Service Management — General



Student Notes

Customer and Users

To avoid confusion regarding roles and terminology the terms 'Customer' and 'User' are used throughout this course to differentiate between those people (generally senior managers) who pay for and own the IT Services (the Customers) and those people who use the services on a day-to-day basis (the Users). The semantics are less important than the reason for differentiation.

The primary point of contact for Customers is the Customer Relationship Manager, whilst the primary point of contact for Users is the Service Desk. A poorly functioning Incident Management process will affect the User population immediately. A service that is poor value for money will have a greater impact on the Customer.

It is therefore important that we distinguish the different, but related, needs of Users and Customers in the provision of services. Certainly, their goals may be at odds and need to be balanced; for example Users may demand high availability whereas Customers look for value for money at different levels of availability. There are information flows that should be maintained and key process elements that should be defined for use by both parties.

The term Super or Expert is often applied to Users who have been nominated by the business to act as the primary contact for incidents and problems. They can also play a first –line support role for minor incidents or service requests. This has to be managed carefully or two possible issues will arise:

1. Users will stop using the Service Desk and
2. The Super User will be so tied up doing support they are unable to complete their everyday role.

— Customers and Users

- **Customer**

*This term is used for the Customer management who have responsibility for the **funding** of the service*

- **User**

*This term is used for the person **using** the service*

- **Super or Expert User**

The User to deal with first-line support problems and queries

Student Notes

Challenges to the IT Organization

Organizations are increasingly dependent upon IT to satisfy their corporate aims and meet their business needs. This growing dependency leads to a demand for high quality IT services that match those needs. Add to this demand economy, reliability, flexibility and consistency and the challenges facing most IT organizations become obvious.

Many IT organizations have been guilty of concentrating on technical issues or focusing internally. These days with demands from the business as mentioned in the previous paragraph IT has to change their focus and concentrate on a more Customer oriented approach. This means that the IT organization should try to provide whatever is agreed with their Customers and develop a more professional and business like relationship with them.

One of the main problems in IT service delivery is that Customers frequently don't know what IT requirements they need. Therefore, IT organizations should aim to translate their business requirements into solutions - Customers don't buy IT products; they buy services (or solutions).

Once the appropriate IT solution has been found Customers want to know when they can receive it and should be satisfied that it will fulfill their business requirement. They want it to be consistent and to know that they are getting value for money. In other words, the price they pay should be a fair one for the product or service they receive.

Customers want to be told what they are getting, plus when, how and what to do if they have a problem with it.

By working in partnership with the Customer, IT organizations should be able to justify their costs and subsequently the investment in continually improving the services they provide.

IT organizations should be seen as a valuable part of the business chain and not an expensive, unreliable resource.

Challenges to the IT Organization

- *Contribution to solving business challenges*
 - This means contributing earlier in the planning cycle
- *A measurable contribution to the business value chain*
- *Service provision as opposed to IT product delivery*
- *A business like relationship*
- *A consistent and stable service*
- *Less emphasis on technology*

Student Notes

The Support Problem

In a lot of IT organizations there is no structured customer support mechanism in place. There is usually some sort of Service Desk and some sort of a 2nd and 3rd line support. But all these departments are trying to solve the same incidents on their own. Often there is very little communication and cooperation between the departments that results in incidents not solved quickly enough and an inconsistency in the quality of response times. This is one of the reasons such organizations have a low Customer confidence / perception and that those Customers start solving their own issues resulting in high "Peer support". The costs involved in situations like this are hard to estimate, especially the lost opportunity costs, but can be high, directly affecting the business.

Most organizations are very reactive and interrupt driven. Support resources are under managed and they are continually fire fighting, resolving incident & problems repeatedly rather than eliminating them. There is often an over dependency on key staff which is compounded by the fact that the knowledge in their heads is not documented. A further problem is that a lot of IT staff lack focus on the Customer's needs and issues. IT staff resources and related cost requirements are most of the time very unclear and it is not always known what some people do and why they are there. They don't always fully know themselves.

In many IT organizations, uncoordinated and unrecorded change takes place every day. This poor change control costs a lot of money and soaks up resources because things have to be done over and over again. A lack of Change Management can have major negative effects on other processes as this lack of control over changes to the IT infrastructure makes such changes more susceptible to failure.

There are very few SLA's that succeed in their supposed objective of improving the quality of service. That is if SLA's exist in the first place. One of the main reasons for this is that management information is not available – decisions are based on 'I think' rather than 'I know'. Measuring Service Management that drives improvement is very difficult if the baseline cannot be identified. This can make a Service Management improvement program hard to justify. Value for money can't be judged without a good understanding of costs (including the cost of changes). An understanding of the service costs also provides a sound basis for decisions for IT development.

— The Support Problem

This can be broken down into 3 main areas: _____

- *Customer*

- no structured customer support mechanism in place
- low customer confidence in/perception of IT
- a lack of focus on customer's needs

- *Management*

- support under managed and under resourced
- problems being resolved repeatedly rather than eliminated
- an inconsistent quality of call response and response times
- uncoordinated and unrecorded changes

- *Decision Making Information*

- no management information available – decisions being based on 'I think' rather than 'I know'

Student Notes

Why Implement Service Management?

Having recognized that IT departments are now in the business of service provision they should adopt a whole new way of thinking and embrace the same business concepts as those used by all service providers. There is a lot of catching up to do.

The Service Management approach with ITIL is that new way of thinking. But...it should not be implemented because it is currently fashionable. If you don't understand why you are implementing ITIL, you will not succeed. The driving factor should be the desire to deliver added value and value for money to the customer.

Whilst there are short-term benefits, many organizations will need to plan a long-term program of process improvements before they can be considered best in class. It is important to realize this is one of the greatest benefits for the organization of implementing the Service Management methodology. It will give the organization (an):

- Improved quality of service - more reliable business support.
- More focused IT Service Continuity procedures and more confidence in their ability to follow them when required.
- Clearer view of current IT capability.
- Better information on current services (and possibly on where changes would bring most benefits).
- Greater flexibility for the business through improved understanding of IT support.
- More motivated staff; improved job satisfaction through better understanding of capability and better management of expectations.
- Enhanced Customer satisfaction as service providers know and deliver what is expected of them.
- Increased flexibility and adaptability within the services.
- System-led benefits, e.g. improvements in security, accuracy, speed, availability as required for the required level of service.
- Improved cycle time for changes and greater success rate.
- Operating costs will decrease as less effort is wasted giving Customers products or services they don't want.
- Profits margins will improve as more repeat business is won – it is much cheaper to sell to an existing Customer than to court a new one.
- Efficiency will improve, as staff will work more effectively as teams.
- Morale and staff turnover will improve as staff achieves job satisfaction and job security.
- Service quality will be constantly improving, resulting in an enhanced reputation for the IT department, which will tempt new Customers and encourage existing Customers to buy more.
- The IT department will become more effective at supporting the needs of the business and will be more responsive to changes in business direction.

The importance and level of these will vary between organizations. The issues arise when trying to define these benefits for any organization in a way that will be measurable later on. Following ITIL guidance can help to quantify some of these elements.

— Why Implement Service Management? —

- *Professionalism*
- *Focus on benefits to the customer/business*
- *Decision making metrics*
- *Clear points of contact*
- *Part of a QM strategy - focus on continuous improvement*
- *Cost reduction - based on the standardization of the expensive processes (20/80)*
- *Avoid reinventing the wheel*
- *Long term survival!*

Student Notes

The Objectives of ITSM

Service Management is a process-oriented approach to delivering customer-focused IT services that meet cost and performance targets set in partnership with Line-of-Business (LOB) customers and embodied in service level agreements (SLA's) and operational level agreements (OLA's).

The challenges facing the IT Managers of today are to co-ordinate and work in partnership with the business to create new business opportunities whilst reducing the Total Cost of Ownership (TCO).

This means that IT organizations must be responsive to the ever changing needs of the business and flexible enough to adapt to these changes without causing disruption to the business flow.

Customer expectations are high as they not only require this responsive and flexible service but expect IT organizations to meet these demands whilst maintaining or improving the quality of the services they deliver.

In the current environment this also means performing these tasks in the most economical way.

This is where ITIL comes in by providing IT Service Managers with a comprehensive and consistent set of best practices, whilst promoting a quality approach to achieving business effectiveness and efficiency in the use of information systems.

Important note: The intention when implementing ITIL processes is that they support but do not dictate the business processes of an organization.

— The Objectives of ITSM

- *Align IT services with the ever changing needs of the business*
- *Improve the quality of IT services*
- *Reduce the long-term cost of service provision*

Service Management is all about the delivery of customer-focused IT services using a process-oriented approach

Student Notes

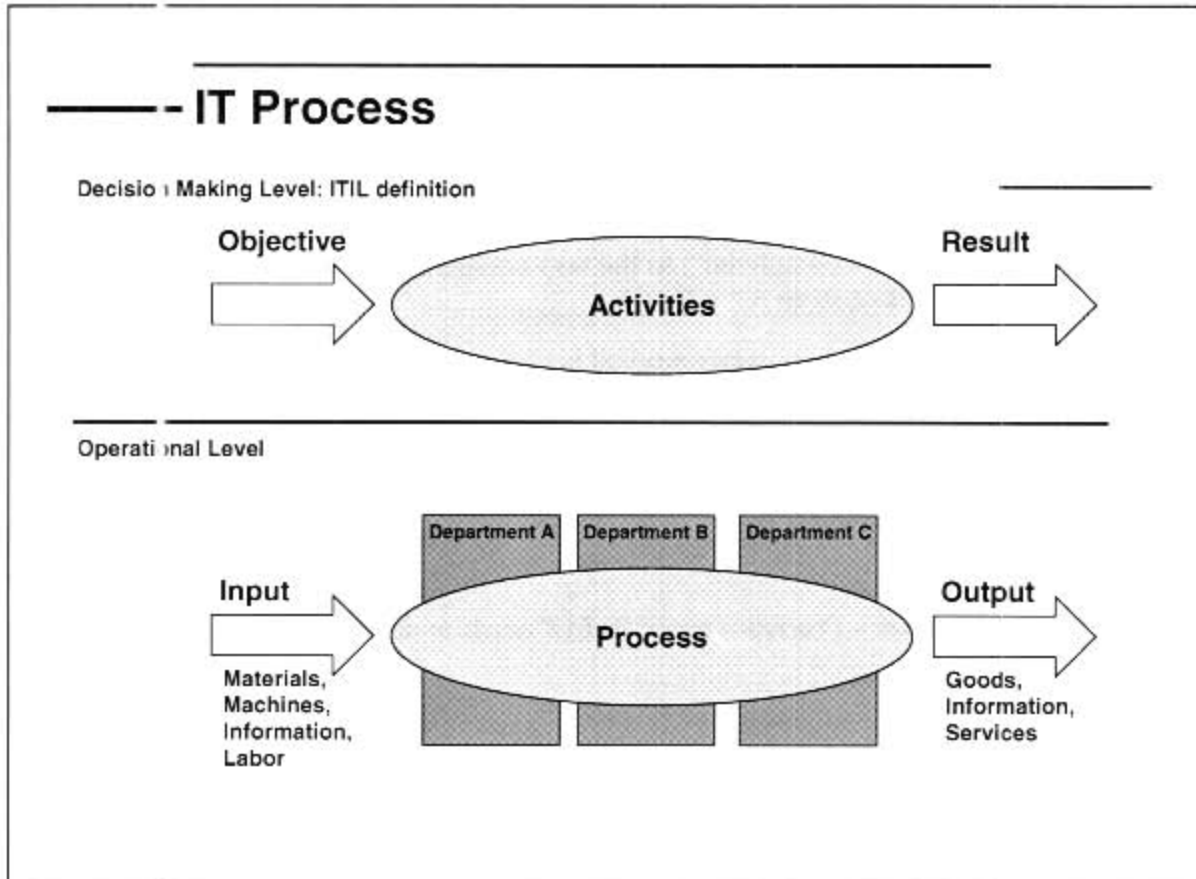
IT Process

As mentioned previously, IT Service Management is based on processes. A process is a bundle of logical activities combined to achieve a certain goal (result). The benefits of processes are:

- In a process the goals (results) are described and how they are going to be achieved.
- For every process the inputs and outputs are defined: what needs to be done to achieve the goal(s) and what are the things that other processes need from us to achieve theirs (in other words: our result).
- A whole organization can be run with a number of different processes. These can be monitored one by one which is better and easier than monitoring the whole.
- People can be made responsible for the efficiency, effectiveness and result of their process, which provides a means of monitoring and controlling an organization.
- An organization can improve by setting a norm then relating results to it. This can show the ways to improve activities in a process. And/or one can increase the norm and in this way improve continuously.
- By creating clearer roles and responsibilities, then organizing them efficiently and effectively it becomes easier to avoid conflict of interest. For example, a support engineer will not prioritize his own problems as most important because "he does not like to solve incidents".
- Activities that have to be executed in several departments but are related to one result can be controlled better if there is one overall main process.

Processes are the highest level of defining activities and are, most of the time, a standard for the whole organization. Procedures (work instructions) are more about detail and they describe who executes certain activities in a process. Procedures can be varying from department to department or activity to activity. For example: the Change Process demands that every change will be requested by a RfC (Request for Change), but the information contained within each RfC could be different from department A to B.

Most organizations are structured in departments and IT Staff that execute different activities in a process are part of those departments. For example: to solve an incident one requires 1st line support, 2nd and 3rd line support and specialists. They all are - most likely - part of 3 or 4 different departments, but in some "moment of time" part of a sole process, with only one objective: to restore the service as quickly as possible. The same IT Staff can be part of other processes in other moments in time. Whilst this is the biggest benefit of processes it could cause problems if process managers and department managers have not previously agreed how to allocate resources.



Student Notes

Roles & Responsibilities within Processes & Procedures

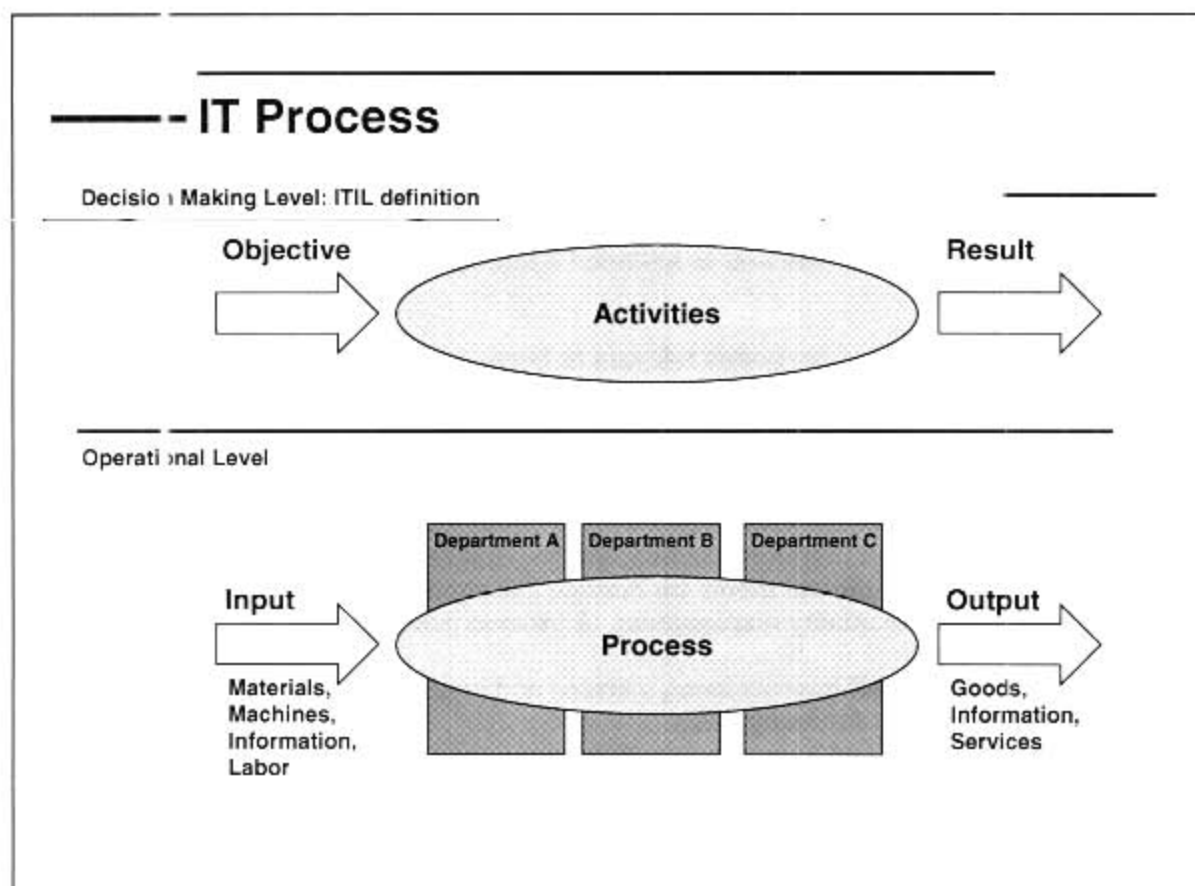
Each process can be broken down into a series of tasks. Each task will be executed by a *role*. This may be embodied in a human being or performed by a piece of software. If human-centric, then there will be a set of competencies that an individual needs in order to perform the role.

The execution of the role is governed by a set of *rules*. These will range from the simple ("All boxes on the form should be completed") to the very complex ("Credit is only allowed if a set of criteria are met according to an algorithm").

Often, a process will span various organizational boundaries. It is important, therefore, that each process should have an *owner*. This is another *role*.

The process owner is responsible for the *process definition*, which should be treated as a CI, subject to the usual Change Control Process. The process owner is responsible for ensuring that everybody who is involved in the execution of the process is kept informed of any changes that occur.

*A good point to remember – Processes cover **WHAT** needs to be done whilst procedures cover **HOW** to do it.*



Student Notes

Quality

'We have learned to live in a world of mistakes and defective products as if they were necessary to life. It is time to adopt a new philosophy...' (W.Edwards Deming, 1900-93)

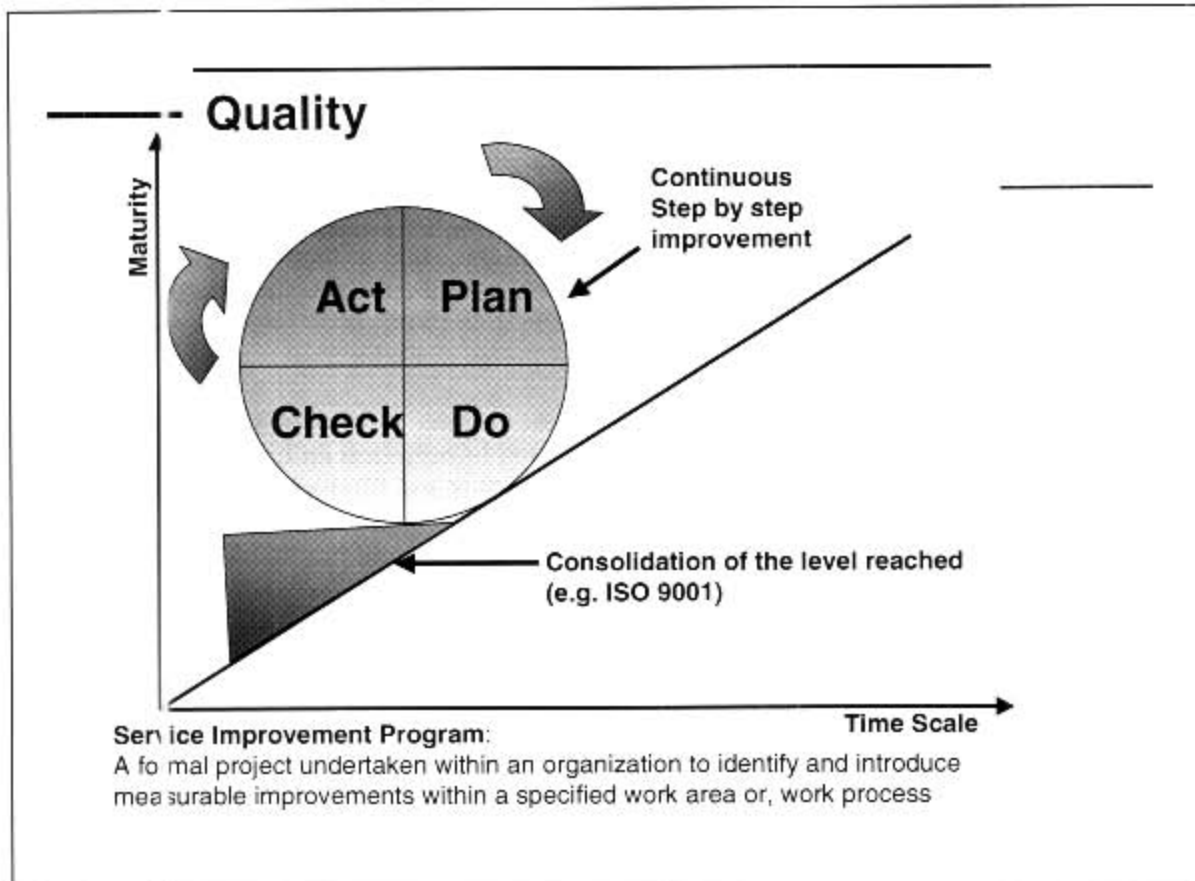
The way that an organization plans to manage its operations so that it delivers quality services is specified by its quality management system. The quality management system defines the organizational structure, roles & responsibilities, policies, procedures, processes, standards and resources required to deliver quality IT services. However, a quality management system will only function as intended if management and staff are committed to achieving its objectives.

Excerpts from Deming's fourteen points relevant to Service Management:

- Break down barriers between departments (improves communications and management).
- Management should learn their responsibilities and take on leadership. Process improvement requires commitment from the top; good leaders motivate people to improve themselves and therefore the image of the organization.
- Improve constantly. A central theme for Service Managers is continuous improvement; this is also a theme for quality management. A process-oriented approach is key to achieving this target.
- Install education and self-improvement, learning and improving skills have been the focus of Service Management for many years.
- Training on the job (linked to continuous improvement).
- Transformation is everyone's job - the emphasis being on teamwork and understanding.

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'. The consolidation phase enables the organization to take stock of what has been taking place and to ensure that improvements are embedded. Often, a series of improvements have been made to processes that require documentation (both to allow processes to be repeatable and to facilitate recognition of the achievement of some form of quality standard).

W. Edwards Deming is best known for his management philosophy establishing quality, productivity, and competitive position. As part of this philosophy, he formulated 14 points of attention for managers. Some of these points are more appropriate to Service Management than others.



Student Notes

ITIL....

ITIL was originally a set of about 60 books developed in the late 1980's as a set of best practices for IT by the CCTA (Central Communications and Telecom Agency) of the UK government. The CCTA still owns the books. Currently, ITIL may be thought of as more than the set of books. ITIL has become a widely accepted base for running the business of IT.

From the beginning, ITIL has been publicly available. This means that any organization can use the framework described in the books. Because of this, the IT Infrastructure Library guidance has been used by a diverse range of organizations, such as local and central government, energy, public utilities, retail, finance, and manufacturing. Very large organizations, very small organizations and everything in between have implemented ITIL processes.

The IT Infrastructure Library documents industry best practice guidance. It has proved its value from the very beginning. Initially, CCTA collected information on how various organizations addressed Service Management, analyzed this and filtered those issues that would prove useful to CCTA and to its Customers in UK central government. Other organizations found that the guidance was generally applicable and markets outside of government were very soon created by the service industry.

Being a framework, ITIL describes the contours of organizing Service Management. The models show the goals, general activities, inputs and outputs of the various processes, which can be incorporated within IT organizations. ITIL does not cast in stone every action that should be done on a day-to-day basis because that is something which will differ from organization to organization. Instead it focuses on best practice that can be utilized in different ways according to need.

Thanks to this framework of proven best practices, the IT Infrastructure Library can be used within organizations with existing methods and activities in Service Management. Using ITIL doesn't imply a completely new way of thinking and acting. It provides a framework in which to place existing methods and activities in a structured context. By emphasizing the relationships between the processes, any lack of communication and co-operation between various IT functions can be eliminated or minimized. ITIL provides a proven method for planning common processes, roles and activities with appropriate reference to each other and how the communication lines should exist between them.

An ITIL approach lends itself well to supporting today's complex IT world in the light of business objectives. The ITIL umbrella includes the ITIL books (as a core), ITIL Certification, ITIL Consultants and Services, ITIL-supporting software and tools, ITIL and ITIL-based training (like this course), and user groups such as the itSMF.

The itSMF is a totally independent, not-for-profit organization owned and run by its members. It promotes and helps to set the standards for best practice in IT Service Management. There are national chapters in many parts of the world. For further details of the chapters, and how to contact them, access the web site www.itsmf.com.

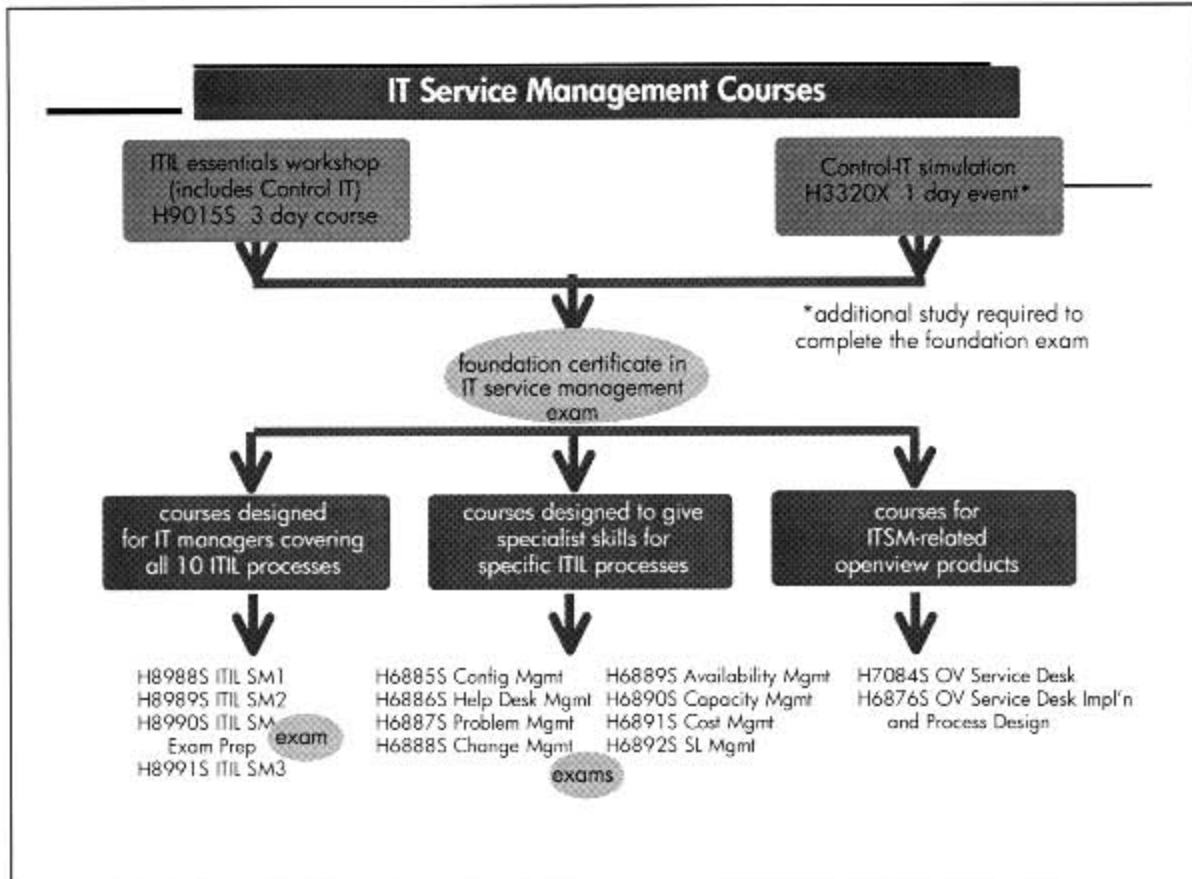
ITIL

- *Was gathered from Users, Suppliers, Consultants*
- *Proven in practice*
- *Is under constant development*
- *Is supported by tools*
- *Is the world wide de facto standard for IT Service Management*
- *Offers certification of consultants and practitioners*
- *Managing the infrastructure now in top 3 concerns*
- *Avoid reinventing the wheel*
- *Has its own international user group (IT Service Management Forum)*

Student Notes

IT Service Management Courses

The Service Delivery and Service Support books are the books that are used to cover the IT



Student Notes

Model (According to ITIL)

The Service Delivery and Service Support books are the books that are used to cover the IT Service Management methodology. The Service Delivery book looks at what service the business requires of the provider in order to provide adequate support to the business Users. To provide the necessary support the book covers the following topics:

- Capacity Management.
- Financial Management for IT Services.
- Availability Management.
- Service Level Management.
- IT Service Continuity Management.

Very much related to the Service Delivery topics is Customer Relationship Management. This process is often the bridge between the technology focused IT organization and the Business that wants to realize their business objectives. CRM is the entrance to IT for the customer

The Service Support book is concerned with ensuring that the Customer has access to the appropriate services to support the business functions. Issues discussed in this book are:

- Service Desk.
- Incident Management.
- Problem Management.
- Configuration Management.
- Change Management.
- Release Management.

The Service Desk is the entrance for the end-user. All IT Service related issues could be directed to the Service Desk, which will be the interface between the end-user and the service support processes.

Very much related to Availability Management is Security Management. Right now it is not officially part of the Service Delivery and Support sets, however reference to security can frequently be found in many of the processes.

Model (According to ITIL)

The Service Delivery and Service Support books are the books that are used to cover the IT Service Management methodology. The Service Delivery book looks at what service the business requires of the provider in order to provide adequate support to the business Users. To provide the necessary support the book covers the following topics:

- Capacity Management.
- Financial Management for IT Services.
- Availability Management.
- Service Level Management.
- IT Service Continuity Management.

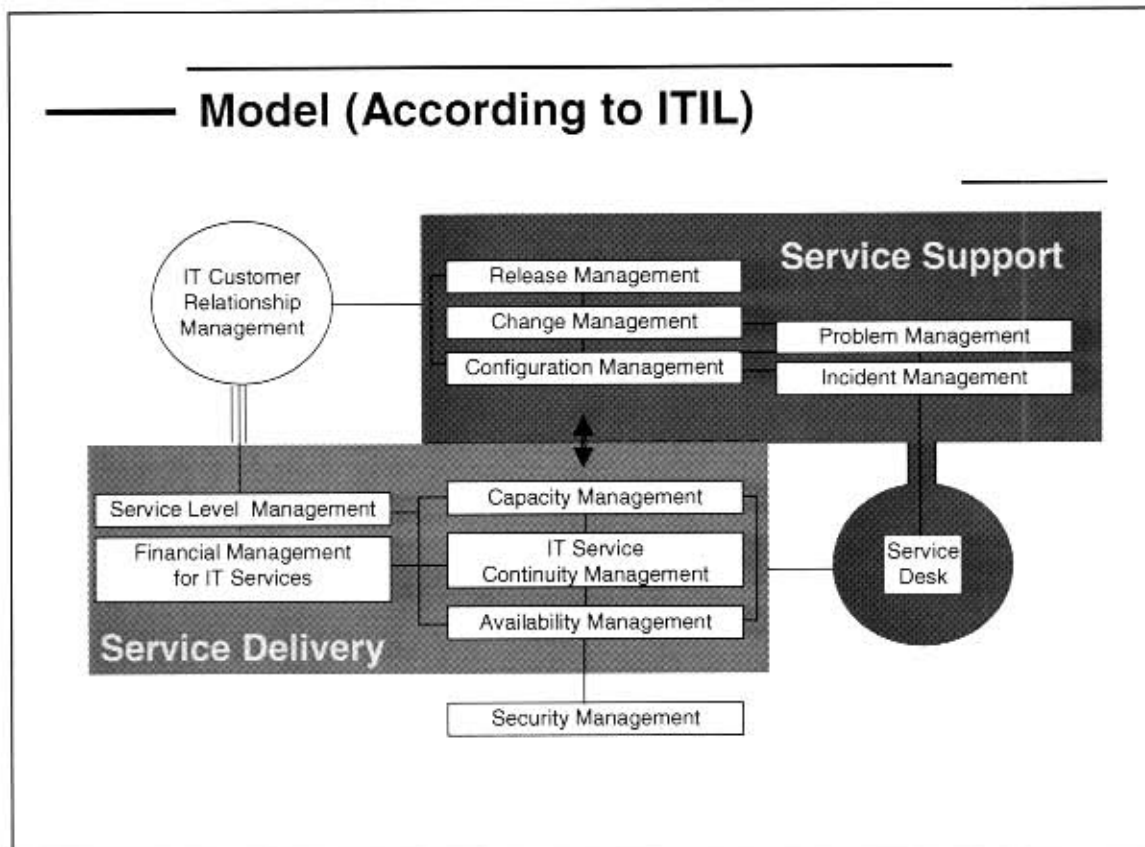
Very much related to the Service Delivery topics is Customer Relationship Management. This process is often the bridge between the technology focused IT organization and the Business that wants to realize their business objectives. CRM is the entrance to IT for the customer

The Service Support book is concerned with ensuring that the Customer has access to the appropriate services to support the business functions. Issues discussed in this book are:

- Service Desk.
- Incident Management.
- Problem Management.
- Configuration Management.
- Change Management.
- Release Management.

The Service Desk is the entrance for the end-user. All IT Service related issues could be directed to the Service Desk, which will be the interface between the end-user and the service support processes.

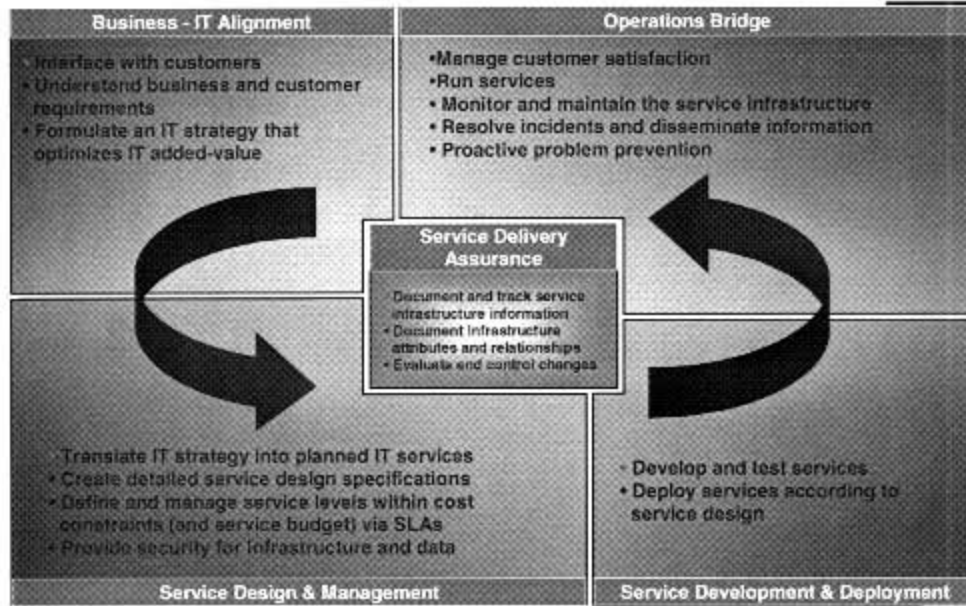
Very much related to Availability Management is Security Management. Right now it is not officially part of the Service Delivery and Support sets, however reference to security can frequently be found in many of the processes.



Student Notes

HP Reference Model

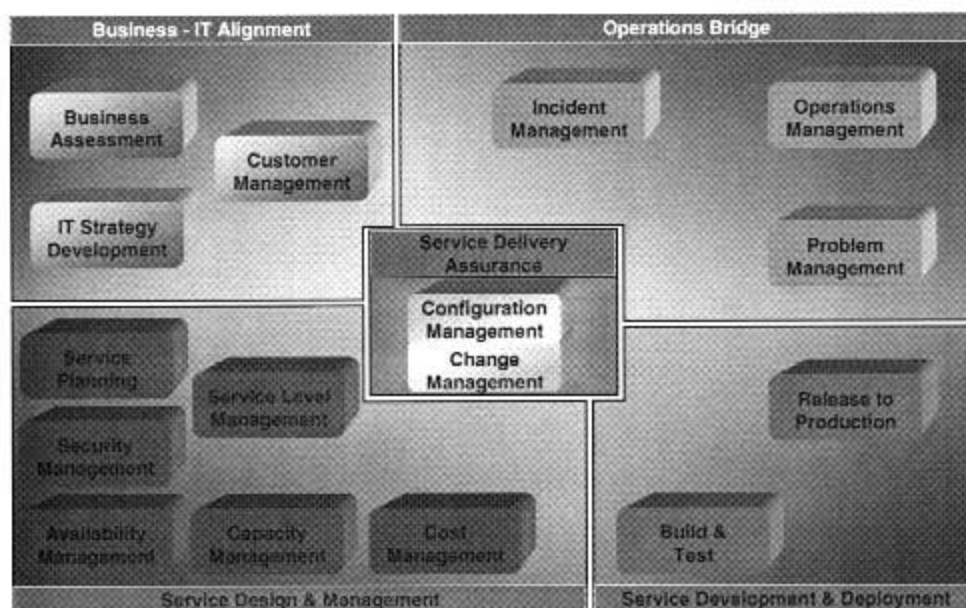
HP Reference Model



Student Notes

HP Reference Model

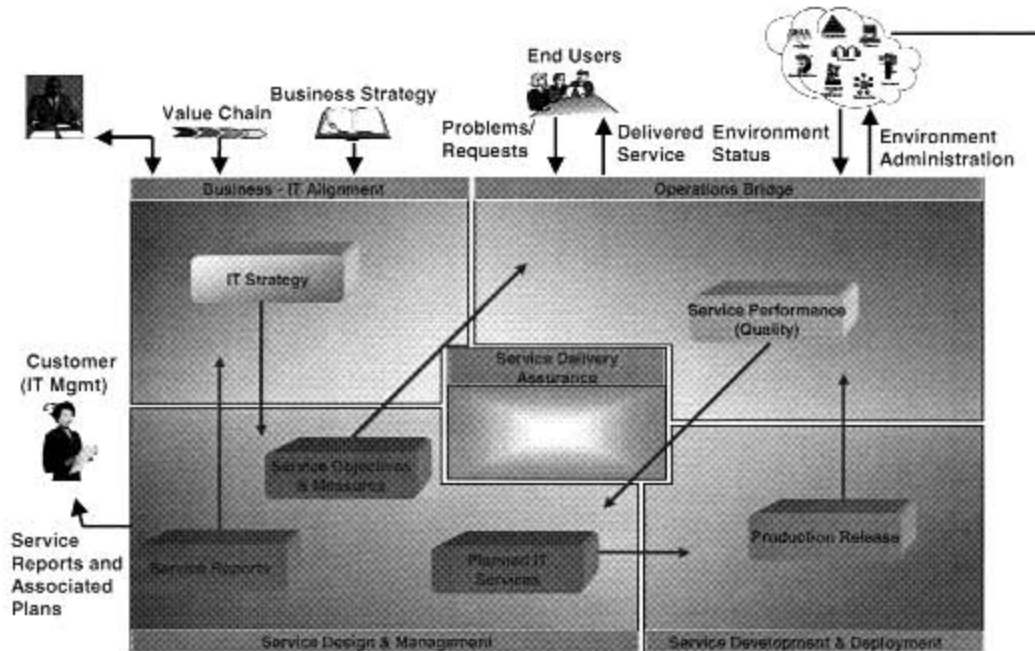
HP Reference Model



Student Notes

High-level Linkages

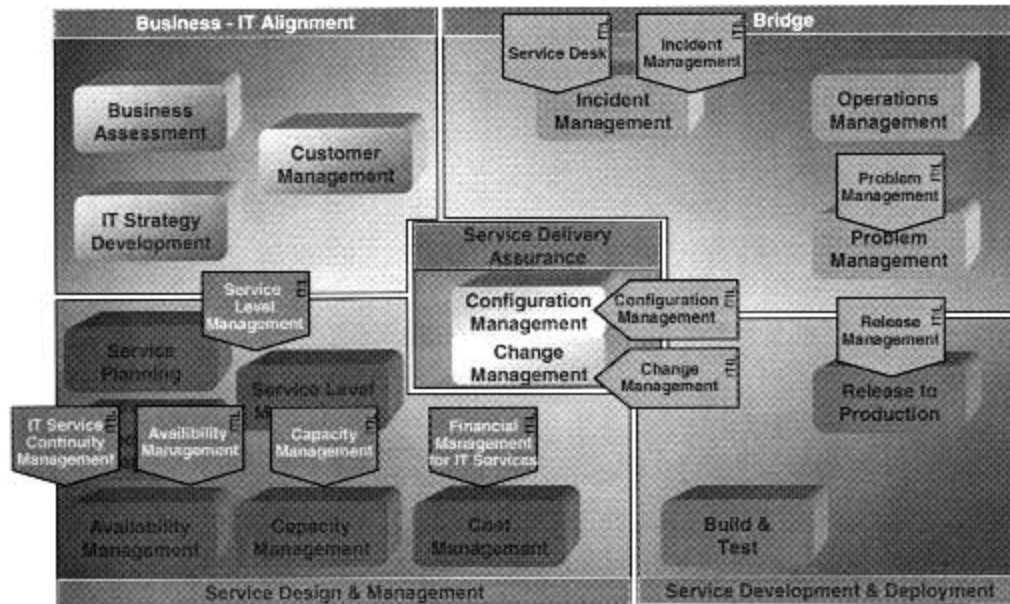
High-level Linkages



Student Notes

HP Reference Model

HP Reference Model



Student Notes

Module 1
Introduction to IT Service Management

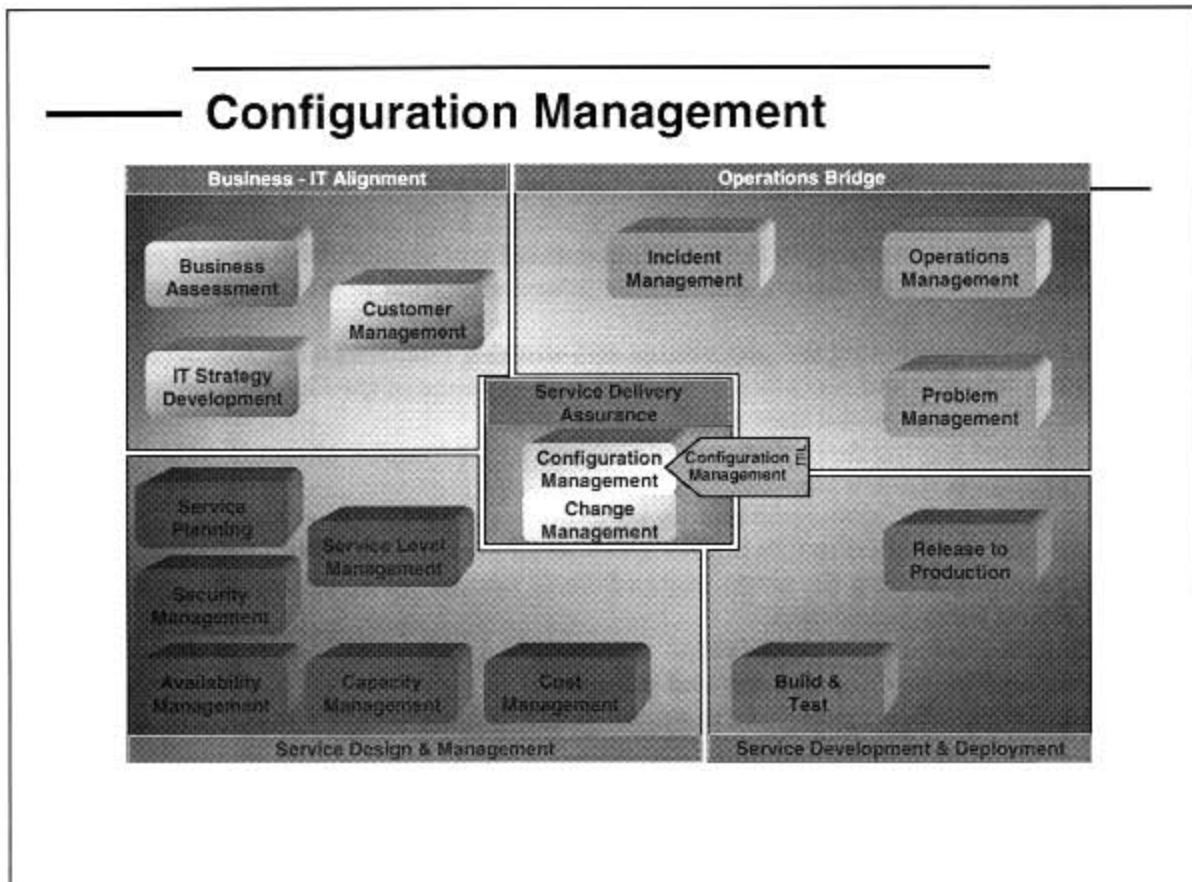
Module 2 — Configuration Management

This module introduces Configuration Management, a discipline that allows IT management to gain tight control over IT assets such as hardware devices, computer programs, documentation, outsourced services, facilities, job descriptions, process documentation, and any other items (called Configuration Items) that are related to the IT infrastructure.

Implementation of the Configuration Management discipline allows management to:

- Specify version, ownership, and status information for Configuration Items (CI's) in existence throughout the IT infrastructure.
- Describe the relationships between those items.
- Maintain current records about those items.
- Control changes to those items by ensuring those changes are consistent with the objectives of appropriate authorities.
- And audit the IT infrastructure to make sure it contains only authorized CI's.

Configuration Management



Student Notes

Configuration Management - Goals

..... To be efficient and effective, all organizations need to control their IT infrastructure and services. Configuration Management provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of Configuration Items (CIs) in existence.

Detailed objectives for Configuration Management should include:

- Providing everyone working in Service Management and support with correct and accurate information on the present configurations with their physical and functional specifications.
- Defining and documenting the procedures and working practices to be followed.
- Identifying, labeling and recording the names and versions of the CIs that make up the IT services, infrastructure and their relationships.
- Controlling and storing definitive, authorized and trusted copies of specifications, documentation and software.
- Reporting the current status and history of all items on the IT infrastructure.
- Ensuring that all changes to CIs are recorded as soon as practicable.
- Tracking and reconciling the actual state of the IT infrastructure against the authorized configuration records and data.
- Educating and training the organization in the control processes.
- Reporting metrics on CIs, changes and releases.
- Auditing and reporting exceptions to infrastructure standards and Configuration Management procedures.
- Providing accurate information on configurations and their documentation to support all the other Service Management processes.
- Providing a sound basis for Incident Management, Problem Management, Change Management and Release Management.
- Account for all the IT assets and configurations within the organization and its services.
- Verify the configuration records against the infrastructure and correct any exceptions.

Configuration Management — Goals

- *Providing information on the IT infrastructure*
 - To all other processes
 - IT Management
- *Enabling control of the infrastructure by monitoring and maintaining information on*
 - All the resources needed to deliver services
 - Configuration Item (CI) status and history
 - Configuration Item relationships

Student Notes

Configuration Management - Responsibilities

The basic activities of Configuration Management are as follows:

Planning.

Planning and defining the purpose, scope, objectives, policies and procedures, and the organizational and technical context, for Configuration Management.

Identification and naming.

Selecting and identifying the configuration structures for all the infrastructure's CIs, including their 'owner', their interrelationships and configuration documentation. It includes allocating identifiers and version numbers for CIs, labeling each item, and entering it on the Configuration Management Database (CMDB).

Control.

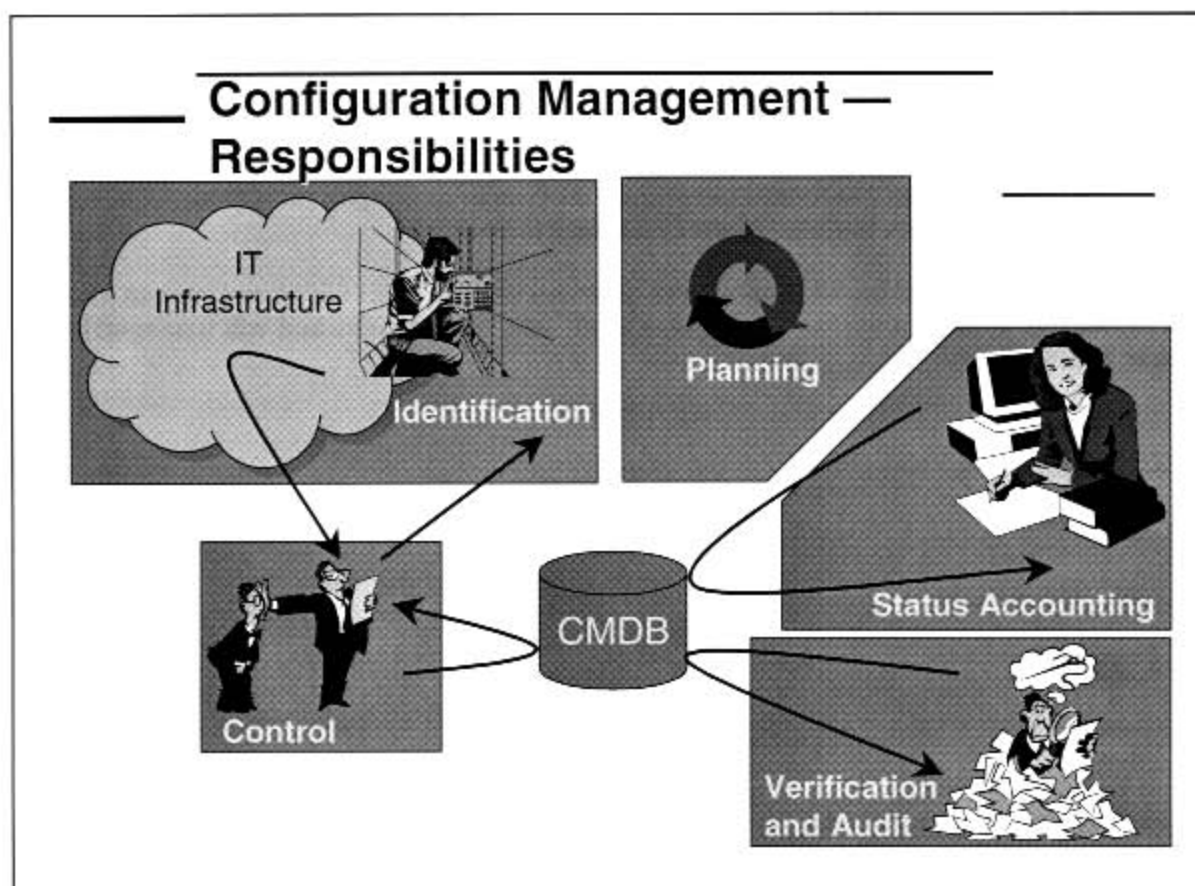
Ensuring that only authorized and identifiable CIs are accepted and recorded, from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without appropriate controlling documentation, e.g. an approved change request, and an updated specification.

Status accounting.

The reporting of all current and historical data concerned with each CI throughout its life cycle. This enables changes to CIs and their records to be traceable, e.g. tracking the status of a CI as it changes from one state to another for instance 'under development', 'being tested', 'live', or 'withdrawn'.

Verification and audit.

Configuration verification and audit comprises a series of reviews and audits that verify the physical existence of CIs and check that the CIs are correctly recorded in the CMDB and controlled libraries. It includes the verification of release and configuration documentation before changing the live environment.



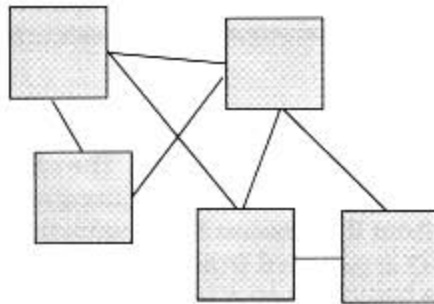
Student Notes

Configuration Item (CI)

The IT Infrastructure consists of configuration items. A configuration item is a documented element from the IT Infrastructure, such as hardware, software, accommodation, people and documentation (category). The recording of a CI contains characteristics such as type, version, supplier, customer etc (attributes). The relationship between the CIs are also recorded in the CMDB. These are vital for the accurate prediction of the impact of proposed change. Last but not least we record the status - such as in development, tested, implemented, maintained, history - of every configuration item.

A definition of a CI could be: "it is needed to deliver a service, it is unique and we can identify it. If we want to change it we have to register a RfC because it can be and will managed by Change Management"

Configuration Item (CI)



- *A Configuration Item*
 - Is needed to deliver a service
 - Is uniquely identifiable
 - Is subject to change
 - Can be managed
- *A Configuration Item has*
 - a Category
 - Relationships
 - Attributes
 - a Status

Student Notes

CIs - Scope and Detail

The IT Infrastructure consists of configuration items. A configuration item is a documented element from the IT Infrastructure, such as hardware, software, accommodation, people and documentation (category).

Scope CMDB

The over-riding factor in deciding both scope and detail is the information needed to manage the service, irrespective of the cost or difficulty of obtaining and maintaining that data. A more pragmatic view is that not only should those factors be taken into account but also, and perhaps most importantly, managers should consider the consequences of inaccurate and out-of-date data being stored on the CMDB.

Before the transition to arranging a CMDB is made, a decision needs to be made on what part of the IT-infrastructure the Configuration Management will be controlling. The choice of Scope influences the range of diagnoses of Problem Management, for the coordination of Change Management, etc. This choice is gathered from the Mission Statements that is set up for the processes. The choice of Scope also partially is gathered from an analysis of the services and their contribution to, or impact on, the business activities of the customers. Besides that the Scope can be gathered from the determination of a Service Level Agreement.

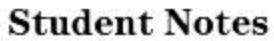
Detail CMDB

With the subdividing in levels a hierarchy of components and units is created. Choices are made on what main CI's are and in how many levels these CI's should be detailed. The highest level is the IT-infrastructure itself. The lowest useful level is the level where it is still possible to conduct control. The embodying of a CI in the CMDB is only effective when the control over the CI and the information that comes along with it are useful for other ITIL-processes.

With setting up the hierarchy of a CMDB the following rules apply:

- When there are more levels, more information should be maintained. This involves more work and results in a bigger CMDB.
- When there are lesser levels, there is less control and information over the IT-infrastructure.

When the CMDB does not have enough depth, changes to lower laying components cannot be kept up with correctly. Each adjustment to components of a mother CI will result in an alternative version of the mother CI; a PC that appears with two types of hard drives will then have a version A and a version B. Should there appear many adjustments on daughter components, then the variation numbering eventually will be opaque and hard to keep up with.

[illegible]

Naming and Attributes

Naming

The name of a CI must be unique. Every CI in the controlled infrastructure must be identified and we only can do this by giving this CI a unique number. Like your car: this care is unique in the whole world because of a combination of your license plate number and the state/country where you live in.

Naming should be simple and logical. Simple because what's the need to make in difficult? IT Staff and customers must have a clue how to read and assembly the CI identification. So try as much as possible to find a logical and simple identification: like A1234567 instead of PC_BUILD_A_LOK1.4_1234.

Throughout the whole lifecycle of a CI the first given identification should stay the same. Of course the exception makes the rule! So that's another reason why you should not implement I numbers as PC_BUILD_A_LOK1.4_1234 because it is related to the building where it is installed.

Attributes

The following attributes are examples that could be used in the CMDB. Note that hardware CI types will have different attributes from software CI types.

Attribute	Description
CI Name	The unique name by which this type of CI is known.
Copy or Serial Number	The number that uniquely identifies the particular instances of this CI, for example, for software the copy number, for hardware the serial number.
Category	Classification of a CI (e.g. hardware, software, documentation)
Type	Description of CI type, amplifying 'category' information (e.g. hardware configuration, software package, hardware device).
Model Number	Model of CI (corresponding, for example, to supplier's model number (hardware) e.g. Dell model xxx, PC/aa model yyy).
Warranty expiry date	Date when the supplier's warranty expires for the CI.
Version Number	The version number of the CI.
Location	The location of the CI, e.g. the library or media where the software CI's reside, the site/room where a service is located.
Owner Responsible	The name and/or designation of the owner responsible for the CI.
Responsibility Date	Date the above owner became responsible for the CI.
Source/supplier	The source of the CI, e.g. developed in-house, bought in from company xxxxx etc.
Licence	License number or reference to license agreement.
Supply Date	Date when the CI was supplied to the organization.
Accepted Date	Date when the CI was accepted by the organization
Status (current)	The current status of the CI; e.g. under 'test', 'live', 'archived'.
Status (scheduled)	The next scheduled status of the CI (with the date or indication of the event that will trigger the status change).
Comment	A comment field to be used for textual narrative

Naming and Attributes

- *Naming Conventions*
 - Unique
 - Logical
 - Unchanging
 - Suitable for the tools being used
- *Examples of Attributes*
 - CI Name
 - Type
 - Location
 - Version
 - Service Details

Student Notes

Impact of Relationship

Knowing the relationships that the CI's have to each other is beneficial for all of the processes.

First of all it could be a tremendous help for the Service Level Manager. When creating a SLA or OLA's or contract, it is very important to know how the infrastructure is built and which CIs are a part of the services being delivered. They also need to understand how end-to-end services are configured.

Secondly, it is very beneficial for the diagnoses of technical problems. It can be used for an impact analysis by seeing what other CIs will / could be affected. It can be use to see if incidents are related and can help with the investigation to find the root cause. If past change records have been related this may highlight if the change was the cause of an incident or problem.

If the Availability Manager wants to predict the availability of certain services it is important that they are able to allocate the CI's that are needed to deliver those services. Based on the information that he/she has about those CI's and their relationships the calculation can start.

Last but not least, relationships are very important to used to analyze the impact of a change. By seeing the relationship between the CI that has to be changed and other CI's the Change Manager can set the category, can invite the right staff for the CAB and can decide what has to be done to make this change a success.

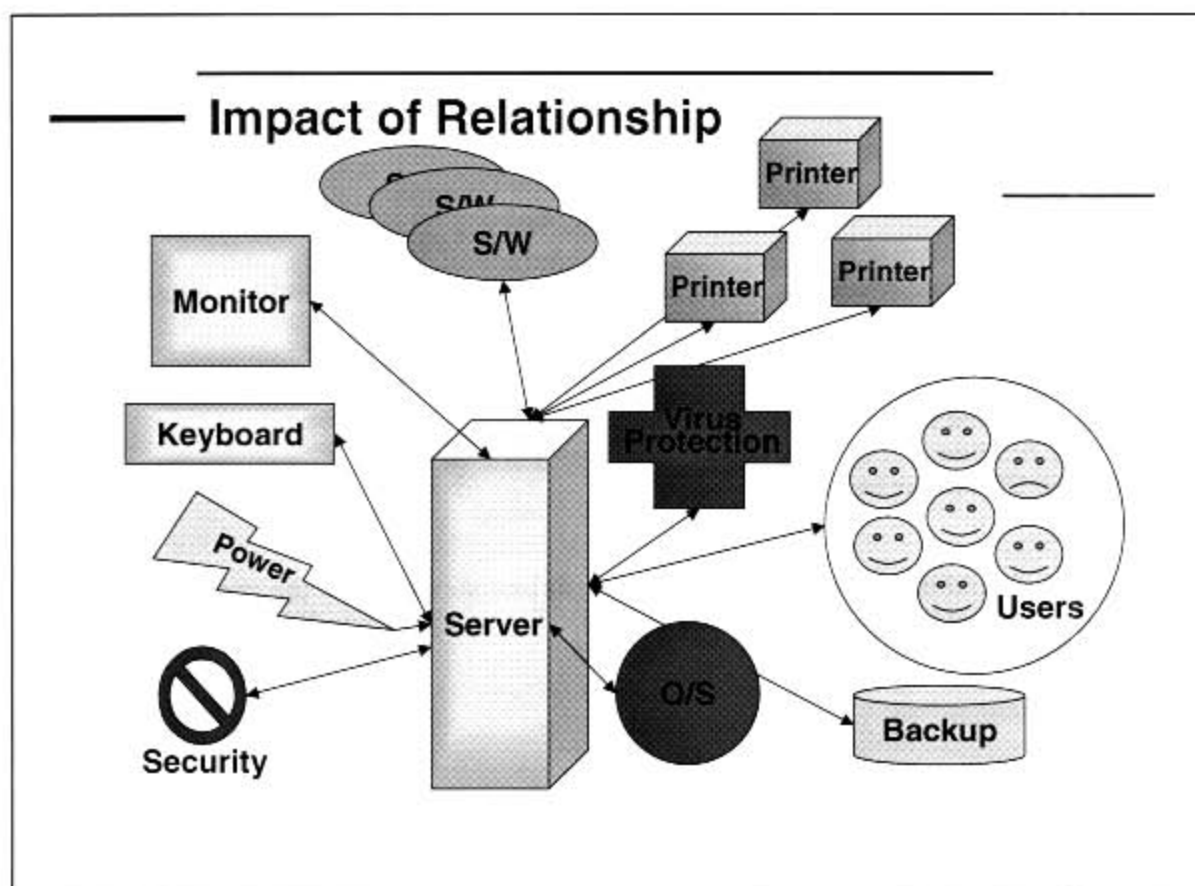
Typical relationships are:

- *Is a component of*; this is the mother-daughter relation of the CI, like a floppy drive is a component of a PC and a software-module is a component of a program.
- *Is a copy of*; a copy of a standard model or a program.
- *Relates to*; a procedure, an SLA or a costumer area.
- *Relates with*; for example a PC that is connected to a LAN-segment.
- *Is used by*; like a CI that is used by a service, so that costs and availability of the service can be calculated, or a software module that is called on by several programs so that 'what the impact of an adjustment is' can be traced.

As when determining the scope and detail, a thorough 'weighing one against the other' on what is needed, the amount of work that comes along with it and the available recourses for that work, should be done with determining the necessary relationships.

Other types relationships:

- *RFC's*; the relation with all RFCs affecting this CI.
- *Relation with Changes*; the relation with of all change records affecting this CI.
- *Relation with Problem*; the relation with all problem records affecting this CI.
- *Relation with Incident*; the relation with all incident records affecting this CI.



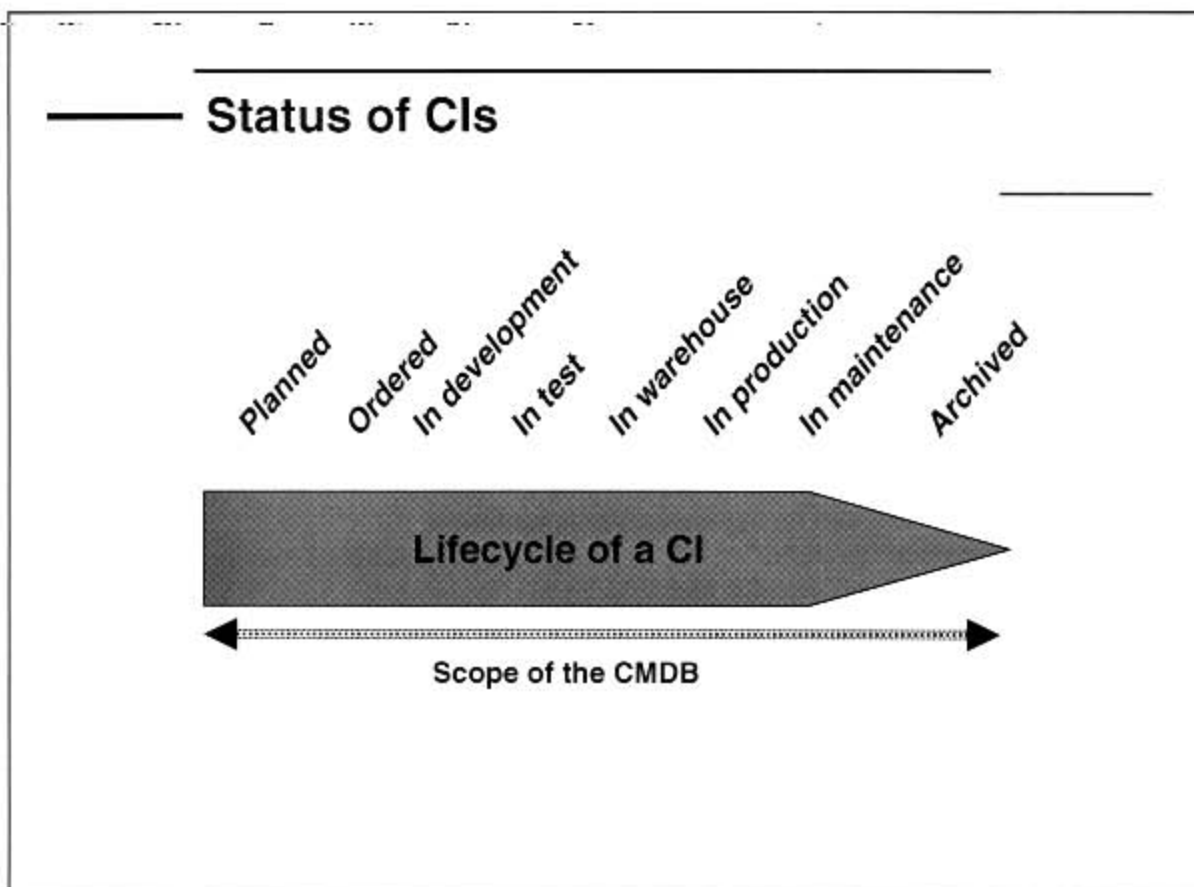
Student Notes

Status of CIs

Reporting on the current and historical data regarding each CI throughout its life cycle enables changes to CIs and tracking of their records through various statuses. For example:

- Ordered.
- Received.
- In development.
- Tested.
- Accepted.
- Change has been approved and taken into consideration in the planning, a new CI and documentation (that is also a CI) is coming.
- In maintenance.
- Down, in technical problems.
- Out of use, added to archives.
- The order has been received or the adjusted version is available.
- Active, the CI is being used.

Status reports should be produced on a regular basis and should show the current, previous and planned states of CIs. These reports can be used to establish baselines and enable changes to be traceable.



Student Notes

Baseline

A configuration baseline is the configuration of a product or system established at a specific point in time, which captures both the structure and details of a configuration. It is a reference for further activities. An application or software baseline provides the ability to change or to rebuild a specific version at a later date.

Configuration baselines should be established by formal agreement at specific points in time and used as reference points for the formal control of a configuration. Configuration baselines plus approved changes to those baselines together constitute the currently approved configuration. Specific examples of baselines that may be identified are:

- A particular 'standard' CI needed when buying many items of the same type (e.g. desktop computer) over a protracted period. If some servers are to include additional printed circuit boards, this could correspond to 'baseline plus'. If all future desktop computers are to have these boards, a new baseline is created.
- An application Release and its associated documentation
 - to be reverted to (should exist physically and be capable of easy reversion)
 - as the state of software for distribution to remote sites
 - as the state of software to be worked on in the future
 - as the state a system should be in before it can be upgraded to accept new hardware
 - or software.

Several baselines corresponding to different stages in the life of a 'baselined item', can exist at any given time – for example, the baseline for a software Release that is currently live, the one that was last live and has now been archived, the one that will next be installed (subject to change under Configuration Management control), and one or more under test. Furthermore, if, for instance, new software is being introduced gradually on a regional basis, more than one version of a baseline could be 'live' at the same time. It is therefore best to refer to each by a unique version number, rather than 'live', 'next', 'old'.

A configuration baseline is also a snapshot, or a position, that is recorded. Although the position may be updated later, the configuration baseline remains fixed as the original state and is thus available to be compared with the current position. A configuration baseline is used to assemble all relevant components in readiness for a change or release, and to provide the basis for a configuration audit and regression, e.g. after a change. The Configuration Management system should be able to save, protect and report on a configuration baseline, its contents and documentation.

Baseline

- *Configuration Baseline*
 - Configuration of a product or system established at a specific point in time, which captures both the structure and details of the product or system
 - A snapshot or a position, which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position (PRINCE 2)

Student Notes

Assets versus Configuration Items

Asset

Component of a business process like people, accommodation, computer systems, paper records, fax machines, etc.

Configuration Item (CI)

Component of an infrastructure - or an item, such as a Request for Change, associated with an infrastructure - and services, which is (or is to be) under the control of Configuration Management. CIs may vary widely in complexity, size and type - from an entire system to a minor hardware component. Examples are: hardware, software, documentation, procedures, functions, accommodations, services, servers, environments, equipment, network components, desktops, mobile units, applications, licenses, telecommunication

Configuration Management Database (CMDB)

Many organizations are already using some elements of Configuration Management, often using spreadsheets, local databases or paper-based systems. In today's large and complex IT infrastructures, Configuration Management requires the use of support tools, which includes a Configuration Management Database (CMDB). Physical and electronic libraries are needed along with the CMDB to hold definitive copies of software and documentation. The CMDB is likely to be based upon database technology that provides flexible and powerful interrogation facilities. The CMDB should hold the relationships between all system components, including incidents, problems, known errors, changes and releases. The CMDB also contains information about incidents, known errors and problems, and corporate data about employees, suppliers, locations and business units.

The CMDB may also be used to store and control details of IT Users, IT staff and business units, although the legal implications of holding information about people in the CMDB should be considered. Storing such information in the CMDB would allow personnel Changes to be related to Changes in CI ownership.

Assets versus Configuration Items

- *Asset*
 - Component of a business process
- *Configuration Item (CI)*
 - Component of an infrastructure - or an item associated with an infrastructure - which is (or is to be) under the control of Configuration Management
- *Configuration Management Database (CMDB)*
 - A database, which contains all relevant details of each CI and details of the important relationships between CIs

Student Notes

Essentials

Configuration Management is the basis of the whole IT Service Management framework. Without it we cannot effectively and efficiently meet the needs of our customer(s). It is closely linked with all the other Support and Delivery processes, both supporting and depending on them. Configuration Management should be planned and developed alongside them.

The Configuration Management Plan (Planning). This should cover up to the next six months in detail then follow with an outline for the next twelve months. The plan itself should include:

- Strategy, policy, scope, objectives, roles and responsibilities.
- Processes and procedures.
- CMDB, relationships with other processes.
- Details about the resources required including tools.

Identification. Identifying the configuration structures for all CIs, including their 'owner', their interrelationships and documentation. Allocating identifiers and version numbers for CIs, labeling each item, and entering it on the CMDB

Control. Ensures that only authorized and identifiable CIs are accepted and recorded and that no CI is added, modified, replaced or removed without appropriate controlling documentation.

Status accounting. Recording information on the current and historical data for each CI throughout its life cycle. Thus enabling Changes to CIs and their records to be traceable.

Verification and audit. A series of reviews and audits that verify the physical existence of CIs and check that the CIs are correctly recorded in the CMDB.

Role in assessing the impact of changes. Facilitates Change Management by providing information on the impact, cost, benefit and risk of proposed changes.

Scope & detail. The way the CMDB is built is very important. We only want to control what is necessary for the organization, so make sure that everybody is involved with the build of the CMDB and that we constantly ask ourselves: is this information / are those measures that we want.

Baseline. The configuration of a product or system established at a specific point in time, which captures both the structure and details of a configuration. It is a reference for further activities and provides an ability to change or to rebuild a specific version at a later date

More than an asset register. Configuration Management is far more than just good Asset Management. Configuration Management maintains not only relevant information on the assets themselves but also information about relationships between assets.

Essentials

- *Goals*
 - Provide information about the IT infrastructure
 - Monitor & Control the IT Infrastructure
- *Responsibilities*
 - Planning, Identification, Control, Status Accounting, Verification & Audit
 - Role in assessing impact of changes
- *Configuration item*
 - Categories, Attributes, Relationships, Status, History, Unique Ref. No.
- *Scope and detail (value of the information)*
- *Baselines*
- *Supports all other processes*
- *More than an asset register*

Student Notes

Management Reporting

Management reports should be designed to support Service Management activities such as progress monitoring, Configuration audits and service planning. The reports should be made available for interrogation and trend analysis by IT Service Management and other groups within the IT services structure. In general, IT Service Management should set the future direction for Configuration Management in the light of these management reports, taking in account the planned Configuration Management workload and growth.

Management reports for Configuration Management should cover the following:

- Results of configuration audits.
- Information on any non-registered or inaccurately registered CIs that have been detected and the corrective action.
- Information on the number of registered CIs and CI versions, broken down by CI category, type and status (and possibly also by location or other CI attributes).
- Growth and capacity information.
- Information on the rate of change of CIs/CMDB and the DSL.
- Details of any backlogs of Configuration Management work or any delays caused by Configuration Management activities, and proposed remedies.
- The Configuration Management staffing position.
- The amount of authorized work done out of hours by other IT service staff.
- The results of efficiency/effectiveness reviews, growth reviews and audits of the Configuration Management system and proposals for tackling actual or potential problems.
- Data and analyses on the number of CIs by type (e.g. services, servers, routers, hubs, software licenses, desktop PCs, etc).
- The value of CIs (or assets).
- The location of CIs by business unit, support group or service.

Module 3 — Service Desk

Since IT Service Management is oriented around the delivery of predetermined levels of service to end Users, it is sensible to install an organization whose fundamental directives are to:

- Support the Users as they require assistance in making use of services present in the IT environment.
- Monitor the IT environment for compliance with those predetermined service levels and properly escalate incidents in service delivery when they arise.

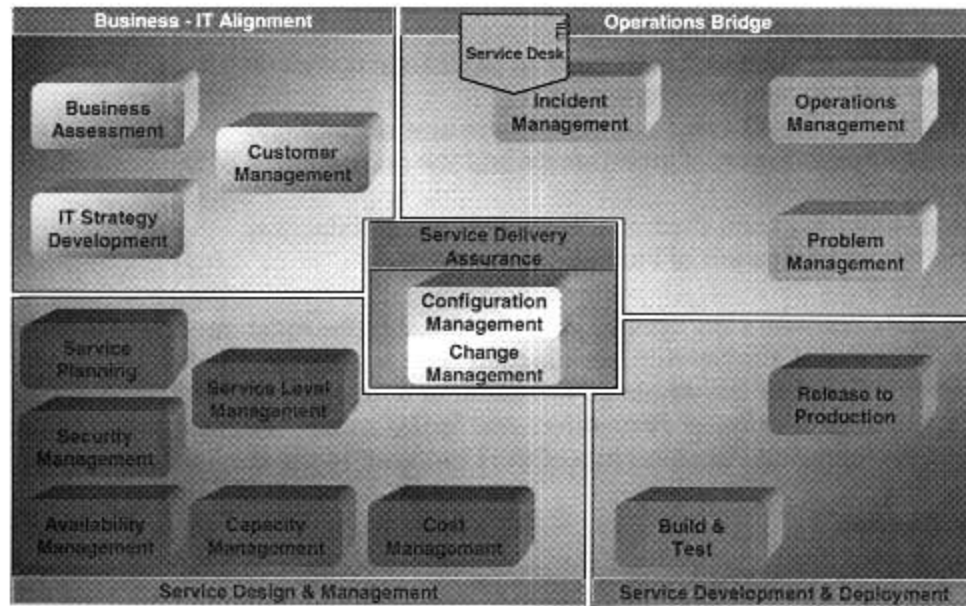
The Service Desk has traditionally been perceived as a sort of catchall collection of individuals who hopefully have the right technical expertise to answer virtually any type of question or complaint. As represented in ITIL, this Service Desk discipline has evolved to the point where it can be executed with a high degree of efficiency, accomplished via several factors:

- The "service" attitude is installed into the discipline's documentation, empowering the Service Desk staff to focus not just on "fixing this incident" but more on "immediately restoring service for the User".

Rigorous processes are defined to facilitate the Service Desk's staff activities.

Service Desk

Service Desk



Student Notes

Service Desk - Goals

The Service Desk provides a vital day-to-day contact point between Customers, Users, IT services and third-party support organizations. Service Level Management is a prime business enabler for this function. A Service Desk provides value to an organization in that it:

- Acts as a strategic function to identify and lower the cost of ownership for supporting the computing and support infrastructure.
- Supports the integration and management of Change across distributed business, technology and process boundaries.
- Reduces costs by the efficient use of resource and technology.
- Supports the optimization of investments and the management of the businesses support services.
- Helps to ensure long term Customer retention and satisfaction.
- Assists in the identification of business opportunities.

Strategically, for Customers the Service Desk is probably the most important function in an organization. For many, the Service Desk is their only window on the level of service and professionalism offered by the whole organization or a department. This delivers the prime service component of '*Customer Perception and Satisfaction*'. Internal to the IT function, the Service Desk represents the interests of the Customer to the service team

Other objectives are:

When a service has been interrupted, the goal of some processes is to restore the service. The Service Desk is the organization that facilitates the other processes. This means that the Service Desk is responsible for a service event from start to finish. While other functions - such as 2nd, 3rd line support - will assist for resolution the Service Desk retains "administrative" control over the incident. Another objective is to be the Single Point of Contact (SPOC) between Customers, Users, IT services and third-party support organizations for all IT related needs, questions, complains, remarks and changes

- The Service Desk should support business activities by understanding IT in a business context and suggesting improvements in service provision.
- The Service Desk will generate management reports.
- The Service Desk will communicate to the customer about there service calls.
- The Service Desk will promote their benefits to the entire organization.

Service Desk is **not** chartered with finding the root cause of a service interruption; that responsibility lies within Problem Management.

Service Desk — Goals

- *To provide a vital day-to-day contact point between Customers, Users, IT services and third-party support organizations*
- *To provide primary contact point for all Calls*
- *To facilitate the restoration of normal operational service with minimal business impact on the Customer within agreed service levels and business priorities*
- *To generate reports, to communicate and to promote*
- *To provide value to an organisation*

Student Notes

Service Desk - Responsibilities

The Service Desk has a lot of activities. The most important are:

- Receiving, recording, prioritizing and tracking service calls.
- Monitoring and status tracking of all registered calls.
- Escalation and referral to other parts of the organizations.
- Reporting about calls and quality of the desk.
- First Line Support (not for Call Centers).
- Keeping customers informed on request status and progress.
- Monitoring and escalation procedures relative to the appropriate SLA.
- Communicating planned and short-term changes of service levels to customers.
- Coordinating second-line and third-party support groups.
- Providing management information and recommendations for service improvement.
- Highlighting customer training and education needs.
- Closing incidents and confirmation with the customer.
- Contributing to Problem identification.

Providing Customers and Users with confirmation that their request has been accepted and its progress, is one of the most important roles of the Service Desk. Yet very few organizations have the staff resources to focus on and maintain this activity. As stated earlier, the use of technologies, such as email, will assist in this. However the real challenge is to create a personalized bond with customers, even through electronic communication.

Service Desk — Responsibilities

- *Receiving, Recording, Prioritizing and Tracking service calls*
- *Monitoring and Status Tracking of all registered calls*
- *Escalation and Referral to other parts of the organizations*
- *Reporting about calls on quality of the desk*
- *First Line Support (not for Call Centers)*
- *Keeping customers informed on request status and progress*
- *Coordinating second-line and third-party support groups*
- *Closing incidents and confirmation with the customer*

Student Notes

Different Desks

Call Center

A Call Center's emphasis is on handling large volumes of telephone-based transactions. Normally a Call Center will not react to those transactions but only register them and refer them to other parts of the organization.

Help Desk

The primary purpose is to manage, coordinate and resolve incidents, as quickly as possible and to ensure that no request is lost, forgotten or ignored. Links to Configuration Management and knowledge tools are generally used as supporting technologies. A Help Desk normally does not handle more than incidents. You can have a skilled and unskilled Help Desk. An unskilled Help Desk does not handling a lot of incidents, however it is not the same as a Call Center

Service Desk

The Service Desk extends the range of services allowing business processes to be integrated into the Service Management infrastructure. It not only handles Incidents, Problems and questions, but also provides an interface for other activities such as customer Change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management for IT Services, and IT Service Continuity Management.

Many Call Centers and Service Desks naturally evolve into Service Desks to improve and extend overall service to the Customers and the business. All three functions share common characteristics: they represent the service provider to the Customer and to the User (internal or external) they operate on the principle that customer satisfaction and perception is critical they depend on blending people, processes and technology to deliver a business service.

Different Desks

- **Call Center**

Handling large call volumes of telephone-based transactions, registering them and refering them to other parts of the organization

- **Help Desk**

Managing, coordinating and resolving Incidents as quickly as possible

- **Service Desk**

Allowing business processes to be integrated into the Service Management infrastructure. It not only handles Incidents, Problems and questions, but also provides an interface for other activities

Student Notes

Inputs and Outputs

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 could be: 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:

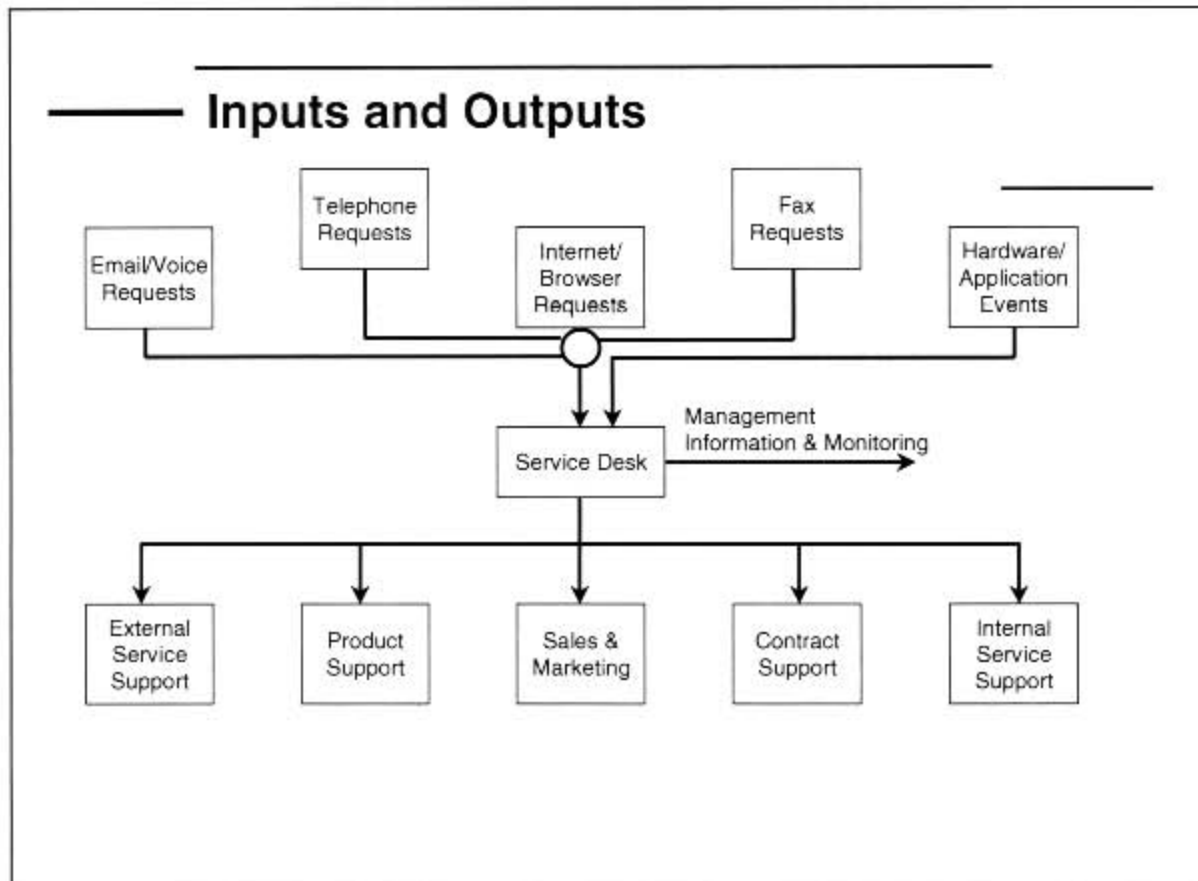
- Incident product purchases.
- Application queries.
- Requests for equipment moves, installations, upgrades and enhancements.
- Requests for consumables.

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

- Support personnel are freed from unnecessary telephone interruptions.
- Workloads are better managed.

The usage of form-based inputs increases the integrity of the data supplied and assists in allocation to the best-suited support specialist, team or department. The Service Desk tool should automatically provide the Customer or User with a receipted unique reference number, which also allows for online querying of the request's progress.

Providing Customers and Users with confirmation that their request has been accepted and its progress, is one of the most important roles of the Service Desk. Yet very few organizations have the staff resources to focus on and maintain this activity. As stated earlier, the use of technologies, such as email, will assist in this. However the real challenge is to create a personalized bond with customers, even through electronic communication.



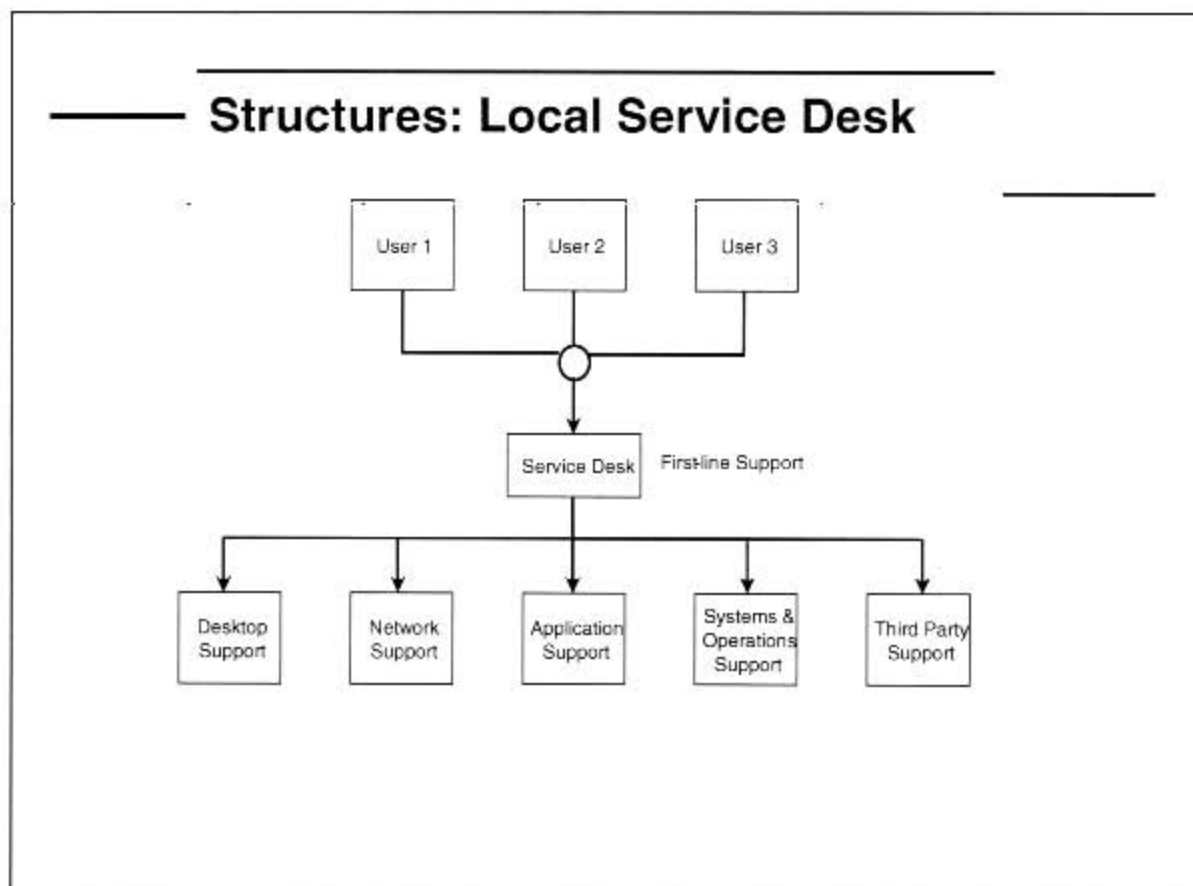
Student Notes

Structures: Local Service Desk

Traditionally, organizations have created local support desks to meet local business needs. Local Service Desks are also implemented for local support on site. If your organization is maintaining several local support desks, it is important that operational standards are introduced.

Considerations for implementing a local Service Desk structure include:

- Establishing common processes across all locations and, where possible, common procedures.
- Making localized skills known and available to other Service Desks.
- Ensuring compatibility of hardware, software and network infrastructure.
- Using the same escalation processes, and the same impact, severity, priority and status codes across all locations.
- Using common management reporting metrics.
- Using a (logically) common shared database.
- If available, putting in place the ability to pass or escalate requests between Service Desks, preferably automatically.



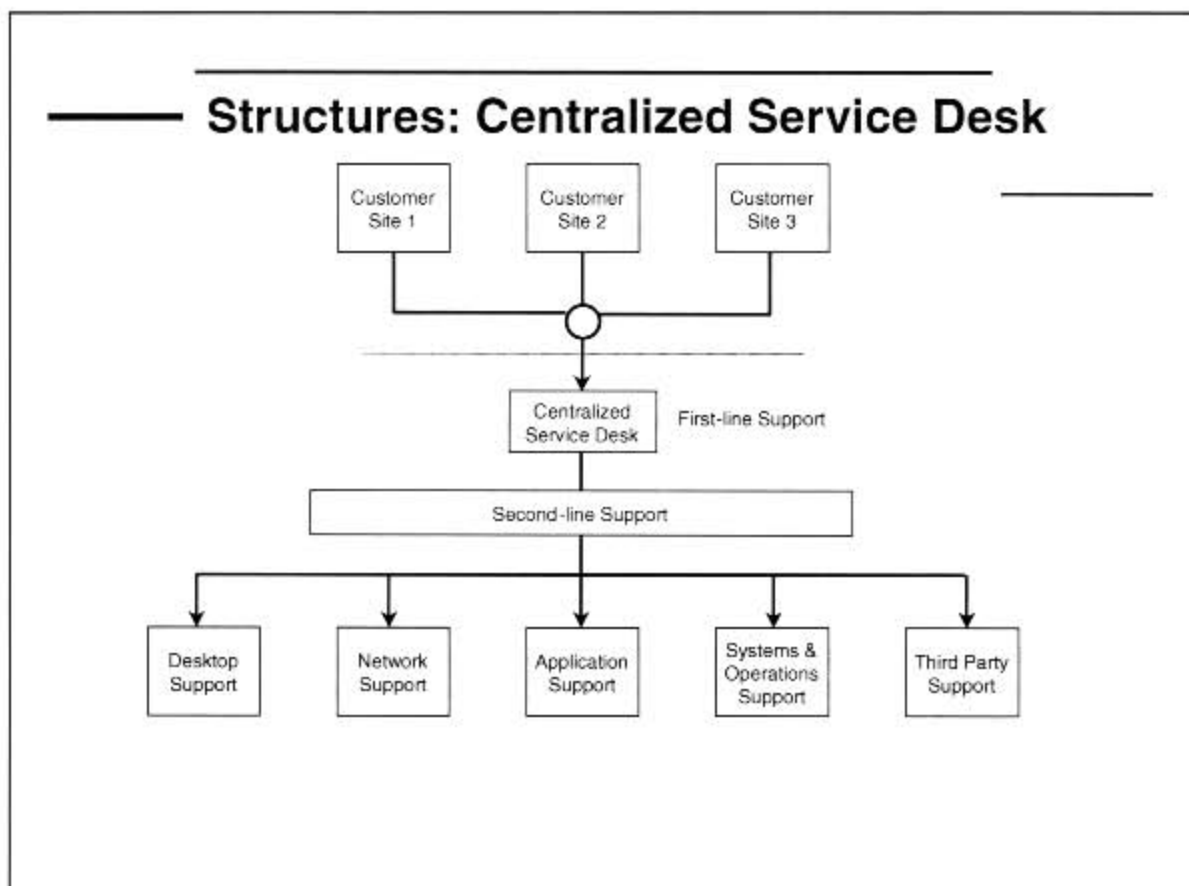
Student Notes

Structures: Centralized Service Desk

Local Service Desks are practical but because of multiple locations you are duplicating skills and resources and that is expensive. Therefore it is good to establish a central Service Desk if the kind of support allows it and if it is technically possible. In this option, all service requests are logged to a central physical location. If your organization has multiple locations, having a central support service has major business benefits, including:

- Reduced operational costs.
- Consolidated management overview.
- Improved usage of available resources.

Of course other parts of the services still have to be supported on location. That's why you see a lot of organizations where Local and Central desk are combined.



Student Notes

Structures: Virtual Service Desk

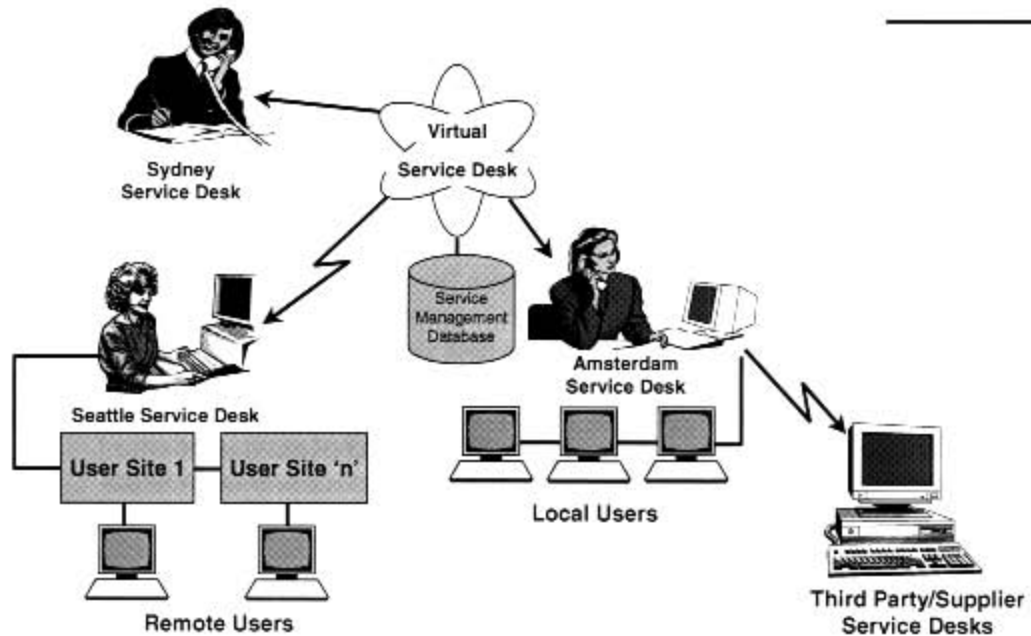
To a great extent the physical location of the Service Desk and the associated services are immaterial, due to advances in network performance and telecommunications. The 'Virtual Service Desk' can be situated and accessed from anywhere in the world. If your organization has multiple locations, a single global support Service Desk has similar business benefits to a Central Service Desk.

However, the prime operational restriction to the Virtual Desk is the need for a physical presence by a specialist or replacement engineer.

Considerations when setting up a Virtual Service Desk include the following:

- All persons accessing the Virtual Service Desk should use common processes, procedures and terminology.
- A common, agreed-on language should be used for data entry.
- Customers and Users still need to interact with a single point of contact. Consider global telephone numbers, local numbers that route to the Virtual Desk and Automatic Call Distribution (ACD) technology.
- There will be the need for a physical presence on site by a specialist or maintenance engineer from time to time.
- Network performance should be 'fit for purpose'. This should be reviewed in terms of forecast workloads. For example, if the local Service Desk in Holland is only handling ten requests a day, then network volume may not be a major consideration. However, a narrow bandwidth is not practical if several hundred requests are processed.
- For the Virtual Desk, the support tools in place should allow for 'workload partitioning' and authorized 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.
- Consistent ownership and management processes for Incidents should be used throughout the Virtual Service Desk, with automated transfers of Incidents and Incident views between local desks.

Structures: Virtual Service Desk



Student Notes

Considerations

Establishing a Service Desk is not easy. Therefore here some tips.

- First establish that the business need is clearly identified and understood. Without this it is very hard to implement a desk.
- Make sure management commitment, budget and resource are made available. All kinds of processes and procedures have to be implemented, tools have to be deployed and roles and responsibilities defined. Without management commitment this is not going to be enforced.
- Ensure the proposed solution aligns with your service support strategy
- Identify, achieve and communicate quick wins. Good public relations and fast results are going to help you to promote the desk.
- Define clear objectives and deliverables
- Start simple; don't try to do everything at once; Adopt a phased approach.
- Involve/consult your customers and end users Don't use jargon but speak their language. Talk with them about their expectations and explain them your objectives and task
- Sell the benefits to support staff. Tell them that one Single Point of Contact is also in their benefits. They will have more time to do the "real" work.
- Train IT staff to be service staff. Communication is one of the most critical success factors. Service Desk should not be technical focused but service oriented.
- Educate customers and users in the use of the new service and its benefits
- Advertise and 'sell' your service.

When preparing to set up a Service Desk, if possible, provide a room/location away from the main support area with:

- A pleasant and comfortable area for Customers and Service Desk staff
- A low noise environment
- Privacy
- Install a library of all your product, hardware and software documentation and reference material used by Customers
- Ensure an up-to-date Service Catalogue is available at all times
- Install conference phone facilities and hands-free units
- Provide seating and desk space for round-table discussion – this helps defuse any 'them and us' situation
- Provide beverage facilities to offer Customers, or at least easy access to them
- Publish to the Customer base the location of the unit and its operating times.

When considering the level of service and the environment being provided, ask yourself *'Is this how I would like to be treated?'*

Considerations

- The business need is clearly identified and understood
- Management commitment, budget and resource is made available
- Identify, achieve and communicate quick wins
- Define clear objectives and deliverables
- Start simple; don't try to do everything at once
- Involve/consult end users and customers and educate them on the new service and its benefits
- Sell the benefits to support staff
- Train IT staff to be service staff
- Advertise and 'sell' your service

Student Notes

Essentials

Goals. The main goals of the Service Desk are:

- To act as the SPOC between Users and IT Service Management.
- To facilitate the restoration of normal service as soon as possible. They are not concerned with finding the underlying root cause of incidents; this is the responsibility of Problem Management.
- To provide an interface for the other Processes, provide information on service performance, and to act as the marketing tool for IT.

Responsibilities

- The Service Desk plays a key role in the Incident Management Process by receiving, recording and tracking all incidents and service requests. They are responsible for all calls from registration to closure even when other parties are carrying out the resolution.
- Escalation Management. Telephone pick-up times and telephone talk times are key influencers on Customer perception, it is vital that, if these are in place they are communicated and monitored. The Service Desk is also responsible for managing urgent requests and service breaches. There should be clear procedures for all these situations
- Referral. A main responsibility is in making an initial assessment of requests, attempting to resolve them or passing them on to the relevant support group as outlined in the SLA.. They also

Support Changes. By providing an interface for RFCs and supporting the integration and management of change across distributed business, technology and process boundaries.

Inputs and outputs. Customer interaction is no longer restricted to the telephone and personal contact, email and the Internet/Intranet and fax can also be valuable tools. The usage of form-based inputs increases the integrity of the data supplied and assists in allocation to the best-suited support specialist, team or department. It is important to remember though, providing Customers and Users with confirmation that their request has been accepted and its progress, is one of the most important roles of the Service Desk. The real challenge is to create a personalized bond with customers, even through electronic communication.

Types of Service Desk. Selecting the right Service Desk structure will be dependent upon a number of factors. There is no “universal” configuration that will suit all. Flexibility is crucial however as when business requirements change the support needs to be adaptable enough to change with it. No matter what type of desk is in place, Local, Central or Virtual or any combination of these, all of the above goals, responsibilities etc. still apply.

Considerations. It is imperative that the business needs and goals have been clearly defined and understood. The second step is to gain management commitment at the most senior level to budget and resources. Next look at where you can make an immediate positive impact and gain some quick wins ensuring the benefits of your services are well defined, not only with the Customer but with IT management and other support staff. Make sure you communicate your objectives and give regular progress reports. Involve Users, Customers and other support staff whenever possible in process and procedure design. Provide training for everyone. Advertise and sell your service.

Essentials

- *Goals*
 - Provide a SPOC for all Users' requirements
 - Facilitate the restoration of normal service ASAP
 - Deliver high quality support to meet business goals
 - Support Changes, generate reports, communicate & promote IT
- *Responsibilities*
 - Receive, record & track all calls
 - Escalation and referral
 - Play a key role in the management of the incident lifecycle
- *Inputs & Outputs*
- *Types of Service Desk – Local, Central, Virtual*
- *Considerations*
- *Remember: The Service Desk is a function and not a process*

Student Notes

Module 4 — Incident Management

Since IT Service Management is oriented around the delivery of predetermined levels of service to end Users, it is sensible to install an organization whose fundamental directives are to:

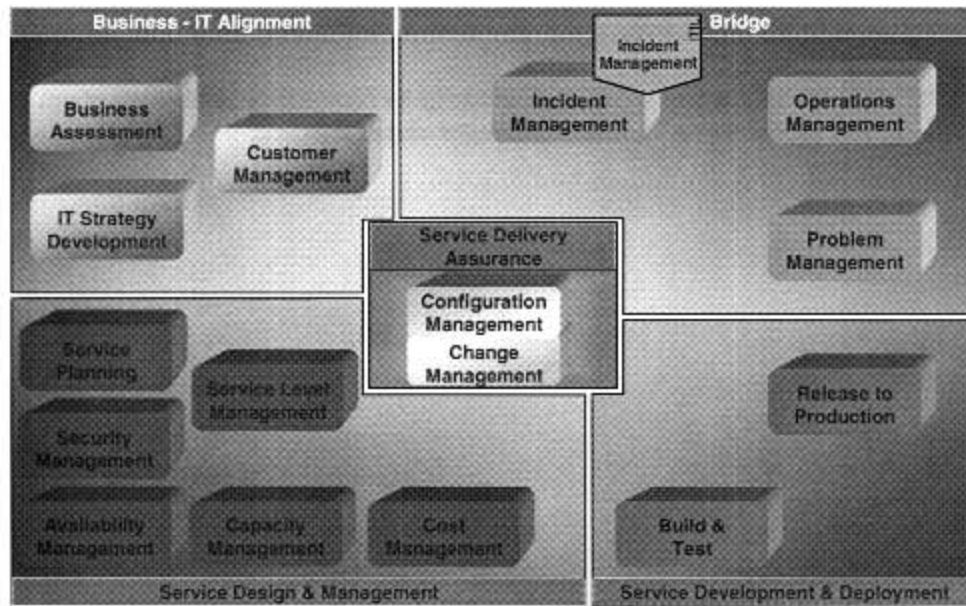
Monitor the IT environment for compliance with those predetermined service levels and properly escalate incidents in service delivery when they arise.

The Incident Management function has the responsibility to solve incidents as quickly as possible.

Indeed the importance of the Incident Management process can be summarized as follows: when a User experiences an incident the Incident Management process will make sure that the User's service will be on-line again as quickly as possible.

Incident Management

Incident Management



Student Notes

Incident Management - Goals

The main objective Incident Management is to:

- Resolve the service event as quickly as possible, at least within the targeted time as documented in the service level agreement.
- To keep communication going between the IT organization and their customer about the status in relation to a service event (e.g. Escalation, estimated time until solved etc).

Evaluate an incident to determine whether it is likely to reoccur or is the symptom of a chronic problem. If it is, inform a Problem Manager about this.

Incident Management — Goals

- *To restore normal service operation as quickly as possible*
- *Minimize the adverse impact on business operations*
- *Ensuring that the best possible levels of service quality and availability are maintained according to SLA's*



Student Notes

Incident Management – Responsibilities

Incident detection and recording.

The Service Desk is responsible for recording and monitoring the resolution of all incidents; this is a very reactive process. To enable effective and efficient reaction a formal method of working must be implemented. At this point they record basic details of the Incident, alert specialist support groups as necessary and start procedures for handling the service request.

Classification of all incidents and initial support.

This is the process of identifying the reason for the incident and hence the corresponding resolution action. Here the CMDB can be checked for known errors and problems, an assessment of the impact and urgency can be made to help define priority and some initial support given. Typically the initial support could be providing a work around. Many incidents are regularly experiences and the appropriate resolution actions are well known.

Investigation and diagnosis.

After an initial assessment of the Incident further related information is collected and analyzed. The investigation and detection may become an iterative process, starting with a different specialist support group and following elimination of a previous possible cause. It may involve multisite support or even outside vendors. It demands a rigorous, disciplined approach and detailed recording of actions taken with corresponding results.

Resolution and recovery.

The Incident has been successfully resolved or circumvented or a RFC has been raised.

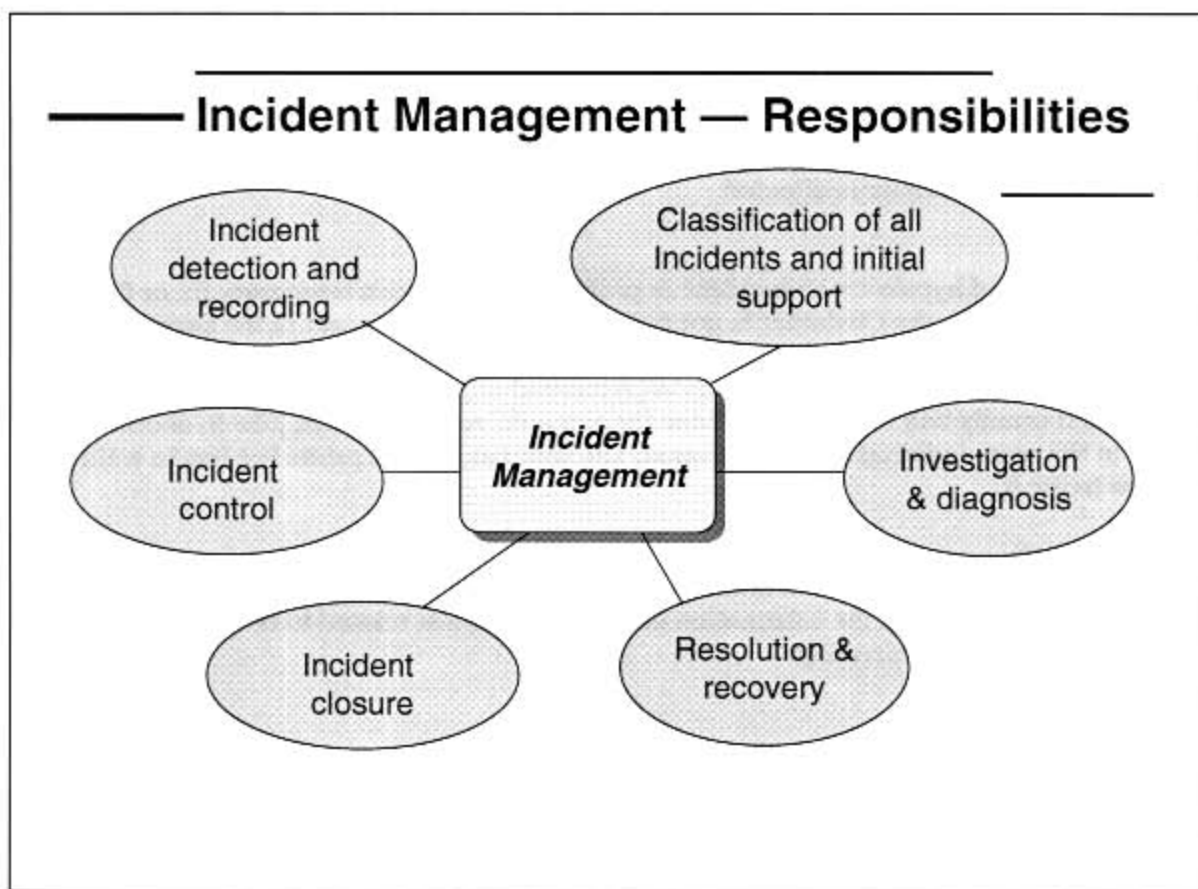
Incident closure.

This can only be done once the User is satisfied with the resolution or work-around. At this stage the Service Desk should ensure that:

- details of the action taken to resolve the Incident are concise and readable
- classification is complete and accurate according to root cause
- the resolution is agreed with the Customer
- all details applicable to this Incident are recorded

Incident control.

See the Incident Life Cycle slide and notes that follow.



Student Notes

Terminology

Incident

Any event that is not part of the agreed service is called an incident. Most of the time this incident interrupts the service, occasionally it only reduces the service. In 99 out of 100 cases the incident has already interrupted or reduced the level of service...but in that one time staff can see it coming. Even then it is necessary to register the incident but hopefully it can be solved before the customer is affected.

Workaround

This is a method of bypassing an incident or problem either from a temporary fix or from a technique that means the Customer is not reliant on a particular aspect of the service that is known to have a problem. It is usually the first solution that restores the service. It is not a permanent solution but something that is implemented to get the service up and running. A workaround usually will reduce the service for example: rerouting print jobs to another printer in the same building is a workaround. The user can get the prints but has to walk a distance to get it.

Service Request

This can be surmised as every incident not being a failure in the IT Infrastructure. A service request could be a request for information or a change request related to one of the services that an organization is delivering.

Terminology

- **Incident**

Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service

- **Work-Around**

Method of avoiding an Incident or Problem

- **Service Request**

Every Incident not being a failure in the IT Infrastructure

Student Notes

The Incident Life Cycle

Incident Detection & Recording.

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

Registration of data according to the interruption or reduction of the service is very important for:

- Tracking the incident throughout the whole incident life cycle.
- Adding useful information that can help, inform and assist support organizations so they are able to find a solution or a workaround (sooner).
- Gathering historical information for future use.
- Collecting information (e.g. For reports) about number of incidents, efficiency, availability and trend analysis and other management purposes.

Classification and Initial Support.

The Service Desk determines the priority of incidents as they receive them. In consultation with the Customer, the Service Desk will calculate the priority from the impact and urgency of the incident. Recording priorities in a SLA then making that SLA available to the Service Desk staff can greatly assist this step in the life cycle. The call is categorized (e.g. hardware, software) and the Service Desk operator should carry out incident matching.

Consulting the CMDB is necessary to get more information about the service that is interrupted, the SLA data, the CI's that are related to this service and hopefully related past incidents, know errors and change records.

Service Request or Incident.

If the call is a Service Request then the Service Desk operator follows the appropriate Service Request procedure. If it is an incident, after providing some initial support (assess incident details, find quick fixes) they will resolve it or forward it on to 2nd or 3rd line support for further investigation.

Investigation and Diagnosis.

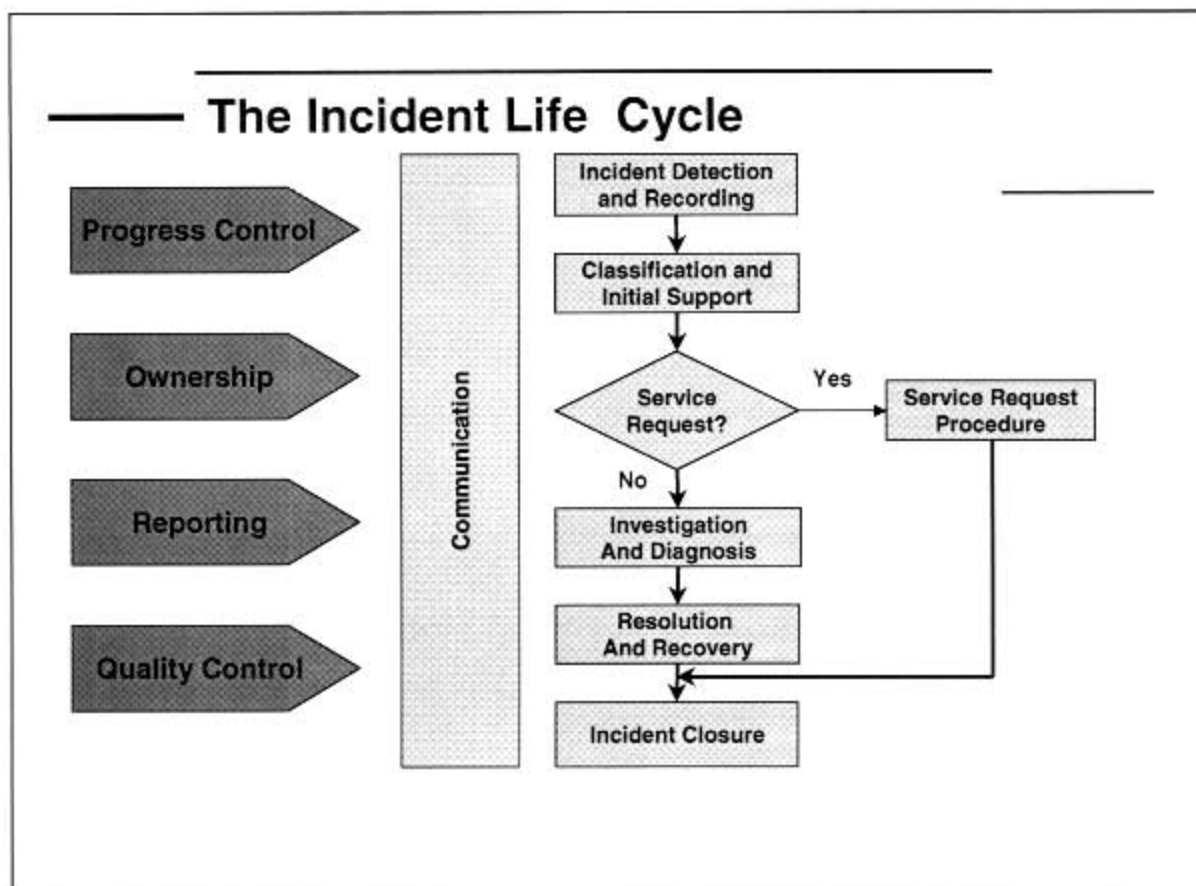
Other support groups will start analyzing the incident with the only purpose to find a permanent solution, or - if this is not possible - to find a workaround.

Resolution and Recovery.

After successful execution of the resolution or some circumvention activity, service recovery can be affected and recovery actions carried out, often by specialist staff (2nd or 3rd support). The Incident Management system should allow for the recording of events and actions during the resolution and recovery activity.

Incident Closure.

If a permanent solution or a workaround is found this is implemented and the service restored. The solution group will inform the Service Desk staff who will liaise with the customer to check if the offered solution / workaround has restored the service to their satisfaction. If this is the case then the Service Desk staff can close the incident.

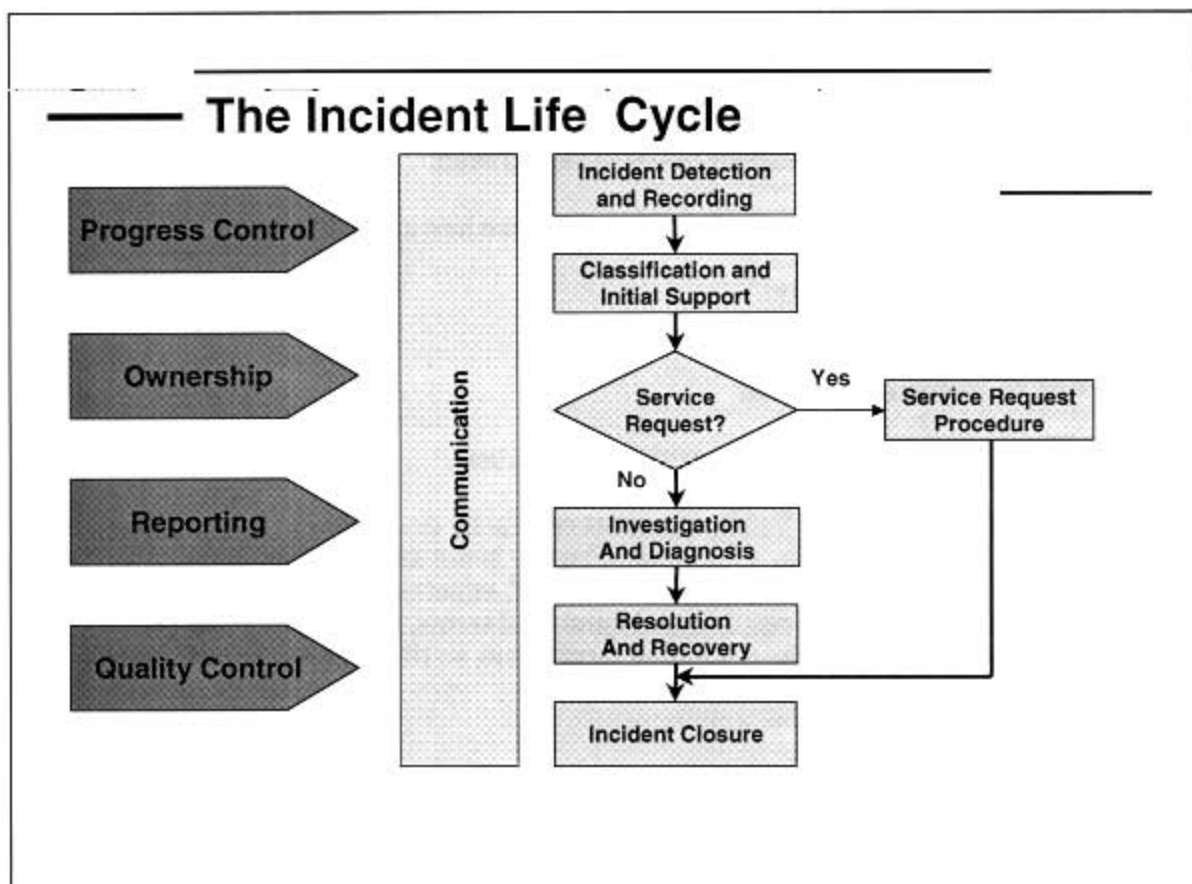


Student Notes

Module 4

Incident Management

Throughout the whole process the Incident Manager has a responsibility to track and monitor progress and quality as well as providing necessary reports. In most cases the Incident Management role will be taken on board by the Service Desk Manager. The Service Desk also has a responsibility to keep the Customer / User informed at all times about the progress of the call.



Student Notes

Classification - Prioritization

The Service Desk determines the priority of incidents as they receive them. In consultation with the Customer, the Service Desk will calculate the priority from the impact and urgency of the incident, considered against the criteria described in the Service Level Agreement. Impact is determined by the effect upon the activities of the business and urgency is determined by how quickly the incident needs to be resolved.

When determining priority Service Desk staff should take into consideration:

- Potential cost of non resolution,
- Threat of injury to customers or staff,
- Legal implications,
- Disruption to customers and staff

Impact is NOT about the technical complexity of resolution.

By prioritizing calls at this point, 2nd line support can easily determine which calls need more urgent attention than others and in what order. Priority is not simply about queuing incidents for resolution; it is also about the resources (time, staff, expertise, research and 3rd party support) that will be allocated to resolution. In practical terms, sometimes a low priority incident may be allowed to miss its resolution target time, so that a higher priority incident can be dealt with within target.

Classification — Prioritization

- *Impact*
 - Evidence of effect upon business activities
 - Service Levels in danger
- *Urgency*
 - Evidence of effect upon business deadlines
- *Prioritize resources*
 - Manpower
 - Money
 - Time

Student Notes

Classification - Categorization

The categorization of incidents can produce a first step towards problem definition. This demonstrates the need for Incident Management and Problem Management to establish common categorization terminology.

Appropriate categories should be created both for recording reported incidents (usually in Customer terms) and for recording the finally detected causes (usually in technical terms).

Categorization of incidents and problems and creative analysis may reveal trends and lead to the identification of specific problem areas that need further investigation.

Examples of incident categories are:

- Application
 - Service not available
 - Application bug/query
- Hardware
 - Automatic alert
 - Printer not printing
- Service Request
 - Password forgotten
- Security Incident
 - Virus

Classification — Categorization

Examples of Incident categories are:

- *Application*
 - Service not available
 - Application bug/query
- *Hardware*
 - Automatic alert
 - Printer not printing
- *Service Request*
 - Password forgotten
- *Security Incident*
 - Virus

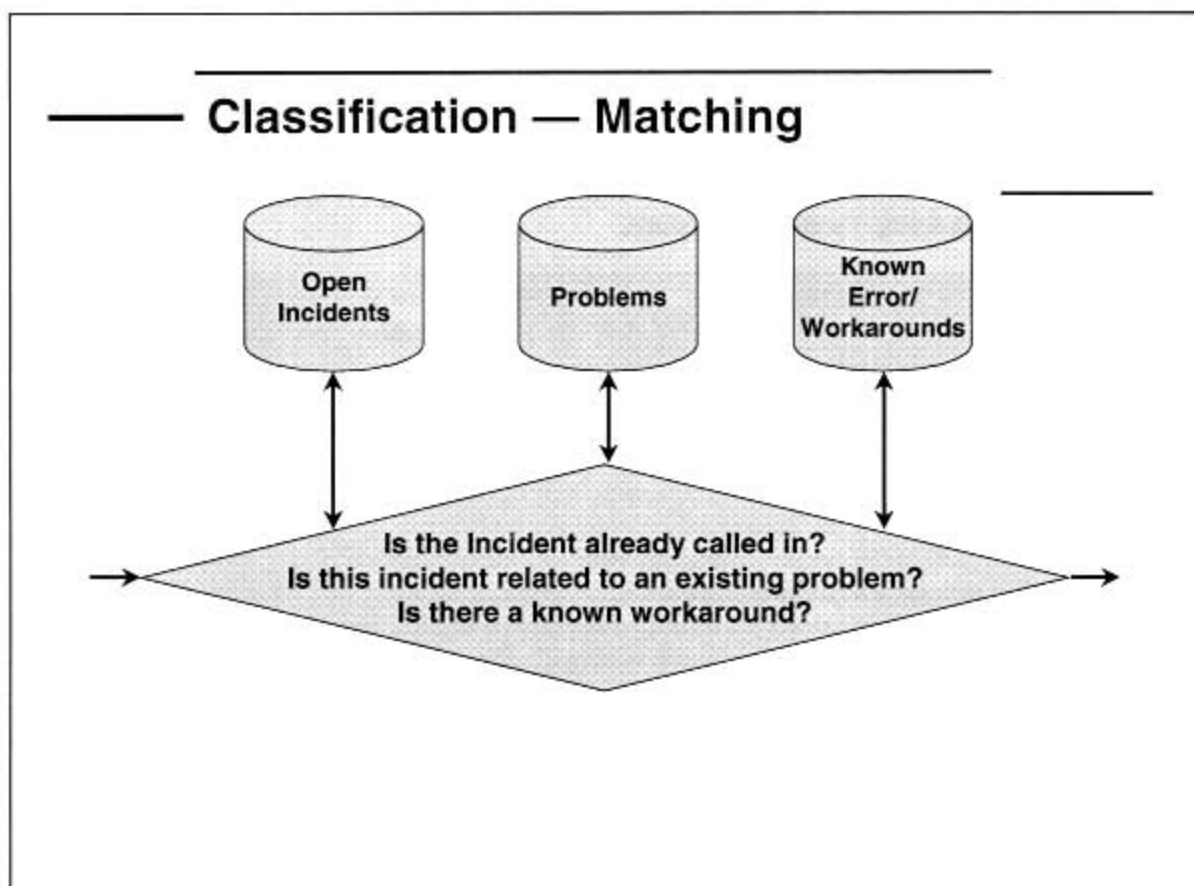
Student Notes

Classification - Matching

After categorization the incident should be matched with the incident, problem and known error database to see if any incidents with the same or similar symptoms already exist. If they do exist most likely there is a workaround that can be used to restore the service. Another alternative is that there is an outstanding incident that the new one can be related to. For example:

A user contacts the Service Desk to inform them he is having problems sending emails, the call is recorded. The Service Desk then receives five more calls from five different users all experiencing the same problem. In this situation the five new calls can be "related" to the first incident.

If the incident cannot be matched then it is a unique incident and must be recorded as such.



Student Notes

Routing Incidents

Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups. These support groups generally have more specialist skills, time or other resources to solve incidents. In this respect, the Service Desk would be first-line support.

The diagram opposite illustrates the different roles played during the Incident Life Cycle. Below demonstrates a step by step procedure.

Step 1: Attempt to resolve Incident by the service desk:

Perform initial evaluation and search for solution or workaround. If solution is found close the incident. If not refer to the next level.

Step 2: Assign Service Call to 2nd line support:

If no solution can be found at the service desk refer to second line support. If 2nd line support can find solution, refer back to service desk who will close the incident. If not refer to the next level

Step 3: Assign Service Call to 3rd line support:

If no solution can be found at the 2nd line support refer to third line support. If 3rd line support can find solution, refer back to service desk who will close the incident. If not refer to the next level.

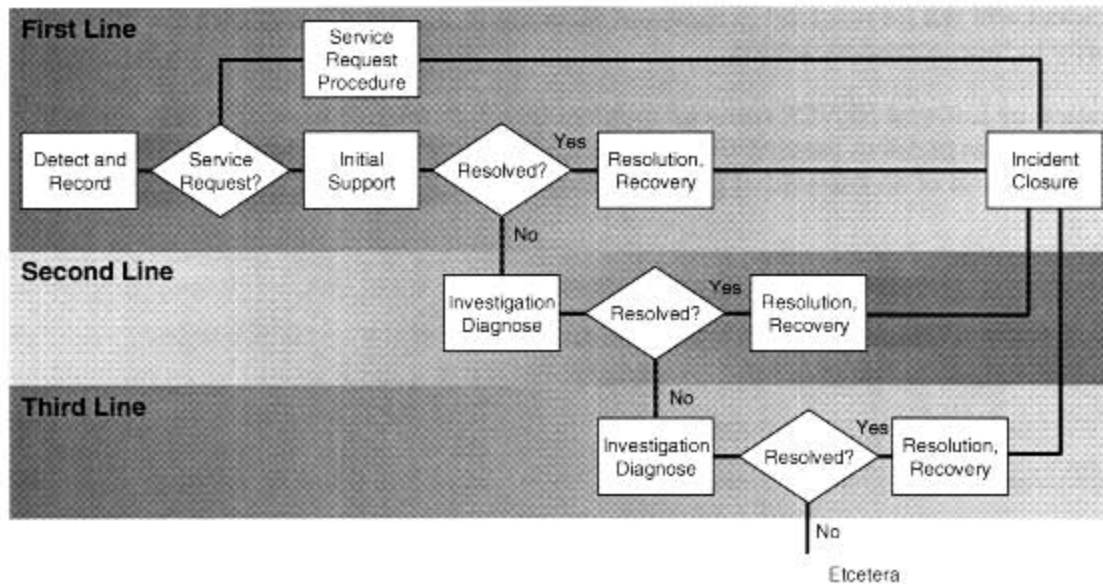
Step 4: Assign Service Call to Specialist:

If no solution can be found at the 3rd line support refer to a specialist. If the specialist can find solution, refer back to service desk who will close the incident.

If it is not clear which support group should investigate or resolve a User-related incident, the Service Desk, as the owner of all incidents, should coordinate the Incident Management process. If there are differences of opinion or there are any other issues arising, then the Service Desk should escalate the incident to the Problem Management team.

Note that third- and/or second-line support may include external suppliers, who can be given direct access to the incident registration tool.

Routing Incidents



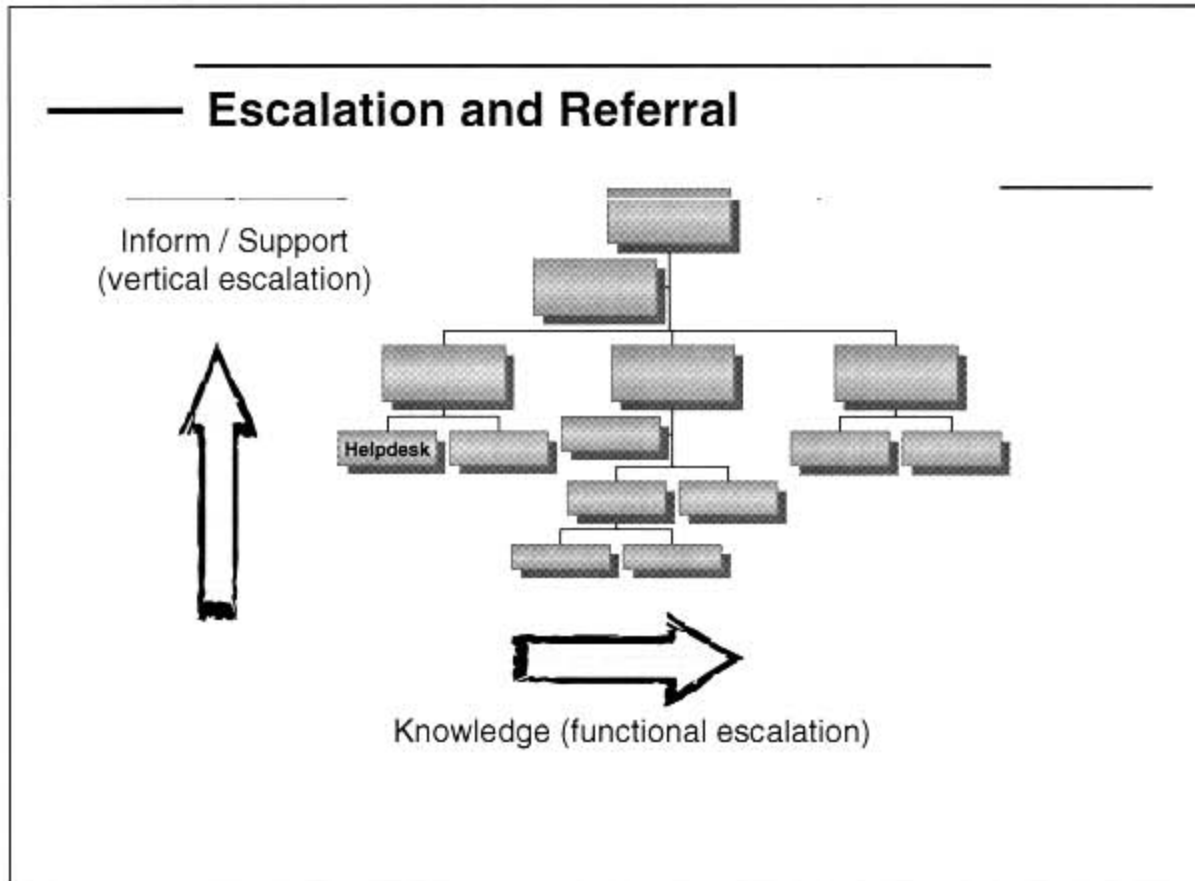
Student Notes

Escalation and Referral

Incident routing is called horizontal escalation or referral and primarily takes place because of a lack of knowledge or expertise. When referring incidents care should be taken by the Service Desk that SLA resolution times are not exceeded.

Hierarchical or vertical escalation can take place at any moment during the Incident Life Cycle. It usually occurs when major incidents are reported or when it becomes apparent that an incident will not be resolved in time and SLAs are in danger. This allows the relevant authority to take corrective action.

Escalation or Referral NEVER turns an incident into a problem, although it may result in ownership of an incident passing to the Problem Manager for administrative reasons and/or the identification of an associated problem. Problems are NOT simply very serious incidents.



Student Notes

Essentials

Goals

The goals of Incident Management are to remedy as quickly as possible failures or potential failures in the service to customers. Customers should suffer as few failures as possible and must be able to continue their daily work as quickly as possible.

The Incident Management process also plays a role in ensuring service quality and that agreed service levels are met.

Responsibilities

Usually there is a clear point of contact in the organisation, where the customer can obtain information and report incidents: in ITIL this is the Service Desk.

After the customer has reported an incident, or after receiving such a report from an automated system, the Service Desk records the relevant data in as much detail as possible. Recording is important in order to keep an eye on the status of incidents. Further, the Service Desk sets priorities for the solving of the incident and categorizes it for resolution and referral. Subsequently it will try to match it: i.e. it will check whether similar incidents have occurred before and what solution was then applicable. If the incident has not occurred before, the Service Desk, possibly supported by a 'second line' member of staff, will carry out an investigation in order to resolve the incident. If the incident manager does not succeed in concluding the investigation within the set criteria (for example, time, lack of expertise), the problem management process will be initiated. The most important thing is to resume the service to the customer as quickly as possible. The incident can be closed only after the customer is satisfied.

As a result of these procedures, there is a clear point of contact for the client as well as insight into the incidents occurring and a guarantee that service will be resumed as quickly as possible.

Essentials

- *Goals*
 - Restore service ASAP whilst minimizing impact
 - Ensure service quality and availability meet SLA's
- *Responsibilities*
 - Incident detection & recording
 - Classification and initial support
 - Investigation & diagnosis
 - Resolution & recovery, Incident closure
 - Incident Control
 - Incident ownership, monitoring, tracking & communication
- *Concentrates on Incident Lifecycle Management*
- *Classification – Priority & Category & Incident Matching*

Student Notes

Management Reporting

Reporting is VERY important. Quality Improvement is fundamentally based on INFORMATION; there will be no information without high quality registration and flexible reporting.

- For the Service Level Managers / Account Managers it is vital to have reports for their customers, that can give information about performance in relation to the agreed performance in the SLA's. This information also provides input for negotiation of the service levels in future SLA's.
- For (incident) management it is important to know about how the Service Desk / incident management process performs. How effective is the staff with handling calls. Did they refer the calls to the right support group? How many incidents were solved within the Service Desk / 1st line support? Were the terms in the SLA met?
- For other parts of the organization and the process managers it is important to know how reliable CI's are. What the downtime was on CI's? What type of incidents occurred? Were incidents related to bad changes, capacity issues or security issues?

Suggested reports:

Daily reviews of individual Incident and Problem status against service levels. E.g. areas requiring escalation by group; possible service breaches; all outstanding Incidents.

Weekly management reviews. E.g. service availability; major Incident areas; related Incidents that require Problem records to be generated; Known Errors and required Changes; service breaches; Customer satisfaction; trends; major services affecting the business; staff workloads.

Monthly management reviews. E.g. service availability; overall performance, achievements and trend analyses; individual service target achievements; Customer perceptions and levels of satisfaction; Customer training and education needs; support staff and third-party performance; application and technology performance; content of review and reporting matrix; cost of service provision/failure.

Proactive service reports. Consider the following reports to aid this:

- Planned changes for the following week
- Major incidents/problems/changes from the previous week
- 'Unsatisfied' customer incidents from previous weeks
- Previous weeks' poorly performing infrastructure items (e.g., server, network, application).

Module 5 — Problem Management

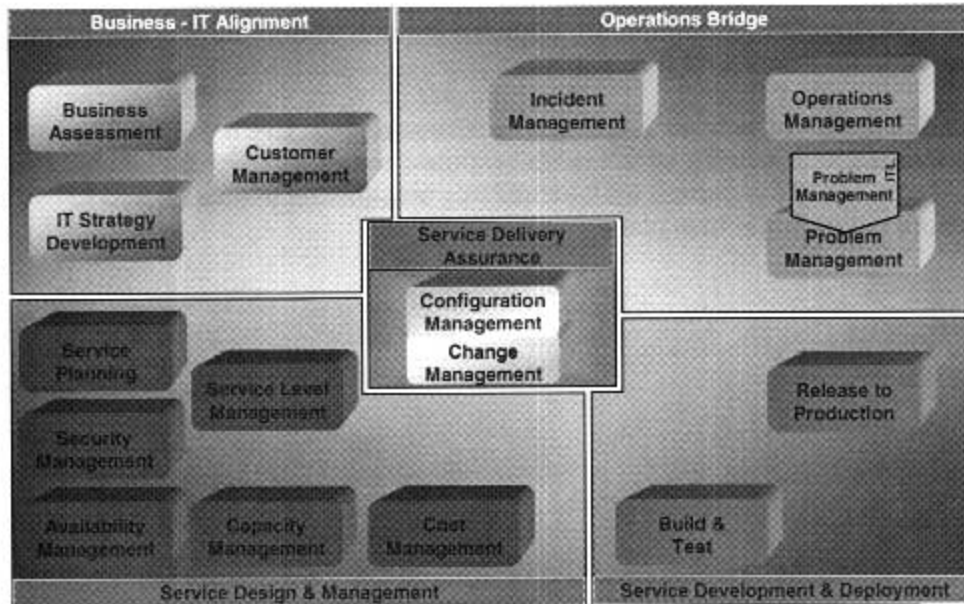
This module introduces the ITSM discipline of Problem Management, which is aimed at handling all types of failed IT services. Its main objective is to identify the root causes of those failures and recommending changes in Configuration Items (CIs) to Change Management. The Problem Management processes use information collected from a variety of other areas, including Incident Management and Change Management.

Problem Management focuses on these areas:

- Problem control: getting to the root cause of incidents,
- Error control: correcting problems, management information related to problems, and known errors

Problem Management

Problem Management



Student Notes

Problem Management - Goals

The first objective of Problem Management is to minimize the adverse impact of incidents and problems on the business that are caused by errors within the IT Infrastructure. The second one is to prevent recurrence of incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation. Part of Problem Management's responsibility is to ensure that previous information is documented in such a way that it is readily available to first-line and other second-line staff.

The Problem Management process has both reactive and proactive aspects. The reactive aspect is concerned with solving problems in response to one or more incidents. Proactive Problem Management is concerned with identifying and solving problems and known errors before incidents occur in the first place.

Problem Management — Goals

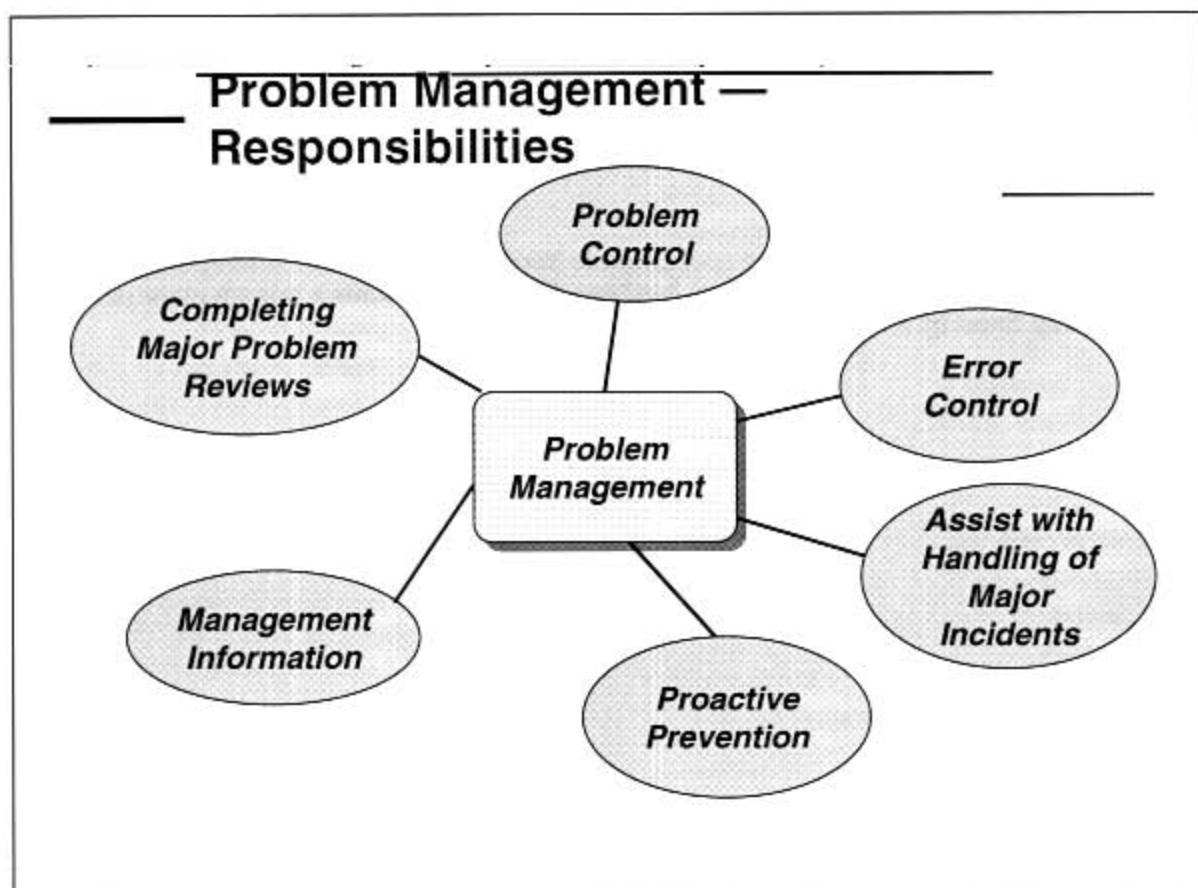
- To minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure
- To prevent recurrence of Incidents related to errors
- Improve productive use of resources



Student Notes

Problem Management – Responsibilities

- *Problem Control.* This part of the process is where problems are identified and recorded. Each problem is then classified before being allocated to the appropriate support group who will perform root cause analysis in order to find a permanent solution.
- *Known Error Control.* This part of the process is about controlling the known errors and generating RFC's to Change Management to remove the known errors from the infrastructure. It maintains the knowledge and known error / workaround databases. It publishes the known errors so that the Incident Process can solve incidents sooner and it will investigate whether or not problems and/or known errors are also present in other parts of the controlled infrastructure.
- *Assist with handling of major incidents.* Major incidents are those that have an extreme impact on the User community. The Service Desk notifies the Problem Manager who, in these circumstances, should arrange a formal meeting with relevant support staff.
- *Proactive Prevention:* Prevent the introduction of new incidents, problems. For example, preventative maintenance, communicating with other departments such as software development, and trend analysis.
- *Identifying Trends.* This part of the process it to do with actively monitoring incidents and, with the use of statistical methods tries to identify trends so that problems can be recognized. Trends alone are usually not enough to identify a problem. Some human expertise is necessary to determine if the trend actually leads to a problem.
- *Management info.* Creates reports about the effectiveness and performance of Problem Management and supplies this information to management and other processes
- *Completing major problem reviews.* Problem management files requests for change. Only after the implementation of a change the determination can be made whether the change actually did what problem management hoped for: the reduction or elimination of incidents. The Post Implementation Review (PIR) checks if that is the case.



Student Notes

Terminology

Problem

Unknown root cause of one or more incidents.

It can also be described as a condition identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident.

Known Error

An incident or problem for which the root cause is known and for which a temporary workaround / fix or a permanent solution has been found. It remains a known error unless it is permanently fixed by a change.

Terminology

- *Problem*
 - The unknown root cause of one or more incidents (not necessarily - or often - solved at the time the incident is closed)
- *Known Error*
 - A condition that exists after the successful diagnosis of the root cause of a problem when it is confirmed that a CI is at fault. (The error is removed by implementing a change)

Student Notes

Problem Control

Identification the ways to identify a problem are:

- If there was an incident with considerable impact that has been solved the Problem Manager should immediately register a problem right so an investigation can be launched to find the root cause.
- During trend analysis a number of incidents with similar symptoms may be discovered.
- Someone discovers a source of potential problems.
- If an incident is closed with the code "workaround"
- If a problem is forwarded from another domain.

Classification The step to collect data so the problem can be categorized and prioritized:

- Which CI's are involved?
- What are the related incidents?
- What are the symptoms?
- What are the causes?
- What are the resolutions / work around?
- What are the changes related to this CI's?
- What service levels are related?
- What is the danger?
- Which customers are involved?
- How much time do we need to (hopefully) find an answer (both duration and effort)?
- How urgently needs the problem to be solved?
- How high is the possible positive benefit if we solve the problem (impact)?

Assign Resources

Classification (categorization and prioritization) of a problem enables the appropriate resources to be assigned (or reassigned). This ensures that problems are handled efficiently and effectively, it also highlights those with the highest business impact.

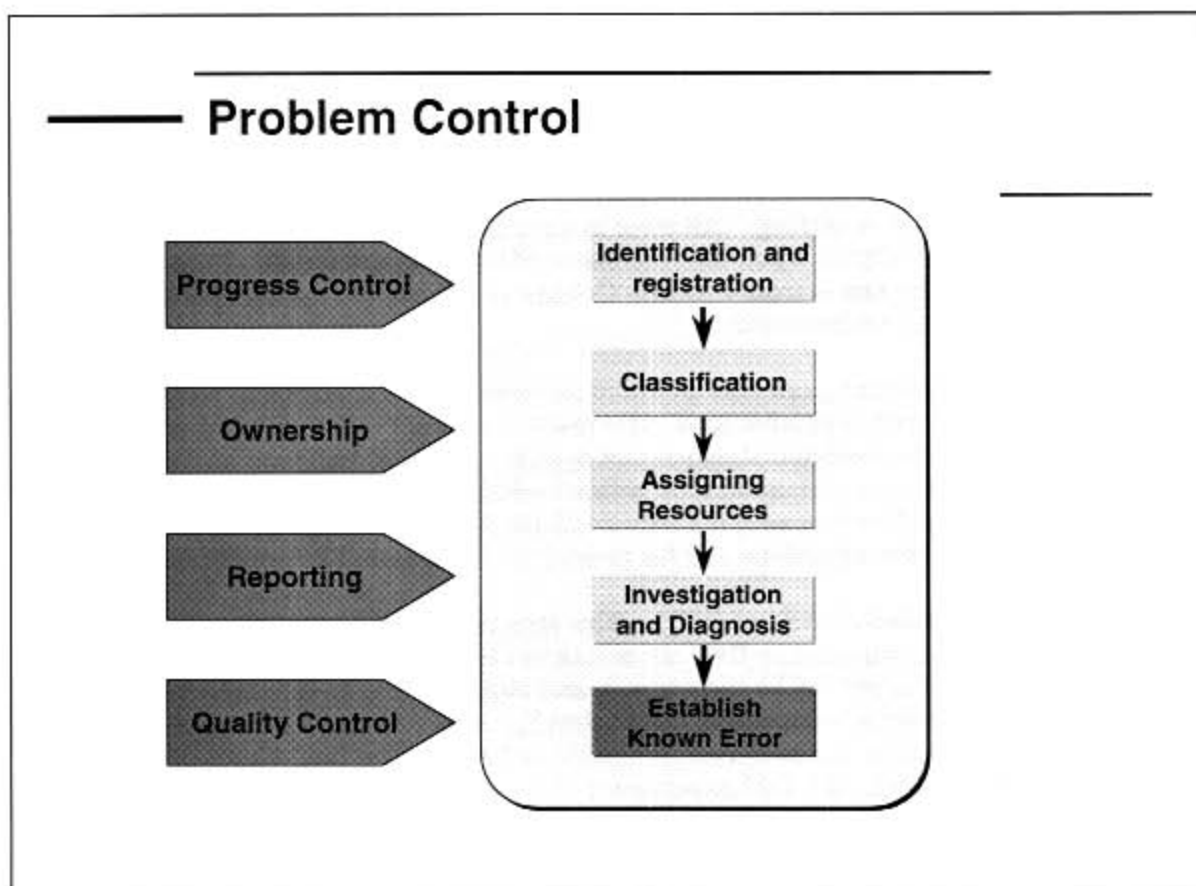
Investigation and diagnosis

The aim of investigation and diagnosis is to detect the underlying cause of one or more incidents. Investigation activities should include available workarounds for the incidents related to the problem, as registered in the incident record database. Records of recent changes should also be interrogated, because these may provide pointers to the cause. Historical information of CI's (from the CMDB) could be useful as well.

Establish Known Error

After the previous phase the known error will be determined. This phase records that known error and routes the error to the error control process.

Throughout the whole process the Problem Manager has a responsibility to track and monitor progress and quality as well as providing necessary reports.



Student Notes

Error Control

Known Error control is responsible for the registration, monitoring and handling of all known errors right from the start (the identification) until the successful implementation of the change has taken away the root cause.

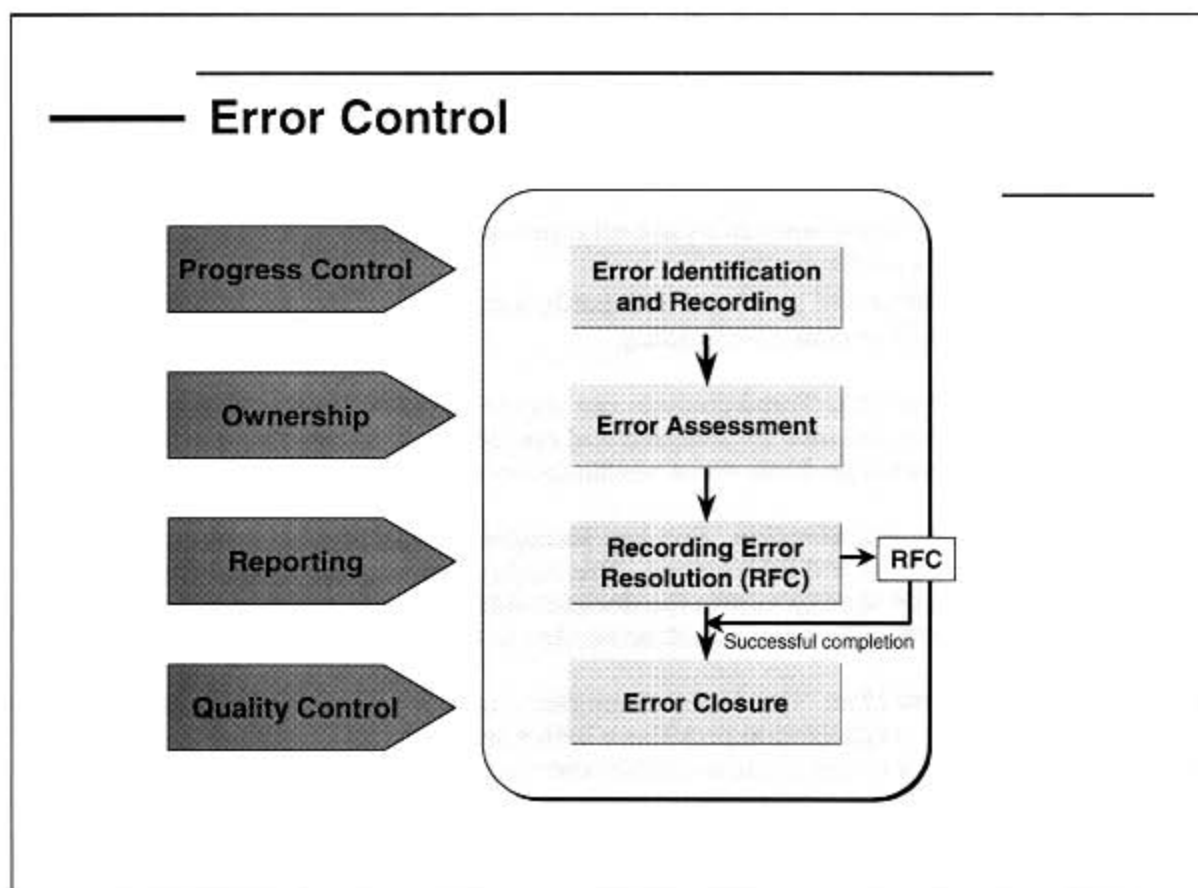
The steps are:

Error identification and recording. An error is identified when a broken CI is detected. A Known Error status is assigned when the root cause of a Problem is found. There are two sources of known errors, one is from Problem Control of the live environment and the other is from the development environment.

Error assessment. This step performs an initial assessment of the means of resolving the error, in collaboration with specialist staff. The resolution process for each known error should be recorded in the Problem Management system. It is vital that data on the CIs, symptoms, and resolution or circumvention actions relating to all known errors is registered in the Known Error database because it's then available for incident matching, providing guidance during future investigations and for providing management information.

Recording error/resolution (send out RFC). This step records the resolution process for each known error and completes an RFC according to Change Management procedures. The priority of the RFC is determined by the urgency and impact of the error on the business. The RFC identifier should be included in the Known Error record and vice versa in order to maintain a full audit trail, or the two records should be linked. The final stages of error resolution – impact analysis, detailed assessment of the resolution action to be carried out, amendment of the item in error, and testing of the Change – are under the control of Change Management.

Error Closure. Following successful implementation of changes (determined by a Post Implementation Review) to resolve errors, the relevant known error record is closed, together with any associated incident or problem records.



Student Notes

Proactive Problem Management (Proactive Prevention)

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

- *Trend analysis.* Incident and problem reports can provide information for proactive measures to improve service quality. Incident and problem analysis can identify trends such as:
 - The post change occurrence of a particular problem type.
 - Initial faults of a particular type.
 - Recurring incidents and problems with particular CIs.
 - The need for staff or customer training.
- *Targeting support action.* Trend analysis can lead to the identification of faults in the IT infrastructure, which can then be analyzed and corrected. It can also lead to the identification of general problem areas needing more support attention.
- *Informationing the organization.* Problem Management can provide information on problems, known errors and RfCs issued. This helps determine the health of the business and the details can be used to inform the decision making process within the organizations and other Processes such as Service Level Management and Service Desk.

By redirecting the efforts of an organization from reacting to large numbers of incidents to preventing Incidents, an organization provides a better service to its Customers and makes more effective and efficient use of the available resources within the IT support organization.

Proactive Problem Management (Proactive Prevention)



Student Notes

Incidents versus Problems

Incidents and problems (and changes) are separate entities. An incident never becomes a problem.

The slide shows a model in which incidents, problems and even changes can be alive simultaneously.

Start: Only an incident

When an incident occurs, the Incident Management process will try to solve the incident as quickly as possible. The incident can only be closed when the incident is resolved to the Customer's satisfaction. If during the incident investigation phase no solution is found, then the Incident Management process seeks the help from Problem Management, so the root cause of the incident can be determined.

Investigated and Escalated: Incident and Problem exist simultaneously

Problem management defines a problem with high urgency and immediately assigns resources. Those resources diagnose the problem and find the root cause of the underlying incident.

Diagnosed: Incident, Problem and Known Error exist simultaneously

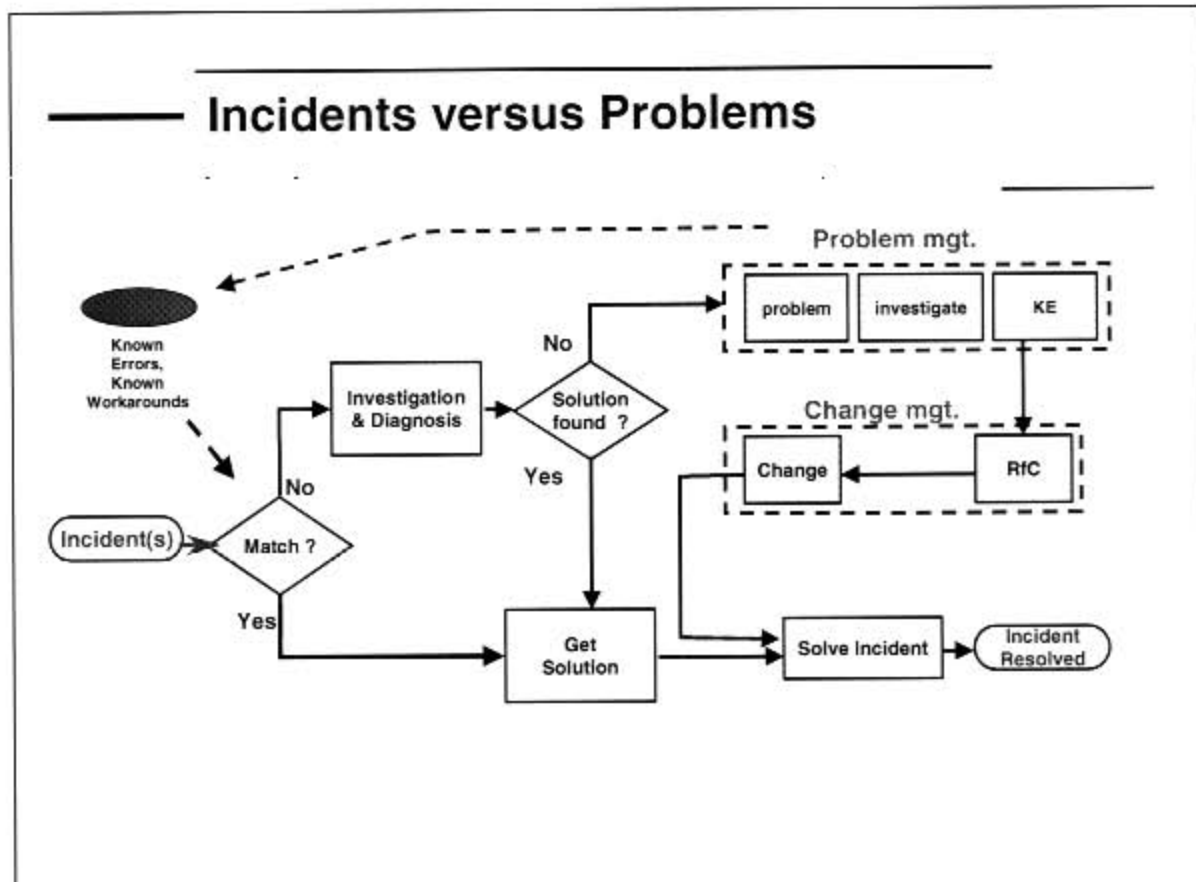
A known error is defined and, after figuring out how to solve it, an RFC is raised to change management to resolve the situation.

Change underway: Incident, Problem, Known Error and Change exist simultaneously

The change is implemented successfully. The Post implementation review shows that the change actually eliminated the known error successfully. Investigation also shows that the incident has been solved and so the problem, opened for this reason can now be closed also.

Finale: Incident solved, change, problem and known error closed

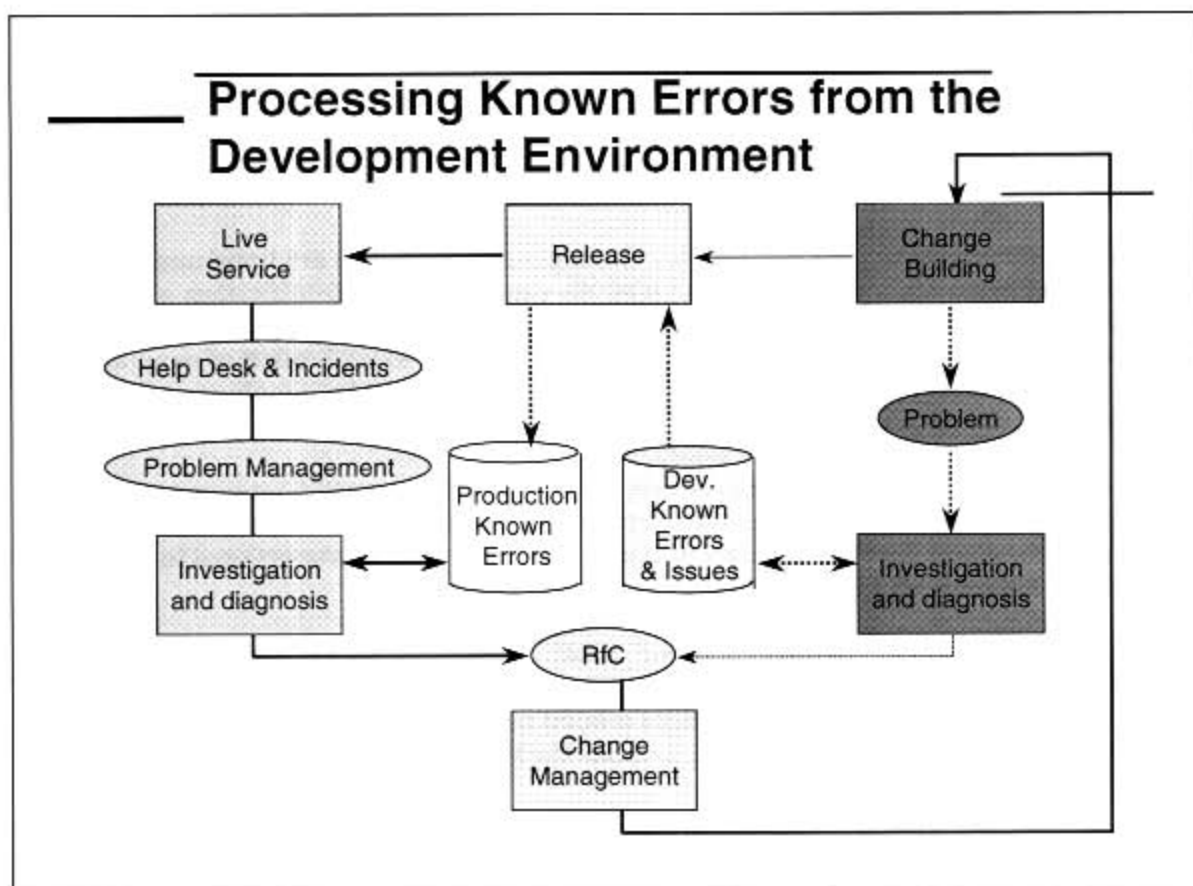
If somewhere during the diagnosis phase the problem team finds a workaround, the incident can be closed (with the OK from the Customer). This does not mean that the problem no longer exists. The only change in the problem record will be that the urgency will drop from urgent to non-urgent. It is up to the problem process to decide if there are enough resources free at that moment in time pursue diagnosis of the problem or that these resources can better be used elsewhere.



Student Notes

Processing Known Errors from the Development Environment

The second source of known errors arises from development activity. For example, implementation of a new application or packaged release is likely to include known, but unresolved, errors from the development phase. When an application or a release package is implemented the data relating to known errors from development needs to be made available to Problem Management who in turn should notify the Service Desk.



Student Notes

Reactive – Proactive

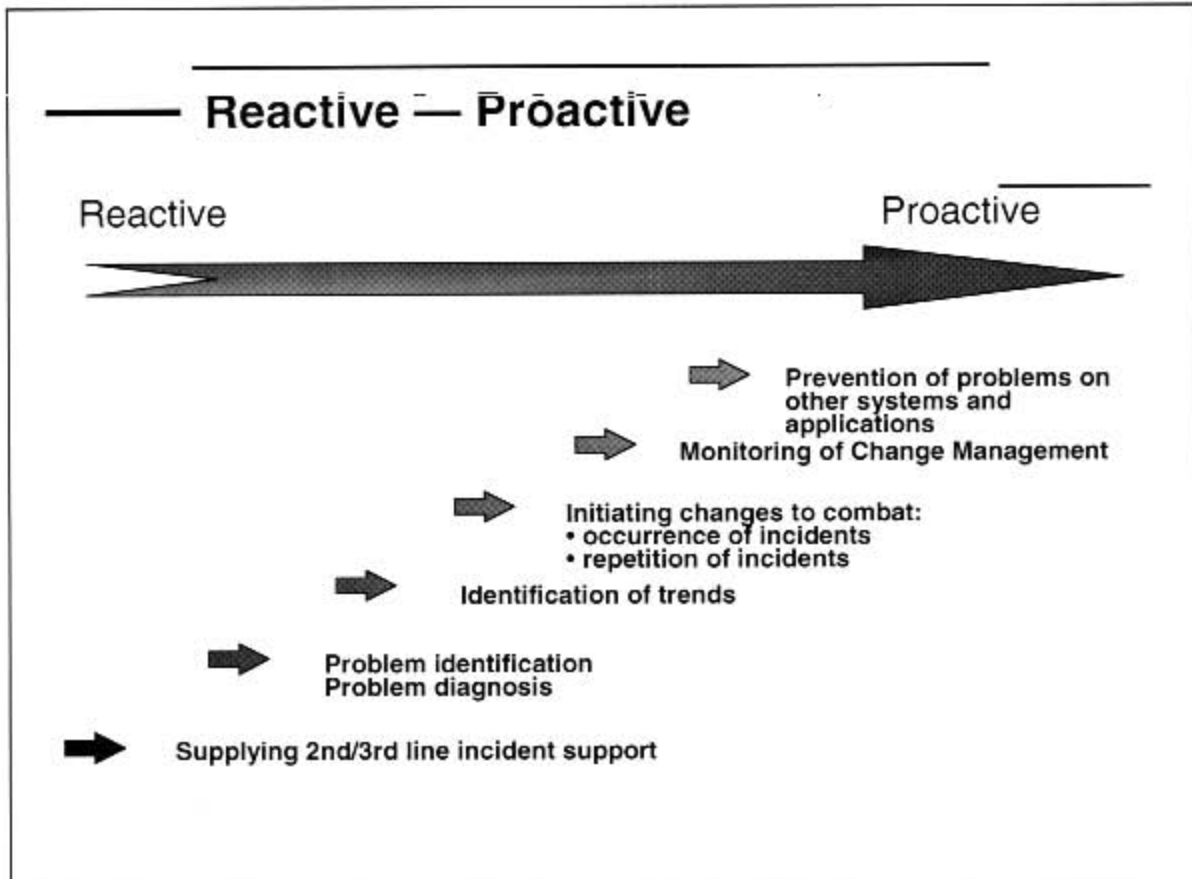
The activities described so far in problem and error control are mainly reactive. Proactive Problem Management activities are concerned with identifying and resolving problems and known errors before incidents occur, in other words minimizing the adverse impact on the service and business-related costs. Problem prevention ranges from prevention of individual problems through to strategic decisions. The latter may require major expenditure to implement, such as investment in a better network.

The main activities within proactive Problem Management processes are trend analysis and the targeting of preventative action. Trend analysis can lead to the identification of faults in the IT infrastructure, which can then be analyzed and corrected as described in the problem and error control sections. Trend analysis can also lead to the identification of general problem areas needing more support attention. It should be possible to make meaningful comparisons by expressing this in terms of financial cost to the organization.

Incident and problem analysis reports provide information for proactive measures to improve service quality. The objective is to identify 'fragile' components of an IT infrastructure and investigate the reasons for the fragility – in this context 'fragility' is proportional to the impact to the business should the CI fail.

Categorization of incidents and problems and creative analysis may reveal trends and lead to the identification of specific (potential) problem areas that need further investigation. For instance, analysis may indicate that incidents related to the usability of recently installed client-server systems is the problem area that has the most growth in terms of negative impact on business.

Analysis of Problem Management data may reveal: - that problems occurring on one platform may occur on another platform – for example, a problem concerning network software on a midrange system may well be of significance on a mainframe system - the existence of recurring problems – for example, if three routers are substituted serially, because of the same failure, it may indicate that the router-type concerned is not appropriate and should be replaced by another type, or when a software application is involved then complete redevelopment might be necessary which would be classed as a major change.



Student Notes

Essentials

Goals

The goals of problem management are to increase the quality of the IT infrastructure by examining the causes of the incidents or potential incidents and permanently removing them. Preventing incidents from occurring in the first place and to minimize the impact when they do occur.

Responsibilities

Problems and known errors.

A problem is a 'fault' in the ICT infrastructure, the cause of which is unknown and as a result of which incidents occur. If the cause of the problem is known, it is called a known error.

The problem manager

The problem manager is responsible for analysing incidents, investigating their causes and managing the resolution of underlying problems through formal change control. The problem manager monitors the progress of problems and takes care of the recording of known errors.

The process

Problems are defined, recorded and classified either in a reactive (at the request of incident management) or pro-active (based on trend analyses) way.

The problem manager subsequently organises a team of specialists who will investigate the problem. After successful diagnosis, the known error found is recorded and, if possible, a (temporary) solution is employed. On the basis of the results and the known error, the team formulates a request for change (RFC) in order to remove the known error from the ICT infrastructure.

The result of problem management is that the number of incidents will in the long-term decrease significantly.

Essentials

- *Goals*
 - Minimize impact of Incidents & Problems
 - Prevent recurrence of Incidents
 - Improving productive use of resources
- *Responsibilities*
 - Problem Control, Error Control (including raising RfCs), Assist with Major Incidents, Proactive Prevention, Management Information, Complete Major Problem Reviews
- *Reactive to proactive (stop problems occurring/recurring)*

Student Notes

Management Reporting

Management information should provide insight into the effort and resources spent by the organization on investigating, diagnosing and resolving problems and known errors. Besides this, it is important to provide insight in the progress made and the results obtained as a result. Metrics have to be selected carefully. Only through careful and meaningful measurement can management form an opinion on the quality of the process.

Some suggested metrics are:

- The number of RfCs raised and the impact of those RfCs on the availability and reliability of the services covered.
- The amount of time worked on investigation and diagnosis per organizational unit or supplier, split by problem types.
- The number and impact of incidents occurring before the root problem is closed or a known error is confirmed.
- The ratio of immediate (reactive) support effort to planned support effort in problem management.
- The plans for resolution of open problems with regard to resources:
 - People
 - Other used resources
 - Costs (against budget)

Module 6 — Change Management

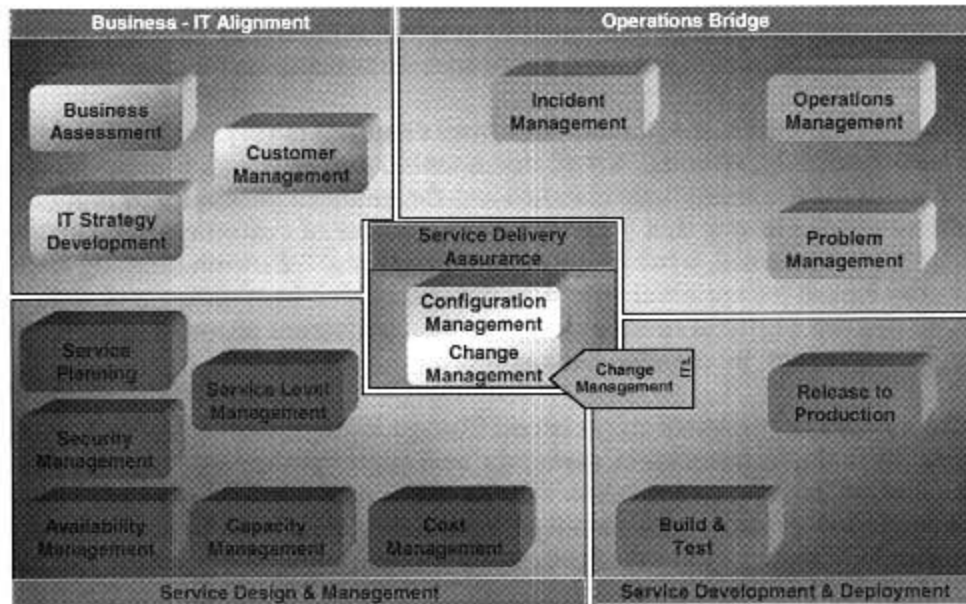
IT is becoming increasingly critical in business operations. The rate of change of business conditions is rising. The rate of change of technologies is mounting. Users are demanding greater levels of service to meet their objectives. All of these factors demand an IT environment in which change is tightly managed and controlled.

Experience suggests that a high percentage of problems related to IT service quality can be traced back to some change that was made to the system. The business costs resulting from such problems are costly and increasingly unacceptable.

This module describes the Change Management best practice and discusses its foundation role in the implementation of many other ITSM best practices. After all, evolution of the IT infrastructure in any sense, whether it be related to Capacity Management, Network Services Management, or Service Desk, involves change, which involves risk, which invites a rigorous approach to managing that change effectively.

Change Management

Change Management



Student Notes

Change Management - Goal

The first goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of changes upon service quality and business continuity, change impact, resource requirements and change approval. This considered approach is essential to maintain a proper balance between the need for change against the impact of the change. It is particularly important that Change Management processes have high visibility and open channels of communication in order to promote smooth transitions when changes take place.

Within the mission statement, the phrase "approved changes" is very strong and rigid. This almost implies inflexibility, although a well-documented and thorough Change Management policy will account for the small daily changes and the changes necessary to immediately restore a critical service or one that impacts a large number of customers. For example, for a user to change their password, a full Request for Change and follow-on meeting of the Change Advisory Board for approval would be unreasonable. In addition, a change needed immediately to restore a critical service should follow a different processing path from normal changes. This will be detailed later in this module.

For some, the thought of implementing a broad Change Management set of processes across functions, with formal documentation, meetings, and approvals appears to add bureaucracy and that the Change Management process will "tie the hands" of those who need to make changes to keep the IT environment running. In actuality, a proper Change Management (and Configuration Management) set of processes should reduce the need for constant ad hoc changes that may be found in environments with little or no change and Configuration Management policies. For those changes that do need to be made, a well-designed Change and Configuration Management flow should process and approve changes in a timely fashion. These approved changes carry IT management backing and have been screened for risk, cost, and impact.

Everything changes and, in business, where life is sufficiently complex already, the reliance on information systems and technology causes management to spend an astonishing amount of time assessing the impact of business change on IT, analyzing the impact of IT change on the business. Managing change has become a full time occupation. If changes can be managed to optimize risk exposure, severity of impact and disruption, and of course to be successful at the first attempt, the bottom line for the business is the early realization of this process.

Change Management — Goal

*To implement approved changes
efficiently, and with
acceptable risk to the existing
and to the new IT Services*



Student Notes

Change Management - Responsibilities

Change Management is responsible for managing the Change Process. This process is NOT in charge of implementing changes, it only will control that changes are approved and will be implemented efficiently, cost-effectively and with a minimum risk for the new and existing services. In order to do this in a proper way a process is required. But also very detailed procedures and guidelines how to do the different things in the process. To assess the risk of every change it is very important that detailed information about the IT infrastructure is available. That's why we need Configuration Management.

Another one of the responsibilities is that changes are to be planned. Only planned and properly scheduled changes can be effectively controlled as it ensures there is time to oversee what has to be done and that what has to be done will be done. To carry out effective well planned changes we have insight into the resources that are required and available, together with a good tool.

Communication is the key to a successful change process. A lack of communication is very often the reason that changes are not implemented correctly and that incidents will occur. The more people that are informed the more chance the change will be analyzed and monitored properly so that implementation is correct. A communication structure (e.g. the CAB) is therefore necessary. Another thing is of course reports. They will help to communicate the changes done and the how they were carried out.



Student Notes

Terminology

The definitions of the terms are (also see the glossary)

Change:

The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Request for Change:

Form, or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.

Forward Schedule of Changes:

Schedule that contains details of all the Changes approved for implementation and their proposed implementation dates.

Terminology

- **Change**
The addition, modification or removal of approved, supported or baselined CIs
- **Request for Change**
Form, or screen, used to record details of a request for a change to any CI or to procedures
- **Forward Schedule of Changes**
Schedule that contains details of all the Changes approved for implementation and their proposed implementation dates

Student Notes

Change Management Process

The standard ITIL process – in an overview – is:

Request for change

A RfC is the start of the change-life cycle.

Registration and Classification

Gather the necessary information to make decisions on what has to be changed, the category and impact so that authorization can be done properly. A priority and category that is based on the impact of the change is assigned. Risk assessment is of crucial importance at this stage.

Monitoring and Planning

Under responsibility of Change Management all the changes will be scheduled and a planning (with milestones) will be provided if necessary for the optimum control of the change(s)

Approve,

Decide if the change is going to be handled or not

Build & Test

Authorized RfCs should be passed to the relevant technical groups for building of the changes. Change Management has a coordination role, supported by Release Management and normal line management, to ensure that activities are both resourced and also completed according to the schedule. To prevent that changes heavily impact the service quality, it is strongly recommended that changes be thoroughly tested in advance (including back-out procedures where possible).

Authorize Implementation

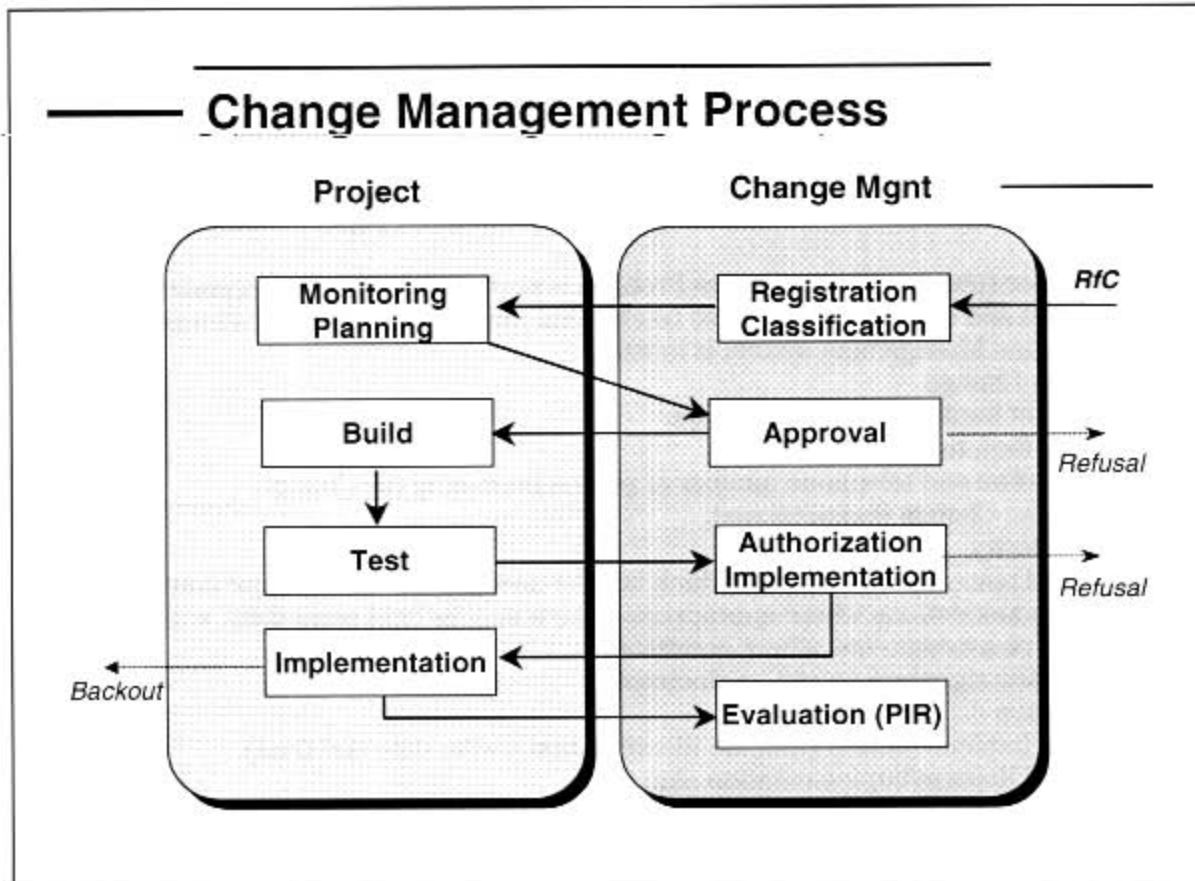
After a properly test and check if all the necessary action has been taken the change can be authorized for release. It also reaffirms that this is still the right time to do the change.

Implementation

Change Management has responsibility for ensuring that changes are implemented as scheduled, though this will be largely a coordination role as the actual implementation will be the responsibility of others (e.g. engineers will implement hardware changes).

Evaluate

Change Management must evaluate all implemented changes after a predefined period has elapsed. This can be done using a Post Implementation Review. This process may still involve CAB members; Change Management asks for assistance in this part of the process. Change Management should also evaluate and take follow-up actions to correct any problems or inefficiencies arising in the Change Management system itself as a result of ineffective changes.



Student Notes

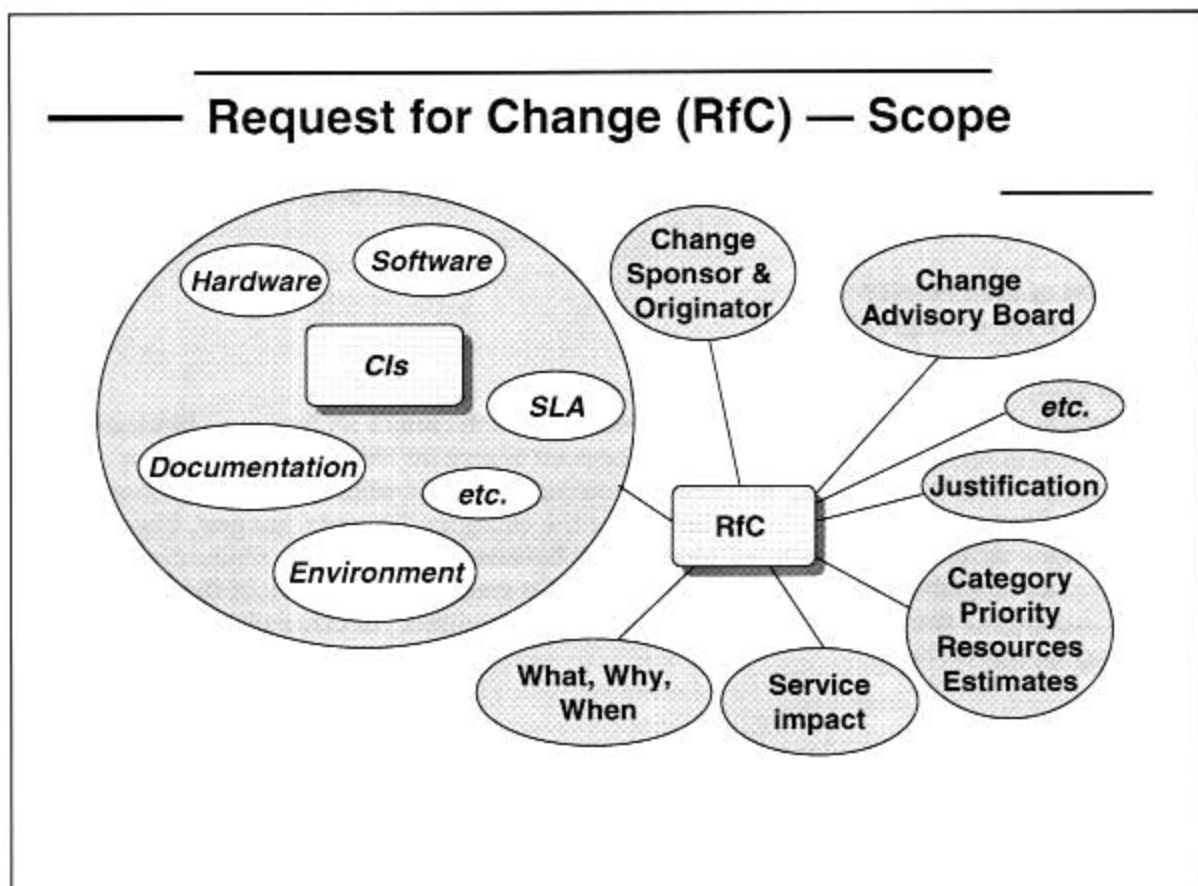
Request for Change (RfC) – Scope

Requests for change are triggered for a wide variety of reasons, from a wide variety of sources. It is the start of the change life cycle. RfCs can be concerned with any part of the infrastructure or with any service or activity. RfCs can, of course, be in paper form, or – as is increasingly the case – be held electronically, perhaps on the company intranet. All RfCs should be logged and given an identification number.

The following items should be included in an RfC form, whether paper or electronic:

- RFC number (plus cross reference to Problem report number, where necessary).
- Description and identity of item(s) to be changed (including CI identification(s) if Configuration Management system is in use).
- Reason for Change.
- Effect of not implementing the Change.
- Version of item to be changed.
- Name, location and telephone number of person proposing the Change.
- Date that the Change was proposed.
- Change priority.
- Impact and resource assessment (which may be on separate forms where convenient).
- CAB recommendations where appropriate (which may be held separately, with impact and resource assessments, where convenient).
- Authorization signature (could be electronic).
- Authorization date and time.
- Scheduled implementation (Release identification and/or date and time).
- Location of Release/implementation plan.
- Details of Change builder/implementer.
- Back-out plan.
- Actual implementation date and time.
- Review date.
- Review results (including cross-reference to new RFC where necessary).
- Risk assessment and management.
- Impact on business continuity and contingency plans.
- Status of RFC – i.e. 'logged', 'assessed', 'rejected', 'accepted', 'sleeping'.

As the change proceeds through its life cycle, the change request should be updated, so that the person who initiated the change is aware of its status. Actual resources used and the costs incurred should be recorded as part of the record.



Student Notes

Priority Setting

Once the RFC is accepted the priority and category are set. The priority indicates the importance of the change and is determined by urgency and impact. The priority code may already be attributed by the Problem Manager, but the definite codes are determined within the Change Management process, taking any remaining RFC's that are in discussion into consideration. The category is determined by the Change Manager. This classification determines how the application will be processed further and therefore is led from the 'weight' of the adjustment.

Subdivision of the Priority

Priority codes for example are:

Urgent,

highest priority: the RFC concerns a problem, which causes an immense hindrance in the use of essential services, or it concerns an urgent adjustment of the IT (for example new functionality because of company considerations or a small emergency law). Changes with this priority fall under the category 'Urgent Changes'. Urgent changes differ from the normal procedures because the necessary resources need to become available immediately for this type. An emergency meeting of the CAB (CAB/EC) or the IT-steering committee may be required. All other planned activities may be put on hold.

High:

causes severe technical trouble for a big group or a number of users or concerns other urgent situations. This change gets top priority in the next scheduled meeting of the CAB.

Medium,

normal priority: not an immense urgency or high impact, but the change may not be postponed to a more convenient moment. This change within the CAB receives an average priority with the attribution of recourses.

Low:

a change is wished for but could wait until a more convenient moment (for example the next release or planned maintenance appointment).

Priority Setting

- **Urgent**
Change necessary now (otherwise severe business impact), approval by CAB/Emergency Committee (CAB/EC)
- **High**
Change needed as soon as possible (potentially damaging)
- **Medium**
Change will solve irritating errors or missing functionality (can be scheduled)
- **Low**
Change leads to minor improvements (that are not contractually necessary)

Student Notes

Impact of a Change

Subdivision of the Category

Categories are attributed by the Change Manager, when needed in deliberation with the CAB, which give an indication of the impact of the change and the burden on the IT-organization. Below an example-subdivision of categories is listed:

Standard:

the confidence that the written procedure will make sure that the risks are negligible is there. The change may be executed without prior contact with a change manager. For this reason standard changes must be mandated by the change manager.

Category 1:

little consequences; a change that does not involve a lot of work. The Change Manager may approve this sort of change without discussing them with the CAB.

Category 2:

substantial consequences; changes that require greater efforts and have a greater impact on the services. Such changes are discussed in the next scheduled meeting of the CAB to predict the necessary efforts and possible consequences. Prior to the meeting some necessary documentation will be sent to the CAB members and potentially to several specialists and developers.

Category 3:

immense consequences: a change that requires a big amount of effort. With a Change like this the Change Manager needs to get authorization from the IT-management or an IT-steering committee and then must discuss it with the CAB.

Most changes end up in the first two categories.

Impact of Change

- **Standard**
The change may be executed without prior contact with the Change Manager
- **Category 1**
Little impact on current services. The Change Manager is entitled to authorize this RfC
- **Category 2**
Clear impact on the services. The RfC must be discussed in the CAB. The Change Manager requests advice on authorization and planning
- **Category 3**
Significant impact on the services and the business. Considerable manpower and/or resources needed. Management is involved in the decision process

Student Notes

The Change Advisory Board (CAB)

The term "Change Advisory Board" is an ITIL term. To some, the term "Board" creates visions of very formal regularly scheduled meetings by the same group of high level executives. Although a CAB meeting could be formal, it may also be informal. In today's business world, the term "team" may better illustrate the typical dynamics of a CAB. The CAB "team" may meet regularly; The CAB meetings could also be a few times a week, with special CAB meetings being called at any time. Some CAB members will probably be scheduled to attend CAB meetings regularly; Other people may be asked to join a CAB session to provide input about a specific Request for Change that is scheduled to be discussed.

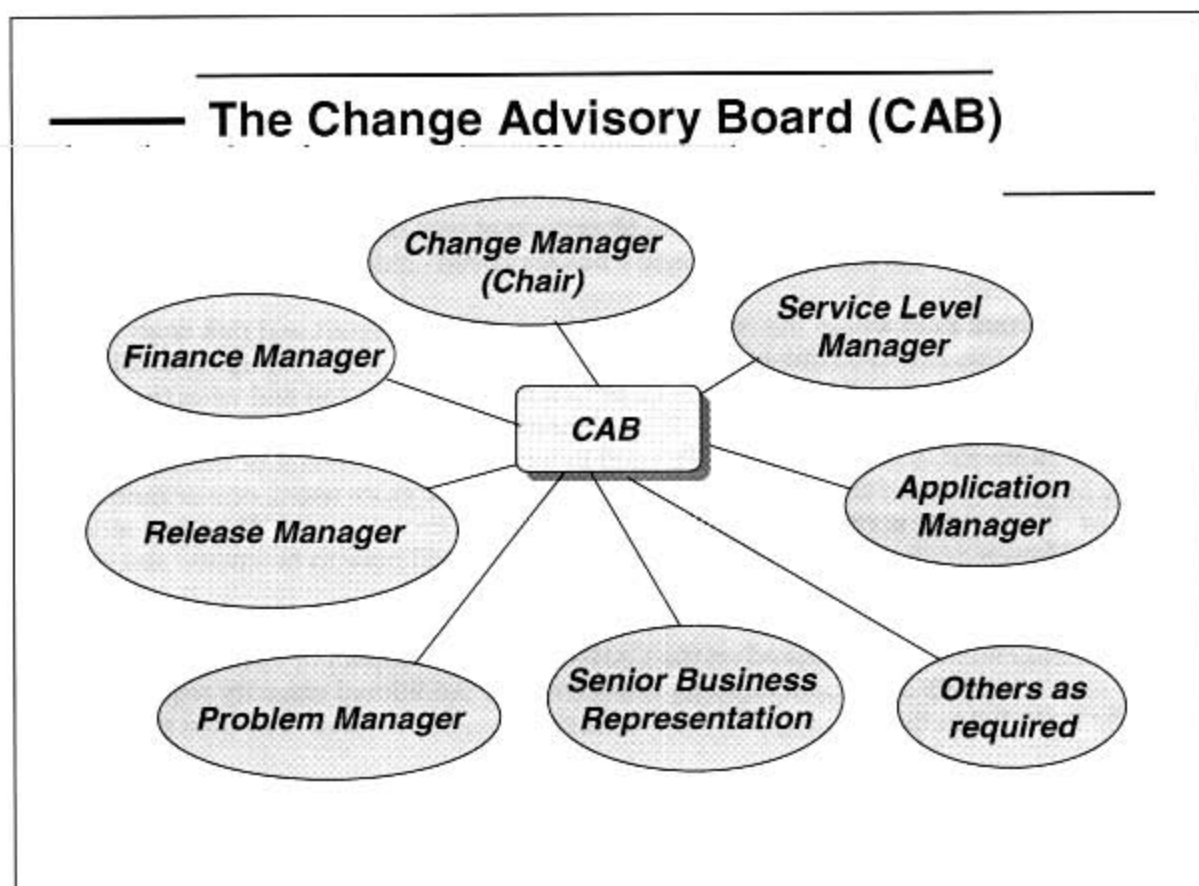
The CAB exists to approve most of the changes and to assist Change Management in the assessment and prioritization of changes. As and when a CAB is called together, the members that are chosen must be capable for adequately assessed from both a business and a technical viewpoint. To achieve this mix, the CAB needs to include people with a clear understanding of the Customer business needs and the User community, as well as the technical development and support functions.

CAB members could be the Change Manager, Customer(s), User manager(s), User group representative(s), applications developers/maintainers (where appropriate), experts/technical consultants, services staff (as required), office services staff (where Changes may affect accommodation and vice versa), contractor's or third parties' representatives (as required – for instance in outsourcing, situations).

It is important to emphasize that the CAB:

- Will be composed according to the changes being considered
- May vary considerably in make-up even across the range of a single meeting
- Should involve suppliers when that would be useful
- Should reflect both User and Customer views
- Is likely to include the Problem Manager and Service Level Manager and Customer Relations staff for at least part of the time.

When major Problems arise, there may not be time to create the full CAB, and it is therefore necessary to identify a smaller organization with authority to make emergency decisions. Such a body is in ITIL known as *the CAB Emergency Committee (CAB/EC)*. Change procedures should specify how the format of the CAB and CAB/EC will be determined in each instance, based on the criteria listed above and any other criteria that may be appropriate to the business. This is intended to ensure that the format of the CAB will be flexible, in order to represent business interests properly when major changes are proposed. It will also ensure that the composition of the CAB/EC will provide the ability, both from a business perspective and from a technical standpoint, to make appropriate decisions in any conceivable eventuality.



Student Notes

Some Relationships

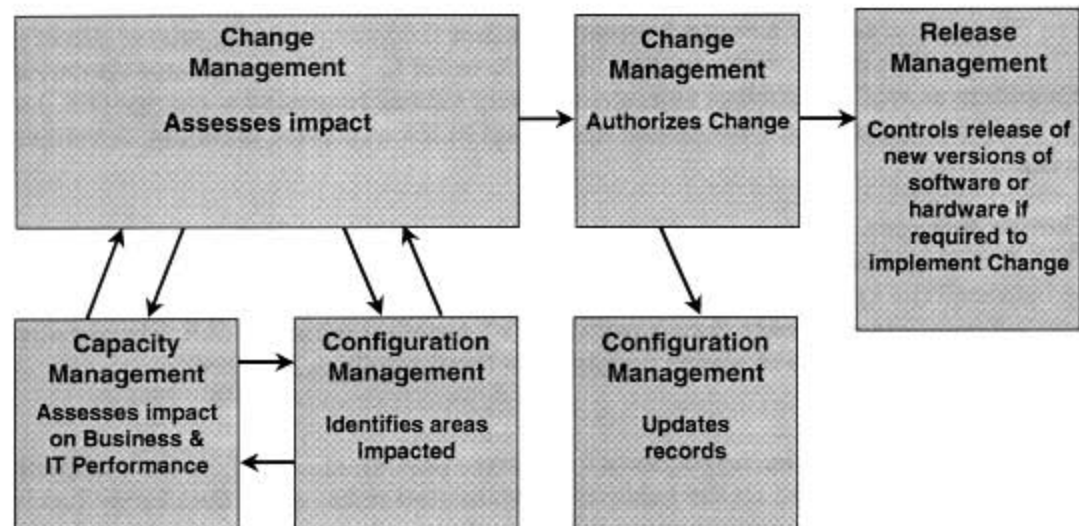
Change Management and Configuration Management are very much related to each other. First of all because of the fact that Configuration Management cannot survive without Change Management - the CMDB cannot be controlled if there is no control over the CIs. The Verification process is a process that can be used to control the effectiveness of Change Management. If - after verification - the Configuration Manager has found CIs in the configuration that are not in the database there are two options: 1) the database is not up to date which could indicate that Configuration Management was not informed about the change or 2) someone has executed an illegal - not approved - change.

The most important field where the processes are related is the impact and risk analysis of a change. Most of this has to be done with the help of the CMDB. Upon receipt of a RFC one of the first things to do is to find out which CI or CIs has to be changed and what the impact is on the existing infrastructure. Change Management must also determine if this one RFC will result in more RFC's because more CIs need to be changed as a result of this request. It must also be ascertained if this change is only effecting one or more users, one or more domains or one or more services in order to assign the right impact code. Based on all this the Change Manager can decide if a CAB is necessary, who will have to be invited and on which level discussions need to take place.

Capacity Management is represented on the CAB to assess the impact of Changes on existing capacity and to identify additional capacity requirements. Additional capacity requirements need to be included in the Capacity Plan and as such treated as RFCs in their own right.

Release Management is represented on the CAB to recommend the content and scheduling of Releases. Release Management is then responsible for implementing the agreed releases.

Some Relationships



Student Notes

Essentials

Goal

The goal of Change Management is to carry through in a systematic way all adjustments in the ICT infrastructure. In this way the risks of disturbance to the service and the resulting decrease in the quality of the services supplied are kept to a minimum.

Request for change (RfC)

A change is any adjustment to one or more configuration items (CIs). It can vary from major (such as the replacement of a control server) to minor (replacement of a printer driver) and may affect any of the components in the CMDB. In order to have the adjustments carried out, customers as well as problem management may submit requests for change (RfC) to the change manager. Internal ICT needs can also result in RfCs (service planning, development, et cetera).

The Change Manager

The change manager is responsible for implementing each change in a systematic way after having balanced the known risks. He also monitors the **progress** of changes. The change manager assesses the **requests for change (RfCs)**, together with the CAB (change advisory board). This board consists of senior people from the disciplines involved.

The Process

The change manager receives the requests for change (**RfCs**), checks them for completeness, **records** and **classifies** them on the basis of the estimated risks. After the change has been authorised in principal, the consequences in terms of capacity are taken up. Availability and costs are analysed by the service planning processes. The proposal may then, after the approval of change management, move on to the development department for **design, building** and **testing**. The change manager, if necessary advised by the CAB, decides on the timing of the release on the basis of test results and a well-founded back-out plan. The back-out plan ensures that the organisation can at all times revert to the previous situation in case of unforeseen problems. Only then will the release authority be granted for the **implementation**. If a release authority relates to software, the release will be followed by a production test by the Software control & distribution process, before trial distribution. In addition, there must always follow an **assessment** of the change and of the way in which the implementation was effected.

Essentials

- Goal
 - Only approved, cost effective changes made with an acceptable amount of risk
- Responsibilities
 - Manage whole change process: accept, filter & record RfCs; assess impact, cost, benefit & risk; justification & approval; manage & coordinate implementation; chair CAB; monitoring & reporting; review & closure
- CAB and CAB/EC:
 - Membership
 - Advisory role
 - Assess impact, urgency & resources
 - Urgent changes
- Urgency/Priority: urgent, high, medium, low
- Impact category: no impact tremendous impact
- Backout
- Process always ends with a review of the change

Student Notes

Management Reporting

Change Management (ideally in consultation with business managers) needs to think about measures that have *specific* meaning. While it is relatively easy to count the number of Incidents that become Problems that become Changes, it is infinitely more valuable to look at the underlying cause of such Changes, and to identify trends. Better still to be able to measure the impact of Changes and to demonstrate reduced disruption over time because of the introduction of Change Management, and also to measure the speed and effectiveness with which the IT infrastructure responds to identified business needs.

Measures taken should be linked to business goals wherever practical – and to cost, service availability, and reliability. Any predictions should be compared with actual measurements.

Regular summaries of Changes should be provided to service, Customer and User management. Different management levels are likely to require different levels of information, ranging from the Service Manager, who may require a detailed weekly report, to the senior management committees that are likely only to require a quarterly management summary.

Consider including the following facts and statistics in management reports:

- The number of Changes implemented in the period, in total and by CI, configuration type, service, etc.
- A breakdown of the reasons for Change (User requests, enhancements, business requirements, service call/Incident/Problem fixes, procedures/training improvement, etc).
- The number of successful changes.
- The number of Changes backed-out, together with the reasons (e.g. Incorrect assessment, bad build).
- The number of Incidents traced to Changes (broken down into problem-severity levels) and the reasons (e.g. Incorrect assessment, bad build).
- The number of RfCs (and any trends in origination).
- The number of implemented Changes reviewed, and the size of review backlogs (broken down over time).
- High incidences of RfCs/prs relating to one CI (these are worthy of special attention), giving the reasons (e.g. Volatile User requirement, fragile component, bad build).
- Figures from previous periods (last period, last year) for comparison.
- The number of RfCs rejected.
- The proportion of implemented Changes that are not successful (in total and broken down by CI).
- Change backlogs, broken down by CI and by stage in the Change Management process.

Module 7 — Release Management

This module introduces the ITSM discipline known as Release Management. As software and hardware are increasingly considered an important organizational asset, indeed frequently of a strategic nature, control of that software becomes mandatory. Following are some of the important considerations:

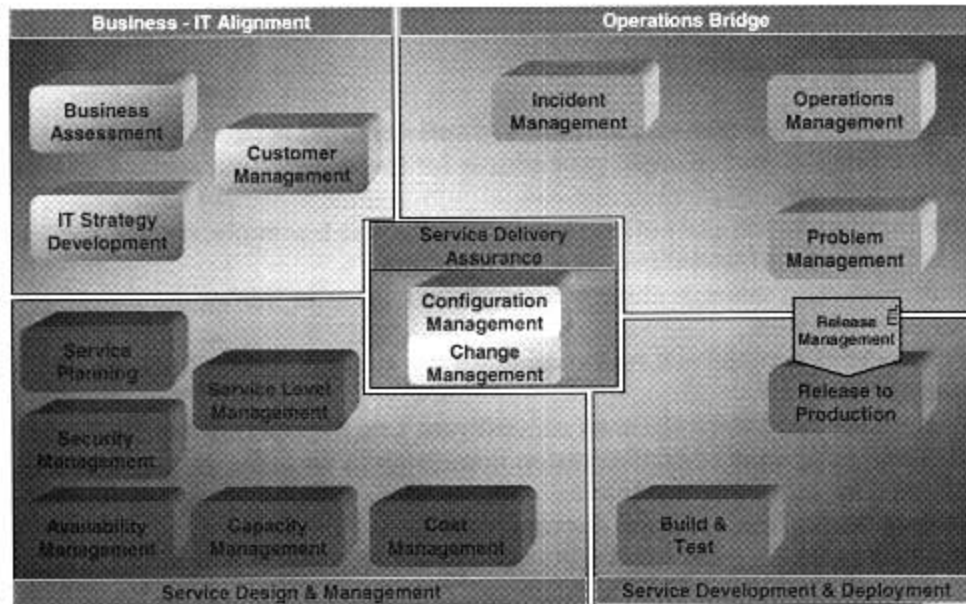
- Preventive activity (e.g., protection from illegal copying).
- Consistency (e.g., client programs are compatible with server programs).
- Licensing (e.g., not exceeding an agreed-upon maximum number of users at any point in time).

Release Management is responsible for the storage of management-authorized software (developed in-house, purchased, or licensed application or utility software, etc.), the release of software into the live environment, distribution of software to remote locations, the implementation of the software to bring it into service and having hardware so that incidents and installations can be performed quickly.

Factors such as the increasing number of interdependent software Configuration Items (CIs), the potential for introduction of viruses, and complex licensing strategies to minimize licensing costs while still making software available where it is needed, all suggest the value of an immediate investment in the implementation of a rigorous Release Management discipline.

Release Management

Release Management



Student Notes

Release Management - Goals

Many service providers and suppliers may be involved in the release of hardware and software in a distributed environment. Good resource planning and management are essential to package and distribute a release successfully 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, both technical and non-technical, are considered together.

The goals of Release Management are:

- To plan and oversee the successful rollout of software and related hardware.
- To design and implement efficient procedures for the distribution and installation of changes to IT systems.
- To ensure that hardware and software being changed is traceable, secure and that only correct, authorized and tested versions are installed.
- To communicate and manage expectations of the customer during the planning and rollout of new releases.
- To agree the exact content and rollout plan for the release, through liaison with change management.
- To implement new software releases or hardware into the operational environment using the controlling processes of configuration management and change management - a release should be under change management and may consist of any combination of hardware, software, firmware and document CIs.
- To ensure that master copies of all software are secured in the definitive software library (DSL) and that the configuration management database (CMDB) is updated.
- To ensure that all hardware being rolled out or changed is secure and traceable, using the services of configuration management.

The focus of Release Management is the protection of the live environment and its services through the use of formal procedures and checks.

Release Management works closely with the Change Management and Configuration Management processes to ensure that the shared CMDB is kept up-to-date following changes implemented by new releases, and that the content of those releases is stored in the DSL. Hardware specifications, assembly instructions and network configurations are also stored in the DSL/CMDB.

Release Management — Goals

- *Plan and oversee the SW & HW rollouts*
- *Design and implement efficient procedures*
- *Ensure that changes to hardware and software are controlled*
- *To manage expectations of the customer during rollout*
- *To agree the content and rollout plan for a release*
- *To implement new software releases or hardware into the operational environment*
- *Secure all software masters in the definitive software library*
- *Use services of configuration management to ensure that all hardware being rolled out or changed is secure and traceable*

Student Notes

Release Management - Responsibilities

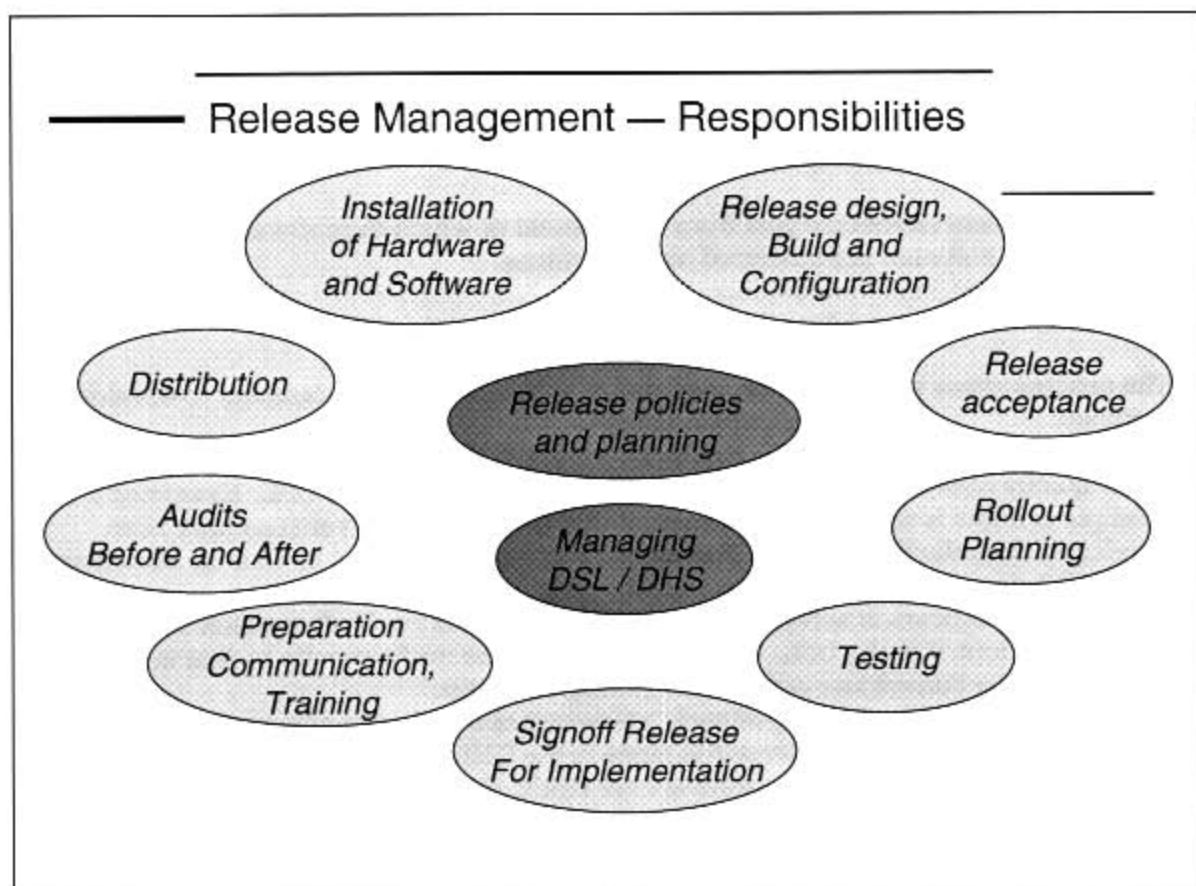
Only authorized software must be accepted into the DSL and it must be protected whilst it resides there. The same holds for hardware that has to be placed in the DHS.

The distribution and implementation processes must be reviewed and audited to ensure procedures are followed, and any necessary changes to them can be corrected.

Configuration Management will carry out software audits with assistance from release management staff.

Release Management 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.



Student Notes

Release and Distribution Process

Environments must be kept separate with a controlled migration path and an audit trail of all releases and back outs. The archive environment can be considered as a sub-environment of the DSL and be subject to the same level of control. If unacceptable errors are found during testing (and changes made) the version number must be incremented. Everything is done under control of Change Management.

Release Management covers the part from the moment of which the software is adopted in the DSL until the software is transferred to the archives.

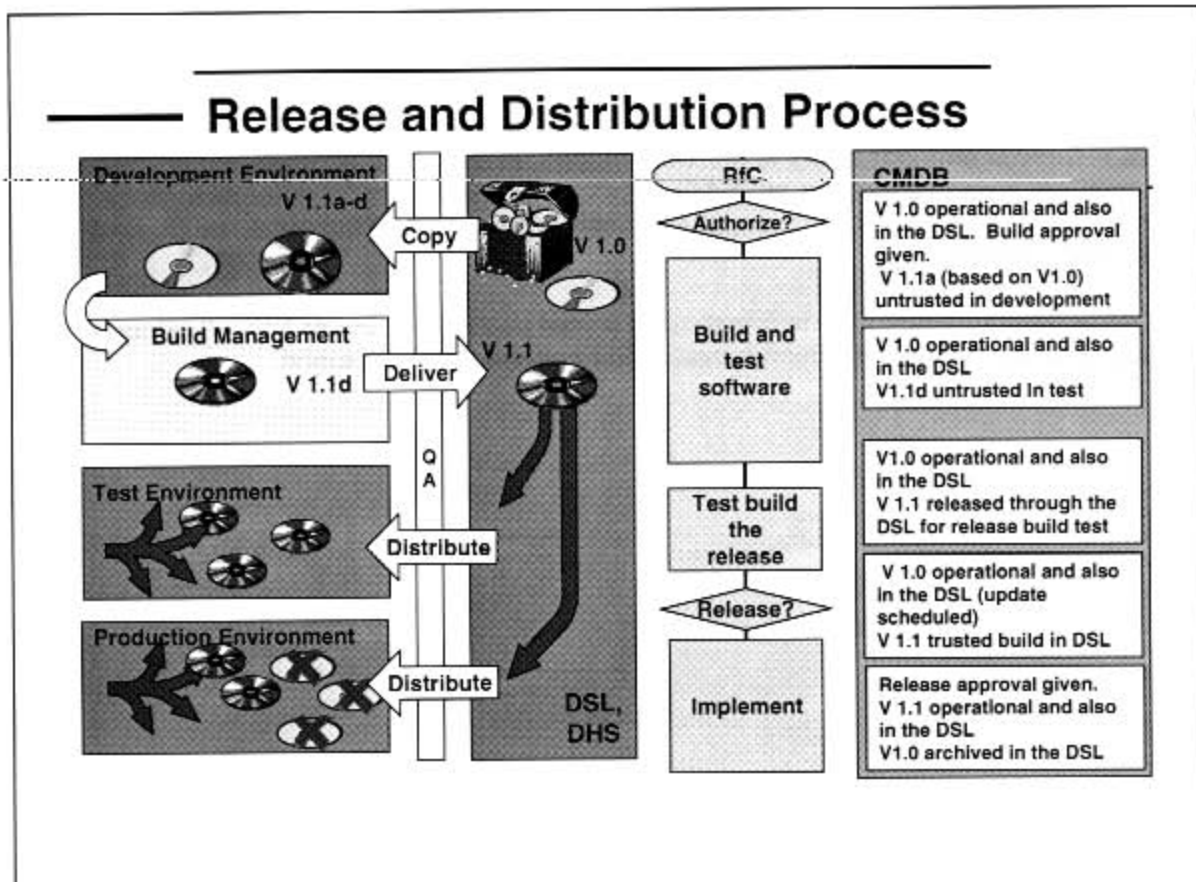
During the life circle of a program the next steps are passed through:

- The process either starts with the purchase of software, or the assignment to develop the software.
- When the software is delivered a quality check will follow.
- In the quality check the software is accepted for adoption into the DSL. Examined for example is if this is really the software that was ordered, if new versions have been developed from the right source, if all adjustments are authorized by Change Management and if all items are registered in the CMDB.
 - Once the software is accepted, a backup of the DSL is made after which the software will be adopted in the DSL. These backups must occur frequently so that in case of a disaster the correct last version can quickly be set up.
 - The compilation and timing of each release are decided on in advance by the Change Management, a 'Release Record' is made in the CMDB and all details are registered.
 - When all components of the software are ready, the packet can be realized in a testing area where all mandatory tests can be executed.
 - When too many errors are found, the software is returned for further development.
 - When the software is approved it will be released for exploitation. The release will then be distributed and taken into exploitation.

Copies of software items can be made available from the DSL for several different areas, of which the 4 most used ones are listed below. A different, more detailed subdivision of course is also possible.

- *Development*: when a new version is being developed, a former from the DSL can be originated from. The development area is the only area in which software may be adjusted or changed.
- *Test*: in a test area certain versions can be tested.
- *Exploitation*: the actual (live) surrounding area from which the software is made available to the users.
- *Archives*: here original (former) versions of software items that are no longer being used are kept.

These copies may only be present in one of these areas at any given moment.

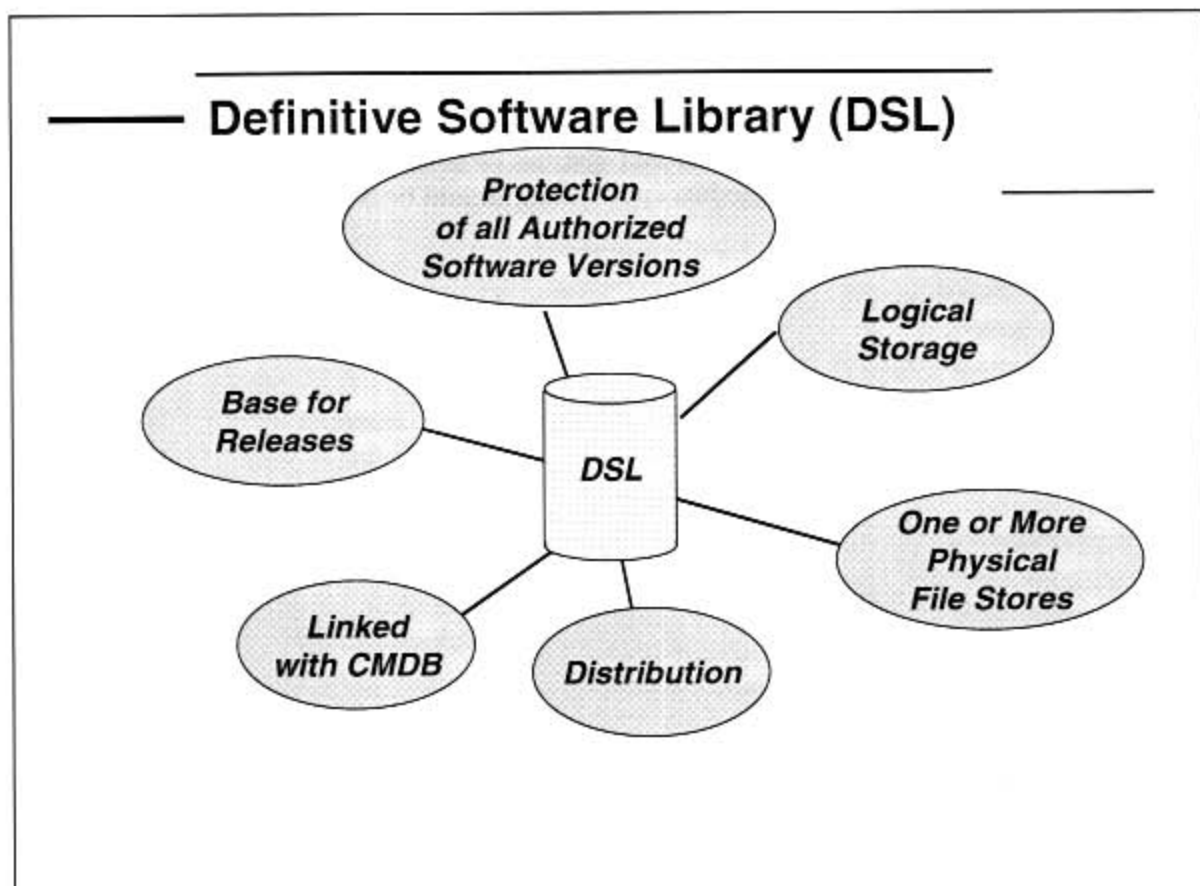


Student Notes

Definitive Software Library (DSL)

The Definitive Software Library (DSL) is a conglomeration of software Configurations Items and documentation in a secure location. Physically, the DSL may be a collection of electronic media (like disks, tapes, and compact disks) in different software formats, files, and electronic (or paper) documentation. The DSL is a logical library. That means that “logically” there is only one entity of software stored. Physically it is possible that there are many copies of a software entity, stored in different places (at a bank, at a contingency center, near development, etc). Because all these entities must be the same, we “logically” still only have one entity.

Every authorized software item is (physically) stored in the DSL. In the DSL all original versions of software that have been transmitted to exploitation are saved.

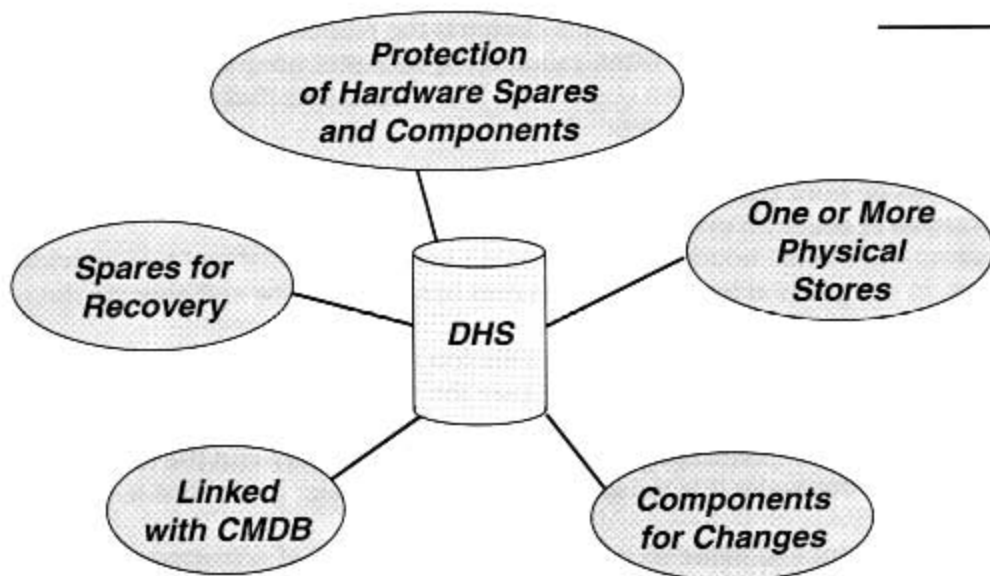


Student Notes

Definitive Hardware Store (DHS)

An area should be set aside for the secure storage of definitive hardware spares. These are spare components and assemblies that are maintained at the same level as the comparative systems within the live environment. Details of these components and their respective builds and contents should be comprehensively recorded in the CMDB. These can then be used in a controlled manner when needed for additional systems or in the recovery from major Incidents. Once their (temporary) use has ended, they should be returned to the DHS or replacements obtained.

Definitive Hardware Store (DHS)



Student Notes

Releases

The Release Manager in advance sets up a Release Policy in which is decided on how and when software updates should be compiled. The first choice made is the one of the level of the Software Release. An inventory is made on which sub items of a program can still be distributed independent of each other.

An example of a problem surrounding this choice is the releasing of individual DLL files (Dynamic Link Libraries) that are often called on by different programs. Sometimes a new version of a DLL is delivered with a packet and this could mean that other software is also influenced by it. The final choice depends on:

- The amount of work that an adjustment of a component of the program causes for other components of other programs (including system software).
- The amount of human hours and time that is necessary to build and test individual changes, in comparison to what it would cost to save up a few and execute them all at once.
- The degree of difficulty of a possible installation with the users; it may for example be easier to install a complete program because the standard mechanisms therefore already exist.
- The complexity of dependability's between the new software and the rest of the IT-infrastructure; the easier it is to isolate software, the easier it is to test it.

It is of great importance to make an evaluation of the number of adjustments that can be tested all together in a certain period of time in advance, a Packaged Release (gathering of different changes within one roll-out) may be so complex that it will never pass through the test phase. As a result of the fast development of new software, the new Release may no longer be up to date by the time it is released. On the other hand, a large amount of adjustments may result in great technical trouble for the service.

Release Numbering ensures each release is allocated a release number so that it can be uniquely identified. There should be a well publicized and predictable release frequency and an agreed limit for change content. Business requirements rather than technical convenience should be the determining factor. Specifications should be frozen sufficiently in advance of the release date to allow for sufficient testing.

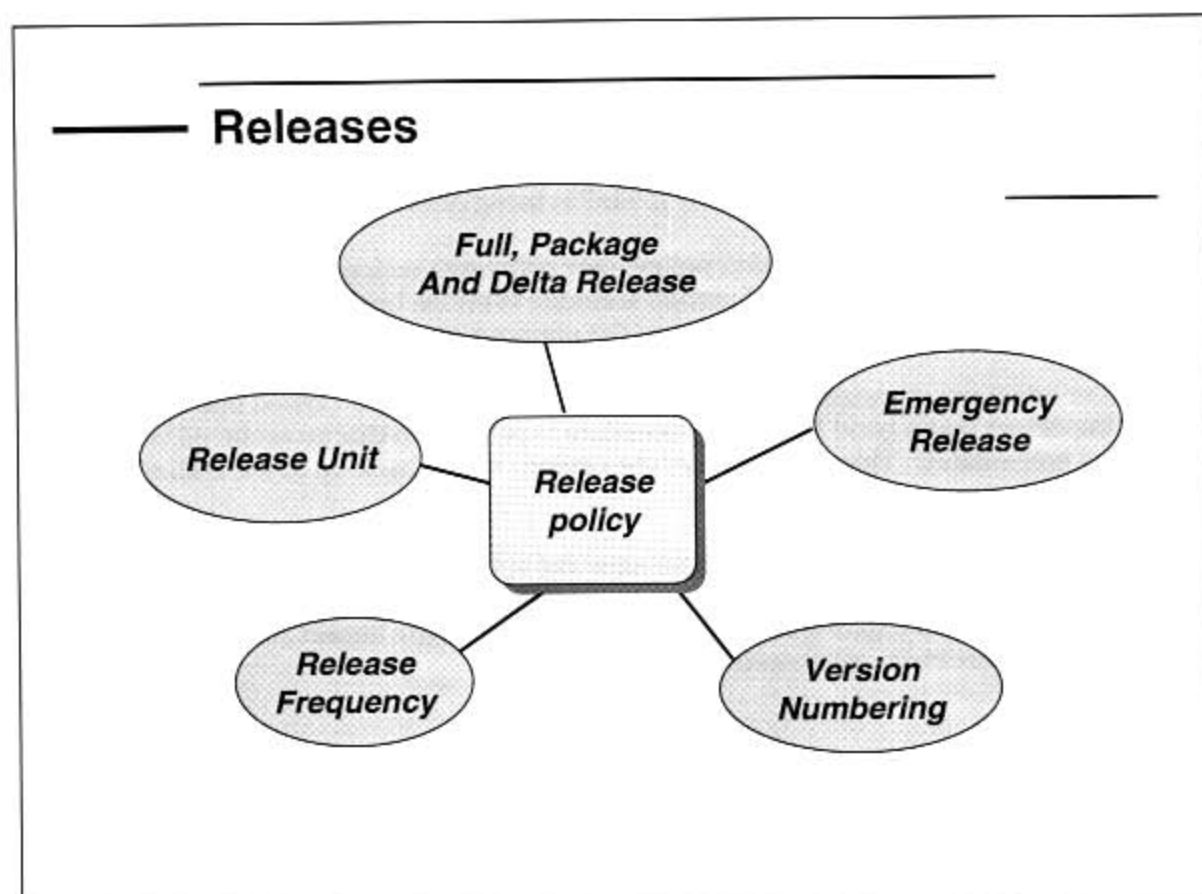
Release Unit - the level at which software of a given type is normally released

Full Release means all components of the release are built, tested, distributed and implemented together.

Delta Release only those CIs that have actually changed since the last release are included.

Package Release individual releases, both full and delta, are grouped together to form a package for release.

Emergency Release occurs when there is an urgent reason to roll out a new version. An emergency release is an urgent adjustment and is performed in name of the Change Management.



Student Notes

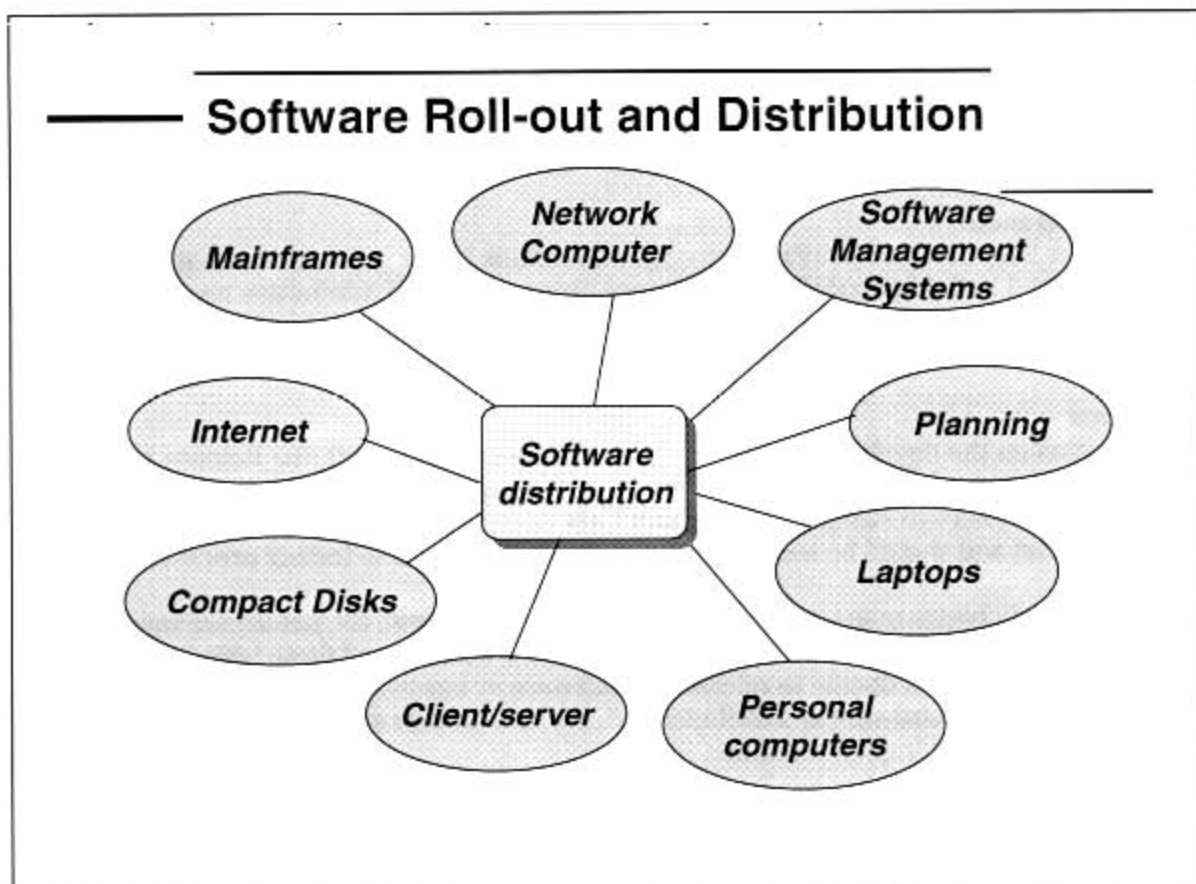
Software Roll-out and Distribution

Procedures must be devised for distributing software releases from the test build environment into the test environment, into the live build environment and into the live environment. They should include details on time, and where a number of users must use the same version over a number of locations. The release record on the CMDB must be updated throughout implementation of releases. Apart from the technical environment, the business environment is also influential, particularly if 24x7 is being delivered globally.

In order to maintain a good distribution policy, new software versions should be planned in advance. When the plan for release of certain software versions becomes known, the releases can be prepared according to the principles of the previous paragraph.

Errors occur when unauthorized installations of the new version are carried out. In this case it is very important that a good Fall Back-procedure is present so that an archived version can be used immediately. This also is one of the reasons why a back-up of the DSL should occur frequently.

When more multiple locations with local management appear, then these locations shall have a copy of the DSL to be able to roll out software. Before each roll out it is important that a plan for distribution and implementation is made. In this plan the impact for the users and the necessary resources are taken into consideration.



Student Notes

Essentials

Goals

Release Management controls all production software and hardware within the IT infrastructure and arranges the distribution within operational environments. Only software and hardware that has been checked will be distributed and precautions are taken to ensure that original versions can be reverted to, should faults occur.

The Release Manager

This manager keeps and administers the original versions of the software and hardware. These are stored in the DSL (definitive software library) and DHL (definitive hardware library). In addition, he monitors the process of providing software and hardware and is responsible build management from the controlled test environment onwards.

The Process

At the conclusion the development process (via change management), the Release Manager checks the software and hardware, after testing and recording, stores it in the DSL and DHL. Releases should undergo stringent testing and User acceptance before release. Back-out plans must exist and should be tested as part of the overall Release testing process.

At the request of change management, versions (release, upgrade, fix, patch) are assembled and tested in a simulated production environment. If the outcome of these tests is positive, change management will decide to release the software or hardware. The approved and released software or hardware is distributed, after which change management will take care of the final operational implementation.

The result is a clear overview of and proper control over the software versions and hardware installations used or to be used.

Essentials

- *Goals*
 - Plan and oversee rollout of SW & HW
 - Design & implement distribution & installation procedures
 - Ensure SW & HW changes are traceable
 - Work closely with Configuration Management & Change Management during implementations
- *Responsibilities*
 - Control DSL & DHL; define release plans & policies; build release; testing; acceptance & sign off; manage release; distribute and install SW & HW; software audits; communication & training
- *Releases & Version Control*
 - Release unit: Full/package/delta/emergency; numbering; frequency; development; testing; live; archive
- *Process*
 - Release Management (operational)
 - Change Management (control)
 - Configuration Management (control & administration)

Student Notes

Management Reporting

A number of key performance indicators (KPIs) should be monitored to assess the effectiveness of the Release Management process. Consider choosing some measures that show a clear indication of at least some of the following:

- Releases built and implemented on schedule, and within budgeted resources
- Very low (ideally no) incidence of Releases having to be backed out due to unacceptable errors
- Low incidence of build failures
- Secure and accurate management of the DSL
- No evidence of software in the DSL that has not passed quality checks and no evidence of reworks on any software that was extracted from the DSL
- DSL sizing matching the demand for space, and timely and accurate housekeeping of the DSL
- Compliance with all legal restrictions relating to bought-in software
- Accurate distribution of Releases to all remote sites
- Implementation of Releases at all sites, including remote ones, on time
- No evidence of unauthorized reversion to previous versions at any site
- No evidence of use of unauthorized software at any site
- No evidence of payment of license fees or wasted maintenance effort, for software that is not actually being used at any particular location
- No evidence of wasteful duplication in Release building (e.g. Multiple builds of remote sites, when copies of a single build would suffice)
- Accurate and timely recording of all build, distribution and implementation activities within the CMDB
- A post-mortem carried out on all Release activities, and all necessary corrective or follow-up action taken, together with any process improvements
- The planned composition of Releases matching the actual composition
- IT and human resources required by Release Management being subject to good ongoing forward planning.

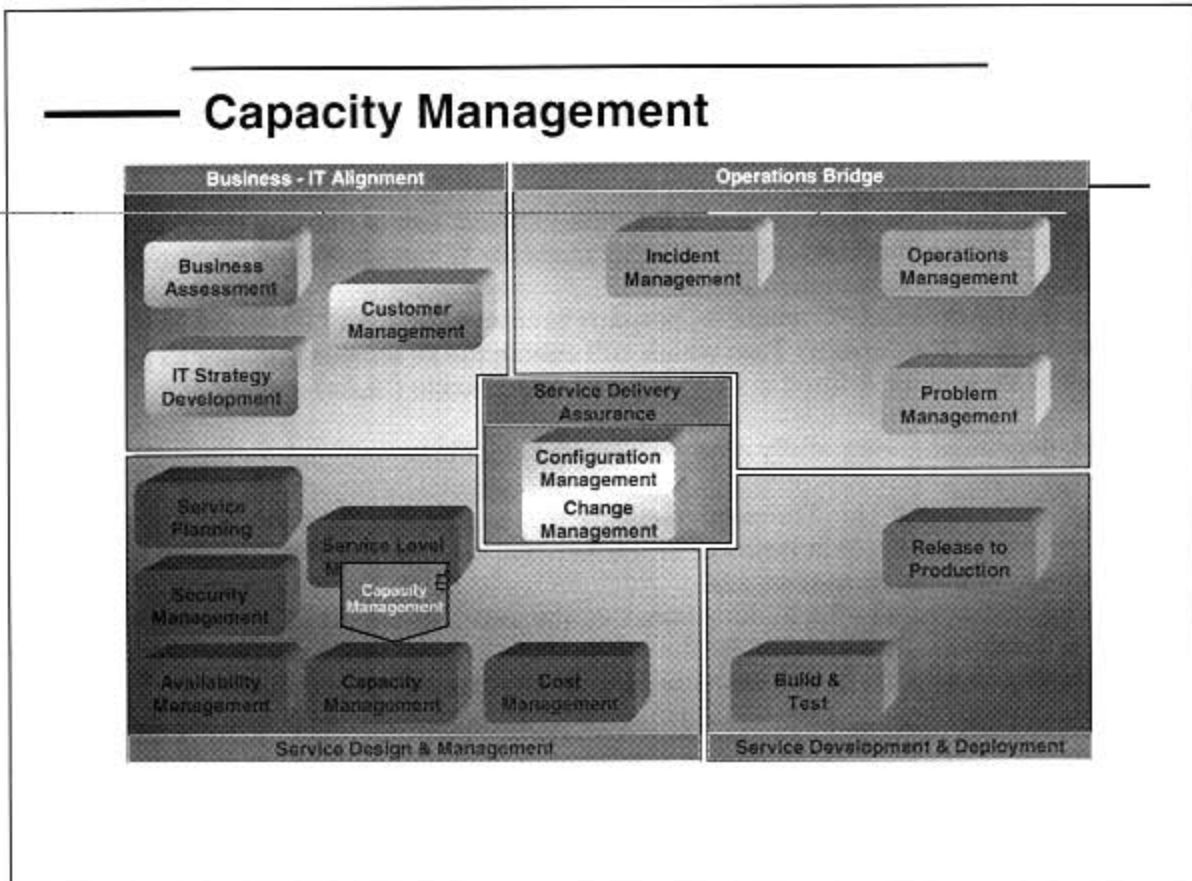
Other metrics that may be monitored include:

- The number of major and minor Releases per reporting period
- The number of problems in the live environment that can be attributed to new Releases, which need only be measured during the first few months of a new Release's life, classified by root cause, (e.g. 'wrong version of file' or 'missing files')
- The number of new, changed and deleted objects introduced by the new Release – e.g. How many modules and programs
- The number of Releases completed in the agreed timescales; this requires the central Release Management function to publish predefined targets (service levels or slas) for software distributions and other common tasks.

Module 8 — Capacity Management

This module introduces Capacity Management, a discipline that ensures cost justifiable IT capacity always exists to match business needs. Capacity Management determines business demands (on IT resources), forecasts workloads, and performs IT resource scheduling. One of the major contributions of Capacity Management is a documented Capacity Plan.

Capacity Management



Student Notes

Capacity Management - Goal

Capacity Management is responsible for ensuring that IT processing and storage capacity matches the evolving demands of the business in the most cost-effective and timely manner. The process encompasses:

- The monitoring of performance and throughput of IT services and the supporting infrastructure components.
- Undertaking tuning activities to make the most efficient use of existing resources.
- Understanding the demands currently being made for IT resources and producing forecasts for future requirements.
- Influencing the demand for resource, perhaps in conjunction with Financial Management.
- The production of a Capacity Plan which will enable the IT service provider to provide services of the quality defined in Service Level Agreements (SLAs).

Capacity Management is essentially a balancing act; balancing:

- Cost against capacity – i.e. The need to ensure that processing capacity that is purchased is not only cost justifiable in terms of business need, but also the need to make the most efficient use of those resources, and
- Supply against demand – i.e. Making sure that the available supply of processing power matches the demands made on it by the business, both now and in the future. It may also be necessary to manage or influence the demand for a particular resource.

Capacity Management — Goal

Balancing Act

*To determine
the right, cost justifiable, capacity of IT
resources such that
the Service Levels agreed with the business
are achieved at the right time*

Student Notes

Capacity Management - Responsibilities

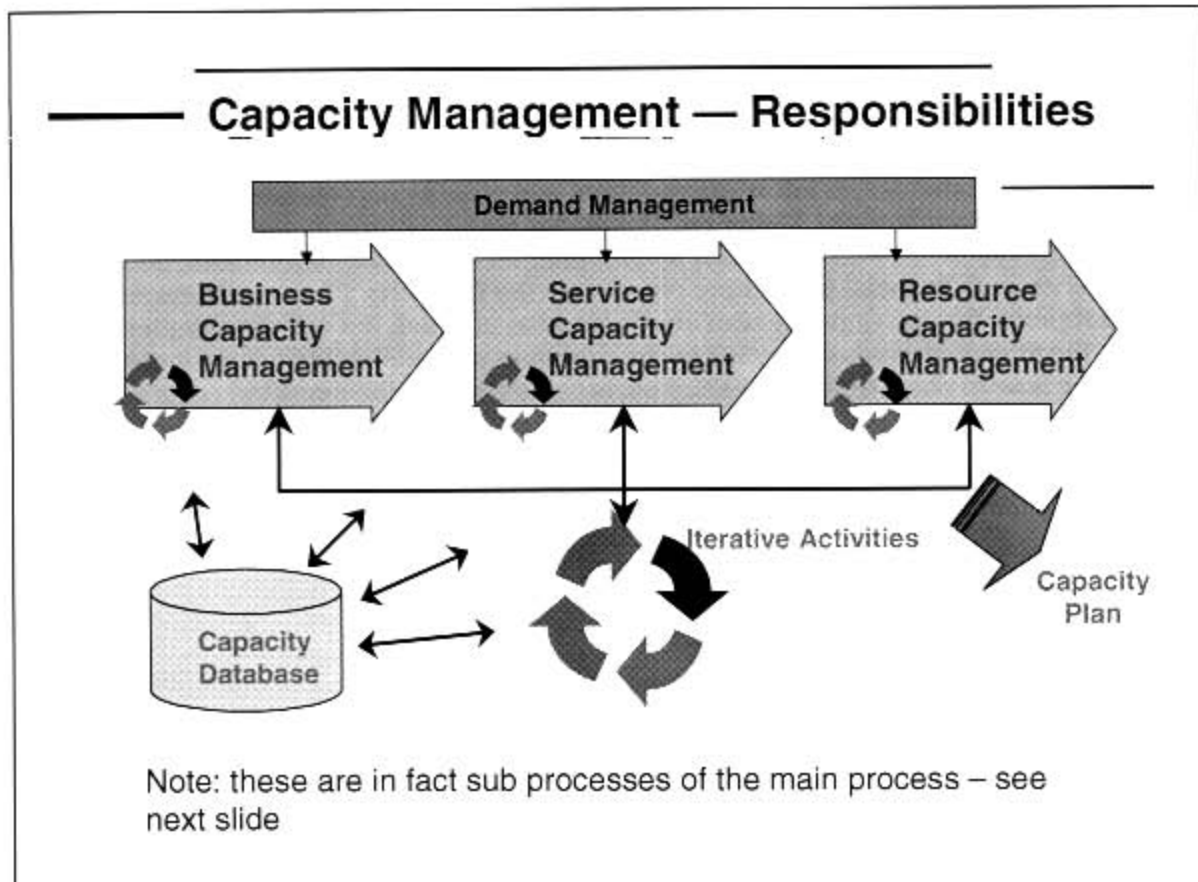
Capacity Management consists of a number of sub-processes, within which there are various activities. The sub-processes of Capacity Management are:

- *Business Capacity Management:* This sub-process is responsible for ensuring that the future business requirements for IT services are considered, planned and implemented in a timely fashion. This can be achieved by using the existing data on the current resource utilization by the various services to trend, forecast or model the future requirements. These future requirements will come from business plans outlining new services, improvements and growth in existing services, development plans etc.
- *Service Capacity Management:* The focus of this sub-process is the management of the performance of the IT services used by the customers. It is responsible for ensuring that the performance of all services, as detailed in the targets in the SLAs and SLRs is monitored and measured, and that the collected data is recorded, analyzed and reported. As necessary, action will be taken to ensure that the performance of the services meets the business requirements. This is performed by staff with knowledge of all the areas of technology used in the delivery of end-to-end service, and will often involve seeking advice from the specialists involved in Resource Capacity Management.
- *Resource Capacity Management:* The focus in this sub-process is the management of the individual components of the IT infrastructure. It is responsible for ensuring that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analyzed and reported. As necessary, action will be taken to manage the available resource to ensure that the IT services that it supports meet the business requirements. In carrying out this work, the Capacity Management process will be assisted by individuals with specialist knowledge in the particular areas of technology.

Each of the sub-processes carry out many of the same activities, but each sub-process has a very different focus: Business Capacity Management is focused on the current and future business requirements, while Service Capacity Management is focused on the delivery of the existing services that support the business and Resource Capacity Management is focused on the technology that underpins all the service provision.

Demand Management: This is an important aspect of the interface between the business and Capacity Management, and has the objective of influencing demand and therefore the use of resources. It requires a full understanding of the business requirements and their demands on IT services and resources. It must be carried out sensitively and without causing damage to the business, Customers, Users or the reputation of IT.

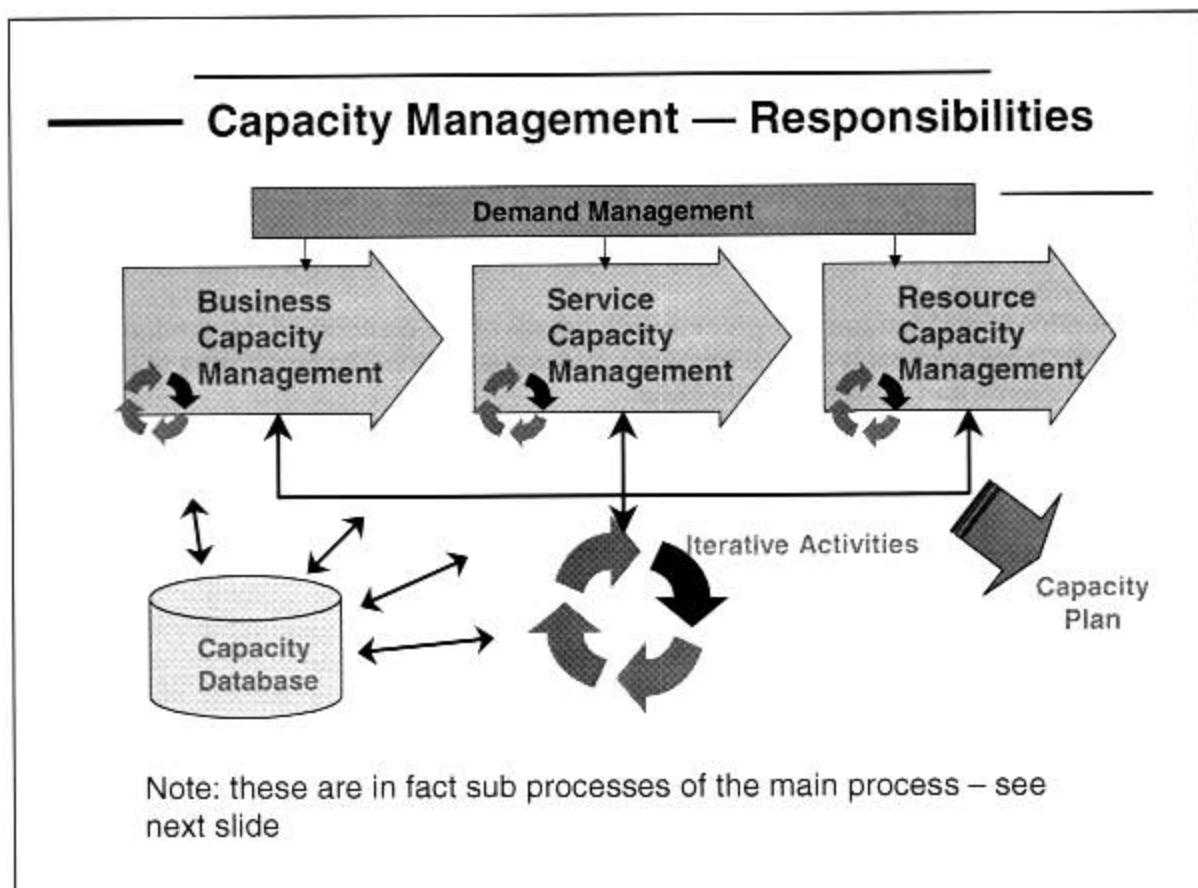
Demand Management can be carried out as part of any one of the sub-processes of Capacity Management.



Student Notes

Iterative Activities: This responsibility ensures and guards that technical resources in the infrastructure provide the best possible value for money. It is done through monitoring, data collection, trend analysis and tuning. It is related to Problem Management through monitoring and tuning because it can prevent the infrastructure for incidents and problems and it can help PM that the infrastructure is used in the best possible way

Capacity Planning provides an information system and ensures appropriate planning. It relies on the **Capacity Management Database (CDB)** for reporting/information on server & network technical data; customer details & forecasts; service details & forecasts; and business volumes & financial data. Other reports are the **Capacity Plan** and Management & technical reports. But the Capacity plan also is the plan in which the current situation is analyzed, the expected needs according to the customer and availability manager are stated, the planning how to come to the new situation is described and the expected costs according to the changes are stated.



Student Notes

The Capacity Management Process

The inputs

There are a number of sources of information that are relevant to the Capacity Management process. Some of these are as follows:

- External suppliers of new technology.
- The organization's business strategy and plans, and financial plans
- The IT strategy and plans and current budgets.
- The Incident and Problem Management processes with incidents and problems relating to poor performance.
- The Service Level Management process with details of the contents of the service level agreements and service level requirements, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs.
- The Change Management process with a forward schedule of changes and a need to assess all changes for their impact on the capacity of the infrastructure.
- The IT operations team with schedules of all the work that needs to be run and information on the dependencies between different services, and the interdependencies within a service.

The sub-processes

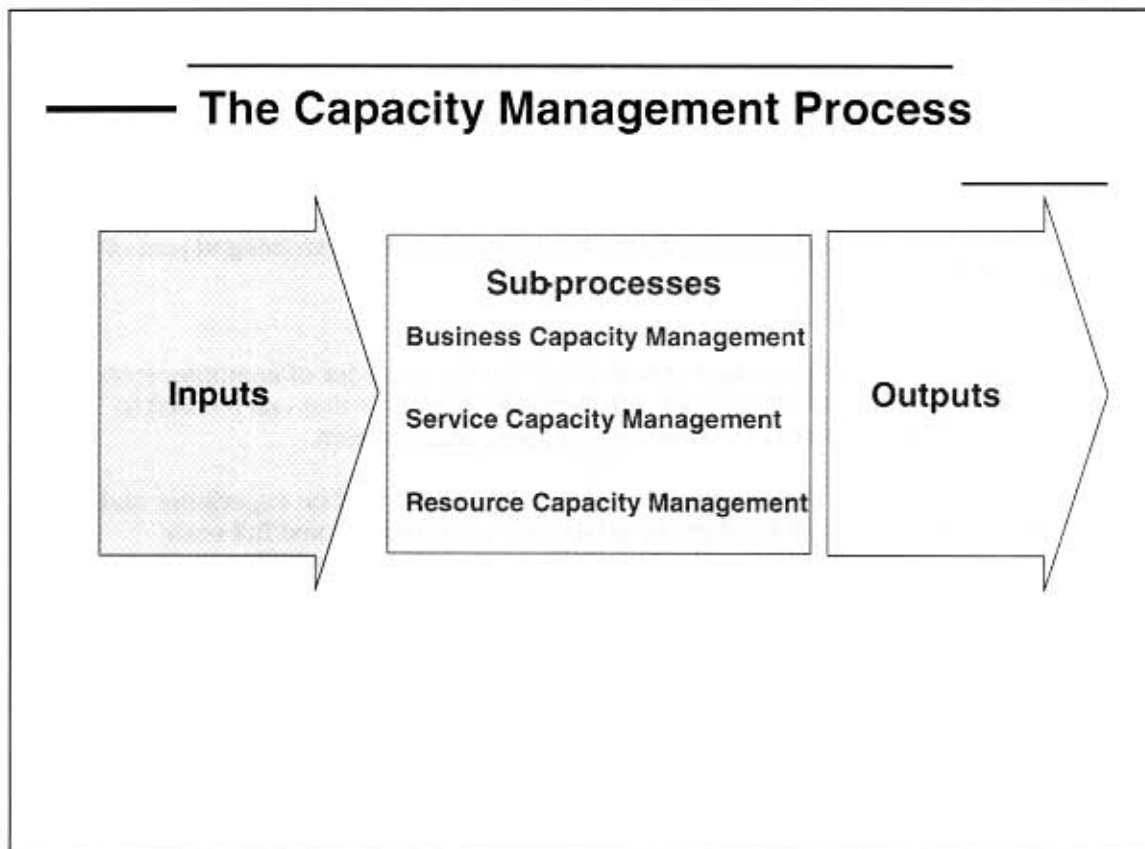
The sub-processes are described on the previous two pages.

The outputs

The outputs of Capacity Management are used within other parts of the process, by other Service Management processes and by other parts of the organization, as follows:

- Within other parts of the Capacity Management process. For example the data monitored and collected as part of Resource and Service Capacity Management will be used in Business Capacity Management to determine what hardware or software upgrades are needed, and when. The *Capacity Database* will hold the information needed by all the sub-processes within Capacity Management.
- By other Service Management processes. For example the Capacity Management process will verify new Service Level Requirements, and will assist the Financial Management process by identifying when money needs to be budgeted for hardware or software upgrades, or the purchase of new equipment.

By other parts of the organization. For example IT Operations will need to implement any changes that Capacity Management may recommend to the schedule of when services are run, to ensure that the most effective and efficient use is made of the available resource. The Capacity Plan will need to be acted upon by the management of the IT service provider and the senior management of the organization.



Student Notes

Sizing and Modeling

Application Sizing

Application Sizing has a finite life-span. It is initiated at the Project Initiation stage for a new application or when there is a major change of an existing application, and is completed when the application is accepted into the operational environment.

The primary objective of Application Sizing is to estimate the resource requirements to support a proposed application change or new application, to ensure that it meets its required service levels. To achieve this Application Sizing has to be an integral part of the applications lifecycle.

Modeling

A prime objective of Capacity Management is to predict the behavior of computer systems under a given volume and variety of work. Modeling is an activity that can be used to beneficial effect in any of the sub-processes of Capacity Management.

The different types of modeling range from making estimates based on experience and current resource utilization information, to pilot studies, prototypes and full scale benchmarks. The former is cheap and a reasonable approach for day-to-day small decisions, while the latter is expensive but may be advisable when implementing a large new project. Some modeling techniques are:

- *Trend analysis* can be done on the resource utilization and service performance information that has been collected by the Service & Resource Capacity Management sub-processes. It can be held in various guises and used to show the utilization of a particular resource over previous period of time, and how it can be expected to change in the future.
- *Analytical modeling* is a representation of the behavior of computer systems using mathematical techniques, e.g. multi-class network queuing theory. Typically a model is built using a software package on a PC, by specifying within the package the components and structure of the configuration that needs to be modeled, and the utilization of the component, e.g. CPU, memory and disks, by the various workloads or applications. When the model is run, the queuing theory is used to calculate the response times in the computer system. If the response times predicted by the model are sufficiently close to the response times recorded in real life, the model can be regarded as an accurate representation of the computer system
- *Simulation modeling* involves the modeling of discrete events, e.g. transaction arrival rates, against a given hardware configuration. This type of modeling can be very accurate in sizing new applications or predicting the effects of changes on existing applications, but can also be very time-consuming and therefore costly. However it can be cost-justified for organizations with very large systems where the cost (millions of dollars) and the associated performance implications assume great importance.
- *Baseline modeling* is when a model is created that reflects accurately the performance that is being achieved. When this model has been created, predictive modeling can be done i.e. ask the “what if?” questions that reflect planned changes. If this baseline model is accurate then the accuracy of the result of the predicted changes can be trusted.

Sizing and Modeling

- *Application Sizing*
To estimate the resource requirements to support a proposed application change to ensure that it meets its required service levels
- *Modeling*
 - Trend analysis
 - Analytical modeling
 - Simulation modeling
 - Baseline models
 - Used to answer the “What if ...” questions

Student Notes

Essentials

Goal

Capacity Management identifies and specifies the demand and needs of the client, translates these needs into the necessary resources and guards the performance of the services.

The Capacity Manager

The Capacity Manager plans the necessary resources and manages the performance of the resources.

The Process

The client has a demand for a new service, which the sub-process Business Capacity Management translates into specific service levels and user volumes. Moreover, the environmental factors and risks are identified that are used at a later stage in the course of a risk analysis (process Availability & Contingency Management). Subsequently, the sub-process Service Capacity Management translates the services into workload/ application level. The sub-process Resource Management then translates the workload requirements into individual resource components. This translation by workload and resource management takes place in accordance with the BSW levelling system (Business-Service-Work unit). Before the Capacity Manager is able to determine a definite resource profile, the Availability & Contingency Management processes determine the necessary additional resources in connection with availability requirements and fall-back arrangements. Data for the various steps are provided by the capacity database. The ultimate resource requirements may result in adjustment of the capacity plan.

The Capacity Management Database (CDB) is used to produce reports on existing and future capacity issues. It is unlikely to be a single database, but will probably exist in several physical locations and will contain many different types of data including business data, service data and technical data.

Iterative activities take care of the monitoring, reviewing and tuning of the services, ensuring that the performance meets the service levels agreed in the SLA.

Remember that Demand Management can be carried out as part of any one of the sub-processes of Capacity Management. Its objective is to influence demand and the subsequent use of resources. To do this effectively requires a full understanding of the business requirements and their demands on those resources.

Capacity management efficiently deploys the resources of the IT organisation and guarantees the performance of the services.

Essentials

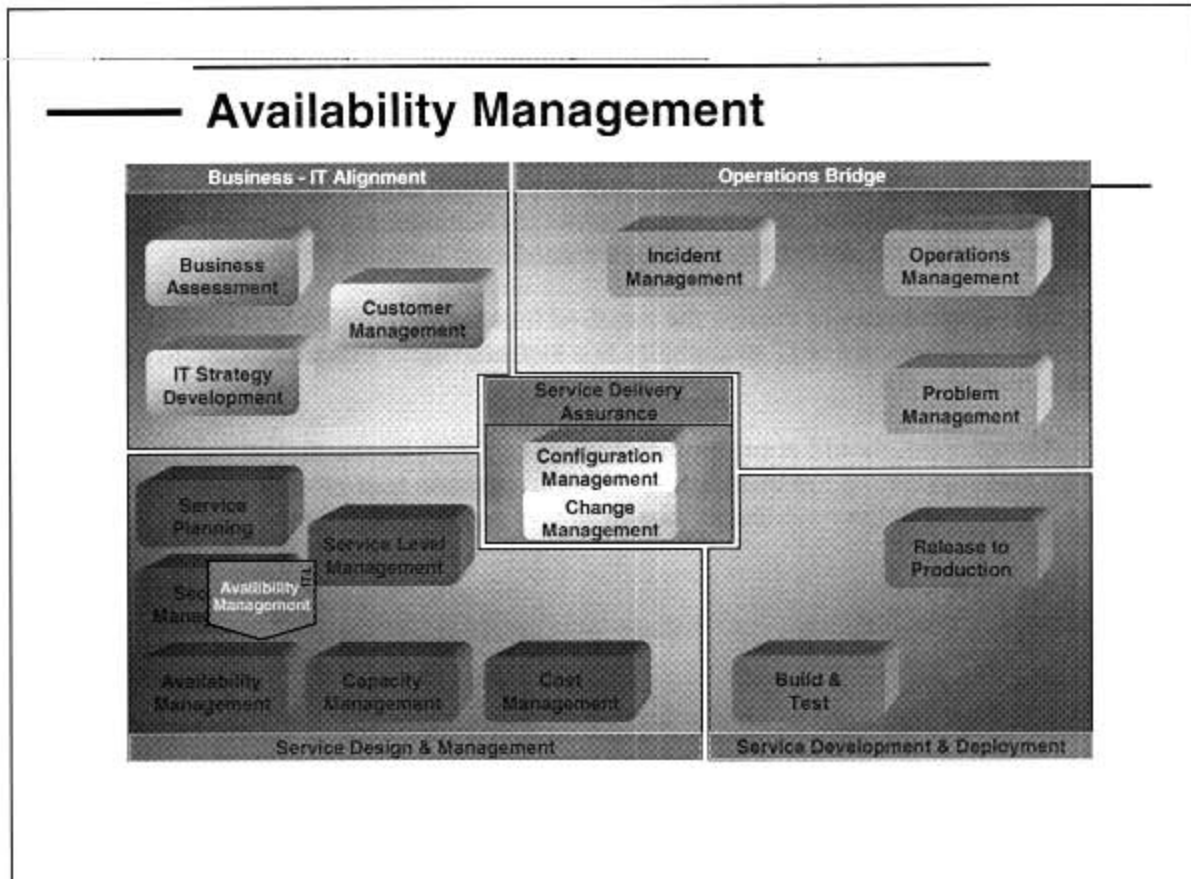
- *Goal*
 - Right amount, right time, efficiently and cost effectively
- *Activities - From Business Needs to Resources*
 - Business Capacity Management
 - Service Capacity Management
 - Resource Management
 - Demand Management
 - Best Value for Money – Monitoring etc.
 - Capacity Planning
 - Capacity Database
- *Application Sizing and Modelling*
- *Defining and monitoring thresholds*

Student Notes

Module 9 — Availability Management

This module introduces Availability Management, a discipline that allows IT management to optimize the use of IT resources, anticipate and calculate expected failures, implement security policies, and monitor for targeted service agreements. Availability Management includes the Security, Serviceability, Recoverability, Maintainability and Resilience of IT resources

Availability Management



Student Notes

Availability Management – Goals

The goal of the Availability Management process is to optimize the capability of the IT infrastructure and supporting organization to deliver a cost effective and sustained level of availability that enables the business to satisfy its business objectives.

This is achieved by determining the availability requirements of the business and matching these to the capability of the IT infrastructure and supporting organization. Where there is a mismatch of the requirement vs. capability, Availability Management will ensure the business are provided with available alternatives and associated cost options.

Availability Management should ensure the required level of availability is provided. The measurement and monitoring of IT availability is a key activity to ensure availability levels are being met consistently.

Availability Management should continuously look to optimize the availability of the IT infrastructure and supporting organization, in order to provide cost effective availability improvements that can deliver evidenced business and end user benefits.

Availability Management — Goals

- *To predict, plan for and manage the availability of services by ensuring that:*
 - All services are underpinned by sufficient, reliable and properly maintained CIs
 - Where CIs are not supported internally there are appropriate contractual arrangements with third party suppliers
 - Changes are proposed to prevent future loss of service

Only then can IT organizations be certain of delivering the levels of availability agreed with customers in SLAs

Student Notes

Availability Management - Responsibilities

The key responsibilities of the process are as follows:

- Determining the availability requirements from the business for a new or enhanced IT service and formulating the availability and recovery design criteria for the IT infrastructure.
- In conjunction with ITSCM determining the vital business functions and impact arising from IT component failure.
- Defining the targets for Availability, Reliability and Maintainability for the IT infrastructure components that underpin the IT service to enable these to be documented and agreed within SLAs, OLAs and contracts.
- Establishing measures and reporting of Availability, Reliability and Maintainability that reflects the business, end user and IT support organization perspectives.
- Monitoring and trend analysis of component's Availability, Reliability and Maintainability
- Reviewing IT Service and component availability and identifying unacceptable levels.
- Investigation of the underlying reasons for unacceptable availability.
- Production and maintenance of an Availability Plan that prioritizes and plans IT availability improvements.

Availability Management — Responsibilities

- *Optimize availability by monitoring & reporting*
- *Determine availability requirements in business terms*
- *Predicting & designing for expected levels of availability & security*
- *Producing the Availability Plan*
- *Collecting, analyzing and maintaining data*
- *Monitoring availability levels to ensure SLAs & OLAs are met*
- *Continuously reviewing & improving availability*

Student Notes

Terminology

Availability: The ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the Customers within the agreed service hours.

Reliability: The ability of component to deliver desired functionality for a given period of time and under certain circumstances. But reliability does not only consider “technology” It also considers people and processes, since a service will be more reliable if Change Management stabilize the environment by controlling it and Problem Management succeed to take away root causes and/or prevent the infrastructure from incidents and problems

The next three aspects are combined in *recoverability*, the ability of a service to recover

Maintainability: The ability of a component or service to return to a state in which the desired functionality will be provided again. Mostly we rely here on processes and people since the component can return sooner if we have a efficient and effective Incident and Problem Process and if the staff has sufficient knowledge to fix the interruption.

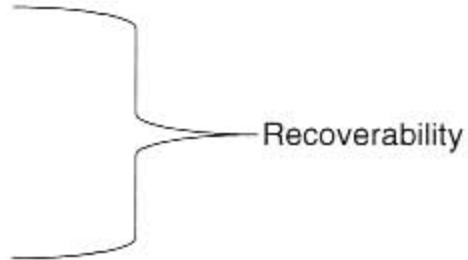
Resilience: The ability of a component or service to keep running where one or more components have failed. Availability always reduces for components in series and increases for components in parallel. That's why resilience most of the time is the ONLY solution when customers request a very high availability.

Serviceability: A contractual term used to define the support to be received from an external supplier in which is covered what they will support in the case of unavailability of one or more services.

Security: The implementation of justifiable controls to ensure continued IT service within secure parameters: Confidentiality, Integrity and Availability. See following pages.

Vital Business Function (VBF): These are the business critical elements of the business process supported by an IT service. An IT service may support a number of business functions that are less critical, e.g. 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

Terminology

- Availability
 - Reliability
 - Maintainability
 - Serviceability
 - Resilience (Redundancy)
 - Security
 - Vital Business Function
- 
- Recoverability

Student Notes

Security

The goal of Security Management is to manage a defined level of security on a service, including managing the reaction to security incidents. By doing this Security Management can ensure the continuity and to protect information of the service and its customers and can help minimize the damage for the service from security breaches. Security Management is intended to assure the safeguarding of information. More specific, the value of the information has to be protected. This value is determined in terms of:

- *Confidentiality*: protecting sensitive information from unauthorized disclosure or intelligible interception;
- *Integrity*: safeguarding the accuracy and completeness of information and software;
- *Availability*: ensuring that information and services are available when required.

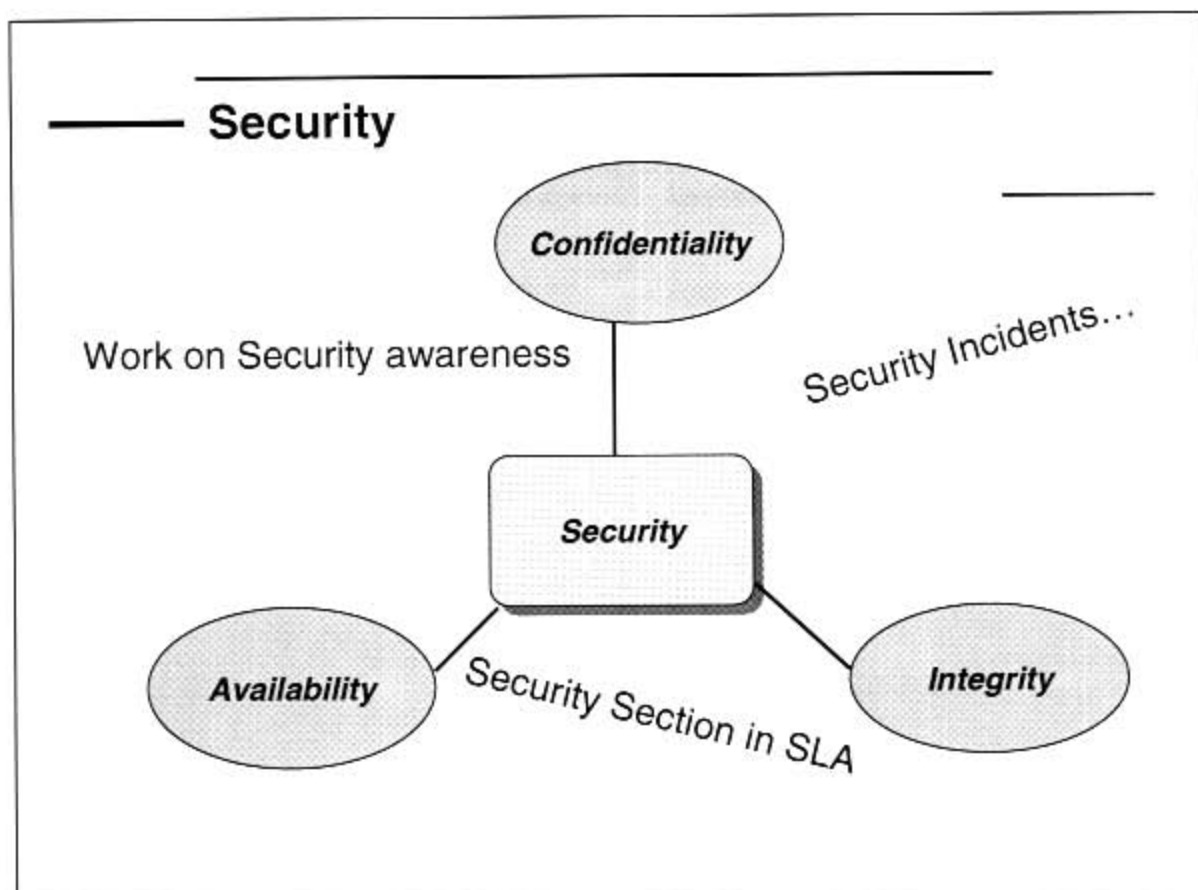
The Security Management function interfaces with IT Service Management processes where security issues are involved. Such issues relate to the Confidentiality, Integrity and Availability of data, as well as the security of hardware and software components, documentation and procedures. For example, Security Management interfaces with Change Management to assess the impact of proposed changes on security, to raise RfCs in response to security problems; to ensure confidentiality and integrity of security data and to maintain the security when software is released into the live environment.

The Incident Management process is the main liaison point for *security incidents*. Security incidents need to be defined according to *SLA security requirements* that are stated in the *security section* of the SLA, so they can be identified within the incident management process

Each SLA must have a security section.

Availability Management can gain guidance from the information contained within the organizations IT security policy and associated procedures and methods. However, the following are typical security considerations that must, amongst others be addressed:

- Products and services must only be available to authorized personnel.
- Products and services must be recoverable following failure to ensure confidentiality and integrity are not compromised and Availability of service not further compromised.
- Products and services must be recoverable within secure parameters, i.e. must not compromise IT security policy
- Physical access to computer and network equipment should be restricted to authorized personnel only.
- Logical access to software should be restricted to authorized personnel only.
- Operating Systems and Systems Management command authority should be commensurate with role and responsibility.
- Data must be available to authorized personnel at agreed times as specified in the SLA.
- OLAs and underpinning contracts must reflect the adherence to security controls required by the IT support organization.

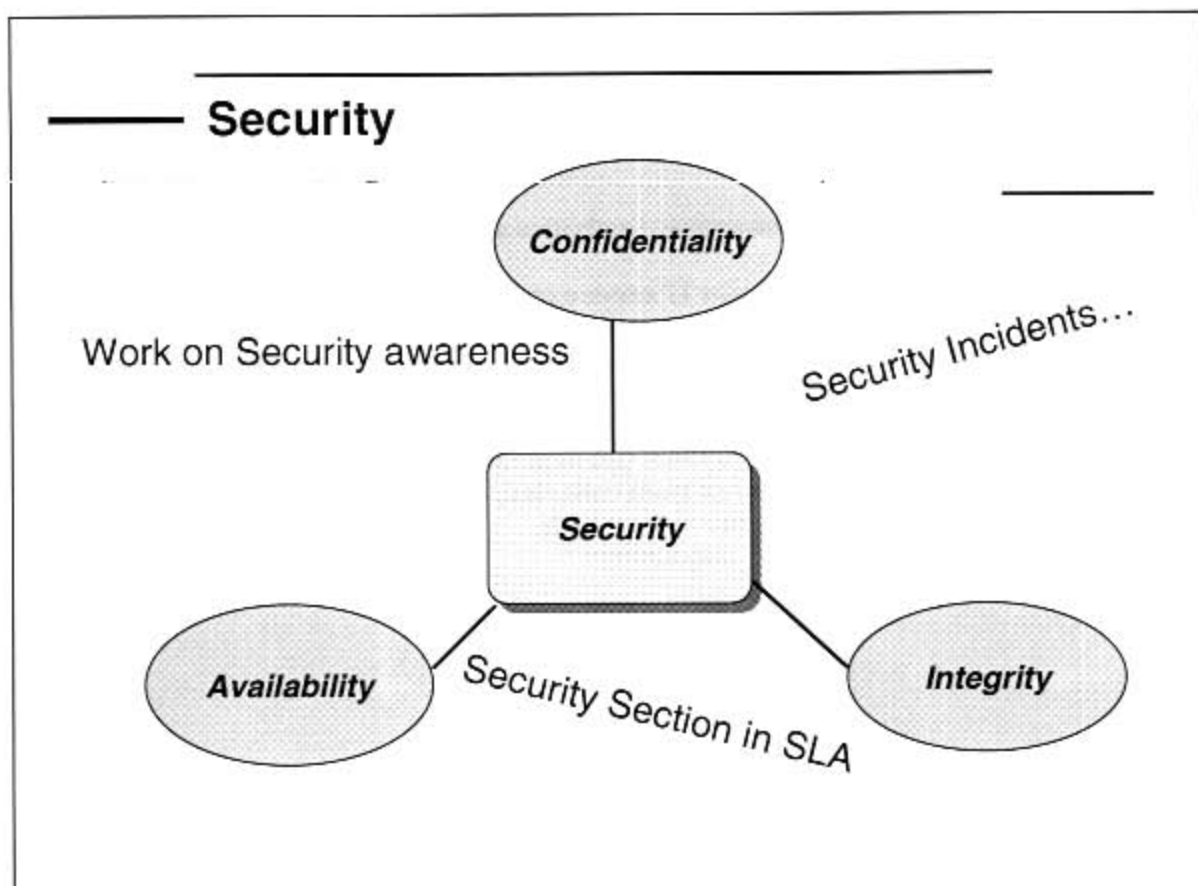


Student Notes

Module 9 Availability Management

Note: to prevent confusion between processes, 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 is NOT one of the ITIL processes covered by ITSM but interfaces with it where security issues are involved. There is a separate ITIL book on Security Management.



Student Notes

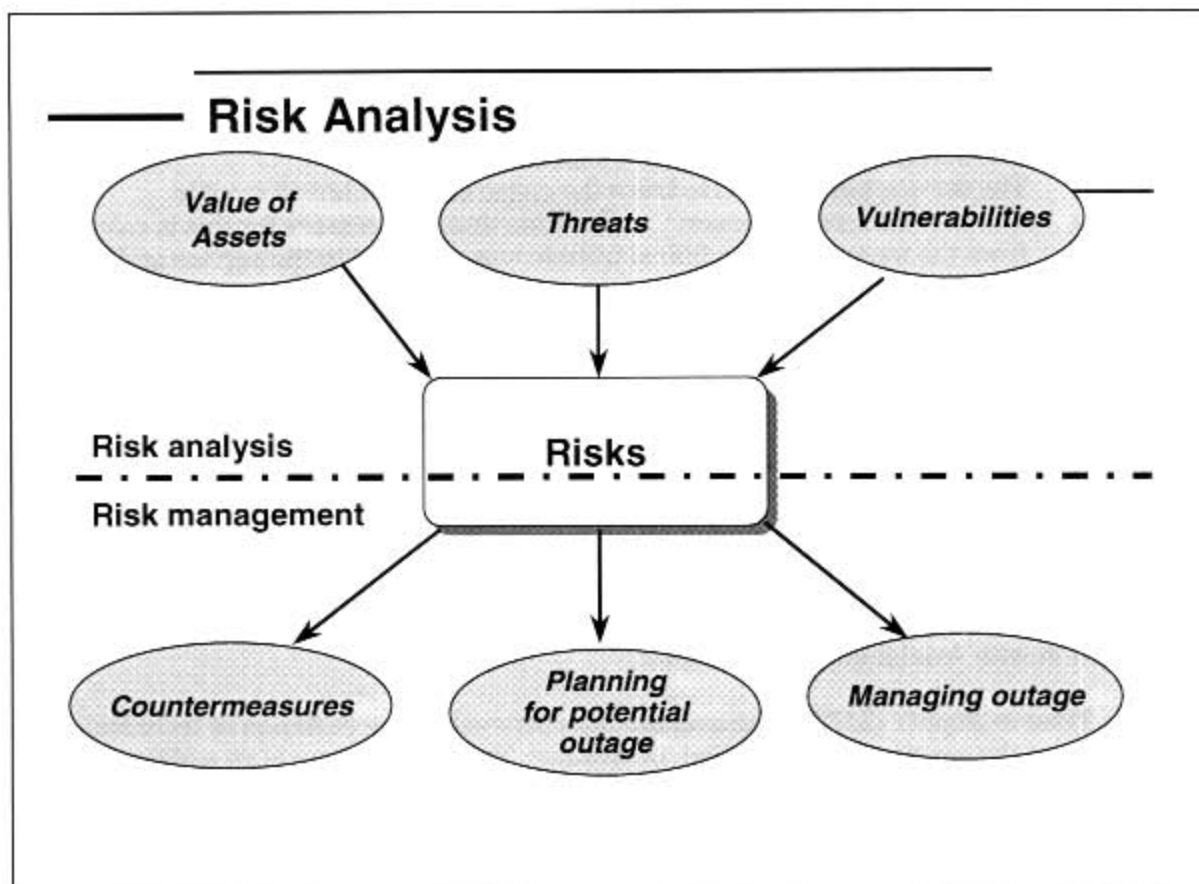
Risk Analysis

To assess the vulnerability of failure within the configuration and capability of the IT support organization it is recommended that the proposed IT infrastructure design and supporting organization (internal and external suppliers) are subject to a formal risk analysis.

Risk is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat.

As a minimum, the following risk assessment activities should be performed:

- Identify risks – i.e. risks to particular IT service components (assets) that support the business process that will cause an interruption to service.
- Assess threat and vulnerability levels – the threat is defined as “how likely it is that an service disruption will occur” and the vulnerability is defined as “whether, and to what extent, the organization will be affected by the threat materializing”.
- Assess the levels of risk – the overall risk can then be measured. This may be done as a measurement if quantitative data has been collected, or qualitative using a subjective assessment of, for example, low, medium or high.



Student Notes

The Unavailability Life-cycle

During the analyzing and planning of services, certain measuring values are led from the phases that a service goes through during technical trouble.

Occurrence of the incident - The user realizes the technical trouble.

Detection The service is informed on the technical trouble

Diagnose The service takes action to trace the cause of the technical trouble

Reparation The service repairs the service. The time that is necessary for this is calculated from the moment the technical trouble was reported to the service and can be divided into:

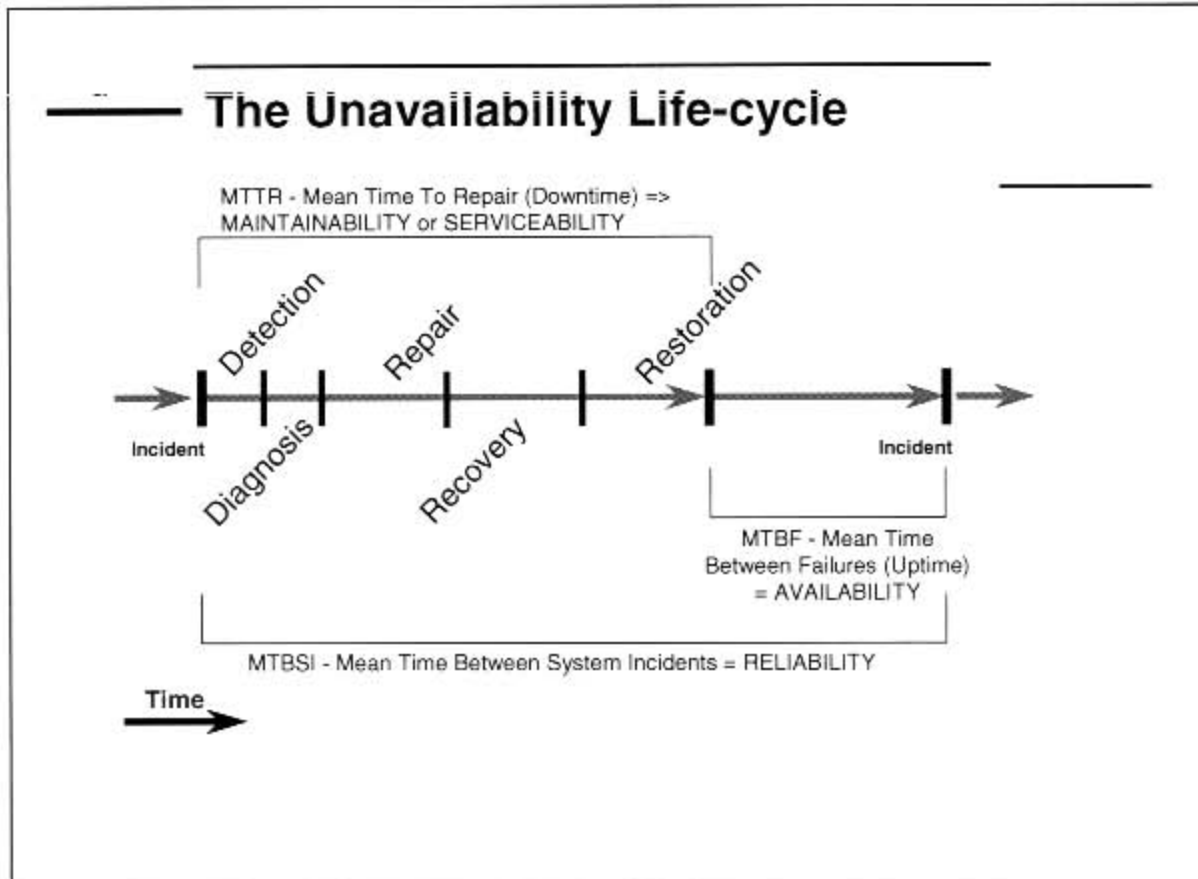
- Time of travel (in case an external party is required) that is necessary.
- Time that is necessary for diagnosis and reparation.

Restoration Time that is necessary to get the service back to working, including activities as configuration and initialization, and the time that is necessary to make the service available to the user.

The downtime partially dependant on how fast the reaction of the IT-organization and possible external suppliers is. To get a good view of that, the average values of the measuring are taken. These averages are used to make predictions on the expected availability of a service in the future and for discussing if improvements are urgent. The following values are most common with Availability Management:

- *Mean Time to Repair (MTTR)* the average time between the occurrence of technical trouble and the repair of it, also called 'Downtime'. The specific time is an addition sum of the detection time and the processing time. This value concerns the elasticity and Serviceability of a service. MTTR measures Maintainability and/or Serviceability
- *Mean Time Between Failures (MTBF)* the average time between the repair of an incident and the reporting of the next incident, also called 'Uptime'. This value concerns the reliability of a service. MTBF measures Availability
- *Mean Time Between System Incidents (MTBSI)* the average time between the reporting of two sequentially occurring incidents, the sum of MTTR and MTBF. MTBSI measures Reliability

From the relation between MTBF and MTBSI it is possible to subtract information on if there is a lot of short technical problems or some large technical problems.



Student Notes

When Is a Service Available?

Customer perception of downtime may differ from that of the IT department because of delays in reporting incidents and the business perception of service restoration extending to the processing of any business back log. Suppliers may also talk about MTTR in a different way to the internal IT department.

Also, for the customer the delivery points are at the desktop and not within the IT department, which also results in different perception about the availability that is delivered. IT thinks it delivers 98% but in reality – at the customer desktop – it is only 94% because of the fact that an end-to-end service is build on several components and that service availability is therefore an result of the availability of all those components together.

When reporting availability data to the business, we should use the language that the business uses. To the business downtime means: idle workforce, lost income, dissatisfied end customers, threat of legal action and failure to comply with legislation. These are clearly related to the impact codes used for incidents.

Both the total duration of downtime and the frequency of downtime affect service quality.

The next thing is an example calculation:

Service A agreed service times 5x8h/week
In week 43 the service was down for 4 hours
then the availability = $(40-4)/40 \times 100\% = 90\%$

This looks simple but – again – in reality it is not simple at all. It all depends on what is agreed, what do we measure, how do we measure, how many customers do we measure and when do we measure. E.g. if only one out of 1000 customer is down for 4 hours is the service then really down for 10% or is it down for 0,01%. For that one customer it is 10% but for the whole company it is a lot less.

Basic availability calculation:

$$\text{Availability} = \frac{\text{Agreed Service Time} - \text{Actual Down Time during Agreed Service Time}}{\text{Agreed Service Time}} \times 100$$

Even when meeting a SLA a service can be perceived as not being available. For example, an Invoicing application is used by the Finance Department Monday – Friday between the hours of 9am and 5pm. A daily backup of this application is done Monday - Friday between the hours of 8pm and 10pm. This scheduled backup has been agreed with the Customer and is in the SLA. A Finance Department User works overtime; at 8pm he loses access to the application due to the backup in progress. To the User the service is unavailable but the SLA has not been breached.

When Is a Service Available?

“An IT service is
not available
to a customer if the functions required during
Service Hours at that particular *Location*
cannot be used although the
agreed SLA conditions
are being met”

NB Simplistic calculation of % availability in the ITIL book is

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

But what does 98% Availability really mean?

Student Notes

Availability Formula

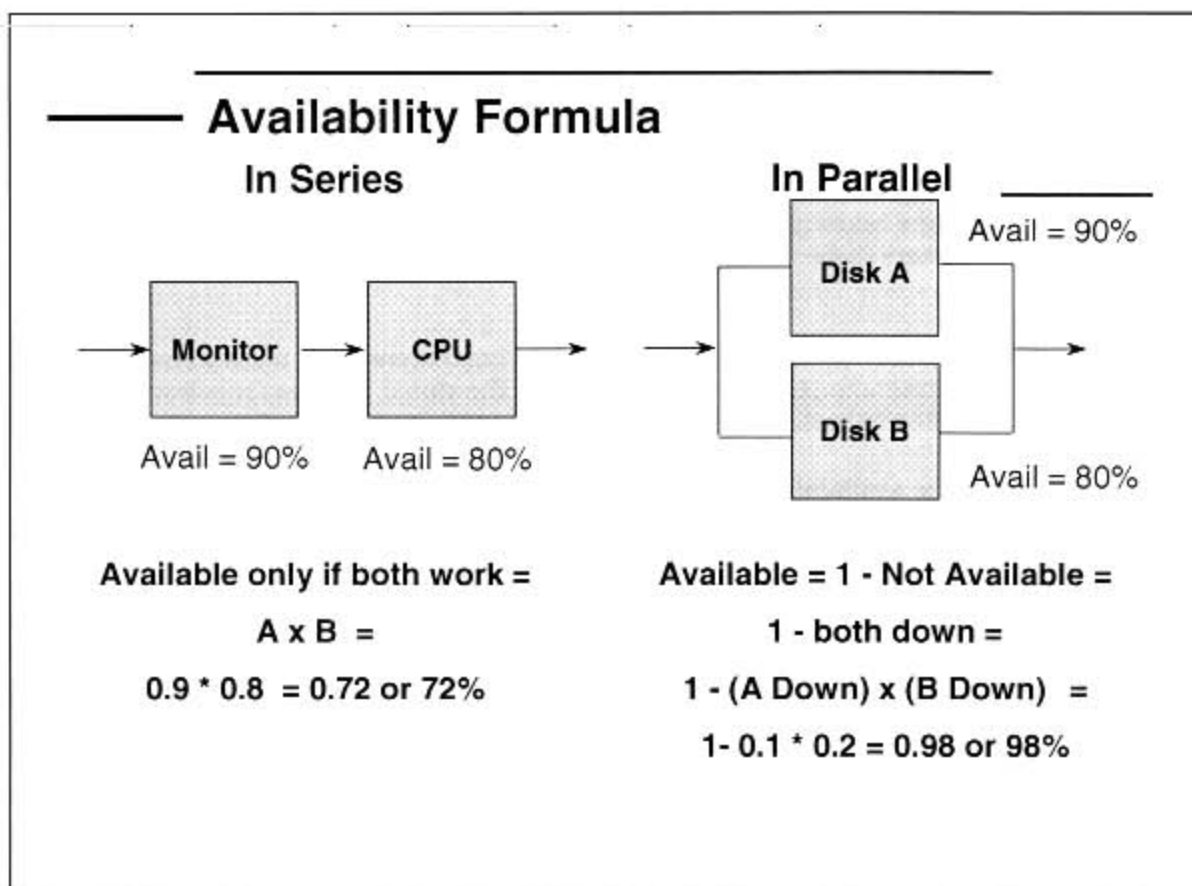
Excessive complexity in calculating predicted availability can be avoided by making a decision on the degree of granularity. The calculation could stay at the level of:

PC availability x Network Availability x Mainframe Availability

Availability always reduces for components in series and increases for components in parallel. However, note that these are long-term predictions and are not guarantees of the level of availability that will be achieved in reality. Also note that some components must be in series.

When making calculations for elements in parallel the availability = 100% - unavailability. Unavailability is only true if all parallel components are broken down. So by having two elements with availability A and availability B in parallel, the availability of the system would become: $100\% - (A \text{ and } B \text{ down}) = 100\% - (100\% - A) \times (100\% - B)$

Note that the predicted failure rate will change throughout a CT's lifecycle.



Student Notes

Essentials

Goals

Availability Management identifies, defines and prepares the measures that are necessary to guarantee the requested availability of services. They monitor the availability for outages and recommend changes to prevent future loss of service

The Availability Manager

The Availability Manager takes measures to improve resilience, concludes maintenance contracts and administers these. He also develops and maintains contingency plans.

Responsibilities

Availability Management is concerned with the design; implementation, measurement and management of IT Infrastructure Availability to ensure the stated business requirements for Availability are consistently met. Availability Management is responsible for:

- Determining the availability requirements from the business for a new or enhanced IT service and formulating the availability and recovery design criteria for the IT infrastructure.
- In conjunction with ITSCM determining the vital business functions and impact arising from IT component failure.
- Defining the targets for Availability, Reliability and Maintainability for the IT infrastructure components that underpin the IT service to enable these to be documented and agreed within SLAs, OLAs and contracts.
- Establishing measures and reporting of Availability, Reliability and Maintainability that reflects the business, end user and IT support organization perspectives.
- Monitoring and trend analysis of component's Availability, Reliability and Maintainability
- Reviewing IT Service and component availability and identifying unacceptable levels.
- Investigation of the underlying reasons for unacceptable availability.
- Production and maintenance of an Availability Plan that prioritizes and plans IT availability improvements.

Risk analysis is an important part of Availability Management. Risk is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat. Use a model like the one described earlier in this module when analyzing potential risks.

Remember that calculating availability is one of the more difficult procedures within the Availability Management process. However it is necessary to help formulate Availability targets for IT components and IT Services. These should be agreed upon and reflected in the SLA.

Availability Management Process

The scope of Availability Management covers the design, implementation, measurement and management of IT infrastructure availability. Availability Management commences as soon as the availability requirements for an IT service is clear enough for these to be articulated. It's an ongoing process, finishing only when the IT service is decommissioned.

Essentials

- *Goals*
 - Plan and manage CI availability
 - Ensure contractual arrangements are in place internally and with third party suppliers
 - Changes are proposed to prevent future loss of service
- *Responsibilities*
 - Predicting & designing for expected levels of availability & security; Availability Plan; collecting, analyzing and maintaining data; monitoring availability levels to ensure SLAs & OLAs are met
- *Assessing risk - CRAMM*
- *Calculating availability*
 - MTBSI
 - MTTR
 - MTBF
 - % availability formulae

Student Notes

The key inputs to the Availability Management process are:

- The availability requirements of the business for a new or enhanced IT service.
- A business impact assessment for each vital business function underpinned by IT
- The Availability, Reliability and Maintainability requirements for the IT infrastructure components that underpin the IT service(s).
- Information on IT service and component failure(s), usually in the form of Incident and Problem records.
- A wide range of configuration and monitoring data pertaining to each IT service and component..
- Service level achievements against agreed targets for each IT service with an agreed SLA.

The key outputs from the Availability Management process are:

- Availability and Recovery design criteria for each new or enhanced IT service.
- Details of the availability techniques that will be deployed to provide additional infrastructure resilience to prevent or minimize the impact of component failure to the IT service.
- Agreed targets of Availability, Reliability and Maintainability for the IT infrastructure components that underpin the IT service(s).
- Availability reporting of Availability, Reliability and Maintainability to reflect the business, end user and IT support organization perspectives.
- The monitoring requirements for IT components to ensure that deviations in Availability, Reliability and Maintainability are detected and reported.
- Availability Plan for the proactive improvement of the IT infrastructure availability.

Essentials

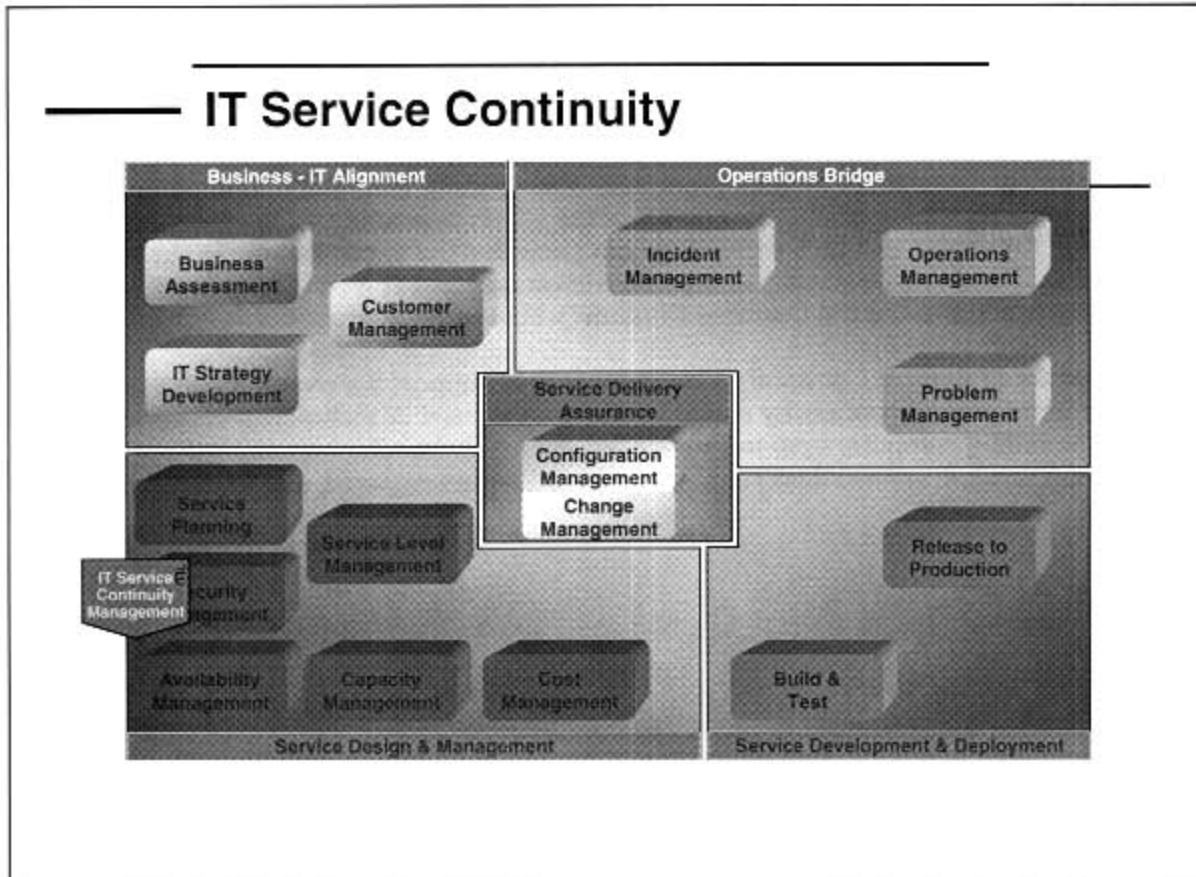
- *Goals*
 - Plan and manage CI availability
 - Ensure contractual arrangements are in place internally and with third party suppliers
 - Changes are proposed to prevent future loss of service
- *Responsibilities*
 - Predicting & designing for expected levels of availability & security; Availability Plan; collecting, analyzing and maintaining data; monitoring availability levels to ensure SLAs & OLAs are met
- *Assessing risk - CRAMM*
- *Calculating availability*
 - MTBSI
 - MTTR
 - MTBF
 - % availability formulae

Student Notes

Module 10 — IT Service Continuity Management

This module introduces IT Service Continuity Management, the discipline that covers unexpected IT service losses. IT Service Continuity Management involves the planning for alternate CIs (Configuration Items), and could include single CIs or an entire alternate (or "Disaster Recovery") site with alternate IT resources. Analyzing risks, researching options, planning alternatives, and documenting the plan are all part of IT Service Continuity Management. IT Service Continuity Management is also responsible for testing the Contingency Plan.

IT Service Continuity Management



Student Notes

Continuity Management

Since the IT Infrastructure Library produced its book on 'Contingency Planning', there have been significant changes in technology and the way in which technology is used within business. The dependencies between business processes and technology are now so intertwined that Contingency Planning (or Business Continuity Management as it is now sometimes referred) incorporates both a business element (Business Continuity Planning) and a technology element (IT Service Continuity Management Planning). 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. In this chapter it is assumed that business continuity is the main driver and that IT Service Continuity Management is a sub-set of the Business Continuity Management process.

The mission for 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.

Continuity Management

Why Plan???

- *Increased business dependency on IT*
- *Reduced cost and time of recovery*
- *Cost to customer relationship*
- *Survival*

**Many businesses fail within a year
of suffering a major IT disaster!**

Student Notes

The Process (1)

Stage 1 - Initiation

The activities to be considered during the initiation process depend on the extent to which contingency facilities have been applied within the organization. Some parts of the business may have established individual continuity plans based around manual workarounds and IT may have developed contingency plans for systems perceived to be critical. This is good input to the process, however, effective ITSCM is dependent on supporting critical business functions and ensuring that the available budget is applied in the most appropriate way.

Stage 2 - Requirements Analysis and Strategy Definition

This stage provides the foundation for ITSCM and is a critical component in order to determine how well an organization will survive a business interruption or disaster and the costs that will be incurred.

This stage can effectively be split into two sections:

Requirements – perform Business Impact Analysis and risk assessment;

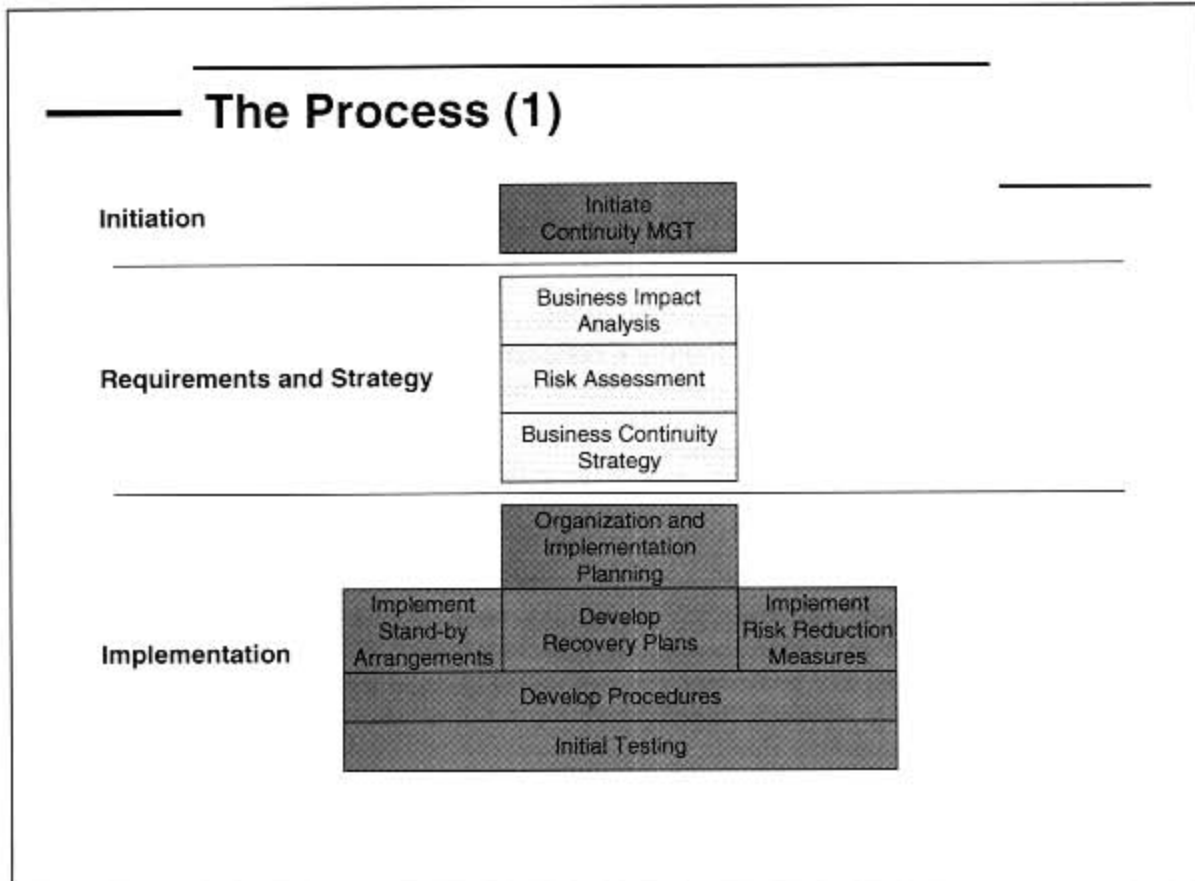
Strategy – determine and agree risk reduction measures and recovery options to support the requirements.

Stage 3 - Implementation

Once the strategy has been agreed the Business Continuity lifecycle moves into the implementation stage, involving IT at a detailed level. The implementation stage consists of the following processes:

- Establish the organization and develop implementation plans.
- Implement stand-by arrangements.
- Implement risk reduction measures.
- Develop recovery plans.
- Develop procedures.
- Undertake initial tests.

Each of the above is considered with respect to the specific responsibilities that IT must action.



Student Notes

Business Impact Analysis

The second driver in determining ITSCM requirements is *the likelihood that a disaster or other serious service disruption will actually occur*. This is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat

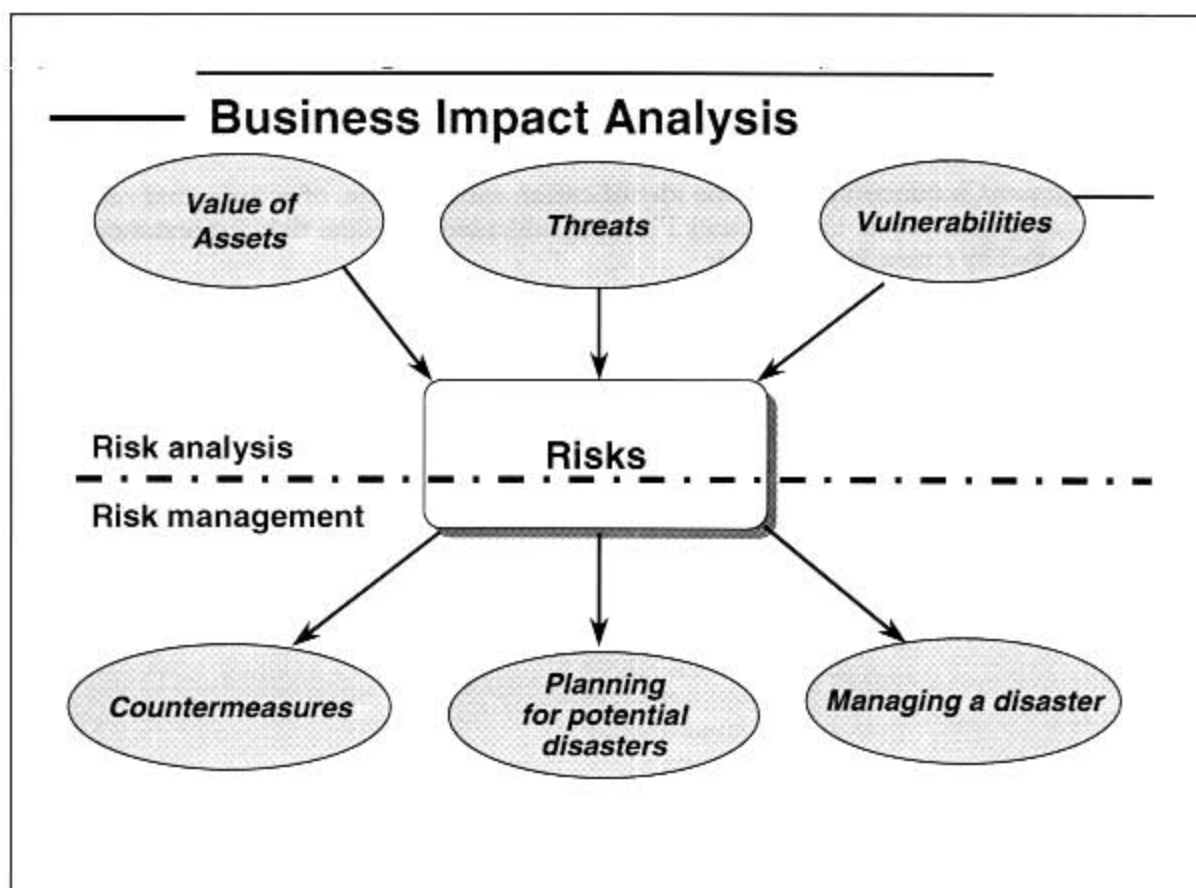
The top section of the model (based on the CCTA Computer Risk Analysis & Management Methodology - CRAMM) refers to assets - if an organization's assets are highly vulnerable and there is a high threat and the impact is high, there would be a high risk. Countermeasures are then applied to manage the business risks by protecting the assets.

As a minimum, the following risk assessment activities should be performed:
Identify risks – i.e. risks to particular IT service components (assets) that support the business process, which will cause an interruption to service. Typical risks for IT include:

- Damage or denial of access to premises.
- Loss of IT systems, networks, PABX, Automatic Call Distribution systems, firewalls, cryptographic systems, Public Key Infrastructure (PKI), etc.
- Loss of data or loss of integrity to data.
- Loss of network services including telecommunications providers.
- Unavailability of key staff, e.g. only one person knowing how to maintain a particular critical network server or business application and no documentation existing.
- Failure of partner or service providers, e.g. outsourcing organizations providing IT systems or services (e.g. support, development or maintenance).
- Loss of service from a partner due to excessive demand on services (e.g. excessive hits or volumes from web-site).
- Breach of security (e.g. fraud, sabotage, computer viruses or malicious software).
- Loss of environment (e.g. air-conditioning).
- Loss of critical paper records or media (e.g. manuals, documents, backups, etc.).
- Loss of utilities (e.g. power, gas, water).

Assess threat and vulnerability levels – the threat is defined as “how likely it is that an service disruption will occur” and the vulnerability is defined as “whether, and to what extent, the organization will be affected by the threat materializing”. A threat is dependent on such factors as:

- Likely motivation, capability and resources for deliberate service disruptions.
- For accidental service disruptions, the organization's location, environment, and quality of internal systems and procedures.
- Business processes are vulnerable where there are single points of failure for the delivery of it services.

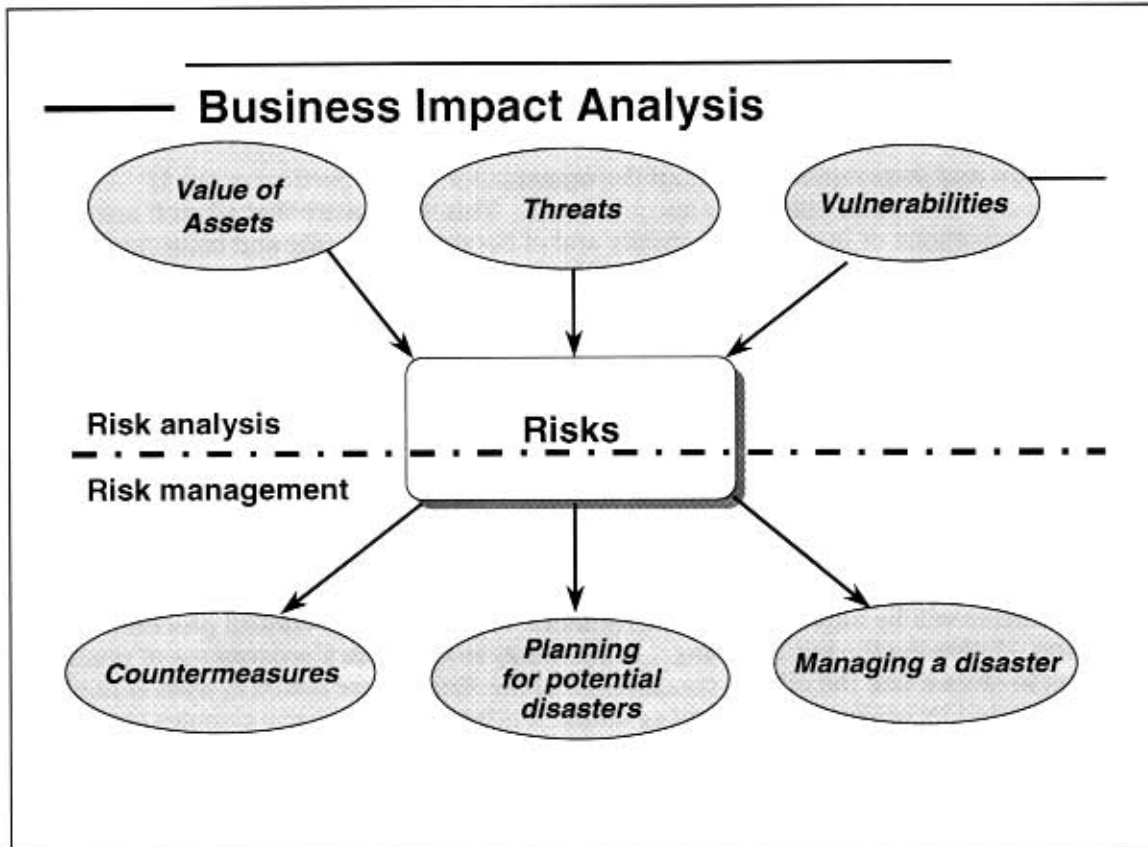


Student Notes

Assess the levels of risk – the overall risk can then be measured.

Following the risk analysis it is possible to determine appropriate countermeasures or risk reduction measures (ITSCM mechanisms) to manage the risks, i.e. reduce the risk to an acceptable minimum level or mitigate the risk.

Risk Management is concerned with the identification and selection of actions that reduce risks to an acceptable level. Contingency Planning addresses residual risk, for instance when PCs are attacked by a new kind of virus



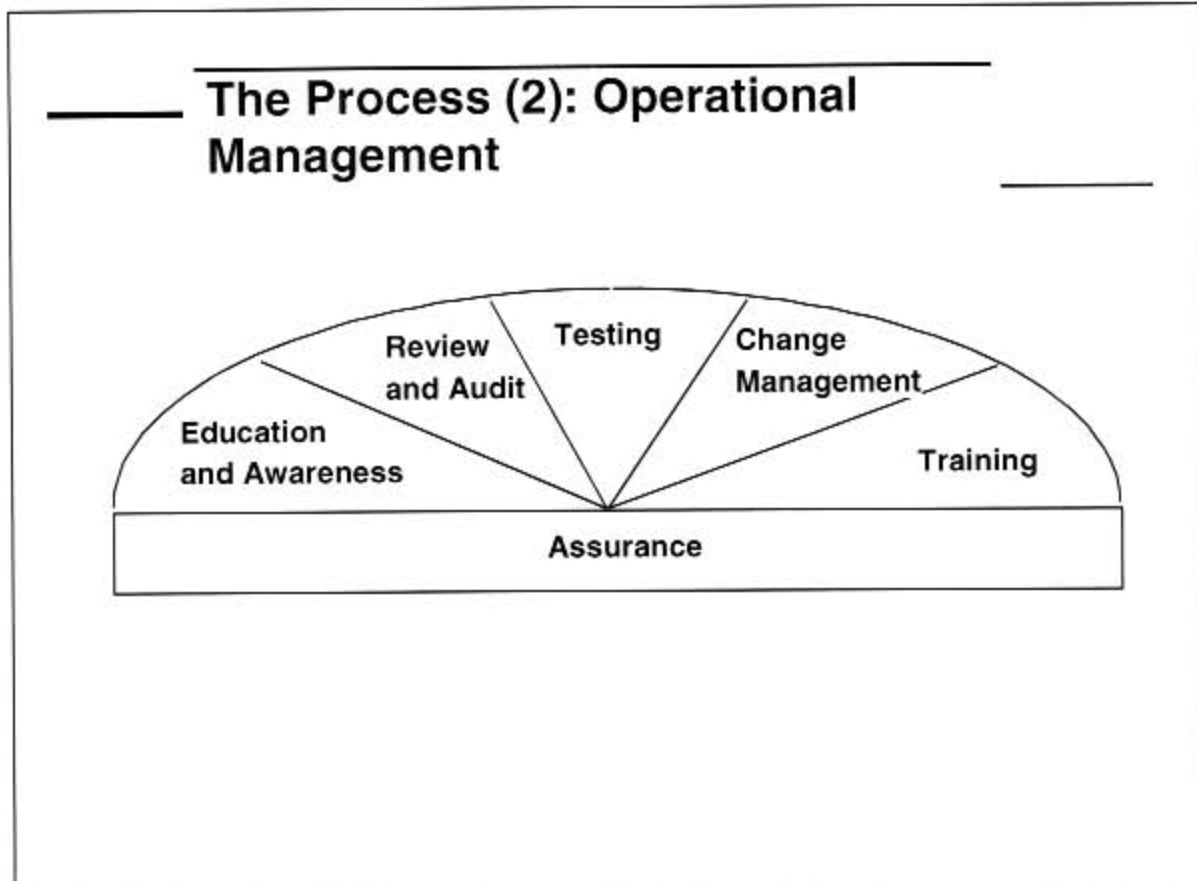
Student Notes

The Process (2): Operational Management

Stage 4 – Operational Management

Once the implementation and planning has been completed there is a need to ensure that the process is maintained as part of business as usual. This is achieved through operational management and includes:

- *Education and awareness* throughout the organization and in particular, the IT department, for service continuity specific items. This will ensure that all staff are aware of the implications of Business Continuity and of Service Continuity and consider these as part of their normal working routine and budget.
- *Training* – IT may be involved in training the non-IT literate business recovery team members to ensure that they have the necessary level of competence to facilitate recovery.
- *Review* – regular review of all of the deliverables from the ITSCM process needs to be undertaken to ensure that they remain current. With respect to IT this will be required whenever there is a major change to the IT infrastructure, assets or dependencies such as new systems or networks or a change in service providers, as well as when there is a change in business direction, business strategy or IT strategy. As organizations typically have rapid change, it is necessary to invest in an ongoing review programme and incorporate ITSCM into the organizational business justification processes. New requirements will be implemented in accordance with the change control process.
- *Testing* – following the initial testing it is necessary to establish a programme of regular testing to ensure that the critical components of the strategy are tested at least annually or as directed by senior management or audit. It is important that any changes to the IT infrastructure are included in the strategy, implemented in an appropriate fashion and tested to ensure that they function correctly within the overall provision of IT services.
- *Change control* – following tests and reviews and in response to day to day changes, there is a need for the ITSCM plans to be updated. ITSCM must be included as part of the change management process to ensure that any changes in the infrastructure are reflected in the contingency arrangements provided by IT or third parties. Inaccurate plans and inadequate recovery capabilities may result in the failure of ITSCM.
- *Assurance* – the final process in the ITSCM lifecycle involves obtaining assurance that the quality of the ITSCM deliverables is acceptable to senior business management and that the operational management processes are working satisfactorily.



Student Notes

The Options

It would be hard to justify the “*Do nothing*” option, since if a system does not need to be recovered, its necessity has to be considered. Customers should be told when this option has been adopted!

- *Manual workarounds.* Can be an effective interim measure until normal IT Services are restored.
- *Reciprocal arrangements.* Organizations agree to back each other up in an emergency, rarely used now except for off-site storage because of practical difficulties, e.g. limited excess IT capacity.
- *Gradual recovery* (sometimes referred to as a “cold standby”). Usually consists of an empty computer environment accept for power and telecommunications, in which an organization can install its own equipment. May be used where a business can function for a period of 72 hours or more without IT services. Can be internal or external, fixed or portable, possibly with guaranteed equipment delivery.
- *Intermediate recovery* (sometimes referred to as “warm standby”). Typically involves the re-establishment of critical systems and services within a 24-7 hour period. Can be internal or external, fixed or portable, and consists of a computer environment containing recovery IT equipment that can be configured to support the business.
- *Immediate recovery* (sometimes referred to as a “hot standby”). Would involve the use of an alternative site with continuous mirroring of live equipment and data. Can be internal or external and is the most expensive option. Would only be used for critical business services here loss of service would cause an immediate business impact.

Choosing one of these options usually depends a lot on the finances available or what the business wants to invest in Service

The Options

- *Do nothing*
- *Manual workarounds*
- *Reciprocal arrangements*
- *Gradual Recovery (cold standby)*
- *Intermediate Recovery (warm standby)*
- *Immediate Recovery (hot standby)*

IMPORTANT: HAVE YOU PLANNED TO RESTORE THE NORMAL SERVICE.....

Think of the security risks when a disaster has happened

Student Notes

The Seven Sections of the Plan

Administration - when and how to invoke the plan; programs of action and personnel involved.

The IT Infrastructure – the parts of the infrastructure that are subject to continuity management

IT Infrastructure Management Operating procedures - instructions required to recommence operations, including SLA details and manuals.

Personnel - information about personnel to transfer to site, who is going to replace personnel that will not come to the contingency site or – in worst case – died. In times of disaster the staff is more interested in how their own family and property is doing than how the IT is doing. We have to come up with a plan to replace staff

Security - details of home site, contingency site and remote storage.

Contingency site - location, contacts, facilities, security and transport arrangements to the site, how to build the site, how to implement infrastructure and applications, how to restore data etc.

Return to Normal - how, where, how long will it take to restore the whole infrastructure especially if we do not restore the whole side but only the most important services.

The Seven Sections of the Plan

- 1. Administration*
- 2. The IT infrastructure*
- 3. IT infrastructure management & operating procedures*
- 4. Personnel*
- 5. Security*
- 6. Contingency site*
- 7. Return to normal*

Student Notes

Roles in Normal Operation and in a Crisis

Normal Operation

The table below outlines the typical responsibilities for ITSCM during times of normal operation. These responsibilities should be clearly defined, communicated to the managers concerned and documented in appropriate role or job descriptions.

In a Crisis (invocation responsibilities)

The table below outlines the invocation responsibilities following a disruption to the normal operating environment. The invocation of crisis control and management responsibilities change in line with command, control and operational roles and responsibilities outlined in the crisis control and recovery plans. These include responsibilities for taking corrective action to minimize impact and contingency or recovery facility invocation.

<i>NORMAL OPERATION</i>	<i>IN A CRISIS</i>
<i>Board level</i>	
Initiate IT Service Continuity, set policy, allocate responsibilities, direct and authorize	Crisis management, corporate decisions, external affairs
<i>Senior Management</i>	
Manage IT Service Continuity, accept deliverables, communicate and maintain awareness, integrate across organization	Co-ordination, direction and arbitration, resource authorization
<i>Junior Management</i>	
Undertake IT Service Continuity analysis, define deliverables, contract for services, manage testing and assurance	Invocation, team leadership, site management, liaison and reporting
<i>Supervisors and Staff</i>	
Develop deliverables, negotiate services, perform testing, develop and operate processes and procedures	Task execution, team membership, liaison

Roles in Normal Operation and in a Crisis

- *Board Level*
- *Senior Management*
- *Junior Management*
- *Supervisors & IT Staff*

Does everybody know what role to play in a crisis situation

Does everybody know what the roles are and to whom they belong during a crisis

Student Notes

Extensive Testing and Reviewing

Testing should be progressive and iterative so that confidence is built up steadily. Testing should cover a realistic time period - it is not enough to demonstrate that the service can be restored, evidence is also required that the service can be supported after restoration despite reduced staff numbers and unfamiliar surroundings.

A Contingency Plan is subsidiary to maintenance. The most important roadblocks are the adjustments in the infrastructure and the changes in the determined Service Levels. A migration, to a new midrange platform for example, with a warm external start can lead to the fact that a similar machine is no longer available. The Configuration Management therefore plays an important role in the protection of the standard configurations that also occur in the Contingency Plan.

Testing a Plan - the Contingency Plan should frequently be tested. A lot of things could go wrong during an emergency so a plan needs to be studied. Besides that the test will show what areas in the plan come short and what changes have been missed. Sometimes changes can be tested on recovery locations to see if they work here as well, before they are processed in the IT-infrastructure.

Extensive Testing and Reviewing

- *Initially then every 6 to 12 months and after each disaster*
- *Test it under realistic circumstances, do it rigorous*
- *Move / protect any live services first!*
- *Review and change plan*
- *What changes? New, more, less of:*
 - *Customers / services / SLRs / risks /*
 - *Dependencies / assets / CIs / staff /*
 - *Contracts / SLAs / countermeasures /*
- *ALL change to be via the Change Advisory Board*

Student Notes

Essentials

ITSCM is a critical tool if the business is to continue to operate in spite of the many risks faced. Failure to implement adequate ITSCM measures will impact that ability following an interruption.

ITSCM must be able to respond quickly and efficiently to the changes and be regularly tested to ensure that the different components of the IT infrastructure will work together.

Organizations that practice ITSCM effectively will have assessed the risks (CRAMM) to Business Continuity, identified minimum acceptable levels of business and put in place tested plans (7 steps and based on one of the various options – cold, warm etc.) to ensure that these can be maintained.

Responsibilities for ITSCM should be integrated with corresponding operational responsibilities to maximize synergy and capitalize on existing knowledge, skills and expertise in the operating environment.

The plan or plans should be given wide but controlled access and details about them should be recorded in the CMDB as they are CIs.

Essentials

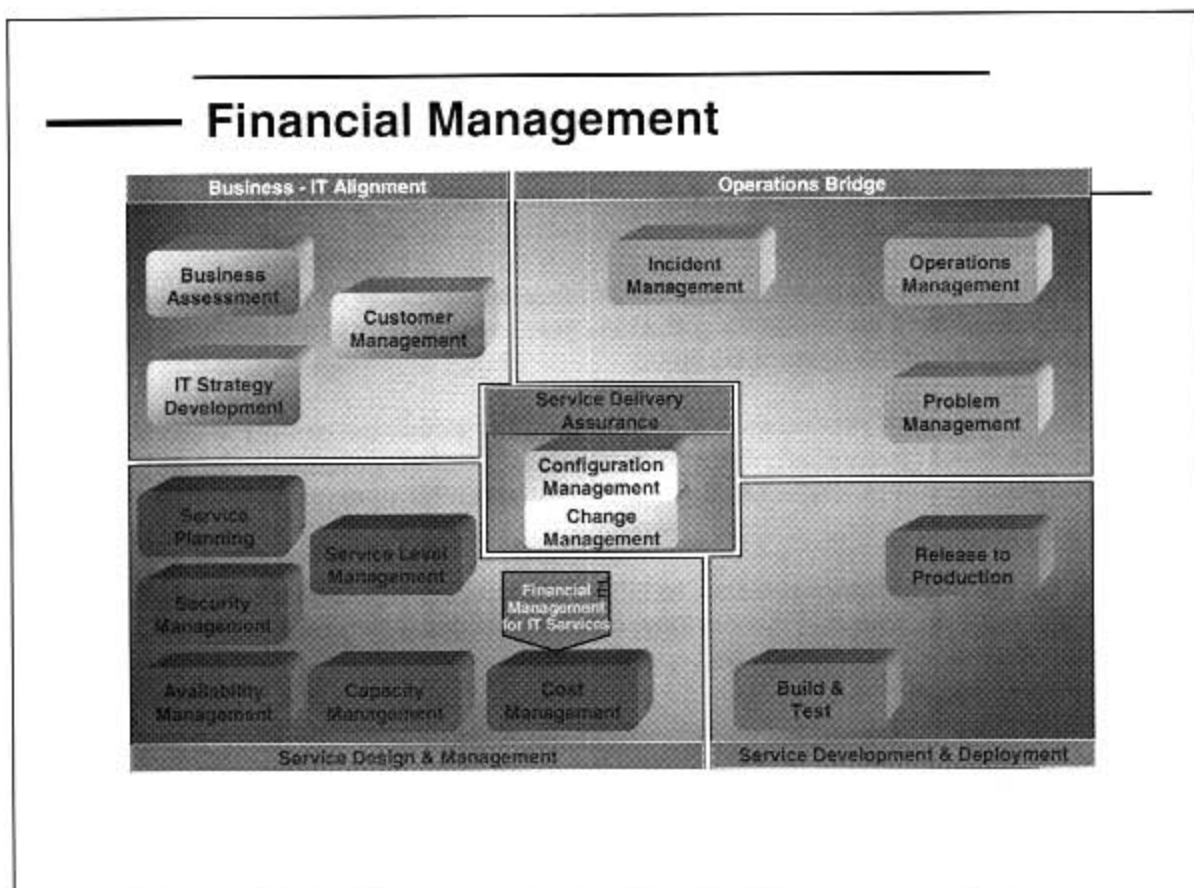
- *Disasters will happen and will affect services!*
- *Assets/Threats/Vulnerabilities/Risks/Countermeasures*
- *Part of service planning & design*
- *The IT Service Continuity Plan*
 - Assists in fast, controlled recovery
 - Must be given wide but controlled access
 - Contents (incl. Admin, Infrastructure, People, Return to normal)
 - Options (incl. Cold, Warm & Hot Standby)
 - Must be tested regularly - without impacting the live service
- *Different Roles*

Student Notes

Module 11 — Financial Management for IT Services (Cost Management)

This module introduces Financial Management for IT Services, the discipline of identifying, calculating and managing the cost of delivering IT services. Financial Management for IT Services influences user behavior through cost awareness or charging and provides budgeting data to management. Cost accounting focuses on the fair allocation of shared costs and charging for IT services.

Financial Management



Student Notes

Financial Management

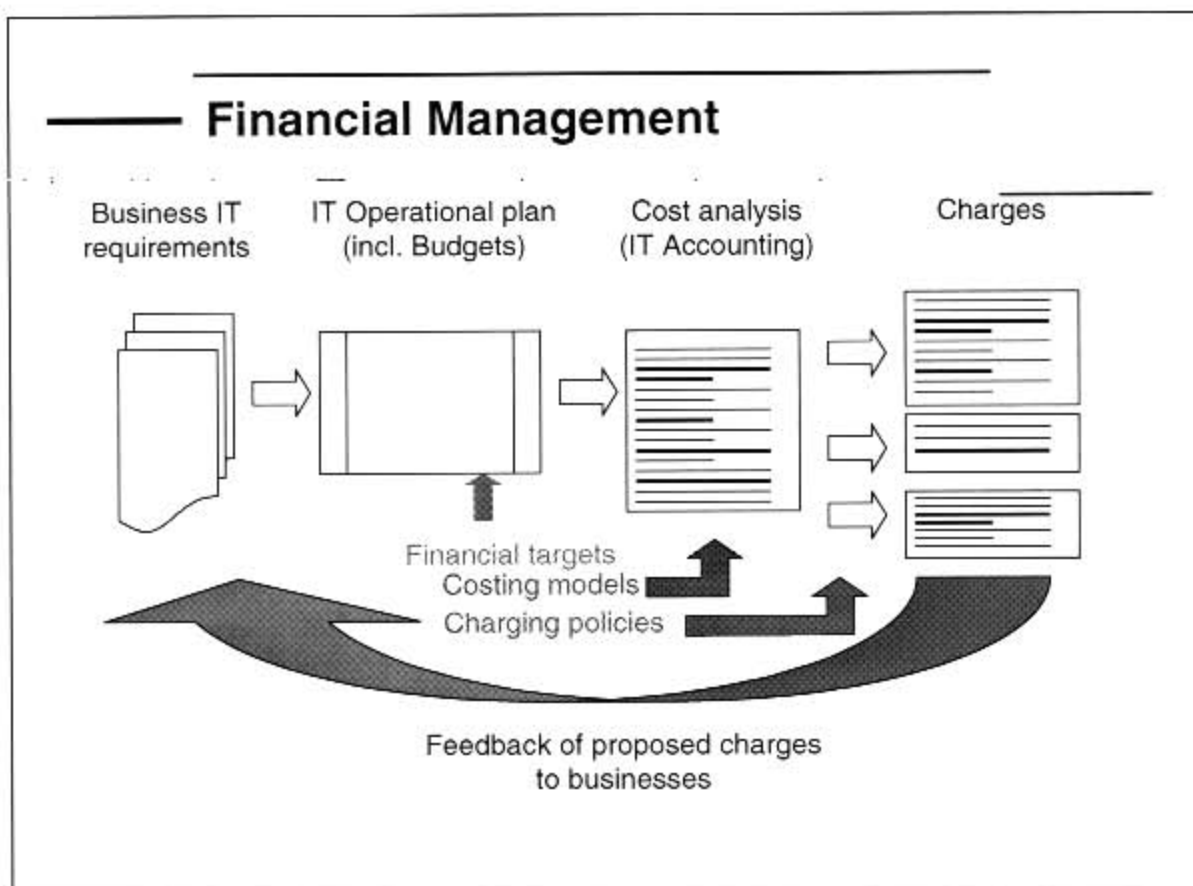
Financial Management is the sound stewardship of the monetary resources of the enterprise. It supports the enterprise in planning and executing its business objectives and requires consistent application throughout the enterprise to achieve maximum efficiency and minimum conflict.

Within an IT organization it is visible in three main processes: Budgeting, IT Accounting & Charging

Budgeting is the process of predicting and controlling the spending of money within the enterprise and consists of a periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets.

IT Accounting is 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, by activity). It usually involves ledgers and should be overseen by someone trained in Accountancy.

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



Student Notes

Budgeting

Budgeting is the process of ensuring that the correct monies are set aside for the provision of IT services and that during the budget period they are not over-spent.

The Budgeting process is a key influence on strategic and tactical plans. It is also the means of delegating control and monitoring performance against predefined targets. It is paramount that budgets are effectively integrated within the enterprise and that managerial responsibility and accountability is matched and communicated in an efficient way.

As all spend affects profitability, it must be recognized that decisions about investment in IT Services and the integrated management IT Accounting function can help provide the competitive edge necessary for survival of an enterprise.

All enterprises have an annual round of negotiations between the business departments and the IT department covering expenditure plans and agreed investment programmes which ultimately sets the budget for IT.

Budgeting enables an organization to:

- Predict the money required to run IT services for a given period.
- Ensure that actual spend can be compared with predicted spend at any point.
- Reduce the risk of overspending.
- Ensure that revenues will be available to cover predicted spend (where Charging is in place).

The benefits of Budgeting should be self-evident, but in summary are:

- Ensuring that the business provides sufficient funds to run the IT Services it requires.
- Ensuring that IT Service Levels can be maintained throughout the year.
- Providing early warning of under- or over-consumption of service (provided that some form of IT Accounting is in place).

Budgeting

- *Ensuring that the correct monies are set aside for the provision of IT services*
- *Key influence on strategic and tactical plans*
- *Budget could have*
 - Limits on capital and 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 enterprise or group of enterprises

Student Notes

IT Accounting

The fundamental benefit of Accounting for IT Services (IT Accounting) is that it provides management information on the costs of providing IT services that support the enterprise's business needs. This information is needed to enable IT and business managers to make decisions that ensure the IT Services section runs in a cost effective manner.

Cost effectiveness is defined here as ensuring that there is a proper balance between the quality of service on the one side and expenditure on the other. Any investment that increases the costs of providing IT services should always result in enhancement to service quality or quantity.

IT Accounting helps the business to:

- Base decisions about the services to be provided on assessments of cost-effectiveness, service by service.
- Make more business-like decisions about IT services and investments in them.
- Provide information to justify IT expenditures.
- Plan and budget with confidence.
- Demonstrate under- or over-consumption of service in financial terms.
- Understand the costs of **not** taking advantage of opportunities for change.

Put simply, there is no prospect of IT service providers maximizing value for money if the costs of providing the services are not accurately known. A key justification for investing in more IT resources is to support new or better business processes. IT Accounting provides the cost basis for cost-benefit analysis.

IT Accounting

- *Base decisions on assessments of cost-effectiveness, service by service*
- *Make more business-like decisions about IT services*
- *Provide information to justify IT expenditures & investments*
- *Plan and budget with confidence*
- *Demonstrate under- or over-consumption of service in financial terms*
- *Understand the costs of **not** taking advantage of opportunities for change*

Student Notes

Different Cost Units

If more detail is required in calculating costs, the chosen major Cost Types of Hardware, Software, Employment, Accommodation and Transfer can be further divided. For instance, Hardware might be divided into *Office, Network, and Central Servers*. The purpose of this is to ensure that every cost identified in the IT department can be placed within a table of costs, by type. This enables analysis to be performed by type e.g. all *Network* costs.

The decision on whether to identify more detailed cost units will often depend upon whether more detail is required to apportion charges. In general, Cost Elements will be the same as budget line items where the purpose of the model is simple recovery of costs.

If a more detailed analysis of costs is required, e.g. for organizations providing shared services, then more detailed Cost Elements will have to be identified. Typical Cost Elements within each major Cost Type are:

<i>Major type</i>	<i>Cost Elements</i>
Hardware	Central processing units, disk storage, peripherals, wide area network, PCs, portables, local servers
Software	Operating systems & options, scheduling tools, applications, databases, personal productivity tools, monitoring tools, analysis packages
People	Payroll costs, Benefit Cars, Re-location costs, Expenses
Accommodation	Offices, Storage, Secure areas
External Service	Security services. Disaster Recovery services, outsourcing services.
Transfer	Consultancy, Security services, Disaster Recovery services, outsourcing services, utilities,

For organizations providing services based upon central mainframes, the hardware costs may be the largest proportion but it is more common to see a rough balance amongst hardware, software and employment. Increasingly, the proportion of costs attributed to networking devices and network services is becoming more significant and may be identified as a separate Cost Type.

Organizations that purchase software products, rather than developing them, will find a higher proportion for costs categorized as Software. Organizations which use outsourcing services (such as offshore development or computing services) will see Transfer costs as the largest proportion of costs.

Different Cost Units

- *Hardware Cost Unit*
- *Software Cost Unit*
- *People Cost Unit*
- *Accommodation Cost Unit*
- *External Service Cost Unit*
- *Transfer Cost Unit*

Student Notes

Categorization of Cost Units

Fixed Costs are those that cannot be influenced, they will be the same even when services will stop. Examples are: Rent; salaries; insurance; s/w license fees; utility standing charges; fixed price contracts; mainframes; h/w maintenance contracts; depreciation.

Variable Costs follow changes in business activity. E.g. overtime; consumables; telecomm charges; fees for contractors; expenses; utility consumption charges; short term lease/hire. Since variable costs follow changes in business activity, there has been a trend in recent years towards converting fixed costs into variable costs.

Direct Costs are those that can be allocated to one specific department or service like some application software; dedicated hardware; identifiable resource; dedicated support teams.

Indirect Costs are those that cannot be allocated to one specific department or service but that has to be divided among more departments and/or services. Management; ITQ; systems software; non-identifiable resource; service desk; accommodation; networks; depreciation & maintenance; fees for multi-service computers. Correctly identifying whether a cost is a direct or indirect cost is important when defending budgets. It is easy to demonstrate that a cut to direct costs will directly affect the quality of service delivered. Indirect costs lend themselves to being cut on a set percentage of the existing budget and it is hard to demonstrate how such a cut will affect services. A recent survey detail in Computer Finance suggests that many business managers want some IT services, such as email and the desktop environment, to be treated as business overheads, with only value-added services dealt with as direct costs.

Capital Costs are typically those applying to the physical (substantial) assets of the organization. Traditionally this was the accommodation and machinery necessary to produce the enterprise's product. Capital Costs are the purchase or major enhancement of fixed assets, for example computer equipment (building and plant and are often also referred to as 'one-off' costs. It is important to remember that it is not usually the actual cost of items purchased during the year that is included in the calculation of the cost of the services but the annualized depreciation for the year.

Operational Costs are those resulting from the day-to-day running of the IT Services section, e.g. staff costs, hardware maintenance and electricity, and relate to repeating payments whose effects can be measured within a short timeframe, usually the less than the 12-month financial year.

Categorization of Cost Units

- **Fixed**
Costs fixed for a reasonable period of time
- **Variable**
Costs that will vary with usage or time
- **Direct**
Costs that can be directly allocated
- **Indirect**
Costs apportioned across a number of Customers
- **Capital**
Assets that are depreciated over time
- **Operational**
Day to day running costs

Student Notes

Charging

The fundamental benefit to the enterprise of charging customers, is that it provides a sound business method of balancing the shape and quantity of IT services with the needs and resources of the customers. Customers are charged for the services they receive and because they are paying, they have a right to influence decisions on its provision. If they do not think the services represent good value for money, they may stop using them or make formal complaints but professional IT departments will invest time in discussing the balance of charges and service levels with their customers.

Services can be improved by spending more, if there is a business justification for it. The introduction of formal Charging, often provides more evidence to support this and hence more enterprises will choose to invest in IT. Conversely, if customers believe that they can save themselves money (directly or indirectly, by reducing overall enterprise expenditure) by changing the way in which they use the IT services, they will be able to discuss this more openly with the IT department.

Charging enables the IT Services management to:

- Make formal evaluations of IT services and plan for investment based on cost recovery and business benefits.
- Recover IT costs in a fair manner.
- Influence customer behavior.

Charging

- *Recover from customers the full costs of the IT services provided in a fair manner*
- *Ensure that customers are aware of the costs they impose on IT and influence customer behavior*
- *Make formal evaluations of IT services and plan for investment based on cost recovery and business benefits*

Note: Charging is optional but you MUST know and understand your costs

Student Notes

Charging and Pricing Options

Pricing is most of the time a very complex exercise. The following has to be considered:

- What is the purpose of pricing, why are we doing it.
- What are the costs of the end-to-end service (and therefore the components).
- What are the prices in the market (in order to benchmark).
- Analyze the demand (for that service) in the market.
- Analyze your customers and those of the competitors.

There are a couple of options if you talk about pricing. They are:

- *Recover of costs*: recover costs fully but nothing more.
- *Cost price plus*: recover the cost but also make a profit.
- *Going rate*: price is comparable with other internal departments' costs within the organization or with similar external organizations.
- *Market prices*: prices that are set conform the current market prices.
- *Fixed price*: a set price is agreed for a set period with the Customer based on anticipated usage.

Most organizations do have an implementation policy. This policy exists nine out of ten times of the following steps:

- *No charging* (IT treated as a support center): most of the times used as communication and information where the customers are informed about the cost of the services that IT is delivering. The customer does not pay for the services and is not going to.
- *Notional charging* (IT treated as a cost center): This is used as a first step to charging, the invoice is made and delivered to the customer but they don't have to pay (yet) This gives the organization the opportunity to get more experience and to fine tune the invoices. And it gives the organization the opportunity to get used to charging. This is sometimes called "soft charging" in which no money changes hands.
- *Actual (or real) charging* (IT treated as a service center): now the invoice has to be paid. The blue dollars becomes green dollars

Charging for Support, Cost and Service centers is based on the cost of service provision. Profit centers focus on the value of the IT service to the customer.

Note: Senior Management and Business Managers will set the charging policy.

Charging and Pricing Options

Charging

- *No charging*
- *Notional Charging*
- *Actual/Real Charging*

Pricing

- *Recover of costs*
- *Cost price plus*
- *Going Rate*
- *Market prices*
- *Fixed Price*

Student Notes

Essentials

Some organizations have a dedicated IT Finance Manager. Others may share the tasks amongst the senior IT managers, especially those responsible for other Service Management processes (SLM and Capacity Management for example) and the IT Director.

The processes must have an “owner”, that is someone responsible for developing and reviewing them. Some of the processes may be “owned” by the Finance department, however if this responsibility is split, care should be taken to avoid giving them to people with primarily administrative roles as they are unlikely to have the time or seniority required to manage the tasks.

The main role of IT Financial Management is to work at an appropriate level with representative of the organization management and the Finance department to develop the policies for Budgeting, IT Accounting and Charging. To implement and maintain the IT Financial Management process, covering these three areas.

Changes to Budgeting and IT Accounting or the introduction of Charging for IT Services are strategic business decisions and therefore lay with very senior management not the IT Finance Manager. This is because such decisions may impact service levels, perceptions of value and usage of services. Business leaders throughout the organization should be fully aware of the changes likely from the implementation of any of the above.

Establishing IT Financial Management gives management better information about the cost of IT Services. As a result of that the organization can create a better “value for money”

On top of this, it helps the IT Services Manager to:

- Base decisions about the services to be provided on assessments of cost-effectiveness, service by service.
- Make more business-like decisions about IT services and their related investments.
- Provide information to justify IT expenditures.
- Plan and budget with confidence.
- Understand the costs of failing to take advantage of strategic opportunities to justify the required expenditure (thereby providing value-added productivity).
- Help the users understand the costs associated with the services that they utilize.

The biggest benefit of establishing Charging is the creation of a business-like relationship. The customer that is charged can demand a better service and the IT organization can justify why it spend the money. Beside this we can create investment plans based on ROI.

Essentials

- *Budgeting & IT Accounting*
 - Knowing & understanding costs
 - Needed to manage changes
 - Input cost units (HSPAET)
 - Input cost types (F/V, D/I, C/O)
 - Need for good estimates of business workloads
- *Charging (but not policy)*
 - Determine charges in SLAs
 - Influence customer behavior
 - Charging does not affect costs
- *General*
 - Sound stewardship
 - Minimize risk in decision making
 - Estimating, planning, budgeting
 - Targets & measures

Student Notes

Module 11
Financial Management for IT Services (Cost Management)

Module 12 — Service Level Management

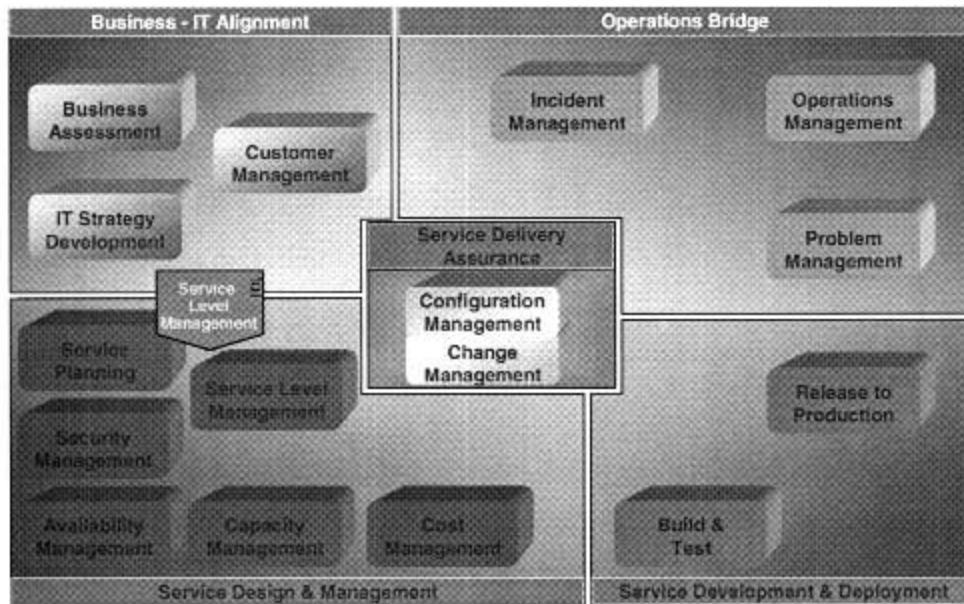
This module introduces Service Level Management (SLM), the discipline of managing the quality and quantity of service delivered by the IT Services organization to the customers. The essence of Service Level Management is the Service Level Agreement, a virtual "contract" between the IT organization and customers that articulates in detail which services are to be delivered along with quality and quantity characteristics, such as performance and availability, for those services.

When masterfully articulated, Service Level Agreements (SLAs) provide the IT organization a definitive yardstick against which most of the organization's activities can be valued. The details of a SLA facilitate measurement of actual system dynamics, giving the IT organization concrete numbers for evaluation and subsequent action.

This discipline is perhaps one of the more complex in terms of its organizational and cultural implications. It is as powerful as it is complex, formalizing the relationship between the customer organization and IT organization. The SLA can serve as a catalyst in establishing other valuable ITSM disciplines in terms of their contribution to fulfilling the SLA.

Service Level Management

Service Level Management



Student Notes

Service Level Management

Service Level Management

Balance between:

Demand for
IT services



Supply of
IT services

By:

- Knowing the requirements of the business
- Knowing the capabilities of IT

Student Notes

Service Level Management – Goals

Service level management (SLM) is essential if IT departments are going to demonstrate a commitment to customer-oriented service provision to the business.

Since IT only exists to provide services, and all activity within IT has an impact on service provision, the SLM team should be central to the management of IT.

The mission for Service Level Management is to maintain and gradually improve IT Service quality, through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and instigation of actions to eradicate poor service – in line with business or cost justification. Through these methods, a better relationship between IT and its customers should be developed.

Service Level Management — Goals

- *Business-like relationship between customer and supplier*
- *Improved specification and understanding of service requirements*
- *Greater flexibility and responsiveness in service provision*
- *Balance customer demands and cost of services provision*
- *Measurable service levels*
- *Quality improvement (continuous review)*

Student Notes

Service Level Management - Responsibilities

Service Catalogue - Details the full range of services that the IT department can deliver and different levels of service that are available to customers.

Service Level Agreement (SLA's)- negotiated to achieve an agreed compromise between the customer's SLR and the ability of the IT department to deliver the required service with the resources at their disposal.

Service Level Requirements are documents that provide a detailed view of the customers needs and are used for setting up, adjusting and renewing services. This document can serve as a blue print for the designing of a service with matching SLA and can be signed as an order of design, if desired.

Operational Level Agreement (OLA) – and *Underpinning Contract*: are documents that support the SLA and are agreed with internal (OLA) and external (UC) suppliers to describe the delivery of one or more components of the end-to-end service. (See also next pages)

Service Specs sheet – this is a detailed document that is the bridge between that what is agreed in the SLA and that what technically is needed internally to deliver the service. It also gives the input for both the SLA, OLA and Contracts (see also next pages)

Service Quality Plan - very important document, it contains all management information that is necessary for steering the IT-organization. In the Service Quality Plan the process parameters of the Service Management and the operational management are registered. For every process target values are defined in the form of Performance Indications. This way for Incident Management solution times with impact levels are set, for Change Management the continuation times and costs of stand adjustments like a move are set and for all processes is decided on which reports are necessary at what times. The Performance Indications are led from the Service Level Requirements and documented in the Specs sheets. When external suppliers are involved in delivering the services, like with Outsourcing of a Service Desk or the maintenance of PC's, then the Performance Indications are also registered in the Underpinning Contracts.

Monitoring, Review & Report – see on one of the next pages.

In the *Service Improvement Plan (SIP)*, which is formally executed in the form of a project, actions, phases and release data that is meant to improve an IT service are documented.

Customer Relationship Management – ongoing relation with the customer to maintain the services and the SLA's



Student Notes

Service Level Management Process

The process is a full loop quality cycle. Once SLA's have been defined the loop is started.

Establish Function

If Service Level Management is not yet in place than the first step is to plan the process itself. Activities like designing procedures, creating service catalogue, creating draft SLA's and awareness campaign are amongst the things that have to be planned for. The following things have to be planned:

- Initial Planning of Activities.
- Plan Monitoring Capabilities.
- Establish Initial Perception of the Services.
- Set-up/Checking of Underpinning Contracts and Operational Level Agreements.

Implementing SLA's

In the implementation phase the following has to be established:

- Produce a Service Catalogue.
- Expectation Management.
- Plan the SLA Structure.
- Establish Service Level Requirements and Draft SLA.
- Wording of SLAs.
- Seek Agreement.
- Establish Monitoring Capabilities.
- Review Underpinning Contracts and Operational Level Agreements.
- Define Reporting and Review Processes.
- Publicize the existence of SLAs.

Managing the ongoing process

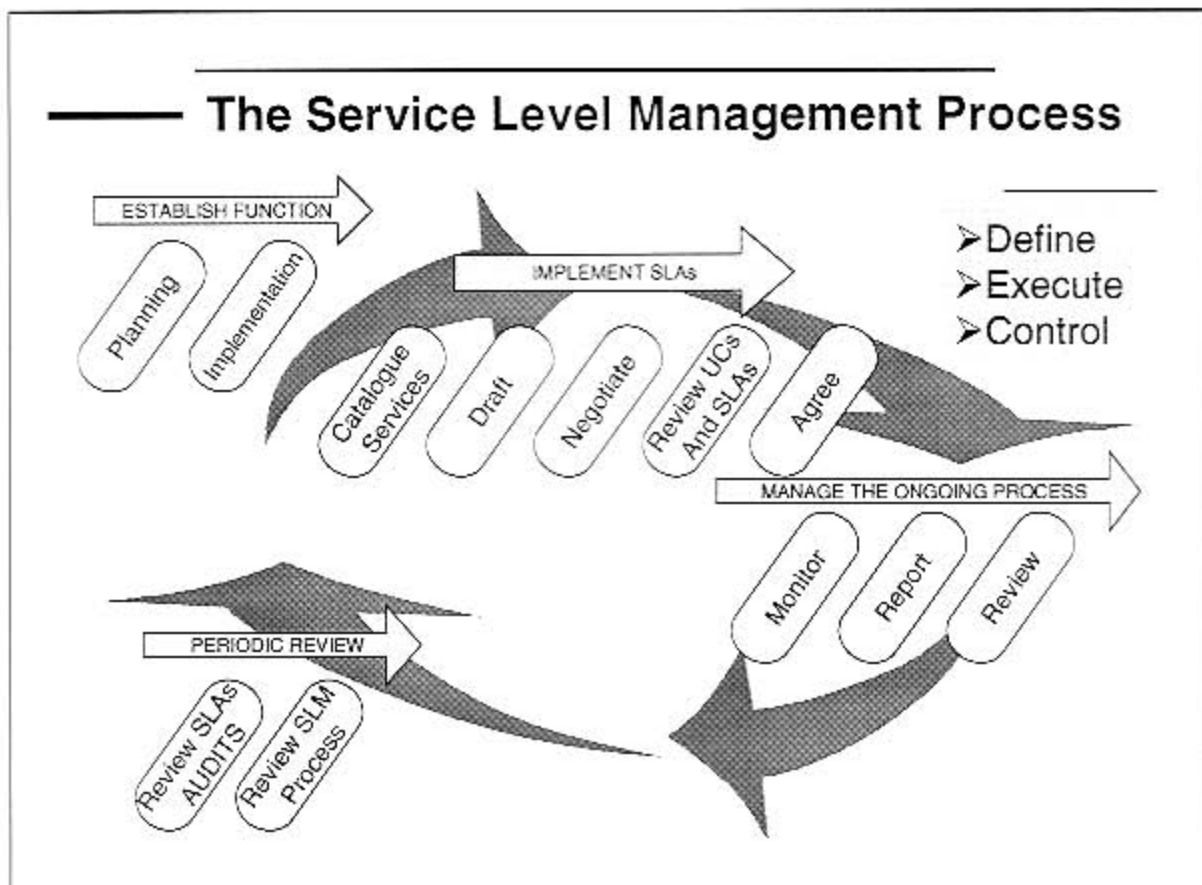
In this phase the following has to be conducted structurally:

- Monitoring and Reporting.
- Ad-hoc Service Review Meetings.

Periodic Review

In this phase the following has to be conducted structurally:

- Periodic service review meetings.
- Creation of service improvement programmes (SIP).
- Maintenance of SLAs, contracts and OLAs.



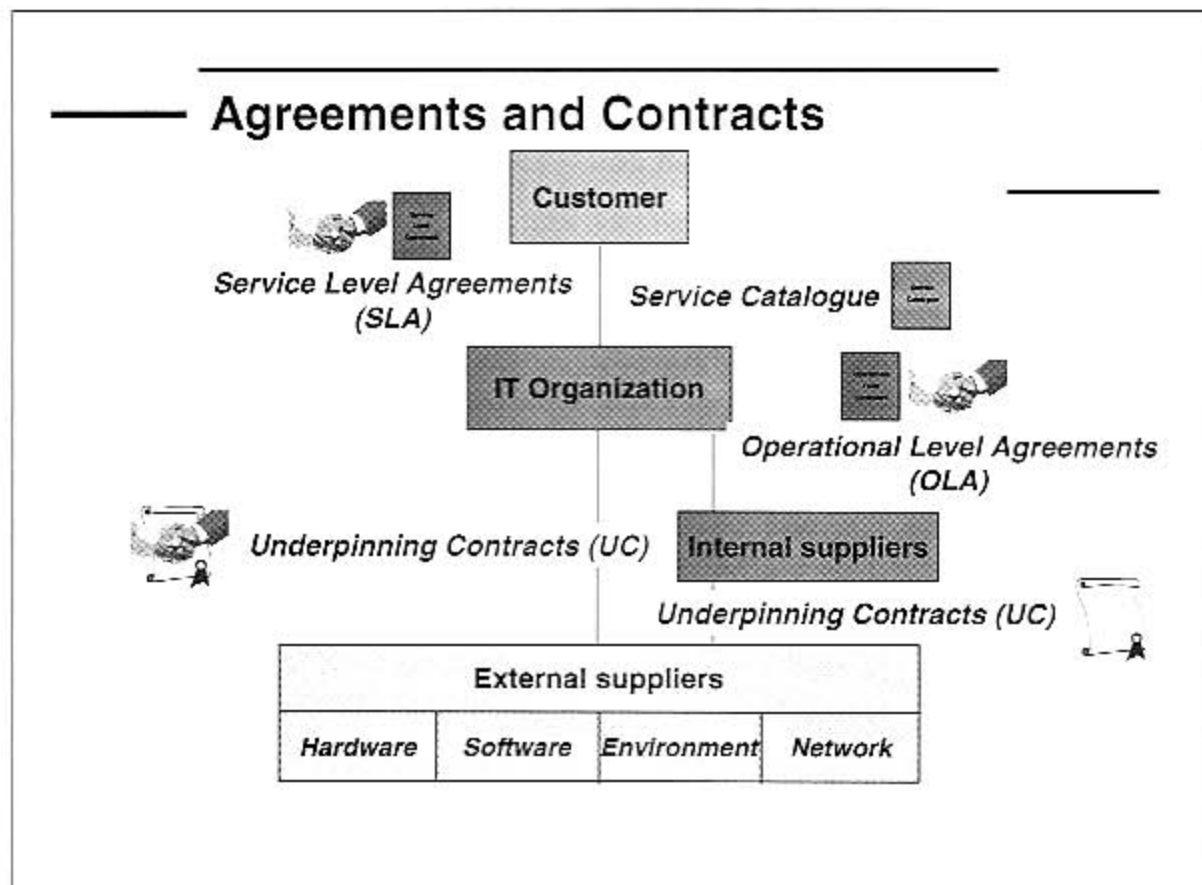
Student Notes

Agreements and Contracts

Supporting contracts and OLAs must be developed that will enable targets in the SLA to be achieved. Internal suppliers will typically be providing environmental and accommodation services and various forms of technical support. If necessary SLAs may need to be modified to align them with existing contracts but it is preferable to renegotiate the contract. Clear benefits arise from supplier contract management being closely aligned organizationally with the management of SLAs.

An Operational Level Agreement is a conformity with an (other) internal IT-department in which agreements on the maintenance of certain components of a service are determined, for example an SPA over the availability of the network or the availability of the printservers. An SPA serves as support for the IT-organization that delivers the service.

An Underpinning Contract is a contract with an external supplier in which agreements on the maintenance of certain components of a service are determined. This is comparable to an external performance of an SPA with the goal to , for example, get to an agreement with an external supplier on the extermination of technical problems in workstations or on the availability of a permanent connection.



Student Notes

Service Quality Plan

The Service Quality Plan is the internal description of everything that has to be done in order to deliver the agreed qualities to the customers.

Service Quality Plan

- *Internal service description, responsibility and internal delivery times to meet the agreed service level*
- *Targeted at IT staff*
- *Describes what we need to do to deliver the desired quality*
- *Describes the actions to take when we do not deliver the correct quality*

Student Notes

Service Improvement Programme

The Service Level Management process often generates a good starting point for a Service Improvement Programme (SIP) – and the service review process may drive this.

Where an underlying difficulty has been identified which is adversely impacting upon service quality, the Service Level Manager must, in conjunction with Problem Management and Availability Management, instigate a SIP to identify and implement whatever actions are necessary to overcome the difficulties and restore service quality. SIP initiatives may also focus on such issues as user training, system testing and documentation. In these cases the relevant people need to be involved and adequate feedback given to make improvements for the future.

At any point in time, a number of separate initiatives which form part of the SIP may be running in parallel to address difficulties with a number of services.

Service Improvement Programme

- *Objective*
 - Controlled improvement
- *Drawn whenever there is a need*
 - Deviation from agreed levels
 - Strategic choice
 - Continuous Improvement
- *More than one simultaneously*

Student Notes

Elements of a Service Level Agreement

Service Level Agreements are conformities in which agreements between the IT-organization and the customer are determined on the services that need to be delivered. The Service Level Agreement describes the service in non-technical terms and tunes in on the language of the customer. The Service Level Agreement, during operational times, serves as a norm for the measuring and steering of an IT-service.

Scope and tone of a SLA will change as the relationship develops. Clauses should reflect the fact that there are obligations on both customer and supplier. The measures included in the SLA should be meaningful. Whether measures included in the SLA represent minimum acceptable, worst case, expected or target service levels should be clearly stated. It can be as important to specify what services are not provided as it is to specify what services are provided - for example, the customer needs to know if the service has only limited security built in to it.

Examples of Service Support Elements

Service Hours:

24x7, 5x8, attended, unattended, etc.

Support

E.g. support hours, specials, extensions, response time, repair time, etc.

Escalation

Who, when, how, what for, etc.

Change

Category, average turnaround, times, standard requests, etc.

Examples of Service Delivery Elements

Availability

E.g. 99%, target within service hours, etc.

Reliability

E.g. number of times service breaks down over a given period, MTBF, MTBSI, etc.

Continuity & Security

What, how, roles, responsibilities, procedures, etc.

Charging

Formula, pricing, method, etc.

Batch Turnaround Times

Input and output: when, where, how, etc.

Transaction Response Times

E.g. 1Mb doc open <=15 secs, 95% <= 2 sec, etc.

Throughput

E.g. volume, number of users, network data, pages, etc.

Elements of an Service Level Agreement

Service Level Agreement

General

Introduction
• Parties
• Signatures
• Service Description
Reporting & reviewing
• Content
• Frequency
Incentives & Penalties

Support

Service Hours
Support
Change Procedures
Escalation

Delivery

Availability
Reliability
Throughput
Transaction response times
Batch turnaround times
Contingency & Security
Charging

Student Notes

Management Reports

In order to protect the Service Level Management, the Service Level measurements have to be defined correctly in advance and have to comply with the externally set target values. The Service Levels have to be measured from the Customer's perspective. This protection does not only involve technical matters, but also procedural matters; as long as the customer has not been informed that the service is back in order he will assume that it is still not working. The internal (technical) target values are usually protected by Availability Management and Capacity Management and for some areas of attention by the processes from the Service Support Set (specifically Incident Management). The measuring of internal values however is not enough because with that, a link to the experience of the user is still not made. Also data like reaction times, escalation times and support should be made measurable. In order to receive a complete view, the management information of both the systems and the Service Management needs to be combined.

Management reports should be produced regularly. In the management reports a comparison between the Service Level Achievements and the actual measured values is made. Examples here of are report over:

- The measured availability or unavailability over a certain amount of time (Downtime).
- The average response times during peak burdens.
- The transaction speeds during peak times.
- The number of functional errors in the IT-service.
- Frequency and duration of degradation, when services perform below their determined level.
- The average number of users during peak burden times.
- The number of success or non-successful attempts to avoid the security.

Management reports besides that can contain measuring values concerning the up-to-date supporting levels and the trend developments, such as:

- The number of finished SLA's.
- The number of times that an SLA was not met up with.
- The costs of the protection and measuring the SLA's.
- The satisfaction of the customer - by performing surveys and registering complaints.
- Statistics on incidents, problems and adjustments.

Management Reports

- *Measured from the customers perspective*
- *Data like reaction times, escalation times and support should be made measurable*
- *Reports should be produced regularly*
- *Reports contains measuring values concerning the up-to-date supporting levels and the trend developments*

Measures should always be SMART

Student Notes

Essentials

Purpose

Service Level Management ensure good communication with the client. Together, they project an important part of the image of the IT organisation.

The Account Manager / Service Level Manager

The Account Manager ensures good communications with the client and the IT management. The Service Level Manager ensures proper consultation with the clients on agreements concluded and any possible adjustments of the services requested.

The Process

The client expects and wishes a certain service, or new services or adjustments to the services. The client's **requests** are analysed and subsequently the service planning processes (see below) **translate** the external wishes into internal requirements. The service's external or client oriented characteristics and requirements are recorded in the **service catalogue**. In addition, the **service quality plan** describes the internal or more technical characteristics and demands applicable to the service. Subsequently, in the course of a process of consultation and **negotiation** clear agreements are reached. This results in an agreement (service level agreement: SLA). The SLAs are administered and catalogued. Change management is always involved in the requests for the development and implementation of new services.

Once the SLA is in place, the service is continuously monitored and reviewed to ensure that the services to the client are proceeding according to the agreement.

This process ensures good communication with the client because there is a central point of contact who takes into account the various interests. This process also monitors the services from the point of view of the service agreements.

Essentials

- *We need to understand what we mean by "Service Management"*
- *Goals*
 - Improve service quality (customer dependence)
 - Measurable service levels
 - Balance between customer demand and IT capabilities
- *Responsibilities*
 - Manage customer relationships
 - Create / maintain Service Catalogue
 - Determine SLRs; Negotiate, prepare & monitor Service Charter, SLAs & OLAs and Service Improvement/Quality plans
- *Minimum requirements for an agreement*
 - Period, service description, throughput, availability, response times, signature

Student Notes

Essentials (2)

Essentials (2)

- *General*
 - SLAs must take account of underpinning contracts where these already exist
 - SLAs can be organized by service or by customer
 - The new generation of service management tools allow SLAs to overlap, usually defaulting to the higher level of service
 - SLAs must be monitored regularly and reviewed regularly
 - Monitor to see if service is being delivered to specification
 - Review to see if service specification is still appropriate

Note: the quality of IT underpins the success of business operations!

Student Notes

Good luck with the Exam



&



=



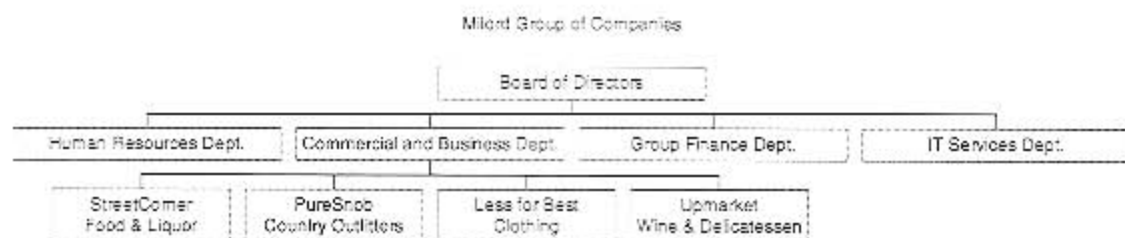
&



Student Notes

The Milord Group

The Milord Group is a holding company that consists of a number of retail chains. The Group has grown partly on its own strengths and partly by taking over other companies. The policy of the Group's board of directors is to diversify activities as much as possible between food and non-food operations, and between high-end and low-end markets. Therefore, within the Group there are discount supermarket chains like "Street Corner" as well as haute couture shops such as "Pure Snob". Because these chains are so different, there is no overall company culture. For example, the discount supermarkets keep a low profile: they maintain low priced facilities as storefronts, their company vehicles are vans, etc. Other, more prestigious, chains want high profile buildings, shiny new company cars, etc. Because they are all part of the same group of companies and therefore have to share their overhead departments, many conflicts occur. Ultimately, the board of directors must resolve all these conflicts.



The Retail Chains

The individual retail chains are self supporting and accountable for their own profit and loss (P&L) accounts. They have their own purchasing, logistics and marketing departments. The overhead departments of Milord support the different needs of each of the chains and are also responsible for developing and enforcing Milord Group standards and procedures. They charge the chains for their services – for instance for the rent of offices and shops, and for the leases of company cars. The chains are not permitted to purchase such services from elsewhere.

Information Technology

The IT department has to manage a great variety of systems: mainframes with terminals, state-of-the-art desktops with Internet access, client/server applications, etc. The IT management policy is to reduce the diversity of systems and technology. In order to do so, IT management has defined a number of company standards, e.g. for the desktop environment. However, because of their commercial independence, the chains are not convinced they have to adhere to these standards.

New projects

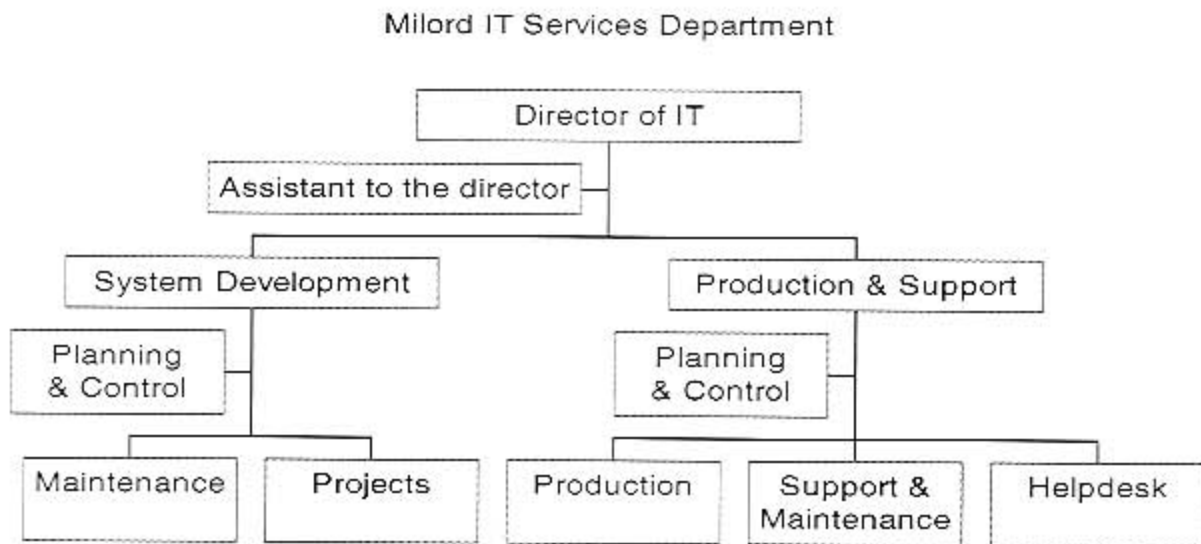
After much discussion, the board of directors and the management of the retail chains have agreed the following priorities for new IT projects:

- Implementing a new financial and logistics retail application, called FISCO
- Improving the state-of-the-art within the Milord Group and the retail chains, to enhance the Group's operating performance, via data mining/warehousing projects and the use of Internet and Intranet facilities.
- Upgrading and standardizing the office desktop infrastructure with new standard pcs and office application suites.
- Improving the efficiency and effectiveness of the IT Services organization itself.

The IT Services department

The IT Services department is located centrally and consists of two branches: systems development and production & support.

The organization chart is shown below:



What's going on?

The Director of IT is not a happy bunny. His major concerns are:

- The stress of keeping the important business support applications up and running and of improving the performance of these systems.
- The FISCO project, which has an enormous impact on the IT organization.
- The improvement and standardization of the IT infrastructure.
- The customer and service focus of the IT organization. This is very important, because one of the chains has threatened to shop outside the company for IT services if the quality of the internal IT services doesn't improve very soon.

Exercises

Exercise No. 1: Service Level Management

After a seemingly endless debate and development period, the new state-of-the-art E-mail application called SpeedMail is scheduled to go live next month. SpeedMail offers its users not only the ability to send messages and exchange documents within the Milord Group, but also connects them with the Internet. The IT Services department is very proud of the successful implementation of this application.

Instructions for the customer representatives:

You represent one group of potential users of the SpeedMail service. You are asked to specify the requirements - from an end user perspective - for the SpeedMail service. Your focus should not be the functionality of the application but the quality of the service in the widest sense.

Question:

Specify - from an end user perspective - the requirements for the new SpeedMail service. What are the issues you would like to have recorded in an agreement between the user department and the IT Services department? (30 min)

Instructions for the IT representatives:

You are very proud of making this new service available to so many users at the same time. You want to make sure that the users are as satisfied as possible with the service, so you want to support them in the best way you can. However, you don't want to make promises you can't keep.

Question:

Specify - from an IT perspective - the support and service (in the broadest sense of the word) you are going to offer your customers. (30 min)

Negotiation:

Start negotiations about what should be in a service agreement between the customer departments and the IT Services organization.

Exercise No. 2: Service Desk, Incident Management and Problem Management

Introduction:

The Director of IT is aware that he must organize things differently if the IT Services department is to stay in business. The main reason for this is the growing pressure from the chains to improve the quality of the IT services. The Director hired an external consultant who advised him to implement a couple of "service processes". As a start, an IT Service Desk was founded as a central point for all questions, complaints and requests for all IT users across the entire Milford Group.

As you can see from the organization chart, the Service Desk is part of Production & Support.

The plan for a central IT Service Desk created a lot of resistance, from within the IT Services department itself as well as from customers.

Question:

Write down possible objections for creating an IT Service Desk, three from customers, three from the IT Services department. Think about the arguments the Director of IT might use to counter these objections.

Scenario:

Initially, the IT Service Desk used a very simple registration to record all questions and complaints. The Service Desk staff has complained about the simplicity and lack of performance of this tool.

Question:

Think about the requirements you would have as member of the Service Desk team. What essential and optional functions should be available in a new registration tool? What would you like to register about the calls that are made to the Service Desk?

Which levels of escalation should be implemented? Please make suggestions, when should who be involved?

Scenario:

Two months have passed since the Service Desk went live. After the usual start-up problems (such as customers still phoning other IT support staff directly), everything seems to be working well. However, the Group managers are still not convinced of the usefulness of the Service Desk; they have asked the Director of IT to justify the need for three extra IT Service Desk staff members. They have also requested a report on the performance of the "new" Service Desk.

Question:

The Director of IT asks you as an external consultant for ideas about this report. What data and key performance indicators would you advise including in this report and why?

Scenario:

It is now approximately 6 months since the Service Desk started. Reports show that after a rise in the number of recorded incidents at the start, the number has remained constant for the last three months. The same goes for the average time needed to restore services and close incidents.

Neither the customers nor the Director of IT are satisfied with the overall performance of the Service Desk.

Question:

As an external consultant, what advice would you give the Director to improve the performance of the Service Desk?

Problem management

Introduction:

Part of the advice that was given to the Director of IT was to implement the Problem Management process. The Director of IT finds it hard to understand the difference between an incident and a problem. He's confused and asks: "If I don't understand, how can I explain it to others?"

Questions:

Think of definitions that can be used to explain the difference between problems and incidents, and between the Incident Management process and the Problem Management process.

Make this all clear with a couple of examples related to the Milord Group case.

You are appointed as the Problem Manager in the Milord IT Service department. What requirements should you impose for the way incidents are registered?

Exercise No. 3: Change and Configuration Management

Introduction:

The business managers are getting worried about their IT department. Rumor has it that the IT department cannot cope with all the changes needed for Year2000. The Director of IT has hired a Change Manager and a Configuration Manager to help organize and control all the changes. A start was made with the creation of a CMDB and a weekly meeting of a Change Advisory Board.

The Change Advisory Board is not a success. Only the BIG changes are addressed. Other changes are not included in the Change Manager's system. The staff thinks it is a waste of time to attend the meetings.

Question:

Write down possible objections for creating a Change Advisory Board, three from customers, three from the IT Services department staff. Think about the arguments the Change Manager might use to counter these objections.

Scenario:

Initially, the Change Manager used a very simple registration mechanism to record all changes. The Configuration Manager tells the Change Manager in a meeting that he has the information and the relations of all the Configuration Items within the organization. The Configuration Manager asks if the Change Manager wants to use this information.

Question:

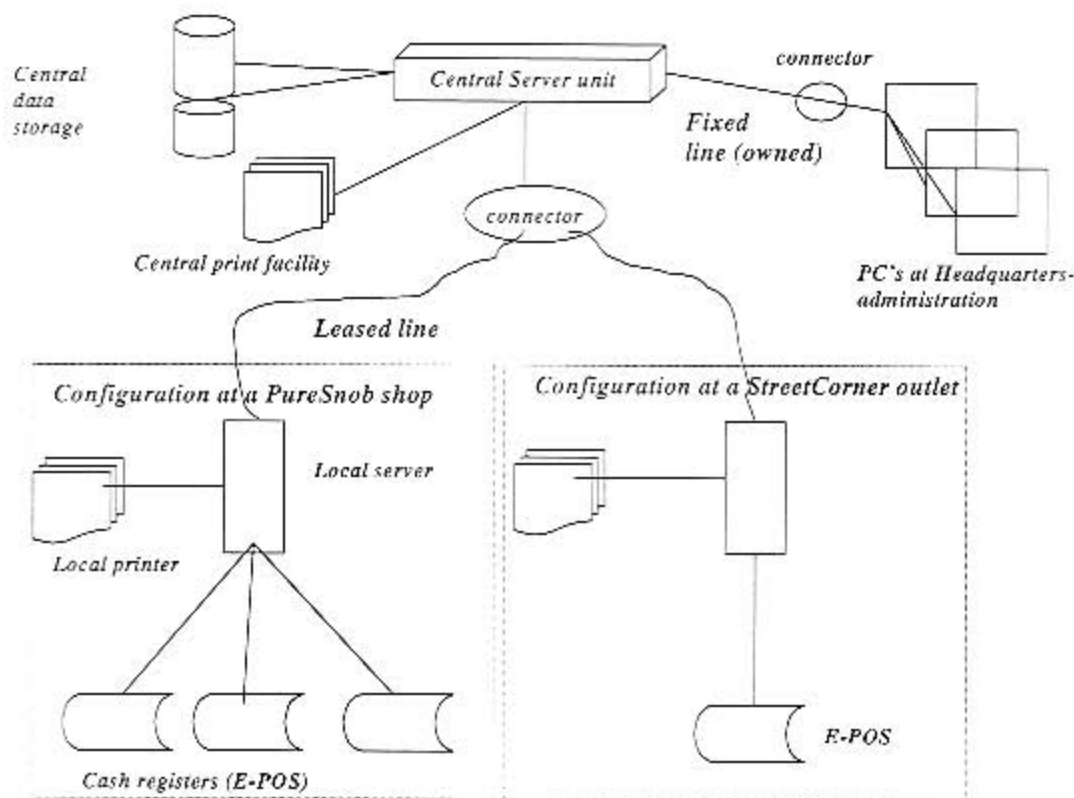
Think about the requirements you would have as Change Manager with regard to Configuration Management. What essential and optional information should be available in a new registration tool?

Exercise No. 4: Availability, IT Continuity, Capacity & Financial Management

Introduction:

The Milord Group finally implemented the FISCO application. This is a fully integrated Enterprise Resource Planning (ERP) system that is used to control stocks, register turnover (revenue), do financial planning, etc.

The operational success of the Milord Group chains is highly dependent of the availability of this system, which is configured as shown below:



You are responsible for the overall availability and performance of this important system.

Questions:

What is the information you would collect about the use and performance of this system? Who would you ask to give you that information? How would you use that information?

Consider the configuration as shown above:

What occurrences might threaten the availability of the service?

What are the weak spots in the configuration?

What options might you have to reduce the vulnerability of the service to failure?

Case Study
The Milord Group

Scenario:

After a long, in-depth study of this configuration, its threats and vulnerabilities, you produced a report addressing the possible countermeasures. The alternatives you presented in the report were:

Extra hardware to reduce the single points of failure, as analyzed.

Extra E-POS hardware in stores with only one cash register.

A Contingency Plan and contract with an external provider: should an emergency arise, they will run the services on another system at an external location.

You presented this plan to the Business Continuity Steering Committee, whose members are the Director of IT and the directors of the individual retail chains, together with the heads of the other central departments. Some of the committee members are enthusiastic about the plan, like the director of the PureSnob chain, who says that it is vital. The directors of the StreetCorner and Less for Best chains, on the other hand, are very concerned about the cost of implementing this Group-wide plan.

Question:

Think about arguments to convince those skeptics that these countermeasures are necessary and worth investing in.

If the director of StreetCorner doesn't want to contribute towards these investments, what kind of a charging system would you advise for this organization?

The director of StreetCorner tells you he knows he's exposed to risks when he doesn't invest in some sort of countermeasures for unavailability but says he cannot afford the options you have presented. He asks you to think of some cheaper alternatives. What alternatives could you suggest?

Answers to Milord Questions

Exercise number 1.: Service management

In general both parties (the supplier and end users) should negotiate about:

The functionality of the e-mail service: what does the supplier offer to the end users. Typical e-mail functions are e.g. speed of delivery, reliability of delivery, possibility of attachments, error handling, gateways to the Internet etc.

The availability: who can use it? When can they use it (days and time-window)? What if the system is not available?

The handling of changes: what if the users want new functionality to be added to the system?

The handling of incidents: how should incidents be reported, who's going to tell the end users what's happening etc...

The capacity of the system: how many messages are expected to be send, how many attachments (small-medium large), the minimum speed of delivery, etc.

Contingency countermeasures: what is going to happen when the systems breaks down and isn't expected to be up-and-running soon?

The costs of system use: how much are they and who's going to pay for it? (invoice or otherwise)

Reports: How is the supplier going to inform the end-user (management) about the level of services provided, the number of incidents reported, the (un)availability of the system, the costs of delivery etc.

Please note:

The levels of services (e.g. service hours) negotiated are not critical here. More imported is to address the right issues as mentioned.

Exercise No. 2: Service Desk, Incident Management and Problem Management

Objections for creating a service desk:

Speed of incident-solving because of an extra stop in the workflow.(both from users and IT perspective)

Less contacts between end-users and IT-specialists. A good relationship may be spoiled.(both from users and IT perspective)

Less job-satisfaction (IT specialists)

Extra (unnecessary) costs involved in having a service desk (extra staff, equipment etc.)(user perspective)

Queuing time (user perspective)

Unable to prioritize between projects and reported incident: who's the boss I should listen to? (IT specialist)

Counter objections:

registration of incidents makes sure no incident is forgotten

service desk may divide the workload between specialists

service desk is always available; IT specialist isn't

registration makes it possible to show the workload and report about it

classification of incidents makes it possible to solve the most important incidents first.

Requirements for a tool:

Essential requirements:

All IT staff involved in the incident management process should have access.

It should be possible to appoint Incident records to a (group of) specialist(s)

The tool should display the status and priority of an incident record.

Reports about incidents and the incident management process should be easy to define and print.

It should register at least:

time and date of the incident

name and other data about the user that report the incident

severity (impact, urgency) of the incident

circumstances under which the incident occurred

the name of the specialist that has or is going to solve the incident

the solution of the incident.

Extra options of an incident management tool are e.g.:

automatic escalation when service levels are in danger

automatic re-rooting

access to a known-error database

information about the configuration of the infrastructure

analyze-options for problem management.

Levels of escalation

In general, two different ways to escalate incidents: horizontally and vertically. See org-chart for possible escalation-procedures.

Refer to Service requirements: when service levels are in danger, horizontal escalation should take place.

Reporting

The incident management report should contain at least:

number of incidents (per type, offered service, group of users/ company)

over-all performance of the process: average solving time (also per service, group of users, company etc.)

Number of incidents solved per IT-staff member in order to show the workload

Severe incidents with huge impact on the service levels.

Problem management

While an incident is the (threat of) the disruption of service itself, a problem is the root cause of that disruption. E.g: many incidents can relate to the same problem.

Examples:

A couple of E-pos terminals have a blank screen. Many incidents are reported. After an analysis, the cause of it was found: the problem was a connector not plugged in.

Forgetting your password to the FISCO-system is an incident. If the same person forgets it twice a day, there sure is a problem.

Every Monday morning the central printer at HQ is down. Restarting it gets it up and running again. That way, the incident is solved. After a while, the service desk gets annoyed and wants the specialist to solve it "for once and for all". After an investigation, the power supply, that automatically switched off during weekends (the root cause) was reconfigured. The incidents never occurred again, the problem was closed.

Incident registration from problem management perspective:

incidents should be registered in the same way (format, language used, classification, and especially the way the incidents were solved)

related incidents should be combined and marked.

It should be possible to define and run queries over the incident-data in order to sort-out incidents that are more or less the same.

Exercise No. 3: Change and Configuration Management

Objections are:

Implementing a CAB is just more bureaucracy: A Cab only meets once a week, while changes have to be implemented every day!

What does a CAB know more than the IT-project team does?

What to do with urgent changes that should be implemented immediately because of the incidents involved?

Since we have standardized the way we work and the c.i.'s we use: what can go wrong anyway?

Just another project meeting!

Change managers response:

A cab is there to oversee all the risks for major changes

If project management sends in it's rfc's on time, there won't be any delays

For quick and urgent changes there is a fast lane in the procedure.

Data needed as a change manager:

Essential:

Insight in all ci;'s, their dependencies and their status.

The rfc's related to the c.i.'s involved.

The possibility to make reports in many ways, e.g. c.i.'s changed in the last period, rfc's to be implemented next week, etc.

Optional;

a track-record of the rfc's related to the c.i.'s: when was it implemented, changed, evaluated, who was involved, who was the supplier etc.?

Case Study
The Milord Group

Exercise No. 4: Availability, IT Continuity, Capacity & Financial Management

Information needed:

How does the PureSnob and StreetCorner- shops want to use the system: when should it be available (service windows) and what amount of transaction is to be expected for both formulae?

What speed requirements do the users have?

What are the consequences (costs, public embarrassment) of an under performing or unavailable system?

Data about the expected use of the system should be collected from the users and management of the business units.

The actual data of the performance should be collected from the service desk (availability data) the customers (number of transactions) and the IT-operations staff (performance, capacity, etc.)

Information can be used to:

review the design of the system: is there enough capacity installed? Is it necessary to reduce the risks for unavailability? Etc.

also: to justify the costs of investing in high-availability countermeasures like reducing the single point of failure.

2.

Occurrences are e.g.:

Lack of power-supply

Disasters like water-flood, bomb threats, human error etc. that damage the c.i.'s involved.

The crash of system-components (c.i.'s)

The unavailability of the data-lines

Weak spots are

- Central server unit (only one present)

The data storage: is it mirrored?

Fixed lines and connector (only one)

Central printer (only one?)

Connector (if that thing breaks down, service nowhere available!)

In the Street Corner outlet: every c.i., because there's no extra E-pos

In the PureSnob outlet: the server and the printer.

Countermeasures are

Invest in reliability (better products), resilience (double configured hardware) and security (make sure no hacker can damage the system.)

Invest in maintainability (have staff around to fix it soon when it's broke), service-ability (have an external party around to fix it) and contingency.

Case Study
The Milord Group

Charging

Because the StreetCorner shop gets lower service-quality than the PureSnob shops, they should pay less for their services. So, actual charging have to take place, where the price per outlet is lower for the StreetCorner-formula than it is for the PureSnob formula. Maybe it is possible to let the PureSnob shop sponsor the StreetCorner-shop by paying for the extra hardware at the HQ.

The suggested countermeasures focus on the resilience and contingency alternatives.

Possible alternatives are also:

- Reliability investments: buy better quality products

- Security countermeasures: make sure nobody can damage the hardware

- Extra service contracts to reduce the MTBF.

- Investing in clerical back-up procedures instead of a contingency plan.

- Invest in reciprocal arrangements.

Case Study
The Milord Group

General Questions

Exercise No. 1: Service Desk and Incident Management

- What are the objectives of the Service Desk?
- Design a Script for PC based incidents concerning standard applications (e.g. Windows, word, etc). Explain why your script is useful?
- What information do you need from a Service Level to be able to measure the effectiveness of the Service Desk and the Incident Management process?
- What is the definition of an incident?
- How can the service desk reduce the number of calls?
- Describe the steps of the incident process.
- Mention the three control tasks of the incident process.

Exercise No. 2: Problem Management

- What are the objectives of Problem Management?
- Describe the steps of the Problem Control process.
- How do you measure the effectiveness of Problem Management?
- Which processes benefit most if problem management is implemented properly? And why is that?
- What is the difference between an incident and a problem?

Exercise No. 3: Change Management

- What are the objectives of Change Management?
- What information should be on a RFC if the RFC concerns the purchase of a new standard software package?
- How do you measure the effectiveness of Change Management?

Exercise No. 4: Configuration Management

- What are the objectives of Configuration Management
- Name at least 5 customers of the Configuration Management Information and tell what information they need.
- Name 3 possible ways to store Configuration Management information.
- How do you measure the effectiveness of Configuration Management?
- What is the difference between scope and detail of a CMDB?

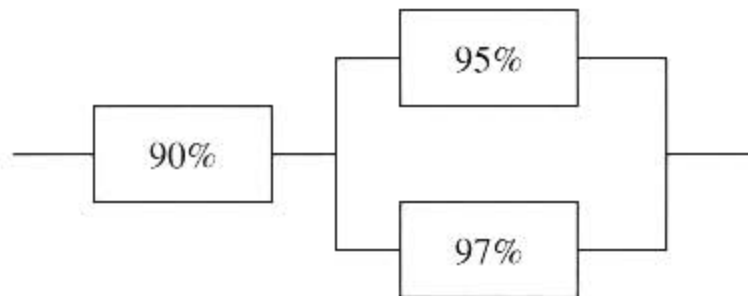
Exercise No. 5: Release Management

- Explain the relation between Release Management, Configuration Management and Change Management.
- Name 7 possible ways to avoid Release Management from a developers point of view.
- What is the DSL?
- What is the difference between a Full and a Package Release?
- Who is responsible for the release policy?

General Question

Exercise No. 6: Availability Management

- What metrics can you identify to measure the Availability of a Network and what are the metrics for a Server?
- Calculate the availability of the network below:



- What is the importance of the items below to Availability?
 - Resilience
 - Serviceability
 - Maintainability
 - Reliability
 - Security

Exercise No. 7: IT Service Continuity Management

- Why do you implement IT Service Continuity Management?
- Give examples of countermeasures you can take to react on contingencies.
- What is the difference between vulnerabilities and Risks?

Exercise No. 8: Capacity Management

- Which thresholds are set by Capacity Management, give examples for the network environment and for the server environment.
- Explain the difference between demand management and resource management. Give examples.

Exercise No. 9: Financial Management for IT Services

- Name 3 different methods to Charge
- Which information is delivered by Financial Management to Service Management
- What is the difference between accounting and charging?

Exercise No. 10: Service Level Management

- What is the difference between an OLA and a SLA;
- Is the Catalogue being used in creating a SLA, an OLA of both? And Why?
- What is the difference between a service catalogue and a quality plan?

General Question

Answers to general Questions

Exercise No. 1: Service Desk and Incident Management

1. To be the contact point for all calls, questions, complaints, requests, remarks
To resolve incidents as quickly as possible
To manage the incident lifecycle

2.	Telephone rings.		
	Help Desk: Can I help you?	End user IT personnel	Continue See 20
	Get user's telephone number and terminal ID.		
	Have you followed your local incident diagnosis scripts?	Yes, with success Yes, without success No	See 12 Continue See 5
	Is your terminal working?	No Yes	See 4 Continue
	Do any applications work?	No Yes	See 6 Continue
	What applications are you using?	Employees DB Application X Application Y	See 26 See 4 See 5

Which service levels are agreed upon: time to react, time to resolve (priorities), feedback information: what and when, where to find the SLA, how to change the SLA

- * Incident is an operational event, not part of the standard operation of a service. It will impact on the service and/or customer productivity.
- * disruption to the agreed service level
- * thread of disruption

By informing the users / customer about occurred incidents and how to prevent these "most common" incidents. Medium: e.g. a weekly or monthly information bulletin from the incident process.

- * accept incident, register data, consult CMDB
- * initial categorization
- * assess and code impact
- * search for resolution and resolve
- * close and code incident
- * Progress control
- * Quality control
- * Management Information

General Question

Exercise No. 2: Problem Management

- minimizing the consequences of incidents
- removal of the causes of incidents
- prevention of incidents and problems
- stabilizing IT services
- ensuring services meet their SLA targets

See Slide

% reoccurrence of incidents

The Customer processes. Incident management. When the cause of incidents is known and a solution is build and implemented, the related incidents won't occur any more

Incident: an operational event, which is not part of the standard operation of the service.

Problem: a condition identified from multiple incidents exhibiting common symptoms or from a single significant incident indicative of a single error, for which the cause is unknown.

Exercise No. 3: Change Management

To implement approved changes efficiently, cost effectively and with minimal risk to the existing and to the new IT infrastructure.

- which ci's are involved
- who's the change sponsor
- who's the change initiator
- what's the service impact
- requested implementation date
- what's the needed IT infrastructure, configurations
- requested functionalities
- Y2000 stability

- # of Back-Outs,
- # of times rescheduling needed,
- # of times re-decisions are needed
- # of incidents as a result of changes

General Question

Exercise No. 4: Configuration Management

Providing information on the IT infrastructure
Control through maintenance and monitoring

Service Desk, Problem management, Change management, Configuration management, Software control & Distribution, Service Level Management, Availability management, Cost management, Capacity management, Contingency planning, Software Development, Third party, Finance, Purchasing, Suppliers

Paper, Database, Online Tools, White Board/Configuration Chart

Audit trails, effect on change management

Scope: which component categories e.g. hardware, software, agreements
Detail: to which depth do you want to store information about each category

Exercise No. 5: Release Management

See Slide

Don't tell anyone about new software
Don't let the sw get registered in a DB
Keep the sw under your own control
Make an illegal copy e.g. from internet
Use a copy that a coworker has got from the DSL
Deliver changed sw directly to the user
Let users get directly in contact with you if they want changes
Make your own release numbering, which you make leading for yourself

See Slide

See Slide

SC & D is responsible for the policy. Change Manager is responsible for the Go/NoGo decision.

Exercise No. 6: Availability Management

MTBF, MTTR, MTBSI

$$0.9 \times (1 - (1 - 0.95) \times (1 - 0.97)) = 0.9 \times (1 - 0.05 \times 0.03) = 0.9 \times 0.9985 = 0.8986 = 89.86\%$$

Together they determine the availability of a service or system. Individual each has influence on the availability so you can choose which factor you find most important to have covered to ensure the desired level of availability.

Resilience: ability of the service to keep running where one or more components have failed.

General Question

Reliability: ability of component to deliver the desired functionality for a given period of time under certain circumstances.

Maintainability: ability of a component or service to return to a state in which the desired functionality will be provided again.

Serviceability: a contractual term used to define the support to be received from an external supplier.

Security: confidentiality, integrity and availability of ci's

Exercise No. 7: IT Service Continuity Management

See Slide

See Slide

See Slide

Exercise No. 8: Capacity Management

E.g Disk storage $\leq 80\%$ of full capacity, network usage $\leq 75\%$, CPU online usage $\leq 95\%$, etc

See Slide

Exercise No. 9: Financial Management for IT Services

See Slide

Cost price, charging price, charge units, # of units, forecasts, etc

Costing: knowing and controlling the costs of the IT service and the cost price of the delivered serviced (focus is internal to the IT department)

Charging: invoicing customers to make clear to them what the service they use costs.

Exercise No. 10: Service Level Management

OLA: operational level agreement. Internal agreement covering the supply of service.

SLA: service level agreement: the specific delivered It services for a customer organization.

The service catalogue describes default IT services and levels. For both internal and external use you need to know what can be delivered of what ought to be delivered under which service levels.

The service catalogue describes default IT services and levels to agree on

OLA's or SLA's. The quality plan defines internal quantity and quality parameters on agreed IT services.

General Question

Glossary by Alphabet

Term	Description	Process
.BCM	Business Continuity Management	Cont
.BRM	See Business Relationship Management	CRM
.CAB	See Change Advisory Board	Chg
.CAB/EC	See Change Advisory Board Emergency Committee	Chg
.CDB	See Capacity Database	Cap
.CFIA	Component Failure Impact Analysis	Avail
.CI	See Configuration Item	Cfg
.CMDB	See Configuration Management Database	Cfg
.CRAMM	CCTA Risk Analysis and Management Method.	All
.DHS	See Definitive Hardware Store	Rel
.DSL	See Definitive Software Library	Rel
.FSC	See Forward Schedule of Changes	Chg
.FTA	See Fault Tree Analysis	Avail
.ICT	The convergence of Information Technology, Telecommunications and Data Networking Technologies into a single technology	All
.IPW™	Implementation of a process Oriented Workflow, a process model created by Quint Wellington Redwood and Dutch Telecom (KPN). The model exists since 1993. An extension to the model is IPW Stadia Model which describes maturities, how to measure them and how to realize them, for the different ITIL processes. See www.quintgroup.com for a full English article.	All
.ISEB	Information Systems Examination Board (UK), which administers and awards IT qualifications including FC in IT Service Management.	All
.ITIL	The CCTA IT Infrastructure Library - a set of guides on the management and provision of operational IT services	All
.ItSMF	IT Service Management Forum, ITIL User Group.	All
.MTBF	See Mean Time Between Failure	Avail
.MTBSI	See Mean Time Between System Incidents	Avail
.MTTR	See Mean Time To Repair	Avail
.OLA	See Operational Level Agreement	Slm
.PIR	See Post Implementation Review	Prb
.RFC	See Request for Change	Chg
.SCI	See Software Configuration Item	Rel
.SLA	See Service Level Agreement	Slm
.SLM	See Service Level Management	Slm
.SLR	See Service Level Requirements	Slm
.SPOF	See Single Point of Failure	Avail
.UC	See Underpinning Contract or Contract	Avail
.UCC	See Utility Cost Center	Fin

Glossary by Alphabet

Term	Description	Process
Absorbed overhead	Overhead which, by means of absorption rates, is included in costs of specific products or saleable services, in a given period of time. Under or over-absorbed overhead. The difference between overhead cost incurred and overhead cost absorbed; it may be split into its two constituent parts for control purposes	Fin
Absorption costing	A principle whereby fixed as well as variable costs are allotted to cost units and total overheads are absorbed according to activity level. The term may be applied where production costs only, or costs of all functions are so allotted.	Fin
Action lists	Defined actions, allocated to recovery teams and individuals, within a phase of a plan These are supported by reference data.	All
Alert phase	The first phase of a business continuity plan in which initial emergency procedures and damage assessments are activated.	Cont
Allocated cost	A cost that can be directly identified with a business unit	Fin
Application Sizing	The process which estimates the resource requirements to support a proposed application change or new application, to ensure that it meets its required service levels.	Cap
Apportioned cost	A cost that is shared by a number of business units (an indirect cost). This cost must be shared out between these units on an equitable basis.	Fin
Asset	Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.	Cfg
Asset Management	The management of Assets	Cfg
Assurance	The processes by which an organization can verify the accuracy and completeness of its BCM.	Cont
Asynchronous /synchronous	Asynchronous in a communications sense is the ability to transmit each character as a self-contained unit of information, without additional timing information. This method of transmitting data is sometimes called start/stop. Synchronous working involves the use of timing information to allow transmission of data, which is normally done in blocks. Synchronous transmission is usually more efficient than the asynchronous method.	Tech
Attribute	Characteristic of a CI held on the CMDB.	Cfg
Audit	A test to ensure a certain function or process is functioning according to the descriptions.	All
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the Customers within the agreed service hours.	Avail
Availability Management	The process that optimizes the capability of the IT infrastructure and supporting organization to deliver a cost effective and sustained level of availability that enables the business to satisfy its business objectives.	Avail
Baseline	Snapshot of the state of a CI (CMDB) and related CI's at a point in time.	Cfg
BCM activity	An action or series of actions as part of a BCM process.	Cont

Term	Description	Process
BCM Lifecycle	The complete set of activities and processes necessary to manage business continuity - divided into four stages.	Cont
BCM process	A set of activities with defined deliverables forming a discrete part of the BCM lifecycle.	Cont
Bridge	A bridge is equipment and techniques used to match circuits to each other ensuring minimum transmission impairment.	Tech
Budgeting	The process of predicting and controlling the spending of money within the enterprise and consists of a periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets.	Cost
Build	The final stage in producing a usable configuration. The process involves taking one or more input Configuration Items and processing them (building them) to create one or more output Configuration Items e.g. software compile and load.	Cfg
Business Capacity Management	This sub-process is responsible for ensuring that the future business requirements for IT services are considered, planned and implemented in a timely fashion.	Cap
Business function	A business unit within an organization, e.g. a department, division, branch.	All
Business process	A group of business activities undertaken by an organization in pursuit of a common goal. Typical business processes include receiving orders, marketing services, selling products, delivering services, distributing products, invoicing for services, accounting for money received. A business process will usually depend upon several business functions for support, e.g. IT, personnel, accommodation. A business process will rarely operate in isolation, i.e., other business processes will depend on it and it will depend on other processes.	All
Business recovery objective	The desired time within which business processes should be recovered, and the minimum staff, assets and services required within this time.	Cont
Business recovery plan framework	A template business recovery plan (or set of plans) produced to allow the structure and proposed contents to be agreed before the detailed business recovery plan is produced.	Cont
Business recovery plans	Documents describing the roles, responsibilities and actions necessary to resume business processes following a business disruption.	Cont
Business recovery team	A defined group of personnel with a defined role and subordinate range of actions to facilitate recovery of a business function or process	Cont
Business Relationship Management	Business Relationship Management has developed which deals primarily with managing the relationships between Customers and IT Service Providers, and also with the communication that takes place between the two.	CRM
Business unit	A segment of the business entity by which both revenues are received and expenditure are caused or controlled, such revenues and expenditure being used to evaluate segmental performance.	All
Call	A contact with the Service Desk	SD

Glossary by Alphabet

Term	Description	Process
Capacity Database, CDB	A Database that will hold the information needed by all the sub-processes within Capacity Management.	Cap
Capacity Management	The process that is responsible for ensuring that IT processing and storage capacity matches the evolving demands of the business in the most cost-effective and timely manner.	Cap
Capacity Planning	Process to provide plans and reports to meet current and future business workloads.	Cap
Capital Costs	Typically those applying to the physical (substantial) assets of the organization. Traditionally this was the accommodation and machinery necessary to produce the enterprise's product. Capital Costs are the purchase or major enhancement of fixed assets, for example computer equipment (building and plant and are often also referred to as 'one-off' costs.	Fin
Capital investment appraisal	The process of evaluating proposed investment in specific fixed assets and the benefits to be obtained from their acquisition. The techniques used in the evaluation can be summarized as non-discounting methods (i.e. simple pay-back), return on capital employed and discounted cash flow methods (i.e. yield, net present value and discounted pay-back).	Fin
Capitalization	Many organizations choose to identify major expenditure as Capital, whether there is a substantial asset or not, to reduce the impact on the current financial year of such expenditure and this is referred to as 'Capitalization'. The most common item for this to be applied to is software, whether developed in-house or purchased.	Fin
Category	Classification of a group of Configuration Items, Change documents or problems.	Cfg
Category	Classification of a group of Configuration Items, Change documents or problems.	Chg
Category	Classification of a group of Configuration Items, Change documents or problems.	Inc
Category	Classification of a group of Configuration Items, Change documents or problems.	Prb
Change Management	Process of controlling Changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved Changes with minimum disruption.	Chg
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.	Chg
Change Advisory Board	A group of people who can give expert advice to Change Management on the implementation of Changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units.	Chg
Change Advisory Board Emergency Committee	A group of people who can give expert advice to Change Management on the implementation of Changes in emergency situations.	Chg
Change authority	A group that is given the authority to approve Change, e.g. by the project board. Sometimes referred to as the Configuration Board.	Chg

Glossary by Alphabet

Term	Description	Process
Change control	The procedure to ensure that all Changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the Change.	Chg
Change document	Request for Change, Change control form, Change order, Change record.	Chg
Change history	Auditable information that records, for example, what was done, when it was done, by whom and why.	Chg
Change log	A log of Requests for Change raised during the project, showing information on each Change, its evaluation what decisions have been made and its current status, e.g. Raised, Reviewed, Approved, Implemented, Closed.	Chg
Change Management	Process of controlling changes to the infrastructure or services with minimum disruption.	Chg
Change record	A record containing details of which CI's are affected by an authorized Change (planned or implemented) and how.	Chg
Channel	Channel is the physical connection from CPU to an I/O device, usually a controller, or indeed another CPU.	Chg
Chargeable Unit	Business work units to which charges can be attached	Fin
Charging	The process of establishing charges in respect of business units, and raising the relevant invoices for recovery from customers.	Fin
CI Level	The detail level of a CI	Cfg
Classification	Process of formally grouping Configuration Items by type, e.g. software, hardware, documentation, environment, application.	Cfg
Classification	Process of formally identifying Changes by type e.g. project scope change request, validation change request, infrastructure change request.	Chg
Classification	Process of formally identifying incidents, problems and known errors by origin, symptoms and cause.	Inc
Classification	Process of formally identifying incidents, problems and known errors by origin, symptoms and cause.	Prb
Closure	When the Customer is satisfied that an incident has been resolved.	Inc
Cold stand-by	See 'Gradual Recovery'	Cont
Command, control and communications	The processes by which an organization retains overall co-ordination of its recovery effort during invocation of business recovery plans.	Cont
Computer Aided Systems Engineering	A software tool for programmers. It provides help in the planning, analysis, design and documentation of computer software.	All
Configuration Baseline	<p>Configuration of a product or system established at a specific point in time, which captures both the structure and details of the product or system, and enables that product or system to be rebuilt at a later date.</p> <p>A snapshot or a position, which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position (PRINCE 2).</p>	Cfg

Glossary by Alphabet

Term	Description	Process
Configuration control	Activities comprising the control of Changes to Configuration Items after formally establishing its configuration documents. It includes the evaluation, co-ordination, approval or rejection of Changes. The implementation of Changes includes changes, deviations and waivers that impact on the configuration.	Cfg
Configuration documentation	Documents that define requirements, system design, build, production, and verification for a configuration item.	Cfg
Configuration identification	Activities that determine the product structure, the selection of Configuration Items, and the documentation of the Configuration Item's physical and functional characteristics including interfaces and subsequent Changes. It includes the allocation of identification characters or numbers to the Configuration Items and their documents. It also includes the unique numbering of configuration control forms associated with Changes and Problems.	Cfg
Configuration item (CI)	Component of an infrastructure - or an item, such as a Request for Change, associated with an infrastructure - which is (or is to be) under the control of Configuration Management. CIs may vary widely in complexity, size and type - from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component.	Cfg
Configuration Management Database (Cmdb)	A database, which contains all relevant details of each CI and details of the important relationships between CIs.	Cfg
Configuration Management Tool (CM Tool)	A software product providing automatic support for Change, Configuration or version control.	Cfg
Configuration Management	The process of identifying and defining the Configuration Items in a system, recording and reporting the status of Configuration Items and Requests for Change, and verifying the completeness and correctness of configuration items.	Cfg
Configuration Management plan	Document setting out the organization and procedures for the Configuration Management of a specific product, project, system, support group or service.	Cfg
Configuration Structure	A hierarchy of all the CIs that comprise a configuration.	Cfg
Contingency Plan	Plan detailing actions and procedures to followed in the event of a major disaster.	Cont
Contingency Planning	Planning to address unwanted occurrences that may happen at a later time. Traditionally, the term has been used to refer to planning for the recovery of IT systems rather than entire business processes.	Cont
Contract	Document between two bodies (i.e. with external suppliers) with separate legal existence.	Avail
Contract	Document between two bodies (i.e. with external suppliers) with separate legal existence.	SLM
Cost	The amount of expenditure (actual or notional) incurred on, or attributable to, a specific activity or business unit.	Fin

Glossary by Alphabet

Term	Description	Process
Cost center	IT is budgeted and there is soft charging for specific services; it is concerned with input and output costs.	Fin
Cost effectiveness	Ensuring that there is a proper balance between the quality of service on the one side and expenditure on the other. Any investment that increases the costs of providing IT services should always result in enhancement to service quality or quantity.	All
Cost management	The term used in this module to describe the procedures, tasks and deliverables that are needed to fulfill an organization's costing and charging requirements.	Fin
Cost unit	The cost unit is a functional cost unit which establishes standard cost per workload element of activity, based on calculated activity ratios converted to cost ratios.	Fin
Costing	The process of identifying the costs of the business and of breaking them down and relating them to the various activities of the organization.	Fin
Crisis management	The processes by which an organization manages the wider impact of a disaster, such as adverse media coverage.	Cont
Crisis management	The processes by which an organization manages the wider impact of a disaster, such as adverse media coverage.	Inc
Customer	Recipient of the service; usually the Customer management has responsibility for the cost of the service, either directly through charging or indirectly in terms of demonstrable business need.	All
Data transfer time	Data transfer time is the length of time taken for a block or sector of data to be read from or written to an I/O device, such as a disk or tape.	Tech
Definitive Hardware Store, DHS	The area for the secure storage of definitive hardware spares. These are spare components and assemblies that are maintained at the same level as the comparative systems within the live environment.	Rel
Definitive Software Library (DSL)	<p>The library in which the definitive authorized versions of all software CI's are stored and protected. It is a physical library or storage repository where master copies of software versions are placed. This one logical storage area may in reality consist of one or more physical software libraries or file stores. They should be separate from development and test file store areas. The DSL may also include a physical store to hold master copies of bought-in software, e.g. fireproof safe. Only authorized software should be accepted into the DSL, strictly controlled by Change and Release Management.</p> <p>The DSL exists not directly because of the needs of the Configuration Management process, but as a common base for the Release Management and Configuration Management processes.</p>	Rel

Glossary by Alphabet

Term	Description	Process
Delta Release	A Delta, or partial, Release is one that includes only those CI's within the Release unit that have actually changed or are new since the last full or Delta Release. For example, if the Release unit is the program, a Delta Release contains only those modules that have changed, or are new, since the last full release of the program or the last Delta Release of the modules - see also 'Full Release'.	Rel
Demand Management	See Business Capacity Management	Cap
Dependency	The reliance, either direct or indirect, of one process or activity upon another.	All
Depreciation	Depreciation is the loss in value of an asset due to its use and/or the passage of time. The annual depreciation charge in accounts represents the amount of capital assets need up in the accounting period. It is charged in the cost accounts to ensure that the cost of capital equipment is reflected in the unit costs of the services provided using the equipment. There are various methods of calculating depreciation for the period, but the Treasury usually recommends the use of current cost asset validation as the basis for the depreciation charge.	Fin
Differential charging	Charging business customers different rates 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 nighttime running.	Fin
Direct cost	A cost, which is incurred for, and can be traced in full to a product, service, cost center or department. This is an allocated cost. Direct costs are direct materials, direct wages and direct expenses.	Fin
Disaster recovery planning	A series of processes that focus only upon the recovery processes, principally in response to physical disasters that are contained within BCM.	Cont
Discounted cash flow	An evaluation of the future net cash flows generated by a capital project by discounting them to their present-day value. The two methods most commonly used are: a) yield method, for which the calculation determines the internal rate of return (IRR) in the form of a percentage b) net present value (NPV) method, in which the discount rate is chosen and the answer is a sum of money.	Fin
Discounting	Discounting is the offering to business customers of reduced rates for the use of off-peak resources (see also Surcharging).	Fin
Disk cache controller	Disk cache controllers have memory, which is used to store blocks of data, which have been read from the disk devices connected to them. If a subsequent I/O requires a record which is still resident in the cache memory, it will be picked up from there, thus saving another physical I/O.	Tech
Downtime	The time an agreed service is not available	Avail
Downtime	The time an agreed service is not available	Inc

Glossary by Alphabet

Term	Description	Process
Duplex (full and half)	Full duplex line/channel allows simultaneous transmission in both directions. Half duplex line/channel is capable of transmitting in both directions, but only in one direction at a time.	Tech
Echoing	Echoing is a reflection of the transmitted signal from the receiving end, a visual method of error detection in which the signal from the originating device is looped back to that device so that it can be displayed.	Tech
Elapsed Time	Time from the start of an incident, whilst the incident is not yet resolved	Avail
Elements of cost	The constituent parts of costs according to the factors upon which expenditure is incurred with materials, labor and expenses.	Fin
Emergency Release	A release that is urgently implemented. Mostly because of an outstanding incident	Rel
End-User	See 'User'.	SD
Environment	A collection of hardware, software, network communications and procedures that work together to provide a discrete type of computer service. There may be one or more environments on a physical platform e.g. test, production. An environment has unique features and characteristics that dictate how they are administered in similar, yet diverse manners.	Rel
Error Control	Error control covers the processes involved in progressing Known Errors until they are eliminated by the successful implementation of a Change under the control of the Change Management process. The objective of error control is to be aware of errors, to monitor them and to eliminate them when feasible and cost-justifiable.	Prb
Expert User	See 'Super User'.	SD
External Target	One of the measures against which a delivered IT service is compared, expressed in terms of the customer's business.	Slm
Fault tree analysis	Technique to analyze the availability of a system	Avail
Financial Management for IT Services	Financial Management is the sound stewardship of the monetary resources of the enterprise. It supports the enterprise in planning and executing its business objectives and requires consistent application throughout the enterprise to achieve maximum efficiency and minimum conflict.	Fin
Financial year	The financial year is an accounting period covering 12 consecutive months. In the public sector this financial year will generally coincide with the fiscal year, which runs from 1 April to 31 March.	Fin
First Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.	Inc

Glossary by Alphabet

Term	Description	Process
First Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.	SD
Fortress approach	IT site made as disaster-proof as possible.	Cont
Forward Schedule of Changes	Contains details of all the Changes approved for implementation and their proposed implementation dates. It should be agreed with the Customers and the business, Service Level Management, the Service Desk and Availability Management. Once agreed, the Service Desk should communicate to the User community at large any planned additional downtime arising from implementing the Changes, using the most effective methods available.	Chg
Full absorption costing	A principle where fixed and variable costs are allocated to cost units and overhead costs are absorbed according to activity levels.	Fin
Full cost	Full cost is the total cost of all the resources used in supplying a service i.e. the sum of the direct costs of producing the output a proportional share of overhead costs and any selling and distribution expenses. Both cash costs and notional (non-cash) costs should be included, including the cost of capital. Calculated as a total cost of ownership, including depreciation / planned renewal)	Fin
Full Release	All components of the Release unit are built, tested, distributed and implemented together - see also 'Delta Release'.	Rel
Functional Escalation	Escalation or Referral to more or other knowledge	Inc
Gateway	A gateway is equipment, which is used to interface networks so that a terminal on one network can communicate with services or a terminal on another.	Tech
Gradual Recovery	Previously called 'Cold stand-by', this is applicable to organizations that do not need immediate restoration of business processes and can function for a period of up to 72 hours, or longer, without a re-establishment of full IT facilities. This may include the provision of empty accommodation fully equipped with power, environmental controls and local network cabling infrastructure, telecommunications connections, and available in a disaster situation for an organization to install its own computer equipment.	Cont
Hard charging	Descriptive of a situation where, within an organization, actual funds are transferred from the customer to the IT directorate in payment for the delivery of IT services.	Fin
Hard fault	Hard faults describe the situation in a virtual memory system when the required page of code or data, which a program was using, has been redeployed by the operating system for some other purpose. This means that another piece of memory must be found to accommodate the code or data, and will involve physical reading/writing of pages to the page file.	Tech

Glossary by Alphabet

Term	Description	Process
Service Desk	The single point of contact within the IT directorate for users of IT services.	SD
Hierarchical Escalation	Escalation to a higher hierarchical layer	Inc
Host	A host computer comprises the central hardware and software resources of a computer complex, e.g. CPU, memory, channels, disk and magnetic tape I/O subsystems plus operating and applications software. The term is used to denote all non-network items.	Tech
Hot stand-by	See 'Immediate Recovery'	Cont
Immediate Recovery	Previously called 'Hot stand-by', provides for the immediate restoration of services following any irrecoverable incident. It is important to distinguish between the previous definition of 'hot standby' and 'immediate recovery'. Hot standby typically referred to availability of services within a short timescale such as 2 or 4 hours whereas immediate recovery implies the instant availability of services.	Tech
Impact	Measure of the business criticality of a Change. Often equal to the extent to which a Change can lead to distortion of agreed or expected service levels.	Chg
Impact	Measure of the business criticality of an Incident. Often equal to the extent to which an Incident leads to distortion of agreed or expected service levels.	Inc
Impact	Measure of the business criticality of a Problem. Often equal to the extent to which the Problem will benefit the business once implemented successfully.	Prb
Impact analysis	The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes. Business impact analysis identifies the form the loss or damage will take; how that degree of damage or loss is likely to escalate with time following an incident; the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level; and the time within which they should be recovered. The time within which full recovery of the business processes is to be achieved is also identified.	Chg
Impact scenario	Description of the type of impact on the business that could follow a business disruption. Will usually be related to a business process and will always refer to a period of time, e.g. customer services will be unable to operate for two days.	Inc
Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.	Inc
Incident Life Cycle	All activities from the moment an incident happens to the moment an incident is closed	Inc

Glossary by Alphabet

Term	Description	Process
Incident Management	The process that seeks to restore normal service operation as quickly as possible and that minimizes the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.	Inc
Indirect cost	An indirect cost is a cost incurred in the course of making a product providing a service or running a cost center or department, but which cannot be traced directly and in full to the product, service or department, because it has been incurred for a number of cost centers or cost units. These costs are apportioned to cost cost/cost units. Indirect costs are also referred to as overheads.	Fin
Intelligent customer	The purchaser (as distinct from the provider) of services. The term is often used in relation to the outsourcing of IT/IS.	Slm
Interface	Physical or functional interaction at the boundary between Configuration Items.	Tech
Intermediate Recovery	Previously called 'Warm stand-by', will typically involve the reestablishment of the critical systems and services within a 24 to 72 hour period, and will be used by organizations that need to recover IT facilities within a predetermined time to prevent impacts to the business process.	Cont
Internal target	One of the measures against which supporting processes for the IT service are compared. Usually expressed in technical terms relating directly to the underpinning service being measured.	Slm
Invocation (of business recovery plans)	Putting business recovery plans into operation after a business disruption.	Cont
Invocation (of stand by arrangements)	Putting stand-by arrangements into operation as part of business recovery activities.	Cont
Invocation and recovery phase	The second phase of a business recovery plan.	Cont
ISO 9000	Guidelines and assurance of processes and procedure standards for quality assurance systems.	All
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, by activity). It usually involves ledgers and should be overseen by someone trained in Accountancy.	Fin
IT Customer Relationship Management	See Business Relationship Management	CRM
IT directorate	That part of an organization charged with developing and delivering the IT services.	All
IT Infrastructure	All means needed to deliver a service, e.g. hardware, software, environment, documents.	All

Glossary by Alphabet

Term	Description	Process
IT Service Continuity Management	The process 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.	Cont
IT Services	Services are the deliverables of the IT Services section as perceived by the customers; the services do not consist merely of making computer resources available for customers to use.	All
Known Error	An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified. If a business case exists, an RFC will be raised, but, in any event, it remains a Known Error unless it is permanently fixed by a Change.	Prb
Latency	Latency describes the elapsed time from the moment when a seek was completed on a disk device to the point when the required data is positioned under the read/write heads. Latency is normally defined by manufacturers as being half the disk rotation time.	Tech
Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.	Cfg
Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.	Chg
Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.	Inc
Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.	Prb
Live Build Environment	(Part of) the computer system used to build software releases for live use.	Rel
Live environment	(Part of) computer system used to run software in live use.	Rel
Logical I/O	Logical I/O is a read or write request by a program. That request may, or may not, necessitate a physical I/O. For example, on a read request the required record may already be in a memory buffer and therefore a physical I/O will not be necessary.	Tech
Maintainability	Ability of component or service to return to a state in which the desired functionality will be provided again.	Avail
Marginal cost	The variable cost of producing one extra unit of product or service. That is, the cost which would have been avoided if the unit/service was not produced/provided.	Fin
Maturity level/Milestone	See IPW™. The degree to which BCM activities and processes have become standard business practice within an organization. See the IPW Stadia Model (www.quintgroup.com)	All

Glossary by Alphabet

Term	Description	Process
Mean Time Between Failures	Average time between restoration of service following an incident and another incident occurring.	Avail
Mean Time Between System Incidents	Average time between incident occurrence.	Avail
Mean Time To Repair	average downtime between an incident occurring and restoration of service/the system.	Avail
Modeling	An activity to predict the behavior of computer systems under a given volume and variety of work.	Cap
Monitoring	The registration and guarding of the utilization of each resource and service on an on-going basis to ensure the optimum use of the hardware and software resources, that all agreed service levels can be achieved, and that business volumes are as expected.	Cap
Multiplexer	Multiplexers divide data channels into two or more independent fixed data channels of lower speed	Tech
Operational Costs	Those resulting from the day-to-day running of the IT Services section, e.g. staff costs, hardware maintenance and electricity, and relate to repeating payments whose effects can be measured within a short timeframe, usually the less than the 12-month financial year.	Fin
Operational level agreement	An internal agreement covering the delivery of services, which support the IT directorate in their delivery of services.	Slm
Opportunity cost (or true cost)	The value of a benefit sacrificed in favor of an alternative course of action. That is the cost of using resources in a particular operation expressed in terms of foregoing the benefit that could be derived from the best alternative use of those resources.	Fin
Outsourcing	The process by which functions performed by the organization are contracted out for operation, on the organization's behalf, by third parties.	Slm
Overheads	The total of indirect materials, wages and expenses.	Fin
Package assembly /disassembly device	A package assembly/disassembly device permits terminals, which do not have an interface suitable for direct connection to a packet switched network to access such a network. A PAD converts data to/from packets and handles call set-up and addressing.	Tech
Package release	A number of release units packaged together.	Rel
Page fault	A program interruption which occurs when a page that is marked 'not in real memory' is referred to by an active page.	Tech
Paging	Paging is the I/O necessary to read and write to and from the paging disks: real (not virtual) memory is needed to process data. With insufficient real memory, the operating system writes old pages to disk, and reads new pages from disk, so that the required data and instructions are in real memory.	Tech
PD0005	Alternative title for the BSI publication 'A Code of Practice for IT Service Management'.	All

Term	Description	Process
Percentage utilization	Percentage utilization describes the amount of time that a hardware device is busy over a given period of time. For example, If the CPU is busy for 1800 seconds in one-hour period, its utilization is said to be 50%.	Cap
Performance Management	The process that ensures that technical resources in the infrastructure provide the best possible value for money.	Cap
Phantom line error	A phantom line error is a communications error reported by a computer system, which is not detected by network monitoring equipment. It is often caused by changes to the circuits and network equipment (e.g. re-routing circuits at the physical level on a backbone network) while data communications is in progress.	Tech
Physical I/O	Physical I/O means that a read or write request from a program has necessitated a physical read or write operation on an I/O device.	Tech
Post Implementation Review, PIR	A review to see if the change achieved what it should achieve	Chg
Post Implementation Review, PIR	A review to see if the change that should solve the problem, actually did solve the problem	Prb
Pricing	The policy that determines how chargeable units are priced.	Fin
Prime cost	The total cost of direct materials, direct labor and direct expenses. The term prime cost is commonly restricted to direct production costs only and so does not customarily include direct costs of marketing or research and development.	Fin
PRINCE2	The standard UK government method for project management.	All
Priority	Sequence in which an Incident or Problem needs to be resolved, based on impact and urgency.	Inc
Priority	Sequence in which an Incident or Problem needs to be resolved, based on impact and urgency.	Prb
Proactive Problem Management	The process that tries to prevent incidents from happening	Prb
Problem	Unknown underlying cause of one or more Incidents.	Prb
Problem Control	The Problem control process is concerned with handling Problems in an efficient and effective way. The aim of Problem control is to identify the root cause, such as the CIs that are at fault, and to provide the Service Desk with information and advice on Work-arounds when available.	Prb
Problem Management	The process that wants to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure, and to prevent recurrence of Incidents related to these errors.	Prb
Procedure	A connected series of actions, activities, performed by agents, detailed enough to make clear to an agent what he/she has to do.	All
Process	A connected series of actions, activities, Changes etc, performed by agents with the intent of satisfying a purpose or achieving a goal.	All

Glossary by Alphabet

Term	Description	Process
Process Control	The process of planning and regulating, with the objective of performing the process in an effective and efficient way.	All
Profit center	IT is run as a business with profit objectives.	Fin
Program	A collection of activities and projects that collectively implement a new corporate requirement or function.	Tech
Queuing time	Queuing time is incurred when the device, which a program wishes to use, is already busy. The program will therefore have to wait in a queue to obtain service from that device.	Tech
Reciprocal Arrangement	2 organizations running on compatible infrastructure provide each other with IT resources in an emergency.	Cont
Recoverability	The ability of a system to recover. This term combines maintainability, serviceability and resilience	Avail
Reference data	Information that supports the plans and action lists, such as names and addresses or inventories, which is indexed within the plan.	All
Registration	The initial and on-going recording of a CI	Cfg
Registration	The initial and on-going recording of a call	SD
Release	A collection of new and/or changed CI's, which are tested and introduced into the live environment together.	Rel
Release Management	The process that management releases, both the technical and the non technical aspects.	Rel
Release numbering	The policy that determines how releases should be numbered. The number of a release.	Rel
Release Policy	The policy that determines how releases must be treated. It encompasses size, numbering and frequency	Rel
Release unit	The level at which software of a given type is normally released.	Rel
Reliability	Ability of component to deliver desired functionality for a given period of time and under certain conditions.	Avail
Request for Change (RFC)	Form, or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.	Chg
Resilience	Ability of service to keep running where one or more components have failed.	Avail
Resolution	Action, which will resolve an Incident. This may be a Work-around.	Inc
Resource Capacity Management	The focus in this sub-process is the management of the individual components of the IT infrastructure. It is responsible for ensuring that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analyzed and reported.	Cap
Resource cost	This term is used to describe the amount of machine resource that a given task will consume. This resource is usually expressed in seconds for the CPU or the number of I/Os for a disk or tape device.	Fin
Resource Management	Process that ensures that adequate resources are available and functional at the required time.	Cap

Glossary by Alphabet

Term	Description	Process
Resource profile	Resource profile describes the total resource costs, which are consumed by an individual online transaction, batch job or program. It is usually expressed in terms of CPU seconds, number of I/Os and memory usage.	Cap
Resource unit costs	Resource unit may be calculated on a standard cost basis to identify the expected (standard) cost for using a particular resource. Because computer resources come in many shapes and forms, units have to be established by logical groupings. Examples are; a) CPU Time or instructions, b) disk I/Os, c) print lines, d) communication transactions.	Fin
Resources	The term resources refers to the means the IT Services section needs to provide the customers with the required services. The resources are typically computer and related equipment, software, facilities or organizational (people).	Cap
Restoration of Service	The moment a customer has confirmed that the service can be used again after an incident or a contingency	Avail
Restoration of Service	The moment a customer has confirmed that the service can be used again after an incident or a contingency	Cont
Return to normal phase	The phase within a business recovery plan which re-establishes normal operations.	Cont
Revenue Cost	Also called running cost, value diminishes with usage, such as paper or salaries. Usually a variable cost.	Fin
Risk	A measure of the exposure to which an organization 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.	Avail
Risk	A measure of the exposure to which an organization 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.	Cont
Risk Analysis	The identification and valuation of assets and threats; the assessment of vulnerabilities and risks by considering the threats to assets.	Avail
Risk Analysis	The identification and valuation of assets and threats; the assessment of vulnerabilities and risks by considering the threats to assets.	Cont
Risk Management	The management of risks to assets: the selection and use of countermeasures.	Avail
Risk Management	The management of risks to assets: the selection and use of countermeasures.	Cont
Risk reduction measure	Measures taken to reduce the likelihood or consequences of a business disruption occurring (as opposed to planning to recover after a disruption).	Avail
Risk reduction measure	Measures taken to reduce the likelihood or consequences of a business disruption occurring (as opposed to planning to recover after a disruption).	Cont
Role	A set of responsibilities, activities and authorizations.	All
Roll in roll out (RIRO)	RIRO is a term, which is used on some systems to describe swapping.	Tech

Glossary by Alphabet

Term	Description	Process
Rollout	The moment or period that a (set of) system(s) is implemented. This term is usually used when multiple systems are implemented on different moments	Rel
Rotational Position Sensing	RPS is a facility which is employed on most mainframes and some minicomputers. When a seek has been initiated the system can free the path from a disc drive to a controller for use by another disc drive, while it is waiting for the required data to come under the read/write heads (latency). This facility usually improves the overall performance of the I/O subsystem.	Tech
Second Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.	Inc
Second Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.	SD
Security	Confidentiality, Integrity and Availability of CI's.	Sec
Security Awareness	The measure to which an organization aware of it's security situation	Sec
Security Incidents	Incidents that threaten the security of an organization, e.g. viruses, hacker attacks, etc	Inc
Security Incidents	Incidents that threaten the security of an organization, e.g. viruses, hacker attacks, etc	Sec
Security Level	The level to which an organization has been secured	Sec
Security Management	The process that is responsible for the design and activation of all security measures needed to reach the desired security level	Sec
Security Section	The section in the SLA which describes the needed security level	Sec
Security Section	The section in the SLA which describes the needed security level	Slm
Seek time	Seek time occurs when the disc read/write heads are not positioned on the required track. It describes the elapsed time taken to move heads to the right track.	Tech
Self-insurance	A decision to bear the losses that could result from a disruption to the business as opposed to taking insurance cover on the risk.	Cont
Service achievement	The actual service levels delivered by the IT directorate to a customer within a defined lime-span.	Slm
Service Capacity Management	The focus of this sub-process is the management of the performance of the IT services used by the customers. It is responsible for ensuring that the performance of all services, as detailed in the targets in the SLAs and SLRs is monitored and measured, and that the collected data is recorded, analyzed and reported. Process that determines resource profiles needed to process current and future business workloads.	Cap
Service catalogue	Written statement of IT services, default levels and options.	Slm

Term	Description	Process
Service Desk		SD
Service hours	Hours to which the service is available.	
Service improvement program	A formal project undertaken within an organization to identify and introduce measurable improvements within a specified work area or, work process.	All
Service Level Agreement	Written agreement between a service provider and the Customer(s) that documents agreed service levels for a service.	Slm
Service level management	The process of defining, agreeing, documenting and managing the levels of customer IT service, that are required and cost justified.	Slm
Service Level Requirement	Requirements, expressed by the customer that are inputs into negotiations towards SLA.	Slm
Service provider	Third-party organization supplying services or products to customers.	Avail
Service quality plan	The written plan and specification of internal targets designed to guarantee the agreed service levels.	Slm
Service Request	Every Incident not being a failure in the IT Infrastructure.	SD
Service Window	Hours/times to which service is available	Avail
Service Window	Hours/times to which service is available	Slm
Serviceability	Contractual term used to define the support received from an external supplier.	Avail
Services	Services are the deliverables of the IT Services section as perceived by the customers; the services do not consist merely of making computer resources available for customers to use.	All
Simulation modeling	Simulation modeling, as the name implies, employs a program, which simulates computer processing by describing in detail the path of a job or transaction. It can give extremely accurate results. Unfortunately, it demands a great deal of time and effort from the modeler. It is most beneficial in extremely large or time critical systems where the margin for error is very small.	Cap
Single point of failure	A component that will cause unavailability to a service when it fails	Avail
Soft fault	A soft fault describes the situation in a virtual memory system when the operating system has detected that a page of code or data was due to be reused, i.e. it is on a list of "free" pages, but it is still actually in memory. It is now rescued and put back into service.	Tech
Software Configuration Item (SCI)	As 'Configuration Item', excluding hardware and services.	Rel
Software Environment	Software used to support the application such as operating system, database management system, development tools, compilers, and application software.	Rel
Software Library	A controlled collection of SCI's designated to keep those with like status and type together and segregated from unlike, to aid in development, operation and maintenance.	Rel

Glossary by Alphabet

Term	Description	Process
Software work unit	Software work is a generic term devised to represent a common base on which all calculations for workload usage and IT resource capacity are then based. A unit of software work for I/O type equipment equals the number of bytes transferred; and for central processors it is based on the product of power and cpu-time.	Cap
Solid state devices	Solid state disks are memory devices which are made to appear as if they are disk devices. The advantages of such devices are that the service times are much faster than real disks since there is no seek time or latency. The main disadvantage is that they are much more expensive.	Tech
Specsheet	Specifies in detail what the customer wants (external) and what consequences this has for the service provider (internal) such as required resources and skills.	Shm
Standard cost	A pre-determined calculation of how many costs should be under specified working conditions. It is built up from an assessment of the value of cost elements and correlates technical specifications and the quantification of materials, labor and other costs to the prices and/or wages expected to apply during the period in which the standard cost is intended to be used. Its main purposes are to provide bases for control through variance accounting, for the valuation of work in progress and for fixing selling prices.	Fin
Standard costing	A technique, which uses standards for costs and revenues for the purposes of control through variance analysis.	Fin
Stand-by arrangements	Arrangements to have available assets, which have been identified, as replacements should primary assets be unavailable following a business disruption. Typically, these include accommodation, IT systems and networks, telecommunications and sometimes people.	Cont
Status accounting	Process that records the state of CI's at a given time.	Cfg
Storage occupancy	Storage occupancy is a defined measurement unit that is used for storage type equipment to measure usage. The unit value equals the number of bytes stored.	Cap
Super User	In some organizations it is common to use 'expert' Users (commonly known as Super or Expert Users) to deal with first-line support problems and queries. This is typically in specific application areas, or geographical locations, where there is not the requirement for full-time support staff. This valuable resource however needs to be carefully coordinated and utilized.	SD
Support hours	Hours/times to which support is available.	SD
Surcharging	Surcharging is charging business users a premium rate for using resources at peak times.	Fin
Swapping	The reaction of the operating system to insufficient real memory: swapping occurs when too many tasks are perceived to be competing for limited resources. It is the physical movement of an entire task (e.g. all real memory pages of an address space may be moved at one time from main storage to auxiliary storage).	Tech

Glossary by Alphabet

Term	Description	Process
System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective.	All
Terminal emulation	Terminal emulation is achieved by software running on an intelligent device, typically a PC or workstation, which allows that device to function as an interactive terminal connected to a host system. Examples of such emulation software includes IBM 3270 BSC or SNA, ICL C03, or Digital VT100.	Tech
Terminal I/O	Terminal I/O is a read from, or a write to, an online device such as a VDU or remote printer.	Tech
Test Build Environment	(Part of) the computer system used to build software releases for operational acceptance testing.	Rel
Test environment	(Part of) the computer system used to run software releases for operational acceptance testing.	Rel
Third Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.	Inc
Thrashing	A condition in a virtual storage system where an excessive proportion of CPU time is spent between moving data between main and auxiliary storage.	Tech
Threat	An event that could happen and that would degrade the functioning of a component or a service	Avail
Threat	An event that could happen and that would degrade the functioning of a component or a service	Cont
Tree structures	In data structures, a series of connected nodes without cycles. One node is termed the root and is the starting point of all paths, other nodes termed leaves terminate the paths.	Tech
Underpinning contract	A contract with an external supplier covering delivery of services that support the IT directorate in their delivery of services.	Avail
Unit costs	Unit costs are costs distributed over individual component usage to establish the unit cost. For example, it can be assumed, that if a box of paper with 1000 sheets costs £10, then obviously one sheet costs 1p. Similarly if a CPU costs \$1m a year and it is used to process 1,000 jobs that year, each job costs on average \$1,000.	Fin
Urgency	Measure of the business criticality of an Incident or Problem based on the impact and on the business needs of the Customer.	Inc
Urgency	Measure of the business criticality of an Incident or Problem based on the impact and on the business needs of the Customer.	Prb
Urgent Change	A change that due to business criticality of an Incident has to be implemented urgently	Chg
User	The person who uses the service on a day-to-day basis.	SD
Utility cost center (UCC)	A cost center for the provision of support services to other cost centers.	Fin

Glossary by Alphabet

Term	Description	Process
Variance analysis	A variance is the difference between planned, budgeted, or standard cost and actual cost (or revenues). Variance analysis is an analysis of the factors, which have caused the difference between the pre-determined standards and the actual results. Variances can be developed specifically related to the operations carried out in addition to those mentioned above.	Fin
Variant	CI with the same functionality as another CI but different in some small way.	Cfg
Verification	Process that ensures the CMDB and physical CIs are synchronized.	Cfg
Version	An identified instance of a Configuration Item within a product breakdown structure or configuration structure for the purpose of tracking and auditing change history. Also used for software Configuration Items to define a specific identification released in development for drafting, review or modification, test or production.	Cfg
Version	An identified instance of a Configuration Item within a product breakdown structure or configuration structure for the purpose of tracking and auditing change history. Also used for software Configuration Items to define a specific identification released in development for drafting, review or modification, test or production.	Rel
Version Identifier	A version number; version date; or version date and time stamp.	Rel
Virtual memory system	Virtual memory systems were developed to increase the size of memory by adding an auxiliary storage layer, which resides on disk.	Tech
VSI	VSI (virtual storage interrupt) is an ICL VME term for a page fault.	Tech
Vulnerability	The measure to which a component or a service will be affected by a threat	Avail
Vulnerability	The measure to which a component or a service will be affected by a threat	Cont
Warm stand-by	See 'Intermediate Recovery'	Cont
Waterline	The lowest level of detail relevant to the customer.	Slm
Work-around	Method of avoiding an Incident or Problem, either from a temporary fix or from a technique that means the Customer is not reliant on a particular aspect of the service that is known to have a problem.	Inc
Workload Management	See Service Capacity Management	Cap
Workloads	Workloads in the context of Capacity Management Modeling, are a set of forecasts which detail the estimated resource usage over an agreed planning horizons. Workloads generally represent discrete business applications and can be further subdivided into types of work (interactive, timesharing, batch)	Cap
WORM	WORM or CD-WORM is the term which is frequently used to describe optical read only disks, standing for write once read many.	Tech

Glossary by Process

Process	Term	Description
All	.CRAMM	CCTA Risk Analysis and Management Method.
All	.ICT	The convergence of Information Technology, Telecommunications and Data Networking Technologies into a single technology
All	.IPW™	Implementation of a process Oriented Workflow, a process model created by Quint Wellington Redwood and Dutch Telecom (KPN). The model exists since 1993. An extension to the model is IPW Stadia Model which describes maturities, how to measure them and how to realize them, for the different ITIL processes. See www.quintgroup.com for a full English article.
All	.ISEB	Information Systems Examination Board (UK), which administers and awards IT qualifications including FC in IT Service Management.
All	.ITIL	The CCTA IT Infrastructure Library - a set of guides on the management and provision of operational IT services
All	.ItSMF	IT Service Management Forum, ITIL User Group.
All	Action lists	Defined actions, allocated to recovery teams and individuals, within a phase of a plan These are supported by reference data.
All	Audit	A test to ensure a certain function or process is functioning according to the descriptions.
All	Business function	A business unit within an organization, e.g. a department, division, branch.
All	Business process	A group of business activities undertaken by an organization in pursuit of a common goal. Typical business processes include receiving orders, marketing services, selling products, delivering services, distributing products, invoicing for services, accounting for money received. A business process will usually depend upon several business functions for support, e.g. IT, personnel, accommodation. A business process will rarely operate in isolation, i.e., other business processes will depend on it and it will depend on other processes.
All	Business unit	A segment of the business entity by which both revenues are received and expenditure are caused or controlled, such revenues and expenditure being used to evaluate segmental performance.
All	Computer Aided Systems Engineering	A software tool for programmers. It provides help in the planning, analysis, design and documentation of computer software.
All	Cost effectiveness	Ensuring that there is a proper balance between the quality of service on the one side and expenditure on the other. Any investment that increases the costs of providing IT services should always result in enhancement to service quality or quantity.

Glossary by Process

Process	Term	Description
All	Customer	Recipient of the service; usually the Customer management has responsibility for the cost of the service, either directly through charging or indirectly in terms of demonstrable business need.
All	Dependency	The reliance, either direct or indirect, of one process or activity upon another.
All	ISO 9000	Guidelines and assurance of processes and procedure standards for quality assurance systems.
All	IT directorate	That part of an organization charged with developing and delivering the IT services.
All	IT Infrastructure	All means needed to deliver a service, e.g. hardware, software, environment, documents.
All	IT Services	Services are the deliverables of the IT Services section as perceived by the customers; the services do not consist merely of making computer resources available for customers to use.
All	Maturity level/Milestone	See IPW™. The degree to which BCM activities and processes have become standard business practice within an organization. See the IPW Stadia Model (www.quintgroup.com)
All	PD0005	Alternative title for the BSI publication 'A Code of Practice for IT Service Management'.
All	PRINCE2	The standard UK government method for project management.
All	Procedure	A connected series of actions, activities, performed by agents, detailed enough to make clear to an agent what he/she has to do.
All	Process	A connected series of actions, activities, Changes etc, performed by agents with the intent of satisfying a purpose or achieving a goal.
All	Process Control	The process of planning and regulating, with the objective of performing the process in an effective and efficient way.
All	Reference data	Information that supports the plans and action lists, such as names and addresses or inventories, which is indexed within the plan.
All	Role	A set of responsibilities, activities and authorizations.
All	Service improvement program	A formal project undertaken within an organization to identify and introduce measurable improvements within a specified work area or, work process.
All	Services	Services are the deliverables of the IT Services section as perceived by the customers; the services do not consist merely of making computer resources available for customers to use.
All	System	An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective.
Avail	.CFIA	Component Failure Impact Analysis
Avail	.FTA	See Fault Tree Analysis
Avail	.MTBF	See Mean Time Between Failure

Process	Term	Description
Avail	.MTBSI	See Mean Time Between System Incidents
Avail	.MTTR	See Mean Time To Repair
Avail	.SPOF	See Single Point of Failure
Avail	.UC	See Underpinning Contract or Contract
Avail	Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the Customers within the agreed service hours.
Avail	Availability Management	The process that optimizes the capability of the IT infrastructure and supporting organization to deliver a cost effective and sustained level of availability that enables the business to satisfy its business objectives.
Avail	Contract	Document between two bodies (i.e. with external suppliers) with separate legal existence.
Avail	Downtime	The time an agreed service is not available
Avail	Elapsed Time	Time from the start of an incident, whilst the incident is not yet resolved
Avail	Fault tree analysis	Technique to analyze the availability of a system
Avail	Maintainability	Ability of component or service to return to a state in which the desired functionality will be provided again.
Avail	Mean Time Between Failures	Average time between restoration of service following an incident and another incident occurring.
Avail	Mean Time Between System Incidents	Average time between incident occurrence.
Avail	Mean Time To Repair	average downtime between an incident occurring and restoration of service/the system.
Avail	Recoverability	The ability of a system to recover. This term combines maintainability, serviceability and resilience
Avail	Reliability	Ability of component to deliver desired functionality for a given period of time and under certain conditions.
Avail	Resilience	Ability of service to keep running where one or more components have failed.
Avail	Restoration of Service	The moment a customer has confirmed that the service can be used again after an incident or a contingency
Avail	Risk	A measure of the exposure to which an organization 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.
Avail	Risk Analysis	The identification and valuation of assets and threats; the assessment of vulnerabilities and risks by considering the threats to assets.
Avail	Risk Management	The management of risks to assets: the selection and use of countermeasures.
Avail	Risk reduction measure	Measures taken to reduce the likelihood or consequences of a business disruption occurring (as opposed to planning to recover after a disruption).

Glossary by Process

Process	Term	Description
Avail	Service provider	Third-party organization supplying services or products to customers.
Avail	Service Window	Hours/times to which service is available
Avail	Serviceability	Contractual term used to define the support received from an external supplier.
Avail	Single point of failure	A component that will cause unavailability to a service when it fails
Avail	Threat	An event that could happen and that would degrade the functioning of a component or a service
Avail	Underpinning contract	A contract with an external supplier covering delivery of services that support the IT directorate in their delivery of services.
Avail	Vulnerability	The measure to which a component or a service will be affected by a threat
Cap	.CDB	See Capacity Database
Cap	Application Sizing	The process which estimates the resource requirements to support a proposed application change or new application, to ensure that it meets its required service levels.
Cap	Business Capacity Management	This sub-process is responsible for ensuring that the future business requirements for IT services are considered, planned and implemented in a timely fashion.
Cap	Capacity Database, CDB	A Database that will hold the information needed by all the sub-processes within Capacity Management.
Cap	Capacity Management	The process that is responsible for ensuring that IT processing and storage capacity matches the evolving demands of the business in the most cost-effective and timely manner.
Cap	Capacity Planning	Process to provide plans and reports to meet current and future business workloads.
Cap	Demand Management	See Business Capacity Management
Cap	Modeling	An activity to predict the behavior of computer systems under a given volume and variety of work.
Cap	Monitoring	The registration and guarding of the utilization of each resource and service on an on-going basis to ensure the optimum use of the hardware and software resources, that all agreed service levels can be achieved, and that business volumes are as expected.
Cap	Percentage utilization	Percentage utilization describes the amount of time that a hardware device is busy over a given period of time. For example, If the CPU is busy for 1800 seconds in one-hour period, its utilization is said to be 50%.
Cap	Performance Management	The process that ensures that technical resources in the infrastructure provide the best possible value for money.
Cap	Resource Capacity Management	The focus in this sub-process is the management of the individual components of the IT infrastructure. It is responsible for ensuring that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analyzed and reported.

Glossary by Process

Process	Term	Description
Cap	Resource Management	Process that ensures that adequate resources are available and functional at the required time.
Cap	Resource profile	Resource profile describes the total resource costs, which are consumed by an individual online transaction, batch job or program. It is usually expressed in terms of CPU seconds, number of I/Os and memory usage.
Cap	Resources	The term resources refers to the means the IT Services section needs to provide the customers with the required services. The resources are typically computer and related equipment, software, facilities or organizational (people).
Cap	Service Capacity Management	The focus of this sub-process is the management of the performance of the IT services used by the customers. It is responsible for ensuring that the performance of all services, as detailed in the targets in the SLAs and SLRs is monitored and measured, and that the collected data is recorded, analyzed and reported. Process that determines resource profiles needed to process current and future business workloads.
Cap	Simulation modeling	Simulation modeling, as the name implies, employs a program, which simulates computer processing by describing in detail the path of a job or transaction. It can give extremely accurate results. Unfortunately, it demands a great deal of time and effort from the modeler. It is most beneficial in extremely large or time critical systems where the margin for error is very small.
Cap	Software work unit	Software work is a generic term devised to represent a common base on which all calculations for workload usage and IT resource capacity are then based. A unit of software work for I/O type equipment equals the number of bytes transferred; and for central processors it is based on the product of power and cpu-time.
Cap	Storage occupancy	Storage occupancy is a defined measurement unit that is used for storage type equipment to measure usage. The unit value equals the number of bytes stored.
Cap	Workload Management	See Service Capacity Management
Cap	Workloads	Workloads in the context of Capacity Management Modeling, are a set of forecasts which detail the estimated resource usage over an agreed planning horizons. Workloads generally represent discrete business applications and can be further sub-divided into types of work (interactive, timesharing, batch)
Cfg	.CI	See Configuration Item
Cfg	.CMDB	See Configuration Management Database
Cfg	Asset	Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.
Cfg	Asset Management	The management of Assets
Cfg	Attribute	Characteristic of a CI held on the CMDB.

Glossary by Process

Process	Term	Description
Cfg	Baseline	Snapshot of the state of a CI (CMDB) and related CI's at a point in time.
Cfg	Build	The final stage in producing a usable configuration. The process involves taking one or more input Configuration Items and processing them (building them) to create one or more output Configuration Items e.g. software compile and load.
Cfg	Category	Classification of a group of Configuration Items, Change documents or problems.
Cfg	CI Level	The detail level of a CI
Cfg	Classification	Process of formally grouping Configuration Items by type, e.g. software, hardware, documentation, environment, application.
Cfg	Configuration Baseline	<p>Configuration of a product or system established at a specific point in time, which captures both the structure and details of the product or system, and enables that product or system to be rebuilt at a later date.</p> <p>A snapshot or a position, which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position (PRINCE 2).</p>
Cfg	Configuration control	Activities comprising the control of Changes to Configuration Items after formally establishing its configuration documents. It includes the evaluation, co-ordination, approval or rejection of Changes. The implementation of Changes includes changes, deviations and waivers that impact on the configuration.
Cfg	Configuration documentation	Documents that define requirements, system design, build, production, and verification for a configuration item.
Cfg	Configuration identification	Activities that determine the product structure, the selection of Configuration Items, and the documentation of the Configuration Item's physical and functional characteristics including interfaces and subsequent Changes. It includes the allocation of identification characters or numbers to the Configuration Items and their documents. It also includes the unique numbering of configuration control forms associated with Changes and Problems.
Cfg	Configuration item (CI)	Component of an infrastructure - or an item, such as a Request for Change, associated with an infrastructure - which is (or is to be) under the control of Configuration Management. CI's may vary widely in complexity, size and type - from an entire system (including all hardware, software and documentation) to a single module or a minor hardware component.
Cfg	Configuration Management Database (CMDB)	A database, which contains all relevant details of each CI and details of the important relationships between CI's.

Glossary by Process

Process	Term	Description
Cfg	Configuration Management Tool (CM Tool)	A software product providing automatic support for Change, Configuration or version control.
Cfg	Configuration Management	The process of identifying and defining the Configuration Items in a system, recording and reporting the status of Configuration Items and Requests for Change, and verifying the completeness and correctness of configuration items.
Cfg	Configuration Management plan	Document setting out the organization and procedures for the Configuration Management of a specific product, project, system, support group or service.
Cfg	Configuration Structure	A hierarchy of all the CI's that comprise a configuration.
Cfg	Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.
Cfg	Registration	The initial and on-going recording of a CI
Cfg	Status accounting	Process that records the state of CI's at a given time.
Cfg	Variant	CI with the same functionality as another CI but different in some small way.
Cfg	Verification	Process that ensures the CMDB and physical CI's are synchronized.
Cfg	Version	An identified instance of a Configuration Item within a product breakdown structure or configuration structure for the purpose of tracking and auditing change history. Also used for software Configuration Items to define a specific identification released in development for drafting, review or modification, test or production.
Chg	.CAB	See Change Advisory Board
Chg	.CAB/EC	See Change Advisory Board Emergency Committee
Chg	.FSC	See Forward Schedule of Changes
Chg	.RFC	See Request for Change
Chg	Category	Classification of a group of Configuration Items, Change documents or problems.
Chg	Change Management	Process of controlling Changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved Changes with minimum disruption.
Chg	Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.
Chg	Change Advisory Board	A group of people who can give expert advice to Change Management on the implementation of Changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units.
Chg	Change Advisory Board Emergency Committee	A group of people who can give expert advice to Change Management on the implementation of Changes in emergency situations.

Glossary by Process

Process	Term	Description
Chg	Change authority	A group that is given the authority to approve Change, e.g. by the project board. Sometimes referred to as the Configuration Board.
Chg	Change control	The procedure to ensure that all Changes are controlled, including the submission, analysis, decision making, approval, implementation and post implementation of the Change.
Chg	Change document	Request for Change, Change control form, Change order, Change record.
Chg	Change history	Auditable information that records, for example, what was done, when it was done, by whom and why.
Chg	Change log	A log of Requests for Change raised during the project, showing information on each Change, its evaluation what decisions have been made and its current status, e.g. Raised, Reviewed, Approved, Implemented, Closed.
Chg	Change Management	Process of controlling changes to the infrastructure or services with minimum disruption.
Chg	Change record	A record containing details of which CI's are affected by an authorized Change (planned or implemented) and how.
Chg	Channel	Channel is the physical connection from CPU to an I/O device, usually a controller, or indeed another CPU.
Chg	Classification	Process of formally identifying Changes by type e.g. project scope change request, validation change request, infrastructure change request.
Chg	Forward Schedule of Changes	Contains details of all the Changes approved for implementation and their proposed implementation dates. It should be agreed with the Customers and the business, Service Level Management, the Service Desk and Availability Management. Once agreed, the Service Desk should communicate to the User community at large any planned additional downtime arising from implementing the Changes, using the most effective methods available.
Chg	Impact	Measure of the business criticality of a Change. Often equal to the extent to which a Change can lead to distortion of agreed or expected service levels.
Chg	Impact analysis	The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes. Business impact analysis identifies the form the loss or damage will take; how that degree of damage or loss is likely to escalate with time following an incident; the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level; and the time within which they should be recovered. The time within which full recovery of the business processes is to be achieved is also identified.
Chg	Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.

Glossary by Process

Process	Term	Description
Chg	Post Implementation Review, PIR	A review to see if the change achieved what it should achieve
Chg	Request for Change (RFC)	Form, or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.
Chg	Urgent Change	A change that due to business criticality of an Incident has to be implemented urgently
Cont	BCM	Business Continuity Management
Cont	Alert phase	The first phase of a business continuity plan in which initial emergency procedures and damage assessments are activated.
Cont	Assurance	The processes by which an organization can verify the accuracy and completeness of its BCM.
Cont	BCM activity	An action or series of actions as part of a BCM process.
Cont	BCM Lifecycle	The complete set of activities and processes necessary to manage business continuity - divided into four stages.
Cont	BCM process	A set of activities with defined deliverables forming a discrete part of the BCM lifecycle.
Cont	Business recovery objective	The desired time within which business processes should be recovered, and the minimum staff, assets and services required within this time.
Cont	Business recovery plan framework	A template business recovery plan (or set of plans) produced to allow the structure and proposed contents to be agreed before the detailed business recovery plan is produced.
Cont	Business recovery plans	Documents describing the roles, responsibilities and actions necessary to resume business processes following a business disruption.
Cont	Business recovery team	A defined group of personnel with a defined role and subordinate range of actions to facilitate recovery of a business function or process
Cont	Cold stand-by	See 'Gradual Recovery'
Cont	Command, control and communications	The processes by which an organization retains overall co-ordination of its recovery effort during invocation of business recovery plans.
Cont	Contingency Plan	Plan detailing actions and procedures to followed in the event of a major disaster.
Cont	Contingency Planning	Planning to address unwanted occurrences that may happen at a later time. Traditionally, the term has been used to refer to planning for the recovery of IT systems rather than entire business processes.
Cont	Crisis management	The processes by which an organization manages the wider impact of a disaster, such as adverse media coverage.
Cont	Disaster recovery planning	A series of processes that focus only upon the recovery processes, principally in response to physical disasters that are contained within BCM.
Cont	Fortress approach	IT site made as disaster-proof as possible.

Glossary by Process

Process	Term	Description
Cont	Gradual Recovery	Previously called 'Cold stand-by', this is applicable to organizations that do not need immediate restoration of business processes and can function for a period of up to 72 hours, or longer, without a re-establishment of full IT facilities. This may include the provision of empty accommodation fully equipped with power, environmental controls and local network cabling infrastructure, telecommunications connections, and available in a disaster situation for an organization to install its own computer equipment.
Cont	Hot stand-by	See 'Immediate Recovery'
Cont	Intermediate Recovery	Previously called 'Warm stand-by', will typically involve the reestablishment of the critical systems and services within a 24 to 72 hour period, and will be used by organizations that need to recover IT facilities within a predetermined time to prevent impacts to the business process.
Cont	Invocation (of business recovery plans)	Putting business recovery plans into operation after a business disruption.
Cont	Invocation (of stand by arrangements)	Putting stand-by arrangements into operation as part of business recovery activities.
Cont	Invocation and recovery phase	The second phase of a business recovery plan.
Cont	IT Service Continuity Management	The process 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.
Cont	Reciprocal Arrangement	2 organizations running on compatible infrastructure provide each other with IT resources in an emergency.
Cont	Restoration of Service	The moment a customer has confirmed that the service can be used again after an incident or a contingency
Cont	Return to normal phase	The phase within a business recovery plan which re-establishes normal operations.
Cont	Risk	A measure of the exposure to which an organization 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.
Cont	Risk Analysis	The identification and valuation of assets and threats; the assessment of vulnerabilities and risks by considering the threats to assets.
Cont	Risk Management	The management of risks to assets: the selection and use of countermeasures.
Cont	Risk reduction measure	Measures taken to reduce the likelihood or consequences of a business disruption occurring (as opposed to planning to recover after a disruption).

Glossary by Process

Process	Term	Description
Cont	Self-insurance	A decision to bear the losses that could result from a disruption to the business as opposed to taking insurance cover on the risk.
Cont	Stand-by arrangements	Arrangements to have available assets, which have been identified, as replacements should primary assets be unavailable following a business disruption. Typically, these include accommodation, IT systems and networks, telecommunications and sometimes people.
Cont	Threat	An event that could happen and that would degrade the functioning of a component or a service
Cont	Vulnerability	The measure to which a component or a service will be affected by a threat
Cont	Warm stand-by	See 'Intermediate Recovery'
Cost	Budgeting	The process of predicting and controlling the spending of money within the enterprise and consists of a periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets.
CRM	.BRM	See Business Relationship Management
CRM	Business Relationship Management	Business Relationship Management has developed which deals primarily with managing the relationships between Customers and IT Service Providers, and also with the communication that takes place between the two.
CRM	IT Customer Relationship Management	See Business Relationship Management
Fin	.UCC	See Utility Cost Center
Fin	Absorbed overhead	Overhead which, by means of absorption rates, is included in costs of specific products or saleable services, in a given period of time. Under or over-absorbed overhead. The difference between overhead cost incurred and overhead cost absorbed: it may be split into its two constituent parts for control purposes
Fin	Absorption costing	A principle whereby fixed as well as variable costs are allotted to cost units and total overheads are absorbed according to activity level. The term may be applied where production costs only, or costs of all functions are so allotted.
Fin	Allocated cost	A cost that can be directly identified with a business unit
Fin	Apportioned cost	A cost that is shared by a number of business units (an indirect cost). This cost must be shared out between these units on an equitable basis.
Fin	Capital Costs	Typically those applying to the physical (substantial) assets of the organization. Traditionally this was the accommodation and machinery necessary to produce the enterprise's product. Capital Costs are the purchase or major enhancement of fixed assets, for example computer equipment (building and plant and are often also referred to as 'one-off' costs.

Glossary by Process

Process	Term	Description
Fin	Capital investment appraisal	The process of evaluating proposed investment in specific fixed assets and the benefits to be obtained from their acquisition. The techniques used in the evaluation can be summarized as non-discounting methods (i.e. simple pay-back), return on capital employed and discounted cash flow methods (i.e. yield, net present value and discounted pay-back).
Fin	Capitalization	Many organizations choose to identify major expenditure as Capital, whether there is a substantial asset or not, to reduce the impact on the current financial year of such expenditure and this is referred to as 'Capitalization'. The most common item for this to be applied to is software, whether developed in-house or purchased.
Fin	Chargeable Unit	Business work units to which charges can be attached
Fin	Charging	The process of establishing charges in respect of business units, and raising the relevant invoices for recovery from customers.
Fin	Cost	The amount of expenditure (actual or notional) incurred on, or attributable to, a specific activity or business unit.
Fin	Cost center	It is budgeted and there is soft charging for specific services; it is concerned with input and output costs.
Fin	Cost management	The term used in this module to describe the procedures, tasks and deliverables that are needed to fulfill an organization's costing and charging requirements.
Fin	Cost unit	The cost unit is a functional cost unit which establishes standard cost per workload element of activity, based on calculated activity ratios converted to cost ratios.
Fin	Costing	The process of identifying the costs of the business and of breaking them down and relating them to the various activities of the organization.
Fin	Depreciation	Depreciation is the loss in value of an asset due to its use and/or the passage of time. The annual depreciation charge in accounts represents the amount of capital assets need up in the accounting period. It is charged in the cost accounts to ensure that the cost of capital equipment is reflected in the unit costs of the services provided using the equipment. There are various methods of calculating depreciation for the period, but the Treasury usually recommends the use of current cost asset validation as the basis for the depreciation charge.
Fin	Differential charging	Charging business customers different rates 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 nighttime running.
Fin	Direct cost	A cost, which is incurred for, and can be traced in full to a product, service, cost center or department. This is an allocated cost. Direct costs are direct materials, direct wages and direct expenses.

Glossary by Process

Process	Term	Description
Fin	Discounted cash flow	An evaluation of the future net cash flows generated by a capital project by discounting them to their present-day value. The two methods most commonly used are: a) yield method, for which the calculation determines the internal rate of return (IRR) in the form of a percentage b) net present value (NPV) method, in which the discount rate is chosen and the answer is a sum of money.
Fin	Discounting	Discounting is the offering to business customers of reduced rates for the use of off-peak resources (see also Surcharging).
Fin	Elements of cost	The constituent parts of costs according to the factors upon which expenditure is incurred with materials, labor and expenses.
Fin	Financial Management for IT Services	Financial Management is the sound stewardship of the monetary resources of the enterprise. It supports the enterprise in planning and executing its business objectives and requires consistent application throughout the enterprise to achieve maximum efficiency and minimum conflict.
Fin	Financial year	The financial year is an accounting period covering 12 consecutive months. In the public sector this financial year will generally coincide with the fiscal year, which runs from 1 April to 31 March.
Fin	Full absorption costing	A principle where fixed and variable costs are allocated to cost units and overhead costs are absorbed according to activity levels.
Fin	Full cost	Full cost is the total cost of all the resources used in supplying a service i.e. the sum of the direct costs of producing the output a proportional share of overhead costs and any selling and distribution expenses. Both cash costs and notional (non-cash) costs should be included, including the cost of capital. Calculated as a total cost of ownership, including depreciation / planned renewal)
Fin	Hard charging	Descriptive of a situation where, within an organization, actual funds are transferred from the customer to the IT directorate in payment for the delivery of IT services.
Fin	Indirect cost	An indirect cost is a cost incurred in the course of making a product providing a service or running a cost center or department, but which cannot be traced directly and in full to the product, service or department, because it has been incurred for a number of cost centers or cost units. These costs are apportioned to cost cost/cost units. Indirect costs are also referred to as overheads.
Fin	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, by activity). It usually involves ledgers and should be overseen by someone trained in Accountancy.

Glossary by Process

Process	Term	Description
Fin	Marginal cost	The variable cost of producing one extra unit of product or service. That is, the cost which would have been avoided if the unit/service was not produced/provided.
Fin	Operational Costs	Those resulting from the day-to-day running of the IT Services section, e.g. staff costs, hardware maintenance and electricity, and relate to repeating payments whose effects can be measured within a short timeframe, usually the less than the 12-month financial year.
Fin	Opportunity cost (or true cost)	The value of a benefit sacrificed in favor of an alternative course of action. That is the cost of using resources in a particular operation expressed in terms of foregoing the benefit that could be derived from the best alternative use of those resources.
Fin	Overheads	The total of indirect materials, wages and expenses.
Fin	Pricing	The policy that determines how chargeable units are priced.
Fin	Prime cost	The total cost of direct materials, direct labor and direct expenses. The term prime cost is commonly restricted to direct production costs only and so does not customarily include direct costs of marketing or research and development.
Fin	Profit center	IT is run as a business with profit objectives.
Fin	Resource cost	This term is used to describe the amount of machine resource that a given task will consume. This resource is usually expressed in seconds for the CPU or the number of I/Os for a disk or tape device.
Fin	Resource unit costs	Resource unit may be calculated on a standard cost basis to identify the expected (standard) cost for using a particular resource. Because computer resources come in many shapes and forms, units have to be established by logical groupings. Examples are; a) CPU Time or instructions, b) disk I/Os, c) print lines, d) communication transactions.
Fin	Revenue Cost	Also called running cost, value diminishes with usage, such as paper or salaries. Usually a variable cost.
Fin	Standard cost	A pre-determined calculation of how many costs should be under specified working conditions. It is built up from an assessment of the value of cost elements and correlates technical specifications and the quantification of materials, labor and other costs to the prices and/or wages expected to apply during the period in which the standard cost is intended to be used. Its main purposes are to provide bases for control through variance accounting, for the valuation of work in progress and for fixing selling prices.
Fin	Standard costing	A technique, which uses standards for costs and revenues for the purposes of control through variance analysis.
Fin	Surcharging	Surcharging is charging business users a premium rate for using resources at peak times.

Glossary by Process

Process	Term	Description
Fin	Unit costs	Unit costs are costs distributed over individual component usage to establish the unit cost. For example, it can be assumed, that if a box of paper with 1000 sheets costs £10, then obviously one sheet costs 1p. Similarly if a CPU costs \$1m a year and it is used to process 1,000 jobs that year, each job costs on average \$1,000.
Fin	Utility cost center (UCC)	A cost center for the provision of support services to other cost centers.
Fin	Variance analysis	A variance is the difference between planned, budgeted, or standard cost and actual cost (or revenues). Variance analysis is an analysis of the factors, which have caused the difference between the pre-determined standards and the actual results. Variances can be developed specifically related to the operations carried out in addition to those mentioned above.
Inc	Category	Classification of a group of Configuration Items, Change documents or problems.
Inc	Classification	Process of formally identifying incidents, problems and known errors by origin, symptoms and cause.
Inc	Closure	When the Customer is satisfied that an incident has been resolved.
Inc	Crisis management	The processes by which an organization manages the wider impact of a disaster, such as adverse media coverage.
Inc	Downtime	The time an agreed service is not available
Inc	First Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.
Inc	Functional Escalation	Escalation or Referral to more or other knowledge
Inc	Hierarchical Escalation	Escalation to a higher hierarchical layer
Inc	Impact	Measure of the business criticality of an Incident. Often equal to the extend to which an Incident leads to distortion of agreed or expected service levels.
Inc	Impact scenario	Description of the type of impact on the business that could follow a business disruption. Will usually be related to a business process and will always refer to a period of time, e.g. customer services will be unable to operate for two days.
Inc	Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Inc	Incident Life Cycle	All activities from the moment an incident happens to the moment an incident is closed
Inc	Incident Management	The process that seeks to restore normal service operation as quickly as possible and that minimizes the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.

Glossary by Process

Process	Term	Description
Inc	Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.
Inc	Priority	Sequence in which an Incident or Problem needs to be resolved, based on impact and urgency.
Inc	Resolution	Action, which will resolve an Incident. This may be a Work-around.
Inc	Second Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.
Inc	Security Incidents	Incidents that threaten the security of an organization, e.g. viruses, hacker attacks, etc
Inc	Third Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.
Inc	Urgency	Measure of the business criticality of an Incident or Problem based on the impact and on the business needs of the Customer.
Inc	Work-around	Method of avoiding an Incident or Problem, either from a temporary fix or from a technique that means the Customer is not reliant on a particular aspect of the service that is known to have a problem.
Prb	.PIR	See Post Implementation Review
Prb	Category	Classification of a group of Configuration Items, Change documents or problems.
Prb	Classification	Process of formally identifying incidents, problems and known errors by origin, symptoms and cause.
Prb	Error Control	Error control covers the processes involved in progressing Known Errors until they are eliminated by the successful implementation of a Change under the control of the Change Management process. The objective of error control is to be aware of errors, to monitor them and to eliminate them when feasible and cost-justifiable.
Prb	Impact	Measure of the business criticality of a Problem. Often equal to the extent to which the Problem will benefit the business once implemented successfully.
Prb	Known Error	An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified. If a business case exists, an RFC will be raised, but, in any event, it remains a Known Error unless it is permanently fixed by a Change.
Prb	Lifecycle	A series of states, connected by allowable transitions. The lifecycle represents an approval process for Configuration Items, Incident Reports, Problem Reports and Change documents.

Process	Term	Description
Prb	Post Implementation Review, PIR	A review to see if the change that should solve the problem, actually did solve the problem
Prb	Priority	Sequence in which an Incident or Problem needs to be resolved, based on impact and urgency.
Prb	Proactive Problem Management	The process that tries to prevent incidents from happening
Prb	Problem	Unknown underlying cause of one or more Incidents.
Prb	Problem Control	The Problem control process is concerned with handling Problems in an efficient and effective way. The aim of Problem control is to identify the root cause, such as the CIs that are at fault, and to provide the Service Desk with information and advice on Work-arounds when available.
Prb	Problem Management	The process that wants to minimize the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure, and to prevent recurrence of Incidents related to these errors.
Prb	Urgency	Measure of the business criticality of an Incident or Problem based on the impact and on the business needs of the Customer.
Rel	.DHS	See Definitive Hardware Store
Rel	.DSL	See Definitive Software Library
Rel	.SCI	See Software Configuration Item
Rel	Definitive Hardware Store, DHS	The area for the secure storage of definitive hardware spares. These are spare components and assemblies that are maintained at the same level as the comparative systems within the live environment.
Rel	Definitive Software Library (DSL)	<p>The 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 versions are placed. This one logical storage area may in reality consist of one or more physical software libraries or file stores. They should be separate from development and test file store areas. The DSL may also include a physical store to hold master copies of bought-in software, e.g. fireproof safe. Only authorized software should be accepted into the DSL, strictly controlled by Change and Release Management.</p> <p>The DSL exists not directly because of the needs of the Configuration Management process, but as a common base for the Release Management and Configuration Management processes.</p>

Glossary by Process

Process	Term	Description
Rel	Delta Release	A Delta, or partial, Release is one that includes only those CIs within the Release unit that have actually changed or are new since the last full or Delta Release. For example, if the Release unit is the program, a Delta Release contains only those modules that have changed, or are new, since the last full release of the program or the last Delta Release of the modules - see also 'Full Release'.
Rel	Emergency Release	A release that is urgently implemented. Mostly because of an outstanding incident
Rel	Environment	A collection of hardware, software, network communications and procedures that work together to provide a discrete type of computer service. There may be one or more environments on a physical platform e.g. test, production. An environment has unique features and characteristics that dictate how they are administered in similar, yet diverse manners.
Rel	Full Release	All components of the Release unit are built, tested, distributed and implemented together - see also 'Delta Release'.
Rel	Live Build Environment	(Part of) the computer system used to build software releases for live use.
Rel	Live environment	(Part of) computer system used to run software in live use.
Rel	Package release	A number of release units packaged together.
Rel	Release	A collection of new and/or changed CIs, which are tested and introduced into the live environment together.
Rel	Release Management	The process that management releases, both the technical and the non technical aspects.
Rel	Release numbering	The policy that determines how releases should be numbered. The number of a release.
Rel	Release Policy	The policy that determines how releases must be treated. It encompasses size, numbering and frequency
Rel	Release unit	The level at which software of a given type is normally released.
Rel	Rollout	The moment or period that a (set of) system(s) is implemented. This term is usually used when multiple systems are implemented on different moments
Rel	Software Configuration Item (SCI)	As 'Configuration Item', excluding hardware and services.
Rel	Software Environment	Software used to support the application such as operating system, database management system, development tools, compilers, and application software.
Rel	Software Library	A controlled collection of SCIs designated to keep those with like status and type together and segregated from unlike, to aid in development, operation and maintenance.
Rel	Test Build Environment	(Part of) the computer system used to build software releases for operational acceptance testing.
Rel	Test environment	(Part of) the computer system used to run software releases for operational acceptance testing.

Glossary by Process

Process	Term	Description
Rel	Version	An identified instance of a Configuration Item within a product breakdown structure or configuration structure for the purpose of tracking and auditing change history. Also used for software Configuration Items to define a specific identification released in development for drafting, review or modification, test or production.
Rel	Version Identifier	A version number; version date; or version date and time stamp.
SD	Call	A contact with the Service Desk
SD	End-User	See 'User'.
SD	Expert User	See 'Super User'.
SD	First Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.
SD	Service Desk	The single point of contact within the IT directorate for users of IT services.
SD	Registration	The initial and on-going recording of a call
SD	Second Line Support	Often, departments and (specialist) support groups other than the Service Desk are referred to as second- or third-line support groups, having more specialist skills, time or other resources to solve Incidents. In this respect, the Service Desk would be first-line support.
SD	Service Desk	
SD	Service hours	Hours to which the service is available.
SD	Service Request	Every Incident not being a failure in the IT Infrastructure.
SD	Super User	In some organizations it is common to use 'expert' Users (commonly known as Super or Expert Users) to deal with first-line support problems and queries. This is typically in specific application areas, or geographical locations, where there is not the requirement for full-time support staff. This valuable resource however needs to be carefully coordinated and utilized.
SD	Support hours	Hours/times to which support is available.
SD	User	The person who uses the service on a day-to-day basis.
Sec	Security	Confidentiality, Integrity and Availability of CI's.
Sec	Security Awareness	The measure to which an organization aware of it's security situation
Sec	Security Incidents	Incidents that threaten the security of an organization, e.g. viruses, hacker attacks, etc
Sec	Security Level	The level to which an organization has been secured
Sec	Security Management	The process that is responsible for the design and activation of all security measures needed to reach the desired security level
Sec	Security Section	The section in the SLA which describes the needed security level
Slm	.OLA	See Operational Level Agreement
Slm	.SLA	See Service Level Agreement

Glossary by Process

Process	Term	Description
Slm	.SLM	See Service Level Management.
Slm	.SLR	See Service Level Requirements
Slm	External Target	One of the measures against which a delivered IT service is compared, expressed in terms of the customer's business.
Slm	Intelligent customer	The purchaser (as distinct from the provider) of services. The term is often used in relation to the outsourcing of IT/IS.
Slm	Internal target	One of the measures against which supporting processes for the IT service are compared. Usually expressed in technical terms relating directly to the underpinning service being measured.
Slm	Operational level agreement	An internal agreement covering the delivery of services, which support the IT directorate in their delivery of services.
Slm	Outsourcing	The process by which functions performed by the organization are contracted out for operation, on the organization's behalf, by third parties.
Slm	Security Section	The section in the SLA which describes the needed security level
Slm	Service achievement	The actual service levels delivered by the IT directorate to a customer within a defined time-span.
Slm	Service catalogue	Written statement of IT services, default levels and options.
Slm	Service Level Agreement	Written agreement between a service provider and the Customer(s) that documents agreed service levels for a service.
Slm	Service level management	The process of defining, agreeing, documenting and managing the levels of customer IT service, that are required and cost justified.
Slm	Service Level Requirement	Requirements, expressed by the customer that are inputs into negotiations towards SLA.
Slm	Service quality plan	The written plan and specification of internal targets designed to guarantee the agreed service levels.
Slm	Service Window	Hours/times to which service is available
Slm	Specsheet	Specifies in detail what the customer wants (external) and what consequences this has for the service provider (internal) such as required resources and skills.
Slm	Waterline	The lowest level of detail relevant to the customer.
SLM	Contract	Document between two bodies (i.e. with external suppliers) with separate legal existence.
Tech	Asynchronous /synchronous	Asynchronous in a communications sense is the ability to transmit each character as a self-contained unit of information, without additional timing information. This method of transmitting data is sometimes called start/stop. Synchronous working involves the use of timing information to allow transmission of data, which is normally done in blocks. Synchronous transmission is usually more efficient than the asynchronous method.
Tech	Bridge	A bridge is equipment and techniques used to match circuits to each other ensuring minimum transmission impairment.

Process	Term	Description
Tech	Data transfer time	Data transfer time is the length of time taken for a block or sector of data to be read from or written to an I/O device, such as a disk or tape.
Tech	Disk cache controller	Disk cache controllers have memory, which is used to store blocks of data, which have been read from the disk devices connected to them. If a subsequent I/O requires a record which is still resident in the cache memory, it will be picked up from there, thus saving another physical I/O.
Tech	Duplex (full and half)	Full duplex line/channel allows simultaneous transmission in both directions. Half duplex line/channel is capable of transmitting in both directions, but only in one direction at a time.
Tech	Echoing	Echoing is a reflection of the transmitted signal from the receiving end, a visual method of error detection in which the signal from the originating device is looped back to that device so that it can be displayed.
Tech	Gateway	A gateway is equipment, which is used to interface networks so that a terminal on one network can communicate with services or a terminal on another.
Tech	Hard fault	Hard faults describe the situation in a virtual memory system when the required page of code or data, which a program was using, has been redeployed by the operating system for some other purpose. This means that another piece of memory must be found to accommodate the code or data, and will involve physical reading/writing of pages to the page file.
Tech	Host	A host computer comprises the central hardware and software resources of a computer complex, e.g. CPU, memory, channels, disk and magnetic tape I/O subsystems plus operating and applications software. The term is used to denote all non-network items.
Tech	Immediate Recovery	Previously called 'Hot stand-by', provides for the immediate restoration of services following any irrecoverable incident. It is important to distinguish between the previous definition of 'hot standby' and 'immediate recovery'. Hot standby typically referred to availability of services within a short timescale such as 2 or 4 hours whereas immediate recovery implies the instant availability of services.
Tech	Interface	Physical or functional interaction at the boundary between Configuration Items.
Tech	Latency	Latency describes the elapsed time from the moment when a seek was completed on a disk device to the point when the required data is positioned under the read/write heads. Latency is normally defined by manufacturers as being half the disk rotation time.
Tech	Logical I/O	Logical I/O is a read or write request by a program. That request may, or may not, necessitate a physical I/O. For example, on a read request the required record may already be in a memory buffer and therefore a physical I/O will not be necessary.

Glossary by Process

Process	Term	Description
Tech	Multiplexer	Multiplexers divide data channels into two or more independent fixed data channels of lower speed
Tech	Package assembly /disassembly device	A package assembly/disassembly device permits terminals, which do not have an interface suitable for direct connection to a packet switched network to access such a network. A PAD converts data to/from packets and handles call set-up and addressing.
Tech	Page fault	A program interruption which occurs when a page that is marked 'not in real memory' is referred to by an active page.
Tech	Paging	Paging is the I/O necessary to read and write to and from the paging disks: real (not virtual) memory is needed to process data. With insufficient real memory, the operating system writes old pages to disk, and reads new pages from disk, so that the required data and instructions are in real memory.
Tech	Phantom line error	A phantom line error is a communications error reported by a computer system, which is not detected by network monitoring equipment. It is often caused by changes to the circuits and network equipment (e.g. re-routing circuits at the physical level on a backbone network) while data communications is in progress.
Tech	Physical I/O	Physical I/O means that a read or write request from a program has necessitated a physical read or write operation on an I/O device.
Tech	Program	A collection of activities and projects that collectively implement a new corporate requirement or function.
Tech	Queuing time	Queuing time is incurred when the device, which a program wishes to use, is already busy. The program will therefore have to wait in a queue to obtain service from that device.
Tech	Roll in roll out (RIRO)	RIRO is a term, which is used on some systems to describe swapping.
Tech	Rotational Position Sensing	RPS is a facility which is employed on most mainframes and some minicomputers. When a seek has been initiated the system can free the path from a disc drive to a controller for use by another disc drive, while it is waiting for the required data to come under the read/write heads (latency). This facility usually improves the overall performance of the I/O subsystem.
Tech	Seek time	Seek time occurs when the disc read/write heads are not positioned on the required track. It describes the elapsed time taken to move heads to the right track.
Tech	Soft fault	A soft fault describes the situation in a virtual memory system when the operating system has detected that a page of code or data was due to be reused, i.e. it is on a list of "free" pages, but it is still actually in memory. It is now rescued and put back into service.
Tech	Solid state devices	Solid state disks are memory devices which are made to appear as if they are disk devices. The advantages of such devices are that the service times are much faster than real disks since there is no seek time or latency. The main disadvantage is that they are much more expensive.

Glossary by Process

Process	Term	Description
Tech	Swapping	The reaction of the operating system to insufficient real memory: swapping occurs when too many tasks are perceived to be competing for limited resources. It is the physical movement of an entire task (e.g. all real memory pages of an address space may be moved at one time from main storage to auxiliary storage).
Tech	Terminal emulation	Terminal emulation is achieved by software running on an intelligent device, typically a PC or workstation, which allows that device to function as an interactive terminal connected to a host system. Examples of such emulation software includes IBM 3270 BSC or SNA, ICL C03, or Digital VT100.
Tech	Terminal I/O	Terminal I/O is a read from, or a write to, an online device such as a VDU or remote printer.
Tech	Thrashing	A condition in a virtual storage system where an excessive proportion of CPU time is spent between moving data between main and auxiliary storage.
Tech	Tree structures	In data structures, a series of connected nodes without cycles. One node is termed the root and is the starting point of all paths, other nodes termed leaves terminate the paths.
Tech	Virtual memory system	Virtual memory systems were developed to increase the size of memory by adding an auxiliary storage layer, which resides on disk.
Tech	VSI	VSI (virtual storage interrupt) is an ICL VME term for a page fault.
Tech	WORM	WORM or CD-WORM is the term which is frequently used to describe optical read only disks, standing for write once read many.

Glossary by Process

Sample Examination

ITIL
Foundation Certificate in IT Service Management
(ITIL Foundation)
Sample Examination
Based on 2001-2002 module description

Contents
Introduction
Sample Questions
Answer Key

Stichting EXIN
Kantoor Janssoenborch,
Hoog Catharyne
Godebaldkwartier 265, 3511 DT
Utrecht
Postbus 19147, 3501 DC Utrecht
Telephone (030) 234 48 11
Fax (030) 231 59 86
E-mail info@exin.nl
Internet <http://www.exin-exam.nl>

Sample Examination

Place in the Qualification Structure

This is the sample examination for the Foundation Certificate in IT Service Management (ITIL Foundation):

Composition of the Sample Examination

This sample examination consists of 40 multiple-choice questions. These questions are representative of those asked during an actual examination. The questions are designed to fulfil the examination requirements for the ITIL Foundation module specified in the ITIL, PRINCE2, ISPL and DSDM 2001-2002 examination plan.

Each question in this sample examination is multiple choice, with only one correct answer.

Distribution of the Questions Across the Examination Requirements

The 40 questions in this sample examination cover the examination requirements as illustrated in the table below. The questions in the examination are not arranged in the order of examination requirement, but are in random sequence.

Examination Requirement	Number of Questions	Question Number in Sample Examination
General (1, 2)	3	2, 22, 32
ITIL processes (3, 4)		
Service Desk	3	1, 13, 27
Incident Management	4	3, 10, 19, 24
Problem Management	5	4, 18, 20, 35, 36
Change Management	6	5, 6, 25, 34, 37, 40
Configuration Management	5	7, 26, 28, 33, 38
Release Management	2	11, 29
Service Level Management	3	12, 16, 30
Availability Management	2	17, 39
Capacity Management	2	14, 23
IT Service Continuity Management	2	8, 21
Financial Management for IT Services	1	15
Security Management	2	9, 31

Literature, Notes and Calculator

When taking the examination, you may not use literature, notes or a (pre-programmable) calculator.

Time

You have 60 minutes to complete this examination.

Examination Scoring

Each correct answer earns 1 point, for a maximum possible score of 40 points. A score of 26 points or more is considered a passing grade.

No rights can be derived from this provisional data.

Sample Examination

- 1 Which of the following is a Service Desk activity?
 - to function as the first point of customer contact
 - to investigate the cause of disruptions for the customer
 - to trace the cause of incidents
- 2 What is the role of ITIL within IT Service Management?
 - to provide an approach based on the best examples taken from practice
 - to serve as the international standard for IT Service Management
 - to serve as the standard model for IT service provision
 - to serve as a theoretical framework for process design
- 3 The network managers have excessive workloads and have no time to proactively manage the network. One of the contributing factors to these large workloads is the frequency that users contact these managers directly.

Which ITIL process would improve this situation?
 - Change Management
 - Configuration Management
 - Incident Management
 - Problem Management
- 4 Which task is a Problem Management responsibility?
 - to co-ordinate all modifications to the IT infrastructure
 - to record incidents for later study
 - to approve all modifications made to the Known Error database
 - to identify user needs and modify the IT infrastructure based on such needs
- 5 The data in the Configuration Management Database (CMDB) can only be modified after permission is granted to modify the infrastructure.

Which process grants such permission?
 - Change Management
 - Configuration Management
 - Incident Management
 - Service Level Management
- 6 Which concept is part of Change Management?
 - Post Implementation Review
 - Emergency Release
 - Service Request
 - Work-around

Sample Examination

- 7 A new networked computer is installed to replace an existing PC. The old PC is installed as a print server for the local area network.
- Which process is responsible for registering this modification in the Configuration Management Database (CMDB)?
- Change Management
 - Configuration Management
 - Problem Management
 - Release Management
- 8 Because of its increased dependency on information systems, a national realty firm decides that there must be assurances for the provision of IT services following an interruption to the service.
- Which process should be implemented to provide this assurance?
- Availability Management
 - IT Service Continuity Management
 - Service Level Management
 - Service Management
- 9 Data provided for the financial administration of XYZ must only be accessible to authorized users. Security Management takes steps to ensure this.
- By taking these steps, which aspect of data can be ensured?
- Availability
 - Integrity
 - Stability
 - Confidentiality
- 10 A computer operator notices the full storage capacity of her/his disk will soon be used.
- To which ITIL process must this situation be reported?
- Availability Management
 - Capacity Management
 - Change Management
 - Incident Management
- 11 Which activity is a Release Management responsibility?
- to check whether there is any illegal software on computers within the organization
 - to store the original versions of all authorized software within the organization
 - to register where each software version is available

- 12 For which purpose does Service Level Management use data from the Service Desk's incident registration?
- to draw up Service Level Agreements (SLAs)
 - to report on the number and nature of incidents that occurred during a specific period
 - to determine the availability of an IT service using the number of resolved incidents
 - to analyze, together with other data, in order to determine if the agreed service level is being provided
- 13 The Service Desk has handled 2317 calls this month.
- What would these calls include?
- modifications to Service Level Agreements (SLAs)
 - notices regarding modified Configuration Items (CIs)
 - requests to the IT organization for user support
- 14 A steel company is merging with a competitor. The IT departments, along with the IT infrastructures of both companies will be combined.
- Which process is responsible for determining the required disk and memory space required for applications running in the combined IT infrastructure?
- Application Management
 - Capacity Management
 - Computer Operations Management
 - Release Management
- 15 Which concept is not part of Financial Management for IT Services?
- Budgeting
 - Charging
 - Procuring
 - Pricing
- 16 Service Level Requirements are used in the Service Level Management process.
- What do these Service Level Requirements represent?
- the customer's expectations and needs regarding the service
 - what the IT organization expects of the customer
 - the conditions required for the Service Level Agreement (SLA)
 - a paragraph of the SLA with additional specifications required to execute the SLA
- 17 Which of the following is one of the responsibilities of Availability Management?
- to enter into contracts with suppliers
 - to monitor the availability of a charge through system
 - to verify the reliability and the service level of the Configuration Items (CIs) purchased from and maintained by third parties
 - to plan and manage the reliability and availability of IT Service

Sample Examination

- 18 A user complains to the Service Desk that an error continually occurs when using a specific application. This causes the connection with the network to be broken.

Which ITIL process is responsible for tracing the cause?

Availability Management
Incident Management
Problem Management
Release Management

- 19 A serious incident has occurred. The assigned solution team is unable to resolve this incident within the agreed time. The Incident Manager is called in.

Which form of escalation describes the above sequence of events?

formal escalation
functional escalation
hierarchical escalation
operational escalation

- 20 Which of the following best describes a Problem?

one or more Known Errors
a known cause of one or more disruptions
the unknown cause of one or more incidents
a Known Error with one or more incidents

- 21 Which concept is part of IT Service Continuity Management?

Application Sizing
Vulnerability
Maintainability
Resilience

- 22 How does IT Service Management contribute to the quality of IT service provision?

by recording agreements between internal and external customers and suppliers in formal documents
by defining generally accepted norms for service levels
by promoting a customer focus among all the employees of the IT organization
by planning, implementing and managing a coherent set of processes for providing IT services

- 23 Performance Management and Resource Management are parts of which process?

Availability Management
Capacity Management
IT Service Continuity Management
Service Level Management

- 24 An organization has set up an Incident Management Process. In doing so, several groups were created to resolve specific incidents. These groups include:
 PC Solution Team;
 Network Solution Team;
 Service Desk;
 Specialists' Group to support the other teams.

Within an IT organization, support groups are generally categorized by levels. Select the answer that correctly categorizes the support groups mentioned above.

0-line	Service Desk
first-line	both Solution Teams
second-line	Specialists
first-line	Service Desk
second-line	PC Solution Team
third-line	Network Solution Team
fourth-line	Specialists
first-line	Service Desk
second-line	both Solutions Teams
third-line	Specialists

- 25 The management of ABC Inc. has insisted that each request for a new workstation installation be handled with optimum efficiency and effectiveness.

Which ITIL process is designed to achieve this desired outcome?

Change Management
 Customer Liaison
 Problem Management
 Service Level Management

- 26 Which of the following is a Configuration Item (CI)?

a call
 documentation
 an incident
 a process

- 27 How does Problem Management support the Service Desk activities?

It resolves serious incidents for the Service Desk.
 It studies all incidents resolved by the Service Desk.
 It relieves the Service Desk by communicating the resolution directly to the user.
 It makes information on a Known Error available to the Service Desk.

Sample Examination

28 Which of the following is a Configuration Baseline?

- the standard configuration for the Configuration Management Database (CMDB)
- a description of a standardized Configuration Item (CI)
- a set of CIs that is delivered once
- a recorded snapshot of a product or service, to provide a basis for a configuration audit and regression

29 Which of the following is the role of the Definitive Software Library (DSL) in the Release Management process?

- a physical storage area for the original versions of all authorized software in use
- a reference manual that includes all software documentation
- a registration tool for all software items
- a type of Configuration Management Database (CMDB) for software

30 Your Network Department has made an agreement with an external organization in order to fulfil an agreement with its internal customer.

Where would the agreement with the external organization be specified?

- Operational Level Agreement (OLA)
- Service Level Agreement (SLA)
- Service Level Requirement (SLR)
- Underpinning Contract (UC)

31 How does Availability Management work with Security Management?

- by making agreements on the availability of the Security Database
- by making agreements on the security of the Availability Database
- by establishing the security boundaries based on the availability requirements
- by implementing the measures specified by Security Management for securing the data

32 Which question is being answered when an organization specifies its vision and business objectives?

- How do we get where we want to be?
- How do we know we have arrived?
- Where do we want to be?
- Where are we now?

33 Which task is the responsibility of Configuration Management?

- convening the Configuration Advisory Board
- physically managing software items
- installing equipment at the workplace
- recording the relations between Configuration Items (CIs)

- 34 After the requisite search, the common cause of a series of incidents is found. This results in a Known Error.

In the sequence of things, what should happen after the Known Error has been declared?

All incidents must be resolved as quickly as possible.
The error must be resolved using a change.
The error must be included in the Configuration Management Database (CMDB).
The problem must be identified.

- 35 What is the primary task of Error Control?

to figure out the details for work-around
to resolve Known Errors through the Change Management process
to recognize and register Known Errors
to register and manage Known Errors

- 36 Which ITIL process is associated with a Post Implementation Review?

Application Management
Incident Management
Problem Management
Release Management

- 37 When processing a Request for Change (RFC), the Change Manager initiates a number of activities.

Which action is required if this involves a complex change?

The Change Manager reports the change to Problem Management.
The Change Manager reports the change to Incident Management.
The Change Manager presents the change to the Change Advisory Board.
The Change Manager presents the change to the IT Manager.

- 38 What is the difference between Asset Management and Configuration Management?

Asset Management only deals with what you own; Configuration Management deals with everything in your infrastructure.
Asset Management is a superset of Configuration Management, as it includes non-IT assets such as chairs and tables.
Asset Management deals with the financial aspects of Configuration Items;
Configuration Management only deals with the technical details of the infrastructure.
Configuration Management goes much further than Asset Management, because it also specifies the relations between the assets.

Sample Examination

39 Which ITIL process uses Mean Time Between Failures (MTBF)?

- Availability Management
- Capacity Management
- IT Service Continuity Management
- Service Level Management

40 A company sets up an Intranet for its graphic design workstations. The bandwidth must be increased because of the high volume of illustrations sent over the network.

Which ITIL process is responsible for approving the implementation of increased bandwidth?

- Capacity Management
- Change Management
- Availability Management
- Problem Management

The Evaluation

Examination Results

A maximum of 40 points can be earned on an ITIL Foundation examination.

A score of 26 points or higher is considered a passing grade.

The following table relates the number of points earned to a grade.

Failed

Number of Points Earned	Grade
0 – 11	1
12 – 15	2
16 – 18	3
19 – 22	4
23 – 25	5

Passed

Number of Points Earned	Grade
26 – 29	6
30 – 32	7
33 – 36	8
37 – 39	9
40	10

Sample Examination

Sample Examination

The table below shows the correct answers to the questions in this sample examination.

number	answer	points
1	A	1
2	A	1
3	C	1
4	C	1
5	A	1
6	A	1
7	B	1
8	B	1
9	D	1
10	D	1
11	B	1
12	D	1
13	C	1
14	B	1
15	C	1
16	A	1
17	C	1
18	C	1
19	C	1
20	C	1

number	answer	points
21	B	1
22	D	1
23	B	1
24	C	1
25	A	1
26	B	1
27	D	1
28	D	1
29	A	1
30	D	1
31	D	1
32	C	1
33	D	1
34	B	1
35	B	1
36	C	1
37	C	1
38	D	1
39	A	1
40	B	1

Sample Examination

Foundation Certificate in IT Service Management

Exam requirements specifications

Understanding of the importance of IT Service Management and the IT Infrastructure

The candidate has understanding of the importance of IT Service Management and the IT Infrastructure.

The candidate is able to indicate the importance of a methodical and systematic approach to information technology service:

for users and customers of IT Service

for suppliers of IT Service.

Understanding of the Service Management processes and the interfaces between them

The candidate has understanding of the Service Management processes and the interfaces between them.

The candidate is able to:

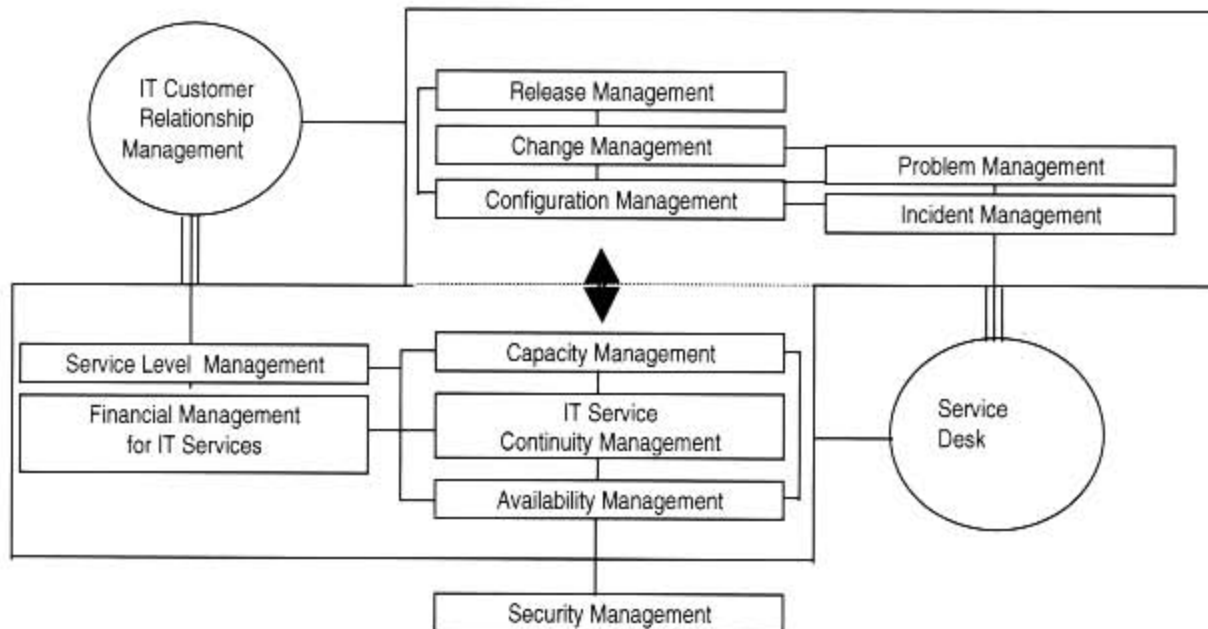
mention the benefits of the description of the Service Management processes for an organization

distinguish between ITIL processes and organizational units

indicate which elements are needed for the description of the ITIL processes.

Knowledge of an ITIL management model

The candidate has knowledge of the following ITIL management model.



The candidate is able to:
distinguish the objectives, activities and results of the various ITIL processes
give examples for each of the connections in the representation of the relationships between the processes.

Basic concepts of ITIL

The candidate has knowledge of the following basic concepts of ITIL:

Application Sizing	Failure
Asset Management*	Fault
Assets	Financial Management for IT Services*
Audit*	First Line Support*
Availability	Forward Schedule of Changes, FSC*
Availability Management	Full Release
Budgeting*	Functional Escalation*
Business Process*	Service Desk
Call*	Hierarchical Escalation*
Capacity Database, CDB	Impact
Capacity Management	Incident
Capacity Planning	Incident Life Cycle*
Category*	Incident Management*
Change	Integrity*
Change Advisory Board	IT Customer Relationship Management*
Change Management	IT Infrastructure
Chargeable Unit	IT Service
Charging	IT Service Continuity Management*
CI Level	IT Service Management
Classification*	Known Error
Confidentiality*	Maintainability
Configuration Baseline*	Mean Time Between Failures
Configuration Item, CI	Mean Time To Repair
Configuration Management*	Mission Statement
Configuration Management Database, CMDB	Modeling*
Costing	Monitoring
Customer	Operational*
Customer Liaison	Operational Level Agreement, OLA*
Definitive Hardware Store, DHS*	Package Release
Definitive Software Library, DSL	Performance
Demand Management	Performance Management
Disaster	Post Implementation Review, PIR*
Downtime	Pricing*
Elapsed Time*	Priority
Emergency Release*	Proactive Problem Management*
Error Control	Problem
Escalation*	Problem Control
Evaluation*	Problem Management

Procedure*	Service Catalogue
Process*	Service Desk*
Process Manager*	Service Improvement Plan*
Quality Assurance	Service Level
Quality Control	Service Level Agreement, SLA
Quality Assurance	Service Level Management
Quality Control	Service Level Requirements*
Recoverability	Service Request*
Recovery*	Service Window*
Registration*	Serviceability
Release Management*	Software Item
Release Policy*	Software Release
Release Unit*	Status*
Reliability	Strategic*
Report*	Tactical*
Request for Change, RFC	Third Line Support*
Resilience	Threat
Resource Management	Underpinning Contract*
Restoration of Service*	Urgency*
Review	Urgent Change
Risk	User
Rollout*	User
Second Line Support*	Verification*
Security	Version*
Security Awareness*	Vulnerability
Security Incidents*	Work-around*
Security Level*	Workflow Position*
Security Management	Workload
Security Section*	Workload Management

EXIN/ISEB Terms