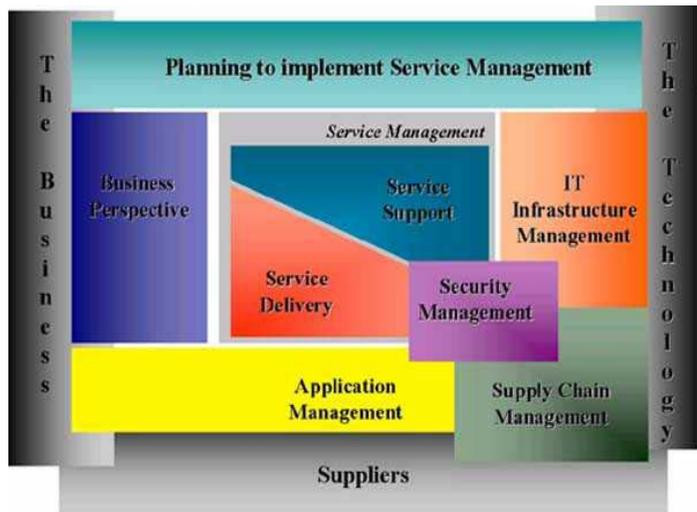


IT Service Management



A Companion to the IT Infrastructure Library

About the Guide

The pocket guide has been designed as a handy reference book for the information technology (IT) Service Management Practitioners and for those taking the foundation Certificate in IT Service Management .It is a complementary publication to complete IT Infrastructure Library (ITIL). This is discussed in more details in the section on IT service Management Best Practice.

The guide explains the processes involved in the two Key area of Service Management. And their application to the complete life cycle:

- **Service Support**
- **Service Delivery**

The advice contained within the guide is neither definitive nor prescriptive, but is a set of guidelines based on ITIL best practice. It is of benefit and is applicable to all IT organizations irrespective of size or the technology in use. The guidelines should be adapted and adopted to fit the each organization, individually based on the organization:

- Business
- Culture
- Structure
- Environment
- Processes

The IT Service Management Pocket guide begins with, and reinforces, the key message that IT service are there solely to support the business and its efficient and effective operation.

Table of Contents

About the Guide.....	2
1. The Philosophy of the Service Management	4
2. IT Service Management Best Practice	5
3. Implementing Service Management	7
4. Service Support Overviews	9
5. Service Desk.....	10
6. Incident Management	13
7. Problem Management	17
8. Configuration Management	21
9. Change Management	25
10. Release Management	31
11. Service Delivery Overview	35
12. Service Level Management.....	36
13. Financial Management for IT Services.....	40
14. Capacity Management.....	45
15. IT Service Continuity Management.....	50
16. Availability Management.....	54
17. The importance of Communication	58
18. Further Guidance and Contact Points.....	59

Table of Figures

Figure 1 - Guidance and Standards.....	5
Figure 2 - The ITIL Publication Framework.....	6
Figure 3 - Process Improvement Model	7
Figure 4 - The Service Support Process	9
Figure 5 - Incident Registration Input	11
Figure 6 - The Incident Life Cycle	14
Figure 7 - Logical Flow from Error to Resolution.....	15
Figure 8 - Errors in the Live and Development Life Cycle.....	18
Figure 9 - IT Incident Matching Process.....	19
Figure 10 - CMDB Interfaces to Service Support Processes.....	23
Figure 11 - Change Procedures - Part 1(normal)	27
Figure 12 - Change Procedures-Part 2(Normal)	28
Figure 13 - Change Procedures-Part 3(Urgent)	29
Figure 14 - Major Activities of Release Management.....	32
Figure 15 - DSL and CMDB role in Release Management	33
Figure 16 - The Service Delivery processes	35
Figure 17 - SLA, OLA and Contract Support Structure.....	38
Figure 18 - Costing, Changing and Budgeting Cycle	41
Figure 19 - Cost Model of Costs by Customer	43
Figure 20 - The Capacity Management Process.....	46
Figure 21 - Iterative Capacity Management Activities	47
Figure 22 - Capacity Management and the Business.....	48
Figure 23 - The Business Continuity Life Cycle.....	51
Figure 24 - The CRAMM Risk Assessment Model.....	53
Figure 25 - Relationships with Support Organisations	55
Figure 26 - The IT Availability Metrics Model	55
Figure 27 - The Availability Management Process.....	56

1. The Philosophy of the Service Management

The three Key objectives of Service Management are:

- To align it services with the current and future needs of the business and its customer.
- To improve the quality of the IT service delivered.
- To reduce the long-term cost of service provision.

It has been widely utilized for decades but more recently the internet has demonstrated that for many modern e-business based organizations:

“IT is the business”

And

“The business is IT”

It is essential therefore to recognize the absolute dependence of most businesses upon the information and communications Technology (ICT) infrastructure and the quantity, quality and the availability of the information that such an infrastructure provides and supports.

The challenges facing the IT Managers of today are to co-ordinate and work in partnership with the business to create new business opportunities. This has to be achieved while reducing the Total Cost of Ownership (TCO). The main method of realizing this goal is the reduction of the overall management and support costs, while developing new business models to maintain or improve the quality of service delivered to the business. In order to do the correct business and IT processes need to be developed and implemented .The management of It is all about the efficient and effective use of the three P’s people processes and products (tools and technology).

The ITIL philosophy adopts a process driven approach which is scalable to fit both large and small It organizations. It considers Service Management to consist of a number of closely related and highly integrated processes. To realize the key objectives of Service Management these processes must use the people and the product effectively and economically in the delivery of the high quality, innovative IT service aligned to business processes.

2. IT Service Management Best Practice

Best practice IT Service Management has evolved since 1989, Which saw the publication of the first elements of the IT Infrastructure Library (ITIL) by the UK Government’s Central Computer and Telecommunication Agency (CCTA).(now the Office of Government Commerce(OGC)).

Available best practice now comprises integrated guidance from OGC and the British Standards Institution (BSI). Its use is supported by a qualification and training structure that has been adopted world-wide to recognize professional. Competence in IT Service Management.

The written guidance ranges from detailed advice in each process within ITIL through the DISC-PD0005 Code of practice to the formal BS15000 standards. Specifying required practices for the organizations.

The following diagram illustrates the need for generic guidance, such as that from ITIL and BSL. This guidance should be supported by an organization’s own internal processes and procedures.

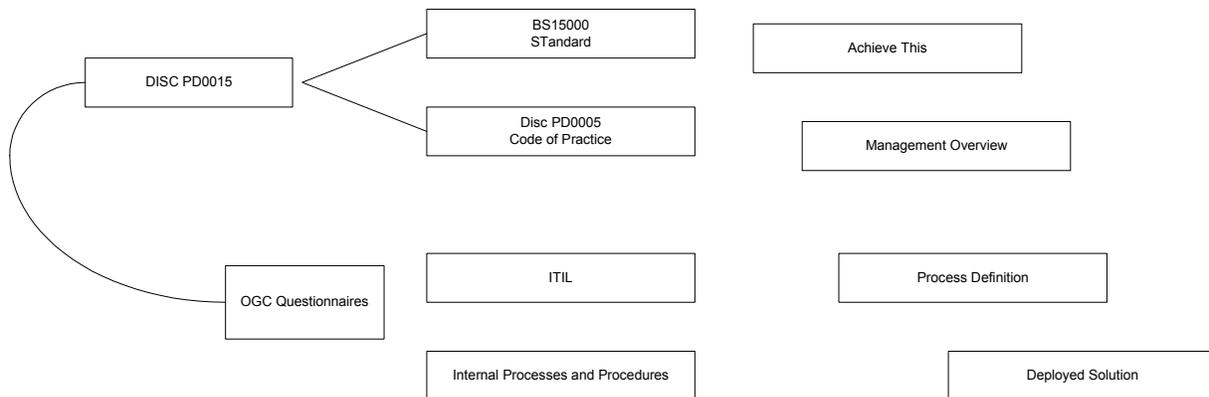


Figure 1 - Guidance and Standards

ITIL Service Management

Service Management Processes are at the heart of ITIL and are considered as two core areas:

Service Support	Service Delivery
Service Desk *	
Incident Management	Service Level Management
Problem Management	Financial Management for IT Services
Configuration Management	Capacity Management
Change Management	It Service Continuity Management
Release Management	Availability Management

* Note that Service Desk is a function not a process

Service Support generally concentrates on the day to day operation and support of the IT services while Service Delivery looks at the long term planning and improvement of IT service provision.

Key Definitions	
Customer	Recipients of a service; usually the Customer management has responsibility for the funding of the service.
Provider	The unit responsibility for the provision of IT services.
Supplier	A third party responsible for supplying or supporting underpinning elements of the It services.
User	The person using the service on a daily basis.

Publications

Within ITIL, a major re-write exercise has been undertaken in order to consolidate and bring the materials up to date, eliminate duplication and enhance navigation. The result is a series of publication within a defined framework.

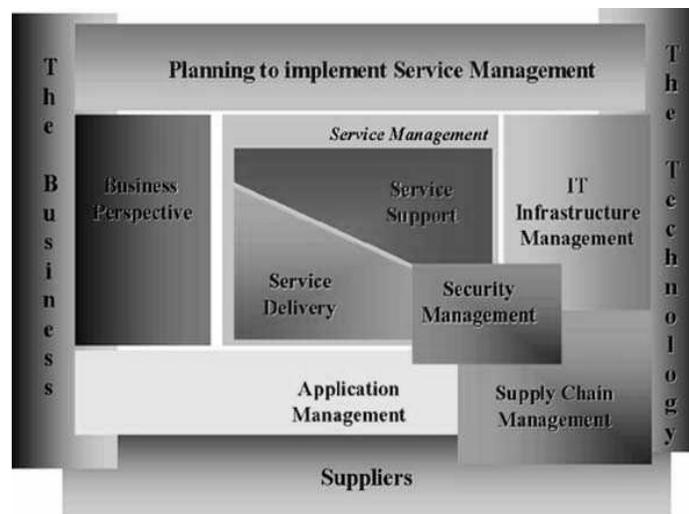


Figure 2 - The ITIL Publication Framework

Best practices guidance and detailed information on the processes themselves can be found in the appropriate sections of the Services Support and Services Delivery books. This pocket guide summarizes the main elements from these publications.

The complete range of ITIL and BSI publications are available from the IT Service Management (itSMF). See Section 18 for further information and contact points.

3. Implementing Service Management

Organizations should not be over ambitious when implementing Service Management. Most will already have elements established and in operation. Therefore, the Service Management implementation activity is actually one of process improvement.

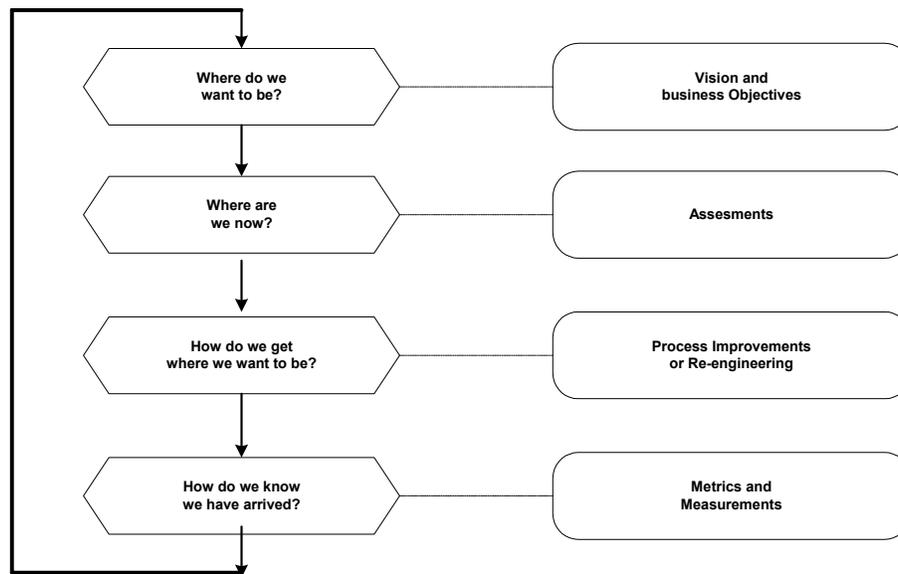


Figure 3 - Process Improvement Model

Tools to assist with assessment and planning are available including self-assessment products such as BSI's workbook: PD0015.

Service Management processes can be implemented consecutively or simultaneously and each process can be broken down into series of activities.

Overall Process improvement is an iterative activity and would normally consist of the following stages:

Process Improvement Definition

- Reviewing where we are now
- Defining the mission statement
- Setting goals and objectives
- Defining roles and responsibilities

Communication

- Raising the awareness
- Publishing and circulating information
- Seminars, briefings and workshops.

Planning

- Producing Statement of requirements
- Designing the process improvements
- Producing the plan
- Identifying resources and defining the training

Implementation

- Developing and improving the processes
- Implementing the plan with reviews and reports
- Developing and customizing the tools
- Training IT staff, Customer, and Users
- Producing documentation, procedure and deliverables
- Testing
- Measurement and reporting of metrics

Review and Audit

- Review and comparison of actual achievements with goals and objectives
- Post implementation project review
- Identifying and publishing the benefits
- Reviewing for effectiveness and efficiency
- Auditing for compliance
- Monitoring, reviewing and developing future improvements.

4. Service Support Overviews

The following diagram illustrates the major interfaces and deliverables within the service Support processes:

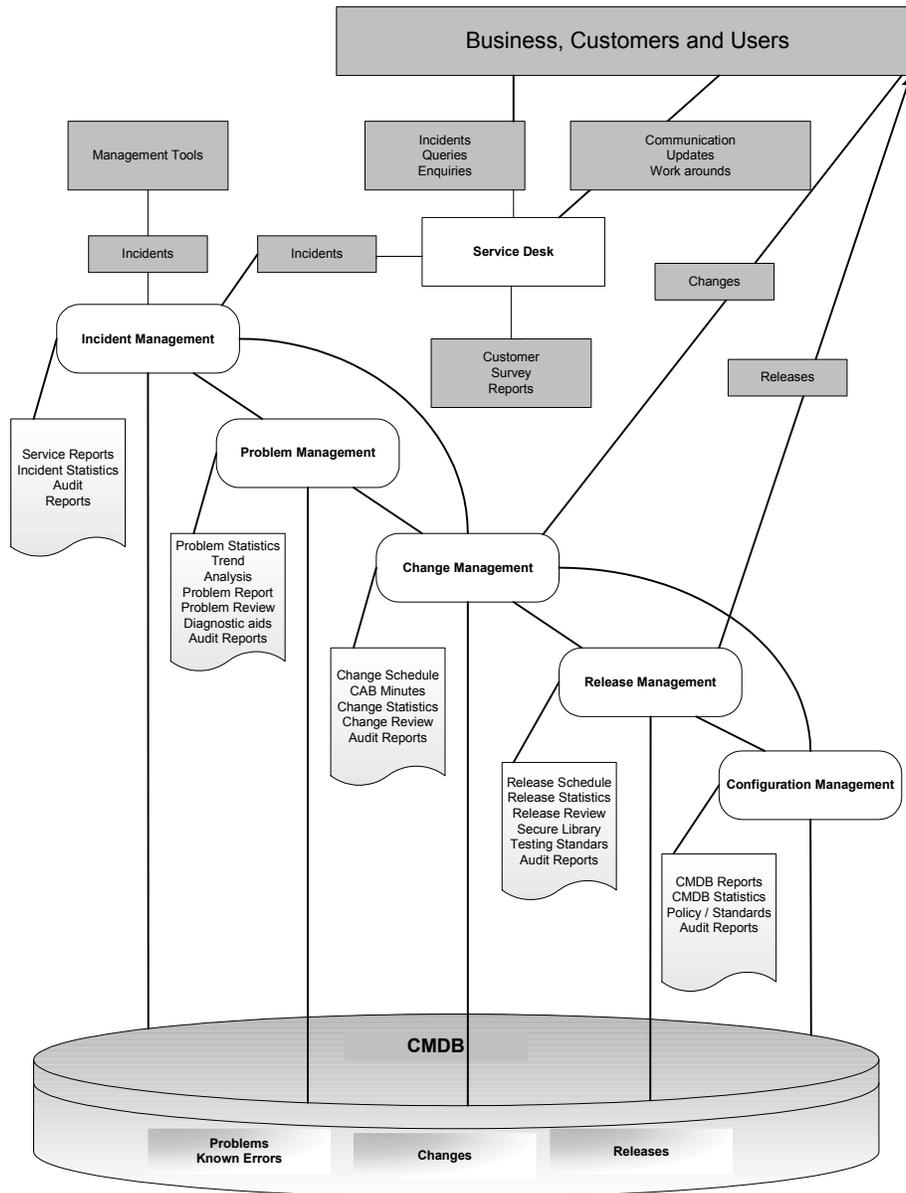


Figure 4 - The Service Support Process

5. Service Desk

Goal

To act as the central point of contact between the User and IT Service Management. To handle incidents and requests, and provide an interface for others activities such as Change, Problem, Configuration, Release, Service Level and IT Service Continuity Management.

Why a Service Desk?

The Service Desk, unlike other disciplines (Processes) described in this book, is a function essential to effective Service Management. More than just a Helpdesk, It is the principal operational interface between IT and their Users. A good first impression by each of its users is predicated upon its performance and attitude. Often a stressful place to work, underestimating its importance, high profile and the skill required to perform the duties we can severely hinder an organization's ability to deliver quality IT services.

The principal reasons for an organization to invest in a Service Desk are:

- To provide a single point of contact for users
- To deliver the high quality support critical for achieving business goals
- To Help identify and lower the cost of ownership for IT services as whole
- To support changes across business, technology and process boundaries
- To aid user retention and satisfaction
- To assist identification of business opportunities

Responsibility

Most of the activities carried out by the Service Desk, fall under the responsibilities of one of the IT Service Management processes. The role and responsibility of the service desk will depend upon the arrangements that the organization has put in place. Among the tasks commonly assigned to the Service Desk are:

- Receive and record all calls from users: deal directly with simple requests and complaints.
- Provide initial assessment of all incidents: make first attempt at incident resolution and /or refer to 2nd line support, based on agreed service levels.
- Monitor and escalate all incidents according to agreed service levels.
- Keeps users informed on status and progress.
- Produce management reports.

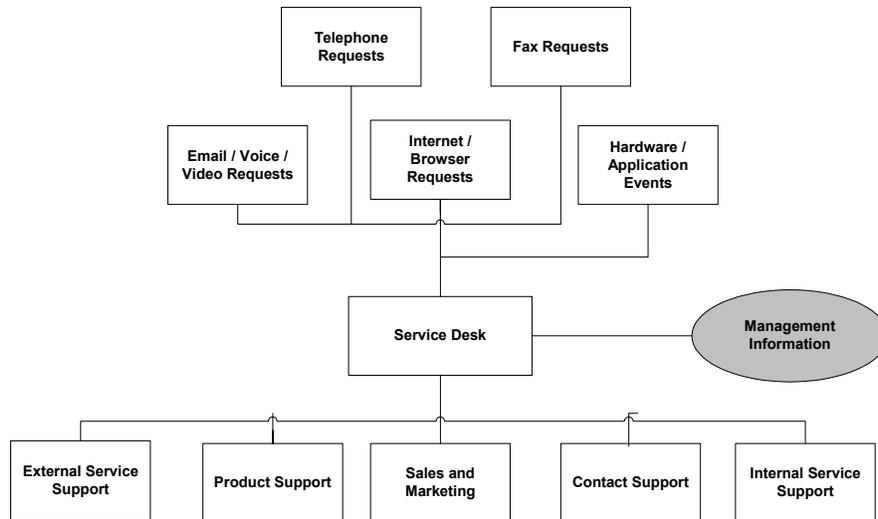


Figure 5 - Incident Registration Input

Key Considerations

User Interaction

Expanding reporting and communication methods beyond telephone contact, Such as Internet and Intranet, Email and Fax can enhance service. The Service Desk still provides the main communication between the user and IT service and:

- Represents the service provider to the user
- Considers user satisfaction and perception as critical
- Depends on the right mix of people, processes and technology to delivery a business service

Setting up a Service Desk

A correct Service Desk Infrastructure is critical to success and requires clear ownership; define business goals, responsibilities, deliverables and management commitment. The following actions need to be carried out when setting up a Service Desk:

- Ensure the business need is identified and understood
- Obtain management support, budget and resources
- Ensure the solution aligns with the service strategy
- Identify, achieve and communicate quick wins
- Define clear objectives and deliverables
- Start simply and phase the implementation
- Involve and educate users
- Advertise and 'sell' the benefits to all parties
- Train IT staff to be Service staff.

Service Desk Technologies

A number of technologies are available to assist the Service Desk. However, remember that technology should be used to complement and enhance the service, not replace it. The technology must support correct business processes, adapting to both current and future demands. It is also important to understand that automation requires an increased need for discipline and accountability.

Types of Service Desk

Three types of Service Desk structure should be considered in the establishing the optimum set up:

- Local Service Desk
- Central Service Desk
- Virtual Service Desk

Benefits

- Improved User service, perception and satisfaction
- Increase User accessibility via the single point of contact
- Improved teamwork and communication
- Better managed infrastructure and control
- More effective and efficient use of the support resources
- Better management information for better decision support

Possible Problems

- User service not considered a priority
- Lack of management commitment
- Resistance to change working practices
- Incorrect or insufficient resources and skill levels
- Insufficient or inadequate marketing of Service Desk.
- Over reliance on technology
- Insufficient funding and budget allocation.

6. Incident Management

Goal

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

Why Incident Management?

- To ensure the best use of resources to support the business
- To develop and maintain meaningful records relating to incidents.
- To devise and apply a consistent approach to all Incidents reported.

Incident Management

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

Examples of Incidents are:

- Application unavailable or in error.
- Hardware outage or constrained use.
- Service Request for information or assistance (e.g. a service extension).

Responsibilities

- Incident detection and recording
- Classification of all incidents and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking and communication.

Role of the Service Desk in Incident Management

The Service Desk will usually play the key role in the Incident Management process, recording and monitoring the progress of Incidents and retaining ownership of them.

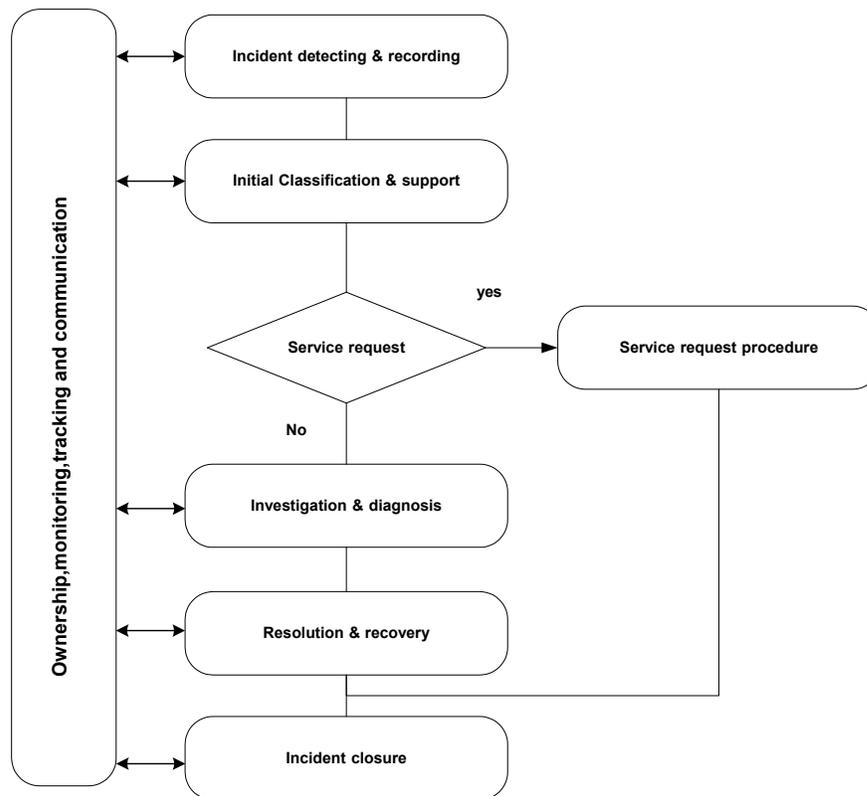


Figure 6 - The Incident Life Cycle

Key Considerations

Critical Success Factors for Incident Management

- An up-to-date Configuration Management (CMDB).
- A knowledge base recording problems and known Error data, resolutions and workarounds.
- Availability of effective automated support tools
- Close links with effective Service Level Management.

Prioritization

Urgency is an assessment of the speed with which an incident needs resolution.

Impact reflects the likely effect the Incident will have upon the business service.

The **Priority** for allocating resources to resolution of an Incident is based upon a combination of impact and urgency, together with other relevant factors such as availability of resources.

Relationship between Incident, Problems and Known Errors

Where the cause of an incident is not identifiable then. If investigation is warranted a problem record is raised. A Problem represents an unknown error in one or more Configuration Items. Once the underlying cause and a workaround or correction via a Request for Change (RFC) is identified it then becomes a known Error record. Details of relationships between Incidents, Problems, Known Errors and RFCs are held within a CMDB.

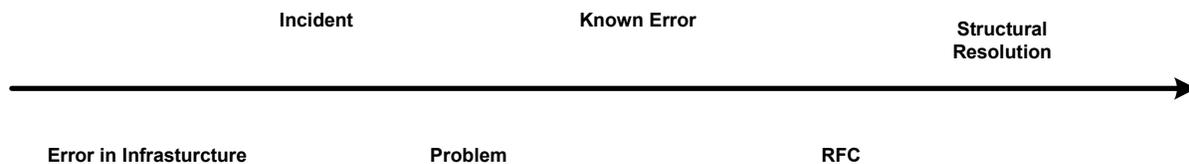


Figure 7 - Logical Flow from Error to Resolution

Newly recorded Incidents will be matched against the database of existing Incidents, Problems, and Known Errors. Available workarounds will be applied to enable speedy resolution of Incidents. This knowledge based needs to be maintained so that only relevant records are presented to the Service Desk.

Handling of Major Incidents

Major Incidents occur when there is an extreme impact on the User community. Where the disruption is excessive. Problem Management must be notified and should arrange a formal meeting of people who might help. The Service desk should ensure that a record of actions and decisions is maintained in the Incident Records.

Benefits

- Reduced business impact of incident by timely resolution
- Proactive identification of beneficial enhancements
- Availability of business focused information related to Service Level Agreement (SLA)
- Improved monitoring of performance against SLAs.
- Better staff utilization leading to greater efficiency.
- Elimination of lost Incidents and Service Requests.
- More accurate CMDB information enabling an ongoing audit while registering Incidents
- Improved User satisfaction
- Less disruption to both IT support staff and Users.

Possible Problems

- Lack of management commitment
- Lack of agreed Customer service level
- Lack of knowledge or resources for resolving Incidents
- Poorly integrated or missing related processes or functions
- Lack ,unsuitability or high cost of software tools
- Users and IT staff bypassing the process

7. Problem Management

Goal

To minimize the adverse effect on the business of Incident and Problems caused by errors in the infrastructure and to proactively prevent the occurrence of Incidents Problems and errors.

Why Problem Management?

To resolved Problems quickly and effectively

To ensure resources are prioritized to resolved Problems in the most appropriate order based on business need

To proactively identify and resolved Problems and Errors thus minimizing Incident occurrences

To improve the productivity of support staff

To provide relevant management information.

Problems and Known Errors

A problem is the unknown underlying cause of one or more Incidents. It will become a Known Error When root cause is known and a temporary workaround or a permanent alternative has been identified.

Responsibilities

- Problem control
- Problem identification and recording
- Problem classification
- Problem investigation and diagnosis.
- Error Control
- Error identification and recording
- Error assessment
- Recording error resolution
- Error closure
- Monitoring resolution progress
- Assistance with the handling of major Incidents
- Proactive prevention of Problems
- Tend analysis
- Targeting support action
- Providing information to the organization
- Obtaining management information from Problem data
- Completing major Problem reviews

Problem Control Vs. Error Control

Problem control focuses on transforming Problems into Known Errors. Error Control focuses on resolving Known Errors Via the Change Management Process.

Key Considerations

Errors from the Development Environment

Errors in software released into the live environment should be incorporated into the Known Error database for live services.

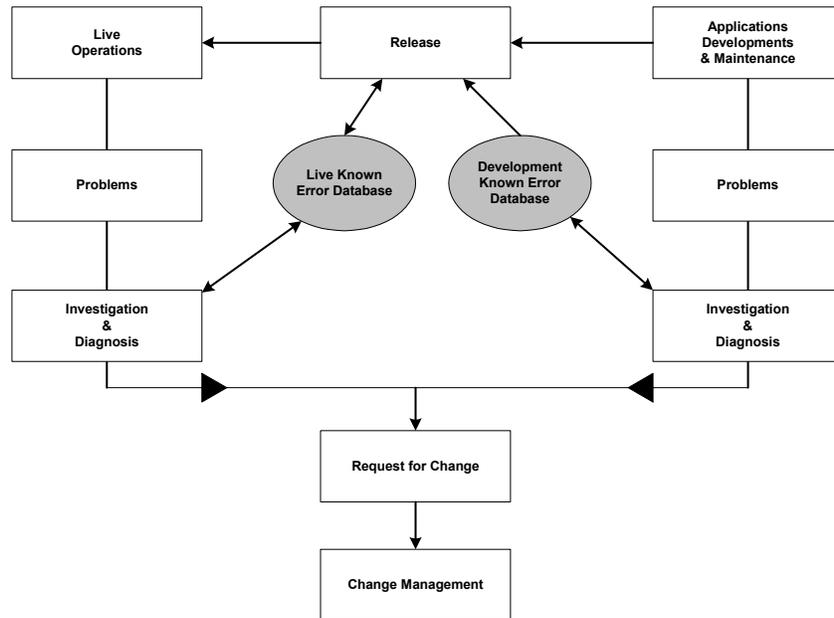


Figure 8 - Errors in the Live and Development Life Cycle

Incident and Problem Management difference

The Incident and Problem Management processes have different imperatives. Incident Management is concerned with restoring the service to the business User as quickly as possible. Problem Management is concerned with establishing the underlying causes of an Incident and their subsequent resolution and prevention. These goals can sometimes resulting conflicting properties.

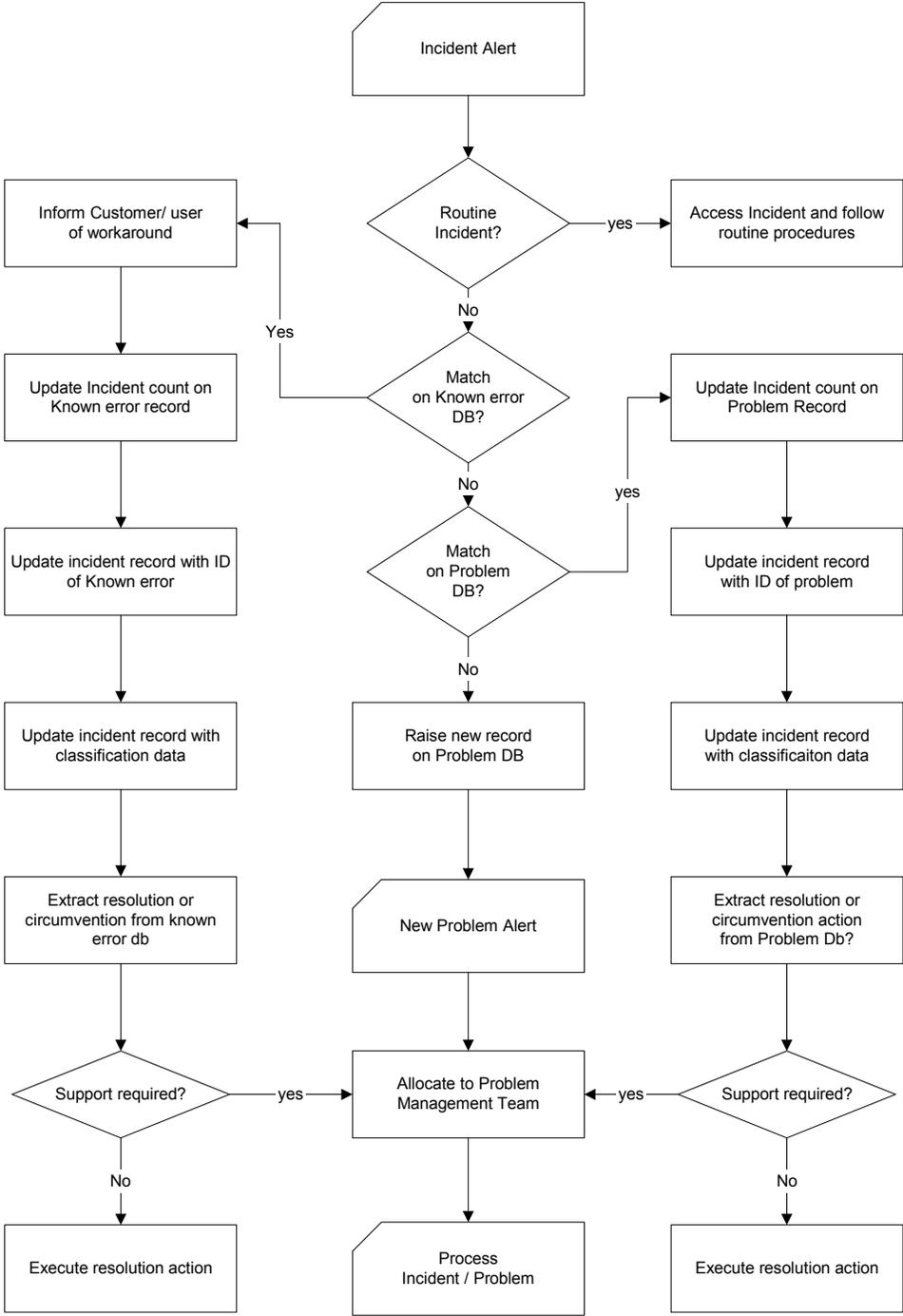


Figure 9 - IT Incident Matching Process

Timing and Planning

Good Problem Management relies on an efficient Incident Management process. So implement in parallel or immediately after Incident Management

If resources are scarce concentrate on Problem and Error Control (reactive) and leave proactive Problem Management until later after service monitoring activities are in place and base data is captured

Focus on a few Key Problems that are causing the greatest pain to the business- experience show that 20% of Problems cause 80% of service degradation.

Benefits

- Improved IT services
- Incident volume reduction
- Permanent organizational Learning
- Improved Service Desk first time fix rate

Possible Problems

Absence of good Incident control process

Lack of management commitment

Undermining of the Service Desk role

Insufficient time and resources to build and maintain the knowledge base

Inability to accurately assess business impact of Incidents and Problems.

8. Configuration Management

Goal

To provide a logical model of the IT infrastructure by identifying controlling, maintaining and verifying the versions of all Configuration Items in existence.

Why Configuration Management?

To account for all assets

To provide accurate information to support other Service Management process

To provide a sound basis for Incident , Problem, Change and Release Management

To verify records against Infrastructure and to correct exceptions.

Responsibilities

These are five basis activities of Configuration Management.

Planning

The Configuration Management plan should cover the next three to six months in detail and the following twelve month in outline. It should be received at least twice a year and will include:

Strategy, policy, scope, objectives, roles and responsibilities

Configuration Management processes, activities and procedures

CMDB, relationships with processes and third parties

Tools and other resource requirements.

Identification

The selection , identification and labeling of all Configuration Items (CIs).It covers recording information about CIs including ownership, relationships, versions and identifiers. CIs should be recorded at level of details justified by the business need –typically to the level of “independent changes”.

Control

Assurance that only authorized and identifiable CIs are accepted and recorded from receipt to disposal. It ensures that no CI is added, modified, replaced or removed without appropriate controlling documentation .e.g. approved RFC updated specification. All CIs will be under Change Management Control.

Status Accounting

The reporting of all current and historical data concerned with each CI throughout its life-cycle. It enables changes to CIs and tracking of their records through various statuses e.g. ordered, received, under test, live, under repair, withdrawn or for disposal.

Verification and Audit

A series of reviews and audits that verifies the physical existence of CIs and checks that they are correctly recorded in the CMDB. It includes the process of verifying Release and Configuration documentation before changes are made to the live environment.

Level of Control

- Identifying critical service and their components is a sensible starting point for Configuration Management
- Although low-level detail may be required in part of the structure, it may not be needed throughout.
- Reviewing data levels and Configuration (CMDB) clean-up exercise can help.
- Target maximum control with minimum records.

Key Considerations

Configuration Management Database

All details and relationship information about CIs should be held in a single place, the configuration Management Database (CMDB). This single depository of information will be accessed across the Service Management processes and it a major driver of consistency between the processes.

Relationships to other Processes

Configuration Management is closely linked with the overall Service Support and Service Delivery processes, both supporting and depending upon those processes. If those other processes are not already in existence they should be planned alongside Configuration Management.

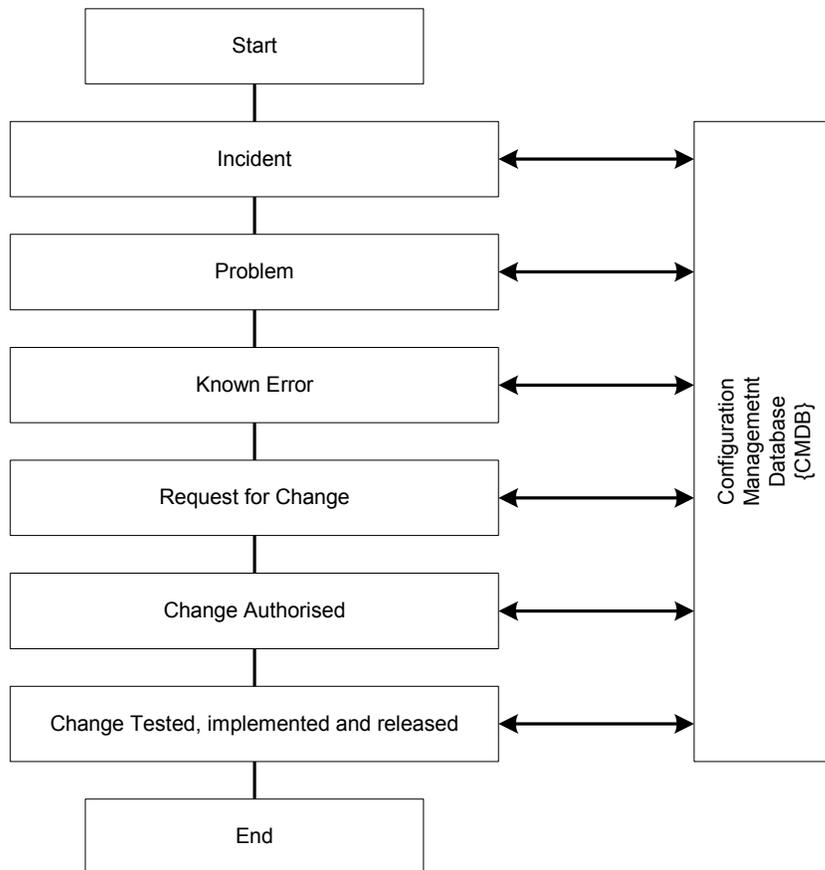


Figure 10 - CMDB Interfaces to Service Support Processes

Configuration Baseline

A baseline in the configuration a product or system established at a specific point in time and capturing both structure and details. It can be created as a:

- Sound basis for future work
- Record of CIs affected and actually changed by an RFC
- A point to fall back to if (or when) things go wrong.

Definitive Software library (DSL)

The Definitive Software Library is where the authorized versions of all Software CDs are stored and protected. It will comprise a single logical (but probably physically multiple) file store for developed software and a secure physical store holding bought-in software. (Refer also Release Management).

Relationship to Asset Management

Configuration Management is not synonymous with Asset Management, which maintains details on assets, usually above a set value; configuration Management maintains not only relevant information on the assets themselves but also information about relationships between assets.

Setting up Configuration Management

The planning process for setting up an appropriate function could take up to 6 months from inception to first phase of implementation. Actual implementation may take much longer, but the benefits of Configuration Management should outweigh the costs.

Benefits

- Provides accurate information on CIs and their documentation to support all other IT Service Management processes.
- Facilitates adherence to legal and contractual obligations.
- Helps with financial planning through clear identification of all assets and associations between them.
- Makes support changes visible and supports and improves Release Management.
- Improve security by controlling the versions of CIs in use and enables the organization to reduce the use of unauthorized software.
- Facilitates impact and trend analysis for Changes and Problems.

Possible Problems

- CIs defined at too high or too low a level
- Implementation without sufficient analysis and design of the process, database and procedure or without sufficient project planning
- Schedules or expectations that are over ambitious
- Lack of management commitment
- Support tools lacks the required flexibility
- Process is circumvented, perceived as bureaucratic and /or is error prone
- Implemented in isolation, without necessary support from Change and Release processes
- Scope too wide or too narrow
- Not linked into application or project life-cycle.

9. Change Management

Goal

To ensure that standardized methods and procedure are used for efficient and prompts handling of all changes. In order to minimize the impact of any related Incidents upon service.

Why Change Management?

Changes within the IT infrastructure may arise reactively in response to Problems or externally imposed requirements .e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiative or from programs, projects or service improvement initiatives. Change Management can:

Ensure Standardized methods processes and procedure are used for all Changes

Facilitates efficient and prompt handling of all changes.

Maintain the proper balance between the need fro change and potential detrimental impact of changes.

Responsibilities

Change Management is responsible for controlling Change to all CIs within the live environment. It is not responsible for change within ongoing projects. Which are controlled by the project change process. However close liaison between development project managers and the change Manager is expected. Change Management would typically comprise:

- Raising and recording Changes
- Assessing the impact, cost , benefits and risk of proposed Changes
- Developing business justification and obtaining approval
- Managing and coordinating Change implementation
- Monitoring and reporting on the implementation
- Reviewing and closing Request for Change (RFCs).

Key Considerations

Change Advisory Board

The Change Advisory Board (CAB) considers RFCs and in the light of the business need makes recommendations as to whether they should be accepted and implemented or rejected, Recommendations are based upon the impact on existing services, the cost of the changes can be adequately assessed from both the business and technical viewpoint. The CAB members are likely to include (dependent upon the agenda):

- Change Manager, Chairing the process
- Relevant It services staff
- Suppliers, maintainers and developers
- Customers and Users
- Office services and other non-IT supporting services

- Experts/technical consultants

Face to face meetings are not always used: some ACB work takes place using electronic communications. However occasional regular meetings e.g. twice yearly can help to maintain the good working relationships upon which effective Change assessment depends.

When urgent major problems arise there may not be time to convene the full CAB. For these cases a CAB/ EC (Emergency Committee) should be identified with authority to make emergency decisions. Membership of CAB / EC may vary depending upon the different criteria related to participation problems.

Change Procedures

The following flowcharts illustrate the normal and urgent Change processes, where the business impact justified it a Change should proceed via the urgent path indicated in the flowcharts. This allows for "fast tracking" of the process with respect to approval channels, testing, and documentation. Urgent Change procedures must not be viewed as an optional route to faster implementation since they carry considerably greater risks than normal Change procedures. The urgent procedure is typically used for emergency Problem resolution.

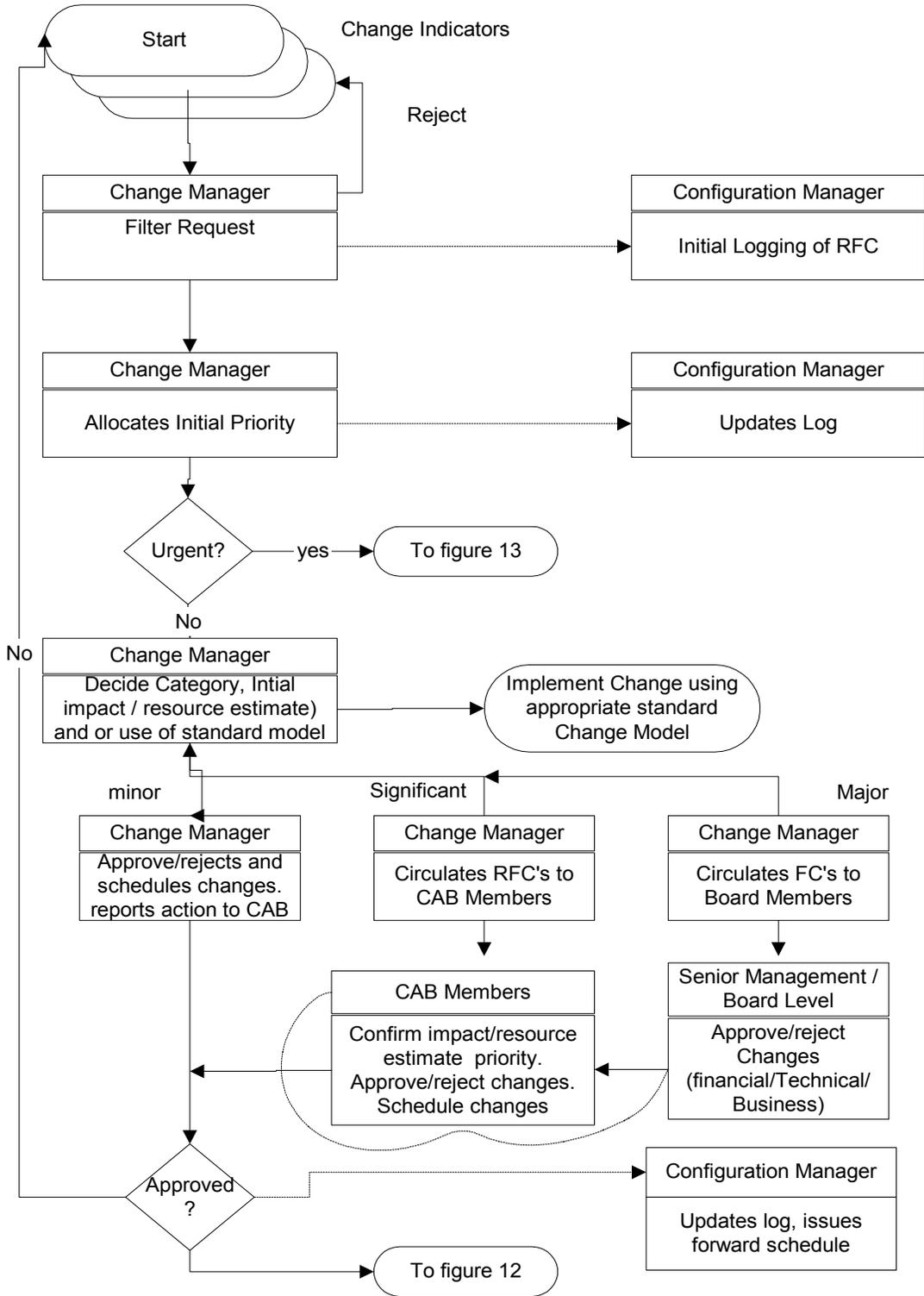


Figure 11 - Change Procedures - Part 1(normal)

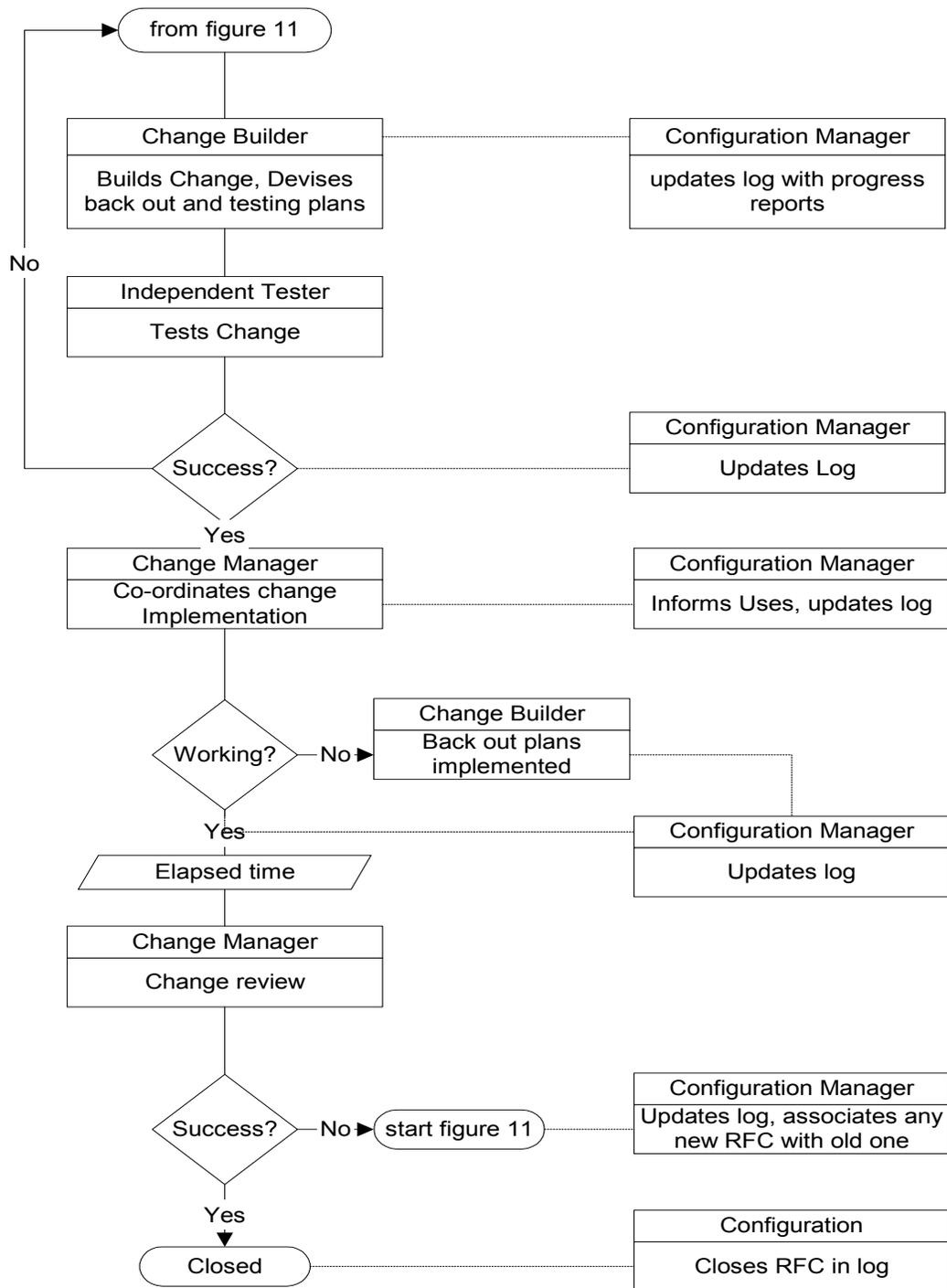


Figure 12 - Change Procedures-Part 2(Normal)

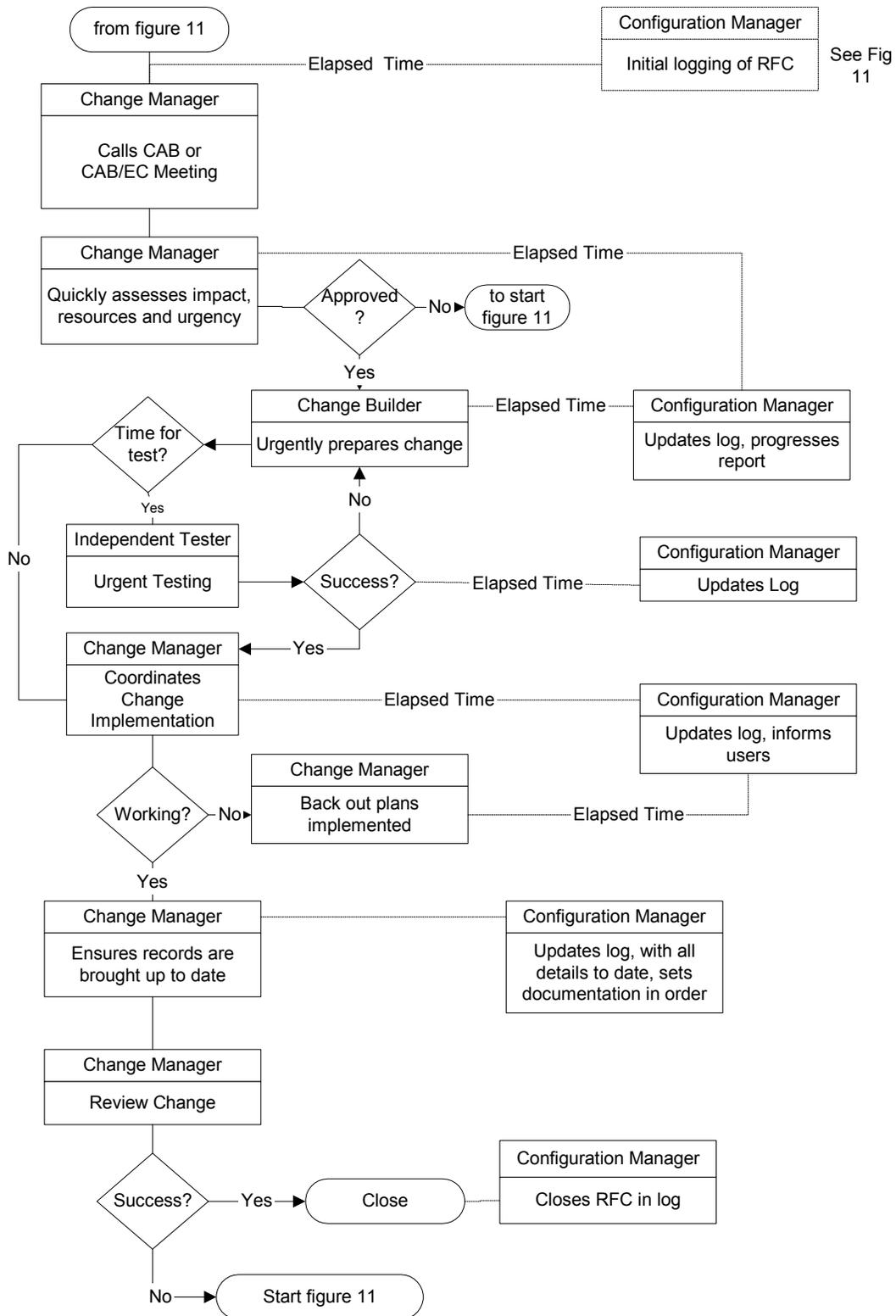


Figure 13 - Change Procedures-Part 3(Urgent)

Standard Changes

A standard change is an accepted solution to an identified and relatively common set of requirements, where authority is effectively given in advance of implementation .e.g. setting up access profiles for a new employee.

Change Models

Modern tools permit the use of sophisticated Change models that can and should be used to ensure the consistence implementation of common types of changes both major and minor .e.g. upgrade of a standard desktop software product.

Integration with Project Management

Change Management should be integrated with the management of large organizational Programs or projects, through planning, building, testing and implementation.

Benefits

- Better alignment of IT services to actual business need.
- Increased visibility and communication of changes to both business and service support staff
- Reduced adverse impact of change on the IT service from improved business and technical impact and risk assessment.
- Better assessment of cost of proposed Changes before they are incurred
- Improved Problem, Supplier and Availability Management through the use of valuable management information relating to changes.
- Improved productivity of Users through less disruption and higher quality services.
- Improved productivity of key IT personnel, due to less distraction to repair faulty Changes.
- Greater ability to absorb a large volume of Changes.

Possible Problems

- Scope incorrectly set .e.g. over-stretching staff, Changes not aligned to project life cycle or inability to address all aspect of change.
- Lack of ownership and knowledge of impacted systems making impact assessment impossible.
- Staff resistance to a process perceived as too bureaucratic.
- Lack of visible management commitment and support to enforce.
- Lack of control over urgent Changes.
- Lack of an accurate CMDB.

10. Release Management

Goal

To take a holistic view of a Change and an IT Service and ensure that all aspects of a Release, both technical and non-technical are considered together.

Why Release Management?

Release Management should be used for:

- Large or critical hardware roll-outs
- Major software roll-outs
- Bundling or batching related sets of changes

Release management co-ordinates the many service providers and suppliers involved with a significant Release of hardware, software and associated documentation across a distributed environment.

Responsibilities:

- Planning and overseeing the successful roll out of new and change software and associated hardware documentation
- Liaison with Change Management to agree the exact content and roll out plan for the Release
- Ensuring that all items being rolled out or changed are secure and traceable via the CMDB
- Managing customers and users expectations of Releases and roll outs.

Release Policy

A release policy document should be produced to clarify the roles and responsibilities for release management. There may be one document per organisation, or an umbrella set of guidelines and specific details for each supported system or IT Service.

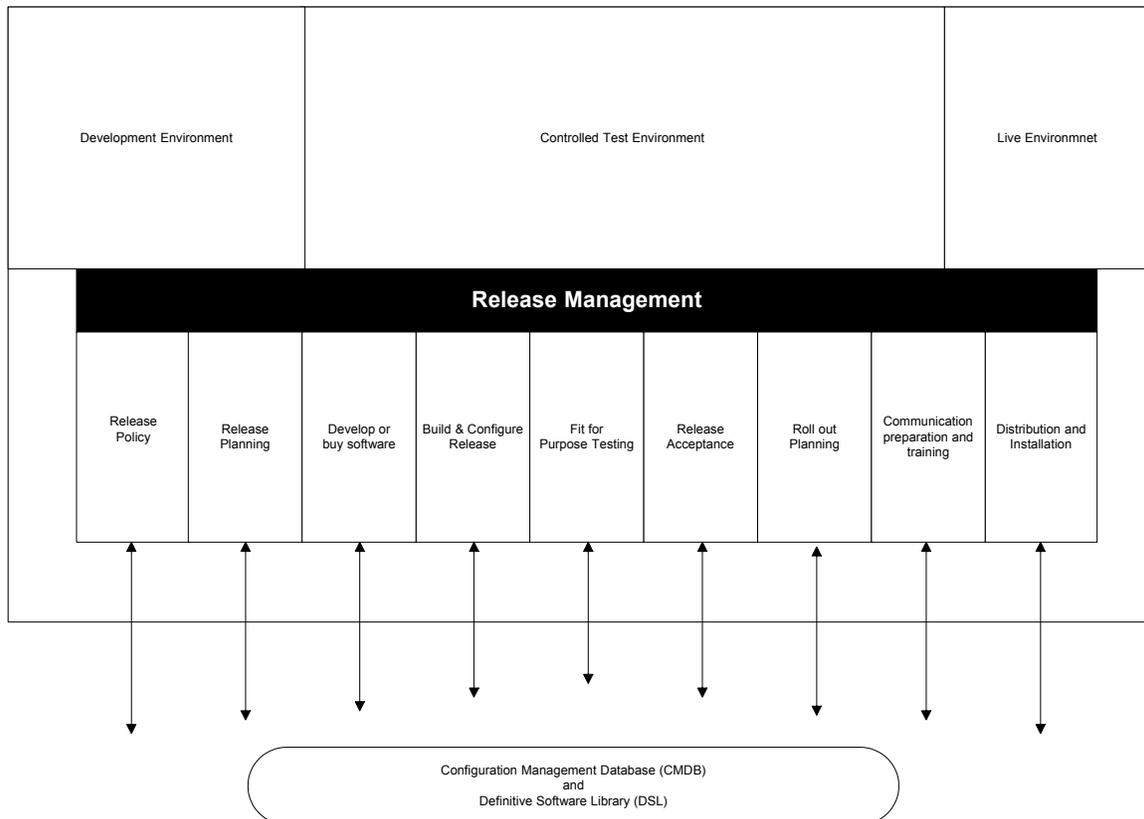


Figure 14 - Major Activities of Release Management

Key Considerations

Types of Release

Full Release: All components of the release are built, tested, distributed and implemented together.

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

Package Release: Individual releases, both full and delta, are grouped together to form a package of release.

Definitive Software Library (DSL)

The DSL contains the master copies of all controlled software in an organisation including purchased software as well as software developed on the exact configuration of the DSL that is required for release management should be defined before development commences.

The following should be considered

- Media
- Naming Conventions
- Environments Supported
- Security Arrangements
- Scope
- Retention period
- Audit Procedures

The CMDB should be updated and referred to throughout the Release Management process, concurrently with updates to the DSL

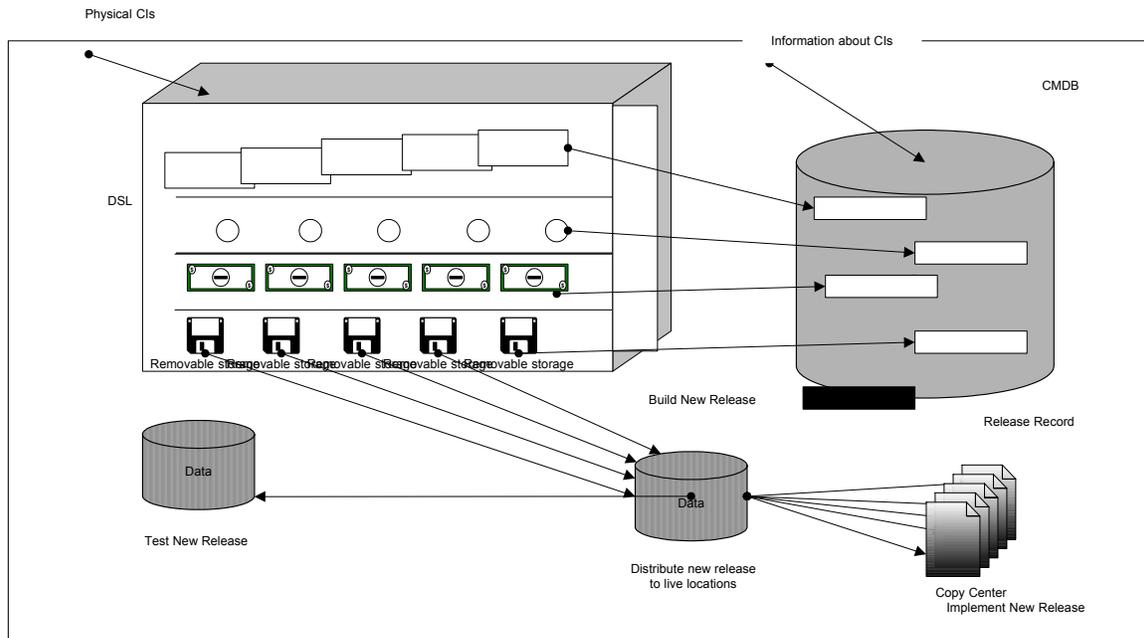


Figure 15 - DSL and CMDB role in Release Management

Definitive Hardware Store (DHS)

An area should be set aside for the secure storage of definitive hardware spares, Spares should be maintained at the same level as the live location, and their details recorded in the CMDB.

Build Management

The software and the hardware components that comprise a new release should be assembled in a controlled manner to ensure a reproducible process. It is quite common to automate the build process to reduce the reliance on human intervention and so make it more reliable. Build management becomes the responsibility of Release Management from the controlled test environment onwards.

Testing and Back-out Plans

Releases should undergo stringent testing and user acceptance before release. Back-out plans to document the consequent action should a release fail, wholly or partly must exist. The back-out plans should be tested as a part of the overall release testing process.

Change, Configuration and Release Management

A central function for Change, Configuration and Release Management offers considerable advantages. Without Change Management, Configuration information will rapidly become inaccurate, without accurate configuration data, Change Impacts are not accurately assessable, and without configuration and change management, releases will not be controllable. Recommended approach is to have a single change and configuration management and release plan that address.

Combined roles and responsibilities

Nature of the CMDB, DSL and DHS together with associated tool and library requirements
Change, Configuration and Release Management procedures as they relate to each other

Definitions

Release: a collection of authorized changes to an IT Service.

Release unite: the portion of the IT infrastructure that is normally released together

Roll out: deliver, install and commission an integrated set of new or changed CIs across logical or physical parts of an organisation

Benefits

When combined with configuration Management, Change management and operational testing, release management can deliver...

- Improved service quality as a result of freater success rate for releases and minimization of disruption to the business.
- Assurance that hardware and software in live use is of known quality reducing the chance of illegal, wrong or unauthorized software being used.
- Better use of resources, either user, testing,, or development
- Greater ability of the organisation to cope with high levels of change
- Better expectation setting for business and service support staff.

Possible Problems

- Resistance from staff to new procedures
- Circumvention or inappropriate use of 'urgent' procedures
- Unclear ownership and role acceptance between operational and development staff
- Inadequate building and testing of Releases, due to insufficient hardware resources
- Inability to recreate all possible environments
- Lack of understanding of the full contents of a Release or pressure to roll our before a release is fully prepared
- Reluctance to back out a failing release

11. Service Delivery Overview

The following diagram illustrates the major interfaces and deliverables within the service delivery processes:

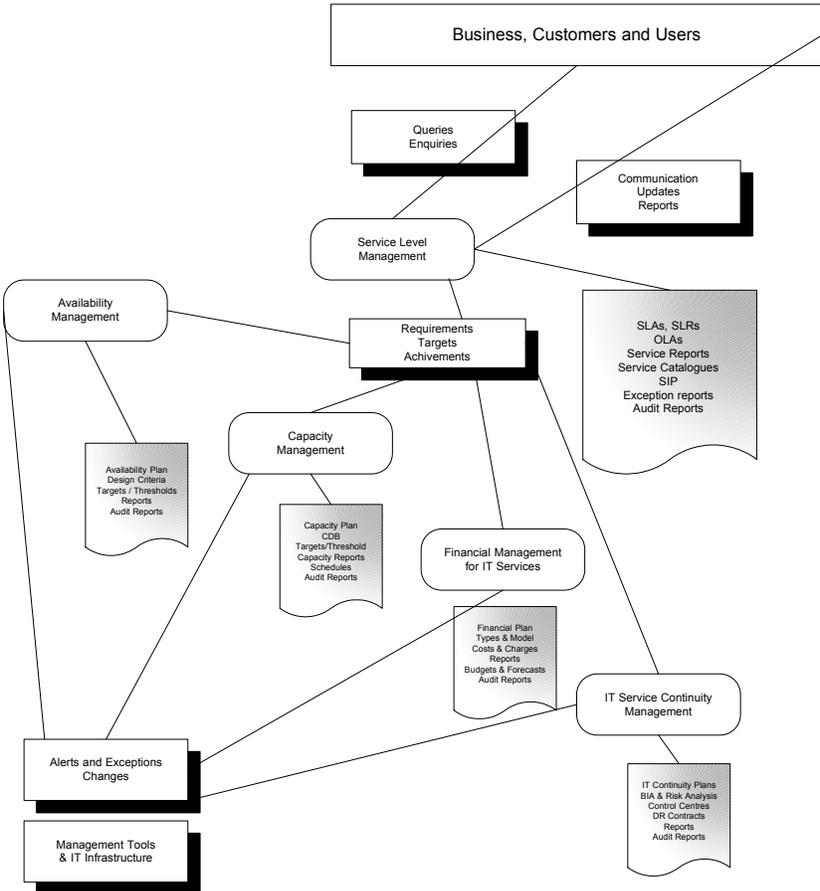


Figure 16 - The Service Delivery processes

12. Service Level Management

Goal

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.

Why Service Level Management

Service Level Management (SLM) ensures that the service targets are documented and agreed in Service Level Agreements (SLAs) and monitors and reviews the actual service levels achieved against their SLA targets. SLM should also be trying to proactively improve all service levels within the imposed cost constraints.

Service Level Management is the process that manages and improves agreed levels of service between two parties

The provider, who may be an internal service department (eg. Engineering, computer department, building services) or an external outsourcing company or third party supplier.

The receiver of the service (ie) the customer who pays the bills

Responsibilities

Negotiating and agreeing service requirements and expected service characteristics with the customer.

- Measuring and reporting of
 - Service level actually being achieved against target
 - Resources required
 - Cost of service provision
- Continuously improving service levels in line with business processes, with a service improvement programme (SIP)
- Co-coordinating other service management and support functions including third party suppliers.
- Reviewing SLA to meet changed business needs or resolving major service issues
- Producing reviewing and maintaining the service catalogue

Service Catalogue

Service Level Management will document the services provided to the customers, detailing the key features of those services, preferably within the CMDB. This catalogue will form the basis for an understanding of all the services offered, their components, features, charges etc.

There may well be the need for a version of the service catalogue aimed at customers, as well as one holding more supplier related information.

Key Considerations

Customer Focus

The service level management process encourages both provider and customer to realize that they have joint responsibility for the service typically this generates...

An understanding of the customer's business process and drivers

An acceptance of the benefits of early discussions of expected changes to workload volumes or the nature of the service

Constructive discussion on better ways of meeting the customer's needs and of transforming business processes.

The SLM Process

The SLM process creates a management framework that disciplines both the provider and the customer. SLM encourages the customer to consider, document and define their real business needs. SLM generally makes the provider more focused and accountable. By including the cost of the IT Services in the measurements, the SLM processes can also help improve the cost effectiveness of the services.

Content of Service Level Agreements

- As a minimum, a service level agreement should include..
- A simple description of the service and the deliverables
- The agreed service hours
- User response times, Incident response times and resolution times and response times to changes.
- Service availability, security and continuity targets
- Customer and provider responsibilities
- Critical business periods and exceptions (holidays, escalation etc)
- All targets contained within an SLA should be capable of being monitored and measured.
- When the service is being provided to an external customer, the sla will normally supplement a contract that will define the minimum acceptable level of service.
- Structure of Service Level Agreements

Some organizations have chosen to adopt a multiple level SLA structure. One example of the three layer structure might be as follows

Corporate level: covering all the generic SLM issues appropriate to every customer throughout the organization (such as response times when calling the service desk)

Customer Level: veering all SLM issues relevant to the particular customer group, regardless of the service being used.

Service level: covering all SLM issues relevant to the specific service in relation to a specific customer group (1 for each service covered by the SLA)

Operational Level Agreements (OLAs)

OLAs are also known as back to back agreements. They define support requirements internally. The most common use of an OLA is to define the relationship between the Service Desk and internal support groups.

OLAs are required to ensure that the SLA targets agreed between customer and provider can be delivered in practice. OLAs describe each of the separate components of the overall service delivered to the customer often with one OLA for each support group and a contract for each supplier. OLAs or SLAs may be agreed with external suppliers to supplement external contracts.

Underpinning Contracts

It is important to ensure that all targets contained within both SLAs and OLA that rely on external suppliers are underpinned by the appropriate level of maintenance and support contracts, and are documented and agreed within such contracts.

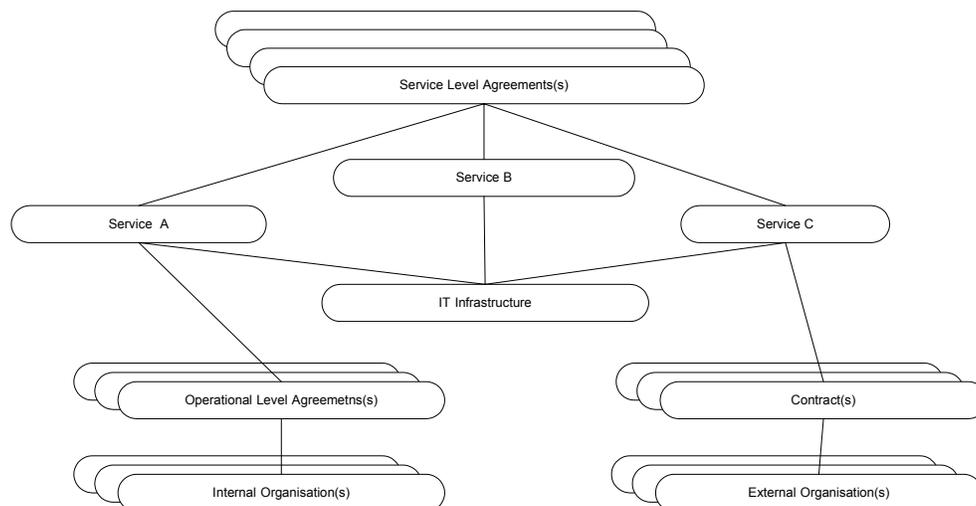


Figure 17 - SLA, OLA and Contract Support Structure

Service Improvement Programme

SLAs generally concentrate on the quality of the service that will be delivered in the next twelve months. In rapidly changing environments, a service improvement programme (SIP) should be produced to demonstrate to the customers, the steps that will be taken to improve the service in the next revision of the SLA.

Beyond SLAs

Any organizations consider SLM to consist purely of the creation of SLA that are then promptly forgotten about. In reality a SLA is a means to an end, a mechanism for the management of a relationship between customer and provider for mutual benefit.

The true benefits of Service Level Management will come only when both parties see the benefits of their active involvement in the whole process.

Benefits

- Both parties have a clearer view of responsibilities and there are specific service targets to aim for
- Service monitoring and reviews will allow weak areas to be identified, so that remedial action can be taken.
- Misunderstandings between customers and IT service providers are avoided
- SLM underpins supplier management and SLAs are a key part of managing supplier relationships
- IT services will be designed to meet service Level Requirements (SLR's) of future business requirements.
- SLAs can be used as a basis for charging and will demonstrate what customers receive for their money.
- OLAs and support contracts with external suppliers are better aligned with the business services required.

Possible Problems

- Ensuring targets are verified and achievable before agreeing and committing to them
- Monitoring, measuring and reporting of actual achievements
- Incorrect scoping, with inadequate resources and time
- Not enough seniority /authority given to SLM to push through negotiations / improvements
- SLAs may not be supported by adequate underpinning contracts or agreements.
- SLAs may be too lengthy, not concise, not business focused and therefore not used.
- Business requirements not clearly understood with no business justification for the requested service levels.
- Lack of focus on business critical services / processes
- A resistance to change.
- The service levels to be provided are dictated to customers
- Customer perception and expectation
- SLM not used to trigger service improvements
- SLM not aligned with complete service life cycle.

13. Financial Management for IT Services

Goal

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

Why Financial Management for IT Services?

Financial Management for IT Services is an internal part of Service Management. It provides the essential management information to ensure that services are run efficiency, economically and cost effectively. An effective Financial Management system will:

- Assist in the Management and reduction of overall long term costs
- Identify the actual cost of services and their provision
- Provide accurate and vital financial information to assist in decision making
- Identify how IT adds value to Customer's business
- Enable the calculation of Total Cost of Ownership and Return on Investment
- Make Customer aware of what services actually cost , If appropriate
- Support the recovery of cost from customers if appropriate in a fair and equitable manner
- Provide Measurements of value for money and provide incentives to produce quality services aligned to business needs
- Helps influence Customer behavior for example by providing incentives for using non-critical resources
- Provide better cost information and control of external contracts and suppliers
- Assists in the assessment and management of changes

Responsibilities

- Enables the organization to account fully for the spend on IT services and to attribute the costs to the services delivery to the organization's Customers.
- Assist management decision on IT investment by supporting details business cases for changes to IT services.
- Control and manages the overall IT budget and enables the fair and equitable recovery of costs (by charging) for the provision of IT services.

Key Considerations

Concepts

Budgeting and Accounting (mandatory): understanding the cost of providing each service, whether recorded or not is essential to delivery and maintenance of cost effective and efficient services. These activities enable an organization to:

- Predict the money required to run IT services for a given period.
- Ensure that the actual spend can be compared with the predicted spend at any point.
- Account for the money spent in IT services in a given period.
- Calculated that cost of IT services provision.

Changing (Optional): can have clear business benefits, acting as an incentive to the provider and giving leverage to the customer who can demand value for Money, Changing enables an organization to:

Recover the cost of IT Services from The customers for the service.
Operate the IT services as a business unit if required.

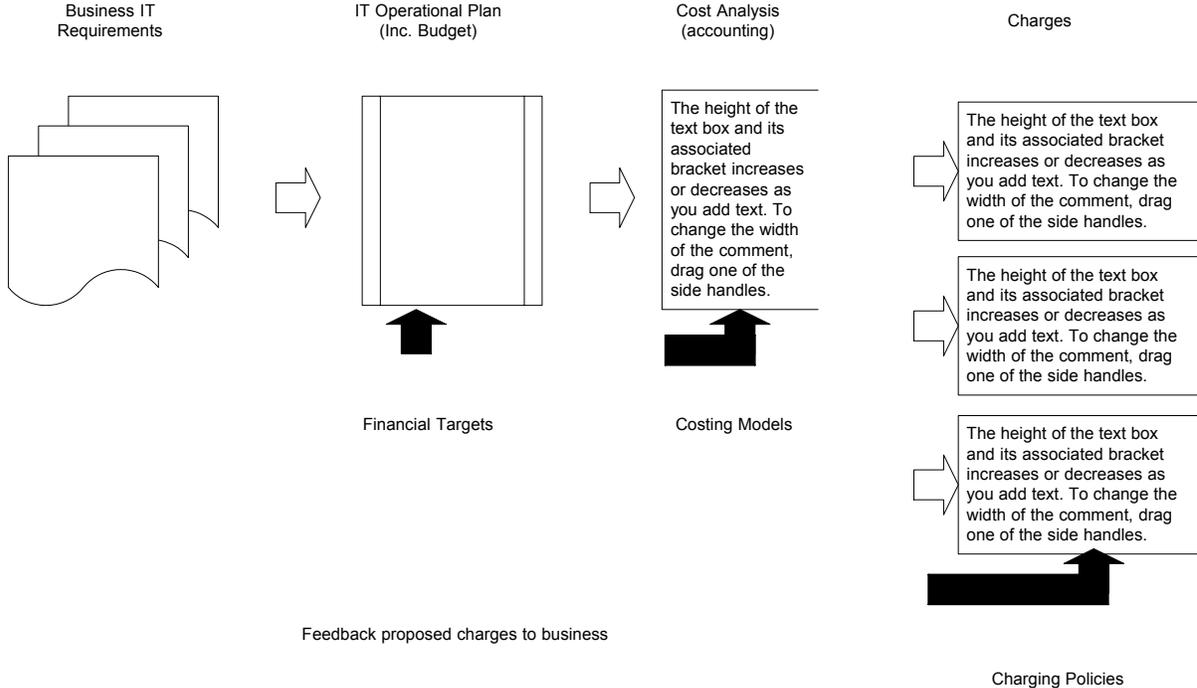


Figure 18 - Costing, Changing and Budgeting Cycle

Changing

Changing needs to be seen as begin simple, understanding; fair and realistic, Senior IT and Business Manager will set the changing policy. Possible charging policies are:

Cost	Price = Cost
Cost-plus	Price = Cost ± X%

Going rate Price is comparable with others internal departments costs within the organization or with similar organization

Market rate Price matches that charged by external suppliers

Fixed rate A set price is agreed for set period with the customer based on anticipated usage.

Cost Elements

Typical major cost types for an organization's cost might be:

Type	Includes
Hardware	Mainframes, disk storage, networks, PCs, portables, Local Servers
Software	Operating Systems, applications, databases, monitoring and management tools
People	Payroll costs, benefits, re-location costs, expenses, consultancy
Accommodation	Office, storage, secure areas, utilities
External Services	Security Services, Disaster Recovery Services, Outsourcing Services
Transfer	Internal changes from other cost centers with in organizational

Each cost can be categorized for accounting purpose between different alternatives, including the following:

Either	Or
Capital Outright purchase of fixed assets e.g. new server	Operational Day-to day cost of running a service: Staff , electricity, maintenance, consumables
Direct Costs Which can be directly allocated to a single Customer or Customer group	Indirect It could be absorbed or unabsorbed Costs which must be apportioned Across all or a number of customer group
Fixed Costs fixed for a reasonable period Of time (salaries, depreciation, Standing changes)	Variable Costs that vary with usage or time (Overtime, electricity etc.)

Cost Model

A framework, in which all known costs necessary to calculate the overall cost of IT service provision can be recorded and allocated to specified Customer. Most Cost models are based on calculating the cost for each Customer but other models can be developed to show the cost for each service or the costs for each location.

Hardware	Software	People	Accommodation	External Services	Transfer
----------	----------	--------	---------------	-------------------	----------

Cost Elements

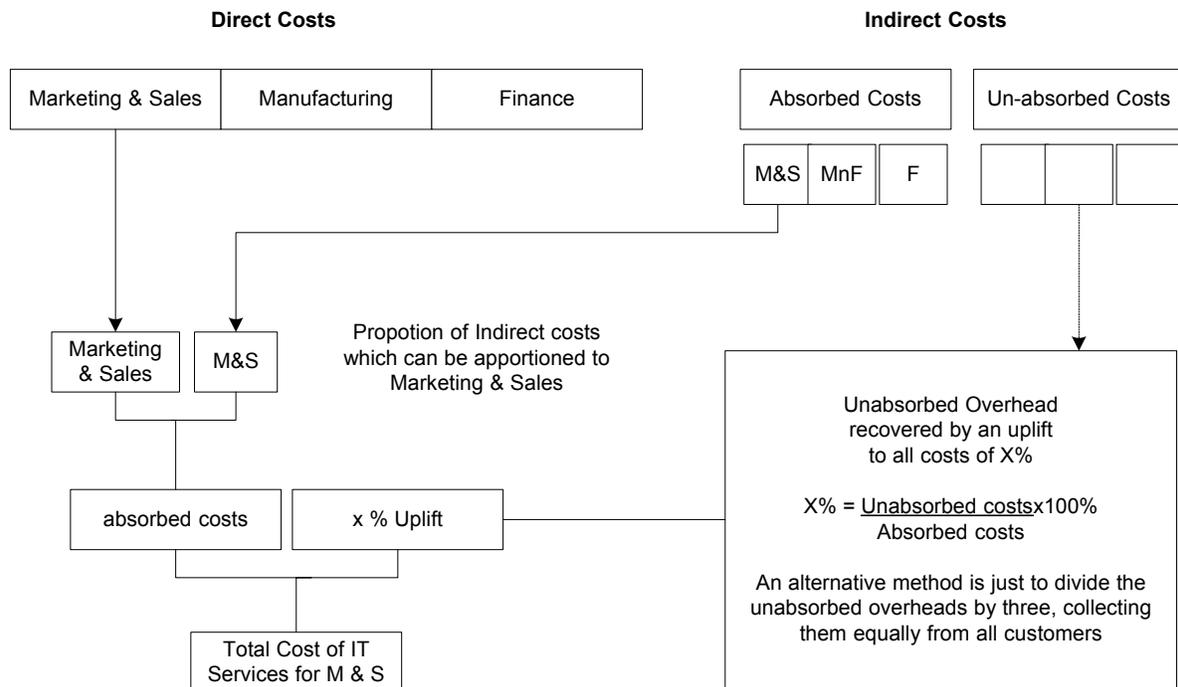


Figure 19 - Cost Model of Costs by Customer

Benefits

- Reduced long terms costs
- Increase confidence in setting and managing budgets
- Accurate cost information to support IT investment
- More efficient use of IT throughout the business
- Increase awareness and professionalism with in IT
- Ensuring that the business provides sufficient funds to run the IT services
- Recovering IT costs in a fair manner, related to usage
- Influencing Customer and User behavior
- Allowing comparison with alternative service Providers

Possible Problems

- Budgeting, accounting and charging are often new disciplines in IT and there are limited skills available.
- The lack of availability of planning information both within and outside IT, could cause problems and delays
- It staff with accountancy skills are rare , so key activities may rely on uncommitted external resources
- Enterprise IS strategies and objectives may not be well developed and prediction of capacity not accurate

- Senior IT Business Manager may resent the administrative overheads of financial processes
- IT may not be able to respond to changes in Customer demands once costs become an influence
- The financial processes are so elaborate that the cost of the system exceeds the value of the information
- The monitoring tools providing resources usages information are inaccurate irrelevant or too costly
- If the charges are seen as excessive Customer may go elsewhere for their IT Services.

14. Capacity Management

Goal

To understand the future business requirements (the required service delivery), the organisation's operation (the current service delivery), the IT infrastructure (the means of service delivery) and ensure that all current and the future capacity and performance aspects of the business requirements are provided cost effectively.

Why Capacity Management?

Capacity Management ensures that IT processing and storage capacity provision match the evolving demands of the business in a cost effective and timely manner. The process encompasses:

- Monitoring the performance and the throughput of IT Services and supporting IT Components
- Tuning activities to make efficient use of resources
- Understanding the current demands for IT Resources and deriving forecasts for future requirements
- Influencing the demand for resources, in conjunction with other service management processes
- Producing a capacity Plan predicting the IT resources needed to achieve agreed service levels

Success in Capacity Management

Success depends on a number of factors

- Accurate business forecasts
- An understanding of current and future technologies
- An ability to demonstrate cost effectiveness
- Interaction with other effective service management processes
- An ability to plan and implement the appropriate IT capacity to match business need

Inputs	Sub-Processes	Outputs
Technology	Business Capacity Management:	Capacity Plan
SLAS, SLRS and Service Catalogue	Trend forecast, model, prototype size and document future business requirements	Capacity Database
Business Plans and Strategy		Baselines and profiles
IS, IT Plans and Strategy		Thresholds and alarms
Business requirements and volumes	Service capacity	Capacity reports (regular, ad-hoc and exception)
		SLA and SLR

Operational Schedules	Management: Monitor, analyse tune and report on service performance , establish baselines and profiles of use of services, manage demand for service	recommendations
Deployment and Development plans and programmes		Costing and charging recommendations
Forward schedule of Change		Proactive changes and service improvement
Incidents and Problems		Revised operational schedule
Service reviews	Resource Capacity Management:	Effectiveness reviews
SLA Breaches	Monitor, analyse, tune and report on the utilization of components, establish baselines and profiles of use of components.	Audit Reports
Financial Plans		
Budgets		

Figure 20 - The Capacity Management Process

Responsibilities:

There are three principal areas of responsibility:

Business Capacity Management (BCM):

IS responsible for ensuring that the future business requirements for IT Services are considered, planned and implemented in a timely fashion, these future requirements will come from business plans outlining new services. Improvements and growth in existing services, development plans etc. This requires knowledge of :

- Existing service levels and SLAs
- Future service levels and SLRs
- The Business plan and capacity plan
- Modeling techniques (Analytical, simulation, trending and baselining)
- Application sizing methods

Service Capacity Management (SCM)

Focuses on managing the performance of the IT services provided to the customers and is responsible for monitoring and measuring services, as detailed SLAs and collecting, recording, analyzing and reporting on data. This requires knowledge of:

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

Resource Capacity Management (RCM)

Focuses on management of the components of the IT infrastructure and ensuring that all finite resources within the IT infrastructure are monitored and measured, and collected data is recorded, analysed and reported, this requires knowledge of:

- The current technology and its utilization
- Future or alternative technologies
- The resilience of systems and services

Key Considerations

Overlapping Activities

The service and resource capacity management sub-processes carry out many similar activities. However the two sub processes each have a very different focus the former is focused on the services that support the business, and the latter is focused on the technology that underpins all the service provision.

Performance and Capacity Issues

Capacity management should be focal point for all IT Performance and capacity issues. Other technical domains, e.g network management may carry out the bulk of the relevant day-to-day duties, but overall responsibility should lie with a centralized capacity management process.

Alternative Activities

The main capacity management activities of monitoring, analysis, tuning and implementation are iterative in nature.

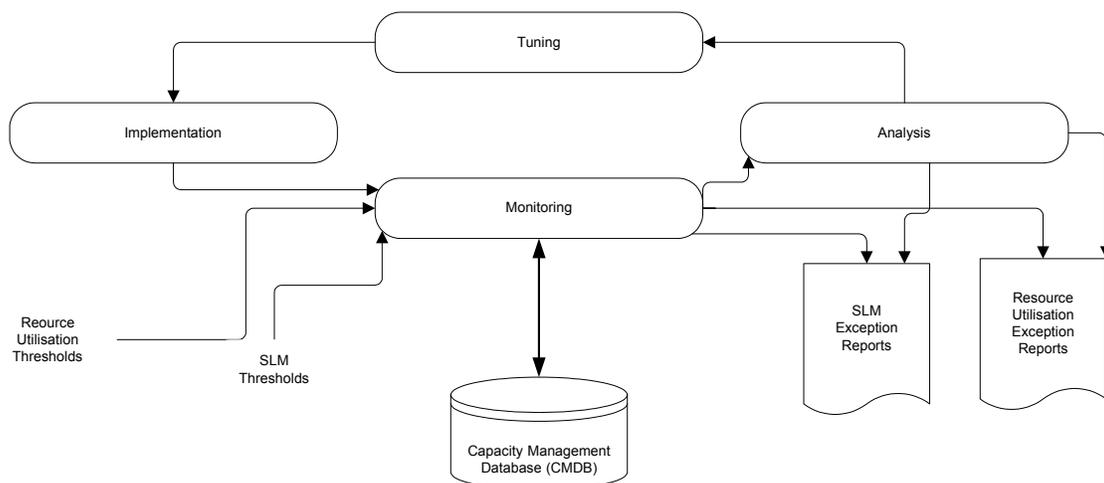


Figure 21 - Iterative Capacity Management Activities

The Capacity Management Database

The Capacity Management Database (CDB) is used as the basis for the production of all capacity management reporting on existing and future capacity issues, it is unlikely to be a

single database, but will probably exist in several physical locations and will contain many different types of data, including:

- Business data
- Service data
- Technical data
- Financial data
- Utilisation data

Capacity Management and the Business

Capacity management must understand the technical infrastructure and its capabilities and also the likely effects of the use of new equipments and technologies

However, even more importantly, it must also work closely with the business it needs to be able to translate business prediction and workload estimates into capacity requirements in terms of quantity and determine when they will be required

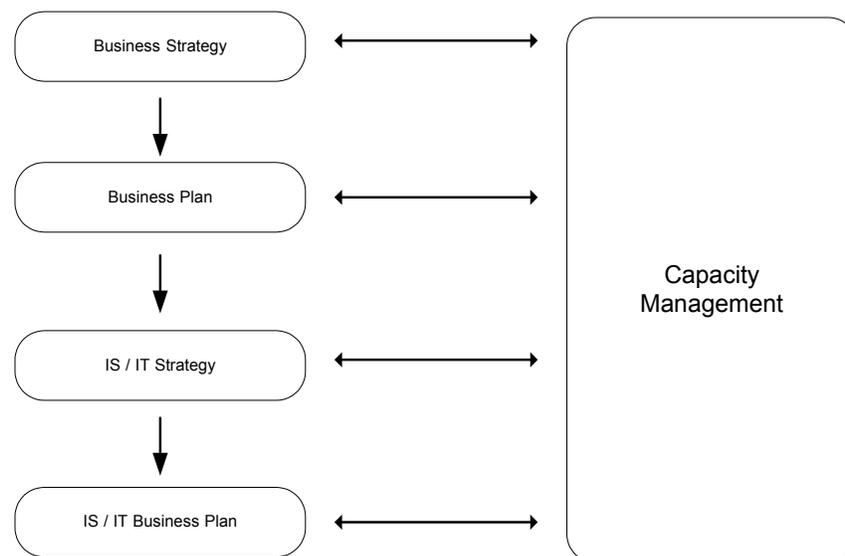


Figure 22 - Capacity Management and the Business

Demand Management

This is an important aspect of the interface between the business and capacity management and has the objective of influencing demand and therefore the use of resources. It requires a full understanding of the business requirements and their demands on IT services and resources. It must be carried out extensively and without causing damage to the business, customers, users or the reputation of IT.

A Balancing Act

Capacity Planning is essentially a balancing act:

Cost against capacity
Supply against demand

Benefits

- Increased efficiency and cost savings resulting in more economic provision of IT Services
- Deferred expenditure
- Elimination of unnecessary spare capacity and optimization of equipments
- Elimination of expensive panic buying
- Reduced risk of performance Problems and failure
- More confident and improved forecasting
- Early and improved forecasting
- Early and improved awareness of capacity issues within the application development life-cycle
- Better and more informed acquisition of IT resources
- Better relationships with customers and users with improved understanding of service levels and SLAs
- Service improvements through better control
- Less need for reactive support

Possible Problems

- Customer expectations exceed technical capacity
- Over expectation of the benefits to be gained from tuning
- Unrealistic and unachievable performance figures from equipments suppliers and manufacturers
- Unavailability of necessary business information due to commercial and or security concerns
- Unreliable and inaccurate business forecasts and information
- Incomplete or inaccurate information, particularly from distributed systems, networks and PCs
- Too much data: many tools provide vast amounts of capacity information
- Lack of financial resources and technical resources and skills

15. IT Service Continuity Management

Goal

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.

Why IT Service Continuity Management?

IT Service Continuity management is concerned with managing an organisation's ability to continue to provide a pre-determined and agreed level of IT services to support the minimum business requirements, following an interruption to the business.. This includes:

Ensuring business survival by reducing the impact of a disaster or major failure.

Reducing the vulnerability and risk to the business by effective risk analysis and risk management.

Preventing the loss of customer and user confidence

Producing IT recovery plans that are integrated with the fully support the organisation's overall Business Continuity Plan.

Responsibilities

The available IT Service Continuity options must be understood and the most appropriate solution chosen in support of the business requirements

Roles and responsibilities need to be identified, and endorsed and communicated from a senior level to ensure respect and commitment for the process

IT recovery plans and business continuity plans should be aligned and regularly reviewed, revised and tested.

Roles in Normal Operation	Roles in Crisis Situation
Board Level	
Initiate IT Service Continuity, set policy, allocate responsibilities, direct and authorise.	Crisis management, corporate decisions, external affairs.
Senior Management	
Manage IT Service Continuity, accept deliverables, communicate and maintain awareness, integrate across organisation.	Co-ordination, direction and arbitration, resource authorization.
Junior Management	
Undertake IT Service Continuity analysis, define deliverables, contract for services, manage testing and assurance	Invocation, team leadership, site management, liaison and reporting
Supervisors and Staff	
Develop deliverables, negotiate services, perform testing, develop and operate processes and procedures.	Task execution, team membership liaison

Key Considerations

- IT and Business Continuity Awareness
- The best way to raise awareness is to highlight the potential risks and business impacts facing an organisation. Awareness of the need for IT Service Continuity Management will come from:
 - The range of risks facing an organisation and its vulnerability
 - The potential business impacts that could result should any of the risks materialise.
 - The likelihood of each of the risks materializing
 - Personal responsibilities and liabilities, e.g. Of directors
 - External pressures, e.g. From regulators or shareholders.

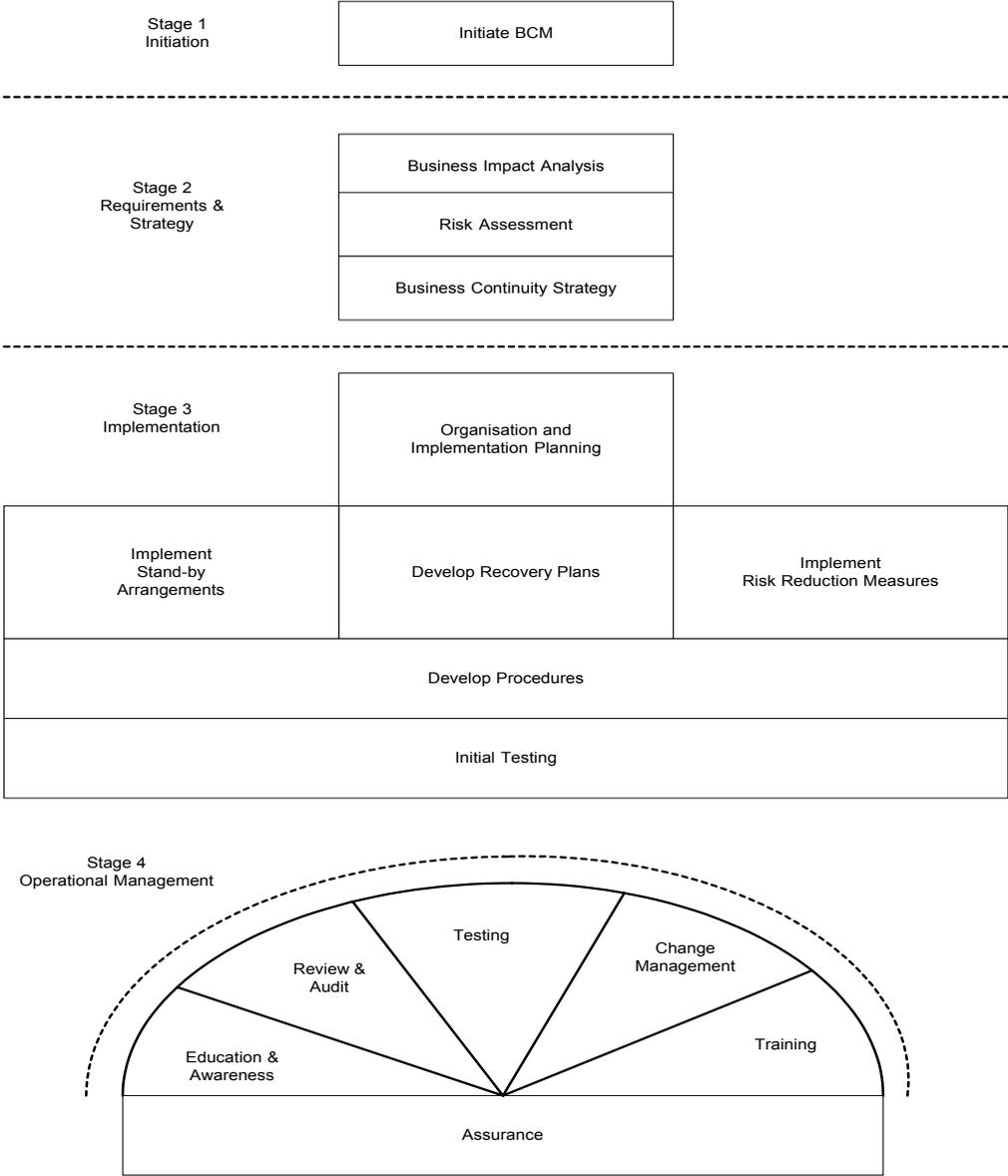


Figure 23 - The Business Continuity Life Cycle

Recovery Options

Options need to be considered for:

People and accommodation

IT Systems, networks, and processes

Critical services such as power, water, post, etc

Critical assets such as paper records, reference material, etc

Option	Description
Do Nothing	Rarely used, because few business processes can function effectively without IT
Manual back-up	Can be an effective interim measure until the IT Service is resumed
Reciprocal arrangement	Organisations agree to back each other up in an emergency, rarely used now except for off-site storage because of practical difficulties, e.g. limited excess IT Capacity
Gradual recovery: (sometimes referred to as "cold standby")	Usually consists of an empty computer environment in which an organisation can install its own equipments. May be used where a business can function for a period of 72 hours or more without IT Services, Can be internal or external, fixed or portable, possible with guaranteed equipment delivery.
Intermediate Recovery: (Sometimes referred to as "warm standby")	Typically involves the re-establishment of critical systems and services within a 24-72 hour period. Can be internal or external, fixed or portable and consists of a computer environment containing recovery IT Equipment that can be configured to support the business.
Immediate recovery (sometimes referred to as "hot standby")	Would involve the use of an alternative site with continuous mirroring of live equipment and data. Can be internal or external as is the most expensive option. Should only be used for critical business services where loss of service would cause an immediate business impact.

Risk Analysis

Many methods of risk assessment and analysis exist, such as the CCTA Risk analysis and management method (CRAMM). This involves the identification of risks, the associated threats, vulnerabilities and impacts together with the subsequent implementation of cost justifiable countermeasures.

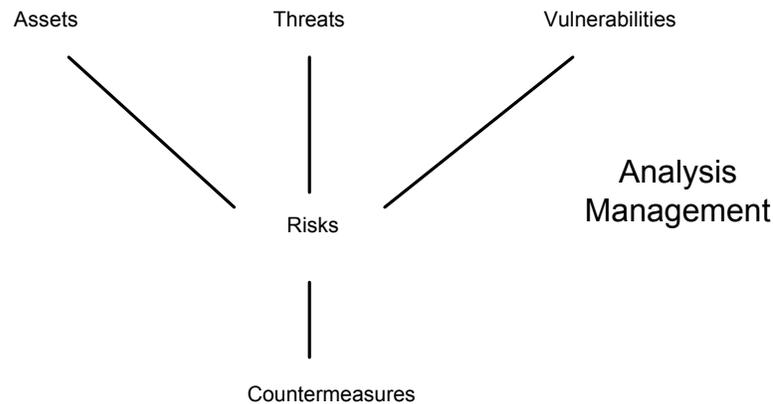


Figure 24 - The CRAMM Risk Assessment Model

Benefits

- Management of risk and the consequent reduction of the impact of failure
- Potentially lower insurance premiums
- Fulfillment of mandatory or regulatory requirements
- Improved relationships between the business and IT through IT becoming more business focused, and more aware of business impacts and priorities.
- Reduced business disruption during an incident with an ability to recover services efficiently in business priority order
- Increased customer confidence, possible competitive advantage and increased organizational credibility.

Possible Problems

- Obtaining management commitment and resources
- Gaining buy-in-and assistance from the business
- The process and cost of testing and invoking plans for live services
- Availability of components, resources and data to test the IT recovery and business continuity plans
- Overlooking critical components, applications, and dependencies and misinterpreting business impacts
- Incorrect business impacts and or business focus.
- Poor integration with other business and Service management processes.

Testing the Recovery Plan

Plans should be tested after initial development, and thereafter atleast annually, and following major changes, Testing will range from inspection or walk-through, to announced testing of components, or to full un-announced test involving the business and IT.

16. Availability Management

Goal

To optimize the capability of the IT infrastructure and supporting organisation to deliver a cost effective and sustained level of availability that enables the business to satisfy its objectives.

Why Availability Management?

Availability Management ensures services are available when the customer needs them, and is influenced by:

- Business demand
- The cost required to meet it
- The configuration and complexity of the IT infrastructure including the level of redundancy, the reliability of the infrastructure and its components, and the level of infrastructure maintenance
- The process and procedures used by IT services
- Human factors and external events

Responsibilities

- Optimise availability by monitoring and reporting on all key elements of availability
- Determining availability requirements in business terms
- Predicting and designing for expected levels of availability and security
- Producing the Availability Plan
- Collecting, analyzing and maintaining availability data and reporting on that data
- Ensuring service levels are met by monitoring service availability levels against SLAs and monitoring OLA targets and external supplier serviceability achievements.
- Continuously reviewing and improving availability

Key Considerations

Elements of Availability Management

Availability: the percentage of agreed service hours for which the component or service is available.

Reliability: the prevention of failure, and the ability to keep services and components operable

Maintainability: the ability to restore services or components back to normal operation

Serviceability: the support for which external suppliers can be contracted to provide parts of the IT infrastructure.

Security: the implementation of justifiable controls to ensure continued IT service within secure parameters, viz: confidentiality, integrity and availability (for more details refer to the ITIL security management publication or to BS7799/ISO17799). The information

security management standards.) Security should be considered in all aspects of the following diagram:

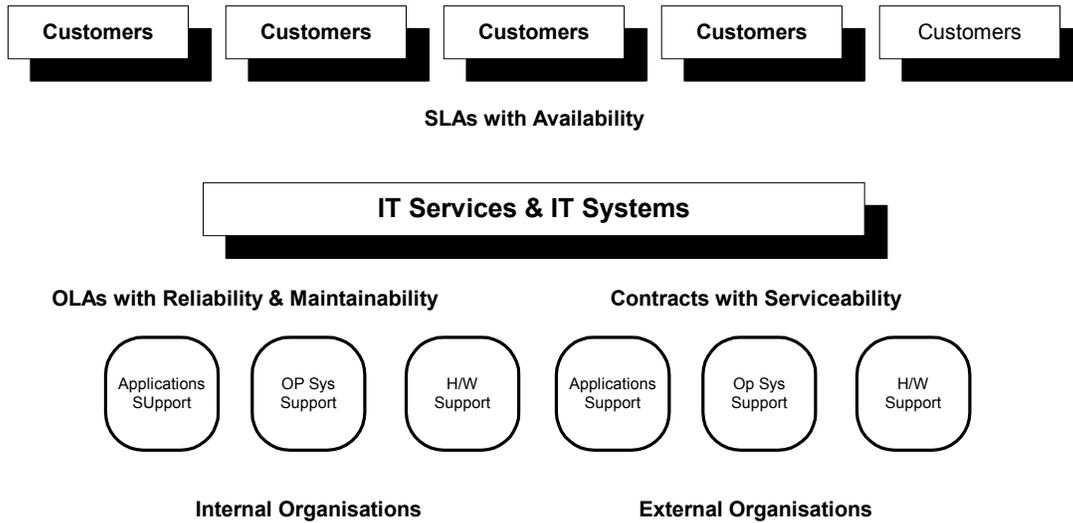


Figure 25 - Relationships with Support Organisations

Availability Metrics

The IT Availability Metrics Model (ITAMM) assists in assessing the range of metrics and perspectives that should be considered when establishing availability measurement and reporting. The model can be used to establish what needs to be measured in order to give a comprehensive view of the availability of IT Services.

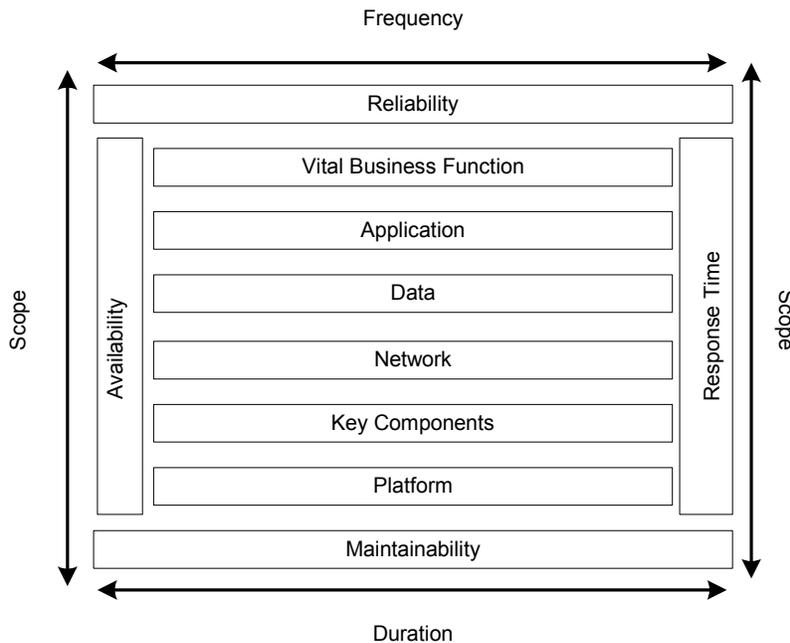


Figure 26 - The IT Availability Metrics Model

Measuring Availability

Measurements need to be meaningful and add value if availability measurement and reporting are to ultimately deliver benefit to the IT and business organisation. This will be strongly influenced in the combination of what you measure and how you report it.

The Availability Plan

The Availability plan should be a long term plan for the proactive improvement of IT availability within the imposed cost constraints. The plan should have goals, objectives and deliverables and should consider the wider issues of people, processes, tools and techniques as well as having a technology focus.

Availability Management Principles

Availability is at the core of business need and user satisfaction
 Recognising that when things go wrong, you can still achieve user satisfaction
 Improving availability can only be achieved when you understand how the technology integrates with and supports the business.

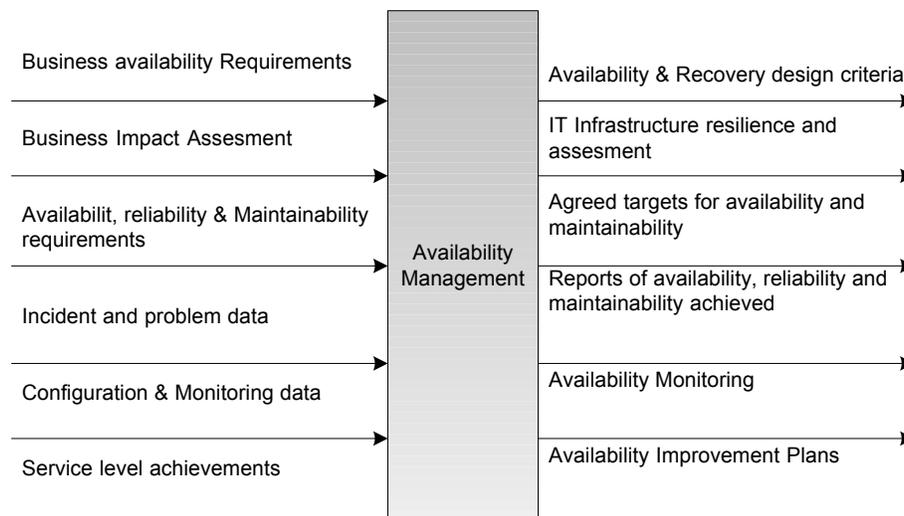


Figure 27 - The Availability Management Process

Useful Definitions

High Availability

A characteristic of the IT Service that minimizes or masks the effects of IT component failure to the user.

Continuous Operation

A characteristic of the IT Service that minimizes or masks the effects of planned downtime to the User.

Continuous Availability

A Characteristic of the IT Service that minimizes or masks the effects of ALL failures and planned downtime to the user.

Benefits

- Addresses the fundamental business requirement for high levels of availability
- Services are designed and managed to cost effectively meet specified business requirements
- Availability levels are measured to fully support service level management
- Shortfalls in service levels are identified and corrective actions taken
- Frequency and duration of IT failures is reduced
- Change IT mindset from a reactive to a proactive attitude
- IT Support “adds value” to the business

Possible Problems

- Measures of availability that are meaningless to the business
- Not measuring availability at the point of service delivery.
- Difficulties in finding skilled and experienced staff
- Justification to management in relation to expenditure
- Lack of management commitment
- Lack of suitable software
- Dependence on suppliers for serviceability data i.e reliability and maintainability
- Difficulty in determining business and customer availability requirements
- Lack of information about the IT infrastructure, if there is no configuration Management database.

Business Value

Effective Availability Management will influence Customer satisfaction and determine the perceived reliability of the business on the market.

17. The importance of Communication

Effective and efficient communication is part of the foundation on which the success of many organisation's depends. In the business world there are many pressures on time, and often it is communication that suffers when time and resource constraints apply. In service Management there are many areas that are involved in regular communication with their business customers to ensure that the services delivered to them meet their requirements at appropriate cost. Notable examples include service desk, change management and service level management.

Everyone within IT has a responsibility to provide good communication but there is a prime responsibility at the management level to ensure that communication is embedded within the service management process.

Developing and fostering effective communication with customers and users of IT has always been an important issue, Very often this was something that was left almost to chance and to the personal actions of individuals within IT departments. In the modern business world this is not sufficient.

Organisations can be said to operate at three key levels, strategic, tactical and operational and there are specific corporate functions at each level, for IT to be fully integrated with their business customers, effective two way communication must take place at the same three levels and also between these levels.

The ability to listen, influence, negotiate and agree is vital.

Many communication techniques exist, and include seminars reports, circulars, email, memos, newsletters, meetings, awareness, campaigns, focus groups, presentations, road-shows, internet and intranet.

The Need for improvement

During review exercises of organizational, departmental, or team performance, communication is one of the most commonly mentioned topic that people suggest requires improvement.

18. Further Guidance and Contact Points

itSMF Ltd
Webbs Court
8 Holmes Road
Earley
Reading RG6 &BH
United Kingdom
Tel: +44(0)118 926 0888
Fax: +44(0)870 706 1531
e-mail; service@itsmf.com
www.itsmf.com

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

OGC
Rosebery Court
St Andrews Business Park
Norwich NR7 0HS
United Kingdom
Tel: +44(0)1603 704567
Fax: +44(0)1603 704817
e-mail: info@ogc.gov.uk
www.ogc.gov.uk
www.itil.co.uk

British Standards Institution
389 Chiswick High Road
London W4 4AL
United Kingdom
Tel: +44(0)208 996 9001
Fax: +44(0)208 996 7001
E-mail: info@bsi-global.com
www.bsi-global.com