SERVICE MANAGEMENT OVERVIEW
Contents

CONTENTS ............................................................................................................................................... 2
IT SERVICE MANAGEMENT ...................................................................................................................... 3
SERVICE DESK ........................................................................................................................................ 6
PROBLEM MANAGEMENT .......................................................................................................................... 10
CHANGE MANAGEMENT ........................................................................................................................... 13
RELEASE MANAGEMENT ........................................................................................................................ 18
CONFIGURATION MANAGEMENT .............................................................................................................. 20
MANAGING THE INCIDENT - PROBLEM - CHANGE LIFECYCLE ............................................................ 21
SERVICE LEVEL MANAGEMENT .............................................................................................................. 23
COST MANAGEMENT ................................................................................................................................ 29
CAPACITY MANAGEMENT ........................................................................................................................ 32
IT SERVICE CONTINUITY MANAGEMENT ............................................................................................... 35
AVAILABILITY MANAGEMENT ............................................................................................................... 38
IT SERVICE MANAGEMENT SUMMARY ................................................................................................. 40
IT Service Management

Introduction

IT Service Management is a set of management disciplines aimed at achieving and maintaining provision of high quality IT services at optimum cost. The disciplines are embodied in the CCTA’s IT Infrastructure Library (ITIL).

The IT Infrastructure Library (ITIL) is a set of manuals maintained by the CCTA which has the aim of giving advice and guidance on the provision of high quality IT services on a wide variety of topics. ITIL has been developed in collaboration with industry experts, consultants, trainers and practitioners and is linked to a customer group, the IT Service Management Forum (ITSMF) which organises regular seminars and meetings throughout the country.

ITIL divides Service Management into two main areas:

Service Support consists of the following disciplines:

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

Service Delivery consists of these disciplines:

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

Formal Service Management Training

The Information Systems Examination Board (ISEB), formerly the Systems Analysis Examination Board (SAEB), currently administers two formal qualifications under the auspices of the British Computer Society. These are the Foundation Certificate in IT Service Management, and the Manager’s Certificate in IT Service Management. The certificates are gained by attending accredited training courses, and then taking formal examinations. The syllabus for both courses and examinations is based upon the IT Service Management modules of the IT Infrastructure Library.

In addition to the above, each discipline within the Support & Delivery sets may be studied and practised in detail. There is a certificate for each separate discipline, attainment of which is achieved by a combination of assignments set during a 3 day training event.
The Need for Service Management

The aim of IT Service Management is to improve the quality of the IT services provided to the customer whilst containing or reducing costs. There are several reasons why high quality IT services are becoming more important to organisations:

- increased dependency on IT services
- higher visibility of IT service failure
- increased complexity of IT services and service provision
- higher customer expectations
- external initiatives such as market testing, outsourcing, Compulsory Competitive Tendering, Facilities Management etc.
- Charging for IT services
- Quality systems - BS5750/ISO9001

Costs

What are the main costs associated with introducing Service Management?

Staff

Carrying out the various roles within the IT Service Management disciplines may require the creation of new posts within the IT department. This will depend upon the size of the organisation, and the scope of the Service Management activities. In small organisations, roles may be shared between existing staff, whilst in larger organisations, dedicated staff may be required. However, it should be noted that increased efficiency brought about by Service Management disciplines can eventually free staff from other areas and ultimately reduce costs.

Training

There will inevitably be training costs involved in moving staff into these new areas and developing their expertise.

Consultancy

Specialist skills may be required to assist an organisation implement one or more of these disciplines.

Tools and Equipment

Specialised software tools may be required to support the Service Management activities. The philosophy of ITIL is to satisfy the main tool requirements of the IT Service Management disciplines with one integrated Service Management database and associated tool set.

Cultural Change

In addition to these purely financial costs, there must also be a major cultural change within the IT department. The transition to a service culture will impose a management burden / cost on senior managers.

Benefits

The main benefits to be derived from adopting Service Management principles are:

- **Greater efficiency and effectiveness** - IT resources are targeted to maintaining and improving aspects of the service which have the most cost-effective benefit to customers.

- **Higher quality IT services** - there is less risk of failure and, when things do go wrong, normal service levels can be restored more quickly.
• **IT unit more business oriented** - IT Service Management principles give the IT organisation the framework to be run as a business or cost centre.

• **Services better matched to customers needs** - formal links with customers on a day-to-day, medium and longer term means that IT services and the service providers can react to business needs.

• **Better management information and metrics** - the collection of management information is recognised by ITIL as a key requirement to ensure that processes function efficiently and effectively.

• **Cost savings** - Ultimately, cost saving will be achieved through ensuring that the optimum use is made of IT resources.
Service Desk

Objectives

The Service Desk is an extremely important pivotal element of Service Management and, together with Service Level Management, makes up the two formal IT Service Management interfaces between customers and IT service providers. The scope of the ITIL Service Desk is much greater than merely being a telephone answering and message passing service. ITIL is very specific about the overall objectives of the Service Desk, and these are seen as being fundamental principles applicable to any organisation:

- To be a single point of contact for customers to report difficulties with IT services.
- To be a focal point for all interested parties
- To restore ‘normal’ service as quickly as possible and thereby maximise service availability
- To take responsibility for the control of incidents from logging through to closure
- To be aware of business needs and the impact of difficulties on business processes.

Terminology

In order to understand the aims of the Service Desk, and the close relationship between the Service Desk and Problem Management more fully, it is necessary to consider the ITIL definitions of “incidents” and “problems”, together with the associated term of “known error”.

An ‘Incident’ is a single occurrence of a difficulty, which is affecting the normal or expected service to the customer. The usual priority when an incident occurs must be to restore normal service as quickly as possible, with minimum disruption to the customers. This may involve the implementation of a ‘workaround’ solution.

A ‘Problem’ is the underlying cause of one or more incidents, the exact nature of which may not yet have been diagnosed. For the Service Desk, restoring service to the customers is the priority and this may involve some investigation and diagnosis. The province of Problem Management is ensuring that the underlying causes are identified and logged.

A ‘Known Error’ is a problem which has been diagnosed and for which a resolution or workaround exists. A Known Error is the result of investigation into a problem and may document either a workaround or a permanent solution. It is Problem Management’s responsibility to ensure that both problems and the associated known errors are logged. This will increase the Service Desk’s chance of resolving future incidents.
Structure and Scope

There are several options that can be considered relating to the architecture and scope of the Service Desk:

Structure

The Service Desk may be set up as:

- A single user system running on a stand alone PC,
- A multi-user system running, for example, a UNIX server, allowing access by a number of Service Desk operators as well as technical support staff,
- A distributed system composed of a number of remote Service Desks able to function independently but logging incidents on a common, centralised database.

The selection of the kind of system depends on the size and the amount of distribution or centralisation within the organisation itself. If a distributed Service Desk is considered, some analysis of the volume and nature of incidents at the remote sites must be carried out to justify implementation of remote incident logging.

Scope

Whichever form of Service Desk is considered to be right for the organisation, another consideration will be the level of skill that is required by the Service Desk operators. The Service Desk could be a non-expert Service Desk in that all incidents, once logged are passed on to specialist groups within the IT organisation. Alternatively, the Service Desk could be an expert one, which aims to resolve a high proportion of incidents without having to refer them to specialist or technical domains.

Service Desk Activities

The following activities are considered to be the responsibility of the Service Desk and comprise ‘Incident Control’ activities.

- The **logging** of ALL calls with a unique call number.

- **Initial support and classification** of incident involving assigning impact, priority and categorisation codes to each call. The impact code conveys the amount of disruption experienced by the customer and allows determination of the priority that should be placed on the call. Once the priority has been established, the appropriate escalation procedures will be defined. The categorisation code is given to each incident to allow the Service Desk to convey the type of incident, assist with incident matching & diagnosis, establish trends, and provide management information.

- **The investigation and diagnosis** of incidents using, when possible, diagnostic scripts and known error logs. This phase may involve referring the incident to technical specialists.

- **The resolution** of incidents, which may involve applying a circumvention or a fix, recovering or restoring services, and ensuring that the customer is kept informed of progress.

- **The formal closure** of incidents, which involves: reviewing the incident log, informing the customer and assigning a closure category. This may be an appropriate time to carry out some form of satisfaction survey.

- **Monitoring and tracking** calls to ensure that they are being progressed in a timely way, and that escalation procedures are being carried out if necessary.
INCIDENT MANAGEMENT WORKFLOW

NEW Incident
Phone/E-mail/Web

Incident LOGGED
Priority/Category Assigned
SLA Targets Set

Routine Incident / Known Error?

yes

Incident Resolved by Service Desk

no

Assign To Support Group or 3rd party

Problem Management

Problem Management
Close related Incidents

RESOLVED
Auto-assign to Service Desk

yes

Customer Agreement?
(Req’d for all calls not resolved by SD)

no

CLOSED
Service Desk Equipment

The use of the right tools and equipment is invaluable in the successful implementation of a Service Desk. Some consideration should be given to:

**Telephony and communications** including hands free operation of telephones, Automatic Call Distribution (ACD), call queuing on busy signal, call redirection capability, answer machines giving both pre-recorded messaging and message receiving capabilities, public address facilities, call statistic collection facilities.

**Diagnostic Aids** such as scripts to follow for common customer calls and easy, electronic access to logs of known problems and errors. This can be achieved by the use of an integrated fully populated Configuration Management Database.

**Integrated systems** will allow incidents and problem details to be passed rapidly and accurately to technical domains and to Problem Management.

Tools chosen must be capable of producing useful and accurate management information.

Possible Difficulties

The following difficulties may arise with the implementation of an ITIL based Service Desk:

- Customers may attempt to **by-pass** the SD and report incidents direct to other IT staff.

- **Cultural acceptance and resistance to change.** Customers may have informal links with support teams and both customers and IT staff may resent the involvement of the Service Desk.

- **Over expectation.** Management must guard against in initial over expectation. It takes time for the skills and procedures and trend data to be fully developed for the Service Desk to become fully effective.

- **Compatibility.** There may be problems of compatibility between tools in use within various service support and delivery functions. Compatibility difficulties may also be experienced in passing problem and error data from development regimes into the Service Desk system.

- The Service Desk may become a **bottle-neck** when a high number of incidents occur or a major problem is experienced.
Problem Management

Problem Management is a wide ranging function covering a variety of diverse activities, which have both short and long term aims. Problem Management’s overall objective is getting to the root cause of incidents, and then instigating actions to improve or correct the situation. In ITIL terms, Problem Management has both a reactive, and a ‘proactive’ mode.

Reactive mode

**Incident Control** - in conjunction with the Service Desk, Problem Management ensures that incidents are dealt with rapidly and effectively.

**Problem Control** - in conjunction with technical domains, Problem Management gets to the root cause of incidents and ensures they are logged as problems.

**Error Control** - Problem Management ensures that sufficient resources are applied to the resolution or circumvention of problems, and that the Known Errors are logged.

**Management Information** - using the incident information accumulated by the Service Desk, Problem Management produces reports on the effectiveness and efficiency of the levels of support provided to customers.

‘Proactive’ mode

Problem Management must:

**Analyse** the mass of information accumulated within incident and problem records.

**Identify** components that are weak, and identify any trends that may become apparent in the nature of incidents and problems over time.

**Instigate** actions to improve or correct weak components or trends.

**Prevent** the occurrence of incidents and problems by feeding back information into development and procurement activities.

Responsibilities and Activities

Initially, Problem Management should be involved in the establishment or review of the Service Desk to ensure that the tools, coding schemes and the processes for dealing with incidents are integrated into ongoing Problem Management activities. Aside from these initial, set-up activities, the work of the Problem Manager can be broken down into day to day and longer term duties:

Day-to-day Responsibilities

**Intervention when escalation times are exceeded** - The Problem Management function must be informed, preferably automatically, when escalation times are likely to be exceeded so the appropriate action can be taken.

**Arbitration where ownership of an incident or problem is in dispute** - Problem Management must ensure that incidents are not ‘bounced’ between technical domains with no group taking responsibility for investigation, diagnosis or resolution.

**Liaison with suppliers and vendor staff** - It is the responsibility of Problem Management to liaise with suppliers and vendors to ensure that incidents and problems are satisfactorily resolved.
Control of major incidents and problems - Problem Management must take control of major incidents and problems, relieving the Service Desk of what may be a time consuming and long running activity.

Post mortem reviews - It is important that as soon as possible after the resolution of a major incident or problem, a post mortem is held. Problem Management must ensure that this is carried out.

Longer Term Responsibilities

Feedback - Information from the investigation and diagnosis of incidents and problems, and the analysis of related information should be fed back into development and procurement functions, into training requirements and into the production of manuals and documentation.

Liaison - Problem Management may be required to liaise with other Service Management functions, particularly Contingency Planning and Service Level Management.

Ensuring that procedures are adhered to - ITIL places the responsibility for auditing the Problem Management function with the Problem Manager. Suitable metrics should be devised which measure the effectiveness and efficiency of the function.

Trend analysis - The Problem Manager must ensure that the volume and nature of incidents is analysed so that, over time, trends can be identified. Information can then be fed back to assist in other areas such as Cost and Capacity Management.

Targeting actions to reduce worst peaks - The Problem Manager should use the incident analysis and trend information to identify the aspects of service support that cause the most ‘pain’ so that problem areas can be targeted.

Benefits

Effective Problem Management will lead to:

- A cycle of increasing IT quality through a reduced number of incidents having a lower impact on service quality due to quicker recovery.
- Improved customer productivity through higher service availability.
- Learning from past experiences.
- Improved productivity of support staff through ensuring that the effort spent on investigating, diagnosing and resolving incidents and their underlying problems is prioritised according to business impact.
- A good reputation for IT directorate and their staff by dealing efficiently with customers difficulties
- Greater control of IT services through meaningful management information.
Change Management

What is Change Management and Why is it Needed?

As technology develops, both hardware and software components are much less liable to fail, and are therefore more reliable. Customers have therefore come to expect much higher rates of availability and reliability of IT services as a consequence of similar improvements at the component level.

With a reduction in the overall number of failures, attention focuses on those failures that do occur, and what is done to recover from them. Statistical evidence, shows that a significant number of failures are attributable to the result of badly applied changes to both hardware and software systems.

It is a natural trait of many of the most committed technical staff to feel obliged to 'improve' systems, even when customers have not reported anything wrong! This tendency to fix something which is not broken is not always in the best interests of the organisation as a whole, and may be something which should be brought under control. At the other end of the spectrum, an organisation that rigidly adopts a ‘fix-on-fail’ policy cannot hope to react to the demands of its customers who will want functional changes made to services to satisfy their business requirements.

The IT Infrastructure Library recommends:

- A single, centralised change management system for the whole of the IT infrastructure.
- Integration as part of a comprehensive configuration management system

Anything that needs to be controlled could be brought into the scope of Change Management, but in most IT organisations, it is likely that the change management system will cover:

- Hardware
- System Software
- Communications Equipment and Software
- 'Live' Applications Software
- All documentation and procedures relevant to the running, support and maintenance of live systems.
- Environmental Equipment

Roles and Responsibilities

ITIL defines a number of roles, which should be carried out within the process.

**Change Manager**

The Change Manager has overall responsibility for managing the change management process and ensuring that there are no bottlenecks causing delays in processing change requests. The process design must suit the size and the needs of the organisation, so the role of Change Manager in a small organisation may be a part-time role, shared with other duties. In a large organisation, the Change Manager may have a number of staff to assist in making sure the process runs smoothly, and change requests are dealt with appropriately.
Change Advisory Board (CAB)

The Change Advisory Board is the body which is responsible for assessing proposed changes for impact and estimating the resource requirements. They will advise the Change Manager on whether changes should be approved and assist in scheduling changes.

The Change Manager is responsible for arranging CAB meetings at suitable frequencies, and may involve anyone with an interest in reviewing and assessing change requests.

The CAB Executive Committee (CAB/EC)

It may not always be possible or desirable to convene a full CAB meeting to assess certain changes, if they are urgent for example. It is recommended, however, that even urgent changes are given some form of assessment, and the Change Manager may call on a subset of the CAB, who can be contacted quickly, to give some approval to urgent changes.

Normal Change Procedures

Change Initiation

It is normal to allow changes to be initiated by any technical staff, but to route customer change requests through some form of customer liaison structure, or the normal customer management structure. This will eliminate impractical changes, allow multiple requests to be co-ordinated and ensure that changes are supported by a wide customer base.

In either case, change requests should be logged, preferably on a centralised or common database, and given a unique identification number.

Initial Filter

The Change Manager should filter requests and reject any that are incomplete, impractical, undesirable or repetitive. An appeal process should be available.

Assign Priority

The Change Manager must decide whether the change is urgent or not. Urgent changes should be dealt with via special urgent change procedures, while non-urgent requests continue to be processed by the route described below.

Decide Category

The Change Manager should categorise requests. ITIL suggests three categories, described as ‘Minor’, ‘More than minor’, and ‘Major’. Categorisation is carried out by evaluating factors such as the resources required to carry out the change, the impact of implementing it (or not implementing it) and the risks associated with implementation.

Change Assessment

The Change Manager should have authority to assess and authorise ‘Minor’ changes, which are of low risk, low impact and low resources.

‘Major’ changes may have to be referred to a higher authority, the board for example, to be authorised, as they are liable to be costly or have a high impact.

For ‘Normal’ or ‘more than minor’ changes, the CAB members should assess changes for impact and estimate the required resources. They will decide whether to support the change, confirm the priority and schedule the change accordingly. The Change Manager should have the final decision on whether the change is authorised.

This whole process may be iterative and change requests may need to be referred elsewhere for further investigation into impact, cost and risk.
Change Building
If the change is authorised, the appropriate person or group will prepare and build the change, and will devise back-out (regression) and testing plans.

Change Testing
An independent testing authority should test the change and also the proposed regression plans. Only when such testing is satisfactorily completed should further progress be allowed.

Implementation
When testing is completed satisfactorily, the Change Manager will co-ordinate the implementation of the change and invoke the back-out plan if required.

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 improve future estimating.

Urgent Change Procedures
Even urgent changes should be dealt with in a strictly controlled way - but special procedures must exist to allow this to be done quickly. In general, the normal processes should be carried out, but rapidly. Assessment may be carried out by the CAB/EC, and it is important that testing is carried out if time allows.

It will not always be possible to update all records as the change progresses - priority often has to be given to actually getting the urgent change installed. It is however important that as soon as possible after the urgency is overcome all normal procedures are carried out and appropriate records are brought up to date. The review process should ensure that this is done.
CHANGE MANAGEMENT WORKFLOW

INITIATION
RFC Logged on AHD

Rejected?

yes

CLOSE

PRIORITISATION

no

Urgent?

yes

Urgent Procs pg 14

no

CATEGORISATION
(Resource, Impact, Risk)

MAJOR
CAB or Higher Authority

SIGNIFICANT
CAB Authorises

MINOR
CM Authorises

Authorised?

no

CLOSE

yes

SCHEDULING
(Resources Assigned)

BUILD
(Back-out & Test Plans)

TESTING
(Change & Back-out Plan)

IMPLEMENT

Successful?

no

Back-out Plan Invoked

yes

SIGN-OFF
(Requester / Authoriser)

REVIEW

CLOSE

Exception Report
Release Management

Interfaces to Configuration Management and Change Management.

Whereas configuration management is responsible for managing the logical control of Configuration Items (CIs), including software CIs – Release Management (RM) is responsible for the physical aspects of software control. Release Management activities will normally be triggered by the Change process e.g. in response to a request to build, distribute and implement a new software release.

Purpose

The RM function involves:

- Physical storage, protection, distribution and implementation of all software
- Ensuring only correctly released and authorised versions of software are in use
- Managing the organisations rights and obligations regarding software

Benefits

The benefits to the organisation of having an effective RM function are that:

- the important rights and obligations regarding software will be managed
- valuable software assets will be securely protected and released into the live environment in a controlled way to the customers who require to use them.

Main Elements

The main elements of RM are:

**Definitive Software Library (DSL)**

The DSL is a secure software library, containing all versions of software CIs, in their definitive, quality controlled form.

Although the DSL is logically a single library, ring-fenced from other parts of the environment, it may have to consist of more than one physical location.

Strict controls must exist regarding input to and output from the library.

**Release Build**

Release building is a set of processes whereby a software release is built from items in the DSL, selected by reference to the Configuration Management Database (CMDB).

A release record will be created in the CMDB when the Change Advisory Board decides the contents of the release.

**Distribution**

This is the process of copying the software releases from the build environment into the test and, later, live environments, which may be very widely distributed.

**Implementation**

The process of bringing the software into live use at the target locations. There may be a requirement to coordinate this action over many widely distributed locations so that they each ‘go live’ at exactly the same time.
Release Policy

As part of an overall release policy the organisation must decide the normal release units for each software item. The policy must decide whether delta releases are to be allowed and the extent to which full and package releases will be used. Urgent releases will invariably be required and so the policy should accommodate these.

A Delta Release is a release of software, which contains only those components that have changed since the last release.

A Full Release is a release of software that contains all components, whether they have changed or not.

A Package Release is a release of one or more Full releases, which are introduced into the test and the live environments, together with documentation, as a unit.

Any of the above types of release may have to be made urgently.
Configuration Management

Almost all of the information that is required to successfully implement Service Management is available somewhere within the installation. Unfortunately it tends to be scattered around the organisation, usually stored in a variety of differing formats.

The central repository of information for IT Service Management is known as the Configuration Management Database (CMDB). The CMDB need not exist physically as a single datastore, but must appear as such to the user. In other words, a virtual CMDB using compatible underlying datastores may be more practical and easier to achieve for medium to large organisations.

Scope

Configuration Management techniques should be applied to any component of the IT infrastructure which needs to be controlled. This will include hardware, software, networks, documentation and staff. To achieve the full benefit, other components such as incident logs, problem records and change requests will be brought into Configuration Management, and registered on the CMDB.

Concepts

There are a number of basic terms that apply to Configuration Management. These are:

**Configuration Item** - any component, which it is wished to control, is a configuration item (CI). CIs may themselves be broken down into sub-components which are also CIs.

**Attribute** - an attribute is any piece of information that may be used to describe a CI. Size, cost, weight, age, status could all be attributes of one or more CIs.

**Relationship** - a relationship is the link or association that exists between two or more CIs.

**Baseline** - a baseline is a set of CIs that is frozen at some procedural point, or point in time. A standard PC configuration or a particular version of a software application can be thought of as baselines.

**Lifecycle** - all CIs have their own lifecycle, and many CIs may share a similar lifecycle. A lifecycle is merely the stages that a CI goes through during its useful life within the organisation.

Activities

Planning and implementing Configuration Management is a major task, and it is important that the scope of the function and the design of the processes and database are carried out effectively. The level of breakdown of CIs, the amount of attributes and the nature of the relationships must all be considered. Implementation will be made easier if it is phased in alongside Change Management.

**Identification** - Configuration Management must ensure that all relevant CIs are identified as components of the IT Infrastructure and, once appropriate quality checks have been carried out, must ensure that the CI details, attributes and relationships are entered on the CMDB.

**Control** - In order to exercise control and management over CIs, the Configuration Manager must agree and freeze the specification of CIs, and then only allow changes if pre-defined Change Management procedures have been followed, and if the appropriate authority has been given.

**Status Accounting** - This function of Configuration Management records and reports on the current and historical status of all CIs.

**Verification** - The verification function of Configuration Management ensures that the CMDB remains accurate and consistent. Regular and ad-hoc audits may be carried out and operational checks to ensure
accuracy of records may be made. Regular reviews of the Configuration Management function itself should be made to ensure processes and procedures for maintaining the CMDB are working effectively and efficiently.

Managing the Incident - Problem - Change Lifecycle

The Vicious Circle

Problems and changes are often very closely linked. If adequate procedures do not exist to manage both problems and changes then a “vicious circle” can result.

An incident reported to the Service Desk is investigated and the underlying problem is identified. In order to overcome the problem a change is proposed. At some later point this change is implemented.

As occurs all too often, if the problem has not been managed properly, or the change has not been adequately tested or assessed for impact, then when the change is finally implemented further incidents will result. In some cases the new incidents can be more serious than the ones the change was supposed to correct.

A Configuration Management system can assist the organisation to manage problems and changes efficiently and effectively, and thereby break this vicious circle. Each of the disciplines involved in the process benefit from the effective use of the CMDB.

Service Desk

When the Service Desk logs an incident (as a CI on the CMDB), a few simple questions (Who are you?, Where are you?) are all that are required to gain access to a wealth of information about the customer, the equipment held, the services accessed, the problem history, the incident history, known error logs, the change history etc., etc.

Problem Management

Configuration management will assist the Problem Manager by providing:

- automatic escalation
- problem logging
- highlighting trends - incident/problem history
- problem matching and known errors identification
- relationship identification and information on recent changes
- the 'cost of a fix' to be compared with the 'cost' if no action is taken.

Although some problems may be resolved without the need for changes, to overcome the majority of problems some form of change will be required.

Change Management

The management of change is one of the most difficult areas to control. In many installations it is not done properly and as a result, problems occur which impact upon service quality.
The management of change is one of the areas where configuration management can be of greatest assistance. It can help in the following ways:

- pre-change status is known
- identification of affected CIs
- identification of owners (for impact assessment)
- cross reference to incidents/problems and other changes
- improves resource assessment - reference to past records
- allows release record to be created
- speeds up the change management process
- risk assessment

To implement the changes that have been approved and prepared, some form of implementation (e.g. a software release or hardware amendment/installation) will be required. For hardware changes this is often straightforward and CM will just be used to record that the change has been implemented. Software changes are, on the other hand, one of the most difficult areas to control, perhaps because software is less tangible than other configuration items and because it is possible to create many identical copies of the same software and have them in existence at the same time.

**Release Management**

Configuration Management can help in managing the control and distribution of software, by assisting in the following tasks:

- recording the location of software, code control
- release building
- identifying who needs new releases
- implementation
- software audits, licence management, observing the data protection act, identifying unused software
- software recovery from corruption, loss or disaster
Service Level Management

Definition

“A Service Level Agreement is a written agreement between the customer and the IT service provider that documents agreed service levels for an IT service”.

Motivations for SLAs

Organisations are motivated towards SLAs because of:

- Increased dependency upon IT services
- Higher visibility of service failures
- Customer Demands
- Management initiatives
- Interest in Facilities Management
- Charging for services.

The establishment of SLAs is often, though not always, the initiative of the IT services provider. In any case, SLAs cannot be set up without the co-operation of both customers and IT providers, and it is the IT service providers who will have to ensure that monitoring and reporting of service levels is carried out.

Much preparation will be required to ensure that customers and IT services are accurately identified, and that the SLA structure reflects what may be complex relationships between customers and services. It will be necessary also to ensure that support service levels underpin SLAs by the establishment of Operational Level Agreements (OLAs) and contracts.

Benefits

The main benefits of Service Level Agreements are that:

- Both sides have a clearer view of requirements and responsibilities
- The metrics within an SLA provide a target to aim for
- SLAs allow better forward planning in that knowledge of customer’s future requirements will ensure that sufficient IT capacity is available when required
- SLAs provide essential measurement criteria where Facilities Management agreements exist - they should be included as part of the formal contract
- IT service providers can use SLAs as a way of measuring and demonstrating their performance
- The Service Improvement Programme (SIP) will indicate weak areas or will show when targets are easily being met over long periods.
Difficulties

There are a number of common difficulties to do with implementing and managing Service Level Agreements. These include:

- Ensuring that the proposed service targets are actually achievable
- Verifying this achievability prior to the signing of the agreement
- Monitoring the actual achievements accurately and impartially, to avoid disputes with the customers
- Under estimating the resources and effort involved in planning for and then monitoring SLAs

Typical SLA Contents

There are no hard and fast rules for which elements should be included in the SLA, other than the rule that all service levels and targets quoted in SLAs must be able to be monitored. ITIL recommends that the following elements should be considered for inclusion.

**Contents** - Details such as version number, date created, date amended, start and end dates together with a table of contents.

**Administration** - Details of who is responsible for maintaining the SLA, how it is updated and distributed and a history of releases and issue dates.

**Signatures** - The signatures of the IT and Customer representatives and their job titles.

**Contacts and Support** - Details of who to contact concerning the agreement, who to contact for support, hours of availability of support, escalation procedures and any penalty or bonus clauses which may apply.

**Specification of Parties** - A short description of the IT service provider and the customer.

**Summary of Responsibilities** - A description of any responsibilities imposed on either party.

**Management Reporting** - Specification of management reporting on the SLA with contents and delivery times.

**Specification of Services** - The specification of the agreed service levels. This will include a more detailed description of the service involved, the hours of availability, maintenance times, support times, deliverables and delivery times, quality targets such as availability, reliability, usability and priorities. This section should also specify the procedures for requesting changes, and the contingency plans, if any.

**Review Procedure** - A description of the procedure to review the SLA, agreed by both parties. This should include the scheduled review dates and the procedures for amending the SLA content.

**Index and Definitions** - It may be necessary to include appendices such as a glossary of terms and definitions.
Planning for SLAs

The following steps will be required when planning SLA's:

**Awareness Campaign**

The objectives of the awareness campaign are to:

- raise the profile of SLA's throughout the organisation
- advise customers of potential benefits
- inform customers and IT staff of how they will be affected
- discuss and agree an implementation schedule
- seek customer support and co-operation

Seminars and presentations, followed up by circulars and newsletters detailing progress will be the main vehicles for the campaign

**Catalogue Existing Services**

This entails detailing all the services currently offered by the IT department, recording who their customers are, and recording any existing customer expectations and deadlines.

**Formulate Agreement Structure**

This can be a difficult task. The aim is to 'map' customers and services to SLA's. It will involve:

- deciding how many SLA's are needed
- establishing which services are to be included in each SLA
- determining which customers are to be covered by each SLA, and the signatories
- deciding the exact elements to be included in each SLA
- proposing the initial service levels to be included in the first draft of each SLA.

The structure or mapping of customers to services can be quite complex, and the Service Catalogue will be invaluable information for defining the top-level structure.

**Establish Initial Service Levels**

Existing service levels should be reviewed and discussed with customers, and these will form the basis for initial service levels to go into the SLA.

It is important that monitoring activities are instigated if not already in place. A key rule for SLAs is not to include any levels or targets that cannot be monitored and reported on.

**Negotiate with Customers**

Initial drafts of the proposed SLA's should go to the customers for comment prior to negotiation of service levels.

Where customers demand more ambitious levels than currently provided, and where this would require additional expenditure or resource, then they must be made aware of the potential cost, and be prepared to pay if necessary. Provision of historical data about recent service level achievements will assist customers in providing accurate estimates of future workloads.
Wording of Agreements

Keep wording clear and concise. Avoid technical or legal jargon wherever possible, and provide a glossary for those technical terms that are unavoidable.

Review Underpinning Contracts

Examine contracts for support services upon which you are dependent, for example, hardware engineer cover, communications equipment support etc. You cannot offer better levels of service in SLAs than you are provided with by your own internal or external support arrangements.

Service Monitoring

It is pointless to offer something in an SLA that neither party can monitor for achievement. Monitoring capabilities must be examined and upgraded as required.

It may also be necessary to set up interfaces with the Service Desk to monitor aspects of customer satisfaction that cannot automatically be monitored at machine level.

Service Reviews

Plan regular review meetings with customers to discuss service achievements during the previous period and to agree any necessary action or new targets.

Ideally, meetings should be held quarterly, and reports of service level achievements should be distributed a few days before the meeting.

SLA Schedule

Providing financial planning considerations allow, it can be helpful to spread the SLA manager's workload by staggering re-negotiation of SLA's throughout the year. This would also result in an even distribution of review meetings.

Contingency Planning

Brief details of contingency plans should be included in the SLA. Consideration must also be given to different service levels prevailing following implementation of contingency plans. Where appropriate, separate SLA's may need to be agreed.

Other Planning Considerations

A number of support disciplines will be required if SLA's are to be managed successfully. These include Service Desk, Change and Problem Management, Capacity Management, and Cost Management, ideally all underpinned by Configuration Management.. Where these functions do not exist, consideration should be given to the need to establish them.

Plan for Growth

You should:

- anticipate new services requiring SLAs
- identify changes in throughput and usage rates of existing services
- staff the service level management function accordingly.
Reporting

At the end of each agreement period, a few days prior to each service review meeting, a summary report detailing services achievements during the full period should be produced and distributed to customer and computer management.

Ideally such reports should be in graphical format and easy to assimilate.

Comparative results from previous periods will help to set the results in context, so should be made available.

In between reviews interim reports (weekly and perhaps monthly) may be necessary, particularly if there are lengthy agreement period (E.g. 13 weeks, 6 months).

A daily report may be required by the Service Level Manager, but if possible this should be restricted to just exception details.

Service Improvement Programme (SIP)

An agenda item of Service Reviews is ‘Service Improvement’. In order to continue to strive towards service excellence, it is important not to sit back & relax even if all service targets are being achieved and customer satisfaction ratings are good, but to continually review the way customer service is provided with a view to identifying areas for improvement. In this way IT departments can continue to gain competitive advantage in the provision of customer service.

IT SERVICE STRUCTURE
<table>
<thead>
<tr>
<th>CUSTOMERS</th>
<th>Service Deliverers</th>
<th>Service Support staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level Agreements</td>
<td>Help Desk</td>
<td>Operating systems</td>
</tr>
<tr>
<td>Service Contracts</td>
<td>Operations</td>
<td>Networks</td>
</tr>
<tr>
<td>Reporting of Incidents</td>
<td>Installations</td>
<td>Applications Development</td>
</tr>
<tr>
<td>Requests for Change</td>
<td>Project Management</td>
<td>Hardware &amp; Software Maintenance</td>
</tr>
<tr>
<td></td>
<td>Account Managers</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Management</td>
</tr>
</tbody>
</table>

- **Help Desk**
- **Operations**
- **Installations**
- **Project Management**
- **Account Managers**

**Service Support staff**
- Operating systems
- Networks
- Applications Development
- Hardware & Software Maintenance
- Admin
- IT Management
**Cost Management**

There are two distinct sides to the topic of Cost Management: Costing and Charging. These two elements are described below.

**Costing**

This is the process of determining the true cost of providing IT services and identifying where, and by whom, resources are being used.

Even where charging is not in place, most organisations will have some idea of what it costs to provide services and all organisations need to manage costs, even though they may not charge for the services provided.

**Charging**

This element is concerned with recovering costs from customers in a fair and equitable way.

**Benefits**

The most significant benefit from performing accurate costing of providing IT services is that senior management can be made aware of the true cost of providing those IT services which support the organisation's business needs. The IT Services department cannot take decisions on quality of service against cost without this information. As a general rule, any increase in the cost of providing a service should result in an increase in the quality of that service.

Costing enables the IT Services Manager to:

- make decisions based on the cost effectiveness of each service
- make decisions about services and investment with the benefit of full business information
- provide proper, costed justification for IT expenditure
- plan and budget with confidence in the financial forecasts
- understand the costs of failing to take advantage of strategic opportunities to justify the required expenditure (thereby providing value added productivity)

In summary, IT service providers are unlikely to provide maximum value for money if they do not know the cost of providing the service. It follows therefore, that if the aim of the IT services department is to offer maximum value for money, then costing is essential.

**IT Costing**

**Cost Units**

The ITIL module 'Cost Management for IT Services' includes considerable detail on the various accounting techniques which should be adopted when costing IT services. Many organisations will have accounting and financial departments whose job is to carry out these practices on behalf of the whole organisation. It is useful, however, for IT staff to have some understanding of the basic principles.

It is suggested that costs should be examined and allocated to ‘Cost Units’. A Cost Unit refers to the accumulated costs from a particular source that will be used for calculating a unit cost or rate.

There are five major cost units, which can be used to allocate IT costs:
• **Equipment** cost unit - covering all central and distributed hardware devices.
• **Software** cost unit - covering all application and system software including PC based tools.
• **Organisation** cost unit - covering costs relating to staff, training salaries, overtime etc.
• **Accommodation** cost unit - covering buildings and ancillary service costs.
• **Transfer** cost unit - this cost unit can be used to account for internal costs, which may be cross-charged to other departments.

**Projecting Costs**

This is the process of estimating the costs of providing the IT services over the coming financial period, usually one year. Firstly, this is defined as the total cost of the resources needed to provide the services. This is then split down to the cost units defined above and then the usage by individual services is estimated for each of the cost units.

Information for estimating usage by the services will be available from several sources:

- **Service Level Agreements** - these should always contain customer estimates of service usage.
- **Capacity Plans** - will contain longer-term estimates of resource requirement which will affect costing, e.g. equipment upgrade.
- **Customer business plans** - may be used in conjunction with SLAs.
- **The organisation's strategy** - the IT departments cost estimates must be compatible with the overall business forecasts for the organisation.

The total costs of providing the IT services are broken down for each workload by cost units.

**Charging for IT services**

**Why Introduce Charging for IT Services?**

There are a number of valid reasons why you might wish to charge for IT services:

- To improve cost consciousness amongst the customer departments
- To achieve better utilisation of resources
- To allow comparisons to be made of the costs of buying the service from alternative suppliers, as required for initiatives such as outsourcing
- To allow demand management by differential charging
- To recover IT costs in an equitable manner, according to IT demands
- To inform customers how charges are derived, allowing them to influence usage/charges
- To raise revenue

**Charging Options**

Charging for IT services involves balancing the costs of providing the services against the charges that are to be made. Whether the aim is to break-even or to make a profit, the basic principles remain the same. In some circumstances, the IT department may even be subsidised by the owning organisation, in effect running at an operating loss or making a negative profit.

There are many charging methods available. Some of the most commonly used are described below:
Direct Charging
This is where dedicated equipment, goods or services provided to one customer (or customer group) can be passed directly to the customer. The cost may be the full purchase cost, annual proportion, rental etc.

Resource Usage
This is where customers are charged according to monitored resource usage, for example CPU seconds, Filestore transfers, I/Os etc.

The main advantage of this method is that it can accurately reflect the true resources that are being consumed. A disadvantage is that monitoring may be difficult to achieve.

Output Related
This is where a fixed cost is made for each particular transaction type or unit of business process. For example, 50p per pay-slip, or £1 per change of name transaction.

These kind of charges must be based upon accurate monitored data. This method is recommended by the Audit Commission because charges are easy for customers to understand. It also gives them the opportunity to influence their charges, which may be a problem for the IT service provider.

Apportionment
This method is used where shared goods or services are provided and where it may be difficult to identify usage by individual customer groups. Examples of services whose cost may be apportioned include a corporate database back-up, or the corporate contingency plan. Apportionment must be seen to be fair and equitable, and customers must feel content with the outcome.

Market Price
This is where charges are made according to ‘what the market will bear’. To establish a competitive market price it will be necessary to conduct market research and to set charges relative to those made by alternative suppliers.

Overall Charging System
It is likely that it may require a combination of some, or all of these methods to arrive at an overall acceptable charging system.

Common Difficulties
Many difficulties may be encountered when implementing a charging policy. There may be problems, for example, of surplus capacity, especially if output related charging is adopted and there may be problems with obtaining accurate information on which to base charges.

The ITIL module on Cost Management gives some guidance on how to overcome these difficulties.
Capacity Management

Capacity Management is concerned with having the appropriate IT capacity, and making the best use of it. It is also concerned with balancing capacity so as not to incur the performance penalties resulting from too little capacity, while not incurring the cost penalties of carrying too much capacity.

Benefits

The benefits to be derived from effective Capacity Management are usually seen in improvements in overall efficiency, effectiveness and the provision of more economic services. Some of the major benefits are described below:

Reduced Risk and Increased Efficiency - Effective Capacity Management will ensure that there is always adequate capacity to run the workloads that the organisation demands. Capacity Management reduces the risk that lack of capacity may prevent the IT service provider supplying the quality services needed to support the organisation's business.

Cost Savings - Good Capacity Management will lead to cost savings. Some of the ways in which cost savings may be achieved are:

- the ability to accurately budget for changes in capacity
- the provision of better quality IT services will improve the productivity of the services customers, e.g. by reduced response times
- IT capacity costs are controlled, and possibly reduced, as there will be no unplanned excess capacity, and available capacity is used efficiently.
- low cost performance improvements can sometimes be identified which will contribute to more economical service provision
- planned buying is cheaper than panic buying!

Value to Other Disciplines - Capacity Management is valuable to other disciplines, especially Service Level Management, and Cost Management.

Possible Problems

There are a number of possible problems associated with the implementation of Capacity Management principles. These are listed below:

Over Expectation - Major savings are seldom made through tuning. A one-off saving can sometimes be made by correcting a design or installation error. Once the error is corrected these savings cannot be repeated.

Customer Expectation - Customer expectations of response times are often not technically feasible or affordable. For new applications, customers must be made aware of realistic response times, turn round times and throughput rates at the earliest opportunity.

Vendor Influence - Sizing should be the responsibility of the Capacity Manager, not the vendor. Beware of throughput estimates based on benchmark figures or numbers of terminals connected supplied by vendors.

Lack of Information - Acquiring information from customers on their intended use of systems is often difficult. The Capacity Manager must help by supplying statistical information on existing usage to allow more informed projections. The use of Service Level Agreements will greatly assist in this area.
Scope

The key elements of Capacity Management are described below:

Performance Management

This element is concerned with monitoring systems, analysing the data, detecting trends and implementing tuning techniques to improve performance. This is an iterative process. Monitoring facilities should be designed into systems to allow future tuning to be carried out.

Capacity Management Database (CDB)

The CDB is conceptually a single database, though in practice may consist of several, perhaps many, physical storage areas comprising all the information required to carry out Capacity Management. Much of the information required for the CDB may be found in the CMDB.

The CDB should allow access to:

- Mainframe technical data
- Network technical data
- Business metrics - number of terminals, branches, staffing, clients accounts supported etc.
- Service related data - numbers of transactions processed, payslips produced etc.

Workload Management

The aims of workload management are to:

- Identify, document and understand each workload
- Determine the resource requirements of each workload
- Understand working patterns and peaks
- Implement an effective workload forecasting system to identify changes in volumes and changes in functionality

Demand Management

Effective workload management facilitates demand management. Once working patterns and peaks are understood, peaks and troughs in usage can be identified. Demand management is concerned with taking steps to influence customer behaviour to smooth these peaks and fill the troughs to achieve optimum usage.

Application Sizing

The primary objective of Application Sizing is to estimate the IT resources required to support a proposed application and meet service levels. This applies to both in-house developments and to bought-in packages. Capacity Management should be involved in the selection and development of software to ensure that the right IT resources are available when the application goes live, and that there is no deleterious effect on existing services.
Modelling

Modelling can be described as the ability to predict the behaviour of a computer system under a given volume and variety of work.

There are various modelling techniques available, ranging from best guesses, through to the use of sophisticated software tools. The two most viable methods, which give acceptable degrees of accuracy, are simulated modelling and analytical modelling.

Simulated modelling involves using as much as possible of the real system or configuration under controlled conditions, while analytical modelling involves the use of mathematical algorithms to model workloads. Both methods have advantages and disadvantages to do with cost, accuracy and ease of use.

Resource Management

Resource Management is a title used to cover a number of diverse activities that might be undertaken by the Capacity Management function. These include:

- Holding diagrams and schedules - Capacity Management should ensure that useful diagrams, maps, pictures and schedules are maintained.
- Resilience - Capacity Management should be involved in ensuring that any resilience features exploited are sized for throughput and capacity.
- Storage Management - this activity is to do with ensuring that magnetic media is stored and identified correctly, and archiving, back-up and tidying processes are working correctly.
- External Interfaces and new technology - Capacity Management should be keeping abreast of new developments via user groups, seminars, conferences and shows etc.

Production of a Capacity Plan

The overall objective of Capacity Management is to produce a Capacity Plan at agreed intervals which fits into the business planning cycle, for example the financial year. ITIL recommends that a forward looking Capacity Plan is produced and updated periodically in line with both changes to business demand and advances in the technology available.

The Plan should document current resource usage, identify potential scenarios for future development, and predict the resources required to support the most likely scenario.
IT Service Continuity Management

Service Continuity Management for IT Services can only really be effective if it is seen as being an integral part of an overall plan to ensure the continuity of the business in the event of any disaster.

There is little point in spending thousands of pounds ensuring continuity of the IT services, if the business or elements of the business itself are vulnerable to the risk.

Why is Service Continuity so important?

Business Dependency - Most organisations are now heavily or totally dependent upon their IT services and the underlying systems. Without these systems, organisations may not be able to carry on their business and their loss, even for a very short period, may have a serious effect and may even cause the business to fail.

Manual back-up inadequate - Most modern online systems have been designed to perform functions that are not capable of being performed manually. The speed of processing and the volume of data may mean that manual back-up systems are just not feasible.

Minimise impact on the business - A properly implemented and tested contingency plan will help limit the potential damage that would result if a major incident did occur. The aim of the plan is to minimise the impact on IT services, and therefore the business processes that rely on them.

Maintain continuity of essential business processes - One of the key activities leading to the production of a Contingency Plan is to determine the relative business priority of each IT service, the minimum requirements in the event of a major incident and the length of time before the full service must be restored. This means that recovery can be targeted to those services that are most crucial to the organisation.

To speed-up recovery - The process of developing a contingency plan involves agreeing, pre-defining and testing the actions and procedures to be followed if a major incident does occur. Upon real invocation, the plan can be actioned rapidly and effectively.

Sound financial reasons - A working contingency plan may be essential to avoid crippling financial losses should a disaster occur. Although some organisations may look upon Contingency Planning as a form of insurance policy, the availability of externally offered contingency services now make the provision of adequate contingency plans relatively affordable.

Your competitors will have a plan - Most organisations now have to compete hard to win business. It is important that businesses get up and running again following a disaster to avoid losing out to competitors.

Marketing investment - Organisations trying to attract new customers or retain existing customers may find that they can exploit the existence of a fully tested recovery plan in marketing their services.

Obligations - Many organisations may have legal, moral or even political obligations to discharge which are dependent upon their IT services being available. In such circumstances it may be essential that a contingency plan exists
Steps To Be Taken

There are number of steps which should be taken to arrive at a properly devised and tested Continuity Plan for IT services:

**Business Impact Analysis**

The scope of the Business Impact Analysis should cover the entire organisation. The main objectives of the analysis will be to:

- Identify those business processes, and their underlying IT services that are crucial to the continued survival of the company or organisation’s business processes.
- Assess how long the processes can survive without that particular service being provided.
- Define the services’ key deliverables; what are they, when and where are they produced?
- Identify the obligations that the organisation is under in respect of those services.
- Define the extent and nature of any manual or back-up processes that can be used in place of the IT services.

When all these questions have been fully answered, then it will be possible to prioritise the business activities and identify those most important to the survival of the business.

As total security from all eventualities is generally prohibitively expensive, the priority list generated from the business impact analysis will determine where the contingency planning budget can be spent to best effect. Note that this may be a complex assessment as the business priority of systems may vary from hour to hour, day to day, week to week and month to month.

**Risk Analysis & Management**

Risk Analysis can be regarded as two distinct areas: firstly analysing and assessing risks and secondly managing risks by adopting suitable countermeasures.

**Risk Analysis** involves the identification and valuation of assets, the identification and determination of the levels of threat to the assets (accidental and deliberate) and the identification and determination of the levels of vulnerabilities of the identified assets posed by the identified threats.

**Risk Management** involves the reduction of vulnerability of the assets through the adoption of cost effective countermeasures.

**IT Contingency Plan Options**

When planning the approach to contingency planning and disaster recovery, there are several options that can be considered. These are as follows:-

**Do Nothing** - This may be a common approach, but is usually adopted for all the wrong reasons - these reasons typically being "It will never happen to us" or "We just don't have time to do anything". Do Nothing may be a viable option, but only if the business impact and risk analysis reveals that there is no cost-justifiable action that can be taken.

**Clerical Back-up Procedures** - This option, in most cases, is not viable for the long term, but may form an essential element of an overall contingency plan to cover, for example, the initial period following a disaster.

**Reciprocal Arrangements** - This option is typically used when two organisations make use of compatible components and agree that each will provide the other, in an emergency, access to those components. This may be viable for components such as laser printers, but will not be viable as an option for large on-line transaction processing systems.

**The Fortress Approach** - This option is usually only adopted when financial, logistical or security reasons rule out other options. To implement this option, extremely high levels of resilience have to be built into the
computer system(s), extensive physical security has to be implemented and very sophisticated environmental controls have to be in place.

**Hot Start** - A hot start facility provides the environment and all the necessary hardware and ancillary equipment to support a computer installation, normally at a remote location. It may even include office facilities for staff. Restoring IT services using hot start facilities will involve the recovery of systems and application software from off-site back-ups.

The main types of hot start arrangement are:

- **Internal** - the facilities are provided from resources within the organisation
- **External** - the facilities are provided by an external supplier, which may be for a relatively short period
- **Mobile** - the facilities are portable and can be transported to a pre-arranged site

**Cold Start** - A cold start facility provides the accommodation and environmental requirements for a computer installation, but not the computer hardware itself.

The main types of cold start are:

- **Fixed** - the facilities are located in a fixed, predefined location
- **Portable** - the facilities are provided by the erection of a prefabricated or portable building

Either of these cold start arrangements could be provided internally, or by external suppliers.

**Dormant Contracts** - This option involves the lodging of a contract to supply existing hardware with a hardware supplier. Typically, the contract is reviewed each year to allow for addition of newly acquired hardware or the deletion of obsolete items, and will involve a small cost to the department in keeping the contract up to date with the hardware inventory.

**Insurance** - Organisations may already have extensive insurance policies. However, it is worth ensuring that the cost of replacing the buildings and equipment are fully covered. Insurance may also be an option for relatively low cost, easily accessible items such as PCs.

**Written Plan**

Regardless of the option chosen, a predefined, documented and protected plan is required. This will clarify roles and responsibilities, detail recovery instructions, and provide essential logistical and management information.

The plan should be tested regularly and it is essential that it is kept up to date. The plan should come within the scope of Change Management, and Service Continuity Management should be represented on the Change Advisory Board.
Availability Management

Terms

The following terms are used in Availability Management and are defined as follows:

Availability

This is the proportion of time that the service is actually available for use by the customer within the agreed service times. This is calculated as follows:

\[
\text{Availability} = \left( \frac{\text{actual time}}{\text{expected time}} \right) \times 100\%
\]

This sounds straightforward, but calculating availability may be a complicated business and may need to reflect individual customers’ own perception of service availability.

Reliability

This is the capability of a component to perform a required function under defined conditions for a certain period of time. This is usually expressed as:

- mean time between system incidents (MTBSI), or
- number of breaks in a period

Maintainability

Maintainability is a measure of the ability of components to be retained in, or restored to a normal working state. It is often specified as:

- MTTR - Mean Time To Repair (or Recover)

Maintainability is concerned with ensuring components have appropriate levels of preventive or corrective maintenance applied to them.

Serviceability

Where external suppliers are responsible for supporting or servicing components, maintaining availability, reliability and maintainability levels may become the contractual responsibility of the supplier. Serviceability is the term given to the activity of managing these aspects of external contracts.

Security

IT Security is a huge topic in its own right. This element of Availability Management is concerned with ensuring that measures are taken to improve the confidentiality, the integrity and the accessibility of services and information whilst preserving and improving overall availability.

Availability Relationships and Techniques

Availability management is one of the key functions underpinning Service Level Management, and provides many of the key metrics used in SLAs, OLAs and contracts with external suppliers.

There are many opportunities to improve levels of overall availability, and many of the ITIL disciplines can assist in this. For example, an efficient Service Desk which is adept at logging, diagnosing and resolving incidents can play a major part in optimising availability by reducing the time taken to react to incidents. It is also possible for many network management systems to detect incidents, automatically log them and take corrective action when appropriate.

There are many technical enhancements and measures which can be made to maintain and improve availability of IT components, and the services that they underpin. Some examples are:
- Redundant components, where if one CI fails, another one can take over
- Disc mirroring or RAID arrays that are resilient to component failure
- Fault tolerant technology
- Multiple routes through networks and data centre configurations
- Ensuring that maintainers of hardware, communications and environmental equipment maintain adequate spares holdings
IT Service Management Summary

An **IT service** is a set of related functions provided by IT systems in support of one or more business areas, which in turn may be made up of software, hardware, communications facilities, documentation, and people. These are perceived by the customer as a coherent and self contained entity.

An IT service provider is required to provide one or more IT services to customers and to manage effectively the underpinning activities, commonly referred to as **infrastructure management**. The totality of IT service provision and the management of the IT infrastructure is referred to as **IT service management**.

The IT Infrastructure Library embodies best practice for IT service management. The Library covers each element separately, but the greatest benefit is derived from viewing the processes and procedures as an inter-related set so that the maximum value is obtained.

Implementation of ITIL conformant processes and procedures for IT Service Management must be driven by business needs. Short-term (operational) goals aimed at providing stability and flexibility of service may be met through the implementation of the Service Support disciplines. Medium-term (tactical) goals aimed at providing the high quality, cost-effective services that support the business may be met through the implementation of Service Delivery.

The Future

Future developments will see a greater emphasis on IT Service Management as a way of bridging the often problematical gap between the business and the IT technology. The future will see further improvements in the scope and capabilities of supporting software tool sets, and a greater integration into other areas, as the ITIL is revised and updated.