

ITIL Foundation for IT Service Management

H1846S K.01



Student guide

ITIL Foundation for IT Service Management

H1846S K.01



Student guide

Use of this material to deliver training without prior written permission from HP is prohibited.

© Copyright 2006 Hewlett-Packard Development Company, L.P.

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

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

Printed in the US

ITIL Foundation for IT Service Management

Student guide

November 2006

Module 1 — Introduction

| | |
|---|----|
| IT is the business..... | 2 |
| The Four Ps | 3 |
| People | 3 |
| Processes | 3 |
| Products | 4 |
| Partners | 4 |
| IT Service Management..... | 5 |
| Course Format..... | 6 |
| IT Service Management Foundation Certificate | 7 |
| Examination for the Foundation certificate in IT Service Management | 8 |
| IT Infrastructure Library (ITIL) | 9 |
| Process Management..... | 11 |
| ITIL Philosophy..... | 12 |
| Best Practice — A Working Definition | 14 |
| The Drivers for High Quality IT Services..... | 15 |
| ITIL Objectives | 17 |
| Continuous Improvement..... | 19 |
| Service Culture | 21 |
| Achieving a Service Culture..... | 22 |
| What Is an IT Service? | 23 |
| Core ITSM Components..... | 24 |
| Service Support Disciplines | 25 |
| Service Delivery Processes | 26 |
| Service Management | 27 |

Module 2 — Service Desk

| | |
|--|----|
| Mission of Service Desk..... | 2 |
| Objectives of Service Desk..... | 4 |
| Common Features and Characteristics (1 of 2)..... | 6 |
| Common Features and Characteristics (2 of 2) | 8 |
| Staffing Options | 10 |
| Skills and Mindset | 11 |
| Service Desk Implementation..... | 12 |
| Local Service Desks..... | 13 |
| Central Service Desk..... | 14 |
| Virtual Service Desk | 15 |
| ‘Follow the Sun’ Option..... | 16 |
| A Self-Service Strategy | 17 |
| Outsourcing the Service Desk..... | 19 |
| Potential Benefits | 19 |
| Care Needed | 20 |
| Service Desk Questions: Responsibilities | 21 |
| Service Desk Questions: Functions | 22 |
| The Function of the Service Desk | 22 |

Module 3 — Incident Management

| | |
|--|----|
| Mission of Incident Management..... | 2 |
| Objectives of Incident Management..... | 3 |
| Scope of Incident Management..... | 4 |
| Definition — An Incident | 5 |
| Incident Determination (1 of 3) | 6 |
| Incident Determination (2 of 3)..... | 7 |
| Incident Determination (3 of 3)..... | 8 |
| Definition — A Problem..... | 9 |
| Definition — A Known Error..... | 10 |
| Inputs, Outputs, and Activities | 11 |
| Relationships between Incidents, Problems, Known Errors and Changes..... | 13 |
| Example Coding System for Incident/Request Classification | 14 |
| Impact + Urgency = Priority | 15 |
| Example of a Priority Coding System..... | 16 |
| Incident Status — Examples | 17 |
| Escalation..... | 18 |
| Functional Escalation..... | 19 |
| Hierarchical Escalation..... | 20 |
| Incident Manager Responsibilities..... | 21 |
| Service Desk/First Line Responsibilities | 22 |
| Second Line/Third Line Support Staff Responsibilities | 23 |
| Benefit of Incident Management | 24 |
| Incident Management Elements | 25 |

Module 4 — Problem Management

| | |
|--|----|
| Mission of Problem Management | 2 |
| Scope/Objectives of Problem Management | 3 |
| Key Definitions (Refresher) | 5 |
| Incident Management and Problem Management | 6 |
| Problem Control | 7 |
| Error Control | 8 |
| Known Errors — Development | 9 |
| Problem Management Responsibilities | 10 |
| Proactive Problem Management | 11 |
| Problem Management Techniques | 12 |
| Pain Value Analysis | 13 |
| Ishikawa Diagram | 14 |
| Core Activities | 15 |
| Terminology | 16 |

Module 5 — Configuration Management

| | |
|---|----|
| Mission of Configuration Management | 2 |
| Scope of Configuration Management | 3 |
| Objectives of Configuration Management | 4 |
| Configuration Management – Key Definitions | 5 |
| Configuration | 5 |
| Configuration Item | 6 |
| CI Types | 6 |
| Attribute | 6 |
| Relationship | 7 |
| Lifecycle | 7 |
| Core Activities of Configuration Management | 8 |
| Planning for Configuration Management | 9 |
| Configuration Management Database (CMDB) | 11 |
| Key ITIL Interfaces | 12 |
| Configuration Management's Contribution to License Management | 13 |
| License Management | 13 |
| Identification | 14 |
| Physical and Logical Identification | 14 |
| Naming Conventions | 15 |
| What Do We Need to Identify? (1 of 4) | 16 |
| What Do We Need to Identify? (2 of 4) | 17 |
| What Do We Need to Identify? (3 of 4) | 18 |
| Baseline | 18 |
| Variant | 18 |
| What Do We Need to Identify? (4 of 4) | 19 |
| Lifecycle | 19 |

| | |
|--|----|
| Configuration Control (1 of 2) | 20 |
| Controlling Information in the CMDB | 20 |
| Configuration Control (2 of 2) | 21 |
| Configuration and Change Management | 22 |
| The Relationship between Configuration and Change Management | 22 |
| Configuration Status Accounting | 24 |
| Tracking the Status of CIs | 24 |
| Configuration Audit and Verification | 25 |
| Components Recorded in the CMDB | 26 |
| Configuration Items | 27 |

Module 6 — Change Management

| | |
|--|----|
| Mission of Change Management..... | 2 |
| Scope of Change Management | 3 |
| Objectives of Change Management..... | 4 |
| Scalability | 5 |
| Core Elements | 6 |
| Request for Change (RFC) | 6 |
| Change Advisory Board (CAB) | 6 |
| Change Advisory Board/Emergency Committee (CAB/EC) | 7 |
| Forward Schedule of Changes (FSC) and Projected Service Availability (PSA) ... | 7 |
| Normal/Urgent Change | 7 |
| Change Model | 8 |
| Standard Change | 8 |
| Post Implementation Review (PIR) | 8 |
| CAB | 9 |
| Logging Changes | 10 |
| Change Initiation | 10 |
| Initial Logging and Filtering | 10 |
| Initial Priority | 11 |
| Change Categorization | 11 |
| Assessing and Scheduling Normal Changes | 12 |
| Assessing Normal Changes..... | 12 |
| Change Assessment and Approval | 12 |
| Change Scheduling | 13 |
| Building and Implementing Normal Changes | 14 |
| Change Building..... | 14 |
| Change Testing..... | 15 |
| Implementation | 15 |
| Change Review..... | 15 |
| Documentation..... | 15 |
| Assessing and Scheduling Urgent Changes | 16 |
| When are Urgent Changes Allowed? | 16 |
| Urgent Change Assessment and Approval..... | 16 |
| Urgent Change Scheduling | 17 |

| | |
|--|----|
| Building and Implementing Urgent Changes | 18 |
| Urgent Change Building | 18 |
| Urgent Change Testing | 18 |
| Urgent Change Implementation | 18 |
| Urgent Change Review | 19 |
| Urgent Change Review | 19 |
| Documentation of Urgent Changes | 19 |
| What Happens if an Urgent Change Fails? | 20 |
| Change Models (1 of 2) | 21 |
| Change Models (2 of 2) | 22 |
| Change and Program Management | 23 |
| Controlling Changes to IT Infrastructure | 24 |
| Assessing the Impact of Change | 25 |

Module 7 — Release Management

| | |
|---|----|
| Mission of Release Management | 2 |
| Scope of Release Management | 4 |
| Objectives of Release Management | 6 |
| Definition of a Release | 7 |
| Licensing Issues | 8 |
| Definitive Software Library (DSL) (1 of 2) | 9 |
| Definitive Software Library (DSL) (2 of 2) | 10 |
| Quality Assurance | 10 |
| Definitive Hardware Store (DHS) | 11 |
| Release Policies | 12 |
| Release Policies | 12 |
| Release Units | 12 |
| Release Types | 13 |
| Release Scales / Identification | 14 |
| Release Scales | 14 |
| Release Identification | 14 |
| Elements | 15 |
| Release Records | 16 |
| Release Management Activities (1 of 2) | 17 |
| Release Planning | 17 |
| Designing, Building and Configuring a Release | 17 |
| Testing and Release Acceptance | 18 |
| Release Management Activities (2 of 2) | 19 |
| Rollout Planning | 19 |
| Communication, Preparation and Training | 19 |
| Distribution and Installation | 19 |
| Definitive Software Library | 20 |
| Scope of Releases | 21 |

Module 8 — Service Level Management

| | |
|--|----|
| Mission of Service Level Management | 2 |
| Scope of Service Level Management | 3 |
| Objectives of Service Level Management | 4 |
| Levels of Service | 5 |
| Managing Expectations | 6 |
| The Service Level Management Process | 7 |
| Establish the Process | 7 |
| Implement SLAs | 8 |
| Manage the Ongoing Process | 8 |
| Periodic Reviews | 8 |
| The Cruise Director | 9 |
| Service-based SLA Structure | 10 |
| Customer-based SLA Structure | 11 |
| Multi-level SLAs | 12 |
| SLA Contents (1 of 2) | 13 |
| SLA Contents (2 of 2) | 15 |
| Example Service Catalog | 16 |
| Example Service Level Agreement Management / Red Amber Green Chart | 17 |
| Service Improvement Program (SIP) | 18 |
| Integration With Other Disciplines | 19 |
| Availability Management | 19 |
| Capacity Management | 19 |
| Incident and Problem Management | 20 |
| Change Management | 20 |
| Configuration Management | 20 |
| Financial Management | 20 |
| Service Continuity Management | 20 |
| Security Management | 21 |
| Application Development | 21 |
| Service Level Agreement Purpose | 22 |
| Service Level Structures | 23 |

Module 9 — Availability Management

| | |
|--|----|
| Mission of Availability Management | 2 |
| Scope of Availability Management | 3 |
| Objectives of Availability Management | 4 |
| Key Concepts | 5 |
| Availability | 6 |
| Reliability | 7 |
| Maintainability and Serviceability | 9 |
| Maintainability | 9 |
| Serviceability | 9 |
| Security Management | 10 |
| Service Agreements | 12 |
| Service Agreements | 12 |
| Expanded Incident Lifecycle | 13 |
| Availability Management and Incidents | 14 |
| Availability Components | 15 |
| Designing for Availability and Recovery | 15 |
| Availability Plan | 16 |
| Availability Measurement and Reporting | 16 |
| Techniques and Tools | 17 |
| Component Failure Impact Analysis (CFIA) | 17 |
| Fault Tree Analysis (FTA) | 17 |
| The CCTA Risk Analysis and Management Method (CRAMM) | 18 |
| Service Outage Analysis (SOA) | 18 |
| The Expanded Incident Lifecycle | 18 |
| Technical Observation Post (TOP) | 18 |
| Example CFIA | 19 |
| Fault Tree Analysis (FTA) | 20 |
| Availability Management Responsibilities | 21 |
| Continuous Operation | 22 |

Module 10 — Capacity Management

| | |
|--|----|
| Mission of Capacity Management | 2 |
| Cost against Capacity | 2 |
| Supply against Demand..... | 2 |
| Scope of Capacity Management | 4 |
| Objectives of Capacity Management | 5 |
| Capacity Management | 6 |
| Capacity Management Strategy | 7 |
| Capacity Management | 8 |
| Business Capacity Management | 8 |
| Service Capacity Management | 9 |
| Resource Capacity Management..... | 9 |
| Capacity Management Activities | 10 |
| Iterative Activities (Performance Management) (1 of 2)..... | 11 |
| Iterative Activities (Performance Management) (2 of 2) | 12 |
| Demand Management | 13 |
| Capacity Database (CDB) Inputs and Outputs..... | 15 |
| Application Sizing | 16 |
| Modeling | 17 |
| Types of Modeling | 18 |
| Business and IT Planning | 20 |
| Capacity Planning | 21 |
| The Capacity Plan | 22 |
| Information Needed for Capacity Management | 23 |
| Service Capacity Management | 24 |

Module 11 — Financial Management

| | |
|---|----|
| Mission of Financial Management | 2 |
| Scope of Financial Management | 4 |
| Budgeting | 4 |
| IT Accounting | 4 |
| Charging | 4 |
| Objectives of Financial Management | 5 |
| Budgeting..... | 6 |
| IT Accounting..... | 7 |
| Cost Types and Cost Elements | 8 |
| The IT Accounting System — Cost Models..... | 9 |
| Cost Classification..... | 9 |
| Cost Units | 11 |
| Cost Centers | 11 |
| Monitoring | 11 |
| Cost Model..... | 12 |
| Investment Appraisal | 13 |
| Charging..... | 14 |
| When Do You Charge? | 15 |

| | |
|------------------------------------|----|
| Benefits of Charging | 17 |
| Problems of Charging | 18 |
| Charging and Pricing Policies..... | 19 |
| Determine Charging Policy | 19 |
| Chargeable Items..... | 19 |
| Pricing Policy | 20 |
| Pricing Methods..... | 20 |
| Differential Charging | 21 |
| Billing | 22 |
| Pricing Methods | 23 |
| When to Set Charging | 24 |

Module 12 — IT Service Continuity Management

| | |
|--|----|
| Mission of IT Service Continuity Management | 2 |
| Scope of IT Service Continuity Management | 3 |
| Objectives of IT Service Continuity Management | 4 |
| Business and IT Responsibilities | 5 |
| Business Responsibilities..... | 5 |
| IT Responsibilities | 6 |
| Possible Threads | 7 |
| The Process — Stages 1 and 2..... | 8 |
| Business Impact Analysis (BIA)..... | 9 |
| Risk Analysis and Management..... | 10 |
| Definitions..... | 10 |
| Graphical Representation of Priorities | 11 |
| Service Continuity Strategy | 12 |
| The Process — Stage 3 (Implementation) | 13 |
| Typical Organization Structure..... | 14 |
| Standby Arrangement/Risk Reduction | 16 |
| The IT Service Continuity Plan..... | 19 |
| Produce the plan..... | 19 |
| Recovery Plans | 20 |
| Key Areas | 20 |
| Test the Plan..... | 21 |
| The Process — Stage 4 (Operational/Ongoing) | 23 |
| Education and Awareness | 23 |
| Training | 23 |
| Testing | 23 |
| Change Management..... | 24 |
| Review | 24 |
| ITSCM Analysis Method | 25 |
| Defining an Intermediate Recovery Site | 26 |
| IT is the business..... | 27 |

Module 13 — Security Management (EXIN Only)

| | |
|---|----|
| Mission Statement..... | 2 |
| What is Security Management?..... | 3 |
| Why the Need for Security Management? | 4 |
| Objectives of Security Management | 5 |
| ITIL and Security | 6 |
| ITIL and Security – Together a Controlled Process | 6 |
| Who is Responsible for Security Management? | 7 |
| Information Security Model (ISM)..... | 8 |
| Information Security Model (ISM) – The Business Perspective | 8 |
| IT Security Management Process..... | 9 |
| Key Security Concerns..... | 11 |
| Goals of Security Management: Security Policy | 13 |
| Goals of Security Management: Confidentiality | 14 |

Appendix A — Candidate Registration Form

Glossary

Introduction

Module 1

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

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

IT is the business

IT is the business.....



“IT is the business”
and
“The business is IT”

It is no longer possible to separate the IT department from the process of delivering the "End Product" of the business as IT is now truly "Customer facing" in most organizations. It is also fair to say that the business cannot ignore or underestimate the importance of IT to its own survival. The relationship is now a true symbiosis where both sides have to work as one to survive and prosper.

The Four Ps



The Four Ps

IT Service Management (ITSM) is all about the efficient, effective and economical use of:

- People
 - Customers, Users & IT Staff
- Processes
 - ITIL
- Products
 - Tools and technology
- Partners
 - Vendors and Suppliers

The key objectives of IT Service Management can only be realized by the best utilization of the four P's; people, processes, products and partners.

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

The Service Management processes are the hub of ITIL and the main focus is on two core areas, Service Delivery and Service Support

Service Delivery processes are concerned with tactical /medium term management cycles.

Service Support processes are concerned with operational /short term management cycles.

Products

There are numerous tools available that are viewed as conforming to ITIL guidelines. In other words, they have been developed to be consistent with IT Service Management procedures. However, while tools significantly help in the implementation and running of IT service provision they are by no means a solution in their own right:

“In order to support the ITIL processes several different types of tools are required, the one commonality in all of the tools is that they should be capable of providing a service level view of the environment.”

“...IT has to be able to provide a reliable, high quality service for an acceptable fee. This is not achieved through tools alone; any fool can implement a tool!”

From “A Fool with a Tool is Still a Fool” (Hewlett Packard White Paper – by Lindsay Parker)

Partners

In most organizations there are many groups providing each part of the overall service, with groups split across organizational boundaries and reporting lines. Service management processes include the management of the services from all contributors, irrespective of their function or reporting line. The third party supplier is encouraged to find and implement improvements, be responsive to customer needs and is discouraged from becoming complacent.

The Customer may not be aware that a part or all of the service they use is provided by a third party because the service, when controlled by good service management processes, is seamless.

IT Service Management

IT Service Management



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

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

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

IT Service Management comprises eleven disciplines, which are split into two core sets. These core sets are known as Service Delivery and Service Support. The IT Infrastructure Library contains manuals relating to each of the eleven disciplines. In practice, the eleven disciplines are so closely inter-related they should not be viewed in isolation. Implementation, therefore, is best seen as a phased, project-oriented introduction of one overall topic - IT Service Management.

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

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

Course Format

Course Format



- Brief lectures
- F1 Simulation or Practical assignments
- Example questions, mock examinations
- Formal ISEB/EXIN examination

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

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

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

IT Service Management Foundation Certificate

IT Service Management Foundation Certificate



- ISEB/EXIN IT Service Management Foundation certificate
- Multiple choice examination (1 hour)
- 65% required to pass (26 from 40)
- Pre-requisite for the Practitioner and Manager's certificates
- Keep your Foundation certificate and number
 - You'll be asked for it on Practitioner and Manager courses

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

The ISEB was formed in 1967 and currently functions under the auspices of the British Computer Society (BCS). The ISEB aims to provide industry-recognized qualifications that measure competence, ability and performance in many areas of IS, with the aim of raising industry standards, promoting career development and providing competitive edge for employers.

EXIN, the Dutch based IT examination provider is an independent organization establishing educational requirements, and developing and organizing examinations in the field of Information Technology. The goal of EXIN is to promote the quality of the ICT (Information Communication Technology) sector and the ICT professionals working in this sector by means of independent testing and certification.

Examination for the Foundation certificate in IT Service Management

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

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

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

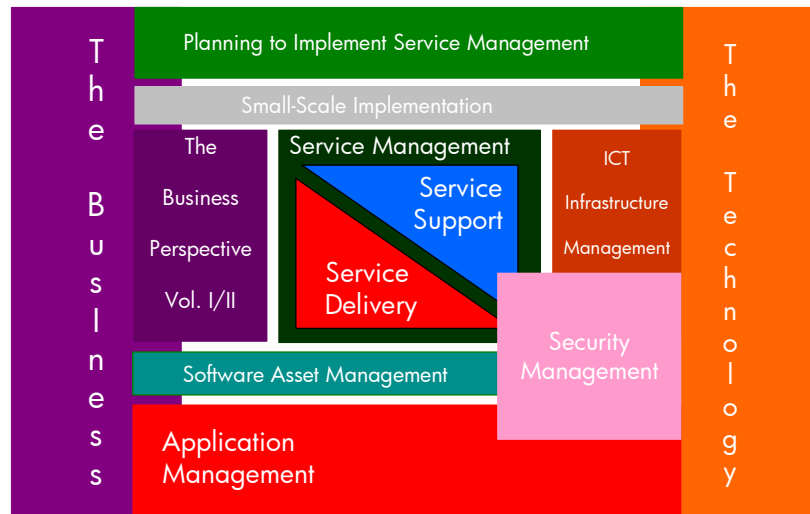
Possession of the Foundation certificate is an essential pre-requisite for those wishing to progress to the Manager's certificate in IT Service Management, or one of the Practitioner's certificates.

We recommend that, once you have passed the Foundation exam, you enter your Foundation Candidate Number in the space provided below as a backup plan (in case you file your original certificate away so securely you cannot find it).

My Foundation Candidate Number: _____

IT Infrastructure Library (ITIL)

IT Infrastructure Library (ITIL)



The IT Infrastructure Library was developed originally by the Central Computer and Telecommunications Agency (CCTA) as a set of comprehensive and inter-related codes of practice in achieving the efficient support and delivery of high quality, cost effective IT services. Renamed the Office of Government Commerce (OGC) they maintain the library and produce updates. The Stationery Office (UK) publishes the material.

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

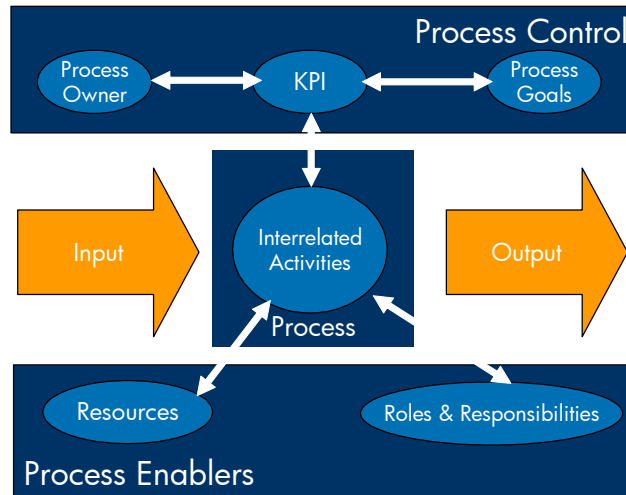
The itSMF (IT Service Management Forum) was set up to support and influence the IT Service Management industry. It has, through its very large membership, been influential in promoting industry best practice, and driving updates to ITIL.

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

- *The Business Perspective Vol. I/II* – describes many issues related to understanding and appreciating IT services an integrated aspect of managing a business. Sections include:
 - Business Continuity Management
 - Partnerships and outsourcing
 - Surviving changes
 - Adapting the business to radical change
 - Volume II shows how senior management can identify and then implement the right IT responses to a whole range of external factors - from legislation to the changing economic climate.
- *ICT Infrastructure Management* – IT Operations management issues e.g.:
 - Network Services management
 - Operations Management
 - Managing local processors
 - Computer Installation and acceptance
 - Systems management
 - Environmental Management
- *Application Management* – the software development lifecycle including:
 - Software lifecycle support
 - Testing an IT service for operational use
- *Security Management* – protecting the IT infrastructure against unauthorized use based on SLA requirements, contractual requirements, legislation, policy and a basic level of security.
- *Planning to Implement* - planning and implementing programs to optimize IT Service Management.
- *Software Asset Management* - This guide has been developed to assist with understanding what Software Asset Management (SAM) is and to explain what is required for it to perform effectively and efficiently, as identified in industry 'best practice'. This is a complementary guide to the core materials of the ITIL.
- *Small-Scale Implementation* - Adapted to provide sound processes for small organizations, this vital title will help any organization with a small resource base implement all the key elements of ITIL. At the same time, it will act as a starting point for larger organizations either those under budget constraints or those who have departmentalized ITIL implementations.

Process Management

Process Management



To understand the processes that constitute the IT Service Management portfolio, it is important to comprehend the fundamental theory of process management.

Every process has an input, an output plus a logical set of interrelated activities, which define what is required, what has to be done and an expected result.

In addition, a process control layer defines the goal(s) or objective(s) of the process as well as how the process will be measured relative to a desired outcome. These are represented by Key Performance Indicators or KPIs.

Finally, process enablers define the resources needed, such as people, tools and infrastructure, as well as the roles and responsibilities of individuals, groups or functions necessary to achieve the process goal(s).

ITIL Philosophy

ITIL Philosophy



- Capture industry “best practice”
- Framework not a methodology
- Organizations should adopt and adapt
- Not standards!
 - BS 15000
 - ISO/IEC 20000
- Scalable — organization size and need
- Platform independent

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

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

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

While ITIL itself is not a Standard, there are currently moves underway to develop a set of worldwide standards based upon an organizations implementation of the ITIL framework. While BS15000 was the first standard for ITSM, today ISO/IEC 20000 has superseded BS15000 as the international published standard for ITSM (and as such have been adopted in many countries).

The ITIL disciplines can be used by any type and size of organization. The most current books (published 2000-2001) have incorporated decentralized processing as well as other changes in organizational and delivery methods. There is currently an exercise underway to further update the books.

Best Practice — A Working Definition



Best Practice — A Working Definition

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

Best Practice is based on:

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

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

Best practice is based on:

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

The characteristics and benefits of a best practice approach are:

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

The Drivers for High Quality IT Services



The Drivers for High Quality IT Services

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

- Increased dependency on IT

Most organizations could not function as a business without acceptable levels of IT service availability and reliability.

- Higher visibility of service failures

If things do go wrong, the impact on the business is more likely to be noticed quickly.

- More exacting User requirements

A general increase in computer literacy, particularly amongst customers, has led to a higher expectation of what is required from IT services, and a reduction in their level of tolerance of faults and failures in the IT services.

- Increased complexity of the IT infrastructure

IT services are delivered by a complex mix of hardware, software, networks and people. It is essential that all these components are managed effectively and efficiently as poor performance of any one component can seriously affect the quality of the overall IT service.

- Charging and competition

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

- Legislative/regulatory drivers

Many organizations are required by either legal or industry regulations to follow certain practices, or achieve/have certain goals or certification. ITIL can (in conjunction with other practices) enable an organization to achieve/prove that these targets have been met.

ITIL Objectives



ITIL Objectives

- Reduce *Costs*
- Improve *Availability*
- Tune *Capacity*
- Increase *Throughput*
- Optimize resource *Utilization*
- Improve *Scalability*
- High quality achieved through:
 - Service Improvement Program – SIP (using Project Management methodologies such as PMI, PRINCE2)
 - Service Culture
 - Supporting Disciplines

The objectives of ITIL are to:

- Reduce costs
 - Although this may be a longer term effect, as there may be an initial increase in expenditure in the short term
- Improve availability
 - Enable the business to have IT systems functioning for more of the agreed time
- Tune capacity
 - Over provision is expensive and under provision causes performance problems
- Increase throughput
 - There are two ways in which to grow a business; through expansion or by doing more with the same resources
- Optimize resource utilization
 - Resources represent a cost to the business. Optimized usage by the IT service provider will ensure that the business benefits gained from the cost-effective utilization of those resources are maximized.

- Improve scalability
 - The size of an organization is an important factor when implementing ITIL processes. In a small organization, many of the roles defined may well be the responsibility of one person. Conversely, a large organization is able to allocate individual processes to specialist groups composed of people with specialist skills.

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

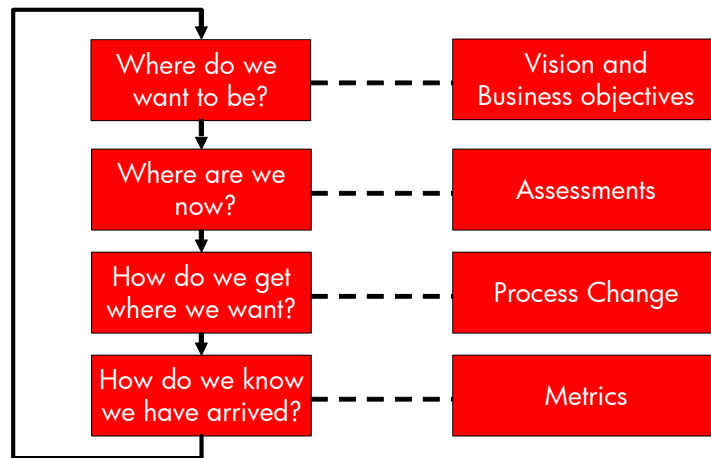
These are:

1. The use of Service Improvement Programs – (SIP), using a Project Management methodology, which covers the management, control and organization of a project, helping to better achieve the objectives of a SIP. The most accepted methodologies for Project Management are:
 - PMI, the **P**roject **M**anagement **I**nstitute, based in the United States
 - PRINCE2 - **P**rojects **i**n **C**ontrolled **E**nvironments 2, based in the United Kingdom and owned by the Office of Government Commerce (OGC)
2. The existence of a Service Culture within IT (and the rest of the organization)
3. The implementation of ITIL disciplines

Continuous Improvement

Continuous Improvement

A process-led approach



Note: EXIN makes reference to Deming

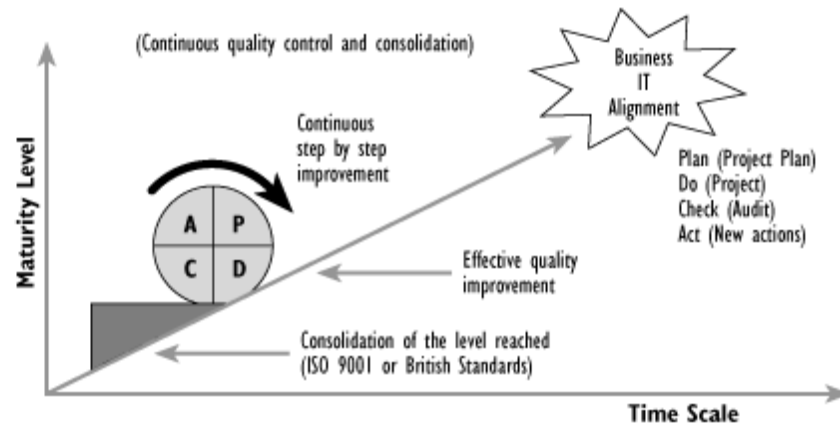
The cycle of continuous improvement begins with the establishment of an organization's (or service provider's) vision and business objectives. The level of service currently provided is then assessed. This work is completed before embarking on process change (such as ITIL implementation). Metrics should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

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

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

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

Deming's Quality Circle:



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

Service Culture

Service Culture



- Recognition that IT only exists to underpin the business of the organization
- A corporate IT mission to deliver agreed levels of service
- A willingness to go that 'extra step' to satisfy Customer needs
- An understanding of the Customers' perspective
- Achieving a Service Culture depends on:
 - Senior management support
 - A good understanding of why IT services are being provided
 - An understanding of the impact on the business of poor service
 - Clear targets to aim for, and from which to progress

A service culture must spring from:

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

Achieving a Service Culture

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

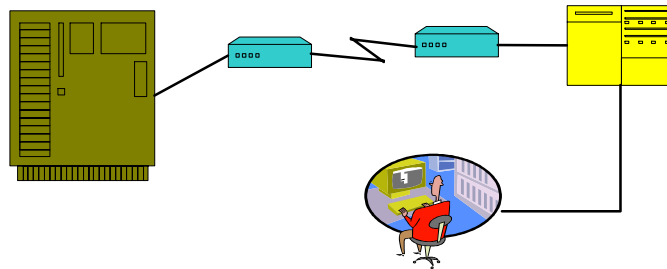
To achieve a service culture, there must be whole-hearted support from the senior management of the organization, and all levels of management and staff must understand why the IT services are provided and the impact on the business of poor service. An organization dedicated to achieving a service culture will have distinct service performance targets for which to aim, and a clear vision of how it will continue to achieve improving levels of service in the future.

What Is an IT Service?



What Is an IT Service?

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

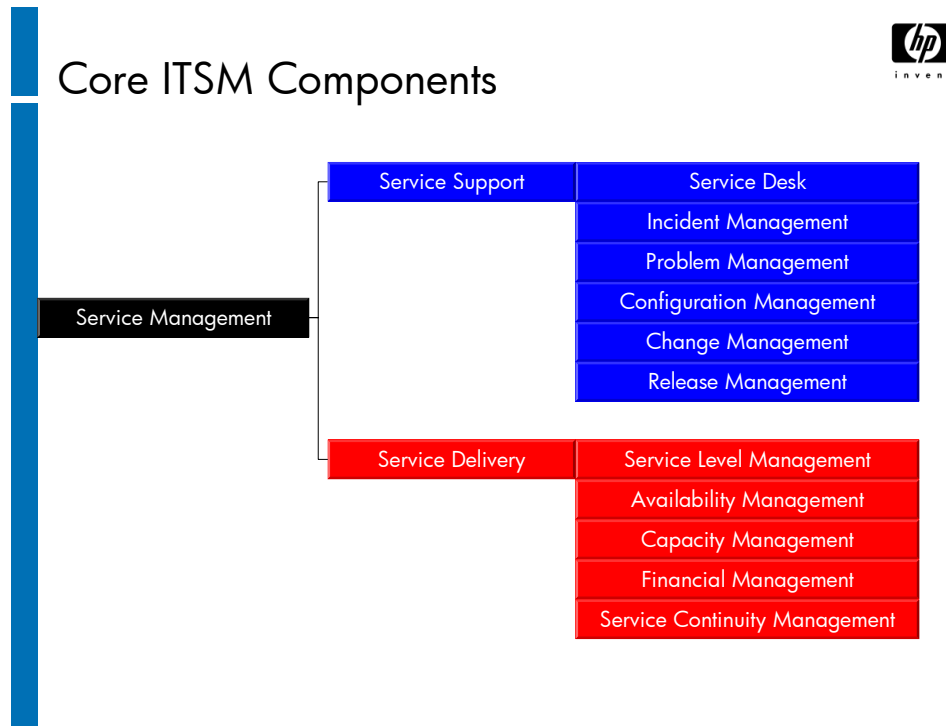


IT Service Management views the IT facilities offered by an IT department as “services”.

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

As IT staff know, there are often many components which make up the overall service delivered to the Customer/User. However, the Customer’s/Users only impression of the quality of the IT services they receive is that which is delivered to their workstation or peripheral device. A failure, no matter where it occurs, or how minor the component, is visible to the Customer/User if it disrupts the delivery of the end-to-end service.

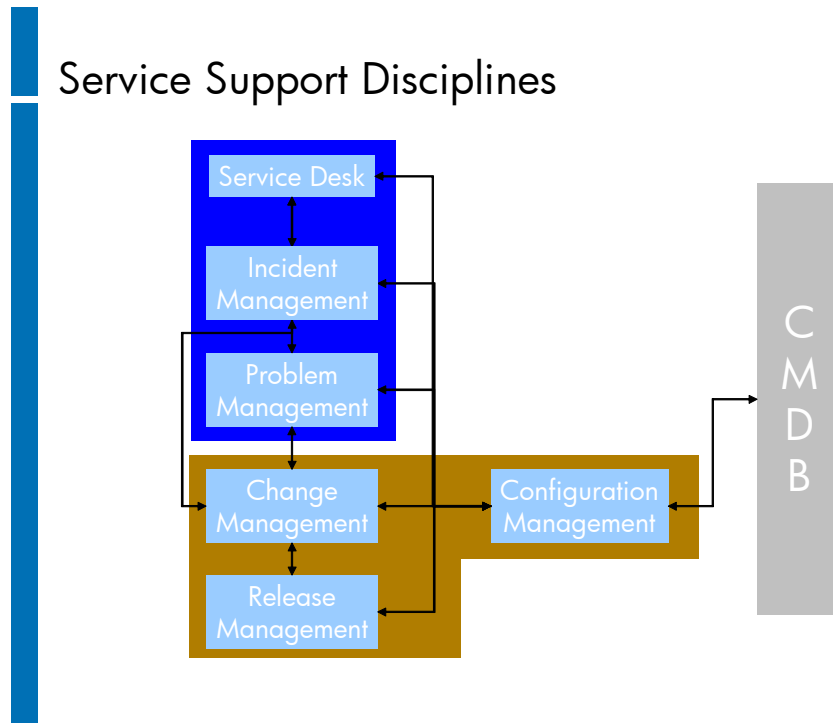
Core ITSM Components



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

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

Service Support Disciplines



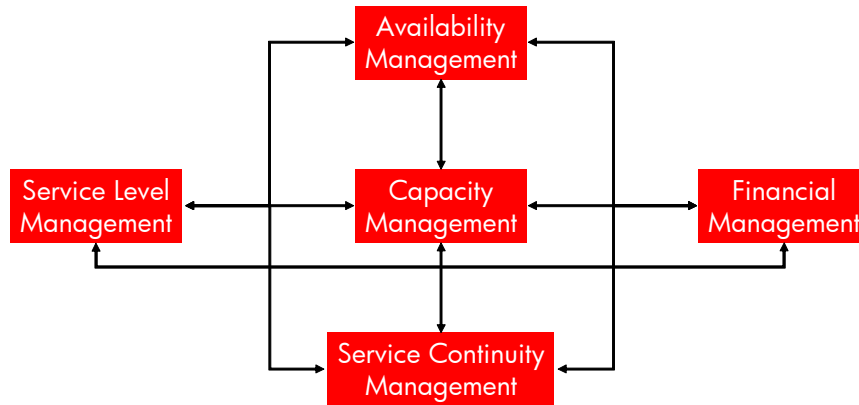
Configuration Management, which is responsible for the Configuration Management Database (CMDB) is the key ITIL discipline, and underpins all other disciplines.

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

All disciplines are considered processes, but Service Desk, which is a function.

Service Delivery Processes

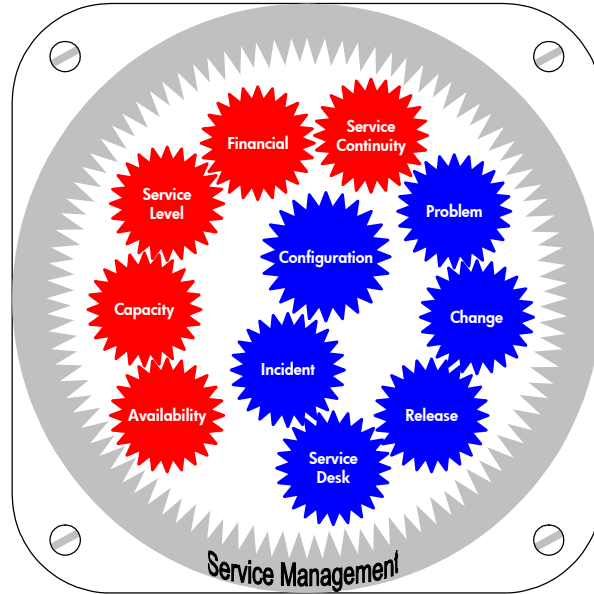
Service Delivery Processes



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

Service Management

Service Management



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

Service Desk

Module 2

Mission of Service Desk

Mission of Service Desk



- To act as the **central (Single) point of contact** between the User and IT Service Provider.
- To handle Incidents and **Requests**, and provide an **interface for other activities** such as Change, Problem, Configuration, Release, Service Level and IT Service Continuity Management.

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

The service desk is the main access point into most of the ITIL processes.

Service Desk supports the mission statement by

- Logging the incident
- Categorizing, diagnosing and prioritizing incidents
- Attempting an initial resolution
- Escalating to the appropriate resolver group when resolution cannot be achieved by the Service Desk
- Controlling further escalations as required
- Maintaining ownership and control of all incidents making sure that none are "lost"
- Maintaining information about the incident to aid current and future resolutions
- Closing all incidents following Incident Management practices

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

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

Objectives of Service Desk



Objectives of Service Desk

- To be the single point of contact for all IT Customers/Users
- To restore service whenever possible
- To maximize service availability
- To manage all incidents to a closure
- To be aware of business needs
- To be aware of the impact of failure upon the business
- To provide business systems support
 - Complaints
 - Queries (IT and non-IT)
 - Handling Change Requests

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

- At an operational level, its objective is to provide a SPOC (Single Point Of Contact) to provide advice, guidance and the rapid restoration of normal services to its Customers and Users.
- The service desk makes an initial diagnosis of the incident and attempts, where possible, to restore service using a variety of tools and techniques (e.g. Knowledge bases, Known Error DataBase (KEDB) etc.).
- Maximizing service availability is achieved by making sure that incidents are resolved and the User is back up and working as quickly as possible. This will be achieved through monitoring, tracking and prompt escalation of incidents.
- The service desk manages ALL incidents to closure. This is the control function of the Service Desk in managing, monitoring and tracking all incidents to make sure none are lost or forgotten about. It is also referring to the fact that ALL incidents are logged – no exceptions!

- Be aware of the business need and impact of failure upon the business – this is a key difference between a Service Desk and a Call Centre/Help Desk. The Service Desk needs an appreciation of what effect the incident has on the business as a whole, not just on the individual who has reported the incident. This appreciation and understanding is required to correctly categorize and prioritize the incident to reduce any negative business impact associated with that incident. (For example, assigning appropriate severity/priority and escalation times.
- Business System Support - The ability (if required) to provide a contact and control point (SPOC) for critical non-IT systems e.g. ATM machines in a bank environment.

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

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

All three organizations share these characteristics:

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

Common Features and Characteristics (1 of 2)

Common Features and Characteristics (1 of 2)



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

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

These features and characteristics are usually integrated into a single “Service Management” tool such as HP OpenView, Remedy, Touchpaper, Assyst etc.

These service management tools also provide a single database into which all incidents can be logged and then monitored and tracked throughout their lifecycle. These tools facilitate a central repository of information about incidents that is usually available to both the Service Desk and other resolving groups, with the addition of some form of “knowledge base” providing access to diagnostic aids and scripts. A common feature within each tool set is an impact coding system. An impact code is assigned to each incident to assist decision-making surrounding the impact upon the business and the urgency required for a resolution to be assessed and acted upon accordingly.

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

Common Features and Characteristics (2 of 2)

Common Features and Characteristics (2 of 2)



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

- Communication with support staff – monitoring of the incident, escalation between and within resolver groups and the liaison role between the User and the resolver groups as required.
- Interface to SLAs – escalation according to rules laid down within the SLA (functional and hierarchical), also monitoring and communications about breaches or potential breaches. In addition lots of management information to do with performance against the SLA is derived from Service Desk metrics.
- Regular progress reporting – liaison with the Users on incident resolution progress can either be reactive or proactive.
- Classification of incident at call opening and closure - The opening category is the Service Desk's "best guess", at this initial stage, of the description of the incident; this helps them identify the correct resolver group to route the incident to, as well as giving Problem Management an indication of how an incident "appears" at first glance. The closure category is based on the "real" reason behind the occurrence of the incident, and not just on the "suspected" reason when the incident was logged. This is useful information for Problem Management.

- Management summaries – management information derived from Service Desk metrics are used by nearly all the other ITIL disciplines to gauge performance against targets and as input for management decision making.
- Operational systems access – password resets, and allocation etc (where applicable and appropriate).

Staffing Options



Staffing Options

- Minimum qualifications
 - Interpersonal skills
 - Business understanding
 - IT understanding
- Skill sets
 - Customer emphasis
 - Technical emphasis
 - Expert
- Staff resourcing
 - Correct numbers and profile

- Minimum Qualifications – The Service Desk agents need the three qualities as a minimum; they do not have to be experts, but do have to have good Customer handling skills and an appreciation of the business in order to work effectively.
- The skill level in IT will determine the level of first time fix that is available via the Service Desk. This may be an important factor to you and hence a high degree of technical knowledge is required in order to promote a high first time fix. In other situations technical knowledge may not be as high a requirement as is another skill, e.g. languages.
- Staff resourcing – having the correct people available when you need them and in the right numbers, e.g. shift patterns/requirements, numbers on each shift (more during the day and fewer at night), correct skills e.g. technical vs. Customer vs. language skills etc. for a multinational support organization.

Skills and Mindset



Skills and Mindset

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

- Teamwork – Internally and with resolver groups.
- Understanding Users' perspective – Realizing that they are angry at the situation and not with you personally; understanding their perspective.
- Professionalism – Do not get angry or lose your temper. Be assertive not aggressive.
- First impressions count – Strive to immediately come across as professional and helpful as you take the call. Your initial tone can help to set the tone for the rest of the conversation.
- Accept ownership – It's now "your" incident as well. Look to get it resolved quickly and efficiently.
- Use Customer terminology – Don't use internal IT jargon where possible. Use the everyday business language used in your organization. Don't set out to deliberately confuse or hide behind technical explanations.
- Assume Users' perspective – Understand what this incident means for them personally.
- Active listening – Give positive reinforcement and feedback signals (i.e. visually = eye contact and nodding etc. Verbally = "yes", "I see", "Can I just re-phrase that" etc.).

Service Desk Implementation



Service Desk Implementation

- Target effectiveness metrics:
 - Key performance Indicators (KPIs) e.g.
 - Work effort: Number of calls logged, Incidents processed per Service Desk workstation
 - Effectiveness/Efficiency: Average Speed of Answer (ASA), % first time fix, number of incidents correctly categorized at initial logging
 - Selecting the correct structure:
 - Local Service Desk
 - Central Service Desk
 - Virtual Service Desk
-
- Target Effectiveness Metrics (KPIs – Key Performance Indicator) – being able to gauge how efficiently and/or effectively you are working. Metrics can show the “workload” e.g. number of calls logged (which is outside the control of the Service Desk), incidents processed per Service Desk workstation, etc. Other metrics show the effectiveness or efficiency of a Service Desk, e.g. Average Speed of Answer (ASA), percentage of incidents handled within agreed response time in the first call, number of incidents correctly categorized at initial logging, etc. which is within their control.
 - Correct Structure – There are three different types of Service Desk which are explained in more detail in later slides.

Local Service Desks



Local Service Desks



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

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

Central Service Desk



Central Service Desk

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

Can be used to support multinational operations

- Enables economies of scale to be applied, with management overview on a central point rather than on a distributed organization.
- Small local Service Desks can be backed up by a central Service Desk (e.g. specialist application only used in one particular location is supported by a local Service Desk, whereas all the other IT is supported by the central Service Desk)

Virtual Service Desk

Virtual Service Desk



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

Tends to be used by very large multinational companies

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

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

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

Workload partitioning - For the virtual desk, the support tools in place should allow for 'workload partitioning' and 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. (From ITIL Service Support book)

'Follow the Sun' Option



'Follow the Sun' Option

- Not a type of Service Desk but an option usually applied to two or more Central Service Desks for global operations
- Where Service Desk support switches between two or more desks to provide 24 hr global cover.
- Telephony switching needed
- Multilingual staff usually required
- Local conditions and cultural issues need to be considered
- Clear escalation channels needed



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

- Usually used by multinational organizations using 3 central Service Desks to give 24/7 global support. The central Service Desks are only operational during "office hours" within their own time zone (e.g. London desk(UK) hands over to Chicago Service Desk(US) , which hands over to the Sydney Service Desk (Australia).
- Telephony switching required to make sure that at 5pm UK time when the London desk shuts down then all calls are then answered by the Chicago Service Desk etc)
- Multi-lingual staff usually required to handle the "out of hours" support calls from different parts of the globe (E.g. Spanish speaker is useful on UK Service Desk to handle Spanish (in same time zone) and Latin American (out of hours) calls).
- Local conditions and cultural issues need to be considered – Cultural differences should not be taken for granted e.g. in some cultures it is not easily accepted for a man to take orders from a woman, In most case engineers (males) are told "what to do" by Service Desk personnel (quite often these are women). Also don't think you always understand what is being said to you – "America and Britain, two nations divided by a common language" etc.
- Clear escalation channels required – to whom do you escalate and where are they?

A Self-Service Strategy



A Self-Service Strategy

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

From the ITIL Service Support book –

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

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

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

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

- Growth of Internet and Intranet has made this possible. Quite a few Service Management tools have a web front-end access or client.
- Can be used to do some self-help and diagnostic work by the User and log a call if this fails. Also used a lot to enable user to self-track progress rather than contacting Service Desk. Can be used to divert away from Service Desk analysts low priority or non-incident calls, giving the analyst more time and focus on higher priority calls.
- Need to be aware of the potential to actually “double” your calls if the system fails or is not “user-friendly”. E.g. log the call to say the web front end is not working, and then log the call the user was going to log via the web!

Outsourcing the Service Desk



Outsourcing the Service Desk

Potential Benefits

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

Care Needed

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

Potential Benefits

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

Care Needed

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

Service Desk Questions: Responsibilities



Service Desk Responsibilities

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

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

Service Desk Questions: Functions



Service Desk Functions

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

- A. A single point of contact between the Customers/Users and the IT department
- B. First-line Incident Management
- C. Business system support
- D. Management of the known error database

The Function of the Service Desk

- **A single point of contact between customers and the IT department** - The Service Desk forms the main day-to-day point of contact between the IT service provider and its Customers. It is therefore essential that the staff, the processes and the tools employed reflect the importance of the role. The Service Desk is also a useful means for the IT service provider to disseminate information into the customer domains.
- **First-line incident support and control** - Incident control is actually the first stage in an overall problem management system (which is discussed in the next section), although it is the Service Desk which has direct responsibility for recording and progressing incidents. Depending on the skills available at the Service Desk and the nature of the incident, the Service Desk may be responsible for carrying out an initial diagnosis of the incident. The Service Desk must have the support of other technical domains within the IT organization as incidents may have to be referred to them for further investigation. The Service Desk retains the responsibility for monitoring the progress of incidents.

- **Business system support** - Ideally, the Service Desk will handle not only technical incidents but also requests from customers who have difficulties or queries about business processes, for example a service extension request. Business process support requests will normally be recorded, and then referred to the appropriate domain without going through the full diagnostic and resolution process.
- **A central source of management information** - Accurately recorded incidents form a huge source of valuable management information which, over time, can be used to highlight trends and identify weak components for corrective action thus improving IT service quality.

Incident Management

Module 3

Mission of Incident Management

Mission of Incident Management



To **restore normal service operation as quickly as possible** with minimum disruption to the business, thus ensuring the best possible levels of service and availability are maintained.

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

Objectives of Incident Management

Objectives of Incident Management



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

- To log and track ALL incidents
 - Via Service Desk
- To maintain meaningful records
- To deal with incidents consistently

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

Scope of Incident Management



Scope of Incident Management

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

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

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

Definition — An Incident



Definition — An Incident



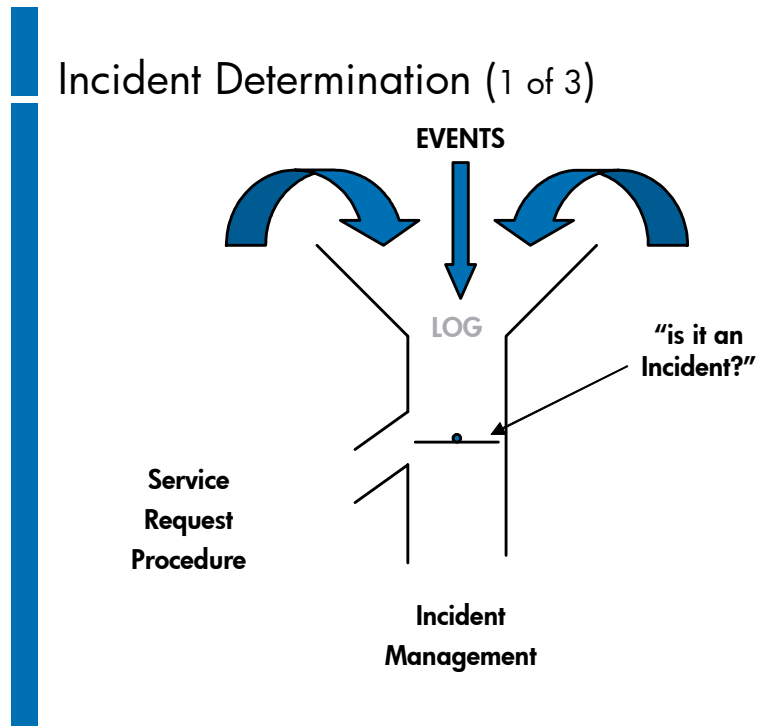
“An **incident** is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service”

The ITIL definition of an incident as shown in the ITIL Service Support (Blue) book.

Note

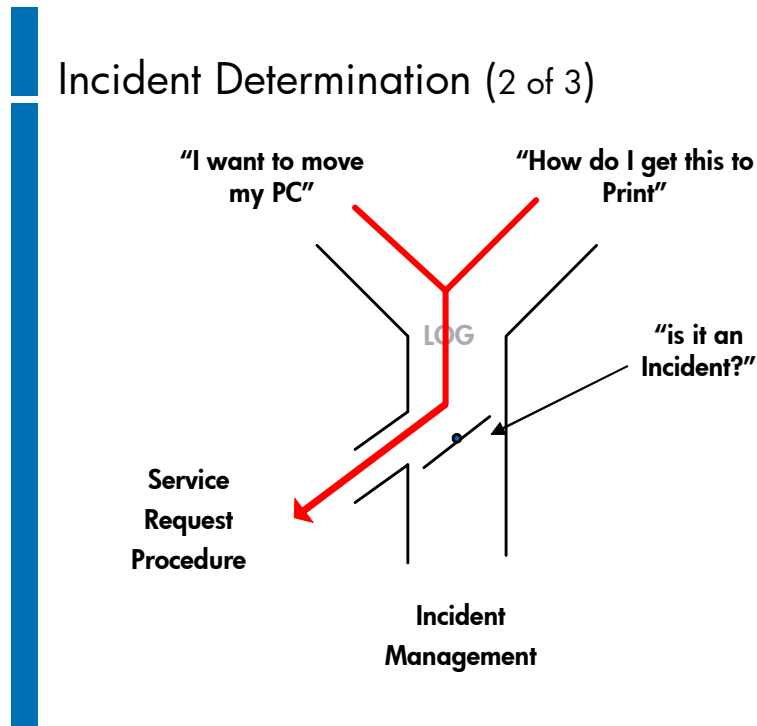
This includes events that have caused or may cause impact to a service (i.e. events that have the potential to impact a service).

Incident Determination (1 of 3)



In the first place, to determine whether an event in the live environment is an "incident" or not, we have to "capture" that event. Incident Management is responsible for this taking place. As that event is captured it has to be logged to make sure we keep a record of future actions on this event. This is to ensure the correct procedure is being followed, that the event is not "lost" in the system and that it can be monitored and tracked to closure. We should also use the logged incident history to help with future resolutions. Once logged, the event passes through a test to see if it should continue to be handled by the rest of the Incident Management process or by the Service Request procedure.

Incident Determination (2 of 3)

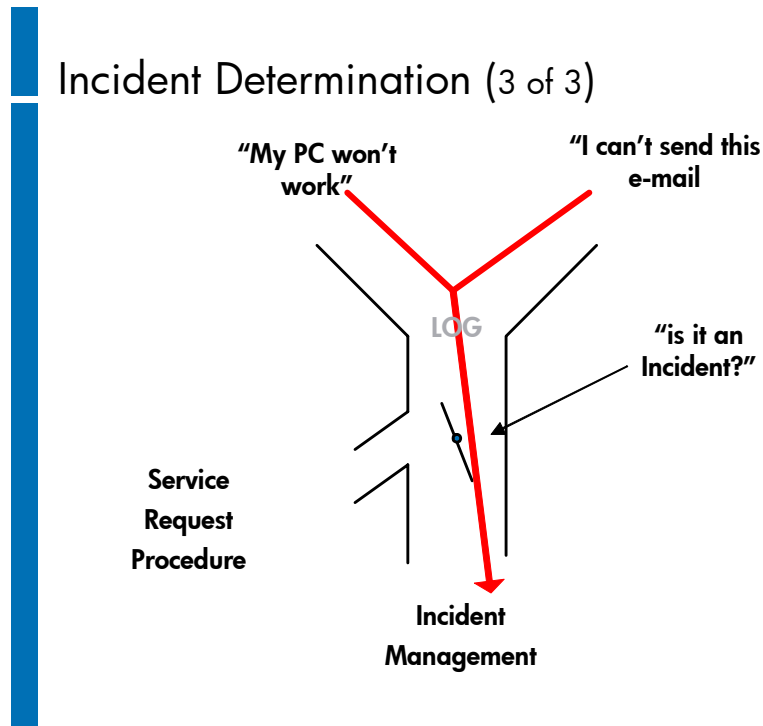


The test applied is whether the event fulfils the definition of an “incident”. An incident is loosely an event that is an “error” in the provision of the service. If the event is not some sort of “error” (see the examples above), then the Incident Management process passes off the event to a Service Request procedure. Under ITIL a “Service Request procedure” is a generic term for a procedure to enable a “service” to be provided to the User, this may be providing basic information or even accessing one of the Other ITIL procedures (e.g. Change Management to move a PC, or Service Level Management to request an extension of hours etc). In most cases this other procedure will still be initiated and may be fully handled by the Service Desk.

Note

A Service Request is defined as an Incident not being a failure in the IT Infrastructure.

Incident Determination (3 of 3)



Where the event can be classed as an "incident" then the Service Desk/Incident Management will continue to follow the Incident Management procedure as set out in the rest of this section.

Definition — A Problem

Definition — A Problem



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

The ITIL Book definition of a problem

Note

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

Definition — A Known Error



Definition — A Known Error

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

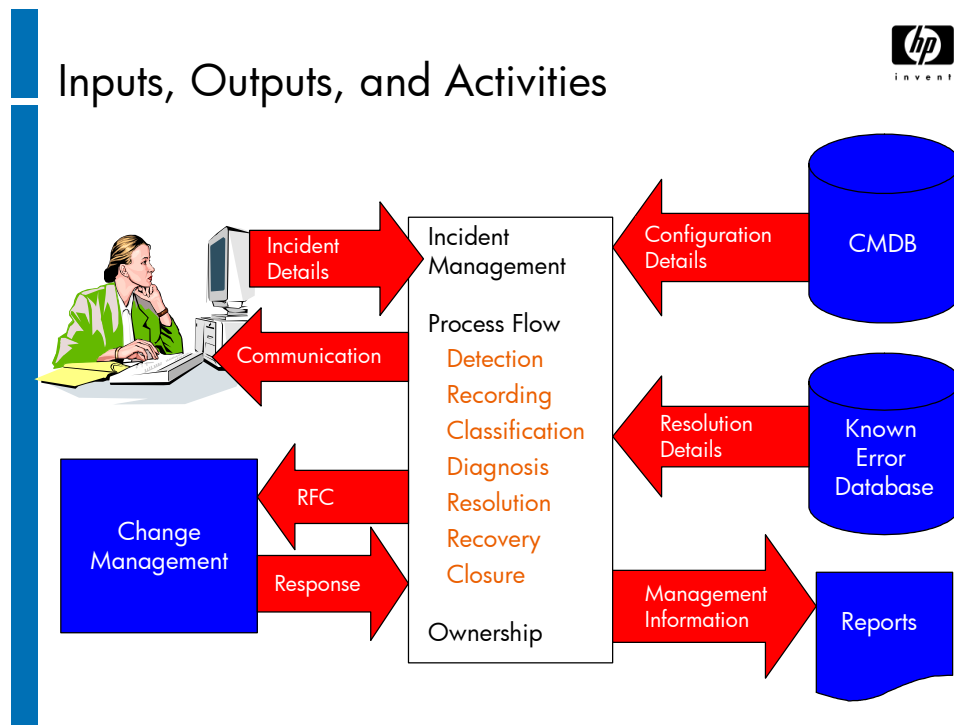
If a business case exists, a Request For Change (RFC) will be raised, but, in any event it remains a known error unless it is permanently fixed by a change.”

The ITIL Book definition of a known error

Note

Known errors are the responsibility of Problem Management not Incident Management. The reason we discuss it here is due to the relationship between known errors and incidents especially with regard to workarounds.

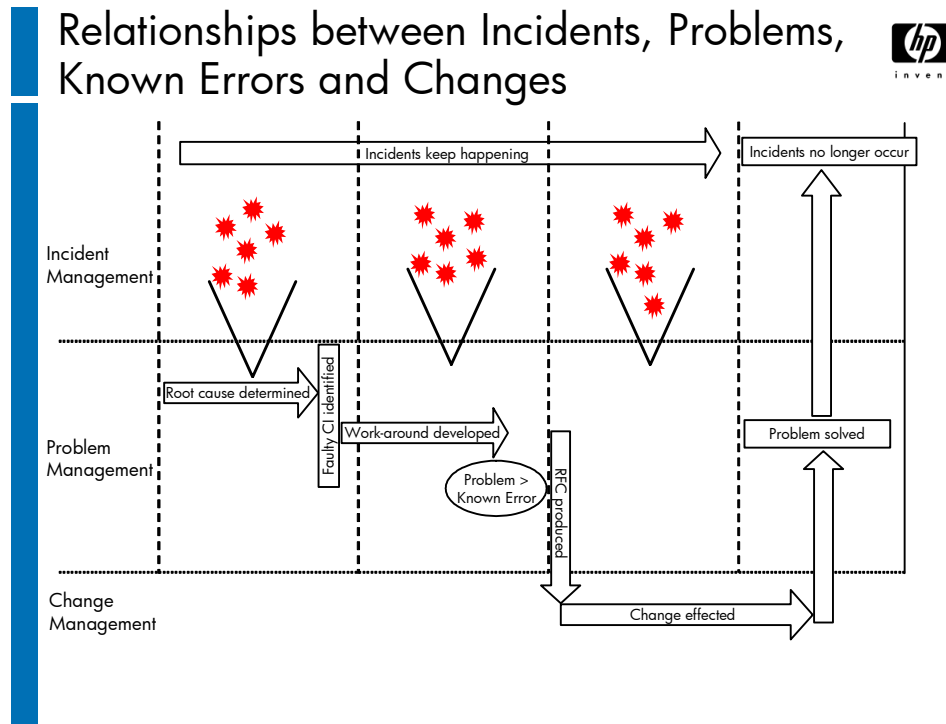
Inputs, Outputs, and Activities



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

- The central column shows the stages/phases that are gone through during the incident resolution process.
 - a. Detection – actually identifying that an incident is taking place, this can either be by a User(s) or from automatic detection tools (e.g. HP Openview, etc.)
 - b. Recording – the actual logging of the incident
 - c. Classification – assigning a “type” to the incident to aid with both the functional escalation (i.e. deciding who to send the incident to in the first place if it cannot be resolved at first line), and for later Problem Management analysis.
 - d. Diagnosis – finding out the cause of the incident and identifying a resolution/workaround.
 - e. Resolution – applying the resolution/workaround
 - f. Recovery – bringing the CI back to operational status and restoring it to the user (i.e. reloading data, applications etc)
 - g. Closure – closing the incident (done by Service Desk Analysts), usually after confirming contact with the User to make sure they are now back up and working OK
 - h. Ownership – This is in effect all the way through the lifecycle and ensures that the incident is not lost, unduly delayed, forgotten about etc. It also means the owner of the incident should monitor it, track its progress and establish a permanent line of communication with the User who requested the incident to be opened.

Relationships between Incidents, Problems, Known Errors and Changes



Note

An incident never "evolves" into a problem. It always remains an incident – there is only ever a relationship between incident and problem! A problem, however, may "evolve" to a known error once the root cause is found and a workaround is developed.

This slide shows the relationship between incidents and problems. Incidents NEVER become problems, they remain as incidents.

As an example: Fifteen reported incidents indicate that Users cannot access e-mail. Upon investigation, fourteen of the reported incidents are found to be related to an identified problem that a server is down. However, the fifteenth incident, which appears to have identical characteristics to the other fourteen incidents, is found to have occurred because Outlook has been corrupted; thus highlighting the difference between an incident (symptom or effect) and a problem (underlying cause).

The slide shows that incidents will keep happening and will be handled by the Incident Management process, while Problem Management should identify the root cause, develop a workaround and through Change Management, establish a permanent fix for the problem (after the permanent fix is applied, incidents will stop happening).

Example Coding System for Incident/Request Classification

Example Coding System for Incident/Request Classification



| Type of Incident | Main Category | Sub-Category | Indication Priority |
|------------------|----------------|----------------------|---------------------|
| Incident | Software | Word processing | 2 |
| | | Spreadsheet | 2 |
| | | Business Application | 1 |
| | Hardware | Mainframe | 1 |
| | | Work Station | 2 |
| | Etc..... | | |
| Service Request | Password Reset | | 1 |
| | Change Toner | | 3 |
| | Help User | Office Software | 3 |
| | Etc..... | Business Application | 2 |

Taken from the ITIL book.

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

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

Impact + Urgency = Priority



Impact + Urgency = Priority

Impact

- Effect on the business
- Defined in the SLA

Urgency

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

Priority

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

The priority of an incident is based on its Impact on the business and the urgency for which a resolution is required.

Further explanation is required for the last statement on this slide

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

Example of a Priority Coding System

Example of a Priority Coding System



| Urgency | Impact | | | |
|---------|--------|------|--------|-----|
| | | High | Medium | Low |
| | High | 1 | 2 | 3 |
| | Medium | 2 | 3 | 4 |
| | Low | 3 | 4 | 5 |

| Priority Code | Description | Target Resolution Time |
|----------------------|--------------------|-------------------------------|
| 1 | Critical | 1 hour |
| 2 | High | 8 hours |
| 3 | Medium | 24 hours |
| 4 | Low | 48 hours |
| 5 | Planning | As planned |

Taken from the ITIL Book

In addition to the above information (usually found in the Service Level Agreement), most organizations include a generic description of what a Priority 1 Critical incident means to them etc. This is meant to give Service Desk staff a guideline of how to prioritize incidents as they come in.

Incident Status — Examples

Incident Status — Examples



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

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

Escalation

Escalation



- Appropriate number and level of resources
- To resolve incidents within the agreed time
- Defined in conjunction with other areas
- Executed by the Service Desk
- Inform the User of the status
- Automatic

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

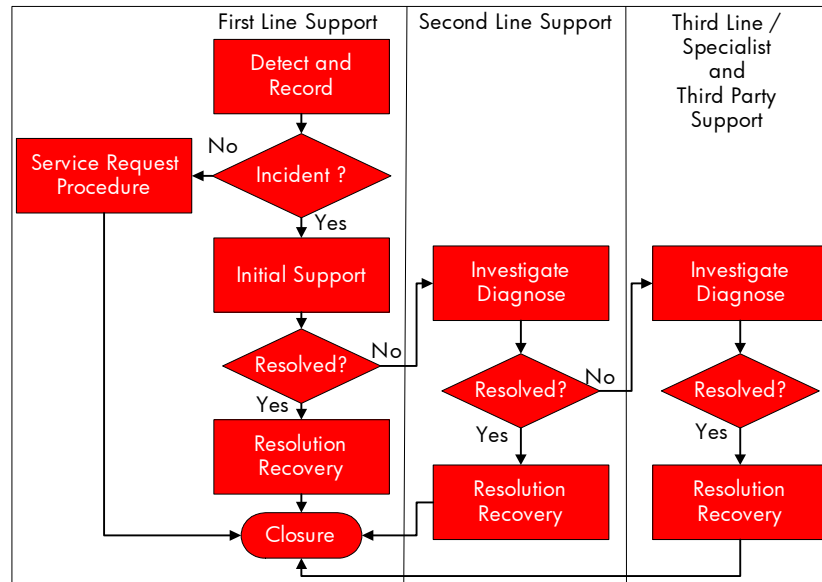
Note

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

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

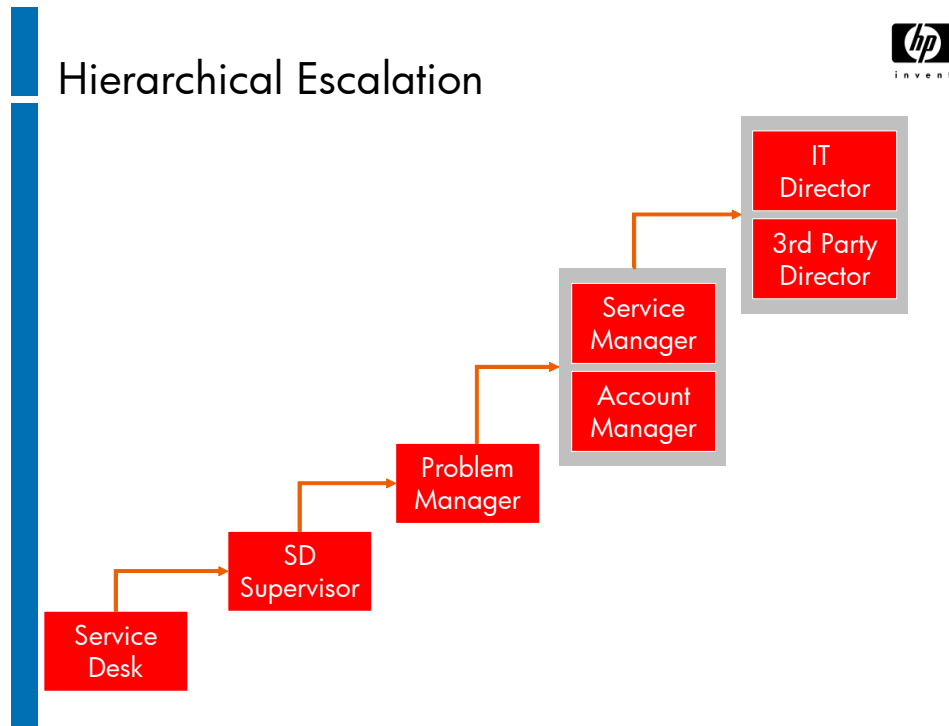
Functional Escalation

Functional Escalation



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

Hierarchical Escalation



This is an example of a Hierarchical escalation path.

Note

This is an example and should not be taken to imply that the Problem Manager is ALWAYS in the escalation chain

You must be aware that there is a separate hierarchical escalation occurring in parallel to this, i.e. the one inside the Customer/Business. It would be a good idea to make sure that IT escalation is occurring BEFORE that in the Customer organization.

Incident Manager Responsibilities



Incident Manager Responsibilities

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

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

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

Service Desk/First Line Responsibilities

Service Desk/First Line Responsibilities



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

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

Second Line/Third Line Support Staff Responsibilities

Second Line/Third Line Support Staff Responsibilities



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

These are the responsibilities of the Second and Third line staff when using the Incident Management process.

Benefit of Incident Management

Benefit of Incident Management



Which one of the following is NOT necessarily a direct benefit of implementing a formal Incident Management process?

- A. Improved User satisfaction
- B. Incident volume reduction
- C. Elimination of lost incidents
- D. Less disruption to both IT support staff and Users

Incident Management Elements



Incident Management Elements

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

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

Problem Management

Module 4

Mission of Problem Management

Mission of Problem Management



To **minimize the adverse effect** on the business of incidents and problems caused by errors in the infrastructure, and to **proactively prevent the occurrence** of incidents, problems, and errors

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

Scope/Objectives of Problem Management

Scope/Objectives of Problem Management



- Identify and resolve IT problems that affect IT services
 - To minimize the impact of problems and incidents
- Recurring incident/problem prevention
- Pro-active problem Management
 - To reduce the overall number of IT incidents
- To ensure that the right level and number of resources are resolving specific problems
- Assist with major incidents, if required
- Entry to IT Service Continuity Management
- Maintaining relationships with third party suppliers
 - Including ensuring vendors comply with their contracts

- Identify and resolve IT problems that affect IT services. This is usually as a result of multiple or service impacting incidents.
- Problem Management is responsible for investigating the root cause of problems. By focusing on recurring incidents/problems they can provide workarounds and develop permanent fixes that prevent disruption to the business caused by such recurrences.
- Pro-active Problem Management – actually trying to find and alleviate problems either before they occur or at least in the early stages of a wide outbreak, and proactively applying the workaround to prevent the problem occurring elsewhere.
- Resources – Problem Management is responsible for allocating and managing the appropriate resources needed to resolve specific problems in a timely manner.
- Major incidents (extremely high impact on the business), if required. The Problem Manager is a likely candidate to become involved in major/high priority incidents at an early stage due to the tools and techniques they can bring to bear on the incident.

- Entry to ITSCM (IT Service Continuity Management) – this is one possible entry route (although a likely one for technically driven invocations of the IT Service Continuity Plan)
- Maintaining relationships with 3rd Party Suppliers – During the resolution of a problem involving 3rd party equipment or technicians, the Problem Manager is responsible for the management of those people and liaison with the 3rd party vendor organization.

Note

Including ensuring that vendors comply with their contracts

– Here we are talking specifically about where a vendor's non-compliance is causing problems to occur in the IT infrastructure. This is generally a Service Level Management issue from a day to day/operational point of view.

Key Definitions (Refresher)



Key Definitions (Refresher)

- Incident
 - “An incident is any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service”
- Problem
 - “A problem is the unknown underlying cause of one or more incidents”
- Known Error
 - “A known error is an incident or problem for which the root cause is known and for which a temporary workaround or permanent alternative has been identified. If a business case exists, an RFC will be raised, but, in any event, it remains a known error unless it is permanently fixed by a Change.”

These are definitions that are key to understanding ITIL principles.

It would be beneficial to memorize these definitions both as foundations for ITIL as well as to assist in decision making. Knowing these definitions will also be useful as you take the Foundation certification exam.

Incident Management and Problem Management

Incident Management and Problem Management



Incident Management

- Restores agreed levels of services
- Uses workarounds

Problem Management

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

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

ITIL recommends that you do not make your Incident Manager your Problem Manager as well due to the potential inherent conflict between the two roles. The former focuses on rapidly restoring the services, the latter on performing root cause analysis to find permanent solutions to problems.

Problem Control



Problem Control

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

This slide shows the stages that are present during Problem Control

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

Error Control




Error Control

- Identify and record errors
- Assess error
- Record error resolution
- Monitor resolution
- Close error (Change Management)

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

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

Known Errors — Development



Known Errors — Development

- Sometimes a system might be allowed to be released into the live environment even though known errors have been detected during testing.
- Problem Management needs to ensure any such known errors, and any resolutions, are recorded in the known error database.

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

Problem Management Responsibilities



Problem Management Responsibilities

Problem Management must ensure:

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

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

Proactive Problem Management



Proactive Problem Management

Proactive Problem Management covers the activities aimed at identifying and resolving problems before incidents occur.

These activities are:

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

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

Problem Management Techniques



Problem Management Techniques

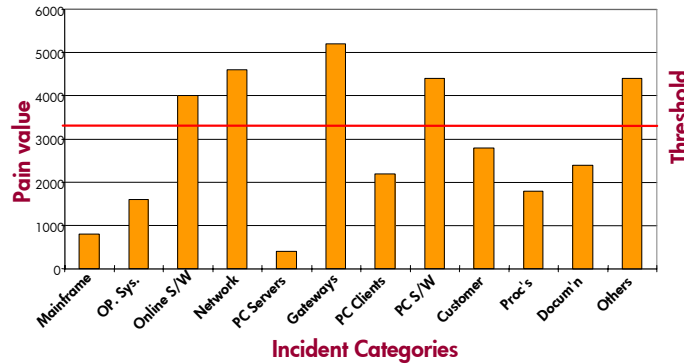
- Pain Value Analysis (PVA)
- Ishikawa Diagrams
- Kepner and Tregoe Analysis (see notes)
- Major Problem Reviews (see notes)

These are the names of four Problem Management techniques. Pain Value Analysis (PVA) and Ishikawa are explained on the next few slides.

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

Pain Value Analysis

Pain Value Analysis (PVA)



Calculate pain value:

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

Address in order of pain value

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

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

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

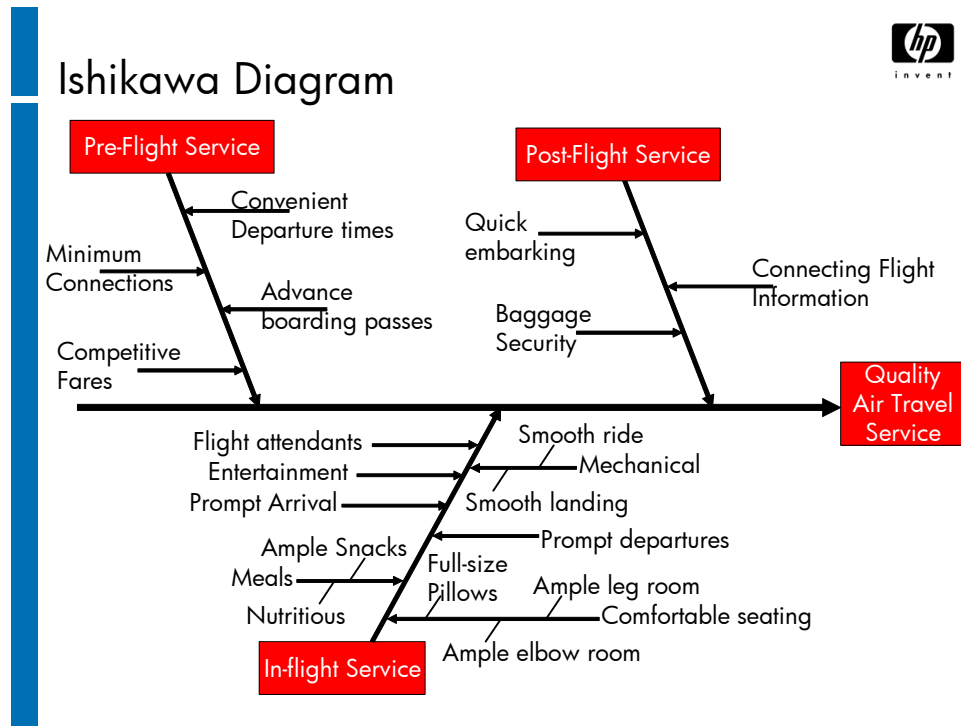
Something like the graph on the slide will result.

Duration in the formula presented in the slide, should be understood as the duration and related costs of resolving the incidents.

Weighting factor should be any data meaningful to the business, it could be a number that varies according to the day of the month, the type of business transaction affected, etc., but in general terms is the cost to the business - this being perhaps the most important factor of all.

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

Ishikawa Diagram



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

Core Activities

Core Activities



Problem Management includes several core activities. Which one of the following most accurately summarizes these?

- A. Problem control, error control, management reporting
- B. Identification, control, status accounting, verification
- C. Incident control, severity analysis, support allocation, reporting
- D. Identification, severity analysis, support allocation, investigation

Terminology



Terminology

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

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

Configuration Management

Module 5

Mission of Configuration Management

Mission of Configuration Management



To provide a logical model of the IT Infrastructure by **identifying, controlling, maintaining and verifying** the versions of **all Configuration Items** in existence with the organisation and determining the relationships between those items.

Configuration Management supports this mission through:

- Identification
- Control
- Status Accounting
- Audit and Verification

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

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

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

Scope of Configuration Management



Scope of Configuration Management

- Configuration Management
 - All information to manage IT components
- Asset Management
 - Accountancy process
 - Items above a certain value
 - Financial information

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

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

- The range of responsibility of Configuration Management
- The breadth of the Configuration Management Database

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

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

Objectives of Configuration Management

Objectives of Configuration Management



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

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

Configuration Management – Key Definitions

Configuration Management – Key Definitions



- Configuration
 - Anything that needs to be controlled
- Configuration Item (CI)
 - A component within a configuration
 - A configuration in its own right
- CI Type
 - E.g. software products, business systems, system software, etc.
- Attribute
 - Describes a CI
- Relationships
 - Primary
 - Parent/child (part of)
 - Secondary
 - Connected to
 - User of
- Lifecycle
 - Stages in the life of a CI

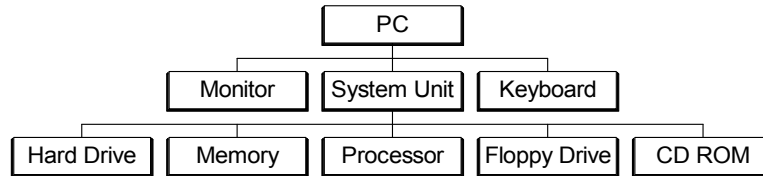
Configuration

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

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

Configuration Item

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



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

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

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

CI Types

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

Attribute

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

Examples of CI's attributes are: an identification number or name, model or make or may relate to the CI's capacity or size.

Relationship

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

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

- A CI is a part of another CI (e.g. a software module is part of a program, a server is part of a site infrastructure) - this is a 'parent/child' relationship
- A CI is connected to another CI (e.g. a desktop computer is connected to a LAN)
- A CI uses another CI (e.g. a program uses a module from another program; a business service uses an infrastructure server).

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

Lifecycle

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

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

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

Specifying lifecycles also allows checking during a stage for:

- A CI's ongoing capacity to support an end to end service
- A CI's progress along the lifecycle continuum
- Problems associated with CIs during different stages of the lifecycle; such as a tendency to malfunction or require frequent servicing

Core Activities of Configuration Management

Core Activities of Configuration Management



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

PICSV is a convenient way of remembering the 5 steps/stages that are needed to implement the Configuration Management process. The individual stages are explained in more detail in the following slides.

Planning for Configuration Management



Planning for Configuration Management

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

Steps in the planning process include:

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

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

There are two key roles that need to be assigned as part of this stage

- A Configuration Manager who is the process owner. They act in a “Policeman” role to make sure others are updating CMDB in line with procedures.
- A Configuration Librarian who updates the CMDB. This can be full time role but is usually is “a hat” other people wear when updating the CMDB as part of other ITIL process (e.g. Change Management).

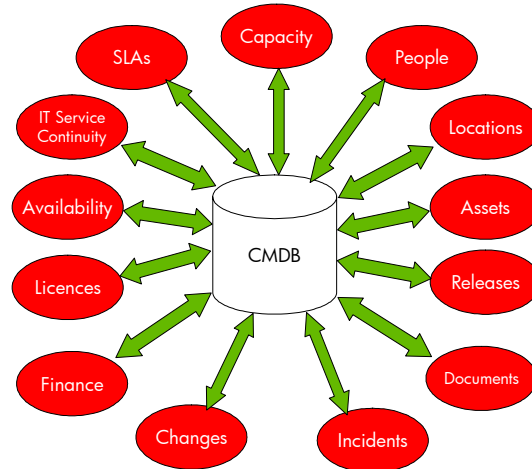
Configuration Management Database (CMDB)

Configuration Management Database (CMDB)



Stores details of :-

- CIs
- Attribute
- Relationships
- Events



The 'core' of an integrated service management tool
= "information bank" for all other ITIL processes

The CMDB is the heart of Configuration Management. It is really an "information" bank that contains all relevant information on CI's and their relationships and history.

Key ITIL Interfaces

Key ITIL Interfaces



- Change Management
 - Without Change Management the information about CIs cannot be kept up to date
 - Without Configuration Management Impact Analysis during Change Management will be less effective
- Release Management
 - Without Release Management the information about CIs and release events will not be maintained
 - Without Configuration Management the responsibility of licence management will be very difficult to accomplish
- Service Desk
 - Without Service Desk (acting as Configuration Librarians) the CMDB information will not be effectively maintained
 - Without Configuration Management It would be difficult for Service Desk to maintain who has what and where type information

The above slide shows some of the key relationships Configuration Management shares with other ITIL processes. It should be clear however, that these are not the only relationships that exist. Configuration Management will contribute to all the other ITIL processes at various points.

Configuration Management's Contribution to License Management

Configuration Management's Contribution to License Management



- Provides information to Release Management to ensure legality of software environment
- Enable Release Management software control responsibilities e.g.:
 - Software license monitoring and control
 - Software auditing

License Management

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

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

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

Identification

Identification



- Logical
 - What items need to be recorded?
 - What do we need to know about them?
- Physical
 - Marking items that are under Configuration Management control

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

Physical and Logical Identification

Identification has two aspects:

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

Naming Conventions

Naming Conventions



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

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

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

What Do We Need to Identify? (1 of 4)

What Do We Need to Identify? (1 of 4)



- The Configuration
 - Where are our boundaries ?
- Configuration Items
 - What are they ?
 - CI or Attribute?
 - Is it needed to deliver a service?
 - Is it uniquely identifiable?
 - Is it subject to change?
 - Can it be controlled and managed?
- CI Types
 - What logical groupings do we need ?
- Attributes of CIs
 - What Level of detail do we need ?

The above slide shows the type of questions that typically need to be answered by an organization when identifying what they will attempt to control by Configuration Management.

What Do We Need to Identify? (2 of 4)

What Do We Need to Identify? (2 of 4)



- Identifying CIs — Level of Breakdown
 - Lowest level of independent change
 - Who are you and what are you doing?
 - Information value

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

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

Choosing the correct level of breakdown is a balance between:

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

What Do We Need to Identify? (3 of 4)

What Do We Need to Identify? (3 of 4)



- Relationship
 - Have we captured them all ?
- Baselines
 - Snapshot of a CI at a time or stage
 - What did a CI look like before a change?
 - Reverting to a previous version of a CI
 - Simplify data capture
 - Simplify database design
- Variant
 - A baseline with minor differences

Baseline

A baseline is a snapshot of a CI at a specific time or stage in its lifecycle. It can also be seen as a “Standard CI”; that is, a generic definition of a CI. Baselines can be used to:

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

Variant

A variant is a baseline with some minor differences. For example a baseline could be a PC with an English or German keyboard. Variants are used when multiple forms of CIs are used, such as an old and new version. The goal is to simplify data capture and maintenance of both the CMDB and the infrastructure itself. In some cases, it is easier to utilize variants of a CI rather increase the total number of CIs recorded in the CMDB.

What Do We Need to Identify? (4 of 4)

What Do We Need to Identify? (4 of 4)



- Lifecycle
 - Allow CIs to be moved, tracked and checked for
 - Cost, time and specification
 - Authorization
 - Completion
 - Allows checking for
 - Responsibility
 - Progress
 - Problems

Lifecycle

The lifecycle states for each CI type should also be defined; e.g. an application release may be build, tested, accepted, installed, or withdrawn.

Lifecycle states allows CIs to be moved, tracked and checked for cost, time, specification, authorization and completion.

With such control, CIs can be check for responsibility, progress and or problems during its lifecycle.

Configuration Control (1 of 2)



Configuration Control (1 of 2)

- Information in the CMDB
 - Access
 - Changes
 - Adding new items
- Examples of controls
 - Registering new CIs
 - New software
 - Versions of CIs from Release Management
 - License control
 - Decommissioned CIs

Controlling Information in the CMDB

Control is concerned with the information held in the CMDB:

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

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

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

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

Configuration Control (2 of 2)



Configuration Control (2 of 2)

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

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

Control requires:

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

Configuration and Change Management



Configuration and Change Management

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

The Relationship between Configuration and Change Management

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

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

- When new CIs are added to the IT infrastructure
- When the status of CIs change
- When the owners of CIs change
- When the location of CIs change
- When relationships affecting CIs change
- When old CIs are removed
- When an unregistered CI is found or information regarding a CI is inaccurate
- When a change is requested, Change Management should use the CMDB to assess that change's impact on the business and other CIs

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

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

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

Configuration Status Accounting



Configuration Status Accounting

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

Tracking the Status of CIs

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

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

Examples of useful reports could be:

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

Configuration Audit and Verification



Configuration Audit and Verification

- Does the CMDB reflect reality?
- Accuracy is improved by
 - Active rather than passive CMDB
 - Automatic updating
 - Integration with other processes
 - Automatic checks
 - Don't rely on auto discovery to be totally accurate

■ Does the CMDB Reflect Reality?

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

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

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

Components Recorded in the CMDB



Components Recorded in the CMDB

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

Which other components could be recorded in the CMDB?

- Data communications equipment
- Documentation
- Personnel

A. 1 and 2

B. 1 and 3

C. 2 and 3

D. 1, 2, and 3

Configuration Items



Configuration Items

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

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

Change Management

Module 6

Mission of Change Management

Mission of Change Management



To ensure that **standardized methods and procedures** are used for efficient and **prompt handling of all changes**, in order to **minimize the impact** of any related incidents upon service.

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

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

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

Scope of Change Management



Scope of Change Management

Covers areas including:

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

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

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

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

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

Objectives of Change Management



Objectives of Change Management

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

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

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

Scalability

Scalability



The Change Management process must be scaleable for:

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

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

Considerations are:

- Different types of change
- Size of change
 - Large
 - Small
- The cost of the change; how expensive, labor-intensive or time-consuming is it?
- The impact of the change; will there be a significant or slight effect on the business and/or IT?
- The timeframe the change must be delivered in
- A separate procedure for urgent changes

Core Elements

Core Elements



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

Request for Change (RFC)

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

Change Advisory Board (CAB)

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

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

To prevent large, unmanageable meetings, the RFCs can be managed electronically with attendance at the meetings being optional.

Change Advisory Board/Emergency Committee (CAB/EC)

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

The CAB/EC can consist of one to three key staff. These people can be predefined but may vary as their selection may depend on the nature of the change. This may just require a telephone conference, and members must be prepared to be available after hours.

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

The FSC contains details of all approved changes and their implementation dates for an agreed period. The FSC is used so that all groups affected by a change can plan for its release. The FSC could have detailed short-term schedules, with less detailed schedules for longer-term planning.

The Projected Service Availability (PSA) contains details of changes to agreed Service Level Agreements and service availability because of the currently planned FSC.

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

Normal/Urgent Change

A Normal change is a change that follows the normal Change Management process and procedures, such as categorization according to its business impact and required resources.

An Urgent change is a change that needs to be carried out in less time than the normal change, always with a business impact justification. It is typically used for emergency problem resolution. Urgent change should not be used as a faster route to implement changes, as risks are higher than normal changes.

More details later in this module.

Change Model

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

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

Standard Change

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

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

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

Post Implementation Review (PIR)

A Post-Implementation Review (PIR) should be carried out to confirm that the Change has met its objectives, that Customers are happy with the results; and that there have been no unexpected side-effects.

CAB

CAB



- Membership
 - Change Manager (Chair) — only permanent member
 - Customer/User representatives
 - Applications developers/maintainers
 - IT Service Management representatives
 - Other IT staff
 - Office services
 - Suppliers
- Meetings
 - RFCs distributed to all members in advance of meeting
 - Attendance at meetings optional
 - Scheduled as necessary (at least every 6 months)

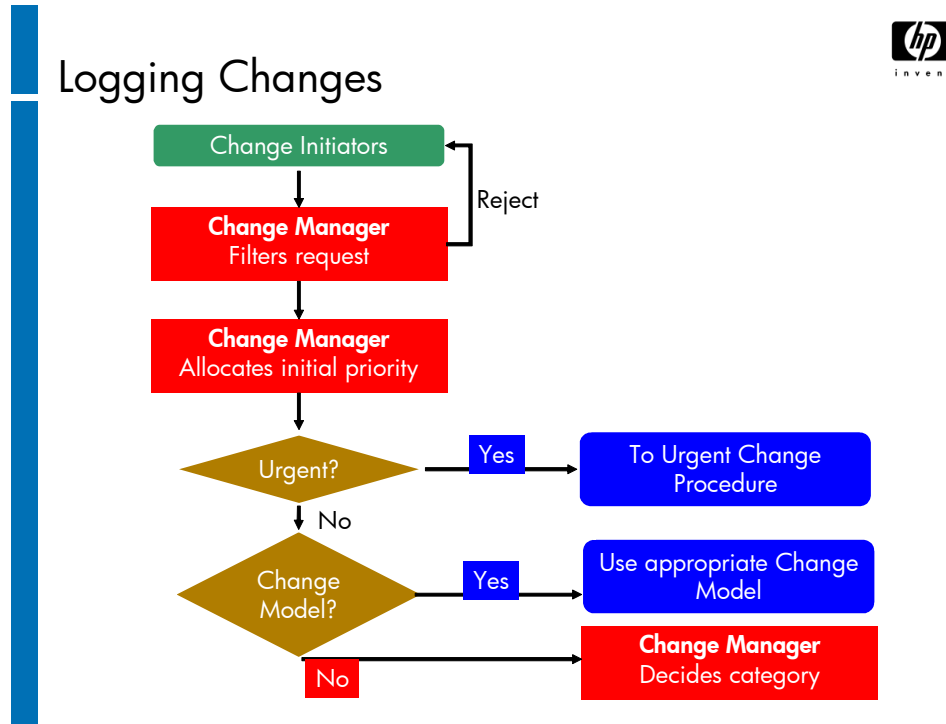
CAB membership will depend on the change being requested, but could consist of anyone who is capable of ensuring that the change is assessed adequately from a business and technical viewpoint. This could include:

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

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

CAB meetings should be scheduled at a minimum of once every 6 months and when major projects are due to deliver products. However in most organizations CABs will be on a much more regular basis, in some extreme cases or during a period of substantial change, possibly on a daily basis. The meeting will then be used to sign-off approved changes, review outstanding changes and to assess future changes.

Logging Changes



Change Initiation

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

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

Initial Logging and Filtering

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

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

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

Initial Priority

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

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

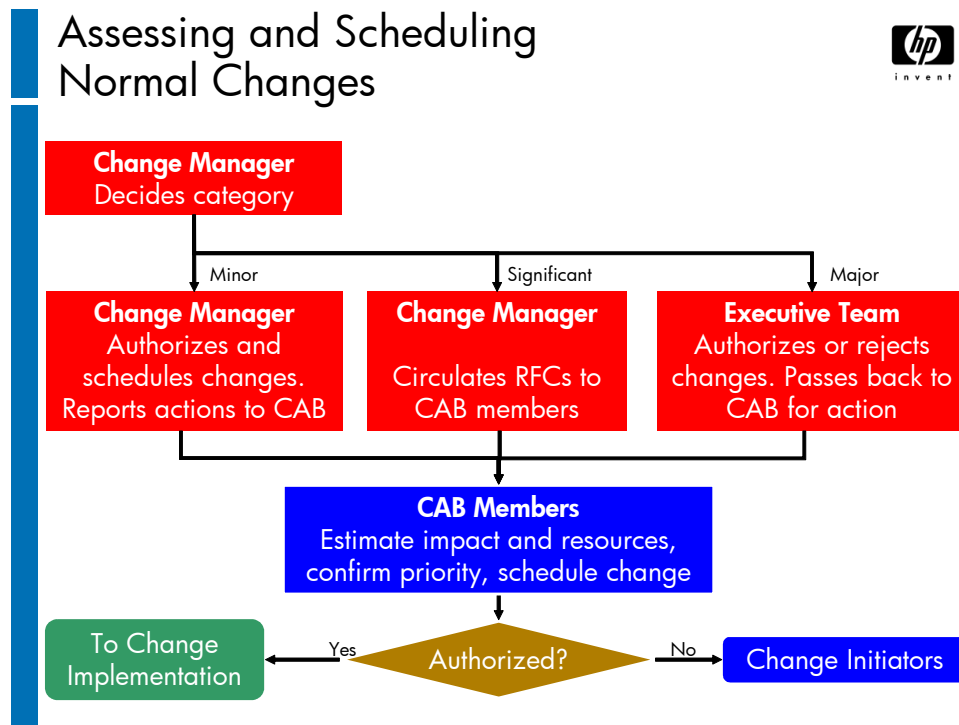
If the change is not urgent the next step is to check whether there is a change model for this type of change. If there is the Change Manager will follow the steps for initiating that procedure, if not it will continue on to the categorization step in the normal procedure.

Change Categorization

The change is then categorized in two ways:

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

Assessing and Scheduling Normal Changes



Assessing Normal Changes

ITIL identifies 3 basic categories:

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

Change Assessment and Approval

Category 1 — Minor

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

Category 2 — Significant

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

Category 3 — Major

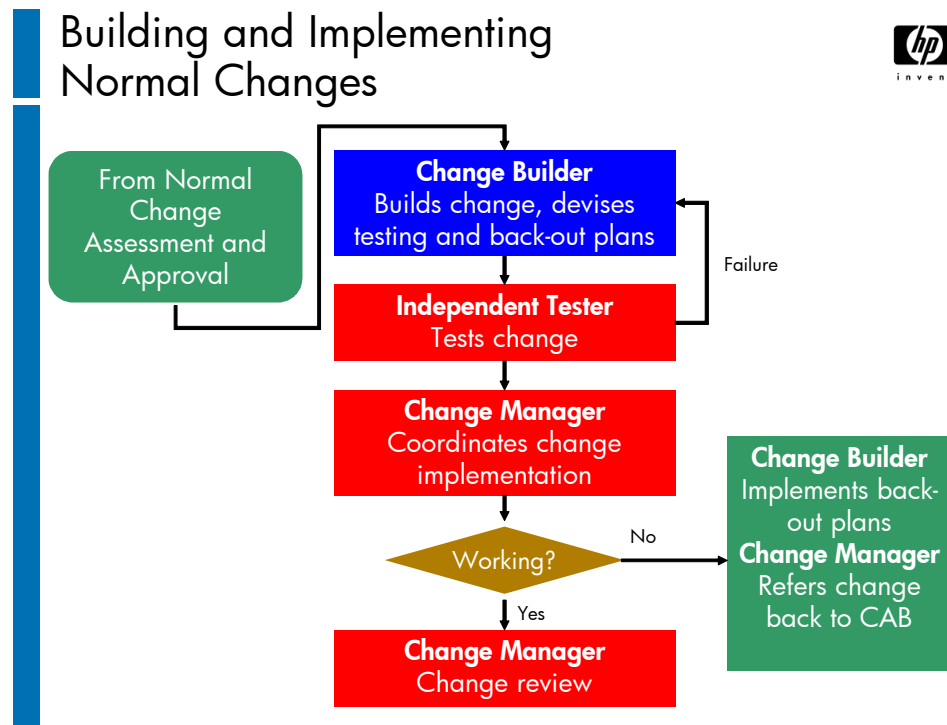
The Chief Information Officer (CIO) or senior IT Manager must refer the request upwards. Approved changes must be passed back to the CAB for scheduling and implementation.

Change Scheduling

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

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

Building and Implementing Normal Changes



Change Building

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

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

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

Change Testing

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

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

Implementation

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

Change Review

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

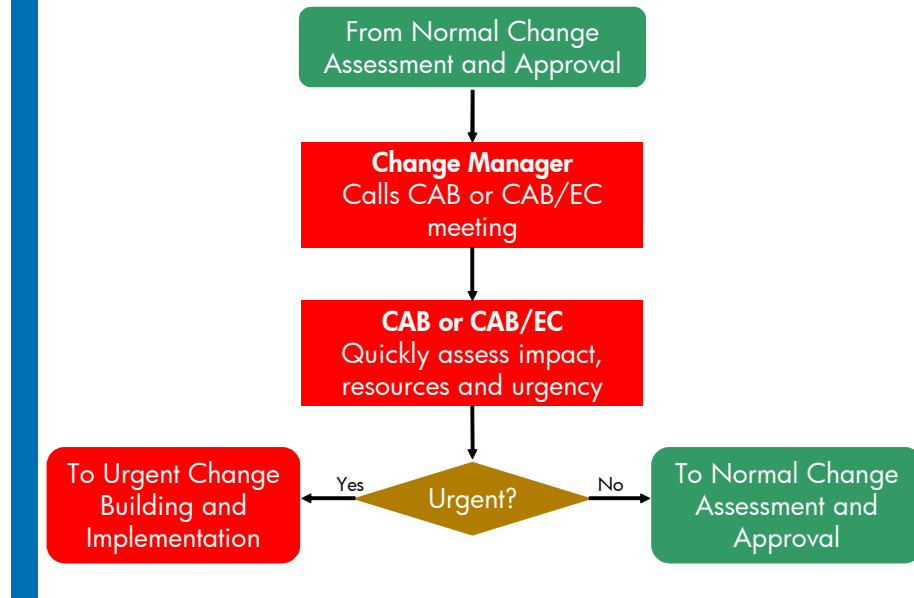
Documentation

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

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

Assessing and Scheduling Urgent Changes

Assessing and Scheduling Urgent Changes



When are Urgent Changes Allowed?

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

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

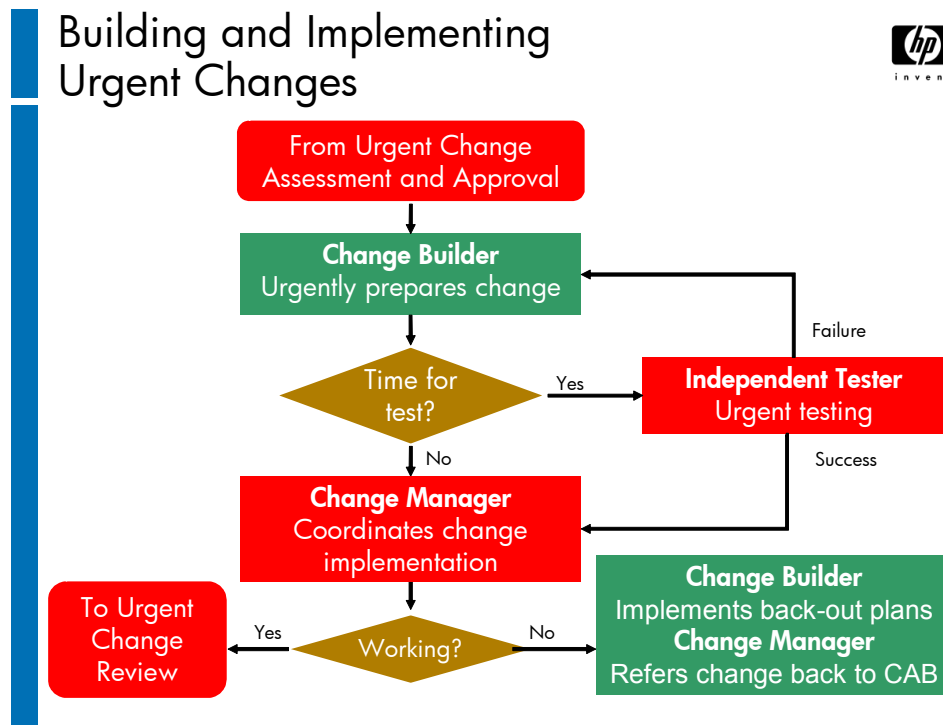
Urgent Change Assessment and Approval

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

Urgent Change Scheduling

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

Building and Implementing Urgent Changes



Urgent Change Building

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

Urgent Change Testing

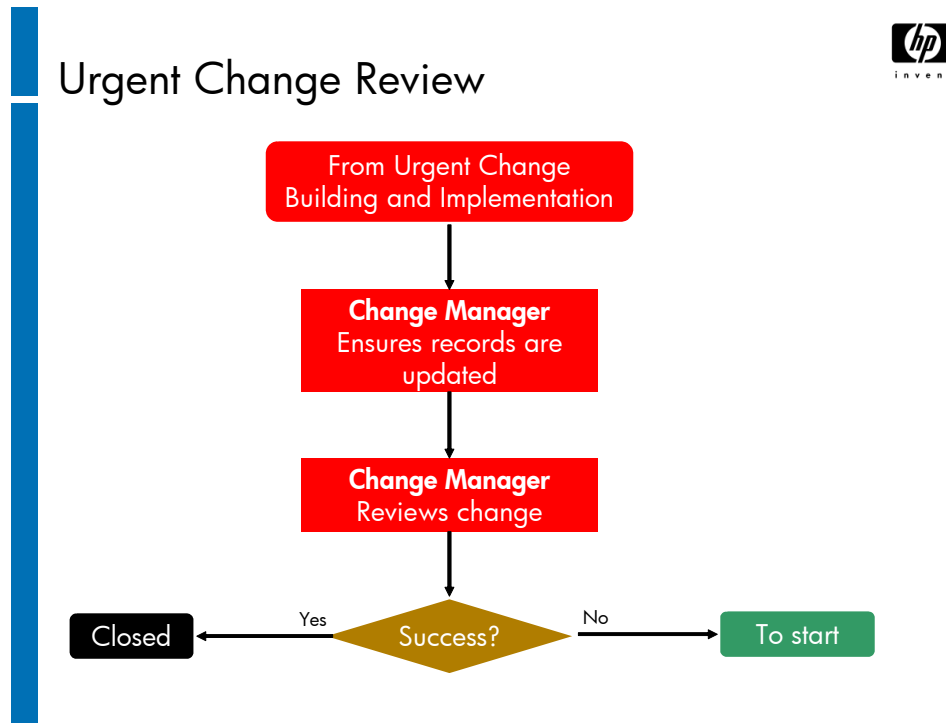
Testing should be carried out as far as possible. Untested changes should not be implemented if at all possible. The cost of reworking a change that failed is usually greater than the cost of testing the change in the first place.

Urgent Change Implementation

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

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

Urgent Change Review



Urgent Change Review

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

Documentation of Urgent Changes

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

This will be checked at the change review

What Happens if an Urgent Change Fails?

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

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

Change Models (1 of 2)



Change Models (1 of 2)

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

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

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

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

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

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

Change Models (2 of 2)



Change Models (2 of 2)

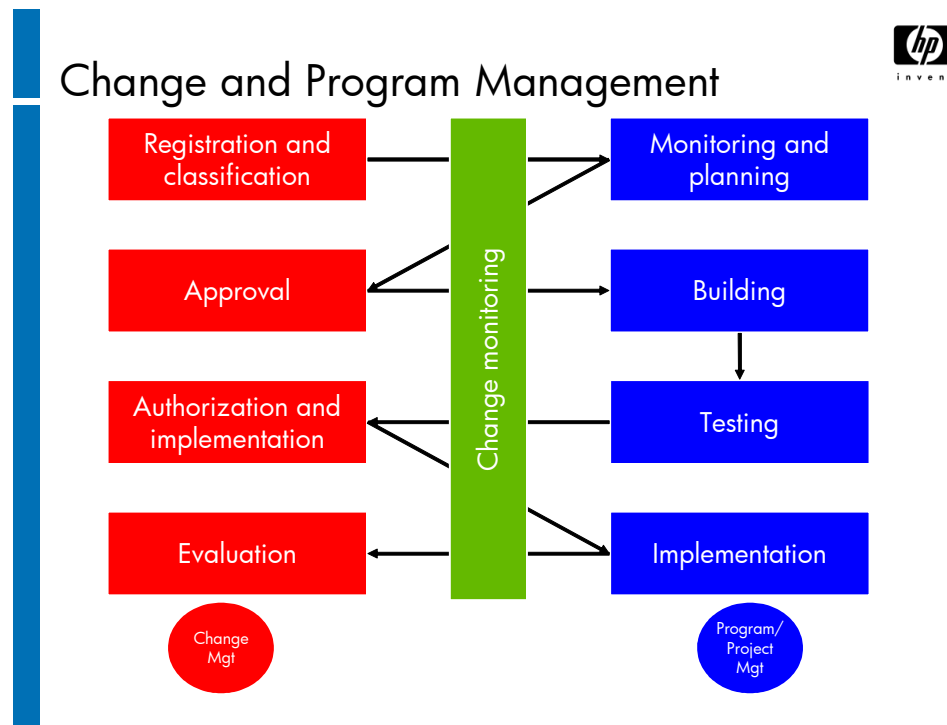
- Models should be predefined and automated so far as possible
- It should be possible to easily create a new model, or variation of an existing model
- Ability to use and easily amend models should be a significant criteria in tool selection

IT Service Management tools can use the concept of a change model to incorporate as much predefined information as possible into a regular Request for Change record, creating a model or template that afterwards can be forwarded automatically to the approver. This ensures consistent implementation of common types of changes and also can decrease the time and resources needed to process the change.

When creating a new model, the predefinition of information should be an easy task. For example, if it is hard to identify the person or group of persons needed to approve a change, then it is not a likely candidate to become a Change Model.

When establishing the criteria for choosing an IT Service Management tool, the ability and ease with which the tool can define, create and amend Change Models should be considered as significant criteria.

Change and Program Management



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

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

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

Controlling Changes to IT Infrastructure



Controlling Changes to IT Infrastructure

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

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

Assessing the Impact of Change



Assessing the Impact of Change

In which of the following circumstances is requesting an urgent change justified?

- A. Only one small component requires changing and it is unlikely to affect any other components
- B. The CAB meeting has been cancelled because most of the members are unavailable at the time previously agreed
- C. The supplier has advised that previous versions will not be supported very much longer
- D. The change is needed to correct an error on a business critical system

Release Management

Module 7

Mission of Release Management

Mission of Release Management



To take a **holistic view of change** to an IT service and ensure that **all aspects of a release into the live environment**, both technical and non-technical, are considered together

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

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

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

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

Major activities include:

- Release policy and planning
- Release design, build and configuration
- Release acceptance
- Rollout planning
- Extensive testing to predefined acceptance criteria
- Sign-off of the release for implementation
- Communication, preparation and training
- Audits of hardware and software prior to and following the implementation of changes
- Installation of new or upgraded hardware
- Storage of controlled software in both centralized and distributed systems
- Release, distribution and the installation of software

Scope of Release Management

Scope of Release Management



- Software
 - In-house applications
 - Packaged software
 - Bespoke software (custom built)
 - Compilers, interpreters, assemblers
 - Operating systems
 - Utility software
 - Anti-virus
- Hardware
- Licenses
- Documentation
 - Technical specifications
 - User manuals
 - Procedures
- Training
- Communication

Release Management includes:

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

- Training
 - Release Management are responsible for allocating training time during a rollout phase
- Communication
 - Key activity in making sure the Customer is fully aware of what is happening, where and when. In order to manage Customer expectations

Objectives of Release Management



Objectives of Release Management

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

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

Definition of a Release

Definition of a Release



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

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

Licensing Issues



Licensing Issues

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

See also License Management in the Configuration Module

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

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

Definitive Software Library (DSL) (1 of 2)

Definitive Software Library (DSL) (1 of 2)



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

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

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

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

Definitive Software Library (DSL) (2 of 2)

Definitive Software Library (DSL) (2 of 2)



Quality Assurance

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

Quality Assurance

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

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

Definitive Hardware Store (DHS)

Definitive Hardware Store (DHS)



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

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

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

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

Release Policies

Release Policies



- Release Units
- Release types
 - Full release (Normal release unit)
 - Δ (Delta) release
 - Package release
- Urgent

Release Policies

Release Management is responsible for defining the frequency, content, type and method of release. A release policy also defines the roles and responsibilities for Release Management which includes procedural details such as:

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

Release Units

The release policy identifies release units, which are components of an IT Service that are normally released together. A release unit typically includes sufficient components to perform a useful function. For example one release unit could be a desktop PC, including hardware, software, licenses, documentation etc.; a different release unit may be the complete payroll application, including IT operations procedures and user training.

Release Types

The release policy also identifies what type of software release will be made. There are three main types of release:

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

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

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

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

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

- **Package** — including at least two releases (e.g. delta, full). A package release is intended to offer a longer period of stability by reducing the frequency of releases.

Where appropriate and where larger amount of change can be confidently handled without problems, individual releases (full releases, delta releases or both) are grouped together to form package releases. For example, changes to one system often require changes to be made to another(s); if these have to be made at the same time they should be included in the same package release.

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

Urgent

Not recommended in ITIL

This is a release that is required to correct a small number of known problems.

Release Scales / Identification



Release Scales / Identification

- Major releases
 - Normally containing large areas of new functionality
 - E.g. V1 to V2
- Minor releases
 - Normally containing small enhancements and fixes
 - E.g. V1.1 to V1.2
- Emergency fixes or patches
 - Normally containing the corrections to a small number of known problems
 - E.g. V1.1.1 to V1.1.2

Release Scales

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

Releases are often divided into:

- Major software releases and hardware upgrades

Normally containing a lot of new functionality, some of which will replace temporary problem fixes
- Minor software releases and hardware upgrades

Normally containing small enhancements or fixes, some of which have already been issued as fixes and emergency fixes
- Emergency fixes or patches

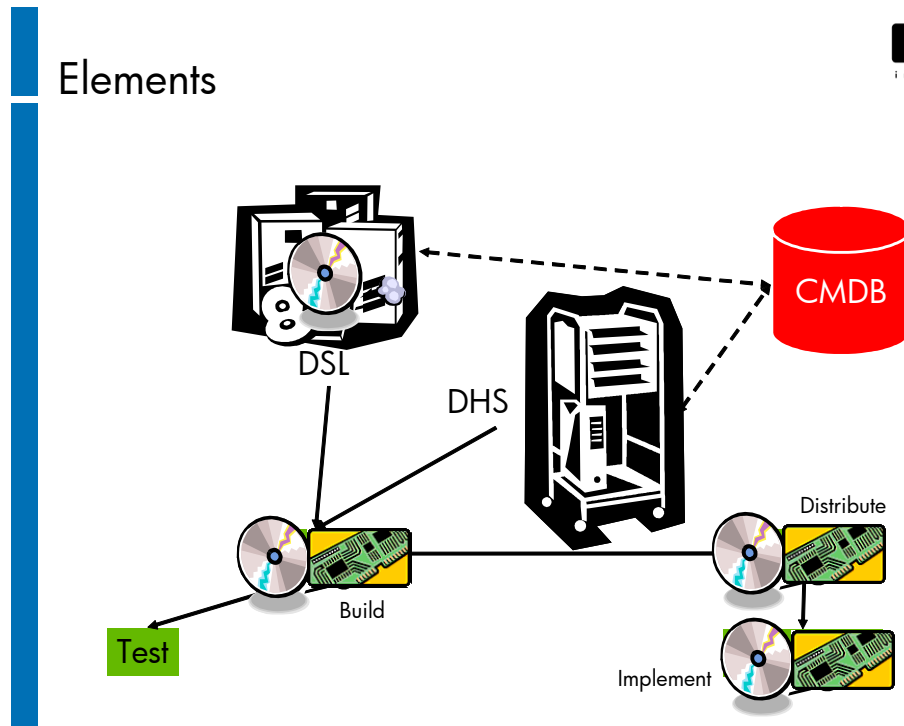
Normally containing corrections to a small number of known problems

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

Release Identification

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

Elements



This slide shows the progression for building, testing, distributing and finally implementing a release into the live environment.

As the CIs, belonging to the release, pass along these phases up to production, their correspondent records in the CMDB should be updated accordingly, to reflect the current status of the CIs.

Release Records



Release Records

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

Release records are held in the CMDB. They contain:

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

The CMDB will maintain records of the CIs impacted by planned and past releases.

Release Management Activities (1 of 2)

Release Management Activities (1 of 2)



- Release Planning
 - Developing a plan for each release
 - Agree and schedule with Change Manager
- Designing, Building and Configuring releases
 - Process for assembling CIs for release
 - CIs are under Configuration Management control
- Testing and release Acceptance
 - Installation procedures
 - System functionality

Release Planning

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

Designing, Building and Configuring a Release

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

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

Testing and Release Acceptance

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

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

Release Management Activities (2 of 2)

Release Management Activities (2 of 2)



- Rollout planning
 - Builds onto the release plan
 - Exact implementation actions
- Communication, Preparation, and Training
 - When and how releases will be rolled out
 - How they will be affected
 - Progress of changes
- Distribution and installation
 - Moving the release to the target environment
 - Deploying the release

Rollout Planning

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

Communication, Preparation and Training

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

Distribution and Installation

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

Definitive Software Library



Definitive Software Library

Which of the following best describes the Definitive Software Library?

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

Scope of Releases



Scope of Releases

Which of the following statements is true?

- A. An urgent release is always a delta release
- B. A full release may contain package and delta release
- C. A full release may contain several delta releases
- D. A package release may contain full and delta releases

Service Level Management

Module 8

Mission of Service Level Management

Mission of Service Level Management



To **maintain** and gradually **improve business aligned IT service quality**, through a constant cycle of **agreeing, monitoring, reporting, and reviewing IT service achievements** and through instigating actions, to eradicate unacceptable levels of service

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

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

Please note:

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

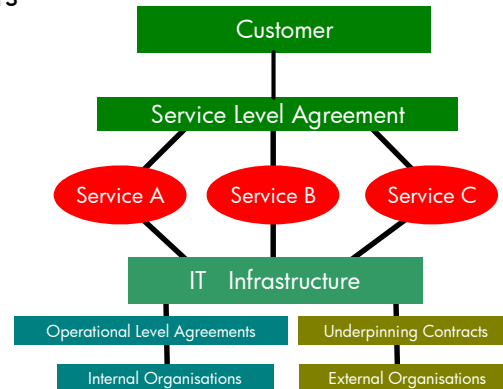
Scope of Service Level Management



Scope of Service Level Management

Three sets of relationships

- Customer and IT
- Internal departments within IT
- IT and external suppliers



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

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

Objectives of Service Level Management

Objectives of Service Level Management

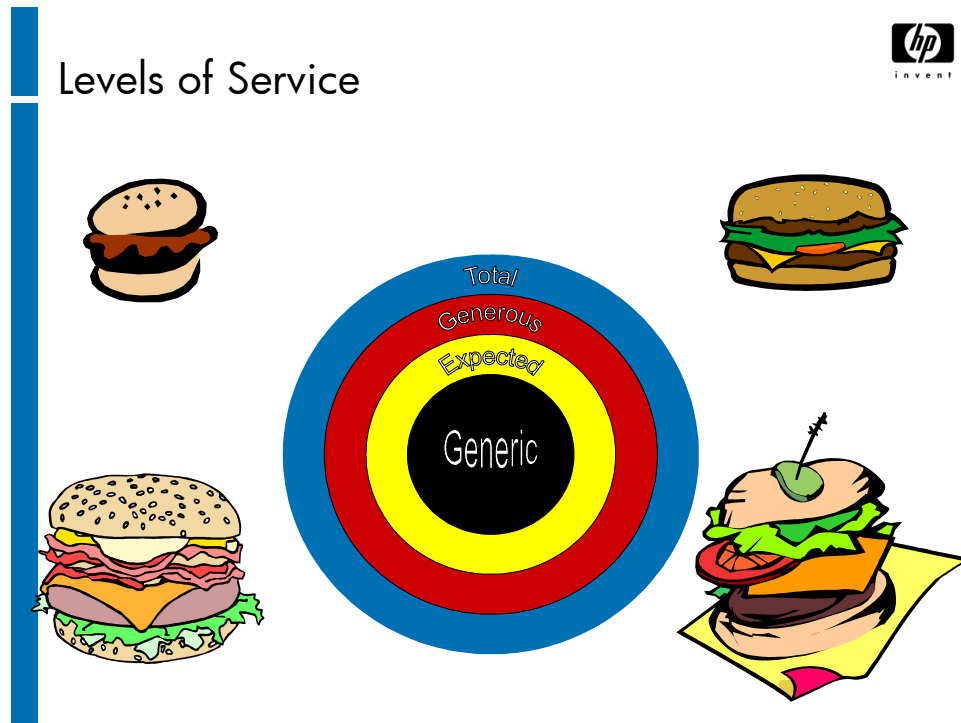


- To catalog IT services
 - IT
 - Customer
- To quantify IT services
- To define internal and external service targets
- To achieve agreed service targets
- Ongoing improvement of service levels
- To review agreements and contracts

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

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

Levels of Service



It is talking about the different levels of service (or product) Generic, Expected, Generous and Total, and setting Customer expectations against these.

A generic burger – a couple of bits of bread with some sort of meat patty in between etc.

McDonald's have gone beyond the generic burger and have done a great job of "expected" because all over the world their restaurants are almost identical. In fact this is now the "standard" you would expect from any fast food outlet.

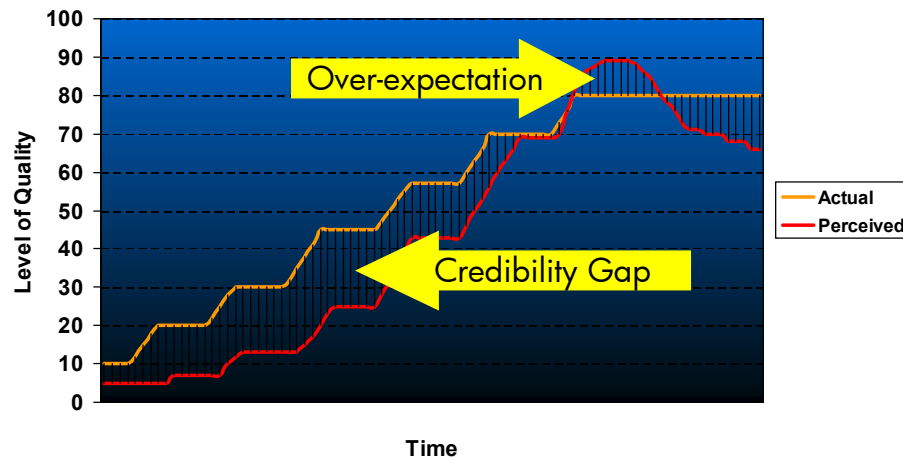
Now think of a restaurant – what they supply has to be better than the expected norm, so here you get a burger, made from fresh ground beef with all the trimmings etc.

Now think of the best tasting, most filling, burger you ever had! This is the equivalent of a total burger.

There are two lessons to take away from this, first, the higher the expectation, usually the higher the cost. The second is that if you continually supply generously then very soon that will become expected and you have to do more to regain your customer satisfaction levels.

Managing Expectations

Managing Expectations

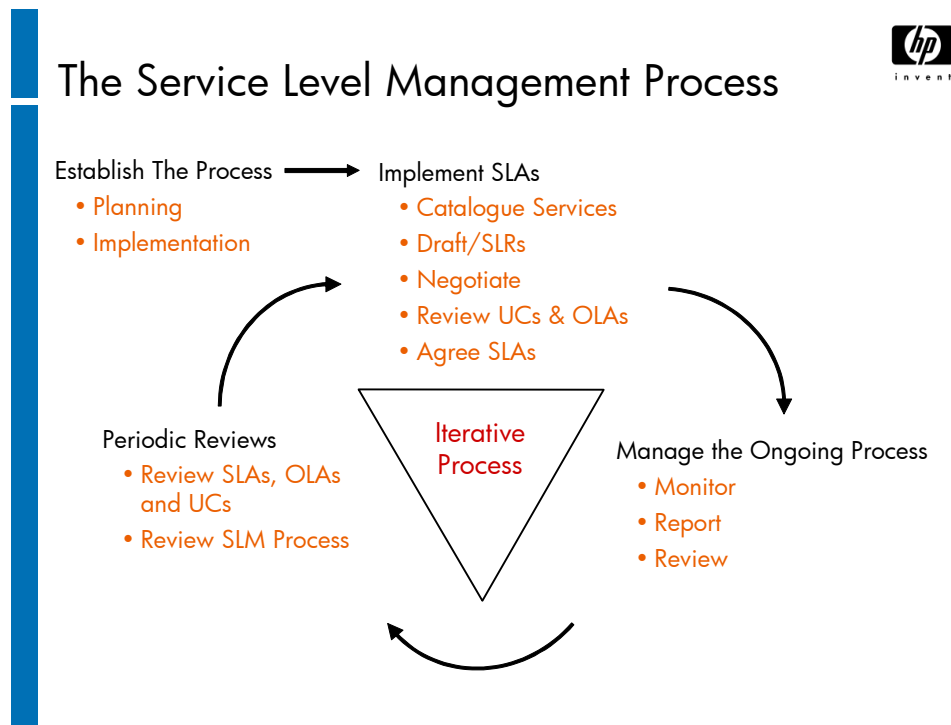


The above slide put the previous analogy into reality.

Where perception outstrips actual level of service, you initially have excellent Customer satisfaction, but that will very quickly fade as expectations and perceptions are not actually met.

Where service levels outstrip perceptions you have poor customer satisfaction even though the facts do not support this. This is called the credibility gap.

The Service Level Management Process



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

Establish the Process

This is the introduction of SLM to an organization, and as such, done only once. The basic activities are:

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

Implement SLAs

This phase consists of:

- **Cataloging IT services:** This includes understanding what services are being used currently, as well as the level of customer expectation
- **Draft SLA/SLRs:** This is where the Service Level Management negotiates and agrees the Service Level Requirements (SLRs) and expected service characteristics with the Customer. It may be better to produce a first outline draft as a starting point (rather than a blank sheet)
- **Negotiate:** This is the beginning of a reiterative process of setting actual levels of service that will be included in the SLA
- **Review underpinning contracts and OLAs:** Service Level Management has to be sure that they can deliver the required level of service before any agreement is signed. This is done together with the internal IT departments and external IT suppliers
- **Agree:** The SLA is finalized and signed by all parties

Manage the Ongoing Process

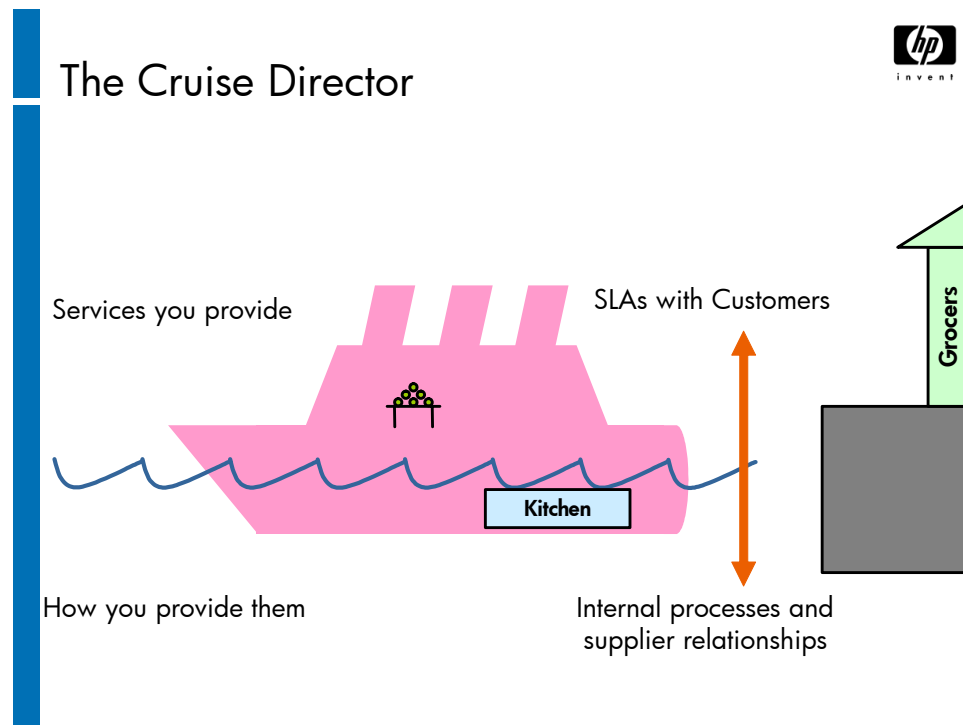
- **Monitor:** Once an agreement is in place, it is continuously monitored to ensure compliance with the SLA, and also to identify areas for improvement
- **Report:** Service Level Management reports are communicated regularly to different parties of the agreements to ensure ongoing awareness and improvement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

Periodic Reviews

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

- SLAs and all related OLAs and UCs
- The SLM process

The Cruise Director

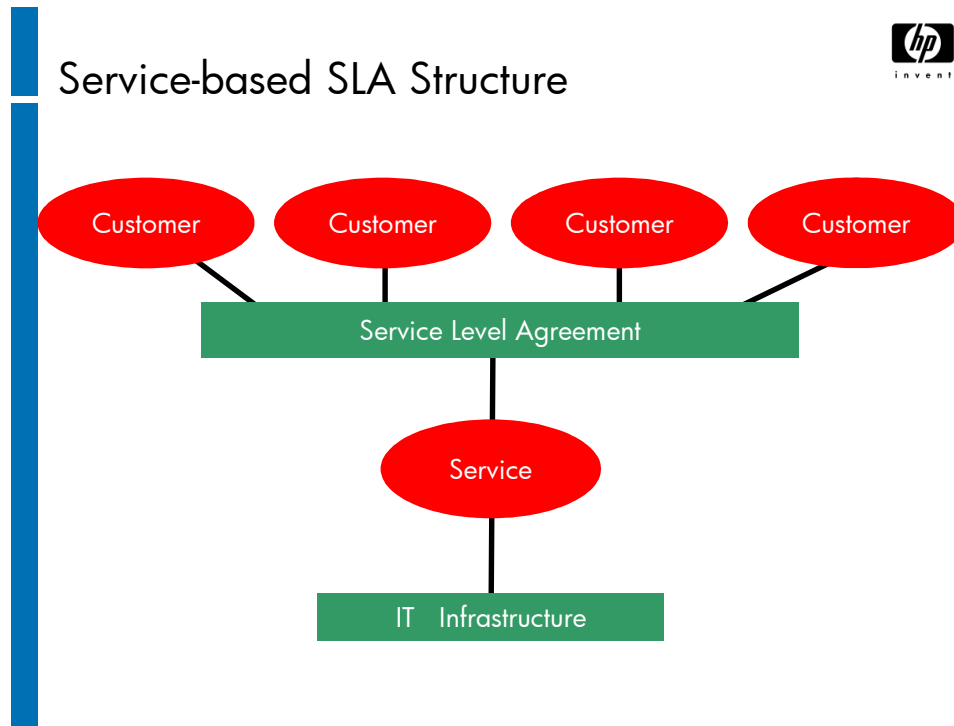


The Service Level Manager can be considered to be the “Cruise Director” on a cruise ship. They are not the captain who has control of the direction of the ship and its operations. However, they are responsible for making the passengers happy and making sure that their needs are catered for within the limitations of what the ship can provide. In other words if the passengers want apples on the table to eat at a midnight feast, the Cruise Director is responsible for working with the kitchens to make sure that apples and not oranges are delivered to the right place at the right time. They also need to make sure that the grocer has delivered apples to the ship before it leaves port.

Each of the above relationships would be managed by a particular type of document.

- An SLA is between the Customer and IT, is written in business language, and is clear and unambiguous.
- An OLA is between IT and its own internal IT support departments, is written in technical language, and is clear and unambiguous.
- An Underpinning Contract is between IT and 3rd party suppliers, is written in legal language.

Service-based SLA Structure

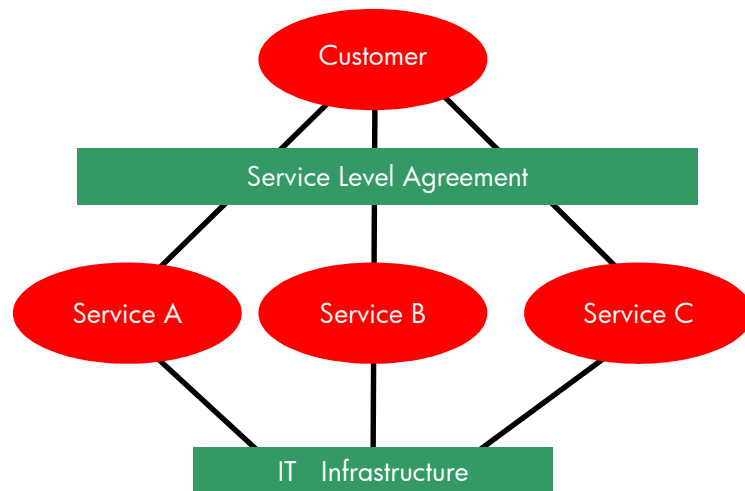


This slide shows a 'service based' SLA structure. There is one SLA covering the use of one service by any number of Customers who use the service. Customers may be in different business units or even in different organizations.

This arrangement may result in one Customer being a party to several different SLAs.

Customer-based SLA Structure

Customer-based SLA Structure

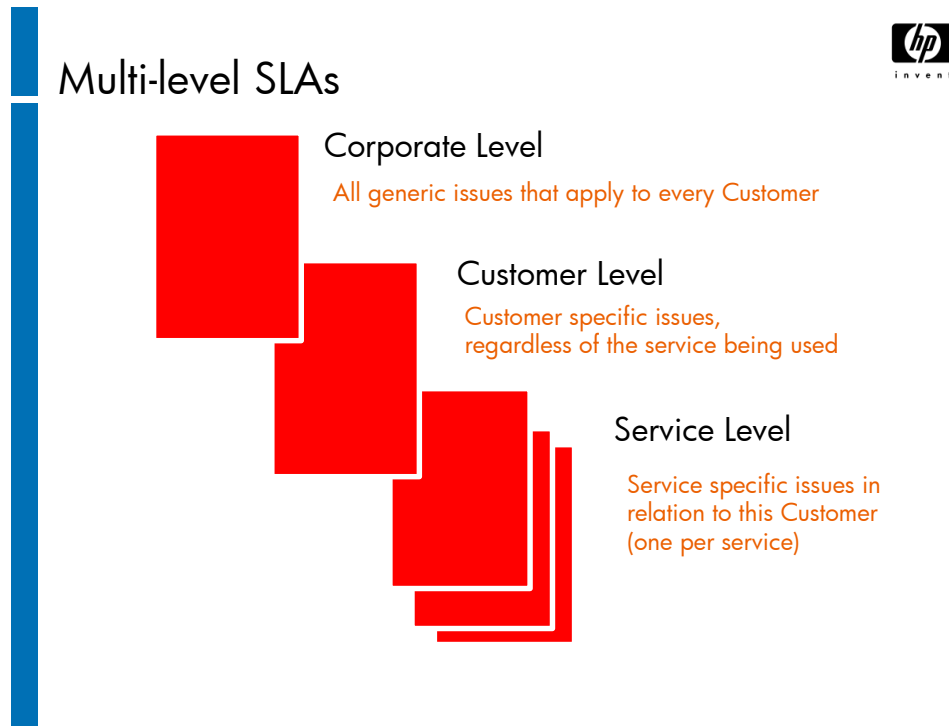


This slide shows a 'customer based' SLA structure. The customer is a party to one SLA which covers all the IT services used by the customer.

This arrangement means that a particular IT service may be specified in more than one SLA.

In practice, the mapping of SLAs between services and Customers depends on many factors including the size and structure of the organization and the location and requirements of Customers. One other major factor is the nature of the IT services themselves. Some IT services may be deemed 'corporate' services which are provided to everyone in the organization, while others are divisional or departmental services.

Multi-level SLAs



Some organizations have chosen to adopt a multi-level SLA structure. For example, a three-layer structure as follows:

1. **Corporate Level:** covering all the generic Service Level Management issues appropriate to every Customer throughout the organization. These issues are likely to be less volatile and so updates are less frequently required.
2. **Customer Level:** covering all Service Level Management issues relevant to the particular Customer group, regardless of the service being used.
3. **Service Level:** covering all Service Level Management issues relevant to the specific service, in relation to this specific Customer group (one for each service covered by the SLA).

SLA Contents (1 of 2)



SLA Contents (1 of 2)

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

The contents of an SLA should include:

- Scope of the agreement and a description of the service
- Service Hours
 - The hours during which the service will be available
 - Extensions to the service hours
 - Special days (e.g. holidays)
- Measures of Availability and Reliability
 - Availability — this is measured as the percentage of agreed time that the Customer could actually access the service. Availability should always be measured from the Customer's perspective, although there should also be internal measures of individual component or system availability.
 - Service Reliability — this should not be confused with the reliability of components, which the Customer will never see. Service reliability is measured as the Mean Time Between Failure (MTBF) of the service or Mean Time Between System Incidents (MTBSI).

- Support Details
 - Support hours
 - Service Desk contact details
 - Extension to support hours
- Respond and Fix Times
 - Target time to respond
 - Target time to resolve incidents
- Deliverables and time scales
- Defines output and transaction cycles such as the generation of monthly reports and processing times for accounting functions
- Change approval and implementation
 - Targets for responding to RFCs
- Charging – details of the charging formula and periods (if charges are being made)

SLA Contents (2 of 2)



SLA Contents (2 of 2)

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

- Service Continuity
 - A brief summary of the Service Continuity plans that have been prepared
- Signatories
- Responsibilities of both parties
 - Defines who will do what and when, respective accountabilities and terms of engagement
- Service reporting and review
 - The content, frequency and distribution list of all periodic reports
 - Schedule of review meetings
- Glossary of terms
 - A common definition of terminology, acronyms and jargon

Example Service Catalog

Example Service Catalog



| Service /Customer | Accounts | HR | Wages | Warehouse | Transport | Admin | Sales | Marketing | Security | Factory | R&D | Design |
|-------------------|----------|----|-------|-----------|-----------|-------|-------|-----------|----------|---------|-----|--------|
| Financials | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | | |
| Payroll | ✓ | ✓ | ✓ | | | | | | | | | |
| Personnel | | ✓ | ✓ | | | | | | | | | |
| Logistics | | | | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | |
| Stock Control | ✓ | | | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | |
| CAD/CAM | | | | | | | | | | ✓ | ✓ | ✓ |
| Production | | | | | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| CRM | ✓ | | | | | ✓ | ✓ | ✓ | | | | |
| Email | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Office Systems | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

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

Example Service Level Agreement Management Red Amber Green Chart

Example:
Service Level Agreement Management
Red Amber Green Chart



| Customer C | J | F | M | A | M | J | J | A | S | O | N | D |
|----------------|---|---|---|---|---|---|---|---|---|---|---|---|
| Financials | | | | | | | | | | | | |
| Payroll | | | | | | | | | | | | |
| Personnel | | | | | | | | | | | | |
| Email | | | | | | | | | | | | |
| Office Systems | | | | | | | | | | | | |
| Warehouse | | | | | | | | | | | | |
| Security | | | | | | | | | | | | |
| Service Desk | | | | | | | | | | | | |

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

Service Improvement Program (SIP)



Service Improvement Program (SIP)

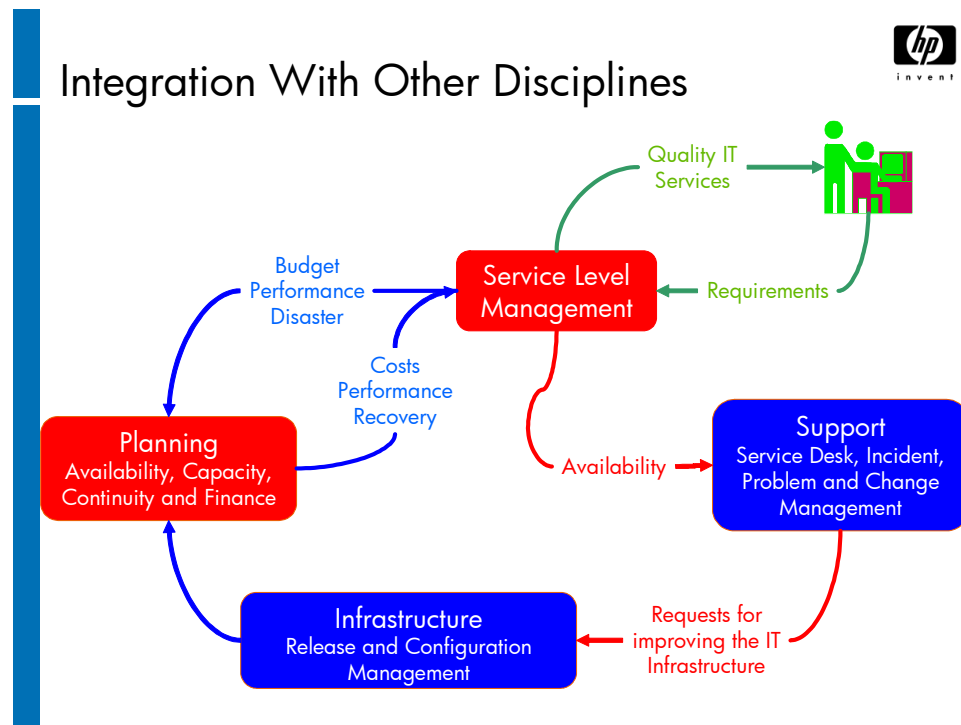
- Long term, formal process
- Aimed at improving service defined in SLAs
- Three components:
 - ITSM processes
 - Service culture
 - Management commitment

The SIP is a long term, formal and planned process of improving the levels of service defined in the SLAs. A Service Improvement Plan is usually developed upon completion of an ITIL assessment or some form of audit to gauge current IT performance relative to business requirements.

It requires at least three components:

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

Integration With Other Disciplines



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

Availability Management

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

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

Capacity Management

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

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

Incident and Problem Management

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

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

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

Change Management

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

Configuration Management

Configuration Management is responsible for the registration of all components of the IT services. As such, this process will also register the service catalogue, SLAs, underpinning contracts, service quality plan, customer organizations and suppliers.

Financial Management

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

Service Continuity Management

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

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

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

Security Management

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

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

Application Development

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

Service Level Agreement Purpose



Service Level Agreement Purpose

Consider the following statements:

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

Which is correct?

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

Service Level Structures



Service Level Structures

A Customer-based SLA structure includes:

- A. An SLA with each individual Customer group, covering all of the services they use
- B. An SLA covering all Customer groups and all the services they use
- C. SLAs for each service that are Customer-focused and written in business language
- D. An SLA for each service type, covering all those Customer groups that use that service

Availability Management

Module 9

Mission of Availability Management

Mission of Availability Management



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 objectives

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

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

Scope of Availability Management



Scope of Availability Management

- All new services
- Existing services where SLAs are in place
- IT Suppliers
- All infrastructure issues that can affect availability
- Not responsible for Service Continuity Management
 - Availability Management – day to day
 - IT Service Continuity Management – Exceptional Circumstances

Availability Management should be applied to:

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

Availability Management is not responsible for Service Continuity Management.

Objectives of Availability Management



Objectives of Availability Management

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

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

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

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

Key Concepts

Key Concepts



- **A**vailability (%)
- **R**eliability (Time)
- **M**aintainability
- **S**erviceability
- **S**ecurity

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

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

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

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

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

Availability



Availability

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

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

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

Basic Availability Calculation

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

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

Where: -

AST = Agreed service time

DT = Actual downtime during agreed service time

Reliability

Reliability



- Freedom from operational failure
- Ability to perform
 - a required function
 - under stated conditions
 - for a stated time
- MTBF/MTBSI
- Resilience
 - The capability of a set of Configuration Items (CIs) to continue to provide a required function, if not immediately then very quickly, when some CIs in the set have suffered a failure

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

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

Measurements of reliability include:

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

Reliability depends on:

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

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

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

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

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

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

Maintainability and Serviceability



Maintainability and Serviceability

- Maintainability
 - Preventative maintenance
 - Restoration and repair times, Mean Time To Repair (MTTR)
- Serviceability
 - The support for which external suppliers can be contracted to provide parts of the IT infrastructure

Maintainability

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

Maintenance or restoration of a service can be divided into 7 separate stages:

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

Serviceability

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

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

Security Management



Security Management

- Goal: To ensure that the security elements of IT services are provided at the level agreed with the customer at all times
- Managing a defined level of security for information, IT services and infrastructure
- **Confidentiality**
 - Protecting sensitive information against unauthorized access and use
- **Integrity**
 - Providing accurate, complete and timely information
- **Availability**
 - Making information accessible as agreed
 - To authorized personnel only

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

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

Security Management, in the context of this course, is the process of protecting and maintaining the Confidentiality, Integrity and Availability (CIA) of data.

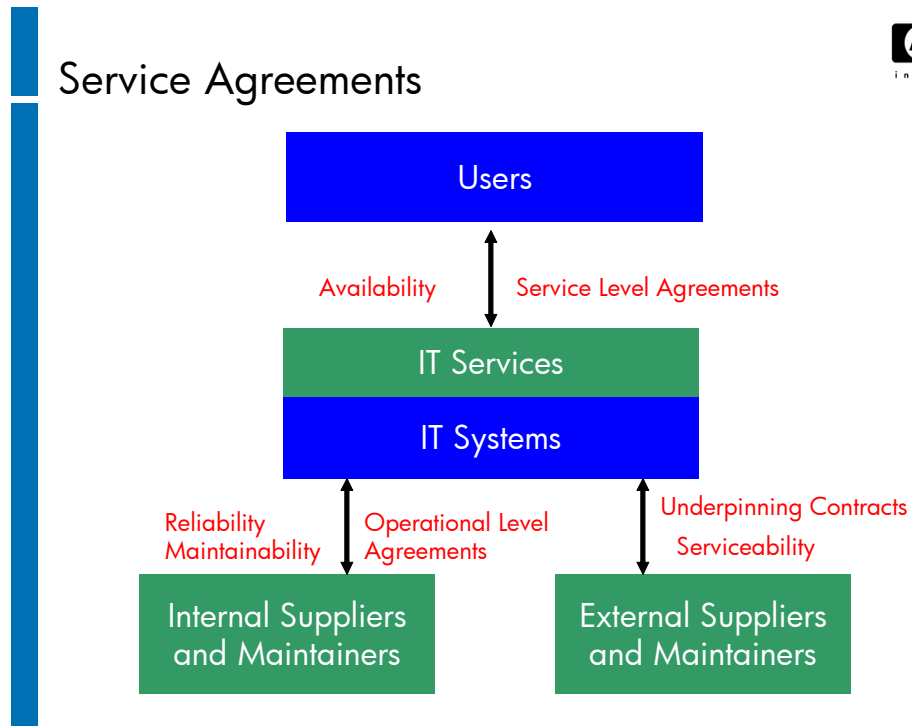
A number of security issues have to be covered by Availability Management:

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

IT Security Management enables and ensures that:

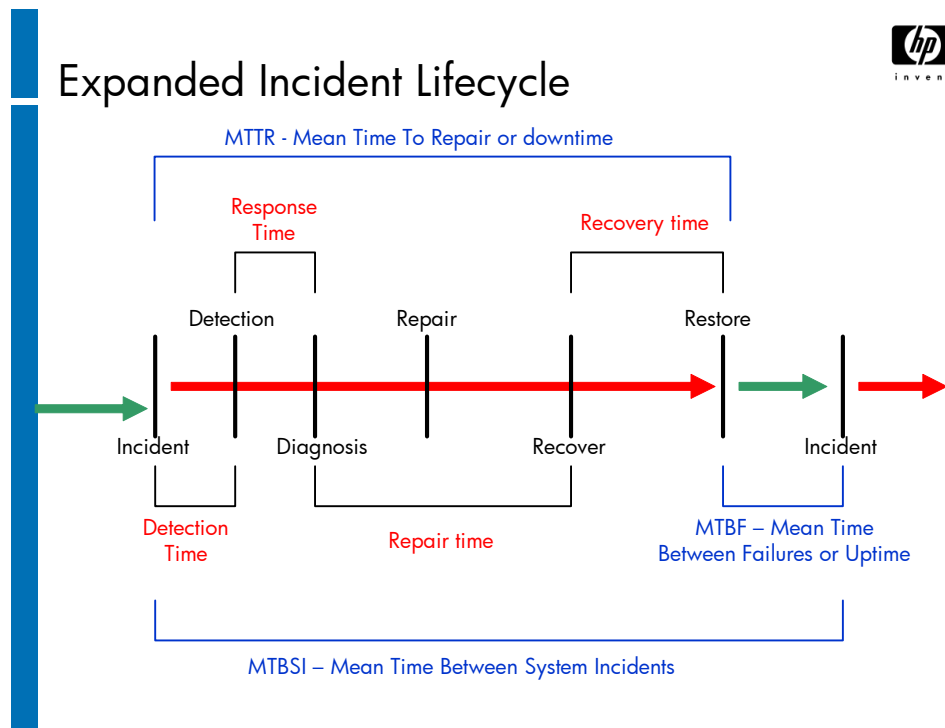
- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, threats, etc
- Security Incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security.

Service Agreements



This slide shows the relationships between the different concepts and which area of the business/documentation they can be found.

Expanded Incident Lifecycle



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

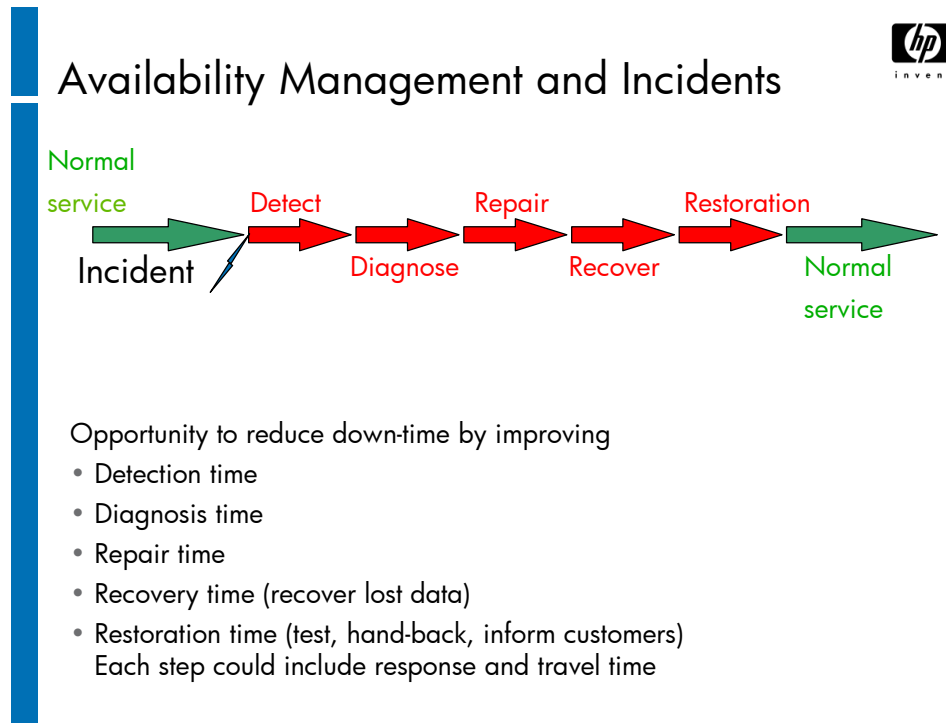
The role of Availability Management in this scenario is to find ways of shortening the elements of downtime, and lengthening uptime. This will be done together with Problem, Change and Capacity Management.

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

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

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

Availability Management and Incidents



Opportunity to reduce down-time by improving

- Detection time – e.g. automated detection tools
- Diagnosis time – e.g. scripting, automated diagnostic tools, better training
- Repair time – e.g. hot swaps
- Recovery time (recover lost data) – backups, standard builds etc
- Restoration time (test, hand-back, inform Customers)
- Each step could include response and travel time

Availability Components



Availability Components

- Design
 - Availability and Recovery
 - Single Point of Failure (SPOF)
 - Risk Analysis
 - Consider Vital Business Functions (VBFs)
- Availability Plan
 - Continuous Improvement
- Measurement
 - Metrics
 - Monitoring
 - Reporting

Designing for Availability and Recovery

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

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

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

Availability Plan

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

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

Availability Measurement and Reporting

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

Techniques and Tools



Techniques and Tools

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

Component Failure Impact Analysis (CFIA)

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

Fault Tree Analysis (FTA)

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

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

The CCTA Risk Analysis and Management Method (CRAMM)

Identifying risks and identifying activities to mitigate them are important activities in availability design and Service Continuity.

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

Service Outage Analysis (SOA)

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

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

The Expanded Incident Lifecycle

Discussed earlier in the chapter under MTBF, MTTR and MTBSI

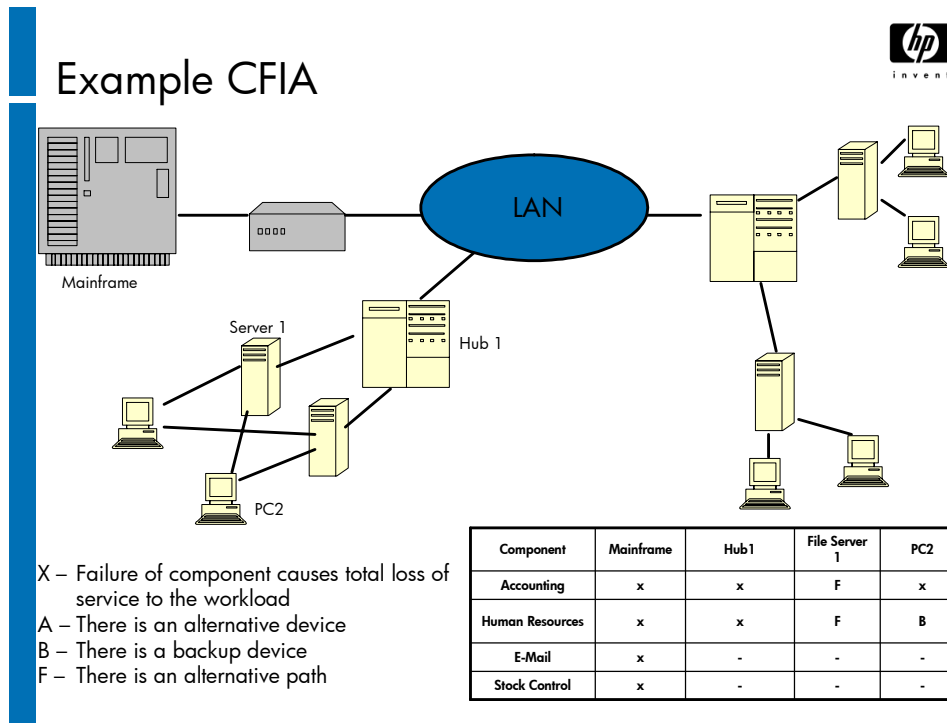
Technical Observation Post (TOP)

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

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

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

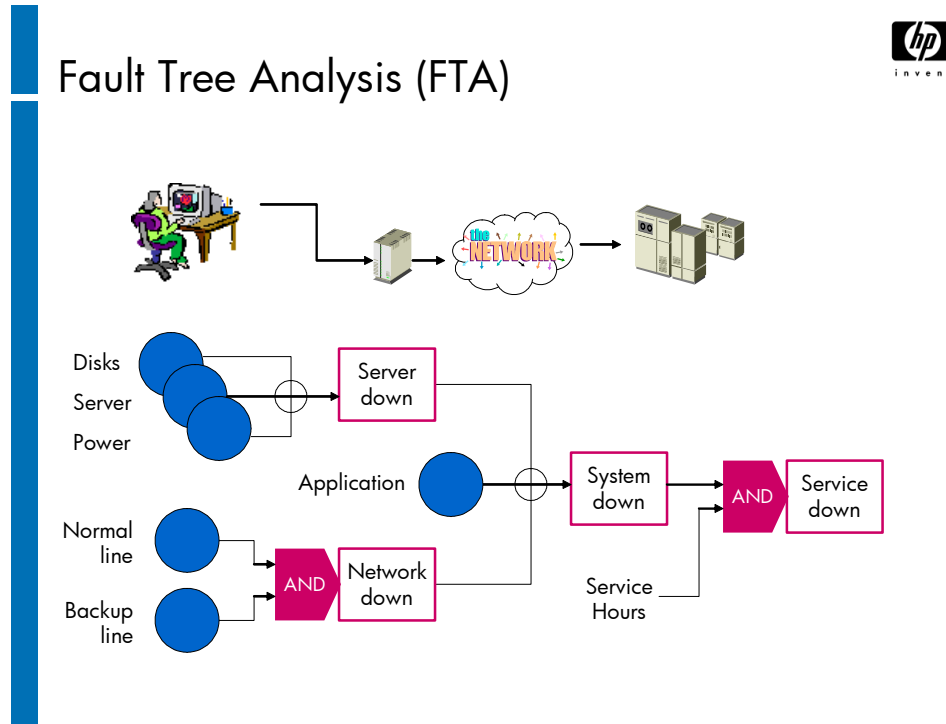
Example CFIA



During the 'design for availability' activities it is necessary to predict and evaluate the impact on IT service availability arising from component failures within the proposed IT infrastructure and service design.

Component Failure Impact Analysis (CFIA) is a relatively simple technique that can be used to provide this information. IBM devised CFIA in the early 1970s with its origins based on hardware design and configuration. However, it is recommended that CFIA be used in a much wider context to reflect the full scope of the IT infrastructure, i.e. hardware, network, software, application and Users.

Fault Tree Analysis (FTA)



FTA makes a representation of a chain of events using Boolean notation. Essentially FTA distinguishes the following events:

- **Basic events** - terminal points for the fault tree, e.g. power failure, disk failure, operator error. Basic events are not investigated in greater depth. If basic events are investigated in further depth, they automatically become resulting events.
- **Resulting events** - intermediate nodes in the fault tree resulting from a combination of events. The top most point in the fault tree is usually a failure of the IT Service.
- **Conditional events** - events that only occur under certain conditions, e.g. Service is down to users only if the system is down and the failure occurred during the time for which the service was agreed to be running (service hours).
- **Trigger events** - events that trigger other events, e.g. power failure detection equipment can trigger automatic shutdown of IT Services.

Availability Management Responsibilities

Availability Management Responsibilities



Which option below is one of Availability Management's responsibilities?

- A. Establish contracts with third party suppliers to ensure critical system availability
- B. Restore IT Services as quickly as possible with minimum disruption to the business
- C. Communicating to users the next IT Services unavailability
- D. Conduct Availability Studies in order to design proper availability and recovery requirements for critical systems that support Vital Business Functions

Continuous Operation

Continuous Operation



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

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

Capacity Management

Module 10

Mission of Capacity Management

Mission of Capacity Management



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

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

Cost against Capacity

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

Supply against Demand

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

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

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

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

Scope of Capacity Management



Scope of Capacity Management

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

Capacity Management will include planning for:

- Hardware
From PCs, through file servers, up to mainframes and super-computers, and also sub-components such as memory, storage devices and processors.
- Software
Operating system and network software, in-house applications, bespoke (custom) software and purchased packages
- Networking equipment
LANs, WANs, bridges, routers, and associated characteristics such as bandwidth, latency, etc.
- Peripherals
Bulk storage devices, printers, tape drives, etc.
- Human resources
But only where a lack of human resources could result in a delay in end-to-end response time
- Environment (or Accommodation)
Cooling, space to host equipment, power, etc.

Objectives of Capacity Management

Objectives of Capacity Management



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

The key objectives are:

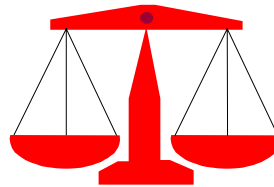
- To ensure that the existing infrastructure is performing optimally in terms of the agreed levels of service
- To understand the way in which the infrastructure is currently being used and will be used in future
- Capacity Management also involves understanding **new technology** and how it can be used to support the business. It may be appropriate to introduce **new technology** to improve the provision and support of the IT Services on which the organization is dependent.
- To build capacity for new services so that existing services are not impacted
- To forecast and plan infrastructure requirements to ensure the ongoing delivery of agreed IT services

Capacity Management

Capacity Management



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



Under capacity causes
performance problems

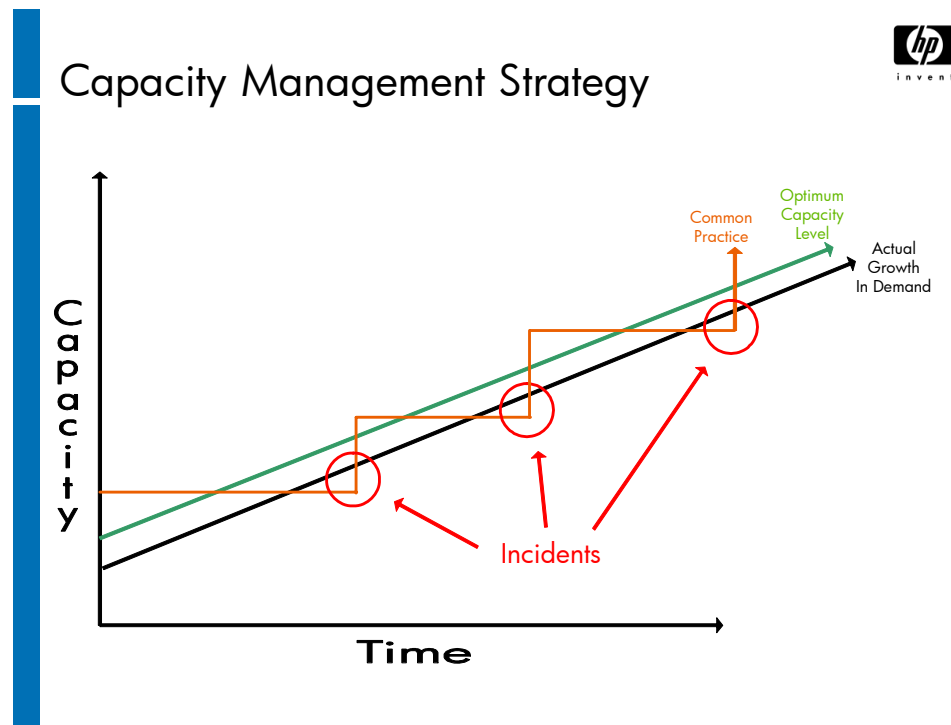
Over capacity is expensive and
increases the cost of services

No Guarantee of meeting all demands

Capacity Management is responsible for ensuring that the capacity of the IT infrastructure matches the evolving demands of the business in the most cost-effective and timely manner. The term, 'cost-effective', is very important:

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

Capacity Management Strategy



This slide shows most organizations approach to Capacity Management (the red line).

An organization has an amount of capacity sufficient for its current operations initially but, as the demand for capacity grows over time, demand outstrips the organization's ability to supply capacity and incidents will start to occur. At that point an organization will often "panic buy" additional capacity to over-compensate for a lack of spare processing capability and provide a short-term contingency. The issue of capacity is then seen to be "solved" and so forgotten about until the next cycle of demand outstripping supply.

This is an expensive scenario, as panic buying is invariably more expensive than planned buying. In an ITIL Capacity Managed environment the organization attempts to follow the green line and provide optimum capacity. This facilitates the planned procurement of capacity and allows for negotiation with alternative sources of supply as well as the opportunity to take advantage of favorable market conditions. Additionally, capacity has historically become cheaper to purchase as technology advances, hence bulk buying is not necessarily the best and cheapest way of buying capacity while the panic buyer has little or no opportunity to evaluate alternatives.

Capacity Management



Capacity Management

- Business Capacity Management
 - Understand future business needs
 - Plan and implement sufficient capacity to support services
- Service Capacity Management
 - Understand IT services, resource usage and variations
 - Ensure that SLA targets can be met
- Resource Capacity Management
 - Understand the utilization of all component parts of the IT infrastructure
 - Optimize use of the current hardware and software resources

Business Capacity Management

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

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

Inputs into this area include:

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

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

Service Capacity Management

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

This last point provides the focus for Service Capacity Management — that of managing service performance as set out in the SLAs.

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

Inputs include:

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

Resource Capacity Management

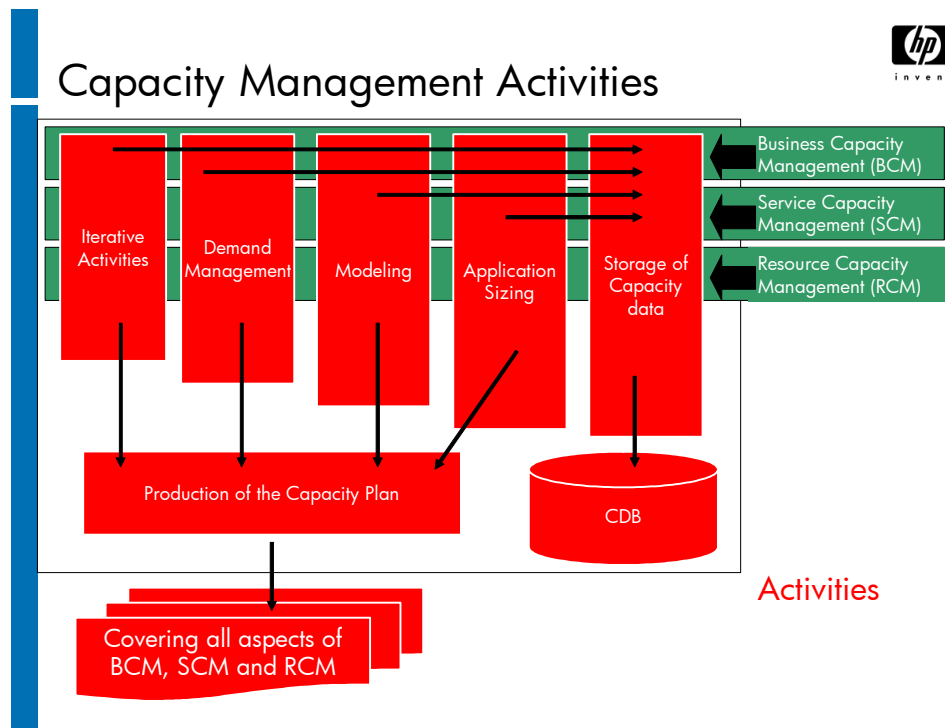
A prime objective of the Resource Capacity Management sub-process is to identify and understand the capacity and utilization of each of the elements (component parts) of the IT infrastructure. The sub-process also maintains awareness of new technologies and developments therein.

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

Inputs include:

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

Capacity Management Activities



The activities in Capacity Management are carried out as follows:

Iterative activities: Ongoing

Demand Management: Ongoing

Data storage in the Capacity Data Base: Ongoing

Application sizing: Ad hoc

Modeling: Ad hoc

Production of the Capacity Plan: Regularly

Iterative Activities (Performance Management) (1 of 2)

Iterative Activities (Performance Management) (1 of 2)



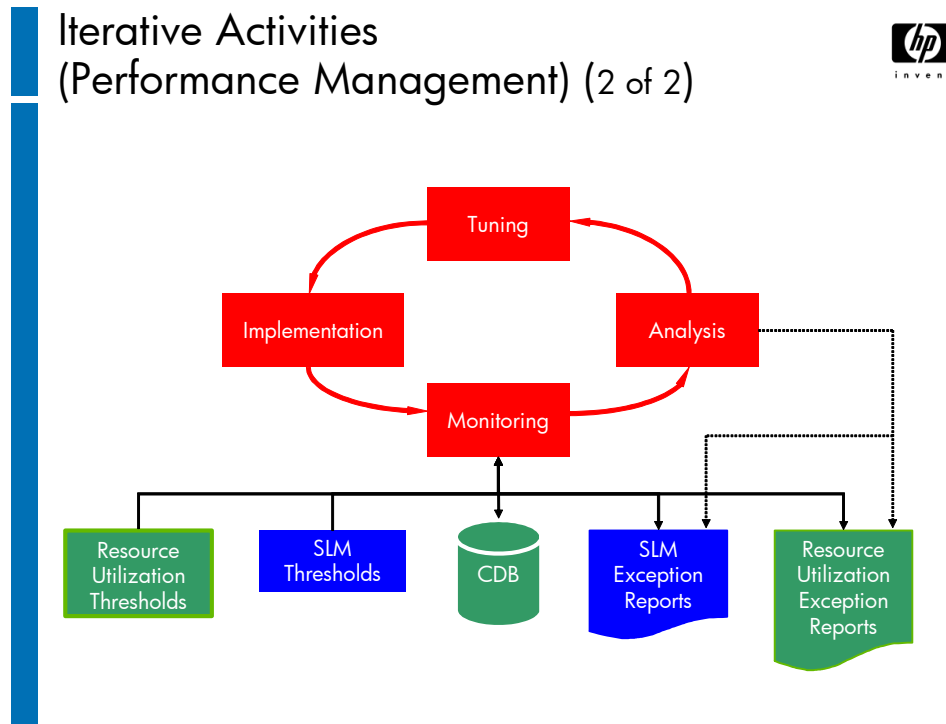
- Focus on meeting agreed service levels
- Ensure optimum performance of resources
- Learn to prevent problems
- Main activities:
 - Monitor
 - Analyze
 - Identify tuning measures
 - Implement tuning measures

The term “Iterative Activities” is also used for Performance Management.

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

More information on the main activities is on the next slide.

Iterative Activities (Performance Management) (2 of 2)



There are four major activities in Iterative Activities (Performance Management):

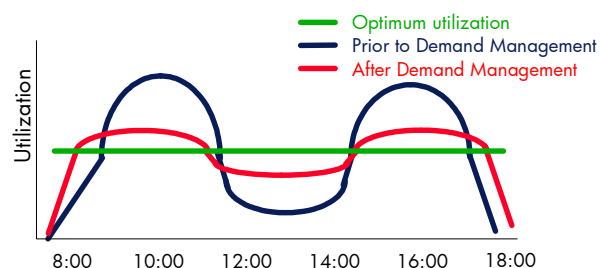
- **Monitoring** is aimed at ensuring that resources and services perform as required to meet the terms of the SLAs. It includes items regarding capacity (e.g. throughput) and performance (e.g. response time). Monitoring is performed on the basis of thresholds set by technical specifications and Service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

Demand Management



Demand Management

- Reactive and Proactive Capacity Management
- Managing demand where capacity is limited
- Resources allocated by business priority
- Influence User behavior
- Increased or reduced charges for specific resources or times
- May require specific restrictions or concurrency levels



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

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

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

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

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

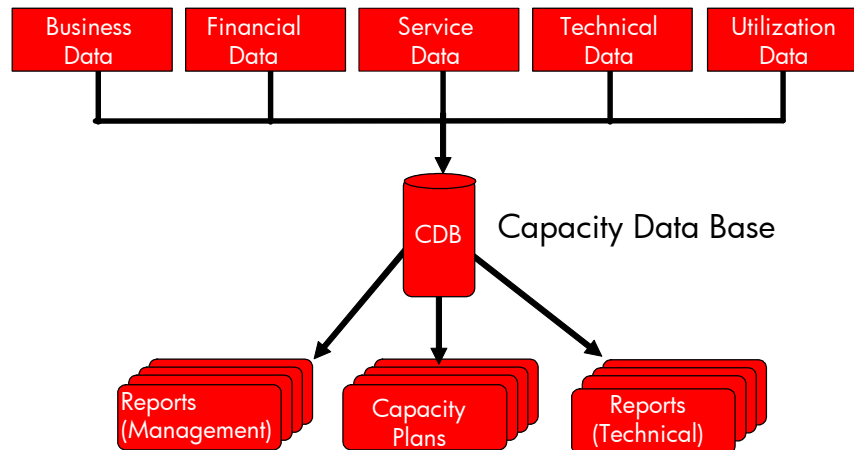
To better control the workload, the demand for the resources needed can be controlled by a number of processes. Prime among these is to control demand by pricing, differential charging is sometimes used to encourage utilization during off-peak times.

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

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

Capacity Database (CDB) Inputs and Outputs

Capacity Database (CDB) Inputs and Outputs



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

Inputs to the CDB:

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

The CDB is used to produce:

- Management reports
- Capacity Plans
- Technical reports

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

Application Sizing



Application Sizing

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

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

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

Modeling

Modeling



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

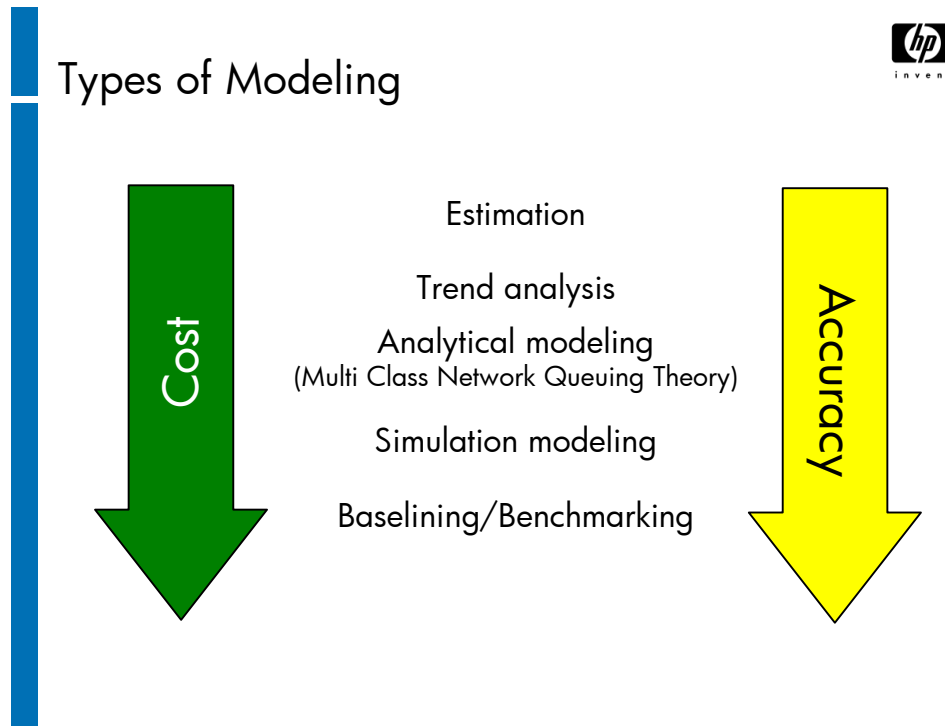
- Answers “What if....?” types of questions under different scenarios
- Be performed at a minimal on a quarterly basis or more frequently if the organization is under a significant period of change

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

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

- Specific configurations
- Specific workloads
- Combinations of workloads

Types of Modeling

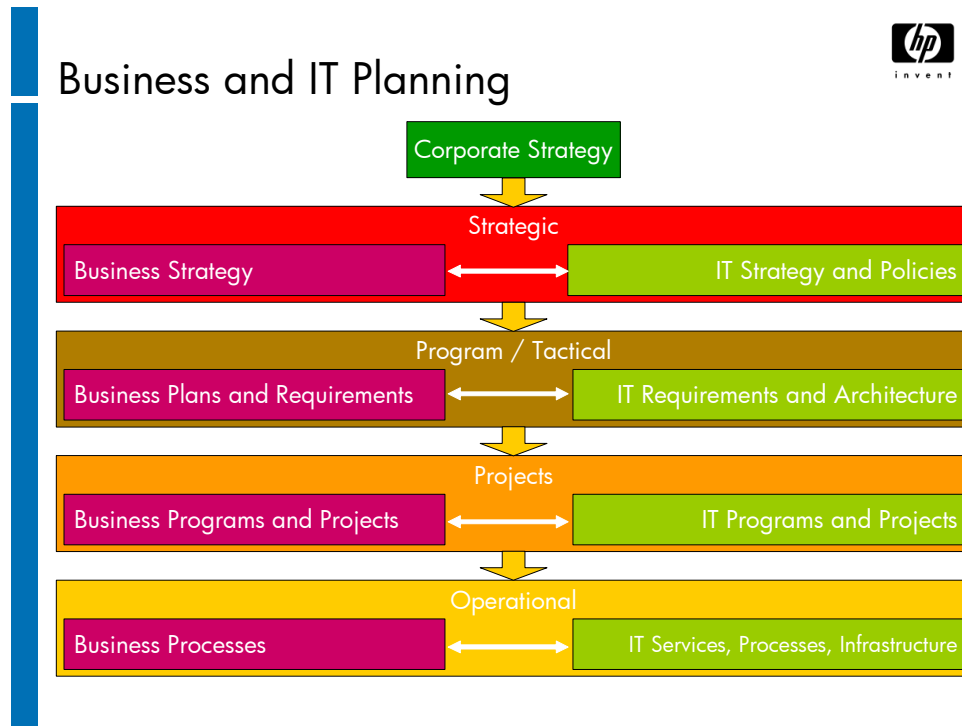


There are five different types of modeling shown here in increasing order of cost and accuracy:

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

- **Simulation Modeling** is used to model discrete events against a specific configuration. This is usually done in a dedicated environment such as a laboratory. Simulation tools that simulate transactions or network traffic are also available.
- **Benchmarking** is an extreme form of simulation modeling where the entire operational environment is replicated or simulated. Workloads are produced to replicate the live environment. The variables are then manipulated or introduced and the actual effect measured.

Business and IT Planning



IT planning takes place at many levels, from strategy through to operation infrastructure planning and is greatly influenced by all levels of business strategy and planning.

It is important that the ICT strategy is:

- Aligned with business strategy and plans
- Appropriate, realistic and achievable
- Business focused
- Balanced between short, medium and long term objectives
- Timely and feasible
- Cost-effective
- Includes implementation milestones that are measurable

Capacity Planning



Capacity Planning

- Planning capacity requirements:
 - Forecast saturation point
 - Identify action to prevent
- Two year period
- Revised every three months
- Uses business plans and data to create scenarios
 - Stored in CDB

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

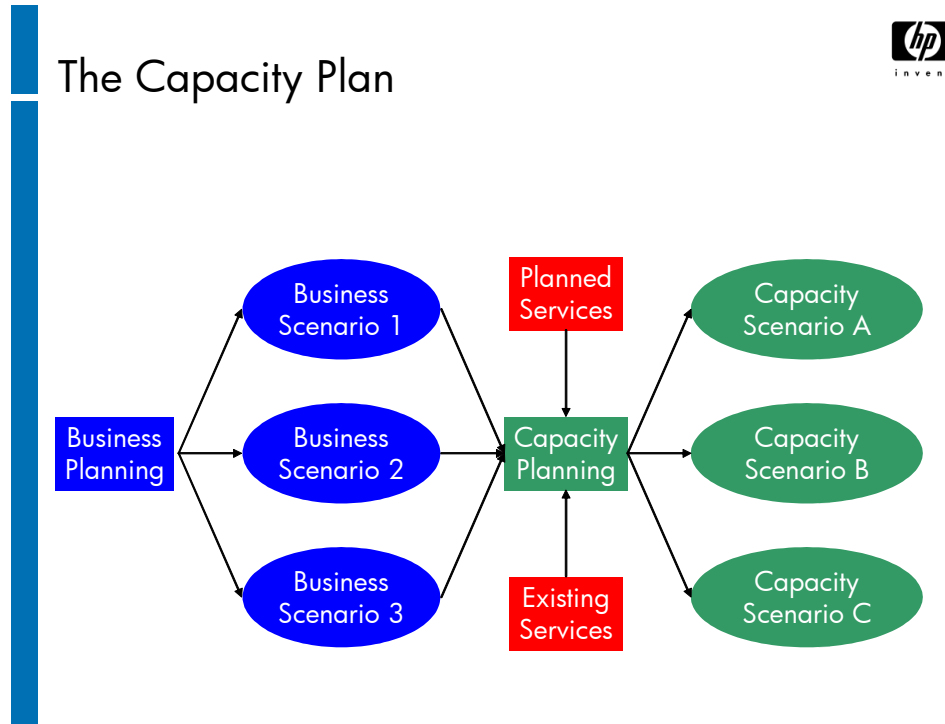
In short, the capacity plan predicts when the system is going to reach saturation point and then identifies what action should be taken to prevent it.

Planning is often done over a one to three-year cycle which can be reviewed quarterly or every six months. The planning process uses scenarios to increase accuracy and is stored in the Capacity Data Base.

Scenario planning is a technique used to identify potential changes in IT usage and consumption patterns. Business data, including the information listed below, is used to predict, as precisely as possible, necessary prospective changes to the IT infrastructure and resourcing model to accommodate changing and emerging business requirements:

- Future business plans
- Number of users/number of calls to the Service Desk
- Number and location of offices/number of Desktops
- Anticipated workloads/seasonal variations
- Web site transaction data

The Capacity Plan



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

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

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

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

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

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

Information Needed for Capacity Management

Information Needed for Capacity Management



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

1. Financial data
 2. Business data
 3. Technical data
 4. Service data
-
- | | |
|----------------|----------------|
| A. 1 and 2 | B. 2 and 4 |
| C. 2, 3, and 4 | D. All of them |

Service Capacity Management



Service Capacity Management

Which of the these is NOT a purpose for which Service Capacity Management information can be used?

- A. DSL Control
- B. Systems throughput calculation
- C. Network performance analysis
- D. Demand Management

Financial Management

Module 11

Mission of Financial Management

Mission of Financial Management



To provide **cost effective stewardship** of the IT assets and the **financial resources used in providing IT services**

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

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

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

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

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

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

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

Scope of Financial Management

Scope of Financial Management



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

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

Budgeting

Forecasting, control and monitoring of expenditure

IT Accounting

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

Charging

Billing Customers for services

Objectives of Financial Management

Objectives of Financial Management



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

The objectives reflected in this mission statement are:

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

Budgeting

Budgeting



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

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

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

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

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

IT Accounting

IT Accounting



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

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

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

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

Cost Types and Cost Elements



Cost Types and Cost Elements

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

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

The IT Accounting System — Cost Models

The IT Accounting System — Cost Models



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

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

Cost Classification

Within each cost element there are different types of cost that will behave in different ways. There are six broad cost categories:

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

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

Any Indirect Costs, which cannot be apportioned to a set of Customers (sometimes called Unabsorbed Overheads), have then to be recovered from all Customers in as fair a way as is possible, usually by uplifting the costs calculated so far by a set amount. This ensures that the sum of all of the costs attributed to each Customer still equals the total costs incurred by the IT organization
- **Fixed** — Costs that do not vary even when resource usage varies are referred to as Fixed Costs (e.g. a maintenance contract for a piece of hardware, or a corporate software license).
- **Variable** — Variable Costs are those that vary with some factor, such as usage or time. They are likely to be used for cost elements which cannot be easily predicted (e.g. out-of-hours cover, major equipment re-location, and the production of additional quarterly reports).
- **Depreciation** — This is an accounting entry, which allows the organization to reduce the value of assets based on the time they have been in use, or their amount of usage.

Cost Units

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

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

- Identify the direct costs of the service (e.g. supporting a payroll system)
- Apportion the indirect costs (e.g. the Service Desk)
- Divide by the projected number of times that service will be used (e.g. number of transactions)
- Add the two figures together
- Add any variable cost (e.g. telephone charges)

Cost Centers

There are 3 types of accounting organization in ITIL:

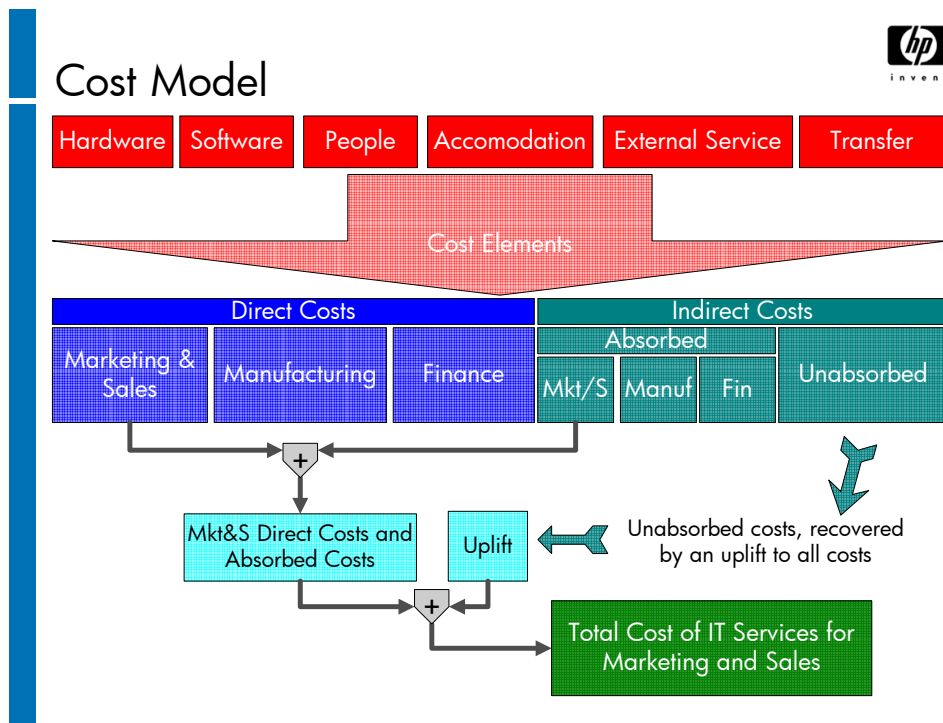
- **Accounting Center** — This type of organization simply identifies the costs of providing service, and may do some budgeting. The focus is on measuring performance and conducting investment assessment.
- **Recovery Center** — This is where the organization analyses its full expenditure and investments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

Monitoring

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

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

Cost Model



This is an example for a Cost Model using Cost-by-Customer calculation, but the same principles can be applied to calculating the costs of individual application services (cost-by-service) or even parts of a service e.g. support and maintenance.

It is assumed that there are 3 businesses or departments, who together are responsible for all of the IT costs. They are Marketing and Sales, Manufacturing and Finance and all of the IT systems and services have been implemented on their behalf.

All three departments have direct and indirect (absorbed and unabsorbed) costs:

- The direct costs for Marketing and Sales are the ones we can clearly attribute to this customer.
- Other costs, such as operations staff or provision of power cannot easily be attributed to a specific customer. These are the indirect or shared costs. In our example we may be able to reliably establish that 90% of the indirect costs are incurred by just two of the three departments. These are the absorbed indirect costs.
- Any other costs (the remaining 10% in this example), which we cannot reliably attribute to any particular customer or subset of the customers will be split equally across all customers. We will charge them an equal amount each. This allows the IT department to recover those remaining "unabsorbed" costs. Now all IT costs have been recovered and in a manner that should appear equitable to all customers.

Investment Appraisal



Investment Appraisal

Evaluation of the financial benefits of alternative IT solutions

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

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

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

There are several types of IA, including:

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

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

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

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

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

Charging

Charging



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

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

Its main aims are to:

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

When Do You Charge?



When Do You Charge?

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

ITIL suggests the ideal charging environment is where:

- Users are in control of their own budget, allowing them to decide when, where and how much to spend on IT Services. Users have an element of choice in their level of usage of the IT services, both overall and at particular times. Where Users can choose between using the in-house IT Services organization or outside suppliers, charging becomes particularly important because Users can choose based on the relative quality and price of services offered.
- Agreements permit changes to planned charges or to capacity available during the agreements period. When IT wants to charge for an annual period to guarantee revenues, new resource requirements can be committed to meet the needs of particular customers, so it may be necessary to build a clause allowing this flexibility into any agreement for the provision of such services.
- In a Profit Center IT Finance Management will probably wish to set prices for a period (e.g. 1 year) to be able to predict revenue. Should capacity demands change it would be necessary to have the flexibility to change capacity provided or re-balance the capacity provided to new or different customers. This flexibility should be built into service level agreements

- Users already paying for other services in the organization, e.g., occupancy or environmental costs, will be less inclined to respond negatively to IT Services charges.
- No Charging System will be adequate, especially if charging by resource usage is the method, without effective monitoring of IT customers and their resource utilization.

Benefits of Charging



Benefits of Charging

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

- Once Customers realize that an IT service has a cost associated with it, they will most likely use this service in a more cost-conscious way. When Users have the perception of a “free” service, they tend to waste resources. A good analogy is the difference in the amount of food people consume at an all-you-can-eat buffet versus an a la carte restaurant.
- Allows comparisons between the internal IT organization and external IT providers.
- Differential Charging describes the technique of charging customers different rates during specific periods for the same service. This is typically used to decrease demand or to generate revenue where spare capacity exists.
- We should recover IT costs in an equitable manner according to IT demands, allowing IT to maintain integrity, consistency and good relationships with each customer or group of customers.
- By informing Users how charges are derived, it will allow them to influence usage/charges.
- When the business objective for IT is to be a profit center, charging will be required to provide the expected income/profit margin for IT.

Problems of Charging



Problems of Charging

- Cost of implementing and running charging system
- Allocation of running costs to Customers
- Negative reaction to IT costs and charges due to increased visibility
- Perception of poor value for money
- Failure to differentiate between internal and external money
- Failure to make equivalent comparisons

- Implementing and operating a charging system requires hardware, software, specialized personnel, training or external consulting services. Consideration should be given with respect to the benefits of charging over the cost of implementation and administration.
- In order to benefit from economies of scale, the IT organization might increase the number of Users of its services, thus decreasing the unit costs associated with the infrastructure necessary to support those services. However, the greater the number of Customers, the more difficult it can be to accurately allocate the costs to Customers.
- When costs become visible to users, some of those Users might be unwilling to pay the higher costs and can react negatively and even refuse to pay.
- Customers may feel that the charges for the services received are too high or higher than they might pay for externally provided services. This is likely to result in a perception of poor value for money.
- Once charging is in place, Customers may fail to differentiate between internal and external money; i.e. external money is a real cost to the business whereas internal money is a transfer cost and doesn't incur taxes etc.
- Users might fail to make equivalent comparisons, e.g. a PC on their desk doesn't only cost the retail or wholesale price of the PC but also has to include the infrastructure costs, support costs, etc.

Charging and Pricing Policies



Charging and Pricing Policies

- Determine Charging Policy
- Chargeable Items
- Pricing Policy
- Pricing Methods:
 - Cost
 - Cost Plus
 - Going Rate (Internal)
 - Market Rate (External)
 - Fixed Price

Determine Charging Policy

The type and configuration of a charging system will be determined by four main factors:

- Level of recovery required
- The need to influence user behavior
- Ability to measure usage
- Level of control of the internal market

Chargeable Items

This is the process of identifying exactly what the Customers will be charged for. The User should see these items as a unit. Both fixed and variable costs should be identified for each chargeable Item.

Pricing Policy

This is the process of identifying exactly how much money the charging process should recover.

Since the level of pricing has a direct impact on the demand for the service, these factors should be taken into account:

- What is the pricing objective?
- What is the true demand for the service?
- Accurate determination of direct and indirect costs
- The level of control of the internal market
- What services are available externally if customers have a choice
- What are the legal, regulatory and tax issues
- Are the Customers “tied” or “untied”?

In many IT organizations, Customers are “tied” to using the internal IT Services. In an “untied” situation charging becomes particularly important because it enables Customers to choose between using the in-house IT Services organization or outside suppliers, based on the relative quality and price of services offered

Pricing Methods

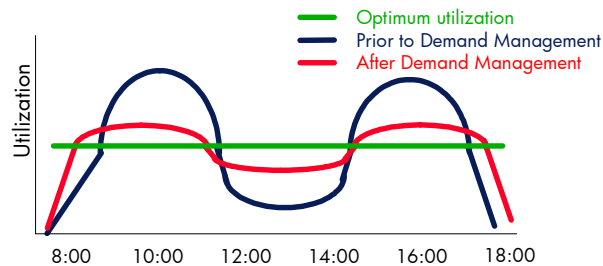
| | |
|-------------|--|
| Cost | The exact cost of service provision |
| Cost-Plus | The mark-up could be set as a fixed percentage or as a target return on investment |
| Going Rate | This is where the cost is similar to other internal departments or to similar organizations |
| Market Rate | This is the price quoted by an external supplier, which could be lower than the internal IT department because of economies of scale |
| Fixed Price | IT and the customers agree on a price for the planning or delivery period, regardless of usage. |

Differential Charging



Differential Charging

- Setting different charges during specific periods
 - For example applying higher charges at peak times, lower charges off-peak
- Used to influence demand



Charging business Customers different rates during specific periods for the same work, typically to dampen demand or to generate revenue for spare capacity. This can also be used to encourage off-peak or night time running e.g. applying higher charges during peak times and lower charges off-peak.

Billing

Billing

Bills must be:

- Simple
- Understandable
- Justifiable

Options:

- Information only
- Notional
- Full/Hard charging



Billing is the process of producing an invoice and recovering the funds from the customer. Billing cycles must be aligned to the business financial cycles to ensure that there is no negative impact on cash flow.

There are three objectives billing:

- Bills must be simple, clear and matched to the ability to pay
- Chargeable Items must be understood by the user
- IT accounting data must be available to back up the bills

Charging information is passed to Customers to make them aware of the cost of the resources used by their business. The options to accomplish this are:

- Calculating and circulating to business managers the full details of the cost of providing each business's IT or services (No Charging or Information Only)
- Same as above, but including details about how much the IT organization would charge, should a charge-back system be operated, without applying transactions to the financial ledgers (Notional Charging)
- Same as above, but applying transactions to the financial ledgers (Full or Hard Charging).

Pricing Methods



Pricing Methods

An IT Department is seeking to set its prices to match those of external suppliers selling comparable services. Which of the following is the best description of this approach?

- A. Market Rate
- B. The going rate that is agreed with Customers
- C. Cost-plus
- D. Profitable

When to Set Charging



When to Set Charging

Consider the following statements:

- It is impractical to introduce an effective charging regime without knowing the true cost of providing IT services
- Charging for IT services is a pre-requisite, or mandatory, for introducing service level agreements

Which is correct?

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

IT Service Continuity Management

Module 12

Mission of IT Service Continuity Management

Mission of IT Service Continuity Management



To support the **overall Business Continuity Management** process by ensuring that the **required IT technical and services facilities can be recovered** within required and agreed business time scales

The goal of IT Service Continuity Management (ITSCM) is to ensure that the required IT technical and services facilities can be recovered within required and agreed timescales.

IT Service Continuity planning is a systematic approach to the creation of a plan and procedures — which are regularly tested and updated — to prevent, cope with, and recover from the loss of critical services for extended periods.

Scope of IT Service Continuity Management

Scope of IT Service Continuity Management



- IT services that support critical business processes
- Identifying and minimizing impact
- Agree the minimum level of business operation following a service disruption
- Does not directly cover longer-term risks
- Does not cover minor disruptions and faults

ITSCM focuses on all IT services that are needed to keep critical business processes functioning. It is also responsible for identifying and minimizing any potential impact on those critical business processes.

ITSCM should agree the minimum level of business operation following a service disruption.

ITSCM does not directly cover longer-term risks such as those from changes in business direction, restructuring, etc. It also does not cover risks of minor disruptions and faults.

Objectives of IT Service Continuity Management

Objectives of IT Service Continuity Management



- Reduce the vulnerability of the organization
- Reduce identified risks
- Plan for recovery of business processes
- To involve 3rd parties to mitigate risk
- Reduce the threat of potential disasters
- To prevent loss of Investor confidence

- To reduce the vulnerability of the organization by maintaining or preserving IT services
- To reduce or avoid identified risks
- To plan for the recovery of key IT services that support critical business processes
- To transfer all or part of the risk to a third party (e.g. insurance or outsourcing)
- To reduce the impact of potential disasters
- To prevent the organization from losing investor confidence

Business and IT Responsibilities

Business and IT Responsibilities



Business Continuity

- Business Processes
- Facilities
- Business Staff
- Strategy for Business Continuity

IT Continuity

- IT Services
- Systems
- Technical Staff
- Strategy for IT Continuity

The dependencies between business processes and technology are now so intertwined that Business Continuity Management (BCM) incorporates both a business element (Business Continuity Planning — BCP) and a technology element (IT Service Continuity Management Planning — ITSCM). Their dependencies on each other determine that one is a sub-set of the other, depending on the nature of the business and the extent to which technology has pervaded the organization. Therefore it is often understood that business continuity is the main driver and that IT Service Continuity Management is a sub-set of the Business Continuity Management process.

Business Responsibilities

The Business is responsible for managing business continuity risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur as a result of a risk.

Business Continuity Management is concerned with the management of Business Continuity that incorporates all services upon which the business depends, one of which is IT.

The minimum business requirements must be determined and agreed between the business and the IT service providers (internal or external) prior to the definition of the scope of ITSCM. It is vital that the prerequisites for recovering services are fully understood, defined and agreed by the business.

- Business Processes
- Facilities
- Business Staff
- Strategy for Business Continuity

IT Responsibilities

ITSCM is a part of the overall Business Continuity Management process and is dependent upon information derived through this process.

The purpose of IT Service Continuity Management is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required, and agreed, business timescales.

- IT Services
- Systems
- Technical Staff
- Strategy for IT Continuity

Possible Threats

Possible Threats

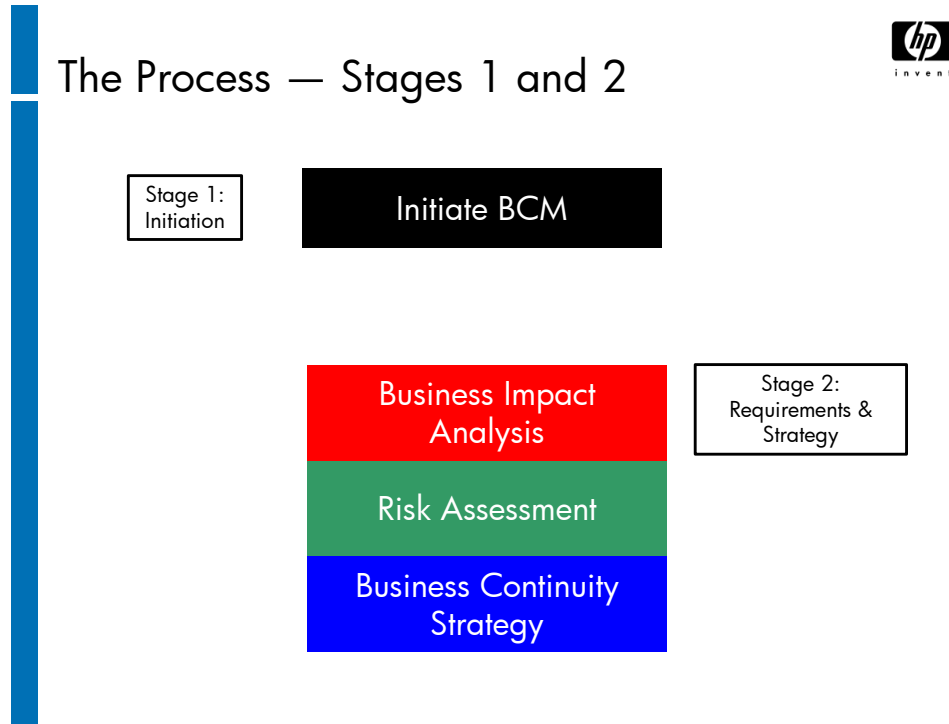


- Damage and denial of access
- Loss of critical support services
- Failure of critical suppliers
- Human error
- Technical error
- Fraud, sabotage, extortion, espionage
- Viruses or other security breaches
- Industrial action
- Natural disasters

The risks to be addressed, e.g., loss of internal IT systems/networks, loss of data, failure of service providers, etc., are those that could result in a sudden and serious disruption to the business, caused by threats:

- Damage or denial of access to premises (terrorism, fire, flood or other physical disasters)
- Loss of critical support services such as telecoms and power
- Failure or non-performance of critical suppliers
- Human error
- Technical error or environmental unit breakdown
- Fraud, sabotage, extortion or commercial espionage
- Infiltration of IT systems by viruses
- Other security breaches
- Industrial action or other unavailability of key staff
- Natural disasters

The Process — Stages 1 and 2



Note that Stage 1, Initiate BCM, is a joint project between the business and IT.

Business Impact Analysis (BIA)



Business Impact Analysis (BIA)

- Purpose:
 - Identify key IT services
 - Determine the effect of unavailability
 - Investigate the time before the effects are felt
 - Assess minimum recovery requirements
 - Document with the business
- Impact scenarios

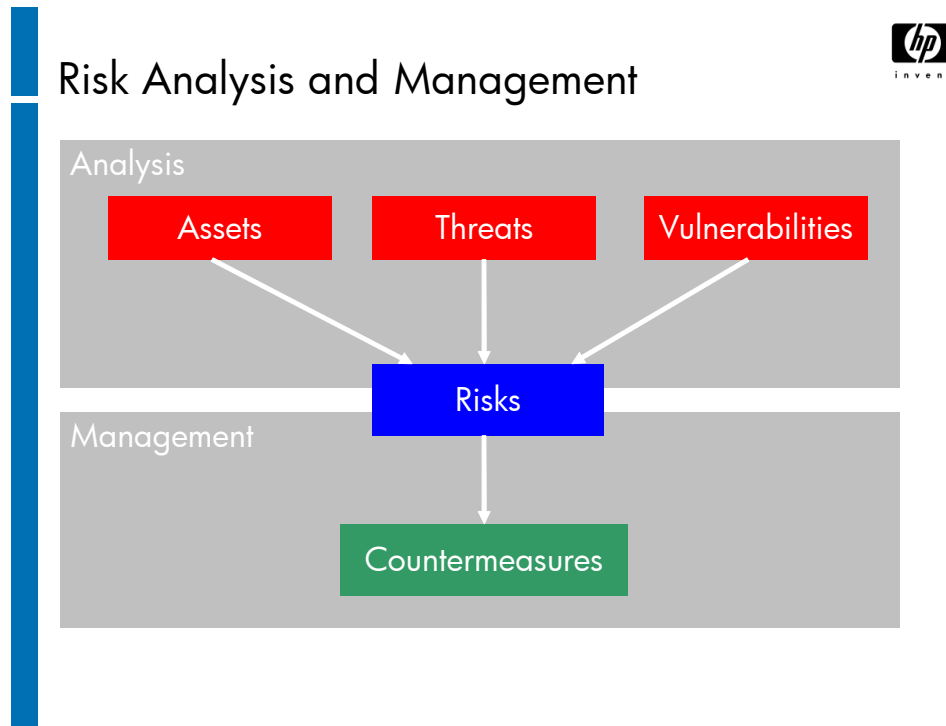
The **purpose** of a business impact analysis is to identify:

- Which IT services support critical business processes
- The damage or loss for the organization if they were unavailable
- The time before those impacts would be felt

This is done using **impact scenarios**, which identify different combinations of service unavailability, and assess the effect of each on the business. This also helps to identify:

- The form that the damage or loss may take
- How the damage or loss could escalate after an incident
- The minimum staffing, facilities and services necessary for business processes to operate at a minimum acceptable level
- The time within which these should be recovered
- The time within which business processes and all supporting staff, facilities and services should be fully recovered

Risk Analysis and Management



ITSCM can now assess just how likely it is that a disaster (or partial disaster) could affect the critical services. This can be done using a tool or methodology such as CRAMM (the CCTA's Risk Analysis and Management Method) to take the following steps.

- Identify the assets that support the key IT services
- Assess the threat
- Assess the vulnerability
- Assess the probability of the risk

Definitions

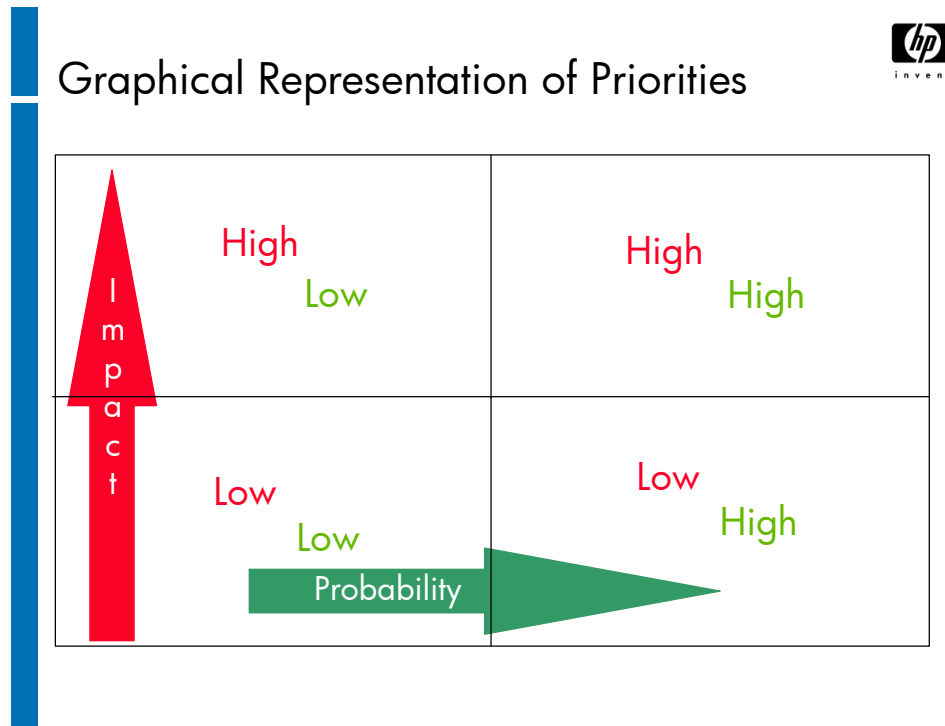
Risk - A measure of the exposure to which an organization may be subjected. This is a combination of the likelihood of a business disruption occurring and the possible loss that may result from such business disruption.

Threat – The possible causes of disruption that might prevent the delivery of services. Threats act upon the assets of an organization or service.

Vulnerability - A weakness of a service and its constituent CIs (assets) which could be exploited by threats.

Countermeasure - An action taken to reduce risk. It may reduce the 'value' of the asset, the threats facing the asset or the vulnerability of that asset to those threats.

Graphical Representation of Priorities



Using an approach like CRAMM requires confidence that:

- All risks and countermeasures have been identified
- All threats and vulnerabilities have been identified and their levels accurately assessed
- All results are consistent across the broad spectrum of the IT infrastructure reviewed
- All expenditure on selected countermeasures can be justified

Service Continuity Strategy



Service Continuity Strategy

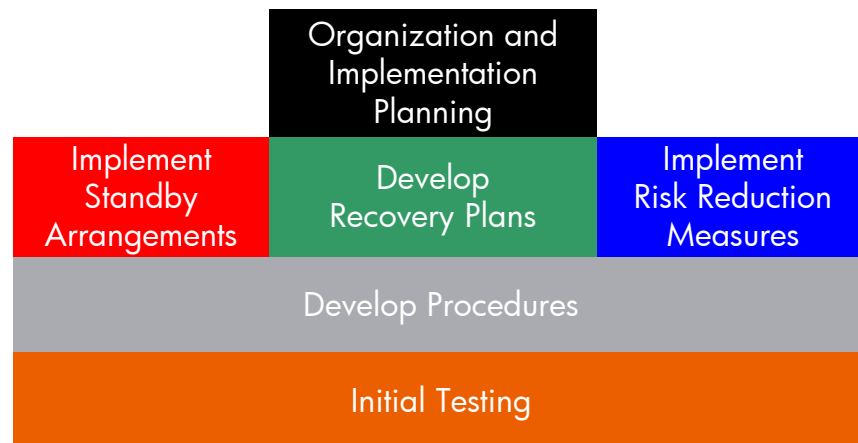
- Which services will we plan for?
- What recovery and preventative options are available?
- What are the costs of each?
- Which services take priority in recovery?

The strategy will outline:

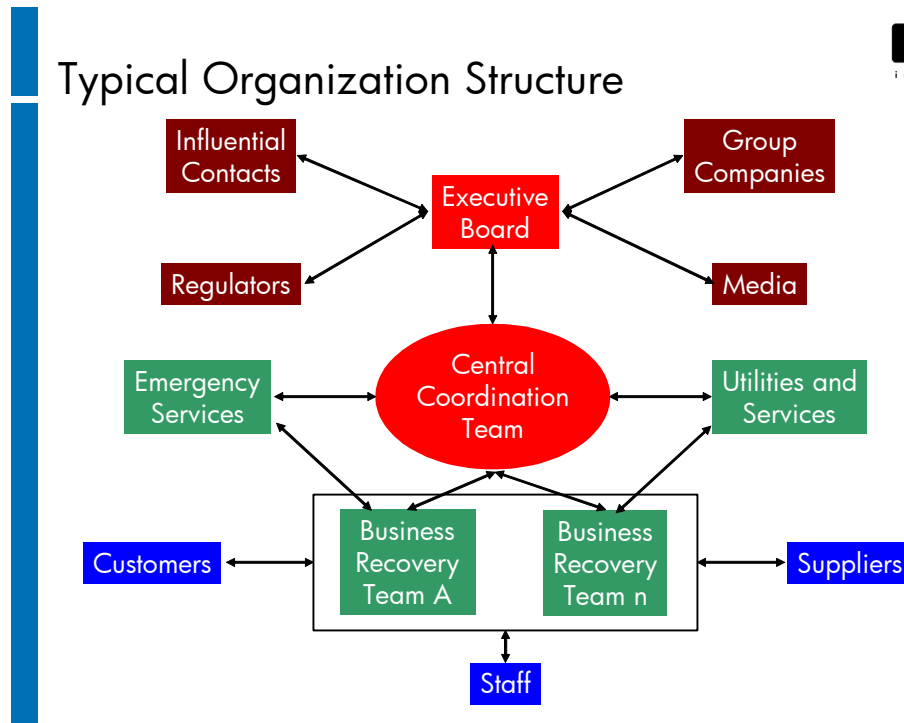
- The services to be included in the Continuity Plan
- What recovery and prevention alternatives will be chosen for each
- The costs of the alternatives
- The priorities for recovery

The Process — Stage 3 (Implementation)

The Process — Stage 3 (Implementation)



Typical Organization Structure



The organization for ITSCM must include:

- **Executive Board:** retain overall authority and control within the organization and will also be responsible for:
 - Crisis management
 - Public relations
 - Liaison with other departments or group companies, the media, regulators, influential contacts, etc.
 - Executive decisions
- **A central coordination team:** consists of people one level below the executive board. They have a good overall understanding of the business processes and priorities, and have operational control over the groups that will invoke stand-by arrangements and recover the business.
 - Overall Recovery Manager, who manages the central coordination team
 - Critical business process or function coordinators
 - Key support function coordinators (including IT)
 - Coordinators for any other critical activities

- **Business Recovery teams:** are responsible for implementing the business recovery plans for their own areas and for day-to-day liaison with staff, Customers and suppliers. A business recovery team may support each coordinator on the central coordination team.

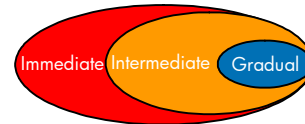
Please note that the planning process must create the appropriate authority for each team or individual to make decisions and take action during a contingency. This authority must be clearly designated in the continuity plans.

Standby Arrangement/Risk Reduction

Standby Arrangement/Risk Reduction



- Standby Arrangement
 - Do nothing
 - Manual workarounds
 - Reciprocal arrangements
 - Dormant contracts
 - Insurance
 - Immediate recovery – hot standby (<24 hrs)
 - Intermediate recovery – warm standby (24-72 hrs)
 - Gradual recovery – cold standby (>72 hrs)
- Risk Reduction Measures
 - Backup/Recovery
 - Fortress Approach
 - Resilience/SPOF elimination



The steps involved in implementing stand-by arrangements include:

- Negotiating and agreeing on the terms for third party recovery facilities
- Preparing and equipping the stand-by site
- Purchasing and installing stand-by equipment
- Ensuring that the recovery contractor is covered by continuity plans

There are a number of options for recovery planning. These include:

- **Do Nothing** — for non-critical or transitional services
- **Manual Workarounds** — Users do some of the work manually as an interim measure. This usually requires temporary staff. Most business critical applications are difficult to reproduce manually. Also, in many cases, the data has to be available before the work can be done
- **Reciprocal Arrangements** — this is an agreement between organizations to use one another's facilities in a disaster. This may work for batch jobs or storage, but is not really feasible in complex and distributed environments. There are also capacity, maintenance and security issues to consider

- **Dormant Contracts** — suppliers agree to keep stock of certain items, which will be available at a fixed price through the year.
- **Insurance** — This is an important element, regardless of which option is chosen, but it is not a replacement for proper stand-by options
- **Immediate Recovery (Hot Standby)** — this is an alternative site, already running critical systems, to be used when the main site is inaccessible or unusable. The recovery time is usually less than 24 hours and generally within 24 hours. Business critical systems are mirrored on the alternative site.
 - **Internal** — within the organization, although not usually in the same building.
 - **External** — provided by a third party supplier and shared by several customers
 - **Mobile** — specific facilities in a truck, which can be transported to the main or alternative site
- **Intermediate recovery (Warm Standby)** — this is similar to Immediate Recovery except that critical systems need to be recovered and run. This usually takes between 24 and 72 hours. There are 3 types of warm standby facility:
 - **Internal:** This is a spare site maintained internal to the organization. It is very expensive, and therefore often used for testing or development. If this is the case, further alternatives may need to be planned
 - **External:** Third parties normally provide these sites for an annual fee, which reduces the cost and shares the risk, but they are often located remotely. Also there is a greater chance of multiple hits. If the site is invoked, there is an additional daily fee, which usually increases the longer it is used. Most commercial sites limit their cover to between 6 and 12 weeks. This is to reduce the risk of multiple hits.
 - **Mobile:** Computer facilities in a truck or trailer, which is driven to an agreed site for a call-out fee. The amount of equipment is limited by the size of the truck. Special licenses may have to be obtained for parking and running the facility
- **Gradual Recovery (Cold Standby)** — an empty facility, with utilities, support staff and telecommunications equipment, that is ready to accommodate new computer equipment. This is used if the new equipment has been delivered but the base site is not ready to receive it. There are two types of cold standby:
 - **Fixed** — usually provided as a remote facility by a third party, or as a permanent site owned or rented and maintained by the organization itself
 - **Portable** — normally a prefabricated building erected at a site predetermined in the contract

Most organizations have to adopt a balanced approach where recovery (using a standby arrangement) and risk reduction measures are complementary and both are required. Here some examples of typical risk reduction measures:

- A comprehensive **backup and recovery** strategy, including off-site storage
- **Fortress Approach** — An approach to IT Service Continuity where the entire IT site is made as disaster-proof as possible
- **Resilience/single points of failure (SPOF) elimination** — such as a single power supply line into a building or WAN link from a single telecommunication provider. SPOFs are generally eliminated by redundancy, which increases the resilience

The IT Service Continuity Plan



The IT Service Continuity Plan

- A working document detailing all processes and procedures
- Under stringent Change Management
- Detailing individual and team responsibilities
- Off-site storage essential
 - Secure storage vs. home storage

Produce the plan

- **A working document** - The continuity plan must be a 'living' document containing all the information required for the comprehensive recovery of IT services. This includes everything from detailed technical recovery scripts to directions for traveling to the hot start site.
- **Individual and team responsibilities** - The plan must detail the responsibilities of all staff involved in recovery, and the staff must be made aware of their roles and obligations. Further detail on the function of the various groups involved is given later in this section.
- **Under strict change management** - The plan must be constantly reviewed to ensure that it does not become outdated or inconsistent with changing business requirements. The contingency planning manager should therefore be a member of the Change Advisory Board, able to review all changes for their potential impact on the contingency plan.

Recovery Plans



Recovery Plans

- Phases
 - Alert Phase
 - Invocation and recovery phases
 - Return home phase
 - Plans on how to “move” from temporary ITSCM state to new permanent state
 - Removal of data from temporary location
- Key areas
 - Roles and responsibilities
 - Action lists
 - Reference data

Recovery Plans must plan for:

- An **Alert phase** during which an incident is reported, an initial damage assessment is completed and a decision is taken on whether or move to the Invocation and Recovery phase
- An **Invocation and Recovery phase** during which stand-by arrangements are invoked and business processes are recovered
- A **Return to Normal phase** during which the return to normal is planned, facilities and assets are refurbished, repaired or replaced, and operations are transferred from the stand-by arrangements to permanent arrangements

Key Areas

- Roles and responsibilities
- Action lists
- Reference data

Test the Plan



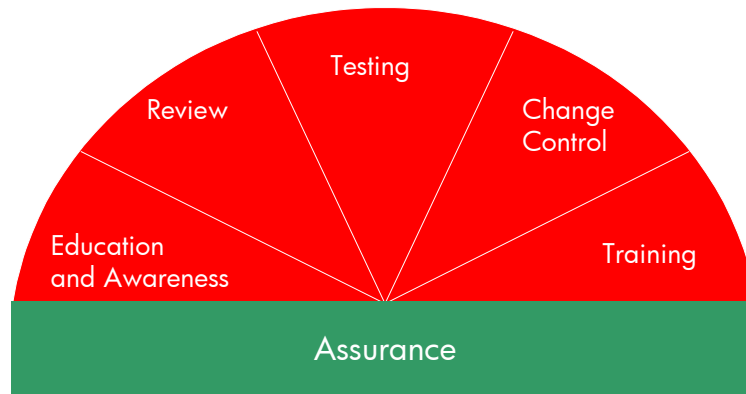
Test the Plan

- Sit down and talk through plan – line by line
 - Immediate Recovery
 - Recommended but planned and risk managed
 - Intermediate Recovery
 - Recommended
 - Gradual Recovery
 - **Not** recommended (suppliers will **not** generally allow this)
 - Return to base
 - Crisis and scenario testing
 - Frequency of testing
 - initially
 - every 6–12 months
 - after every major change to the plan
-
- **Walk through, dry run** - It is essential that a testing schedule is devised which exercises all aspects of the plan. The schedule may consist of a walk-through or a dry-run to familiarize staff with their responsibilities as a prelude to full-scale testing. Such testing is relatively cheap and easy to carry out.
 - **Immediate** – When business demands, an alternative site, already running critical systems, can be used when the main site is inaccessible or unusable within 24 hours. Should be carefully planned, to understand the costs, benefits and risks associated with this type of solution.
 - **Intermediate** - An allowance for testing at intermediate start sites is normally built into the contract with the supplier, and it is important that this option is exercised. The cost is therefore limited to staff time and effort and testing will have limited impact on the live service. Back-up network arrangements may also need to be tested to ensure customers can connect to services recovered at remote sites.
 - **Gradual** - Testing gradual arrangements may also have limited impact on the live service, but may be difficult and costly to arrange.
 - **Return to base** - The Contingency Plan should include details of how to restore services at the home site once the effects of the disaster have been overcome. This may involve relocating services from an interim hot or cold start facility.

- **Crisis and scenario testing** - More comprehensive testing may involve simulations of real incidents and may even involve actors and the emergency services.
- **Frequency of testing** - Tests must be arranged periodically at regular intervals and certainly after any major change to the business or the IT infrastructure. It is recommended that a series of tests are planned which grow in scope and complexity. Internal or external auditors and observers may also be involved to monitor efficiency and effectiveness.

The Process — Stage 4 (Operational/Ongoing)

The Process — Stage 4 (Operational/Ongoing)



Education and Awareness

It is important that the business community understands what continuity plans exist for their services and what their role will be in the event of a disaster.

Their expectations must be realistic, and the priority of their specific service must be clearly communicated before any disaster, probably as part of an SLA.

Training

The recovery teams must know exactly what to do in a disaster. Having a plan is one thing. Being able to implement it is another.

Training could be done as part of the testing schedule. There should be regular training to ensure that staff are familiar with any changes to the continuity plans.

Testing

Regular testing is needed to:

- Ensure that the continuity plans are workable
- Ensure that the plans are current
- Train IT staff
- Ensure that Users understand what will be available

Change Management

Change Management is needed for 2 areas:

- Changes to infrastructure items or services that are covered in the continuity plans
- Changes to the plans themselves

Review

The review will focus on:

- Whether the Service Continuity Management process was followed
- Whether the plans are adequate and scoped correctly
- The results of testing (are the plans workable?)

ITSCM Analysis Method



ITSCM Analysis Method

The activity that aims to identify the potential damage or loss to an organization resulting from disruption to critical business processes is:

- A. Root Cause Analysis
- B. Service Outage Analysis
- C. Business Impact Analysis
- D. Component Failure Impact Analysis

Defining an Intermediate Recovery Site



Defining an Intermediate Recovery Site

An Intermediate Recovery site provides:

- A. A remote computer room, which can be used following a disaster
- B. A back-up computer room, together with replacement computer equipment
- C. Replacement computer equipment which allows immediate recovery without loss of service
- D. A mobile computer room

EXIN

IT is the business.....

IT is the business.....



“**IT** is the business”

and

“The business is **IT**”

Security Management (EXIN Only)

Module 13

Mission Statement

Mission Statement



To interface with all **ITSM processes** where security issues are involved and to **ensure that the security elements of IT services** are provided at the level agreed with the Customer at all times.

It achieves this mission by working closely with the other IT Service Management processes where security issues are involved. For example, Security Management has a specific relationship with Availability Management – one of the prime aspects of security is Availability – and through this Business Continuity.

Another key interface is with Incident Management which is the main liaison point for security incidents. Information security incidents are those events that can cause damage to Confidentiality, Integrity or Availability or information processing. They materialize as accidents or deliberate acts. Information security incidents are usually managed via Incident Control/the Service Desk.

These interfaces and others will be discussed further later on in this chapter.

Important Note

There is a separate ITIL book on Security Management.

What is Security Management?



What is Security Management?

IT Security Management is the process of managing a defined level of security for information, IT services and infrastructure. IT Security Management enables and ensures that:

- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, threats, etc
- Security Incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security

IT Security Management is the process of managing a defined level of security for information, IT services and infrastructure. Also included within the responsibility of IT Security Management is the management of responses to security incidents.

The importance of information security has increased dramatically because of the move of open internal networks to Customers and business partners, the move towards electronic commerce, the increasing use of public networks like the Internet and Intranets. The wide spread use of information and information processing as well as the increasing dependence of process results on information requires structural and organized protection of information

Security Management is more than locking server rooms or insisting on password discipline. IT Security Management enables and ensures that:

- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, threats, etc
- Security incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security

Why the Need for Security Management?

Why the Need for Security Management?



In most organizations Information Security is a key issue in IT Service Management. Therefore some organizations justify Security Management to be treated as a process in its own right. Ensuring safety of information by:

- Managing risks
- Protecting sensitive information against unauthorized access and use (Confidentiality)
- Providing accurate, complete and timely information (Integrity)
- Making information accessible as agreed (Availability)

These are the basic issues of Information Security most relevant for IT Service Management

In most organizations (especially those such as those in the health industry, banks, assurance companies, financial and government) Information Security is a key issue in IT Service Management. Information is one of the most important assets for business. Without it only a few processes are able to perform as intended. The sharing of information with other organizations, which enables quick and automated processing, increases that importance. As a result, some organizations feel fully justified in treating Security Management as a process in its own right. In this way they are ensuring safety of information by:

- Managing risks
- Protecting sensitive information against unauthorized access and use (Confidentiality)
- Providing accurate, complete and timely information (Integrity)
- Making information accessible as agreed (Availability)

Confidentiality, Integrity and Availability are the basic issues of Information Security most relevant for IT Service Management.

Objectives of Security Management

Objectives of Security Management



- Providing a basic level of security for all IT services
- Meeting the security requirements for each of the IT services as agreed in the SLA for that service or defined in contracts, legislation or imposed by external policies



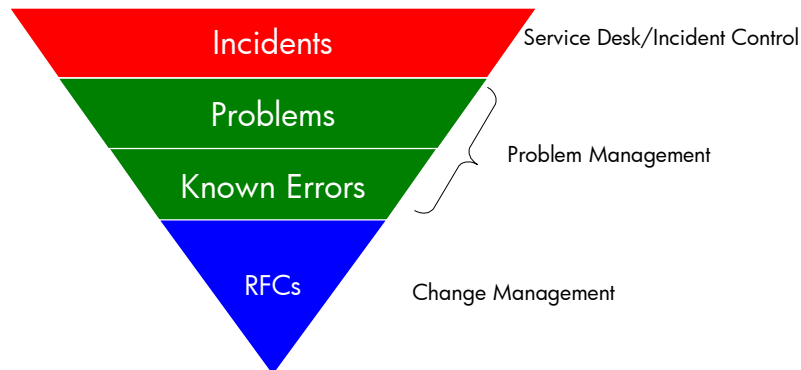
The objectives of Security Management are to provide at the very least a basic level of security for all IT services and to manage a defined level of security (as per SLA) on a service, including managing the reaction to security incidents. By doing this Security Management can ensure the continuity and to protect information of the service and its Customers and can help minimize the damage for the service from security breaches.

ITIL and Security

ITIL and Security



- Security and management are concepts that are symbiotic.
- Security depends on management and management is impossible without proper security.



ITIL and Security – Together a Controlled Process

Security and management are concepts that are symbiotic. Security depends on management and management is impossible without proper security.

The Service Delivery and Service Support processes, as we know, work on a basis of interrelationship. Their main goal is to support the business as per the terms laid out in the SLA in which the agreements with the Customer are specified. Each SLA must include agreements about the security measures to be taken; therefore, security is a key aspect of all of the ITSM processes.

Some of the processes have a more defined role in security than others. The diagram above shows a triangle with, at the top, a relatively large number of incidents, where the security incidents have to be recognized **by incident control/Service Desk function** and dealt with according to the SLA.

Problem Management takes over the issues that cannot be solved immediately and either solves the problem, taking into account the preconditions for security set by the SLA and the basic level of security, or it identifies a known error.

This is followed by the **Change Management** process, in which controlled modifications of the IT infrastructure are made on the basis of Requests for Change (RFCs). Part of this control also involves taking the necessary security measures and maintaining the agreed level of security (as set by the SLA).

Who is Responsible for Security Management?

Who is Responsible for Security Management?

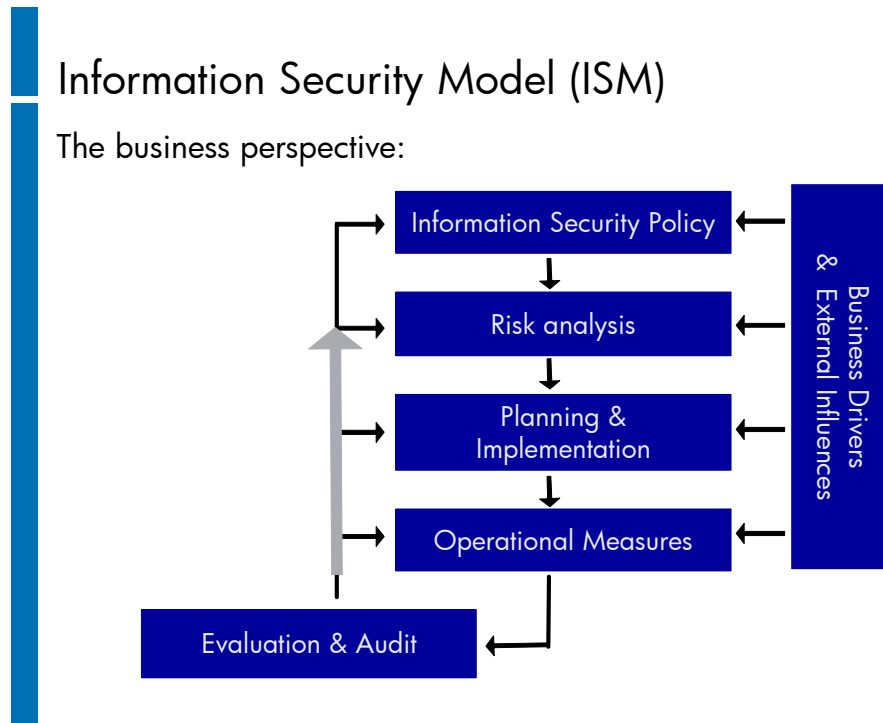


- Needs to be part of every IT Manager's job description
- Management is responsible for risk assessment and risk management, i.e. reducing the chances of a security incident occurring to acceptable levels
- Corporate Executive Management is:
 - Accountable to stakeholders and shareholders for security
 - Responsible for defining the corporate security policy. IT Security Management is governed by that policy

IT Security Management needs to be part of every IT manager's job description. Management is responsible for taking appropriate steps to reduce the chances of a security incident occurring to acceptable levels. This is the process of risk assessment and management.

Corporate Executive Management is accountable to stakeholders and shareholders for security, and is responsible for defining the corporate security policy. IT Security Management is governed by that policy. The existence of the policy registers and reinforces the corporate decision to invest in the security of information and information processing. It provides management with guidelines and direction regarding the relative importance of various aspects of the organization, and of what is allowable and what is not, in the use of IT systems and data.

Information Security Model (ISM)



Information Security Model (ISM) – The Business Perspective

The above diagram illustrates the information security process as seen by the business. It covers all stages, from policy setting and initial risk assessment, through planning, implementation and operation, to evaluation and audit.

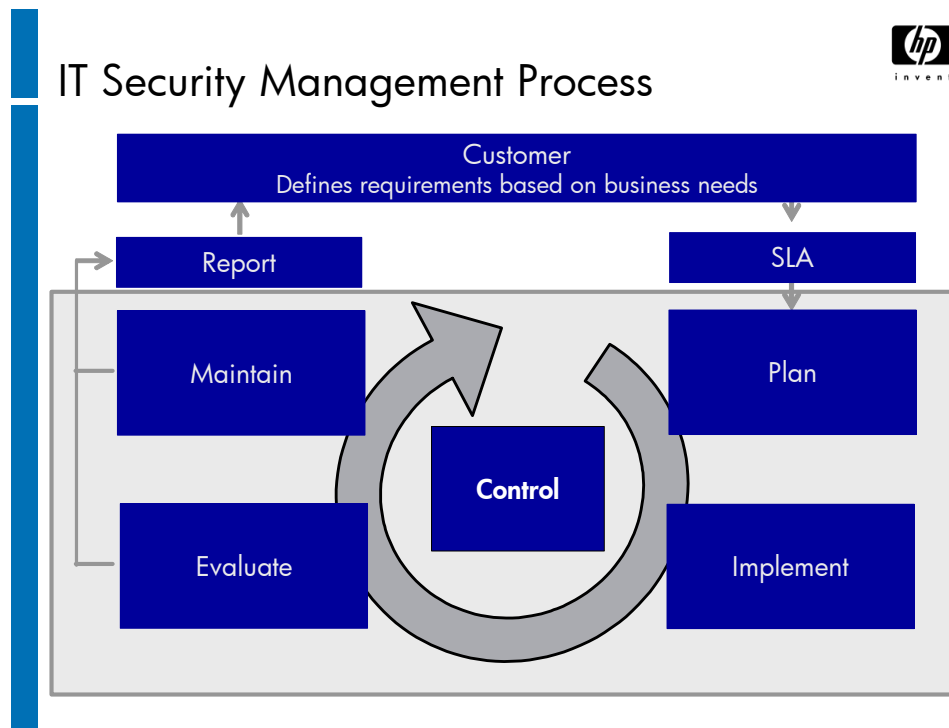
Every organization must have an information security policy that is widely circulated, committed to by everyone within the organization and actively enforced and reviewed.

When introducing IT security, commitment and support from the management is essential. The decision to introduce IT security, along with the necessary investment, must be made by senior management and then laid down in the company's security policy. Management guidelines for organization, conditions, responsibilities, scope and level of detail are also defined there.

Risk analysis serves to define the IT security required to support the business. Both the business perspective and the technical perspective should be taken into account. A risk analysis documents the current state and quality of IT security, and makes suggestions for security measures. The security level defined on that basis is included in an IT security plan.

After implementation, security measures are monitored to evaluate their effectiveness and efficiency. That monitoring is complemented by regular checks/revisions and the resulting evaluation. It serves as input for defining new or revised goals, and for the measures they require

IT Security Management Process



The above diagram provides an overview of the ITIL IT Security Management Process. The process shows the complete route from the collection of a Customer's requirements, through planning, implementation, evaluation and maintenance – under a framework of control - with regular status reporting to the Customer closing the loop.

- **Control**

Control activities are on a par with those for the other ITIL processes. The process is owned by the Security Manager, who creates a framework of conditions, establishes sub-processes and defines roles and responsibilities. Set-up and coordination of the IT Security Management are also supervised by the Security Manager.

- **Planning**

As far as planning is concerned, the process is closely connected to the SLM, with the Service Level Manager in charge. Necessary changes to the IT infrastructure are requested by the Security Manager (request for change – RFC). The Change Manager is responsible for making the changes, as they are subject to the Change Management Process.

■ **Implementation**

Maintaining security awareness - IT security has a lot to do with discipline and compliance with well-documented procedures. For greater efficiency, it is crucial to increase employees' awareness. That can best be achieved by motivating employees in informative meetings and trainings.

Security incident registration - Security incident registration is a part of incident control. It is important to know whether similar incidents have occurred in the past, and what solutions were worked out then.

Security incident handling - Reacting to a Security Incident can be time-critical, especially if other departments or even Customers are involved. Thus, smooth handling is crucial.

■ **Evaluation**

- Internal security audits
- External security audits
- Self assessments

■ **Maintenance**

- Check if security policy is up to date
- Initiate an update of security policy

As discussed previously, intrinsic elements of all activities within the IT Security Management process are risk and vulnerability assessment and management, and the implementation of cost justifiable countermeasures to reduce vulnerability and risk to an acceptable business level. These activities must be closely coordinated with all other areas of Service Management, especially the Availability and IT Service Continuity Management processes.

Key Security Concerns



Key Security Concerns

- Products and services only available to authorized personnel
- Recovery following failure to ensure confidentiality and integrity are not compromised and within secure parameters
- Physical and logical access only to authorized personnel
- Operating system and systems management command authority should be in-line with role and responsibility
- Data must be available to authorized personnel at agreed times as specified in the SLA
- Operational Level Agreement (OLA) and underpinning contracts must reflect the adherence to security controls

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.

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.

Goals of Security Management: Security policy

Goals of Security Management



Which statement is not true regarding goals of Security Management?

- A. Identify potential threats to information and IT assets and develop plans to mitigate risks before they become incidents
- B. Develop and implement procedures that ensure the organization can react quickly to security intrusions
- C. It is not necessary to have a separate Security Incident Management process as the Standard Incident Management process can handle these types of incidents

Goals of Security Management: Confidentiality



Goals of Security Management

What is the description of the term Confidentiality as part of the Security Management Process?

- A. Protection of data against unauthorized access and use
- B. The ability to access data at any moment
- C. The capacity to verify that the data is correct
- D. The correctness of the data

Candidate Registration Form

Appendix A

Information Systems Examinations Board

IT Service Management

Foundation Certificate – Candidate Registration Form

| | | |
|---|--|--|
| IS ENGLISH YOUR 1 ST LANGUAGE? YES / NO | | Candidate No: <i>(Office use only)</i> |
| IF NO, WHAT IS? | | |
| Surname | | Title (Mr, Ms, etc) |
| Other Names | | Date of Birth |
| Home Address | Work Address | |
| Home Telephone Number | Work/Daytime Telephone Number | |
| Email address: | | |
| Are you a BCS member? YES / NO | If yes, please give membership number: | |
| Dates of Course Attended: | Training Provider: | |
| | | |
| Candidate's Signature Date | | |
| Please tick the box if you do not wish your examination mark to be forwarded to your Training Provider (Examination results will automatically be sent to the Training Provider) <div style="float: right; border: 1px solid black; width: 40px; height: 30px; margin-top: 10px;"></div> | | |
| When completed, this form should be sent to: <p style="text-align: center;">ISEB (FCITSM), First Floor Block D, North Star House, North Star Avenue, Swindon, Wilts. SN2 1FA</p> <p style="text-align: center;">Telephone: 01793 417 419 Fax: 01793 417559</p> | | |
| DATA PROTECTION ACT NOTICE The British Computer Society will hold your personal data on its computer database. This information may be accessed, reviewed and used by the Society for administrative purposes (for example, processing your membership application/renewal and contacting you in respect of your membership) and conducting market research. All of these purposes have been notified to the Information Commissioner. If you are based outside the European Economic Area (the "EEA"), information about you may be transferred outside the EEA. The Society, or its approved suppliers, may also send you details of products and services you may be interested in. If you do not wish to receive such information, please tick the box and attach this notice to your completed application form before returning to the BCS. <div style="text-align: right; margin-top: 10px;"> <input type="checkbox"/> </div> | | |

ITIL Glossary of Terms, Definitions and Acronyms

© Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce.

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



Glossary of Terms, Definitions and Acronyms

Baseline v01, 1 May 2006

Note for readers

This glossary may be freely downloaded.

See <http://www.get-best-practice.co.uk/glossaries.aspx> for details of licence terms

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

Acknowledgements

We would like to express our gratitude and acknowledge the contribution of Stuart Rance and Ashley Hanna of Hewlett-Packard in the production of this glossary.

ITIL® Glossary of Terms, Definitions and Acronyms

| Term | Definition |
|----------------------|--|
| Absorbed Overhead | (Financial Management) Indirect cost of providing a Service , which can be fairly allocated to specific Customers . This can be based on usage or some other fair measurement. For example cost of providing network bandwidth or shared servers. See also Direct Cost , Indirect Cost , Unabsorbed Overhead . |
| Acceptance | Synonym for Assurance . |
| Account Manager | (Business Relationship Management) A Role that is very similar to Business Relationship Manager , but includes more commercial aspects. Most commonly used when dealing with External Customers . |
| Accounting | In the context of ITSM , this is a synonym for IT Accounting . |
| Accounting Period | (Financial Management) A period of time for which Budgets , Charges , Depreciation and other financial calculations are made. Usually one year. See Financial Year . |
| Accredited | Officially authorised to carry out a Role . For example an Accredited body may be authorised to provide training or to conduct Audits . See Registered Certification Body (RCB) . (Security Management) Official authorisation for a Certified Configuration to be used for a specific purpose. |
| Activity | A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans , and are documented in Procedures . |
| Agreed Service Time | (Availability Management) A synonym for Service Hours , commonly used in formal calculations of Availability . See Downtime . |
| Agreement | A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a Contract . See Service Level Agreement , Operational Level Agreement . |
| Alert | A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process . |
| Analytical Modelling | A technique that uses mathematical models to predict the behaviour of a Configuration Item or IT Service . Analytical Models are commonly used in Capacity Management and Availability Management . See Modelling . |

| Term | Definition |
|------------------------------------|--|
| Application | <p>Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An Application runs on one or more Servers or Clients.</p> <p>See Application Management, Application Portfolio.</p> |
| Application Management | <p>The Process responsible for managing Applications throughout their Lifecycle.</p> <p>See Application Portfolio.</p> |
| Application Portfolio | <p>A Database used to manage Applications throughout their Lifecycle. An Application Portfolio contains key Attributes of all Applications deployed in the Business.</p> <p>See Portfolio of Services.</p> |
| Application Service Provider (ASP) | <p>An External Service Provider that provides IT Services using Applications running at the Service Provider's premises. Users access the Applications by network connections to the Service Provider.</p> |
| Application Sizing | <p>(Capacity Management) The Activity responsible for understanding the Resource Requirements needed to support a new Application, or a major Change to an existing Application. Application Sizing helps to ensure that the IT Service can meet its agreed Service Level Targets for Capacity and Performance.</p> |
| Assembly CI | <p>(Configuration Management) A Configuration Item that is made up from a number of other CIs. For example a Server CI may contain CIs for CPUs, Disks, Memory etc.; an IT Service CI may contain many Hardware, Software and other CIs.</p> <p>See Component CI, Build.</p> |
| Asset | <p>Something that contributes to an IT Service. Assets can include people, accommodation, Servers, software, data, networks, paper Records, telephones etc.</p> <p>Assets that need to be individually managed are also Configuration Items. For example the door lock on a computer room, or a consumable item would not be a Configuration Item.</p> <p>In the context of Financial Management, items below a specific value are not considered to be Assets as it would not be Cost Effective to track and manage them.</p> <p>See Asset Management, Depreciation, Risk Assessment.</p> |
| Asset Management | <p>(Financial Management) Asset Management is the Business Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle.</p> <p>See Asset Register.</p> |

| Term | Definition |
|---|---|
| Asset Register | (Financial Management) A list of Assets , which includes their ownership and value. The Asset Register is maintained by Asset Management . |
| Assurance | <p>The Activity that obtains management agreement that a Process, Plan, or other Deliverable is complete, accurate, reliable and meets its specified Requirements.</p> <p>Assurance is different from Audit, which is more concerned with Compliance to a formal Standard.</p> |
| Attribute | <p>(Configuration Management) A piece of information about a Configuration Item. Examples are name, location, Version number, and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB).</p> <p>See Relationship.</p> |
| Audit | <p>Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups.</p> <p>See Certification, Assurance.</p> |
| Authorised Examination Centre | A body authorised by an Examination Board to host examinations. The Authorised Examination Centre provides a place where examinations may be taken, and may also provide exam supervision and automated marking. |
| Automatic Call Distribution (ACD) | (Service Desk) Use of Information Technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution. |
| Availability | <p>(Availability Management) (Security Management) Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.</p> <p>See Security Principle.</p> |
| Availability Management | (Availability Management) The Process responsible for defining, analysing, Planning , measuring and improving all aspects of the Availability of IT services . Availability Management is responsible for ensuring that all IT Infrastructure , Processes , Tools , Roles etc are appropriate for the agreed Service Level Targets for Availability . |
| Availability Management Database (AMDB) | (Availability Management) A Database containing all data needed to support Availability Management . The AMDB may be part of the Configuration Management Database . |
| Availability Plan | (Availability Management) A Plan to ensure that existing and future Availability Requirements for IT Services can be provided Cost Effectively . |
| Back-out Plan | (Change Management) (Release Management) A Plan that documents the steps required to recover to a known working state if a Change or Release fails. |

Backup to Brainstorming

| Term | Definition |
|--------------------|--|
| Backup | (Availability management) (IT Service Continuity Management) Copying data to protect against loss of Integrity or Availability of the original. |
| Balance Check | (Financial Management) A calculation to verify that the sum of all individual Costs or Charges equals the total Cost or Charge . Used to check that all amounts have been fully accounted for. |
| Balanced Scorecard | A management tool developed by Drs. Robert Kaplan (Harvard Business School) and David Norton. A Balanced Scorecard enables a Strategy to be broken down into Key Performance Indicators . Performance against the KPIs is used to demonstrate how well the Strategy is being achieved. A Balanced Scorecard has 4 major areas, each of which has a small number of KPIs . The same 4 areas are considered at different levels of detail throughout the Organisation . |
| Baseline | The recorded state of something at a specific point in time. A Baseline can be created for a Configuration , a Process , or any other set of data. For example, a baseline can be used in: <ul style="list-style-type: none"> • Continuous Service Improvement, to establish a starting point for Planning improvements. • Capacity Management, to document performance characteristics during normal operations. • Configuration Management, to enable the IT Infrastructure to be restored to a known configuration if a Change fails. Also used to specify a standard Configuration for data capture, release or Audit purposes. |
| Baseline Security | (Security Management) The minimum level of security required throughout an Organisation . |
| Benchmark | A Baseline used as a reference point. For example: <ul style="list-style-type: none"> • An ITSM Benchmark can be used to compare one Organisation's ITSM Processes with another • A Performance Benchmark may be established by taking measurements of a simulated environment. • See Simulation Modelling. |
| Best Practice | A proven Activity or Process that has been successfully used by multiple Organisations . ITIL is an example of Best Practice. |
| Billing | (Financial Management) Part of the Charging Process . Billing is the Activity responsible for producing an invoice or a bill and recovering the money from Customers . See Pricing . |
| Brainstorming | A technique that helps a team to generate ideas. Ideas are not reviewed during the Brainstorming session, but at a later stage. Brainstorming is often used by Problem Management to identify possible causes. |

| Term | Definition |
|-------------------------------------|---|
| British Standards Institution (BSI) | The UK National Standards body, responsible for creating and maintaining British Standards . See http://www.bsi-global.com for more information. See ISO . |
| BS 15000 | British Standards Institution Specification and Code of Practice for IT Service Management . BS 15000 is based on ITIL Best Practice , and has been superseded by ISO/IEC 20000 . |
| BS 7799 | British Standards Institution Specification and Code of Practice for Information Security Management . BS 7799 has been superseded by ISO/IEC 17799 and ISO/IEC 27001 . |
| Budget | (Financial Management) A list of all the money an Organisation or Business Unit plans to receive, and plans to pay out, over a specified period of time. See Budgeting , Planning . |
| Budgeting | (Financial Management) The Activity of predicting and controlling the spending of money. Consists of a periodic negotiation cycle to set future Budgets (usually annual) and the day-to-day monitoring and adjusting of current Budgets . See Accounting Period . |
| Build | (Release Management) The Activity of assembling a number of Configuration Items to create part of an IT Service . The term Build is also used to refer to a Release that is authorised for distribution. For example Server Build or laptop Build . See Assembly CI . |
| Build Environment | (Release Management) A controlled Environment where Applications , IT Services and other Builds are assembled prior to being moved into a Test or Live Environment . |
| Business | An overall corporate entity or Organisation formed of a number of Business Units . In the context of ITSM , the term Business includes public sector and not-for-profit organisations, as well as companies. An IT Service Provider provides IT Services to a Customer within a Business . The IT Service Provider may be part of the same Business as their Customer (Internal Service Provider), or part of another Business (External Service Provider). |
| Business Capacity Management (BCM) | (Capacity Management) In the context of ITSM , Business Capacity Management is the Activity responsible for understanding future Business Requirements for use in the Capacity Plan . See Service Capacity Management . |
| Business Case | Justification for a significant item of expenditure. Includes information about Costs , benefits, options, issues, Risks , and possible problems. See Cost Benefit Analysis , Investment Appraisal . |

Business Continuity Management (BCM) to Business Operations

| Term | Definition |
|--------------------------------------|---|
| Business Continuity Management (BCM) | (IT Service Continuity Management) Business Continuity Management is the Business Process which sets the Objectives , Scope and Requirements for IT Service Continuity Management . BCM is responsible for managing Risks that could seriously impact the Business . BCM ensures that the Business can always Operate to a minimum agreed level, by reducing the Risk to an acceptable level and Planning to Restore Business Processes . |
| Business Continuity Plan (BCP) | (IT Service Continuity Management) A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation , people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans . |
| Business Continuity Team | (IT Service Continuity Management) The team of people responsible for carrying out Activities defined in a Business Continuity Plan . |
| Business Customer | A recipient of a product or a Service from the Business . For example if the Business is a car manufacturer then the Business Customer is someone who buys a car. |
| Business Driver | Something that influences the definition of Business Objectives and Strategy . For example new legislation or the actions of competitors. The term Business Driver is sometimes used as a synonym for Business Objective or Strategy . |
| Business Impact Analysis (BIA) | (IT Service Continuity Management) BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers , people, other Business Processes , IT Services etc. BIA defines the recovery requirements for IT Services . These requirements include Recovery Time Objectives , Recovery Point Objectives and minimum Service Level Targets for each IT Service . |
| Business IT Alignment (BITA) | Understanding how the IT Service Provider provides value to the Business , and ensuring that IT Strategy , Plans , and Services support the Business Objectives , and Vision . See Service Culture . |
| Business Objective | The Objective of a Business Process , or of the Business as a whole. Business Objectives support the Business Vision , provide guidance for the IT Strategy , and are often supported by IT Services . |
| Business Operations | The day-to-day execution, monitoring and management of Business Processes . See Operate . |

| Term | Definition |
|--|---|
| Business Perspective | <p>An understanding of the Service Provider and IT Services from the point of view of the Business, and an understanding of the Business from the point of view of the Service Provider.</p> <p>See Business IT Alignment.</p> |
| Business Process | <p>A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or Service to a Business Customer. For example, a retailer may have a purchasing Process which helps to deliver Services to their Business Customers. Many Business Processes rely on IT Services.</p> <p>See Vital Business Function, Value Chain.</p> |
| Business Relationship Management (BRM) | <p>(Business Relationship Management) The Process responsible for maintaining a Relationship with the Business. This Process usually includes:</p> <ul style="list-style-type: none"> Managing personal Relationships with Business managers Portfolio Management Ensuring that the IT Service Provider is satisfying the Business needs of the Customers <p>This Process has strong links with Service Level Management.</p> <p>See Account Manager.</p> |
| Business Relationship Manager | <p>(Business Relationship Management) A Role responsible for maintaining the Relationship with one or more Customers. This Role is often combined with the Service Level Manager Role.</p> <p>See Account Manager.</p> |
| Business Service | <p>A Service that is delivered to Business Customers by Business Units. For example delivery of financial services to Customers of a bank, or goods to the Customers of a retail store. Successful delivery of Business Services often depends on one or more IT Services.</p> |
| Business Unit | <p>A segment of the Business which has its own Plans, Metrics, income and Costs.</p> |
| Call | <p>(Service Desk) (Incident Management) A telephone call to the Service Desk from a User. A Call could result in an Incident or a Service Request being logged.</p> |
| Call Centre | <p>(Service Desk) An Organisation or Business Unit which handles large numbers of incoming and outgoing telephone calls.</p> <p>See Service Desk.</p> |
| Call Type | <p>(Service Desk) A Category that is used to distinguish incoming requests to a Service Desk. Common call types are Incident, Service Request and Complaint.</p> |

Capability Maturity Model (CMM) to Capital Expenditure (CAPEX)

| Term | Definition |
|--|--|
| Capability Maturity Model (CMM) | The Capability Maturity Model for Software (also known as the CMM and SW-CMM) is a model used to identify Best Practices to help increase Process Maturity . CMM was developed at the Software Engineering Institute (SEI) of Carnegie Mellon University. In 2000, the SW-CMM was upgraded to CMMI® (Capability Maturity Model Integration). The SEI no longer maintains the SW-CMM model, its associated appraisal methods, or training materials. |
| Capability Maturity Model Integration (CMMI) | Capability Maturity Model® Integration (CMMI) is a process improvement approach developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. CMMI provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. See http://www.sei.cmu.edu/cmmi/ for more information. See CMM , Continuous Improvement , Process Maturity . |
| Capacity | (Capacity Management) The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets . For some types of CI , Capacity may be the size or volume, for example a disk drive. |
| Capacity Management | (Capacity Management) The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term Business Requirements . |
| Capacity Management Database (CDB) | (Capacity Management) A Database containing all data needed to support Capacity Management . The Capacity Management Database is usually separate from the Configuration Management Database (CMDB) because it contains large amounts of rapidly changing data. |
| Capacity Plan | (Capacity Management) A Capacity Plan is used to manage the Resources required to deliver IT Services . The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets . |
| Capacity Planning | (Capacity Management) The Activity within Capacity Management responsible for creating a Capacity Plan . |
| Capital Cost | (Financial Management) The cost of purchasing something that will become a financial Asset , for example computer equipment and buildings. The value of the Asset is Depreciated over multiple Accounting Periods . See Operational Cost |
| Capital Expenditure (CAPEX) | Synonym for Capital Cost . |

| Term | Definition |
|--|---|
| Capital Item | (Financial Management) Synonym for an Asset that is of interest to Financial Management because it is above an agreed financial value. |
| Capitalisation | (Financial Management) Identifying major Cost as Capital, even though no Asset is purchased. This is done to spread the impact of the Cost over multiple Accounting Periods . The most common example of this is software development, or purchase of a software license. |
| Category | A named group of things that have something in common. Categories are used to group similar things together. For example Cost Types are used to group similar types of Cost . Incident Categories are used to group similar types of Incident , CI Types are used to group similar types of Configuration Item . |
| Cause / Effect Diagram | (Problem Management) A technique that helps a team to identify all the possible causes of an effect, such as a Problem . Originally devised by Kaoru Ishikawa and often called an Ishikawa Diagram, The output of this technique is a diagram that looks like a fishbone. |
| CCTA | The UK Government "Central Communications and Telecommunications Agency" was the original author of ITIL . This Organisation no longer exists and its functions are now carried out by of the Office of Government Commerce (OGC) . |
| CCTA Risk Analysis & Management Method (CRAMM). | See CRAMM |
| Central Communications and Telecommunication Agency (CCTA) | See CCTA |
| Certification | Issuing a certificate to confirm Compliance to a Standard . Certification includes a formal Audit by an independent and Accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification. |
| Change | (Change Management) The addition, modification or removal of anything that could have an effect on IT Services . The Scope should include all Configuration Items , Processes , Documentation etc. |
| Change Advisory Board (CAB) | (Change Management) A group of people that assists the Change Manager in the assessment, prioritisation and scheduling of Changes . This board is usually made up of representatives from all areas within the IT Service Provider , representatives from the Business , and Third Parties such as Suppliers . |
| Change Advisory Board / Emergency Committee (CAB/EC) | (Change Management) A sub-set of the Change Advisory Board who make decisions about Emergency Changes . Membership of the CAB/EC may be decided at the time a meeting is called, and depends on the nature of the Emergency Change . |

Change History to Charging Policy

| Term | Definition |
|-------------------|--|
| Change History | (Change Management) Information about all changes made to a Configuration Item during its life. Change History consists of all those Change Records that apply to the CI . |
| Change Management | (Change Management) The Process responsible for controlling the Lifecycle of all Changes . The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services . |
| Change Model | A repeatable way of dealing with a particular Category of Change . A Change Model defines specific pre-defined steps that will be followed for a change of this Category . Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). See Standard Change , Change Advisory Board . |
| Change Record | (Change Management) A Record containing the details of a Change . Each Change Record documents the Lifecycle of a single Change . A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change . Change Records are often stored in a Configuration Management Database . |
| Change Request | Synonym for Request for Change . |
| Change Schedule | (Change Management) A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change. See Projected Service Availability (PSA) . |
| Change Slot | (Change Management) A regular, agreed time when Changes may be implemented with minimal impact on Services . Change Slots are usually documented in SLAs . See Planned Downtime . |
| Chargeable Item | A Deliverable of an IT Service that is used in calculating Charges to Customers . For example, number of Transactions , number of desktop PCs. |
| Charging | (Financial Management) Requiring payment for IT Services . Charging for IT Services is optional, and many Organisations choose to treat their IT Service Provider as a Cost Centre . See Charging Process , Charging Policy |
| Charging Policy | (Financial Management) A Policy specifying the Objective of the Charging Process , and the way in which charges will be calculated. See Cost , Cost Plus , Going Rate , Market Rate . |

| Term | Definition |
|-------------------------------------|--|
| Charging Process | (Financial Management) The Process responsible for deciding how much Customers should pay (Pricing) and recovering money from them (Billing). |
| CI Type | (Configuration Management) A Category that is used to Classify CIs . The CI Type identifies the required Attributes and Relationships for a Configuration Record . Common CI Types include: hardware, Document , User etc. |
| Classification | The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs , Incidents , Problems , Changes etc. are usually classified. |
| Client | <p>A computer that is used directly by a User, for example a PC, Handheld Computer, or Workstation. The term Client is also used to mean the part of a Client-Server Application that the user directly interfaces with. For example an email Client.</p> <p>The term Client is also used to mean Customers or the Business in a general sense. For example Client Manager may be used as a synonym for Account Manager.</p> |
| Client Access Licence | A software license that permits one Client to make use of resources on a Server . |
| Closed | The final Status in the Lifecycle of an Incident , Problem , Change etc. When the Status is Closed, no further action is taken. |
| Closure | The act of changing the Status of an Incident , Problem , Change etc. to Closed . |
| Closure Code | A Category that is assigned to an Incident or Problem before it is Closed . This code identifies the cause, and is intended for use in reporting and Trend Analysis . For example "Customer training required", "Documentation error", "Software bug". |
| COBIT | Control Objectives for Information and related Technology (COBIT) provides guidance and Best Practice for the management of IT Processes . COBIT is published by the IT Governance Institute. See http://www.isaca.org/ for more information. |
| Code of Practice (COP) | A Guideline published by a public body or a Standards Organisation , such as ISO or BSI . Many Standards consist of a Code of Practice and a Specification . The Code of Practice describes recommended Best Practice . |
| Cold Standby | Synonym for Gradual Recovery . |
| Command, control and communications | The Processes and infrastructure that enable an Organisation to effectively pass instructions and information. This enables management control of Resources . This term is typically used in the management of Major Incidents , Business Continuity and IT Service Continuity . |
| Compliance | Ensuring that a Standard or set of Guidelines is followed. See Audit . |

Component to Configuration Identification

| Term | Definition |
|--|--|
| Component | A general term that is used to mean one part of something more complex. For example, a computer System may be a component of an IT Service , an Application may be a Component of a Release Unit . Components that need to be managed should be Configuration Items . |
| Component CI | (Configuration Management) A Configuration Item that is part of an Assembly CI . For example, a CPU or Memory CI may be part of a Server CI . |
| Component Failure Impact Analysis (CFIA) | (Problem Management) (Availability Management) A technique that helps to identify the impact of CI failure on IT Services . A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure). |
| Computer Telephony Integration (CTI) | (Service Desk) CTI is a general term covering any kind of integration between computers and telephone Systems . It is most commonly used to refer to Systems where an Application displays detailed screens relating to incoming or outgoing telephone calls. See Automatic Call Distribution , Interactive Voice Response . |
| Concurrency | A measure of the number of Users engaged in the same Operation at the same time. Used in Capacity Management and License Management . |
| Confidentiality | (Security Management) A Security Principle that requires that data should only be accessed by authorised people. |
| Configuration | A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service , or a recognisable part of an IT Service . Configuration is also used to describe the parameter settings for one or more CIs . |
| Configuration and Change Management (C&CM) | An integrated approach to Planning , implementing and operating Configuration Management , Change Management and Release Management . |
| Configuration Control | (Configuration Management) The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request . |
| Configuration Identification | (Configuration Management) The Activity responsible for collecting information about Configuration Items and their Relationships , and loading this information into the CMDB . Configuration Identification is also responsible for labelling the CIs themselves, so that the corresponding Configuration Records can be found. |

| Term | Definition |
|--|---|
| Configuration Item (CI) | (Configuration Management) Any Component that needs to be managed in order to deliver an IT Service . Information about each CI is recorded in a Configuration Record within the CMDB and is maintained throughout its Lifecycle by Configuration Management . CIs are under the control of Change Management . CIs typically include hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs . |
| Configuration Management | (Configuration Management) The Process responsible for maintaining information about Configuration Items required to deliver an IT Service , including their Relationships . This information is managed throughout the Lifecycle of the CI . The primary objective of Configuration Management is to underpin the delivery of IT Services by providing accurate data to all IT Service Management Processes when and where it is needed. |
| Configuration Management Database (CMDB) | (Configuration Management) A Database used to manage Configuration Records throughout their Lifecycle . The CMDB records the Attributes of each CI , and Relationships with other CIs . A CMDB may also contain other information linked to CIs , for example Incident , Problem or Change Records . The CMDB is maintained by Configuration Management and is used by all IT Service Management Processes . |
| Configuration Record | (Configuration Management) A Record containing the details of a Configuration Item . Each Configuration Record documents the Lifecycle of a single CI . Configuration Records are stored in a Configuration Management Database . |
| Configuration Status Accounting | (Configuration Management) The Activity responsible for recording and reporting the Lifecycle of each Configuration Item . |
| Configuration Structure | (Configuration Management) The hierarchy and other Relationships between all the Configuration Items that comprise a Configuration . |
| Configuration Verification and Audit | (Configuration Management) The Activities responsible for ensuring that information in the CMDB is accurate and that all Configuration Items have been identified and recorded in the CMDB . Configuration Verification includes routine checks that are part of other processes. For example, verifying the serial number of a desktop PC when a User logs an Incident . Configuration Audit is a periodic, formal check. |
| Continuous Availability | (Availability Management) An approach or design to achieve 100% Availability . A Continuously Available IT Service has no planned or unplanned Downtime . |
| Continuous Improvement | The Process responsible for managing improvements to IT Service Management Processes and IT Services . Continuous Improvement continually measures achievement and modifies Processes and the IT Infrastructure to improve Efficiency , Effectiveness , and Cost Effectiveness . See CSIP , SIP , Deming Cycle , Optimise . |
| Continuous Operation | (Availability Management) An approach or design to eliminate planned Downtime of an IT Service . Note that individual Configuration Items may be down even though the IT Service is Available . |

| Term | Definition |
|---|--|
| Continuous Service Improvement Programme (CSIP) | A formal Programme to implement and manage a Continuous Improvement Process . |
| Contract | A legally binding Agreement between two or more parties. |
| Contract Manager | (Supplier Management) A Role responsible for managing Contracts with one or more Suppliers . Contract Managers usually work closely with Service Level Managers to ensure that Supplier Contracts support agreed Service Level Targets for IT Services . |
| Control | A means of managing a Risk , or ensuring that a Business Objective is achieved. Example Controls include Policies , Procedures , Roles , software configurations, passwords, RAID, fences, door-locks etc. A control is sometimes called a Countermeasure or safeguard. Control is also used as a generic term meaning to manage something. |
| Control Objectives for Information and related Technology (COBIT) | See COBIT . |
| Control Processes | The ISO/IEC 20000 Process group that includes Change Management and Configuration Management . |
| Cost | (Financial Management) The amount of money spent on a specific Activity , IT Service , or Business Unit . Costs consist of real cost (money), notional cost such as people's time, and Depreciation . Cost is also used as the name of a Charging Policy that recovers the exact cost of providing the service. See Opportunity Cost , Full Cost , Marginal Cost . |
| Cost Benefit Analysis | An Activity that analyses and compares the costs and the benefits involved in one or more alternative courses of action. See Business Case , Cost Effectiveness , Investment Appraisal . |
| Cost Centre | (Financial Management) A Business Unit or Project to which costs are assigned. A Cost Centre does not charge for Services provided. An IT Service Provider can be run as a Cost Centre or a Profit Centre . |
| Cost Effectiveness | A measure of the balance between the Effectiveness and Cost of a Service , Process or activity. A Cost Effective Process is one which achieves its Objectives at minimum Cost . See KPI , Return on Investment , Value for Money . |

| Term | Definition |
|-----------------------------|--|
| Cost Element | (Financial Management) The middle level of category to which Costs are assigned in Budgeting and Accounting . The highest level category is Cost Type . For example a Cost Type of "people" could have cost elements of payroll, staff benefits, expenses, training, overtime etc. Cost Elements can be further broken down to give Cost Units . For example the Cost Element "expenses" could include Cost Units of Hotels, Transport, Meals etc. |
| Cost Management | (Financial Management) A general term that is used to refer to Budgeting and Accounting , sometimes used as a synonym for Financial Management for IT Services . |
| Cost Model | (Financial Management) A framework used in Budgeting and Accounting in which all known Costs can be recorded, categorised, and allocated to specific Customers , Business Units or Projects . Cost-by-Customer and Cost-by-Service are common types of Cost Model. See Cost Type , Cost Element , Cost Unit . |
| Cost Plus | (Financial Management) A Charging Policy in which Charges are calculated by adding a percentage to the Cost of providing the IT Service . The additional money is often used for future investment. |
| Cost Type | (Financial Management) The highest level of category to which Costs are assigned in Budgeting and Accounting . For example hardware, software, people, accommodation, external and Transfer . See Cost Element , Cost Unit , Cost Model . |
| Cost Unit | (Financial Management) The lowest level of category to which Costs are assigned, Cost Units are usually things that can be easily counted (e.g. staff numbers, software licences) or things easily measured (e.g. CPU usage, Electricity consumed). Cost Units are included within Cost Elements . For example a Cost Element of "expenses" could include Cost Units of Hotels, Transport, Meals etc. |
| Cost-by-Customer Cost Model | (Financial Management) A type of Cost Model in which Costs are identified and allocated to Customers . |
| Cost-by-Service Cost Model | (Financial Management) A type of Cost Model in which Costs are identified and allocated to IT Services . |
| Countermeasure | A synonym for Control . The term Countermeasure can be used to refer to any type of Control , but it is most often used when referring to measures that increase Resilience , Fault Tolerance or Reliability of an IT Service . |
| CRAMM | (Security Management) (Availability Management) (IT Service Continuity Management) CCTA Risk Analysis & Management Method (CRAMM). A methodology and tool for analysing and managing Risks . CRAMM was developed by the UK Government, but is now privately owned. Further information is available from http://www.cramm.com/ |

Crisis Management to Definitive Hardware Store (DHS)

| Term | Definition |
|---------------------------------|--|
| Crisis Management | (IT Service Continuity Management) Crisis Management is the Process responsible for managing the wider implications of Business Continuity . A Crisis Management team is responsible for Strategic issues such as managing media relations and shareholder confidence, and decides when to invoke Business Continuity Plans . |
| Critical Success Factor (CSF) | Something that must happen if a Process , Project , Plan , or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example a CSF of "protect IT Services when making Changes " could be measured by KPIs such as "percentage reduction of unsuccessful Changes ", "percentage reduction in Changes causing Incidents " etc. |
| Culture | A set of values that is shared by a group of people, including expectations about how people should behave, ideas, beliefs, and practices. See Vision . |
| Customer | Someone who buys goods or Services . The Customer of an IT Service Provider is the person or group who defines and agrees the Service Level Targets . The term Customers is also sometimes informally used to mean Users , for example "this is a Customer Focussed Organisation ". |
| Customer Focus | Understanding and meeting the real needs of Customers and Users . This is done to maximise Customer satisfaction and thus to obtain long term benefits for the IT Service Provider . Customer Focus can be displayed by the entire Organisation (see Service Culture) or by specific people or Processes . |
| Customer-Managed Use | (Software Asset Management) The management of licenses by the Customer or IT Service Provider . Licenses may also be managed by the Supplier of the software (Vendor Managed Use). |
| Database | In IT Service Management , a Database is a structured collection of data, used to support one or more Processes . A Database of this sort does not need to be a single physical Database, but may consist of various data sources and tools that together meet the requirements. For example, Configuration Management Database , Capacity Database , Availability Database , Application Portfolio . |
| Definitive Hardware Store (DHS) | (Release Management) One or more physical locations in which hardware Configuration Items are securely stored when not in use. All hardware in the DHS is under the control of Change and Release Management and is recorded in the CMDB . The DHS contains spare parts, maintained at suitable revision levels, and may also include hardware that is part of a future Release . |

| Term | Definition |
|-----------------------------------|---|
| Definitive Software Library (DSL) | (Release Management) One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DSL may also contain associated CIs such as licenses and documentation. The DSL is a single logical storage area even if there are multiple locations. All software in the DSL is under the control of Change and Release Management and is recorded in the CMDB . Only software from the DSL is acceptable for use in a Release . |
| Deliverable | Something that must be provided to meet a commitment in a Service Level Agreement or a Contract . Deliverable is also used in a more informal way to mean a planned output of any Process . |
| Delta Release | (Release Management) A Release that includes only those Components of a Release Unit that have actually changed since the last Release . A Delta Release is also referred to as a partial Release. See Release Type . |
| Demand Management | (Capacity Management) Optimising the use of Capacity by moving Workload to less utilised times, Servers , or places. Demand Management often uses Differential Charging to encourage Customers to use IT Services at less busy times. Demand Management also makes use of other techniques such as limiting the number of concurrent Users . |
| Deming Cycle | Synonym for Plan Do Check Act . |
| Dependency | The direct or indirect reliance of one Process or Activity upon another. |
| Deployment | (Release Management) The Activity responsible for movement of new or changed hardware, software, documentation, Process , etc to the Live Environment . See Rollout . |
| Depreciation | (Financial Management) A measure of the reduction in value of an Asset over its life. This is based on wearing out, consumption or other reduction in the useful economic value. |
| Detection | (Incident Management) A stage in the Incident Lifecycle . Detection results in the Incident becoming known to the Service Provider . Detection can be automatic, or can be the result of a user logging an Incident . |
| Development | The Process responsible for creating or modifying an IT Service or Application . Also used to mean the Role or group that carries out Development work. |
| Development Environment | An Environment used to create or modify IT Services or Applications . Development Environments are not typically subjected to the same degree of control as Test Environments or Live Environments . See Development . |
| Diagnosis | (Incident Management) (Problem Management) A stage in the Incident and Problem Lifecycles . The purpose of Diagnosis is to identify a Workaround for an Incident or the Root Cause of a Problem . |

Diagnostic Script to Efficiency

| Term | Definition |
|-----------------------|--|
| Diagnostic Script | (Service Desk) A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them Classify , Resolve and assign Incidents . Diagnostic Scripts may also be made available to Users to help them diagnose and resolve their own Incidents . |
| Differential Charging | (Financial Management) A technique used in Charging to support Demand Management by charging different amounts for the same IT Service Function at different times. |
| Direct Cost | (Financial Management) A cost of providing an IT Service which can be allocated in full to a specific Customer , Cost Centre , Project etc. For example cost of providing non-shared servers or software licenses. See also Indirect Cost . |
| Do Nothing | (IT Service Continuity) A Recovery Option . The Service Provider formally agrees with the Customer that Recovery of this IT Service will not be performed. |
| Document | Information in readable form. A Document may be paper or electronic. For example a Policy statement, Service Level Agreement , Incident Record , diagram of computer room layout. See Record . |
| Dormant Contract | (IT Service Continuity) A Recovery Option . The Service Provider takes out a Contract with a Supplier to provide required products or Services within agreed times for an agreed price. The Contract is invoked as part of a Recovery Plan , at which time an additional payment is made and the goods or Service are provided. |
| Downtime | (Availability Management) The time when a Configuration Item or IT Service is not Available during its Agreed Service Time . The Availability of an IT Service is often calculated from Agreed Service Time and Downtime. |
| Effectiveness | A measure of whether the Objectives of a Process , Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives . See KPI . |
| Efficiency | A measure of whether the right amount of resources have been used to deliver a Process , Service or Activity . An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. See KPI . |

| Term | Definition |
|---|---|
| Emergency Change | <p>(Change Management) A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes.</p> <p>See Change Advisory Board / Emergency Committee (CAB/EC).</p> |
| Environment | <p>A subset of the IT Infrastructure that is used for a particular purpose. For Example: Live Environment, Test Environment, Build Environment. It is possible for multiple Environments to share a Configuration Item, for example Test and Live Environments may use different partitions on a single mainframe computer. Also used in the term Physical Environment to mean the accommodation, air conditioning, power system etc.</p> |
| Error | <p>A design flaw or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that impacts a CI or IT Service is also an Error.</p> <p>See Known Error.</p> |
| Error Control | <p>(Problem Management) The Activity responsible for managing Known Errors until they are Resolved by the successful implementation of Changes.</p> <p>See Problem Control.</p> |
| Escalation | <p>An Activity that obtains additional Resources when these are needed to meet Service Level Targets or Customer expectations. Escalation may be needed within any IT Service Management Process, but is most commonly associated with Incident Management, Problem Management and the management of Customer complaints. There are two types of Escalation, Functional Escalation and Hierarchical Escalation.</p> |
| Estimation | <p>The use of experience to provide an approximate value for a Metric or Cost. Estimation is also used in Capacity and Availability Management as the cheapest and least accurate Modelling method,</p> |
| European Foundation for Quality Management (EFQM) | <p>The EFQM Excellence Model was introduced at the beginning of 1992 as the framework for assessing Organisations for the European Quality Award. It is now the most widely used organisational framework in Europe and it has become the basis for the majority of national and regional Quality Awards. See http://www.efqm.org/ for more information.</p> |
| Event | <p>An Alert or notification created by any IT Service, Configuration Item or monitoring tool. For example a notification that a batch job has completed. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.</p> <p>See Event Management.</p> |
| Event Management | <p>The Process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations.</p> |

| Term | Definition |
|--|--|
| Examination Board | An Organisation Accredited to develop and manage examinations. IT Service Management Examination Boards are accredited by ICMB to develop ITIL examinations, based on a common syllabus, to Accredit training Organisations , and to award Certificates . See ISEB , EXIN . |
| Examination Institute for Information Science (EXIN) | The Examination Institute for Information Science, is accredited by the ICMB as an Examination Board . See http://www.exin-exams.com/ for more information. |
| Exception Report | A Document containing details of one or more KPIs or other important targets that have exceeded defined thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem. |
| External Customer | A Customer who works for a different Business to the IT Service Provider . See External Service Provider , Internal Customer . |
| External Service Provider | An IT Service Provider which is part of a different Business to their Customer . An IT Service Provider may have both Internal Customers and External Customers . See Internal Service Provider , Application Service Provider , Internet Service Provider . |
| Failure | Loss of ability to Operate to Specification , or to deliver the required output. The term Failure may be used when referring to IT Services , Processes , Activities , Configuration Items etc. A Failure often causes an Incident . See Error . |
| Fault | Synonym for Error . |
| Fault Tolerance | The ability of an IT Service or Configuration Item to continue to Operate correctly after Failure of a Component part. See Resilience , Countermeasure . |
| Fault Tree Analysis | (Problem Management) (Availability Management) A technique that can be used to determine the chain of events that leads to a Problem . Fault Tree Analysis represents a chain of events using Boolean notation in a diagram. |
| Financial Management | A common abbreviation of Financial Management for IT Services |
| Financial Management for IT Services | (Financial Management) The Process responsible for managing an IT Service Provider's Budgeting , Accounting and Charging requirements. |

| Term | Definition |
|------------------------|---|
| Financial year | (Financial Management) An Accounting Period covering 12 consecutive months. A Financial Year may start on any date, for example 1 April to 31 March. |
| First Time Fix Rate | (Service Desk) (Incident Management) A Metric that measures the percentage of Incidents resolved by First-line Support without delay or Escalation . Other definitions of this Metric are possible, for example some IT Service Providers define it as the percentage of Incidents that are Resolved during the initial User phone call. |
| First-line Support | (Service Desk) (Incident Management) The first level in a hierarchy of Support Groups involved in the resolution of Incidents . Each level contains more specialist skills, or has more time or other resources. See Escalation . |
| Fishbone Diagram | Synonym for Cause / Effect Diagram . |
| Fit for Purpose | An informal term used to describe a Process , Configuration Item , IT Service etc. that is capable of meeting its objectives or Service Levels . Being Fit for Purpose requires suitable design, implementation, control and maintenance. |
| Fixed Cost | (Financial Management) A Cost that does not vary with IT Service usage. For example the cost of Server hardware. See Variable Cost . |
| Fixed Facility | (IT Service Continuity Management) A permanent building, available for use when needed by an IT Service Continuity Plan . See Recovery Option , Portable Facility . |
| Fixed Price | (Financial Management) A Cost or Charge agreed with a Supplier or Customer . This Cost or Charge remains the same, even if Resource usage or time to deliver a Project changes. |
| Follow the Sun Support | (Service Desk) A methodology for using Service Desks and Support Groups around the world to provide seamless 24 * 7 Service. Calls , Incidents , Problems and Service Requests are passed between groups in different time zones. |
| Full Cost | (Financial Management) The total Cost of all the resources used in supplying an IT Service , i.e., the sum of the Direct Costs of producing the output, a proportional share of Indirect Costs , and any selling and distribution expenses. See Total Cost of Ownership , Marginal Cost . |
| Full Release | (Release Management) A Release that includes all Components of a Release Unit , including those that have not changed. See Release Type . |

Function to Impact

| Term | Definition |
|-------------------------|---|
| Function | <p>An intended purpose of a Configuration Item, Person, Team, Process, or IT Service. For example one Function of an Email Service may be to store and forward outgoing mails, one Function of a Business Process may be to dispatch goods to Customers. The term Function also has two other meanings:</p> <ul style="list-style-type: none"> perform the intended purpose correctly, "The computer is Functioning" team or group of people, "The Change Management Function". |
| Functional Escalation | Transferring an Incident , Problem or Change to a technical team with a higher level of expertise to assist in an Escalation . |
| Going Rate | (Financial Management) A Charging Policy in which Charges are the same as those charged by other internal departments or internal departments of similar Organisations . |
| Gradual Recovery | (IT Service Continuity Management) A Recovery Option which is also known as Cold Standby. Provision is made to Recover the IT Service in a period of time greater than 72 hours. Gradual Recovery typically uses a Portable or Fixed Facility that has environmental support and network cabling, but no computer Systems . The hardware and software are installed as part of the IT Service Continuity Plan . |
| Guideline | <p>A Document describing Best Practice, that recommends what should be done. Compliance to a guideline is not normally enforced.</p> <p>See Standard.</p> |
| Help Desk | (Service Desk) A point of contact for Users to log Incidents . A Help Desk is usually more technically focussed than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often used as a synonym for Service Desk . |
| Hierarchical Escalation | Informing or involving more senior levels of management to assist in an Escalation . |
| Hot Standby | Synonym for Immediate Recovery |
| Immediate Recovery | (IT Service Continuity Management) A Recovery Option which is also known as Hot Standby. Provision is made to Recover the IT Service in a short period of time, typically less than 2 hours but could be up to 24 hours. Immediate Recovery typically uses a dedicated Fixed Facility with computer Systems , and software configured ready to run the IT Services . Immediate Recovery may take up to 24 hours if there is a need to Restore data from Backups . |
| Impact | <p>A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.</p> <p>See Impact Code.</p> |

| Term | Definition |
|--|---|
| Impact Code | A Category used to represent Impact . For example Major, Minor, Catastrophic. See Priority . |
| Incident | (Incident Management) An unplanned interruption to an IT Service or reduction in the Quality of an IT Service . Any event which could affect an IT Service in the future is also an Incident. For example Failure of one disk from a mirror set. See Incident Management , Incident Record . |
| Incident Management | (Incident Management) The Process responsible for managing the Lifecycle of all Incidents . The primary Objective of Incident Management is to return the IT Service to Customers as quickly as possible. |
| Incident Record | (Incident Management) A Record containing the details of an Incident . Each Incident record documents the Lifecycle of a single Incident . |
| Indirect Cost | (Financial Management) A Cost of providing an IT Service which cannot be allocated in full to a specific customer . For example Cost of providing shared Servers or software licenses. Also known as Overhead . Indirect costs are divided into Absorbed Overhead and Unabsorbed Overhead . See Direct Cost . |
| Information Security Management | (Security Management) The Process that ensures the Confidentiality , Integrity and Availability of an Organisations Assets , information, data and IT Services . Information Security Management usually has a wider scope than the Service Provider . It normally includes handling of paper, building access, phone calls etc., for the entire Organisation . |
| Information Security Manager | (Security Management) The Information Security Manager is the Role responsible for the Information Security Management Process in the IT Service Provider . The Information Security Manager is responsible for fulfilling the security demands as specified in the Information Security Policy and SLAs . The Information Security Manager typically delegates the actual implementation to other personnel in the IT Service Provider . The Information Security Officer and the Information Security Manager work closely together. |
| Information Security Officer | (Security Management) The Information Security Officer is responsible for assessing the business Risks and setting the Information Security Policy . This Role is the counterpart of the Information Security Manager and resides in the Customer Organisation . The Information Security Officer and the Information Security Manager work closely together. |
| Information Security Policy | (Security Management) The Policy that governs the Organisations approach to Information Security Management . |
| Information Systems Examination Board (ISEB) | The British Computer Society Information Systems Examination Board is accredited by the ICMB as an Examination Board . See http://www.bcs.org/bcs/products/qualifications/iseb for more information. |

| Term | Definition |
|------------------------------------|--|
| Information Technology (IT) | The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services . |
| Informed Customer | A manager who works for the Customer , and is a specialist in dealing with and managing IT Service Providers . The Informed Customer is responsible for all aspects of managing the relationship with Service Providers . |
| Infrastructure Service | An IT Service that is not directly used by the Business , but is required by the IT Service Provider so they can provide other IT Services . For example directory services, naming services, or communication services. |
| Insource | Transferring the provision of IT Services from an External Service Provider to an Internal Service Provider . The term Insourcing is used to mean running or managing IT Services as an Internal Service Provider . See Outsource . |
| Institute of IT Service Management | An independently governed professional body, specifically aimed at professionals in IT Service Management "aims to promote and support the standing of its members by establishing high-standards of professional and ethical conduct, ensuring continuing professional development of its members in order to demonstrate their competence and commitment". See http://www.iosm.com/ for more information. |
| Integration Testing | Testing of a Build or Release to ensure that the parts work correctly together. |
| Integrity | (Security Management) A Security Principle that ensures data and Configuration Items are only modified by authorised personnel and Activities . Integrity considers all possible causes of modification, including software and hardware Failure , environmental Events , and human intervention. |
| Interactive Voice Response (IVR) | (Service Desk) A form of Automatic Call Distribution that accepts User input, such as key presses and spoken commands, to identify the correct destination for incoming Calls . |
| Intermediate Recovery | (IT Service Continuity Management) A Recovery Option which is also known as Warm Standby. Provision is made to Recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically uses a shared Portable or Fixed Facility that has Computer Systems and Network Components . The hardware and software will need to be configured, and data will need to be restored, as part of the IT Service Continuity Plan . |
| Internal Customer | A Customer who works for the same Business as the IT Service Provider . See Internal Service Provider , External Customer . |

| Term | Definition |
|--|---|
| Internal Service Provider | <p>An IT Service Provider which is part of the same Business as their Customer. An ST Service Provider may have both Internal Customers and External Customers.</p> <p>See External Service Provider.</p> |
| International Organization for Standardization (ISO) | <p>The International Organization for Standardization (ISO) is the world's largest developer of Standards.</p> <p>ISO is a non-governmental organization which is a network of the national standards institutes of 156 countries.</p> <p>Further information about ISO is available from http://www.iso.org/</p> |
| International Standards Organisation | See International Organization for Standardization (ISO) |
| Internet Service Provider (ISP) | An External Service Provider that provides access to the Internet. Most ISPs also provide other IT Services such as web hosting. |
| Investment Appraisal | <p>(Financial Management) The Activity responsible for carrying out a Cost Benefit Analysis to justify Capital Expenditure for a new or changed IT Services.</p> <p>See Business Case, Cost Effectiveness, Return on Investment, Return on Capital Employed.</p> |
| Invocation | (IT Service Continuity Management) Initiation of the steps defined in a plan. For example initiating the IT Service Continuity Plan for one or more IT Services . |
| Ishikawa Diagram | Synonym for Cause / Effect diagram . |
| ISO/IEC 17799 | <p>(Security Management) ISO Code of Practice for Information Security Management, based on BS 7799 Part 1.</p> <p>See Standard.</p> |
| ISO/IEC 20000 | <p>ISO Specification and Code of Practice for IT Service Management. ISO/IEC 20000 is aligned with ITIL Best Practice, and supersedes BS 15000.</p> <p>See Standard.</p> |
| ISO/IEC 27001 | <p>(Security Management) ISO Specification for Information Security Management. The corresponding Code of Practice is ISO/IEC 17799.</p> <p>ISO/IEC 27001 supersedes BS7799 Part 2.</p> <p>See Standard.</p> |
| ISO 9000 | <p>A generic term that refers to a number of international Standards and Guidelines for Quality Management Systems.</p> <p>See http://www.iso.org/ for more information.</p> <p>See ISO.</p> |

ISO 9001 to IT Service Continuity Management (ITSCM)

| Term | Definition |
|--|--|
| ISO 9001 | An international Standard for Quality Management Systems . See ISO 9000 . |
| IT Accounting | (Financial Management) The Process responsible for identifying actual Costs of delivering IT Services , comparing these with budgeted costs, and managing variance from the Budget . See also Charging . |
| IT Accounting System | (Financial Management) The entire set of Policy , tools and Process that support Financial Management . |
| IT Availability Metrics Model (ITAMM) | (Availability Management) A model that helps to ensure all aspects of Availability are considered when defining Availability Metrics and reports. |
| IT Directorate | Senior Management within a Service Provider , charged with developing and delivering IT services . Most commonly used in UK Government departments. |
| IT Infrastructure | All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver or support IT Services . The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation. |
| IT Infrastructure Library (ITIL) | A set of Best Practice guidance for IT Service Management . ITIL is owned by the OGC and is developed in conjunction with the itSMF . ITIL consists of a series of publications giving guidance on the provision of Quality IT Services , and on the Processes and facilities needed to support them. See http://www.ogc.gov.uk/index.asp?id=2261 for more information. |
| IT Operations | The Process responsible for the day-to-day monitoring and management of one or more IT Services and the IT Infrastructure they depend on. The term IT Operations is also used to refer to the group or department within an IT Service Provider responsible for IT Operations . See Operations Bridge , Event Management . |
| IT Service | A Service provided to one or more Customers by an IT Service Provider . An IT Service is based on the use of Information Technology and supports the Customer's Business Processes . An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement . |
| IT Service Continuity Management (ITSCM) | (IT Service Continuity Management) The Process responsible for managing Risks that could seriously impact IT Services . ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels , by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services . ITSCM should be designed to support Business Continuity Management . |

| Term | Definition |
|--|---|
| IT Service Continuity Plan | (IT Service Continuity Management) A Plan defining the steps required to Recover one or more IT Services . The Plan will also identify the triggers for Invocation , people to be involved, communications etc. The IT Service Continuity Plan should be part of a Business Continuity Plan . |
| IT Service Management (ITSM) | The implementation and management of Quality IT Services that meet the needs of the Business . IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process and Information Technology . |
| IT Service Management Forum (itSMF) | The IT Service Management Forum is an independent Organisation dedicated to promoting a professional approach to IT Service Management . The itSMF is a not-for-profit membership Organisation with representation in many countries around the world (itSMF Chapters). The itSMF and its membership contribute to the development of ITIL and associated IT Service Management Standards . See http://www.itsmf.com/ for more information. |
| IT Service Provider | A Service Provider that provides IT Services to Internal Customers or External Customers . |
| IT Steering Group | A formal group that is responsible for ensuring that Business and IT Service Provider Strategies and Plans are closely aligned. An IT Steering Group includes senior representatives from the Business and the IT Service Provider . |
| ITIL | See IT Infrastructure Library . |
| ITIL Certification Management Board (ICMB) | The body responsible for the maintenance and ongoing development of the ITIL qualification scheme. See http://www.itil.co.uk/icmb.htm for further information. |
| Job Description | A Document which defines the Roles , responsibilities, skills and knowledge required by a particular person. One Job Description can include multiple Roles , for example the Roles of Configuration Manager and Change Manager may be carried out by one person. |
| Kepner-Tregoe Analysis | (Problem Management) A structured approach to Problem solving. The Problem is analysed in terms of what, where, when and extent. Possible causes are identified. The most probable cause is tested. The true cause is verified. |
| Key Performance Indicator (KPI) | A Metric that is used to help manage a Process , IT Service or Activity . Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process , IT Service or Activity . KPIs should be selected to ensure that Efficiency , Effectiveness , and Cost Effectiveness are all managed. See Critical Success Factor . |
| Knowledge Base | (Service Desk) (Incident Management) A Database containing information about Incidents , Problems and Known Errors . The Knowledge Base is used to match new Incidents with historical information, improving Resolution times and First Time Fix Rates . |

| Term | Definition |
|----------------------|---|
| Knowledge Management | The Process responsible for gathering, analysing, storing and sharing knowledge information within an Organisation . The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge. |
| Known Error (KE) | (Problem Management) A Problem that has a documented Root Cause and a Workaround . Known Errors are created by Problem Control and are managed throughout their Lifecycle by Error Control . Known Errors may also be identified by Development or Suppliers . See Known Error Record , Knowledge Base . |
| Known Error Database | (Service Desk) (Incident Management) (Problem Management) A Database containing all Known Error Records . This Database is created by Problem Management and used by Incident and Problem Management . See Knowledge Base . |
| Known Error Record | (Problem Management) A Record containing the details of a Known Error . Each Known Error Record documents the Lifecycle of a Known Error , including the Status , Root Cause and Workaround . In some implementations a Known Error is documented using additional fields in a Problem Record . |
| License Management | The Process responsible for the management of software licenses throughout their Lifecycle . |
| Lifecycle | The various stages in the life of a Configuration Item , Incident , Problem , Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example: <ul style="list-style-type: none">• The Lifecycle of an Application includes Design, Build, Test, Deploy, Operate etc.• The lifecycle of an Incident includes Detect, Respond, Diagnose, Repair, Recover, Restore.• The lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed etc. |
| Live | Refers to an IT Service or Configuration Item that is being used to deliver Service to a Customer . |
| Live Environment | A controlled Environment containing Live Configuration Items used to deliver IT Services to Customers . |
| Maintainability | (Availability Management) A measure of how quickly and Effectively a Configuration Item or IT Service can be restored to normal working after a Failure . Maintainability is often measured and reported as MTTR . See Availability . |
| Major Incident | (Incident Management) The highest Category of Impact for an Incident . A Major Incident results in significant disruption to the Business . See Escalation . |

| Term | Definition |
|---|---|
| Managed Object (MO) | An abstract representation of a Resource that is used for Operational management of that Resource . An MO is defined in terms of the attributes of the Resource , operations that may be performed on it, notifications it may issue and relationships with other MOs. MOs differ from Configuration Items as their status is dynamic, and Changes to their Operational state do not need to be approved by the Change Management Process . |
| Managed Services | Synonym for Outsourced IT Services . Also used in ISO/IEC 20000 as a Synonym for IT Services , whether Outsourced or not. |
| Management Information | Information that is used to support decision making by managers. Management Information is often generated automatically by tools supporting the various IT Service Management Processes . Management Information often includes the values of KPIs such as "Percentage of Changes leading to Incidents ", or " First Time Fix Rate ". |
| Management Information System (MIS) | The IT Service that captures, processes and provides Management Information . The term MIS is also informally used to mean the output of MIS, including data and reports. |
| Management System | The framework of Policy and Processes that ensures an Organisation can achieve its Objectives . |
| Manual Workaround | (Incident Management) (Problem Management) A Workaround that requires manual intervention. (IT Service Continuity Management) A Recovery Option . The Business Process Operates without the use of IT Services . This is a temporary measure and is usually combined with another Recovery Option . |
| Marginal Cost | (Financial Management) The Cost of continuing to providing the IT Service . Marginal Cost does not include investment already made, for example the cost of developing new software and delivering training. See Full Cost , Opportunity Cost |
| Market Price | (Financial Management) A Charging Policy in which Charges are the same as those an external Supplier would charge. |
| Maturity | Synonym for Process Maturity . |
| Maturity Level | A named level in a maturity model such as the Carnegie Mellon Capability Maturity Model Integration . See Process Maturity . |
| Mean Time Between Failures (MTBF) | (Availability Management) A Metric for measuring and reporting Reliability . MTBF is the average time that a Configuration Item or IT Service can perform its agreed Function without interruption. This is measured from when the CI or IT Service starts working, until it next fails. |
| Mean Time Between Service Incidents (MTBSI) | (Availability Management) A Metric used for measuring and reporting Reliability . MTBSI is the mean time from when a System or IT Service fails, until it next fails. MTBSI is equal to MTBF + MTTR . |

Mean Time To Repair (MTTR) to Operate

| Term | Definition |
|--|--|
| Mean Time To Repair (MTTR) | (Availability Management) A Metric for measuring and reporting Maintainability . MTTR is the average time taken to restore a Configuration Item or IT Service after a Failure . MTTR is measured from when the CI or IT Service fails until it is fully restored and delivering its normal functionality. |
| Metric | Something that is measured and reported to help manage a Process , IT Service or Activity . See KPI . |
| Mission Statement | The Mission Statement of an Organisation is a short but complete description of the overall purpose and intentions of that Organisation . It states what is to be achieved, but not how this should be done. |
| Modelling | Any technique used to predict the future behaviour of an IT Service , Configuration Item or Business Process . Models are commonly used in Financial Management , Capacity Management and Availability Management . See Estimation , Analytical Modelling , Simulation Modelling . |
| n-line Support | (Service Desk) (Incident Management) (Problem Management) A generic term for any level of Support Group . See First-line Support , Second-line Support , Third-line Support . |
| Notional Charging | (Financial Management) A Charging Policy where Customers are sent Bills for the IT Services they have used, but money is not actually transferred. This is sometimes introduced to ensure that Customers are aware of the Costs they incur, or as a stage during the introduction of Real Charging . |
| Objective | The defined purpose or aim of a Process , an Activity or an Organisation as a whole. Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement . |
| Office of Government Commerce (OGC) | OGC own the copyright to the ITIL publications. They are a UK Government department that works with public sector Organisations to help them improve their Efficiency , gain better Value for Money from their commercial Activities , and deliver improved success from Programmes and Projects . |
| Office of Public Sector Information (OPSI) | OPSI are the publishers of the ITIL publications. They are a UK Government department who provide online access to UK legislation, license the re-use of Crown copyright material, manage the Information Fair Trader Scheme, maintain the Government's Information Asset Register and provide advice and guidance on official publishing and Crown copyright |
| Operate | To perform as expected. A Process or Configuration Item is said to Operate if it is delivering the Required outputs. Operate also means to perform one or more Operations . For example, to Operate a computer is to do the day-to-day Operations needed for it to perform as expected. See Operation , IT Operations , Business Operations . |

| Term | Definition |
|-----------------------------------|---|
| Operation | <p>A pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.</p> <p>See Operate, IT Operations, Business Operations.</p> |
| Operational | <p>The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short term Planning or delivery of a Business Process or IT Service Management Process.</p> <p>The term Operational is also used to refer to a Configuration Item or IT Service being ready for use.</p> |
| Operational Acceptance | <p>(Release Management) Part of the Release Acceptance Activity, responsible for ensuring that everything needed for IT Operations is in place before the Release is deployed. Operational Acceptance often uses a checklist to ensure that all required documentation, IT Operations Processes, tools and training are in place.</p> |
| Operational Cost | <p>(Financial Management) Cost resulting from running the IT Services. Often repeating payments. For example staff costs, hardware maintenance and electricity (also known as "current expenditure" or "revenue expenditure")</p> <p>See Capital Costs</p> |
| Operational Expenditure (OPEX) | <p>Synonym for Operational Cost.</p> |
| Operational Level Agreement (OLA) | <p>(Service Level Management) An Agreement between an IT Service Provider and another part of the same Business that provides Services to them. For example there could be an OLA with a facilities department to provide air conditioning, or with the procurement department to obtain hardware in agreed times. An OLA may also be between two parts of the same IT Service Provider, for example between the Service Desk and a Support Group.</p> <p>See Service Level Agreement.</p> |
| Operations Bridge | <p>A physical location where IT Services and IT Infrastructure are monitored and managed.</p> <p>See IT Operations, Event Management.</p> |
| Opportunity Cost | <p>(Financial Management) A Cost that is used in deciding between investment choices. Opportunity Cost represents the revenue that would have been generated by using the Resources in a different way. For example the Opportunity Cost of purchasing a new Server may include the loss of interest that the money would otherwise have earned in the bank.</p> <p>See Full Cost, Marginal Cost</p> |
| Optimise | <p>Review, Plan and request Changes, in order to obtain the maximum Efficiency and Effectiveness from a Process, Configuration Item, Application etc.</p> <p>See Continuous Improvement.</p> |

Organisation to Plan

| Term | Definition |
|------------------------|---|
| Organisation | A company, legal entity or other institution. Examples of Organisations that are not companies include International Standards Organisation , ITSMF . The term Organisation is sometimes used to refer to any entity which has People , Resources and Budgets . For example a Project or Business Unit . |
| Outsource | Transferring the provision of IT Services from an Internal Service Provider to an External Service Provider . The term Outsourcing is used to mean making use of an External Service Provider to manage IT Services , or acting as an External Service Provider to manage IT Services . See Insource . |
| Overhead | See Indirect cost |
| Package Release | (Release Management) A single Release that includes a number of Full or Delta Releases . See Release Type |
| Pareto Principle | A technique used to prioritise Activities . The Pareto Principle says that 80% of the value of any activity is created with 20% of the effort. |
| Partnership | A relationship between two Organisations which involves working closely together for common goals or mutual benefit. The IT Service Provider should have a Partnership with the Business , and with Third Parties who are critical to the delivery of IT Services . |
| Percentage utilisation | (Capacity Management) The amount of time that a Component is busy over a given period of time. For example, if a CPU is busy for 1800 seconds in a one hour period, its utilisation is 50% |
| Performance | A measure of what is achieved or delivered by a person, team or Process . See KPI . (Capacity Management) A measure of the overall time taken to carry out one or more Transactions . See Response Time , Throughput . |
| Performance Management | (Capacity Management) The Process responsible for day-to-day Capacity Management Activities . These include monitoring, threshold detection, Performance analysis and Tuning , and implementing changes related to Performance and Capacity . |
| Plan | A Document which identifies a series of Activities and the Resources required to achieve an Objective . For example a Plan to implement a new IT Service or Process . ISO/IEC 20000 requires a Plan for the management of each IT Service Management Process . See Project . |

| Term | Definition |
|----------------------------------|--|
| Plan-Do-Check-Act | <p>A four stage cycle for Process management, devised by Edward Deming. Plan-Do-Check-Act is also called the Deming Cycle.</p> <p>PLAN: Design or revise Processes that support the IT Services.</p> <p>DO: Implement the Plan and manage the Processes.</p> <p>CHECK: Measure the Processes and IT Services, compare with objectives and produce reports</p> <p>ACT: Plan and implement changes to improve the Processes.</p> |
| Planned Downtime | <p>(Availability Management) Agreed time when an IT Service will not be available. Planned Downtime is often used for maintenance, upgrades and testing.</p> <p>See Change Slot, Downtime.</p> |
| Planning | <p>An Activity responsible for creating one or more Plans. For example, Capacity Planning.</p> |
| Policy | <p>Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure etc.</p> |
| Portable Facility | <p>(IT Service Continuity Management) A prefabricated building, or a large vehicle, provided by a Third Party and moved to a site when needed by an IT Service Continuity Plan.</p> <p>See Recovery Option, Fixed Facility.</p> |
| Portfolio Management | <p>(Business Relationship Management) The Process responsible for managing the Portfolio of Services. Portfolio Management includes maximising the value to the Business of existing and proposed new IT Services, and identifying the need to create new IT Services and retire IT Services that are no longer of value. The detailed Planning and implementation work is carried out as part of the Service Planning Process.</p> |
| Portfolio of Services | <p>(Business Relationship Management) A published description of all IT services. The Portfolio is maintained by the Service Provider and includes all IT Services whether they are Live, in Development, or proposed new Services.</p> <p>See Service Catalogue, Application Portfolio.</p> |
| Post Implementation Review (PIR) | <p>A Review that takes place after a Change or a Project has been implemented. A PIR determines if the Change or Project was successful, and identifies opportunities for improvement.</p> |
| Pricing | <p>(Financial Management) Pricing is the Activity for establishing how much Customers will be Charged.</p> <p>See Billing, Charging Process.</p> |
| PRINCE2 | <p>The standard UK government methodology for Project management. See http://www.ogc.gov.uk/prince2/ for more information.</p> |

Priority to Process Control

| Term | Definition |
|------------------------------|---|
| Priority | A Category used to identify the relative importance of an Incident , Problem or Change . Priority is based on Impact and Urgency , and is used to identify required times for actions to be taken. For example the SLA may state that Priority2 Incidents must be resolved within 12 hours. |
| Proactive Problem Management | (Problem Management) Part of the Problem Management Process . The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records , and uses data collected by other IT Service Management Processes to identify trends or significant problems. |
| Problem | The root cause of one or more incidents. See Problem Management , Problem Record . |
| Problem Control | (Problem Management) Part of the Problem Management Process . Problem Control is the Activity responsible for identifying the Root Cause and developing a Workaround or Structural Solution for a Problem. See Error Control . |
| Problem Management | (Problem Management) The Process responsible for managing the Lifecycle of all Problems . The primary objectives of Problem Management are to prevent Incidents from happening, and to minimise the Impact of Incidents that cannot be prevented. Problem Management includes Problem Control , Error Control and Proactive Problem Management . |
| Problem Record | (Problem Management) A Record containing the details of a Problem . Each Problem Record documents the Lifecycle of a single Problem . |
| Procedure | A Document containing steps that specify how to achieve an Activity . Procedures are defined as part of Processes . See Work Instruction . |
| Process | A structured set of Activities designed to accomplish a specific Objective . A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles , responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies , Standards , Guidelines , Activities , and Work Instructions if they are needed. See Business Process . |
| Process Control | The Activity of planning and regulating a Process , with the Objective of performing it in an Effective , Efficient , and consistent manner. |

| Term | Definition |
|---|---|
| Process Manager | A Role responsible for Operational management of a Process . The Process Manager's responsibilities include Planning and co-ordination of all Activities required to carry out, monitor and report on the Process . There may be several Process Managers for one Process , for example regional Change Managers or IT Service Continuity Managers for each data centre. The Process Manager Role is often assigned to the person who carries out the Process Owner Role , but the two Roles may be separate in larger Organisations . |
| Process Maturity | A measure of how reliable, Efficient and Effective a Process is, and of how well it is integrated with other processes. The most mature processes are formally aligned to Business Objectives and Strategy , and are supported by a framework for Continuous Improvement . |
| Process Owner | A Role responsible for ensuring that a Process is Fit for Purpose . The Process Owner's responsibilities include sponsorship, design, and change management of the Process and its Metrics . This Role is often assigned to the same person who carries out the Process Manager Role , but the two Roles may be separate in larger Organisations . |
| Profit Centre | (Financial Management) A Business Unit which charges for Services provided. A Profit Centre can be created with the objective of making a profit, recovering Costs , or running at a loss. An IT Service Provider can be run as a Cost Centre or a Profit Centre. |
| Programme | A number of Projects , that are planned and managed together to achieve an overall Objective . |
| Project | A temporary Organisation , with people and other Resources required to achieve an Objective . Each Project has a Lifecycle that typically includes initiation, Planning , execution, Closure etc. Projects are usually managed using a formal methodology such as PRINCE2 . |
| Projected Service Availability (PSA) | (Change Management) A Document that identifies the effect of planned Changes on agreed Service Levels , based on the Forward Schedule of Change (FSC) . |
| PRojects IN Controlled Environments (PRINCE2) | See PRINCE2 |
| Quality | The ability of a product, Service , or Process to provide the intended value. For example, a hardware Component can be considered to be of high quality if it performs as expected and delivers the required Reliability . Process Quality also requires an ability to monitor Effectiveness and Efficiency , and to improve them if necessary. See Quality Management System . |
| Quality Assurance (QA) | The Process responsible for gaining Assurance that the Quality of a product, Service or Process will provide its intended Value . |

Quality Management System (QMS) to Recovery Point Objective

| Term | Definition |
|---------------------------------|---|
| Quality Management System (QMS) | <p>The set of Processes responsible for ensuring that all work carried out by an Organisation is of a suitable Quality to reliably meet Business Objectives or Service Levels.</p> <p>See ISO 9000.</p> |
| Quick Win | <p>An improvement Activity which is expected to provide a Return on Investment in a short period of time with relatively small Cost and effort.</p> <p>See Pareto Principle.</p> |
| Real Charging | <p>(Financial Management) A Charging Policy where actual money is transferred from the Customer to the IT Service Provider in payment for the delivery of IT Services.</p> <p>See Notional Charging</p> |
| Reciprocal Agreement | <p>(IT Service Continuity Management) A Recovery Option. An agreement between two Organisations to share resources in an emergency. For example, Computer Room space or use of a mainframe.</p> |
| Record | <p>A Document containing the results or other output from a Process or Activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an Audit report, an Incident Record, or the minutes of a meeting.</p> |
| Recovery | <p>(Incident Management) (IT Service Continuity Management) Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users (Restoration).</p> |
| Recovery Centre | <p>(IT Service Continuity Management) Third Party provision of a shared Fixed Facility for use in Recovery.</p> <p>See Recovery Options.</p> |
| Recovery Option | <p>(IT Service Continuity Management) A Strategy for responding to an interruption to Service.</p> <p>Commonly used Strategies are Do Nothing, Manual Workaround, Reciprocal Agreement, Gradual Recovery, Intermediate Recovery, Immediate Recovery. Recovery Options may make use of dedicated facilities, or Third Party facilities shared by multiple Businesses.</p> |
| Recovery Point Objective | <p>(IT Service Continuity Management) The point in time to which data will be restored after recovery of an IT Service. This may involve loss of data. For example a Recovery Point Objective of one day may be supported by daily Backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT Service should be negotiated, agreed and documented.</p> <p>See Business Impact Analysis.</p> |

| Term | Definition |
|-------------------------------------|--|
| Recovery Time Objective | <p>(IT Service Continuity Management) The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets. Recovery Time Objectives for each IT Service should be negotiated, agreed and documented.</p> <p>See Business Impact Analysis.</p> |
| Redundancy | <p>Synonym for Fault Tolerance.</p> <p>The term Redundant also has a generic meaning of obsolete, or no longer needed.</p> |
| Registered Certification Body (RCB) | <p>An Organisation that has been Accredited to perform Certification against a published Standard such as ISO/IEC 17799 or ISO/IEC 20000.</p> |
| Relationship | <p>A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the Business. In Configuration Management it is a link between two Configuration Items that identifies a dependency or connection between them. For example Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to that IT Service.</p> |
| Relationship Processes | <p>The ISO/IEC 20000 Process group that includes Business Relationship Management and Supplier Management.</p> |
| Release | <p>(Release Management) A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.</p> <p>See Full Release, Delta Release, Package Release, Release Identification</p> |
| Release Acceptance | <p>(Release Management) The Activity responsible for testing a Release, and its implementation and Back-out Plans, to ensure they meet the agreed Business and IT Operations Requirements.</p> |
| Release Identification | <p>(Release Management) A naming convention used to uniquely identify a Release. The Release Identification typically includes a reference to the Configuration Item and a version number. For example Microsoft Office 2003 SR2.</p> |
| Release Management | <p>(Release Management) The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management works closely with Configuration Management and Change Management.</p> |
| Release Mechanism | <p>(Release Management) The methodology for deploying a Release to its target Environment. A Release Mechanism may include hardware and software tools as well as Procedures.</p> |
| Release Process | <p>The name used by ISO/IEC 20000 for the Process group that includes Release Management. This group does not include any other Processes.</p> |

Release Record to Resolution Processes

| Term | Definition |
|--------------------------|---|
| Release Record | A Record in the CMDB that defines the content of a Release . A Release Record has Relationships with all Configuration Items that are affected by the Release . |
| Release Type | (Release Management) A Category that is used to classify Releases . A Release Type may be one of Full , Delta or Package Release . |
| Release Unit | (Release Management) Components of an IT Service that are normally Released together. A Release Unit typically includes sufficient components to perform a useful Function . For example one Release Unit could be a Desktop PC, including Hardware, Software, Licenses, Documentation etc.; a different Release Unit may be the complete Payroll Application, including IT Operations Procedures and user training. See Release Type . |
| Reliability | (Availability Management) A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption. Usually measured as MTBF or MTBSI . See Availability . |
| Repair | The replacement or correction of a failed Configuration Item . Often measured as Mean Time to Repair (MTTR) . See Maintainability , Recovery , Restoration of Service . |
| Request for Change (RFC) | (Change Management) A formal proposal for a Change to be made. An RFC includes details of the proposed Change , and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record , or the Change itself. |
| Requirement | A formal statement of what is needed. For example a Service Level Requirement , a Project Requirement or the required Deliverables for a Process . See Statement of Requirements . |
| Resilience | The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure . For example, an armoured cable will resist failure when put under stress. See Fault Tolerance . |
| Resolution | (Incident Management) (Problem Management) Action taken to repair the Root Cause of an Incident or Problem , or to implement a Workaround . In ISO/IEC 20000 , Resolution Processes is the Process group that includes Incident and Problem Management . See Workaround . |
| Resolution Processes | The ISO/IEC 20000 Process group that includes Incident Management and Problem Management . |

| Term | Definition |
|------------------------------------|---|
| Resource Capacity Management (RCM) | <p>(Capacity Management) The Process responsible for understanding the Capacity, Utilisation, and Performance of Configuration Items. Data is collected, recorded and analysed for use in the Capacity Plan.</p> <p>See Service Capacity Management.</p> |
| Resource | <p>A generic term that includes IT Infrastructure, people, money or anything else that might help to deliver an IT Service.</p> <p>See Asset.</p> |
| Response Time | <p>A measure of the time taken to complete an Operation or Transaction. Used in Capacity Management as a measure of IT Infrastructure Performance, and in Incident Management as a measure of the time taken to answer the phone, or to start Diagnosis.</p> |
| Responsiveness | <p>A measurement of the time taken to respond to something. This could be Response Time of a Transaction, or the speed with which an IT Service Provider responds to an Incident or Request for Change etc.</p> |
| Restoration of Service | <p>See Restore.</p> |
| Restore | <p>(Incident Management) Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.</p> |
| Retire | <p>Withdraw an Application, IT Service etc. from use in the Live Environment.</p> |
| Return on Capital Employed (ROCE) | <p>(Financial Management) A measurement of the expected benefit of an investment. Calculated by dividing (Net Profit Before Tax and Interest) by (Total assets minus current liabilities). This ratio is used by business analysts to judge the Effectiveness of the Organisation as a whole. Any changes to IT Services or products are expected to improve this figure.</p> <p>See Cost Effectiveness, Investment Appraisal, Return on Investment.</p> |
| Return on Investment (ROI) | <p>(Financial Management) A measurement of the expected benefit of an investment. Calculated by dividing the average increase in financial benefit (taken over an agreed number of years) by the investment.</p> <p>See Cost Effectiveness, Return on Capital Employed.</p> |
| Return to Normal | <p>(IT Service Continuity Management) The phase of an IT Service Continuity Plan during which full normal operations are resumed. For example, if an alternate data centre has been in use, then this phase will bring the primary data centre back into operation, and restore the ability to invoke IT Service Continuity Plans again.</p> |
| Review | <p>An evaluation of a Change, Problem, Process, Project etc. Reviews are typically carried out at predefined points in the Lifecycle, and especially after Closure. The purpose of a Review is to ensure that all Deliverables have been provided, and to identify opportunities for improvement.</p> <p>See Post Implementation Review.</p> |

Risk to SAM Database

| Term | Definition |
|---------------------------|---|
| Risk | The possibility of suffering harm or loss. In quantitative Risk Management this is calculated as how likely it is that a specific Threat will exploit a particular Vulnerability . |
| Risk Assessment | The initial steps of Risk Management . Analysing the value of Assets to the business, identifying Threats to those Assets , and evaluating how Vulnerable each Asset is to those Threats . See CRAMM . |
| Risk Management | The Process responsible for identifying, assessing and managing Risks . Risk Management can be quantitative (based on numerical data) or qualitative. See Risk Assessment , Risk Treatment , CRAMM . |
| Risk Reduction Measure | Synonym for Control . See Countermeasure . |
| Risk Treatment | The part of Risk Management responsible for choosing and implementing an option for managing a Risk . Options for Risk Treatments include: <ul style="list-style-type: none"> • Applying Cost Effective Controls to reduce the Risk • Deciding to accept the Risk • Avoiding the Risk, by preventing the situation that could lead to it • Transferring the Risk to a Third Party, for example by taking out insurance. |
| Role | A set of responsibilities defined in a Process and assigned to a person or team. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager be carried out by a single person. See Job Description . |
| Rollout | (Release Management) Synonym for Deployment . Most often used to refer to complex or phased Deployments . |
| Root Cause | (Problem Management) The underlying or original cause of an Incident or Problem . |
| Root Cause Analysis (RCA) | (Problem Management) An Activity that identifies the Root Cause of an Incident or Problem . RCA typically concentrates on IT Infrastructure failures . See Service Outage Analysis . |
| Running Costs | Synonym for Operational Costs |
| SAM Database | (Software Asset Management) A Database containing all data needed to support Software Asset Management . The SAM Database could be part of the CMDB . |

| Term | Definition |
|-----------------------------------|--|
| Scalability | The ability of an IT Service , Process , Configuration Item etc. to perform its agreed Function when the Workload or Scope changes. |
| Scope | The boundary, or extent, to which a Process , Procedure , Certification , Contract etc. applies. For example the Scope of Change Management may include all Live IT Services and related Configuration Items , the Scope of an ISO/IEC 20000 Certificate may include all IT Services delivered out of a named data centre. |
| Second-line Support | (Service Desk) (Incident Management) (Problem Management) The second level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems . Each level contains more specialist skills, or has more time or other resources. See Escalation . |
| Security | See Information Security Management |
| Security Management | Synonym for Information Security Management |
| Security Manager | Synonym for Information Security Manager |
| Security Officer | Synonym for Information Security Officer |
| Security Policy | Synonym for Information Security Policy |
| Security Principle | (Security Management) A Strategic Objective in an Information Security Policy . Common Security Principles include Confidentiality , Integrity and Availability . Other Objectives such as Non-Repudiation and Accountability can also be Security Principles. |
| Segregation of duties | (Security Management) A Control that splits up execution of an Activity into multiple Roles which are assigned to different people. This reduces the Risk of a single person exploiting a Vulnerability . For example one person may input financial data and another may check it. |
| Server | A computer that is connected to a network and provides software Functions that are used by other Computers. |
| Service | Providing something of value to a customer that is not goods (physical things with material value). Examples of services include banking and legal support. Service is also used as a Synonym for IT Service . See Business Service , Service Request . |
| Service Capacity Management (SCM) | (Capacity Management) The Activity responsible for understanding the Performance and Capacity of IT Services . The Resources used by each IT Service and the pattern of usage over time are collected, recorded, and analysed for use in the Capacity Plan . See Business Capacity Management , Resource Capacity Management . |

Service Catalogue to Service Level Agreement (SLA)

| Term | Definition |
|--------------------------------|---|
| Service Catalogue | <p>A Document listing all IT Services, with summary information about their SLAs and Customers. The Service Catalogue is created and maintained by the IT Service Provider and is used by all IT Service Management Processes.</p> <p>See Portfolio of Services.</p> |
| Service Culture | <p>A Customer oriented Culture. The major Objectives of a Service Culture are Customer satisfaction and helping the Customer to achieve their Business Objectives.</p> <p>See Business IT Alignment, Customer Focus.</p> |
| Service Delivery | <p>The core IT Service Management Processes that have a Tactical or Strategic focus. In ITIL these are Service Level Management, Capacity Management, IT Service Continuity Management, Availability Management, and Financial Management for IT Services.</p> <p>Service Delivery is also used to mean the delivery of IT Services to Customers.</p> <p>See Service Support.</p> |
| Service Dependency Modelling | <p>A technique that is used to graphically represent the dependency of IT services on Configuration Items.</p> |
| Service Desk | <p>(Service Desk) The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.</p> <p>See Call Centre.</p> |
| Service Hours | <p>(Service Level Management) An agreed time period when a particular IT Service should be Available. For example, "Monday-Friday 08:00 to 17:00 except public holidays". Service Hours should be defined in a Service Level Agreement.</p> |
| Service Improvement Plan (SIP) | <p>A formal Plan to implement improvements to a Process or IT Service. A SIP is managed as part of a Continuous Improvement Process</p> |
| Service Level | <p>Measured and reported achievement against one or more Service Level Targets. Service Level is sometimes used as an informal term to mean Service Level Target.</p> |
| Service Level Agreement (SLA) | <p>(Service Level Management) An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers.</p> <p>See Operational Level Agreement.</p> |

| Term | Definition |
|-------------------------------------|---|
| Service Level Management (SLM) | <p>(Service Level Management) The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.</p> <p>See Service Reporting.</p> |
| Service Level Requirement (SLR) | <p>A Customer Requirement for an aspect of an IT Service. SLRs are based on Business Objectives and are used to negotiate agreed Service Level Targets.</p> <p>See Service Level Agreement.</p> |
| Service Level Target | <p>A commitment that is documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements, and are needed to ensure that the IT Service design is Fit for Purpose. Service Level Targets should be measurable, and are usually based on KPIs.</p> <p>See Service Level, SMART.</p> |
| Service Maintenance Objective (SMO) | <p>(Availability Management) The expected time that a Configuration Item will be unavailable due to planned maintenance Activity.</p> <p>See Planned Downtime.</p> |
| Service Manager | <p>A generic term that can be used to mean any manager within the IT Service Provider. Most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.</p> |
| Service Outage Analysis (SOA) | <p>(Problem Management) (Availability Management) An Activity that identifies underlying causes of an IT Service interruption. SOA identifies opportunities to improve the IT Service Provider's Processes and tools, and not just the IT Infrastructure. SOA is a time constrained, project-like activity, rather than an ongoing process of analysis.</p> <p>See Root Cause Analysis.</p> |
| Service Planning | <p>The Process responsible for implementing and retiring IT Services. Service Planning includes understanding Customer Requirements and Planning the Lifecycle of an IT Service. ISO/IEC 20000 calls this Process "Planning and implementing new or changed services".</p> <p>See Portfolio Management.</p> |
| Service Provider | <p>An Organisation supplying Services to one or more Customers. Service Provider is often used as an abbreviation for IT Service Provider.</p> |
| Service Reporting | <p>(Service Level Management) The Process responsible for producing and delivering reports of achievement and trends against Service Levels. Service Reporting should agree the format, content and frequency of reports with Customers.</p> |

| Term | Definition |
|---|---|
| Service Request | (Service Desk) A request from a User for information or advice, or for a Standard Change . For example to reset a password, or to provide standard IT Services for a new User . Service Requests are usually handled by a Service Desk , and do not require an RFC to be submitted. |
| Service Support | The core IT Service Management Processes that have an Operational focus. These are Incident Management , Problem Management , Configuration Management , Change Management and Release Management . Service Support also includes the Service Desk . See Service Delivery . |
| Serviceability | (Availability Management) The ability of a Third Party Supplier to meet the terms of their Contract . This Contract will include agreed levels of Reliability , Maintainability or Availability for a Configuration Item . |
| Simulation modelling | A technique that creates a detailed model to predict the behaviour of a Configuration Item or IT Service . Simulation Models can be very accurate but are expensive and time consuming to create. A Simulation Model is often created by using the actual Configuration Items that are being modelled, with artificial Workloads or Transactions . They are used in Capacity Management when accurate results are important. A simulation model is sometimes called a Performance Benchmark . |
| Single Point of Contact (SPOC) | Providing a single consistent way to communicate with an Organisation or Business Unit . For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk . |
| Single Point of Failure (SPOF) | Any Configuration Item that can cause an Incident when it fails, and for which a Countermeasure has not been implemented. A SPOF may be a person, or a step in a Process or Activity , as well as a Component of the IT Infrastructure . See Failure . |
| SLAM Chart | (Service Level Management) A Service Level Agreement Monitoring Chart is used to help monitor and report achievements against Service Level Targets . A SLAM Chart is typically colour coded to show whether each agreed Service Level Target has been met, missed, or nearly missed during each of the previous 12 months. |
| SMART | An acronym for helping to remember that targets in Service Level Agreements and Project Plans should be Specific, Measurable, Achievable, Relevant and Time based. |
| Software Asset Management | (Software Asset Management) The Process responsible for management, control and protection of software Assets throughout their Lifecycle . |
| Software Process Improvement and Capability dEtermination (SPICE) | An independent, international Quality Management System for software Development . See http://www.sqi.gu.edu.au/spice/ for more information. See Capability Maturity Model Integration . |

| Term | Definition |
|---------------------------------|---|
| Specification | A formal definition of Requirements . A Specification may be used to define technical or Operational Requirements , and may be internal or external. Many public Standards consist of a Code of Practice and a Specification. The Specification defines the Standard against which an Organisation can be Audited . |
| Stakeholder | All people who have an interest in an Organisation , Project , IT Service etc. Stakeholders may be interested in the Activities , targets, Resources , or Deliverables . Stakeholders may include Customers , Partners , employees, shareholders, owners, etc. |
| Standard | A mandatory Requirement . Examples include ISO/IEC 20000 (an international Standard), an internal security standard for Unix configuration, or a government standard for how financial Records should be maintained. The term Standard is also used to refer to a Code of Practice or Specification published by a Standards Organisation such as ISO or BSI . See Guideline . |
| Standard Change | A pre-approved Change that is low Risk , relatively common and follows a Procedure or Work Instruction . For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request . See Change Model . |
| Standard Cost | (Financial Management) A pre-determined calculation of the Cost of carrying out a common operation. For example a Standard Cost per desktop may be used, rather than calculating the exact Cost each time a desktop PC is provided to a User . |
| Standby | (IT Service Continuity Management) Used to refer to Resources that are not required to deliver the Live IT Services , but are available to support IT Service Continuity Plans . For example a Standby data centre may be maintained to support Hot Standby , Warm Standby or Cold Standby arrangements. |
| Statement of requirements (SOR) | A Document containing all Requirements for a product purchase, or a new or changed IT Service . See Terms of Reference . |
| Status | The name of a required field in many types of Record . It shows the current stage in the Lifecycle of the associated Configuration Item , Incident , Problem etc. |
| Status Accounting | Synonym for Configuration Status Accounting . |
| Storage Management | The Process responsible for managing the storage and maintenance of data throughout its Lifecycle . |
| Strategic | The highest of three levels of Planning and delivery (Strategic, Tactical , Operational). Strategic Activities include Objective setting and long term Planning to achieve the overall Vision . |

Strategic Alignment Objectives Model (SAOM) to Tactical

| Term | Definition |
|---|--|
| Strategic Alignment Objectives Model (SAOM) | A diagram showing the Relationships between Deliverables and Requirements. For example IT Services supporting Business Requirements, IT Infrastructure supporting Technical Requirements. |
| Strategy | A Strategic Plan designed to achieve defined Objectives. |
| Supplier | A Third Party responsible for supplying goods or Services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing Organisations. See Underpinning Contract, Supply Chain. |
| Supplier Management | Supplier Management is one of the ISO/IEC 20000 Relationship Management Processes. It is responsible for ensuring that all Contracts with Suppliers support the needs of the Business, and that all Suppliers meet their contractual commitments. Supplier Management is also responsible for understanding the entire Supply Chain, which includes Suppliers to the IT Service Provider's own major Suppliers. See Supply Chain. |
| Supply Chain | The Activities in a Value Chain carried out by Suppliers. A Supply Chain typically involves multiple Suppliers, each adding value to the product or Service. |
| Support Group | A group of people with technical skills. Support Groups provide the Technical Support needed by all of the IT Service Management Processes. See n-line Support, Technical Support. |
| Support Hours | The times or hours when support is available to the Users. Typically this is the hours when the Service Desk is available. Support Hours should be defined in a Service Level Agreement, and may be different from Service Hours. For example, Service Hours may be 24 hours a day, but the Support Hours may be 07:00 to 19:00. |
| System | A number of related things that work together to achieve an overall Objective. For example: <ul style="list-style-type: none"> • A computer System including hardware, software and Applications. • A management System, including multiple Processes that are planned and managed together. For example a Quality Management System. • A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions. |
| System Management | The part of IT Service Management that focuses on the management of IT Infrastructure rather than Process. |
| Tactical | The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium term Plans required to achieve specific Objectives, typically over a period of weeks to months. |

| Term | Definition |
|----------------------------------|--|
| Technical Observation Post (TOP) | A technique used in Service Improvement , Problem investigation and Availability Management . Technical support staff meet to monitor the behaviour and Performance of an IT Service and make recommendations for improvement. |
| Technical Support | The Process responsible for the technical aspects of supporting IT Services . Technical Support defines the Roles of Support Groups , as well as the tools, Processes and Procedures required. See Support Group . |
| Terms of Reference (TOR) | A Document specifying the Requirements , Scope , Deliverables , Resources and schedule for a Project or Activity . See Statement of Requirements . |
| Test | A Test is used to verify that a Configuration Item , IT Service , Process etc. meets its Specification , and is able to correctly deliver specific Functional or Service Level Requirements . There should be no negative effects on other Processes or IT Services . |
| Test Environment | A controlled Environment used to Test Configuration Items , Builds , IT Services , Processes etc. |
| Third Party | A person, group, or Business who is not part of the Service Level Agreement for an IT Service , but is required to ensure successful delivery of that IT Service . For example a software Supplier , a hardware maintenance company, or a facilities department. Requirements for Third Parties are typically specified in Underpinning Contracts or Operational Level Agreements . See Partnership . |
| Third-line Support | (Service Desk) (Incident Management) (Problem Management) The third level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems . Each level contains more specialist skills, or has more time or other resources. See Escalation . |
| Threat | A threat is any thing that might exploit a Vulnerability . Any potential cause of an Incident can be considered to be a Threat. For example a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management , but also applies to other areas such as Problem and Availability Management . |
| Threshold | The value of a Metric which should cause an Alert to be generated, or management action to be taken. For example "Priority1 Incident not solved within 4 hours", "more than 5 soft disk errors in an hour", or "more than 10 failed changes in a month". |
| Throughput | (Capacity Management) A measure of the number of Transactions , or other Operations , performed in a fixed time. For example 5000 emails sent per hour, or 200 disk I/Os per second. |

Tied Users to Underpinning Contract (UC)

| Term | Definition |
|--------------------------------|--|
| Tied Users | <p>(Financial Management) Users who have no choice about whether to use the IT Services provided by their Internal Service Provider.</p> <p>See Untied Users</p> |
| Total Cost of Ownership (TCO) | <p>(Financial Management) A methodology used to make investment decisions. TCO assesses the full Lifecycle Costs of a Configuration Item, not just the initial cost or purchase price.</p> <p>See Full Cost.</p> |
| Total Quality Management (TQM) | <p>A methodology for managing Continuous Improvement by using a Quality Management System. TQM establishes a Culture involving all people in the Organisation in a Process of continuous monitoring and improvement.</p> |
| Transaction | <p>A discrete Function performed by an IT Service. For example transferring money from one bank account to another. A single Transaction may involve numerous additions, deletions and modifications of data. Either all of these complete successfully or none of them is carried out.</p> |
| Transfer Cost | <p>(Financial Management) Transfer Cost is a Cost Type, which records expenditure made on behalf of another part of the Organisation. For example the IT Service Provider may pay for an external consultant to be used by the Finance department and transfer the Cost to them. The IT Service Provider would record this as a Transfer Cost.</p> |
| Trend Analysis | <p>Analysis of data to identify time related patterns. Trend Analysis is used in Problem Management to identify common Failures or fragile Configuration Items, and in Capacity Management as a Modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.</p> |
| Tuning | <p>(Capacity Management) The Activity responsible for Planning changes to make the most efficient use of Resources. Tuning is part of Performance Management, which also includes Performance monitoring and implementation of the required Changes.</p> |
| Unabsorbed Overhead | <p>(Financial Management) Indirect cost of providing an IT Service, which cannot be fairly allocated to specific Customers. For example Cost of providing an IT Service manager, or other shared Resource which is not measured.</p> <p>Unabsorbed overhead is normally recovered by applying a percentage uplift to the Cost of all IT Services.</p> <p>See also Direct cost, Indirect cost, Absorbed Overhead.</p> |
| Underpinning Contract (UC) | <p>A Contract with an external Third Party that supports delivery of an IT Service by the IT Service Provider to a Customer. The Third Party provides goods or Services that are required by the IT Service Provider to meet agreed Service Level Targets in the SLA with their Customer.</p> |

| Term | Definition |
|--------------------|--|
| Unit Cost | (Financial Management) The Cost of providing a single item. For example, if a box of paper with 1,000 sheets costs £10, then each sheet costs 1p. Similarly if a CPU costs £1m a year and performs 1,000 jobs in a year, the Unit Cost for each job is £1,000. |
| Untied Users | (Financial Management) Users who can choose whether to use the Services provided by an Internal Service Provider or to purchase services from another source. See Tied Users . |
| Urgency | A measure of how long it will be until an Incident , Problem or Change has a significant Impact on the Business . For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the Financial Year . Impact and Urgency are used to assign Priority . |
| Usability | The ease with which an Application , product, or IT Service can be used. Usability Requirements are often included in a Statement of Requirements . |
| User | A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers , as some Customers do not use the IT Service directly. |
| Value Chain | A sequence of Processes that creates a product or Service that is of value to a Customer . Each step of the sequence builds on the previous steps and contributes to the overall product or Service . See Business IT Alignment . |
| Value for Money | An informal measure of Cost Effectiveness . Value for Money is often based on a comparison with the Cost of alternatives. See Cost Benefit Analysis . |
| Variable Cost | (Financial Management) A Cost that depends on how much the IT Service is used, how many products are produced, or something else that cannot be fixed in advance. See Fixed Cost . |
| Variance | The difference between a planned value and the actual measured value. Commonly used in Financial Management , Capacity Management and Service Level Management , but could apply in any area where Plans are in place. |
| Variant | (Configuration Management) A Configuration Item that is identical to another CI except for specific Attributes . Variants are used to group similar CIs together for analysis. For example it may be necessary to identify all Users with a particular model of laptop, even though that laptop has a number of Variants. |
| Vendor-Managed Use | (Software Asset Management) The management of licenses by the Supplier of the software. Licenses may also be managed by the Customer or the IT Service Provider (Customer Managed Use). |

| Term | Definition |
|-------------------------------|--|
| Version | A Version is used to identify a specific Baseline of a Configuration Item . Versions typically use a naming convention that enables the sequence or date of each Baseline to be identified. For example Payroll Application Version 3 contains updated functionality from Version 2. |
| Vision | A description of what the Organisation intends to become in the future. A Vision is created by senior management and is used to help influence Culture and Strategic Planning . |
| Vital Business Function (VBF) | A Function of a Business Process which is critical to the success of the Business . Vital Business Functions are an important consideration of Business Continuity Management , IT Service Continuity Management and Availability Management . |
| Vulnerability | A weakness that could be exploited by a Threat . For example an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be a Vulnerability. |
| Warm Standby | Synonym for Intermediate Recovery . |
| Work in Progress (WIP) | A Status that means Activities have started but are not yet complete. It is commonly used as a Status for Incidents , Problems , Changes etc. |
| Work Instruction | A Document containing detailed instructions that specify exactly what steps to follow to carry out an Activity . A Work Instruction contains much more detail than a Procedure and is only created if very detailed instructions are needed. |
| Workaround | (Incident Management) (Problem Management) Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item . Workarounds for Problems are documented in Known Error Records . Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record . |
| Workload | (Capacity Management) The Resources required to deliver an identifiable part of an IT Service . Workloads may be Categorised by Users , groups of Users , or Functions within the IT Service . This is used to assist in analysing and managing the Capacity , Performance and Utilisation of Configuration Items and IT Services . The term Workload is sometimes used as a synonym for Throughput . |

| Acronym | Term |
|---------|---|
| ACD | Automatic Call Distribution |
| AMDB | Availability Management Database |
| ASP | Application Service Provider |
| BCM | Business Capacity Management |
| BCM | Business Continuity Management |
| BCP | Business Continuity Plan |
| BIA | Business Impact Analysis |
| BITA | Business IT Alignment |
| BRM | Business Relationship Management |
| BSI | British Standards Institution |
| C&CM | Configuration and Change Management |
| CAB | Change Advisory Board |
| CAB/EC | Change Advisory Board / Emergency Committee |
| CAPEX | Capital Expenditure |
| CCTA | Central Computer and Telecommunications Agency |
| CDB | Capacity Management Database |
| CFIA | Component Failure Impact Analysis |
| CI | Configuration Item |
| CMDB | Configuration Management Database |
| CMM | Capability Maturity Model |
| CMMI | Capability Maturity Model Integration |
| COBIT | Control Objectives for Information and related Technology |
| COP | Code of Practice |
| CRAMM | CCTA Risk Analysis & Management Method |
| CSF | Critical Success Factor |
| CSIP | Continuous Service Improvement Programme |
| CTI | Computer Telephony Integration |
| DHS | Definitive Hardware Store |
| DSL | Definitive Software Library |
| EFQM | European Foundation for Quality Management. |

| Acronym | Term |
|---------|--|
| EXIN | Examination Institute for Information Science |
| FTA | Fault Tree Analysis |
| ICMB | ITIL Certification Management Board |
| ISEB | Information Systems Examination Board |
| ISM | Institute of IT Service Management |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITAMM | IT Availability Metrics Model |
| ITIL | IT Infrastructure Library |
| ITSCM | IT Service Continuity Management |
| ITSM | IT Service Management |
| itSMF | IT Service Management Forum |
| IVR | Interactive Voice Response |
| KE | Known Error |
| KPI | Key Performance Indicator |
| MIS | Management Information System |
| MTBF | Mean Time Between Failures |
| MTBSI | Mean Time Between Service Incidents |
| MTTR | Mean Time to Repair |
| OGC | Office of Government Commerce |
| OLA | Operational Level Agreement |
| OPEX | Operational Expenditure |
| OPSI | Office of Public Sector Information |
| PDCA | Plan-Do-Check-Act |
| PIR | Post Implementation Review |
| PRINCE2 | PRojects IN Controlled Environments |
| PSA | Projected Service Availability |
| QA | Quality Assurance |
| QMS | Quality Management System |

| Acronym | Term |
|---------|---|
| RCA | Root Cause Analysis |
| RCB | Registered Certification Body |
| RCM | Resource Capacity Management |
| RFC | Request for Change |
| ROCE | Return on Capital Employed |
| ROI | Return on Investment |
| SAOM | Strategic Alignment Objectives Model |
| SCM | Service Capacity Management |
| SIP | Service Improvement Plan |
| SLA | Service Level Agreement |
| SLM | Service Level Management |
| SLR | Service Level Requirement |
| SMART | Specific, Measurable, Achievable, Relevant, Timely |
| SMO | Service Maintenance Objective |
| SOA | Service Outage Analysis |
| SOR | Statement of Requirements |
| SPICE | Software Process Improvement Capability dEtermination |
| SPOC | Single Point Of Contact |
| SPOF | Single Point Of Failure |
| TCO | Total Cost of Ownership |
| TOP | Technical Observation Post |
| TOR | Terms of Reference |
| TQM | Total Quality Management |
| UC | Underpinning Contract |
| VBF | Vital Business Function |
| WIP | Work in Progress |