ISO/IEC 20000 Foundation *Complete* Certification Kit

the art of service

ISO/IEC 20000 Foundation Complete Certification Kit:

Study Guide Book and Online Course

***Notice of Liability**: The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.*

***Trademarks**: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.*

ITIL® is a Registered Community Trade Mark of OGC (Office of Government Commerce, London, UK), and is Registered in the U.S. Patent and Trademark Office.

Write a Review and Receive a Bonus Emereo eBook of Your Choice

Up to $99 RRP – Absolutely Free

If you recently bought this book we would love to hear from you – submit a review of this title and you'll receive an additional free ebook of your choice from our catalog at http://www.emereo.org.

How Does it Work?

Submit your review of this title via the online store where you purchased it. For example, to post a review on Amazon, just log in to your account and click on the 'Create Your Own Review' button (under 'Customer Reviews') on the relevant product page (you'll find plenty of example product reviews on Amazon). If you purchased from a different online store, simply follow their procedures.

What Happens When I Submit my Review?

Once you have submitted your review, send us an email via review@emereo.org, and include a link to your review and a link to the free eBook you'd like as our thank-you (from http://www.emereo.org – choose any book you like from the catalog, up to $99 RRP). You will then receive a reply email back from us, complete with your bonus ebook download link. It's that simple!

Foreword

As an education and training organization within the IT Service Management (ITSM) industry, we have watched with enthusiasm as ISO/IEC 20000 has grown and progressed since 2005. The evolution of the core principles and practices provided by the standard provides the holistic guidance needed for an industry that continues to mature and develop at a rapid pace.

Our primary goal is to provide the quality education and support materials needed to enable the understanding and application of the ISO/IEC 20000 standard in a wide-range of contexts.

This comprehensive book is designed to complement the in-depth accredited eLearn ISO/IEC 20000 Foundation course provided by The Art of Service. The interactive eLearn course uses a combination of narrated PowerPoint presentations with multiple-choice assessments which will ultimately prepare you for the ISO/IEC 20000 Foundation certification exam.

We hope you find this book to be a useful tool in your educational library and wish you well in you IT Service Management career!

Ivanka Menken
Executive Director, The Art of Service
http://www.theartofservice.com/

How to access the associated ISO/IEC 20000 Foundation eLearning Program:

1. Direct your browser to: www.theartofservice.org
2. Click ‘login’ (found at the top right of the page)
3. Click ‘Create New Account’. If you already have an existing account, please move on to step 5.
4. Follow the instructions to create a new account. You will need a valid email address to confirm your account creation. If you do not receive the confirmation email check that it has not been automatically moved to a Junk Mail or Spam folder.
5. Once your account has been confirmed, email your User-ID for your new account to iso20000f@theartofservice.com .
6. We will add your account to the ISO/IEC 20000 Foundation eLearning Program and let you know how to access the program from now on.

Minimum system requirements for accessing the eLearning Program:

Processor	: Pentium III (600 MHz) or higher
RAM	: 128MB (256MB recommended)
OS	: Windows 98, NT, 2000, ME, XP, 2003, Mac OSX
Browser	: Internet Explorer 5.x or higher (Cookies and JavaScript Enabled), Safari
Plug-Ins	: Macromedia Flash Player 9
Other Hardware	: 16-bit Sound Card, Mouse, Speakers or headphones
Display Settings	: 1024x768 pixels
Internet Connection	: Due to multimedia content of the site, a minimum connection speed of 256kbs is recommended. If you are behind a firewall and are facing problems in accessing the course or the learning portal, please contact your network administrator for help

If you are experiencing difficulties with the Flash Presentations within the eLearning Programs please make sure that:

1) You have the latest version of Flash Player installed, by visiting
http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

2) You check that your security settings in your web browser don't prevent these flash modules playing. There is support for these issues at the following page:
http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_19166&sliceId=2#no_content

Table of Contents

This page intentionally left blank.

1 Introduction

1.1 What is IT Service Management?

IT Service Management is the management of all processes that co-operate to ensure the quality of live services, according to the levels of service agreed with the customer. It addresses the initiation, design, organization, control, provision, support and improvement of IT services, tailored to the needs of the customer organization.

The term IT Service Management (ITSM) is used in many ways by different management frameworks and organizations seeking governance and increased maturity of their IT organization. Standard elements for most definitions of ITSM include:

- Description of the **processes** required to deliver and support IT Services for customers.
- The purpose primarily being to deliver and support the products or technology needed by the business to meet key organizational objectives or goals.
- Definition of roles and responsibilities for the people involved including IT staff, customers and other stakeholders involved.
- The management of external suppliers (partners) involved in the delivery and support of the technology and products being delivered and supported by IT.

The combination of these elements provide the capabilities required for an IT organization to deliver and support quality IT Services that meet specific business needs and requirements.

IT Service Management gives the following benefits to the customer:

✓ Provision of IT services becomes more customer-focused and the relationship between the service provider and the customer is improved through agreements about service quality

✓ The services are better described, in customer language and in more appropriate detail

✓ The availability, reliability, cost and other quality aspects of the service are better managed

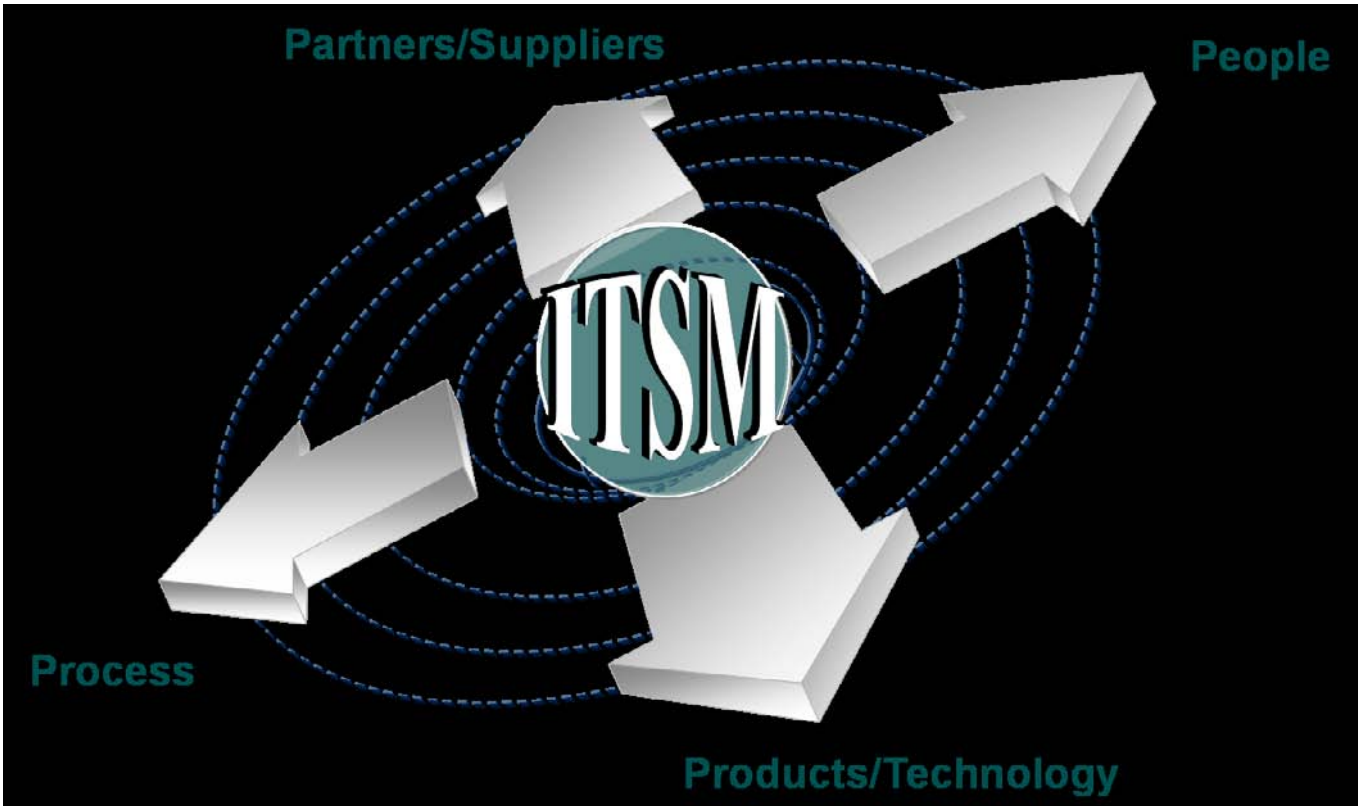
✓ Communication with the IT organization is improved by agreeing on points of contact

Please refer to module 2 in the online learning program for further information on customer focus.

IT Service Management gives the following benefits to the organization as a whole:

- ✓ The IT organization develops a clearer structure, is more efficient and is more focused
- ✓ The IT organization is more in control of the infrastructure and the services it has responsibility for
- ✓ An effective process structure provides a framework for the effective outsourcing of the IT services
- ✓ Best Practice encourages a cultural change
- ✓ Frameworks can provide coherent frames of reference for internal communication (and with suppliers) for the standardization and identification of procedures.

1.2 The Four Perspectives (Attributes) of ITSM



There are four perspectives (“4P’s”) or attributes to explain the concept of ITSM.

- *Partners/Suppliers Perspective:*
  Takes into account the importance of Partner and External Supplier relationships and how they contribute to Service Delivery.
- *People Perspective:*
  Concerned with the “soft” side: IT staff, customers and other stakeholders e.g. Do staff have the correct skills and knowledge to perform their roles?
- *Products/Technology Perspective:*
  Takes into account IT services, hardware & software, budgets, tools.
- *Process Perspective:*
  Relates to end-to-end delivery of service based on process flows.

Quality IT Service Management ensures that all of these four perspectives are taken into account as part of the continual improvement of the IT organization.

1.3 What is ISO/IEC 20000?

ISO/IEC 20000 is the International Standard for IT Service Management processes. ISO/IEC 20000 provides a recognized certification against which an organization can demonstrate to their customers that its IT Service Management processes represent best practice.

The purpose of ISO/IEC 200000 is to promote the adoption of an integrated process approach, to deliver effectively managed services to meet the business and customer requirements. Interest in ISO/IEC 20000 is widespread, as it is the recognized means of benchmarking the delivery processes of IT to the business. It is technology and sector independent, and relevant to both public and private sector organizations.

The main parties that may take specific interest in ISO/IEC 20000 are providers of IT service management services, businesses outsourcing their IT services, businesses managing their own IT services and all providers wishing to benchmark their existing IT service management services.

Personal certification with ISO/IEC 20000 through the EXIN/TÜV scheme will also provide an independent, industry-wide recognition of IT Service Management capabilities.

Please refer to module 1 in the online learning program for further introductory information on ISO/IEC 20000.

1.4 History of ISO/IEC 20000

In 2000, the world's first standard for ITSM, BS15000, was published. In Australia, this became known as AS8018.

In 2002, a second part of the standard was added, called BS15000 – 2. A formal certification scheme was also introduced.

In 2005, ISO/IEC 20000 was first published, based almost entirely on BS15000. This standard comprises two documents, ISO/IEC 20000 – 1 and ISO/IEC 20000 – 2.

In 2007, ISO/IEC 20000 was accepted in Australia as ISO/IEC 20000: 2007. The two versions of the ISO/IEC 20000 standard are available concurrently.

1.5 The Future of ISO/IEC 20000

This is a relatively new standard; however it is widely expected to have a significant impact on the future of IT service management. This is due to the following reasons:

- ISO/IEC 20000 supports established methods e.g. ITIL®, CobiT and Six Sigma
- IT Service Management certification is increasingly in demand
- The standard itself undergoes review to ensure it meets current expectations
- ISO/IEC 20000 is an internationally recognized scheme and will inevitably act as a driver for organizations to differentiate themselves in the market.

1.6 The ISO/IEC 20000 Standard

In terms of IT Service Management, there is an ever-increasing demand to improve services through the use of emerging technologies. Standards provide a common and consistent platform for organizations to work from.

There are two components to the ISO/IEC 20000 Standard.

Part 1 = SHALL

In order to achieve certification, ALL specifications from this part of the standard must be complied with. The 'shalls' have been outlined in this book for each of the service management processes.

Part 2 = SHOULD

This part of the standard is based on 'best practice'. When you are audited, it is recommended that your IT Service Management processes are performed in this way. However, certification can be achieved without demonstrating all practices from Part 2 of the standard. References to the standard will be made throughout this book for further information on ISO/IEC 20000 requirements and best practices.

1.7 Auditing & Certification

Certification requires the adoption of all requirements of the standard, and demonstration of adherence via audit by a third party, which is known as a certification body.

Part 1 of the ISO/IEC 20000 standard has been developed as a standard against which service providers can be certified. A service provider that wishes to express their adherence to quality in ITSM can have its IT organization independently verified.

An audit can be carried out by external auditors from a recognized certification body to provide you with a conformance report and, if successful, a certificate for your organization.

Conformance with the standard can be demonstrated through both internal and external reviews.

Internal reviews can be used to assess on a more detailed level whether the current IT Service Management processes conform to the standard, and establishes areas for improvement. These reviews might be part of an existing Continuous Service Improvement Program.

External reviews tend to be less detailed but are likely to be seen as a more objective and so carry greater weight that internal ones since they are both impartial and independent.

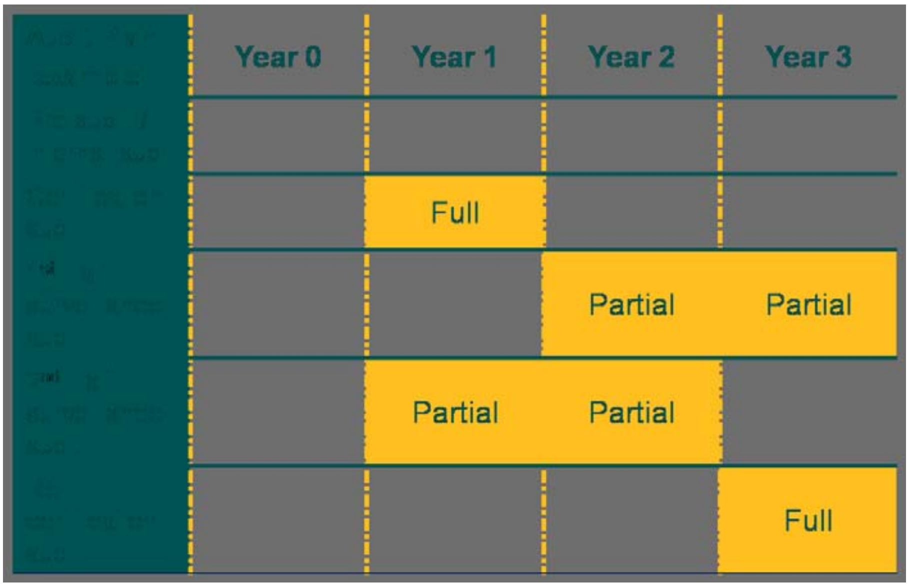
The 7 step certification process includes:

1. Questionnaire
2. Application for assessment
3. Optional pre-audit
4. Initial audit (stage 1)
5. Certification audit (stage 2)
6. Surveillance audits
7. Re-certification audits

There are a growing number of accredited certification bodies. Examples include BSI, Certification Europe Ltd, DNV, DQS, Japan Quality Assurance Organization, LRQA, SGS, STQC and TÜV.

If a Registered Certification Body (RCB, commonly known as an external auditor) conducts the external review and you meet the certification criteria, your organization can become certified as part of the scheme. You can then display the ISO/IEC 20000 certification logo. This demonstrates that you have been independently assessed as having adequate controls and procedures in place and that you are able to consistently deliver a quality of service. Guidelines do apply for the display of certification and the logo as part of any marketing materials.

You will need to re-certify after 3 years and it is considered good practice to partial audits at least once a year to ensure that the focus stays on process management control. Below is an example audit plan over a 3-year period.



[illegible]	Year 0	Year 1	Year 2	Year 3
[illegible]				
[illegible]		Full		
[illegible]			Partial	Partial
[illegible]		Partial	Partial	
[illegible]				Full

Personal certification

Internationally recognized qualified professionals in ISO/IEC 20000 are of increasing importance both to organizations and individuals. Optimizing professionalism is an important factor of successful IT service improvement programs. Staff commitment for such programs can be boosted by challenging and rewarding employees with internationally recognized certifications.

Earning an independent certificate represents solid evidence that you have successfully completed the program requirements and illustrates your dedication to becoming competent and valuable to your organization and their customers.

Chapter 13 outlines the certification pathways for ISO/IEC 20000 toward either the management or auditing track.

Please refer to module 6 in the online learning program for further information on certification.

1.8 Benefits of ISO/IEC 20000

The benefits of ISO/IEC 20000 continue to expand as organizations become more competitive and responsive to certification requirements. As an ISO/IEC 20000 certified organization, your IT service is more likely to be chosen and you will demonstrate a visible commitment to managing the provision of IT services. Beyond the benefits from the customer perspective, implementing the ISO/IEC 20000 standard improves the IT process effectiveness and efficiency and ultimately saves money. Most companies implementing ISO/IEC certification subsequently report increases in process efficiencies, higher customer satisfaction and improved service quality. Customers are assured that the development and delivery of services complies with globally accepted standards.

The benefits to the organization are summarized below:

- Primarily, the organization will become more competitive, reducing the risk, cost and time to market new products and services, whilst improving value for money and service quality.

- Suppliers will be managed more effectively

- Service providers will become more responsive, with services which are business-led rather than technology-driven.

- Your IT service is more likely be chosen, or renewed over that of a competitor that does not demonstrate ISO/IEC 20000 certification, providing both a competitive edge and demonstrating a visible commitment to managing the provision of IT services.

- It will provide enablers to visibly support the business strategy, with opportunities to improve the efficiency of services in all areas, impacting on costs and service.

- An operational benefit is to clearly demonstrate service reliability and consistency, which in any environment is critical to business survival and potential growth.

- Certification audits are continual and should be treated as a mechanism for educating and raising awareness of employees.

- Certification can also reduce the amount of supplier audits thereby reducing costs.

- Finally, the use of qualified and independent auditors can be used as a benchmark.

Please refer to module 3 in the online learning program for further information on the quality components of service management.

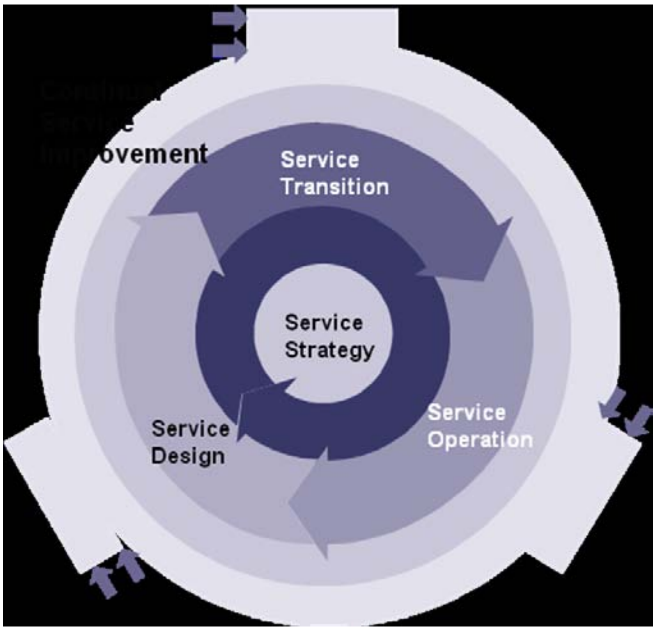
1.9 Associated Frameworks

There are several sources of practical guidance to ITSM. Among them are standards like ISO/IEC 20000 and maturity models such as CMMi, but there are many other useful standards, best practices and frameworks available, such as ITIL® and governance frameworks such as CobiT®.

ITIL®

ITIL® stands for the Information Technology Infrastructure Library. The core publications of the ITIL® Version 3 framework consist of Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. Each provides the guidance necessary for an integrated approach, and addresses capabilities having direct impact on a service provider's performance. The structure of the core is in the form of a lifecycle. It is both iterative and multidimensional. It ensures organizations are set up to leverage capabilities in one area for learning and improvements in others. The core is expected to provide structure, stability and strength to service management capabilities with durable principles, methods and tools. This serves to protect investments and provide the necessary basis for measurement, learning and improvement.

As The Art of Service is an ITIL® education and certification provider, some of the concepts in this book will be based on the ITIL® framework, however it is important to note that, while the framework provides useful guidance toward certification, ITIL® it is not a requirement of the ISO/IEC 20000 standard.



There is often confusion about the differences between ITIL® and ISO/IEC 20000. Below is a brief summary of some of these differences:

ITIL®	*ISO/IEC 20000*
Method / Practice	Standard
Descriptive Processes	Prescriptive (Part 1)
It's about processes and activities	It's about management control
Doesn't say how to manage the processes	Separate section about Management system requirements
Service Lifecycle focus	Process control focus

ITIL® is a Registered Community Trade Mark of OGC (Office of Government Commerce, London, UK) and is Registered in the U.S. Patent and Trademark Office.

CobiT

The CobiT framework provides a uniform structure to understand, implement and evaluate IT capabilities, performance and risks, with the primary goal of satisfying business requirements. The current version of CobiT, edition 4.1, includes 34 High Level Control Objectives, 13 of which are grouped under the ‘deliver and support domain’, which maps closely to ITIL®’s Service Operation phase. COBIT is primarily aimed at auditors, so has an emphasis on what should be audited and how, rather than including detailed guidance for those who are operating the processes that will be audited – but it has a lot of valid material which organizations may find useful. COBIT and ITIL® are not competitive, nor are they mutually exclusive, but can be used in conjunction as part of an organization’s overall managerial and governance framework.

MoF

MoF is incorporated within the Microsoft Enterprise Service Model that enables an organization to meet changing business demands and rapid technological change. Microsoft Enterprise Services provide innovative solutions built on proven practices for people, processes and technology for each stage of the IT lifecycle including planning, preparing, building and operating. MoF’s prescriptive guidance in operating Microsoft technologies compliments ITIL®’s descriptive guidance and each are based on industry best practice. MoF draws extensive IT experience from Microsoft, partners and customers.

Six Sigma

From a process perspective, the statistical representation of Six Sigma describes, in quantitative form, how a process is performing. It is a statistical measure of variation and a methodology for improving key processes. Six Sigma works on the foundation that everything we do can be considered as a process, or part of a process and that every process can be characterized by average performance and variation. Processes are performing optimally when the result of the process is at the expected value.

CMMi

CMMi describes the organizational maturity level, on a scale from Level 1 - Level 5. As ISO/IEC 20000 emphasizes the definition, description and design of processes, developing and implementing a quality system which complies with their requirements, using a maturity model can enable the organization to reach and maintain the system to a pre-defined level of maturity.

1.10 Other ISO Standards

ISO/IEC 20000 demonstrates a relationship with a number of ISO industry standards. These include:

ISO 9000

ISO 9000 is a standard for a generic management system. The standard provides requirements for all business organizations regardless of size, type of complexity. The purpose of ISO 9000 is to demonstrate an organization’s capability to meet its customer’s requirements through a documented Quality Management System (QMS) that is flexible, structures and customer-oriented.

ISO 15504

The purpose of ISO/IEC 15504 is to provide a guide for performing a capability assessment in order to achieve process improvement. This standard targets technology organizations wishing to assess the organization’s capabilities at each of the process stages and determine the effectiveness of the organization’s processes in relation to their goals.

ISO 27001

ISO 27001 reduces an organization's exposure to information security risk through an Information Security Management System (ISMS). Organizations wishing to control their risks and protect their assets may look to the ISO 27001 standard.

ISO 17799

Information security is a complex area, demanded standards to address specific aspects of the process. ISO/IEC 17799 is essentially a set of security controls, or the measures and safeguards for potential implementation.

Please refer to module 5 in the online learning program for further information on industry standards and related frameworks.

1.11 Roles & Responsibilities within ISO/IEC 20000

Achieving ISO/IEC 20000 requires roles and responsibilities to be clearly defined. Clarity on 'who does what' allows processes to remain consistent and efficient in the delivery of service.

ISO/IEC 20000 recognizes that each service provider may implement and allocate roles differently. It does not specify how roles and responsibilities should be documented. Matrices, in various forms, can be used for this purpose.
For example, RACI matrices identify who is responsible, accountable, consulted or informed within each process or activity.

Differences in RACI roles

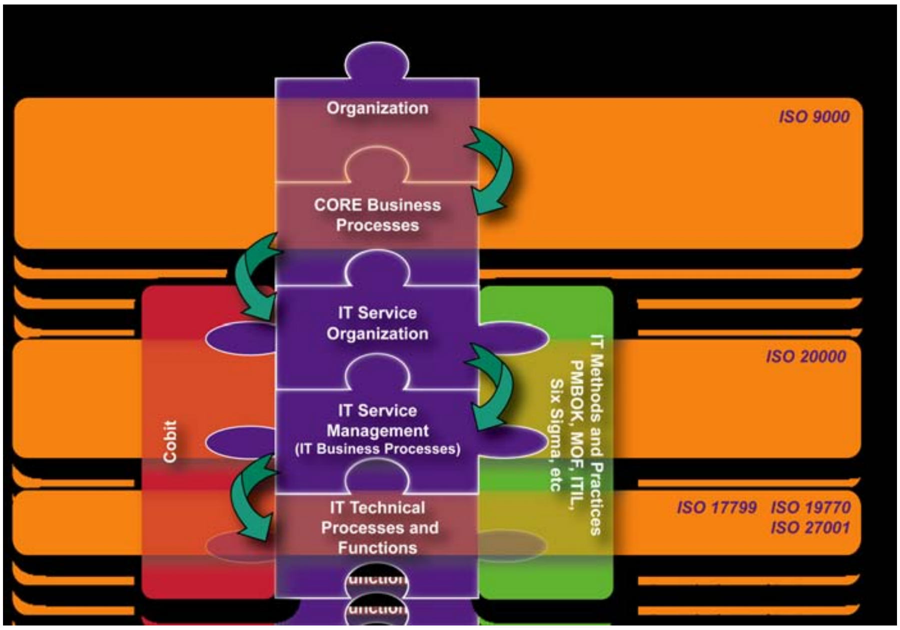
The differences in roles are normally based on guidelines such as:

- **Accountable** (e.g. the buck stops here)
    - Person with YES/NO authority, sign-off, approval, veto;
    - Should be no more than 'one per row';
- **Responsible** (e.g. the doer)
    - Takes initiative to accomplish a task/function/decision;
    - Develops alternatives
    - Consults and informs others
- **Consulted** (e.g. kept in the loop)
    - Asked for input prior to decision/action;
    - Part of two-way communication
    - Can be initiated or solicited;
- **Informed** (e.g. keep in the picture)
    - Told about a decision/action usually after the fact;
    - Permission is not sought from this person;
    - One-way communication;
    - May be prior to going public to a wide audience.

Alternately, a detailed description of each role, for example, the auditor, can be used to clearly state their responsibilities and what needs to be achieved.

1.12 Business and IT Alignment

It is important to illustrate the alignment between the Business and IT. The objective tree is a tool that can be used to understand and explain to other how the Business and IT should be aligned. The image on the following page provides an example of an objective tree. The corporate goals and objectives flow down to the business process level. Business processes are supported by the IT organization. IT goals and objectives flow down in the (IT) business processes and are supported by technical processes and functions. This way all activities, processes and IT services are aligned to the corporate goals and objectives.

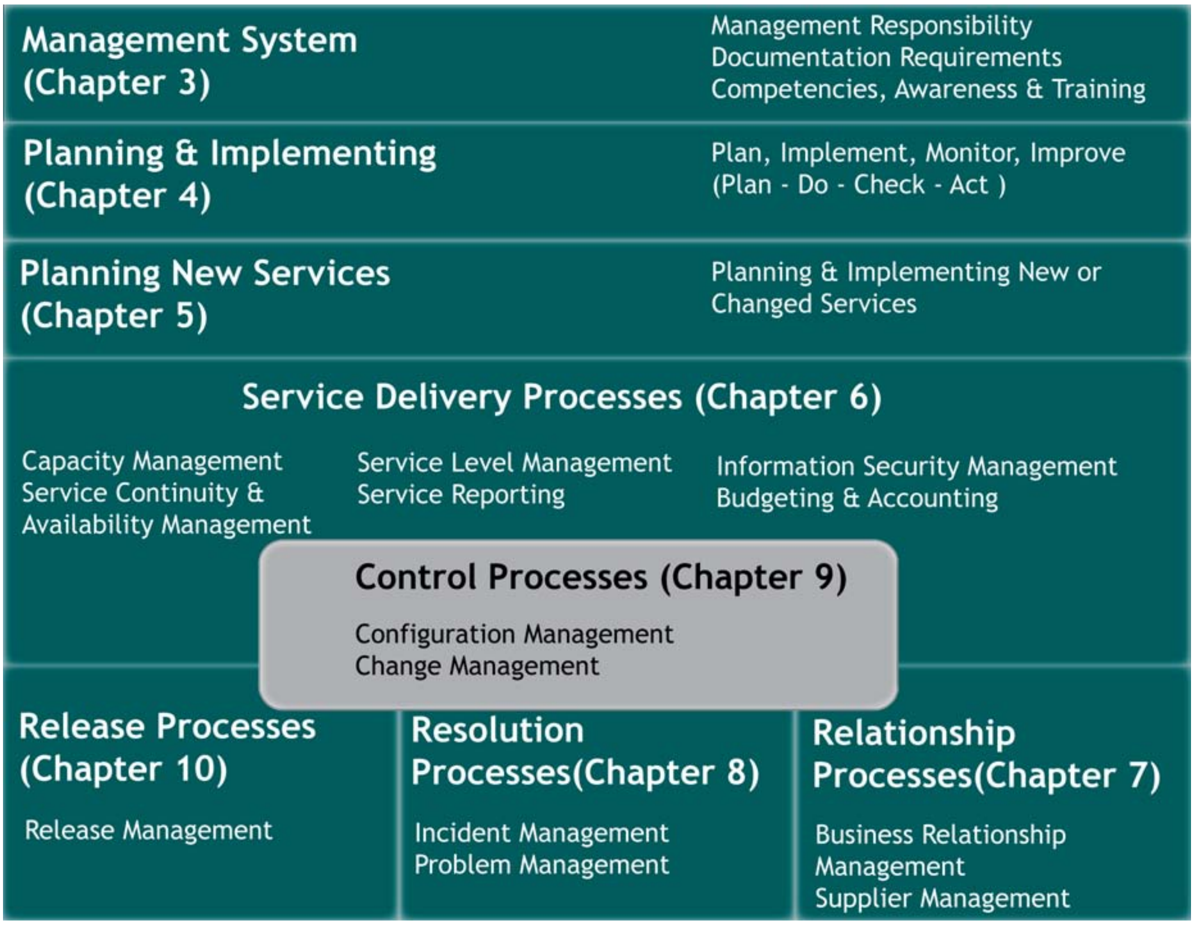

Organization
CORE Business Processes
IT Service Organization
IT Service Management (IT Business Processes)
IT Technical Processes and Functions
ISO 9000
ISO 20000
ISO 17799
ISO 19770
ISO 27001
Cobit
IT Methods and Practices PMBOK, MOF, ITIL, Six Sigma, etc

The image also provides an overview of where some of the standards and frameworks fit into the Business and IT objectives. These are those currently used in IT organizations and with internal clients or business processes.

IT Service Management enables the IT group to provide effective and efficient Information Systems to meet the requirements of the business processes. This in turn enables the organization to meet its Business Objectives. ITSM may also be critical in providing the business with a source of competitive advantage in the market place.

1.13 ISO/IEC 20000 Processes

ISO/IEC 20000 promotes the adoption of an integrated process approach. To develop a quality management system, an organization has to identify its purpose, define the policies and objectives, determine the processes and determine the sequence of these processes. To plan a process, an organization has to define the activities of the process.


Management System (Chapter 3)

Management Responsibility
Documentation Requirements
Competencies, Awareness & Training

Planning & Implementing (Chapter 4)

Plan, Implement, Monitor, Improve
(Plan - Do - Check - Act)

Planning New Services (Chapter 5)

Planning & Implementing New or Changed Services

Service Delivery Processes (Chapter 6)

Capacity Management
Service Continuity & Availability Management

Service Level Management
Service Reporting

Information Security Management
Budgeting & Accounting

Control Processes (Chapter 9)

Configuration Management
Change Management

Release Processes (Chapter 10)

Release Management

Resolution Processes(Chapter 8)

Incident Management
Problem Management

Relationship Processes(Chapter 7)

Business Relationship Management
Supplier Management

ISO/IEC 20000 Part 1 states that ‘the relationships between the processes depend on the application within the organization and are generally too complex to model’.

All processes from all chapters must be adhered to in order to pass the ISO/IEC 20000 audit.

NOTE: Chapters 1 and 2 from the standard look specifically at Scoping and Terms & Definitions.

Please refer to module 4 in the online learning program for further information on service management systems.

1.14 Introduction Review Questions

1. How many steps are there in the certification process?

   a) Twelve
   b) Four
   c) Six
   d) Seven

2. What are the four perspectives of IT Service Management?

   a) Partner, People, Products, Process
   b) Partner, Products, Process, Purpose
   c) People, Process, Partner, Practice
   d) People, Products, Process, Purpose

3. True or False.

   The standard is comprised of three components.

   T F

4. Which of the following statements is true?

   a) In order to achieve ISO/IEC 20000 certification, ITIL® practices must be implemented in the organization.
   b) CMMi is a statistical measure of variation and a methodology for improving key processes.
   c) ISO 17799 is related to information security measures.
   d) There are four phases in the ITIL® framework.

5. Once certification is achieved, how long is it before an organization must be re-certified?

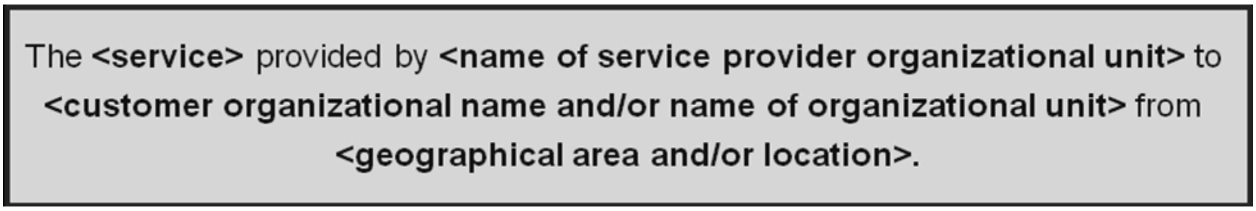
    a) 1 Year
    b) 2 Years
    c) 3 Years
    d) 4 Years

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

2 Scoping

The scope of the certified service must be described in a scope statement. A service provider can receive certification for a) part or all services that it delivers or b) a specific country or customer. The scope statement validates the certification for a specific situation. The typical structure of a scoping statement is:



The **<service>** provided by **<name of service provider organizational unit>** to **<customer organizational name and/or name of organizational unit>** from **<geographical area and/or location>.**

The scope of a certified service must be specific, mentioning the service (or services), the name of the organization (or legal entity), the name of the receiver of the service and the geographical area or location where the service is delivered from. For example, a scoping statement for a large multinational company may only show certification for the in-house IT services within Australia.

Below is a press release based on the attainment of ISO/IEC 20000 for the company, Lockwood & Wilcox. While the article refers to many different components of the business and ISO/IEC 20000 certification, the scoping statement is short and specific.

Lockwood & Wilcox Attains ISO/IEC 20000 and 27001 Certifications for Managed Services and Data Centres

Company Also Renews ISO 14001 Certification, a Key Milestone in Securing a Leadership Position in the Managed Hosting and Storage and Hosted Messaging Services Provider Space

Lockwood & Wilcox, a leading provider of the new world of communications, announced today that it has successfully attained the International Organization for Standardization (ISO) 20000-1:2005 and 27001:2005 certifications for its Global Managed Services Operations in the areas of Managed Hosting, Managed Storage Services and Hosted Messaging Services.

The company's data centres in India have attained the ISO 27001 and renewed the ISO 14001 certifications. These certifications represent another milestone in Lockwood &

Wilcox' path to securing a leadership position in the hosting and managed services space.

ISO is the entity responsible for developing and publishing standards across a variety of business, government and societal subjects. The ISO 20000 and 27001 certifications validate that basic operational best practices are followed in the areas of customer service and security, respectively. ISO certifications serve as a trusted and authoritative element of the standards-based foundation from which Lockwood & Wilcox delivers managed services.

"The managed services offered by Lockwood & Wilcox are characterized by complexity and high levels of information security," said L. Klippan, Vice President, Global Managed Services, Lockwood & Wilcox. "ISO certifications will help us to significantly scale up our Global Command Centre operations and will lead to a consistent and improved customer experience, positioning our company as a true global player in the managed services domain."

Lockwood & Wilcox owns and operates data centres located across three continents, all centrally managed by the Managed Services Operations Centre in India. The ISO certification can externally substantiate the fact that all operational processes at the Lockwood & Wilcox MSOC are built for compliance with the IT Infrastructure Library (ITIL), the prescribed manual for managing IT infrastructure, development, and operations.

"Lockwood & Wilcox continues to pursue a leadership position among global managed hosting and storage service providers," said the Vice President, Data Centre and Application Services, Lockwood & Wilcox. "Our continued data centre expansion in the US, UK, Asia and India, in addition to our portfolio expansion in the areas of virtualization, IBM AIX support, application management and server clustering are some of the key milestones planned to achieve this leadership. Attaining industry-leading certifications and participating in compliance reviews such as ISO and SAS-70 for our worldwide data centres is an integral part of our overall global strategy."

Lockwood & Wilcox offers a full suite of managed IT infrastructure services ranging from collocation to managed hosting and managed storage services, all of which are administered from highly secure locations within its global Tier-1 IP backbone, with a footprint spanning over 100 countries. Lockwood & Wilcox' corporate vision is to help businesses grow through IP enablement solutions. The fulfilment of this goal is a strategic road paved with the pursuit to confront and excel at the most contemporary, elite and rigorous technology and industry benchmarks.

3 Common Terminology

Critical to our ability to participate with and apply the concepts from the ISO/IEC 20000 Standard is the need to be able to speak a common language with other IT staff, customers, end-users and other involved stakeholders. This next section documents the important common terminology that is used throughout the Standard.

Term	*Definition*
Accreditation Body	Assessment organizations that provide certification, testing, and inspection and calibration services. Accreditation by an accreditation body demonstrated competence, impartiality and performance capability of an organization that does audits. Ensures a consistent approach.
Accredited Certification Body	Organization that performs certification audits, commonly referred to as 'professional audit companies' and which has been accredited by an accreditation body.
Availability	Ability of a component or service to perform its required function as a stated instant or over a stated period of time. Note: Availability is usually expressed as a ratio of the time that the service is actually available for use by the business to the agreed service hours.
Baseline	Snapshot of the state of a service is actually available for use by the business to the agreed service hours.
Certification	Procedure by which a 3rd party gives written assurance that a product, process or service conforms to specified requirements. ISO/IEC 20000 certification means meeting the specified

requirements following an independent audit by an accredited certification body.

Change record

Record containing details of which configuration items are affected and how they are affected by the authorized change.

Code of Practice

A standard that recommends ‘good, accepted practice as followed by competent practitioners’. Recommendations in a code of practice use the auxiliary ‘should’. A code of practice will not contain the verb form ‘shall’.

Compliance

Meeting the requirements in ISO/IEC 20000 (or another national or international standard), as assessed by an internal audit or an organization that is not an accredited certification body or qualified to carry out ISO/IEC 20000 certification audits. Compliance includes ‘Self-assessment Audits’.

Configuration Items (CI)

Component of an infrastructure or an item which is, or will be, under the control of configuration management.

Note: configuration items may vary widely in complexity, size and type, ranging from an entire system including all hardware, software and documentation, to a single module or a minor hardware component.

Configuration Management Database (CMDB)

Database containing all the relevant details of each configuration item and details of the important relationships between them.

Document

Information and its supporting medium.

Note 1: In this standard, records are distinguished from documents by the fact that they function as evidence of activities, rather than evidence of intentions

Note 2: Examples of documents include policy statements, plans, procedures, service level agreements and contracts.

Incident

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

Normative

Indicating compulsory provisions in a standard (as opposed to informative provisions which are purely there for information).

Operational Level Agreement (OLA)

Internal agreement which supports the IT organization in the delivery of services

Record

Document stating results achieved or providing evidence of activities performed.

Note 1: In this standard, records are distinguished from documents by the fact that they function as evidence of activities rather than evidence of intentions.

Note 2: Examples of records include audit reports, requests for change, incident reports, individual training records and invoices sent to customers.

Release

Collection of new and/or changed configuration items which are tested and introduced into the live environment together.

Request for change

Form or screen used to record details of a request for change to any configuration item within a service or infrastructure.

Service Catalogue

Written statement of available IT services, default levels, options, prices and which business processes or customers use them

Service Desk

Customer facing support group who do a high proportion of the total support work.

Service Level Agreement

Written agreement between a service provider and a customer

(SLA) that documents services and agreed service levels.

Service Level Requirements Detailed recording of the customer's needs, forming the design criteria for a new or modified service

Service Management Management of services to meet the business requirements.

Service Provider The organization aiming to achieve ISO/IEC 20000.

Shall Verb form that identifies a requirement from the standard.

Should Verb form that identifies a recommendation, i.e. the guidance provisions in ISO/IEC 20000. This is used extensively in ISO/IEC 20000. In ISO/IEC 20000 the word 'should' occurs only in the Notes, as these represent explanations similar to the advice in ISO/IEC 20000.

Specification A standard that sets out 'detailed requirements', using the prescriptive 'shall', to be satisfied by a product, material process or system. In ISO/IEC 20000 the verbs shall (and should) refer to aspects of the management processes, also including policy, procedures, plans and objectives.

Underpinning Contract (UC) Contract with an external supplier that supports the IT organization in their delivery of services

4 Planning & Implementing Service Management

4.1 PDCA

The PDCA or Plan-Do-Check-Act methodology, also known as the Deming Cycle, was created by Walter Andrews Shewhart and made famous by Dr W. Edwards Deming. It is an iterative four-step problem solving process that is typically used for quality control, such as that offered by the ISO/IEC 20000 standard.

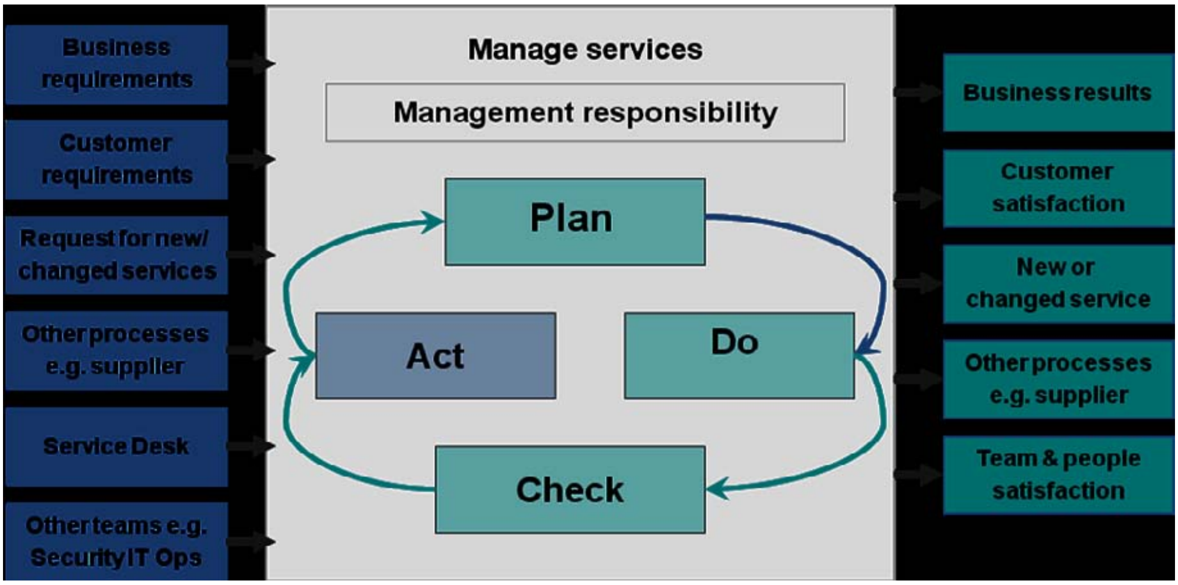
The methodology applies to all processes within ISO/IEC 20000 and outlines how the standard is to be implemented within the organization. PDCA can be described through the following:

Plan: establishing the objectives and processes necessary to deliver results in accordance with customer requirements and the organization's policies

Do: implementing the processes

Check: monitoring and measuring the processes and services against policies, objectives and requirements and reporting the results

Act: taking actions to continually improve process performance


Business requirements
Customer requirements
Request for new/ changed services
Other processes e.g. supplier
Service Desk
Other teams e.g. Security IT Ops
Manage services
Management responsibility
Plan
Act
Do
Check
Business results
Customer satisfaction
New or changed service
Other processes e.g. supplier
Team & people satisfaction

4.1.1 Plan

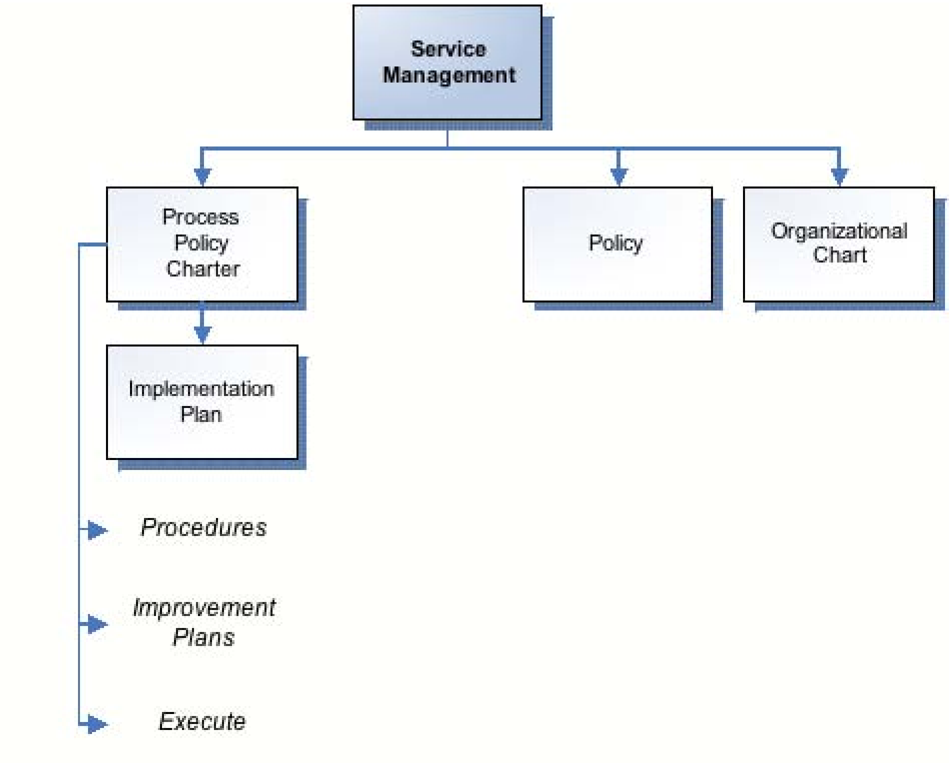
What should be done, when, by who, how and using what?

All components of service management must be planned according to the ISO/IEC 20000 standard. At a minimum plans must define:

- Scope
- Objectives and requirements
- Processes
- Framework of roles and responsibilities
- Interfaces between service management processes
- Approaches to be taken in identifying, assessing and managing issues and risks
- Approaches for interfacing to projects that are creating or modifying services
- Resources, facilities and budgets necessary to achieve the defined objectives
- Tools
- Processes for the measurement, auditing and improvement of quality

Documented responsibilities for reviewing, authorizing, communicating, implementing and maintaining these plans must be available and clear management direction must be provided.

Plans that are specific to each process must be compatible with all service management plans.



4.1.2 Do

What are the planned activities that are to be implemented?

A service management plan to manage and deliver the services must be implemented by the service provider. These plans may include:

- Allocation of funds and budgets
- Allocation so roles and responsibilities
- Documentation and maintenance of policies, plans, procedures and definitions for each process or set of processes
- Identification and management of risks to the service
- Management of teams involving the recruitment and management of staff
- Management of facilities and budget
- Management of teams including service desk and operations
- Reporting of progress against all plans
- Coordination of service management processes

4.1.3 Check

Are the processes providing expected results?
Suitable methods for monitoring and measurements of the service management processes are to be applied by the service provider. These methods are to demonstrate the ability of the processes to achieve planned results.

Reviews are to be conducted at planned intervals to determine whether the service management requirements conform to service management plans, the requirements of the ISO/IEC 20000 standard and are effectively implemented and maintained.

Reviews can be conducted internally by management while audits must be completed by an impartial party that has not been involved with the completion of the work. An audit program is to be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as results of previous audits where applicable. The audit criteria, scope, frequency and methods are to be defined in a procedure. Auditors are not permitted to audit their own work and the selection of auditors and conduct of audits must ensure the objectivity and impartiality of the audit process.

The findings of audits and reviews, along with any remedial actions identified are to be recorded together with the objective of service management reviews, assessment and audits. Any significant areas of non-compliance or concern must be communicated to relevant parties.

4.1.4 Act

How can we adjust the plans to rectify any non-conformances?

A published policy on service improvement must exist and any non-compliance with the standard of service management plans are to be remedied. A clear definition of the roles and responsibilities of service improvement activities is essential.

All suggested service improvement are to be assessed, recorded, prioritized and authorized. A plan is to be used to control the activity. There must be a process in place to identify, measure, report and manage improvement activities on an ongoing basis. This must include improvements to both an individual process and across the organization.

The service provider must perform activities to:

- Collect and analyze data to baseline and benchmark the service provider's capability to manage and deliver service and service management processes

- Identify, plan and implement improvements
- Consult with all parties involved
- Set targets for improvements in quality, costs and resource utilization
- Consider relevant inputs about improvements from all the service management processes
- Measure, report and communicate the service improvements
- Revise the service management policies, processes, procedures and plans where necessary
- Ensure that all approved actions are delivered and that they achieve their intended objectives

An example may be that the ITIL® phase of Continual Service Improvement identifies, through or via measurement and metrics, that a change is needed to the Incident Management process. Details will be compiled in a Request for Change (RFC) and coordinated and authorized through Change Management. Release and Deployment Management will test and prepare the release for the live environment and provide advice, guidance and support to the Service Operation phase, as they will deal directly with the customer. The evaluation process will assess the success of the change and report back to Change Management who will, in turn, via Key Performance Indicators and other metrics, report back to Continual Service Improvement. CSI will then assess that the approved actions were delivered and achieved the intended objective.

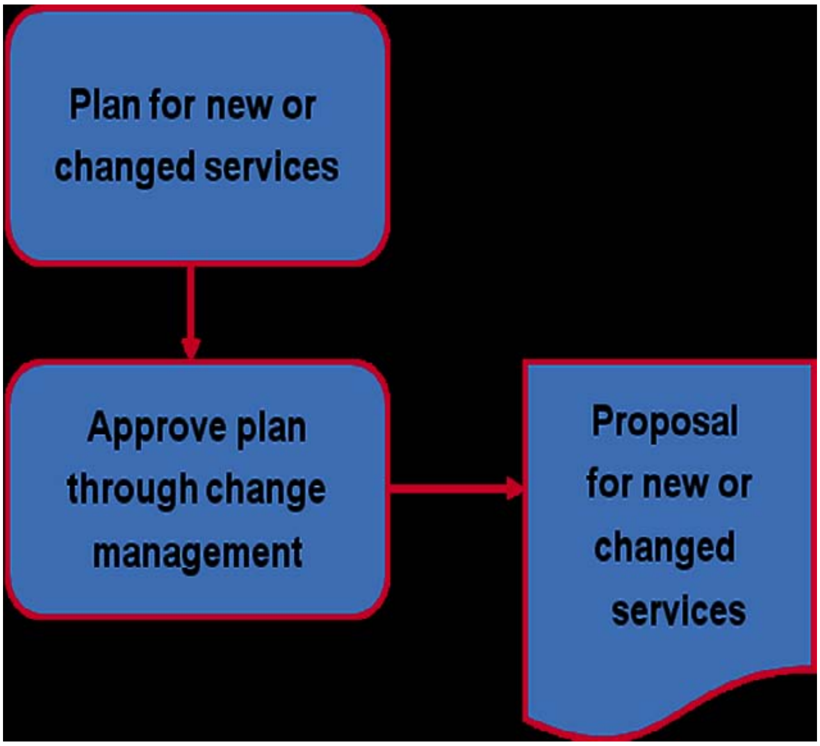
Further information on the objectives and the requirements of planning and implementing service management can be found in Chapter 4, Part 1 of the ISO/IEC 20000 standard.

This page intentionally
left blank.

5 Planning & Implementing New or Changed Services

Within any business or organization that is in operation, the need for new or changed services will always exist. Any new services, changes to the service catalogue or closure of services have to be handled by the change management process and this interface must be documented.

According to the standard, the objective of planning and implementing new or changed services is to ensure that new services and changes to services will be deliverable and manageable at the agreed cost and service quality.


Plan for new or changed services
Approve plan through change management
Proposal for new or changed services

The diagram above demonstrates the process flow from the plan for a new or changed service, through approval via change management to a formal proposal.

Proposals for new or changed services must consider:

- Cost
- Organizational impact
- Technical impact
- Commercial impact

All plans for implementation are to consider adequate funding and resources to make the changes needed for service delivery and management. For example, the Change Management process of ITIL® considers the business, technology and financial criteria before approving or rejecting a change.

The service provider must accept any new or changed service before implementation into the live environment occurs and is to report on the outcomes achieved. A post implementation review comparing actual outcomes against those planned is to be performed through the change management process.

Information about what must be included in the plans for implementing new or changed services can be found in Chapter 5, Part 1 of the ISO/IEC 20000 Standard.

Please refer to module 8 in the online learning program for further information on planning and implementation.

5.1 *Planning and Implementation Review Questions (Chapters 4 & 5)*

1. The PDCA cycle stands for:

a) Plan, Discover, Check, Act
b) Prepare, Do, Check, Act
c) Plan, Do, Check, Act
d) Plan, Do, Check, Analyse

2. Proposals for new or changed services must consider:

a) Organizational impact
b) Technical impact
c) Commercial impact
d) All of the above

3. What occurs during the Check phase?

a) Responsibilities are documented
b) Reviews are conducted
c) Fund and budgets are allocated
d) Targets for improvement are set

4. True or False.

The PDCA cycle is also known as the Deming cycle.

T F

5. What is the objective for the planning and implementation of new or changed services?

    a) To ensure that new services and changes to services will be deliverable and manageable at the agreed cost and service quality
    b) To plan the implementation and delivery of service management
    c) To define, agree, record and manage levels of service
    d) To establish and maintain a good relationship between the service provider and the customer

Answers to all questions can be found in Chapter 12.

6 Service Delivery Processes

6.1 Service Level Management

OBJECTIVE: To define, agree, record and manage levels of service.

Service Level Management focuses on the management of services based on tangible records of services, service level targets and the characteristics of the workload. As part of the audit evidence, auditors will expect to see examples of these and to see evidence of how they are used in practice. This process is fundamental to achieving a reasonable balance between service cost, quality and workloads. Through negotiation and formal agreement of Service Level Agreements (SLAs), Service Level Management establishes an understanding of the responsibilities of the service provider and of the customers. SLAs are further supported by Operational Level Agreements (OLAs) and Underpinning Contracts (UCs).

Service level management is a series of activities including:

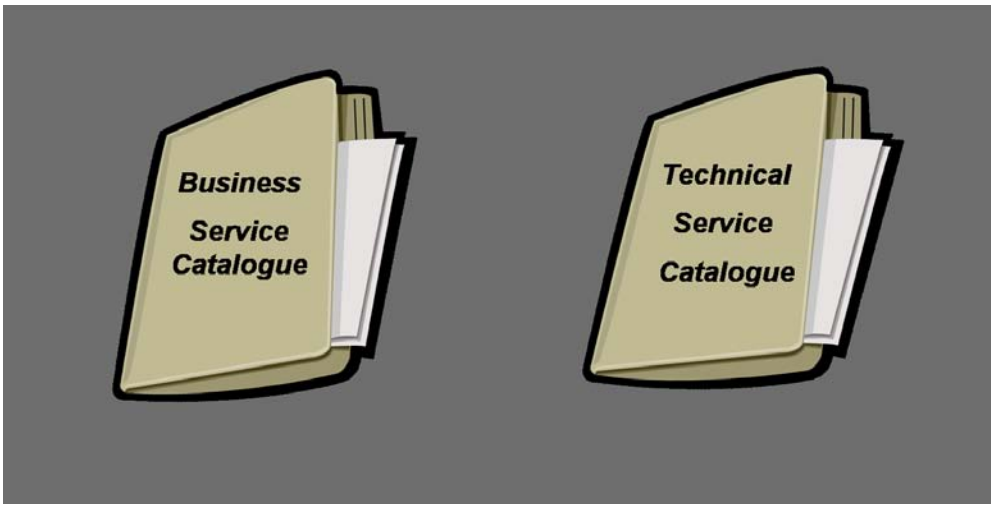
- Composing a service catalogue
- Agreeing on the service to be provided
- Monitoring the service levels
- Reporting on results
- Reviewing service levels

This process should encourage both the service provider and the customer to develop a proactive relationship to ensure that they have a joint responsibility for the service. Customer satisfaction is an important part of service level management but it should be recognized as being a subjective measurement, whereas service targets within the SLA should be objective measurements.

6.1.1 Service Catalogue

Service Level Management must ensure that a Service Catalogue is produced, maintained and contains accurate information on all operational services and those ready for deployment.

There are two aspects to the Service Catalogue:

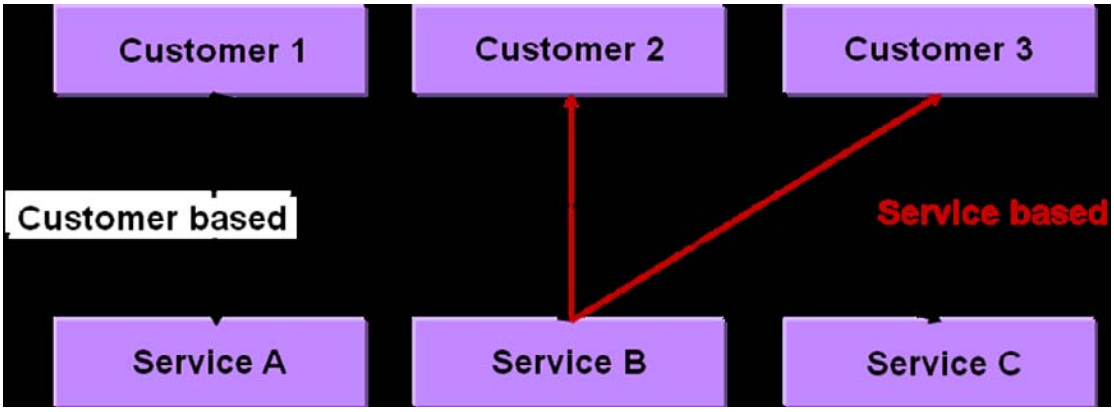


Business Service Catalogue: contains details of all the IT services delivered to the customer, together with relationships to the business units and the business processes that rely on the IT services. This is the customer view of the Service Catalogue.

Technical Service Catalogue: contains details of all the IT service delivered to the customer, together with relationships to the supporting services, shared services, components and Configuration Items necessary to support the provision of the service to the business. This should underpin the Business Service Catalogue and should not form part of the customer view.

6.1.2 Designing SLAs

SLAs can be either Customer or Service based,



Customer based SLA: Separate SLA for each **customer**, covering multiple services. This may be used when individual customers have very different needs and requirements.

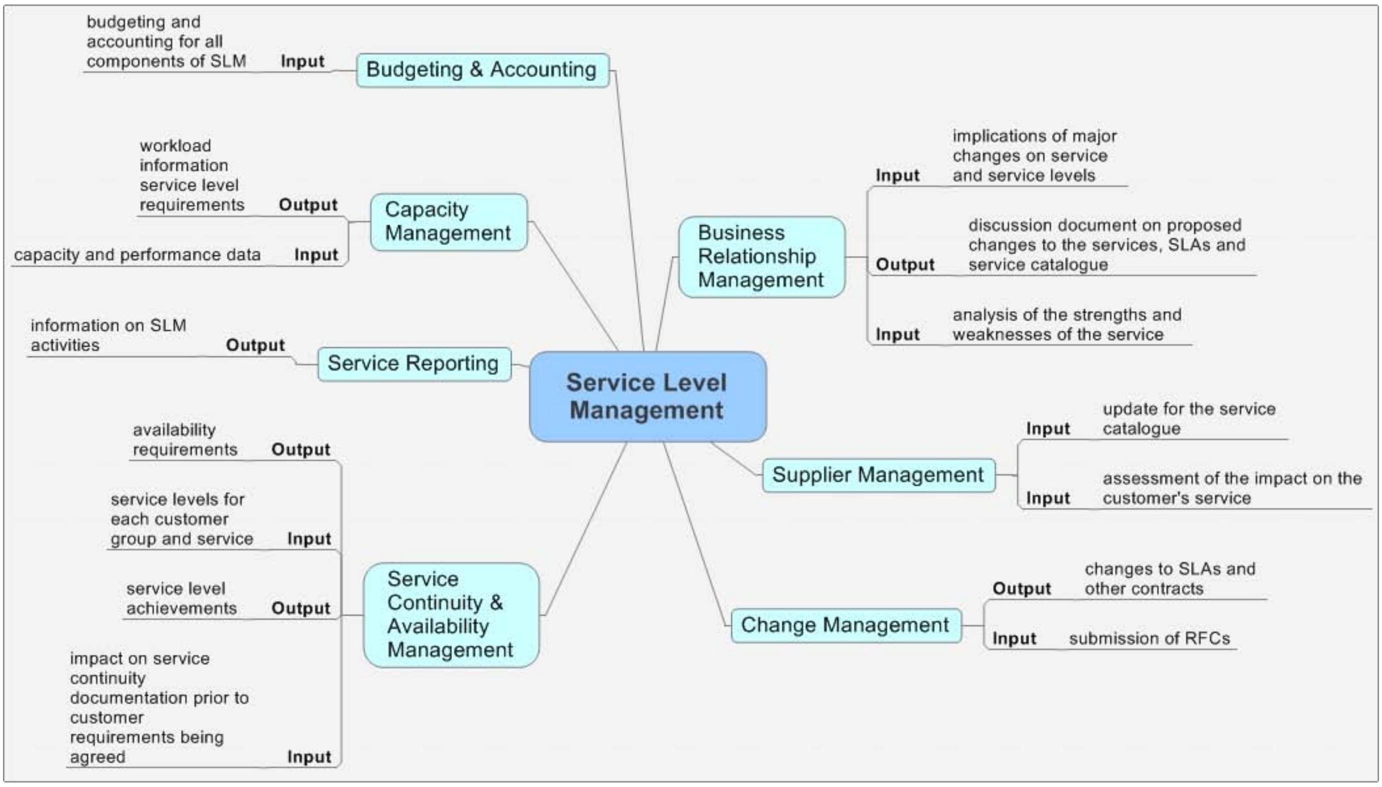
Service based SLA: SLA covers one **service** for all customers of that service. This type of SLA is used when the requirements of the IT service differs little between customers.

Typical contents of SLAs include:

- Introduction
- Service description
- Mutual responsibilities
- Scope
- Service hours
- Service availability
- Reliability
- Customer support
- Contact points & escalation
- Service performance
- Batch turnaround times
- Security
- Charging etc.

It is also common for a combination of SLAs to be used. Information contained within an SLA must be measureable. The language used should always be clear and concise in order to aid understanding. SLAs are not used as legal documents for imposing penalties, otherwise they are in conflict with the goal of improving relationships between customers and the IT Service provider.

6.1.3 Interfaces with Other Processes


Service Level Management
Budgeting & Accounting
Input
budgeting and accounting for all components of SLM
Capacity Management
Output
workload information service level requirements
Input
capacity and performance data
Service Reporting
Output
information on SLM activities
Service Continuity & Availability Management
Output
availability requirements
Input
service levels for each customer group and service
Output
service level achievements
Input
impact on service continuity documentation prior to customer requirements being agreed
Business Relationship Management
Input
implications of major changes on service and service levels
Output
discussion document on proposed changes to the services, SLAs and service catalogue
Input
analysis of the strengths and weaknesses of the service
Supplier Management
Input
update for the service catalogue
Input
assessment of the impact on the customer's service
Change Management
Output
changes to SLAs and other contracts
Input
submission of RFCs

Examples of what Service Level Management *shall* do:

* The full range of services is provided together with the service level targets and workload characteristics. These are agreed and recorded by the parties involved.

* SLAs, together with supporting service agreements, supplier contracts and corresponding procedures are agreed by all relevant parties and recorded. These are maintained by regular reviews to ensure that they are up-to-date and remain effective over time.

Examples of what Service Level Management *should* do:

* A service catalogue defines all services

* Service Level Management manages and coordinates all contributors to the service levels.

* SLAs are formally documented and authorized and supporting services documented and agreed with each supplier.

A complete overview of the requirements of Service Level Management can be found in Chapter 6.1, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.1, Part 2 of the ISO/IEC 20000 standard.

6.1.4 Service Level Management Review Questions

1. What is the objective of Service Level Management?

    a) To define, agree, record and manage levels of service.
    b) To develop effective relationships between customers and the IT organization
    c) To manage all processes within IT Service Management
    d) Design and distribute Service Level Agreements

2. What are the two types of service catalogue?

    a) Business Service Catalogue and Technology Service Catalogue
    b) Business Service Catalogue and Technical Service Catalogue
    c) Business Service Catalogue and Customer Service Catalogue
    d) There is only one type of service catalogue

3. Which of the following is NOT an activity of Service Level Management?

    a) Monitoring service levels
    b) Reporting results
    c) Creating a service catalogue
    d) Identifying the costs of new services

4. Service Level Management *shall*:

    a) Agree and record the full range of services
    b) Ensure all relevant parties agree to all SLAs
    c) Hold regular reviews of all SLAs
    d) All of the above

5. SLAs would NOT include:

    a) Scope
    b) Service availability
    c) Financial trends
    d) Service performance

Answers to all questions can be found in Chapter 12.

6.2 Service Reporting

OBJECTIVE: To produce agreed, timely, reliable and accurate reports for informed decision-making and effective communication.

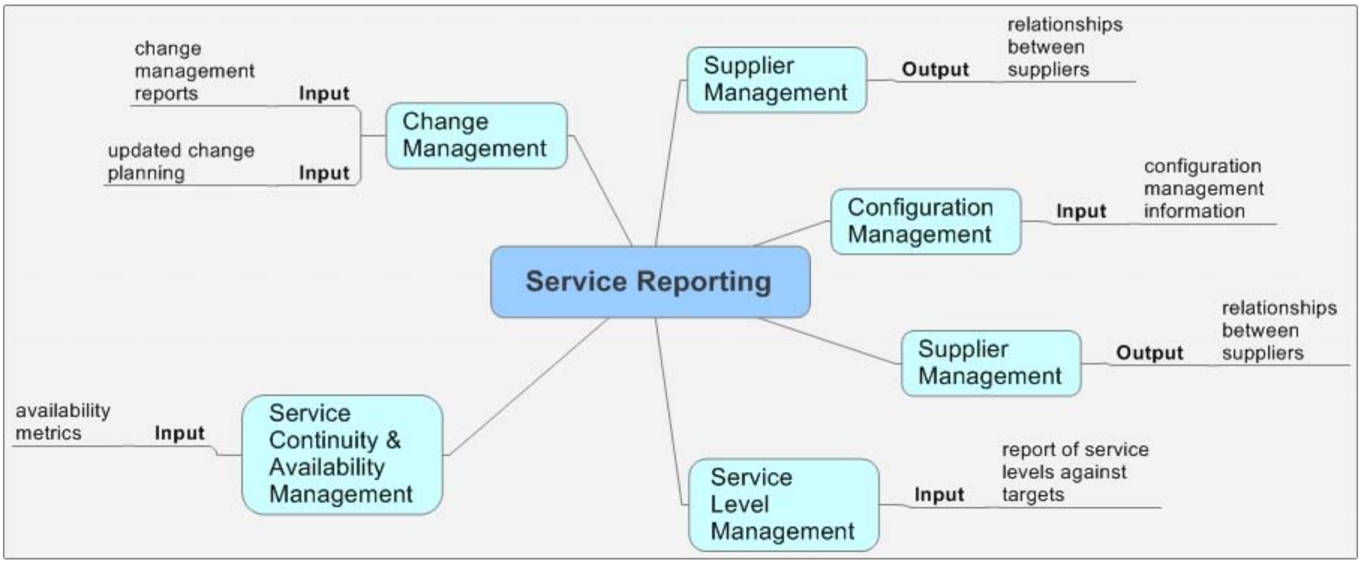
The success of all Service Management processes is dependent on the use of the information provided in service reports. Service Reporting meets the needs and requirements of both internal management and the customer.

It is important that service reports are sufficiently accurate to be used as a decision support tool amongst all processes. The identity, purpose, audience and details of the data source must be clearly outlined for each service report.

Reports to customers (*service reports*) should be provided at the intervals agreed within the SLA. The purpose of these reports is to compare the agreed service levels with the actual service levels measured e.g. availability and downtime, average response time, transaction rates, number of users etc.

Reports to management (*management reports*) are not provided to the customer, but for the purpose of controlling or managing internal processes. They will contain metrics about actual service levels supported and trends such as the number of SLAs concluded, cost of measuring and monitoring, customer satisfaction, progress of improvement etc.

6.2.1 Interfaces with Other Processes


change management reports
Input
updated change planning
Input
Change Management
Supplier Management
Output
relationships between suppliers
Configuration Management
Input
configuration management information
Service Reporting
Supplier Management
Output
relationships between suppliers
availability metrics
Input
Service Continuity & Availability Management
Service Level Management
Input
report of service levels against targets

Examples of what Service Reporting *shall* do:

* A clear description of each service report including its identity, purpose, audience and details of the data source is available.

* Service reports are produced to meet identified needs and customer requirements.

Examples of what Service Reporting *should* do:

* Requirements for service reporting are agreed and recorded for customers and internal management.

* Reports are timely, clear, reliable and concise and of sufficient accuracy to be used as a decision support tool.

A complete overview of the requirements of Service Reporting can be found in Chapter 6.2, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.2, Part 2 of the ISO/IEC 20000 standard.

6.2.2 Service Reporting Review Questions

1. Which of the following is true for service reports?

   a) Service reports show the number of SLAs concluded
   b) Service reports monitor customer satisfaction
   c) Service reports compare agreed service levels with actual service levels measured
   d) Service reports are provided to management

2. Service Reporting receives reports of service levels against targets from which process?

   a) Service Level Management
   b) Supplier Management
   c) Service Continuity & Availability Management
   d) Configuration Management

3. Service Reports would NOT include:

   a) Satisfaction analysis
   b) Trends
   c) Details of all incidents
   d) Performance reporting

4. Which of the following processes depend on Service Reporting?

   a) Change Management
   b) Service Level Management
   c) Budgeting & Accounting
   d) All ITSM processes

5. Service Reporting shall consider:

   a) Target audience
   b) Purpose
   c) Details of data source
   d) All of the above

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

6.3 Service Continuity & Availability Management

OBJECTIVE: To ensure that agreed service continuity and availability commitments to customers can be met in all circumstances.

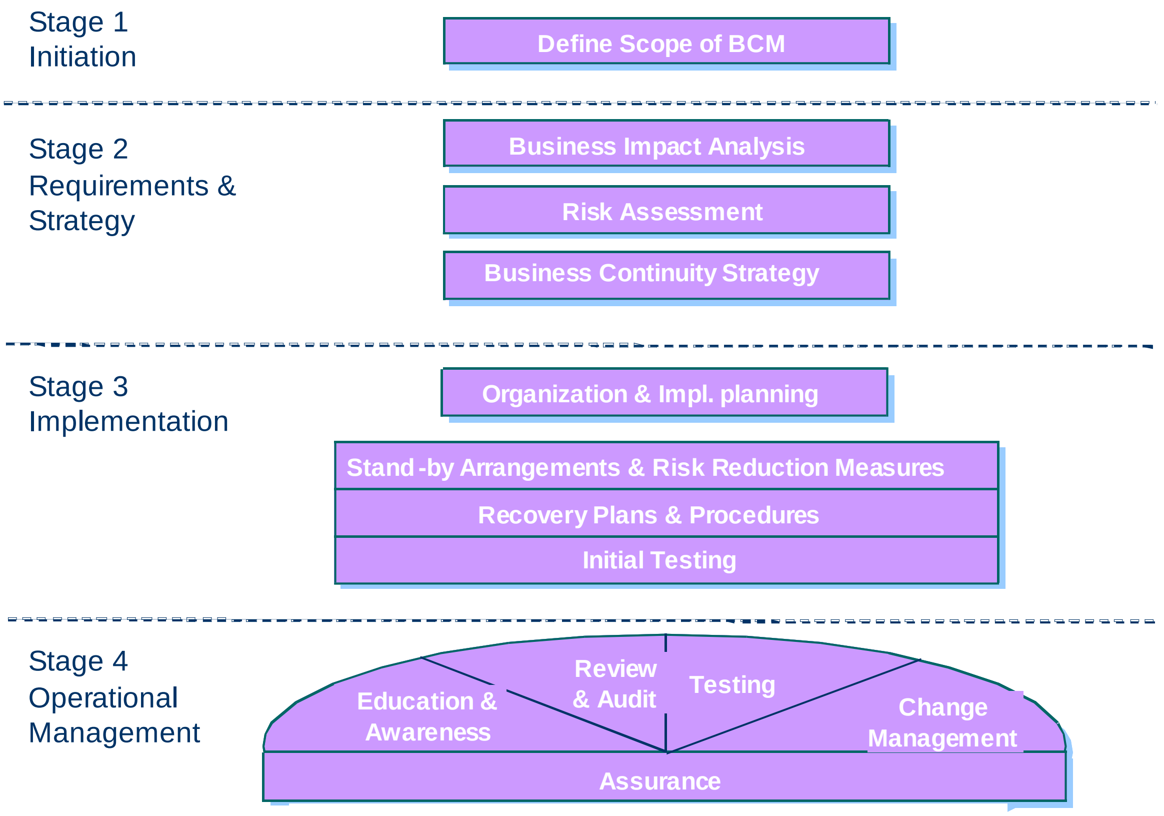
Service continuity and availability management processes contain activities to ensure that systems are made available and will stay that way. According to ITIL, Service Continuity and Availability management are two different, but closely related processes while in ISO/IEC 20000, a combined availability and service continuity management system exists.

Availability Management deals with the day-to-day availability of services whereas Service Continuity Management takes over when a 'disaster' situation occurs and the continuity plan is invoked. For the purpose of ISO/IEC 20000, they are combined as the planning and testing of both service continuity and availability management can be performed as one set of activities. It is important to note, however, that the monitoring and management of activities within each process are to be executed separately.

6.3.1 Activities - Service Continuity Management

IT Service Continuity Management (ITSCM) supports the overall Business Continuity Management (BCM) by ensuring that the required IT infrastructure and the IT service provision can be recovered within required and agreed business time scales. For this reason,

ITSCM is often referred to as 'Disaster Recovery' planning.



The diagram above shows the four stages of ITSCM, incorporating each of the activities that take place to ensure that IT organizations are as prepared and organized as possible in the event of a disaster situation.

Two of the major data sources for ITSCM are developed within Stage 2, including Business Impact Analysis and Risk Assessment.

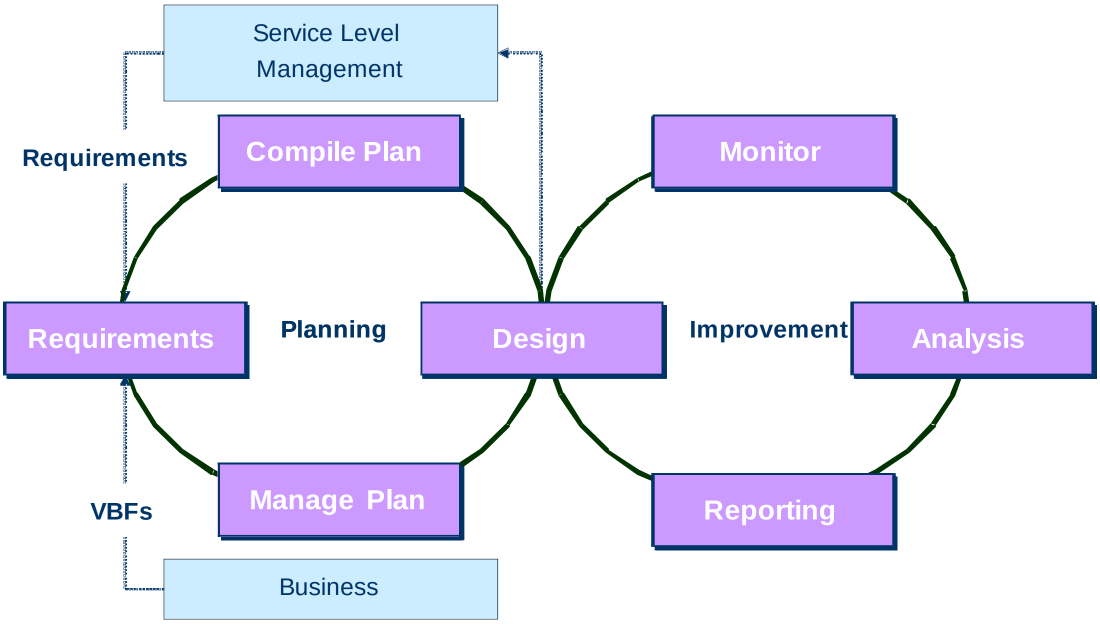
Performing a Business Impact Analysis (BIA) identifies:

- Critical business processes & Vital Business Functions
- Potential damage or loss caused by disruption
- Possible escalations caused by damage or loss
- Necessary resources required to enable continuity of critical business processes
- Time constraints for minimum recovery of facilities and services
- Time constraints for complete recovery of facilities and services

Risk Assessment involves:

- Gathering information on assets (IT infrastructure components),
- Considering the likelihood of Threats from both Internal & external sources occurring
- Vulnerabilities (the extent of impact or effect on organization)

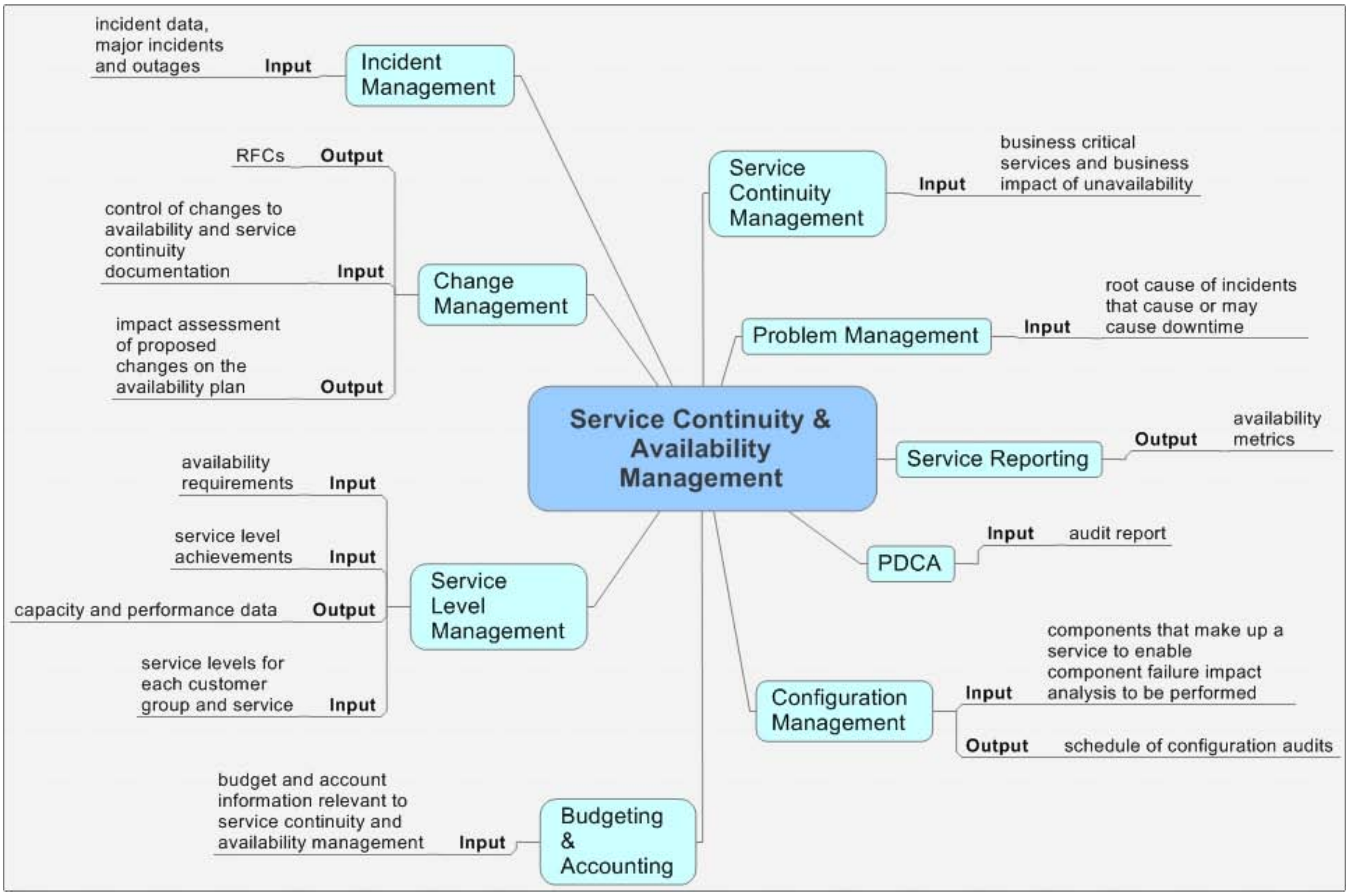
6.3.2 Activities - Availability Management



As shown above, the activities involved in Availability Management can form two continuous cycles of Planning and Improvement. The requirements and Vital Business Functions (VBFs) are input from the business and a plan is developed to meet availability requirements. This then initiates the improvement processes of monitoring, analysis and reporting back to SLM and the business on how well required service levels were met.

Once the availability activities have been completed, access management helps to protect the confidentiality, integrity and availability of all assets. The achievement of that objective must be demonstrated for compliance with the ISO/IEC 20000 standard.

6.3.3 Interfaces with Other Processes


Service Continuity & Availability Management
Incident Management
incident data, major incidents and outages
Input
Change Management
RFCs
Output
control of changes to availability and service continuity documentation
Input
impact assessment of proposed changes on the availability plan
Output
Service Level Management
availability requirements
Input
service level achievements
Input
capacity and performance data
Output
service levels for each customer group and service
Input
Budgeting & Accounting
budget and account information relevant to service continuity and availability management
Input
Service Continuity Management
Input
business critical services and business impact of unavailability
Problem Management
Input
root cause of incidents that cause or may cause downtime
Service Reporting
Output
availability metrics
PDCA
Input
audit report
Configuration Management
Input
components that make up a service to enable component failure impact analysis to be performed
Output
schedule of configuration audits

Examples of what Service Continuity & Availability Management *shall* do:

* Availability and service continuity requirements, including access rights, response times and end-to-end availability of system components, are identified on the basis of business plans, SLAs and risks assessments.

* Availability is measured and recorded. Any unplanned non-availability is investigated and appropriate actions taken.

* The service continuity plan is tested in accordance with business needs and all continuity tests recorded and test failures are formulated into action plans.

Examples of what Service Continuity & Availability Management *should* do:

* Service Continuity & Availability Management requirements is be identified on the basis of the customer's business priorities, service level agreements and assessed risks.

* The Service Continuity Strategy includes risk assessment and defines general approach to meet service continuity obligations.

* Availability Management ensures availability of all components of the service.

A complete overview of the requirements of Service Continuity & Availability Management can be found in Chapter 6.3, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.3, Part 2 of the ISO/IEC 20000 standard.

6.3.4 Service Continuity & Availability Management Review Questions

1. What does performing a BIA identify?

   a) Possible escalations caused by damage or loss
   b) Critical business processes & Vital Business Functions
   c) Necessary resources required to enable continuity of critical business processes
   d) All of the above

2. Which of the following is NOT true about the Service Continuity & Availability Management process

   a) Service continuity management supports overall Business Relationship Management
   b) ITSCM is also known as 'Disaster Recovery'
   c) The monitoring and management of activities within Service Continuity & Availability management must be executed separately
   d) Service Continuity and Availability Management are two separate processes.

3. What role does access management play in Service Continuity & Availability Management?

   a) Performing a Business Impact Analysis
   b) Execution of policies and actions defined in Service Continuity Management
   c) Reporting on service level targets to Service Level Management
   d) Execution of policies and actions defined in Availability Management

4. Risk assessment does not involve which of the following activities:

   a) Gathering information on assets
   b) Considering threats
   c) Day-to-day availability incidents
   d) Vulnerabilities

5. Service Continuity & Availability Management requirements should be identified on the basis of which of the following?

    a) Customer’s business priorities
    b) Service level agreements
    c) Assessed risks
    d) All of the above

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

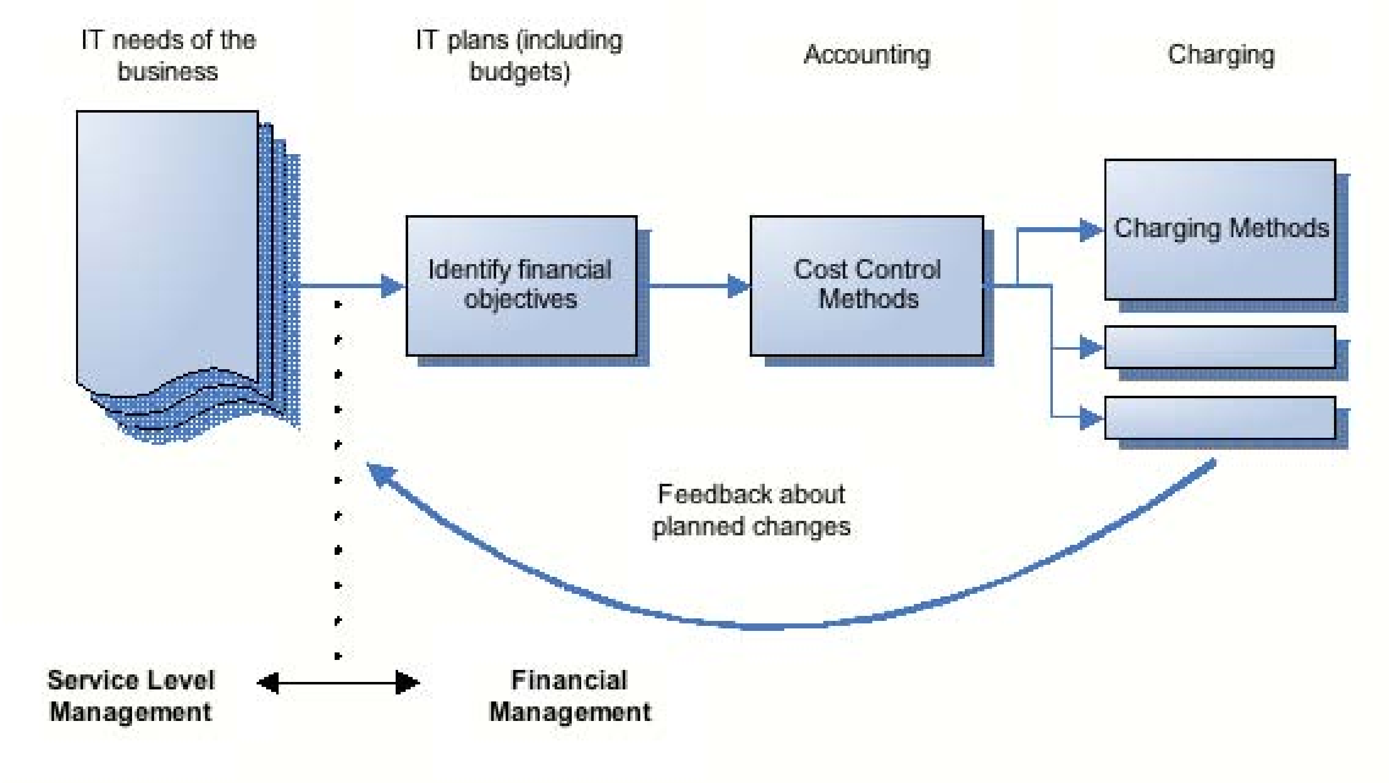
6.4 Budgeting & Accounting for IT Services

OBJECTIVE: To budget and account for the cost of service provision.

Responsibility for many of the financial decisions will lie outside the sphere of the Service Management arena, and the requirements for what financial information is to be provided, in what form and at what frequencies may be dictated from outside.

6.4.1 The Financial Cycle

The following diagram outlines the major processes involved with Budgeting and Accounting:

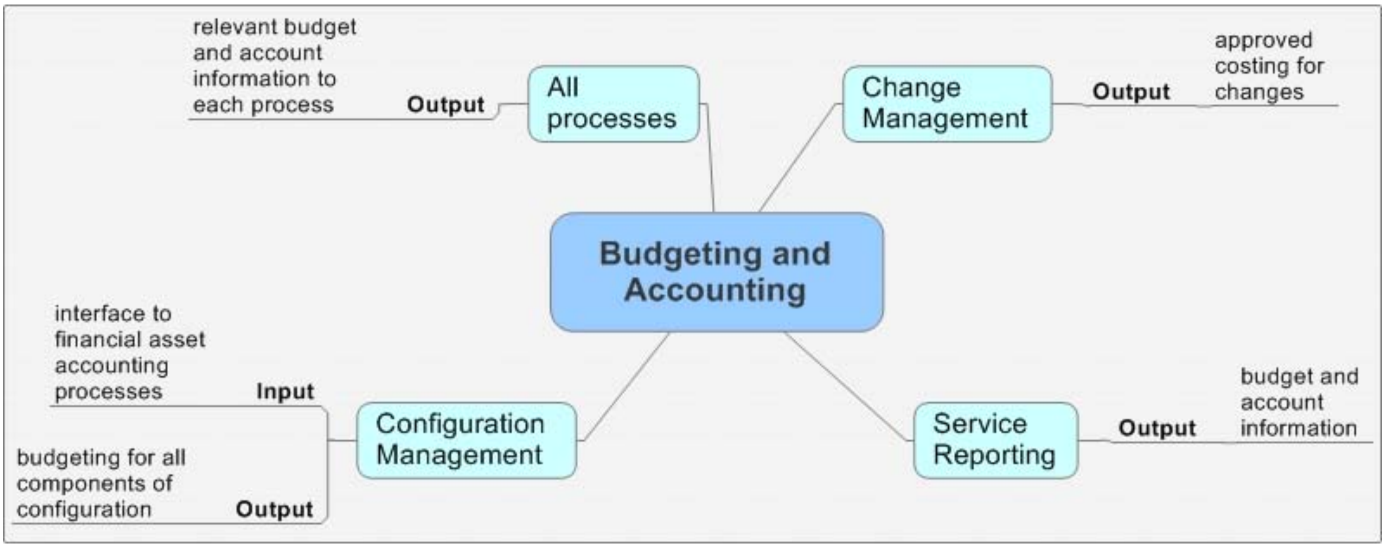


Budgeting is involved with the planning and controlling of activities within the organization. Corporate and strategic planning considers the long-term objectives of a business. Budgeting then defines the financial plans for meeting those objectives during the period covered by the budget (one to five years).

Accounting identifies and understands the costs that IT is responsible for, in order for the IT organization to be run as a business. Costs must always be determined, even when they are not charged to customers.

In practice, many service providers will be involved in charging for IT services. However, as charging is an optional activity, it is not covered by the standard. Service providers are recommended that where charging is in use, the mechanism for doing so is fully defined and understood by all parties.

6.4.2 Interfaces with Other Processes


relevant budget and account information to each process
Output
All processes
Change Management
Output
approved costing for changes
Budgeting and Accounting
interface to financial asset accounting processes
Input
Configuration Management
budgeting for all components of configuration
Output
Service Reporting
Output
budget and account information

Examples of what Budgeting & Accounting *shall* do:

* Clear policies and processes exist for the budgeting and accounting of all components, apportioning indirect costs and allocating direct costs to services, and effective financial control and authorization.

* Costs are budgeted in sufficient detail to enable effective financial control and decision making.

Examples of what Budgeting & Accounting *should* do:

* Budgeting takes into account the planned changes to services during the budget period and, where budgetary requirements exceed available funds, plan for the management of shortfalls.

* All accounting practices used are aligned to the wider accountancy practices of the whole service provider's organization.

* A policy exists on the financial management of services and defines the objectives to be met by budgeting and accounting.

A complete overview of the requirements of Budgeting & Accounting can be found in Chapter 6.4, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.4, Part 2 of the ISO/IEC 20000 standard.

6.4.3 Budgeting & Accounting Review Questions

1. Which of the following activities are covered by the ISO/IEC 20000 standard?

   a) Budgeting, Accounting and Charging
   b) Budgeting and Accounting only
   c) Accounting and Charging only
   d) Charging and Budgeting only

2. Budgeting should:

   a) Account for planned changes to services
   b) Plan for the management of shortfalls
   c) Align with wider accountancy practices
   d) All of the above

3. The objective of Budgeting and Accounting is:

   a) To budget and account for the cost of service provision
   b) To provide cost effective stewardship of the IT assets and the financial resources used in providing IT services
   c) To minimize costing for IT services
   d) To provide financial reporting to the IT organization

4. Which of the following is NOT a requirement in the ISO/IEC 20000 standard?

   a) Budgeting of costs shall be in sufficient detail to enable effective financial control and decision making
   b) Clear policies and processes shall exist for budgeting and accounting
   c) All accounting practices shall be aligned to the wider accountancy practices
   d) Changes to services and costs are approved through the change management process

5. Budgeting & Accounting has interfaces with which processes?

   a) Change Management, Service Reporting and Configuration Management
   b) All service management processes
   c) Change Management and Configuration Management only
   d) Service Level Management, Service Reporting and Configuration Management

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

6.5 Capacity Management

OBJECTIVE: To ensure that the service provider has, at all times, sufficient capacity to meet the current and future needs of the customer's business needs.

With planning and predictions core to the requirements of ISO/IEC 20000, the Capacity Management process is fundamentally proactive.

The Capacity Management process needs to be the focal point for all performance and capacity issues in order to achieve ISO/IEC 20000. The standard does not limit these requirements to the activities of technical specialists responsible for the capacity and performance of technical components but rather requires capacity and performance to be planned and managed for all resources that contribute to the service and to service management.

6.5.1 Sub processes of Capacity Management

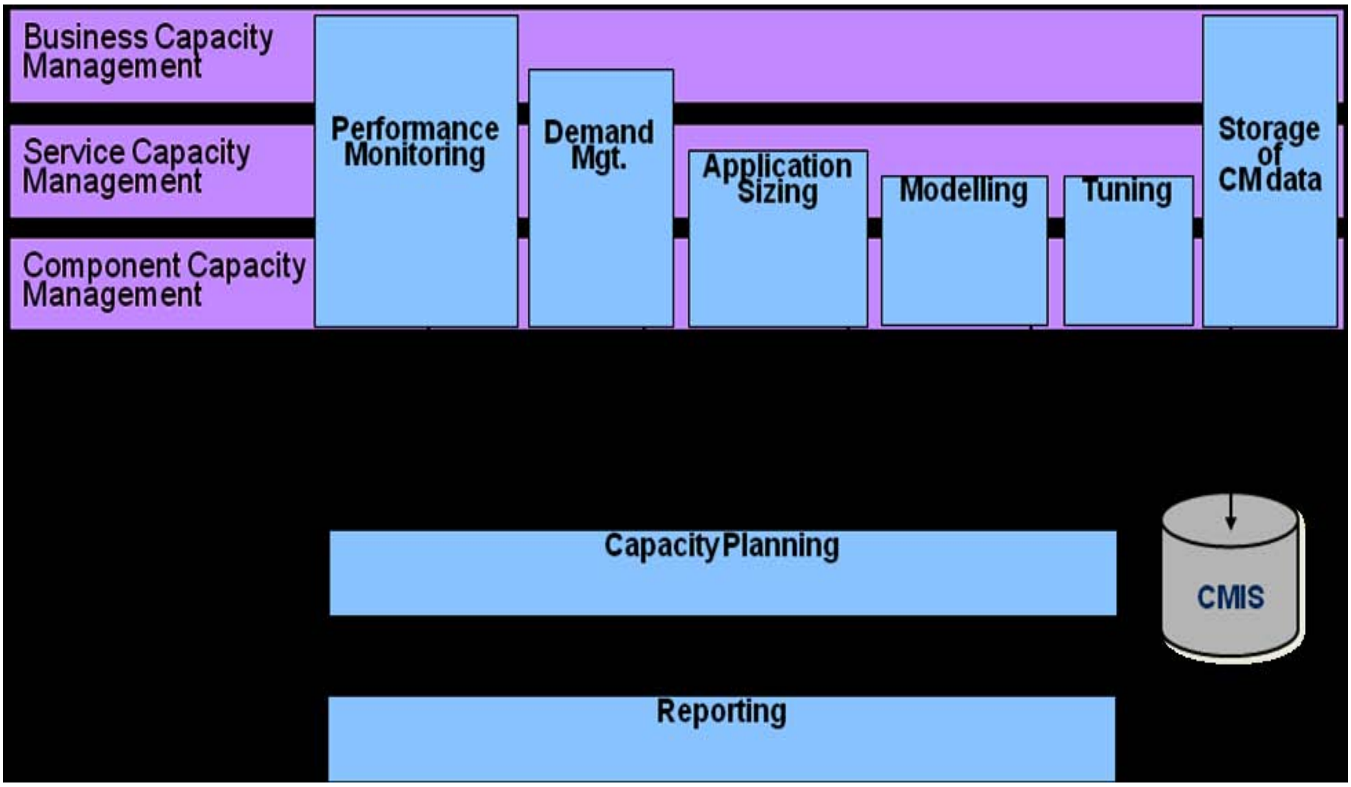
Business Capacity Management – understands the current and future business needs. Through trend analysis, strategic or marketing plans and information from customers, business capacity management plans and implements sufficient capacity in appropriate timescales. This process is primarily proactive.

Service Capacity Management – determines and understands the use of IT services. In order to ensure that appropriate service agreements can be made and delivered, the performance and peak loads need to be understood. Service capacity management establishes baselines and profiles of use for all services and has strong links with service level management in terms of the definition and negotiation of service agreements.

Resource Capacity Management – determines and understands the use of the IT infrastructure and components. Potential problems must be detected early in order to manage resources effectively such as CPU, memory, disks, network bandwidth.

All three components of Capacity Management collate their data and report to Service Level Management and Budgeting & Accounting.

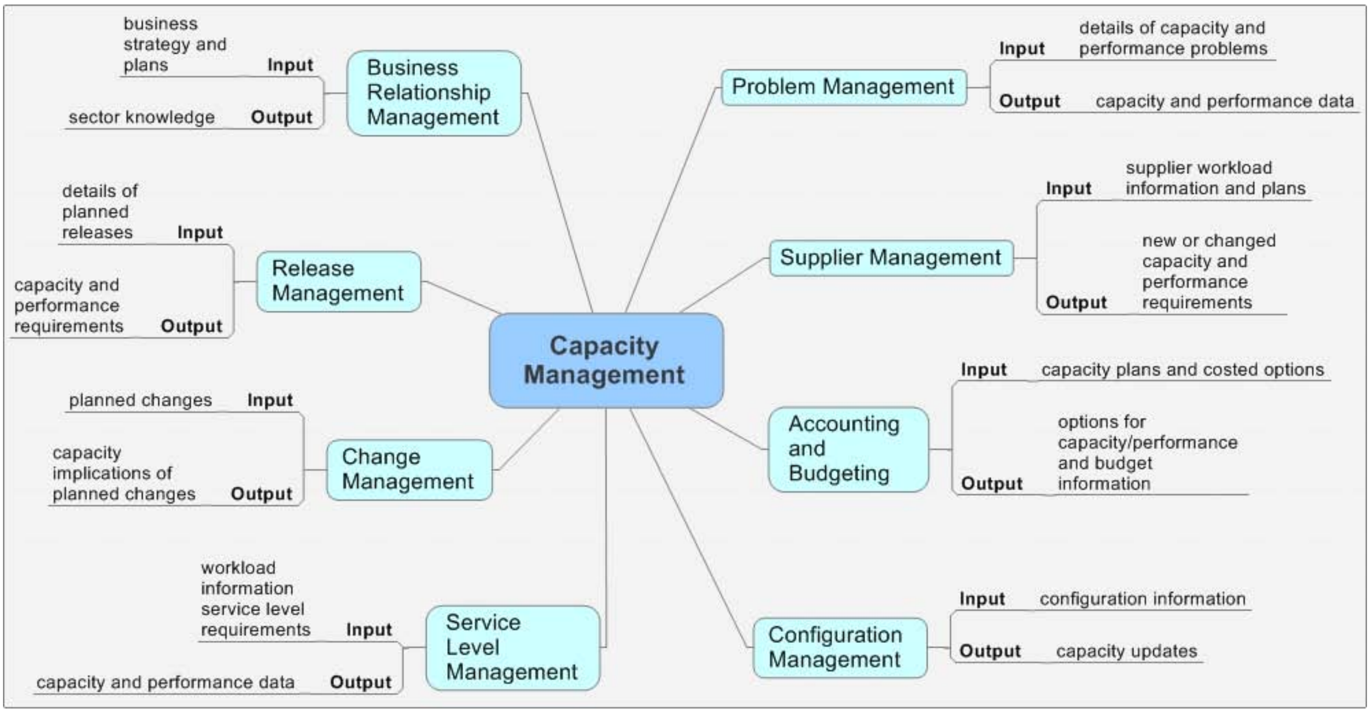
6.5.2 Activities



Capacity Management consists of these main activities:

1. P**erformance Monitoring -** Measuring, monitoring, analyzing and implementing theperformance of *IT Infrastructure components.*
2. **Demand Management -** Aims to influence the demand on capacity.
3. **Application Sizing -** Determining the hardware or network capacity to support new or modified applications and the predicted workload
4. **Modeling** – a proactive activity that can be used to forecast the behavior of the infrastructure and identify areas that could be better utilized.
5. **Tuning** – This activity is the process of making modifications to better utilized identified areas of the current infrastructure
6. **Storage of Capacity Management Data**
7. Capacity Planning
8. Reporting

6.5.3 Interfaces with Other Processes


Capacity Management
Business Relationship Management
business strategy and plans
Input
sector knowledge
Output
Release Management
details of planned releases
Input
capacity and performance requirements
Output
Change Management
planned changes
Input
capacity implications of planned changes
Output
Service Level Management
workload information service level requirements
Input
capacity and performance data
Output
Problem Management
Input
details of capacity and performance problems
Output
capacity and performance data
Supplier Management
Input
supplier workload information and plans
Output
new or changed capacity and performance requirements
Accounting and Budgeting
Input
capacity plans and costed options
Output
options for capacity/performance and budget information
Configuration Management
Input
configuration information
Output
capacity updates

Examples of what Capacity Management *shall* do:

* A capacity plan is produced and maintained.

* Methods, procedures and techniques are identified to monitor service capacity, tune service performance and provide adequate capacity.

* Business needs are addressed, including current and predicted capacity and performance requirements, identified time-scales, thresholds and service upgrade costs, evaluation of affects of anticipated service upgrades, predicted impact of external changes and data and processes to enable predictive analysis.

Examples of what Capacity Management *should* do:

* The capacity plan is produced at least annually and documents costed options for meeting the business requirements and recommend solutions to ensure achievement of the agreed service level targets as defined in the SLA.

* Capacity Management provides direct support to the development of new and changed services.

A complete overview of the requirements of Capacity Management can be found in Chapter 6.5, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.5, Part 2 of the ISO/IEC 20000 standard.

6.5.4 Capacity Management Review Questions

1. What are the three sub-processes of Capacity Management?

   a) Business Capacity Management, Service Capacity Management and Resources Capacity Management
   b) Service Capacity Management, Resource Capacity Management, Performance Capacity Management
   c) Resource Capacity Management, Performance Capacity Management, Business Capacity Management
   d) Business Capacity Management, Service Capacity Management, Performance Capacity Management

2. Which of the following is NOT an activity within Capacity Management

   a) Performance monitoring
   b) Demand management
   c) Budgeting
   d) Tuning

3. Capacity Management receives workload information on service level requirements from which process?

   a) Change Management
   b) Business Relationship Management
   c) Service Level Management
   d) Configuration Management

4. The business needs addressed by Capacity Management shall include:

   a) Identified time-scales
   b) Thresholds and service upgrade costs
   c) Current and predicted capacity and performance requirements
   d) All of the above

5. Capacity plans should be produced:

   a) Bi-monthly
   b) At least annually
   c) Monthly
   d) Every six months

Answers to all questions can be found in Chapter 12.

6.6 Information Security Management

OBJECTIVES: To manage information security effectively within all service providers.

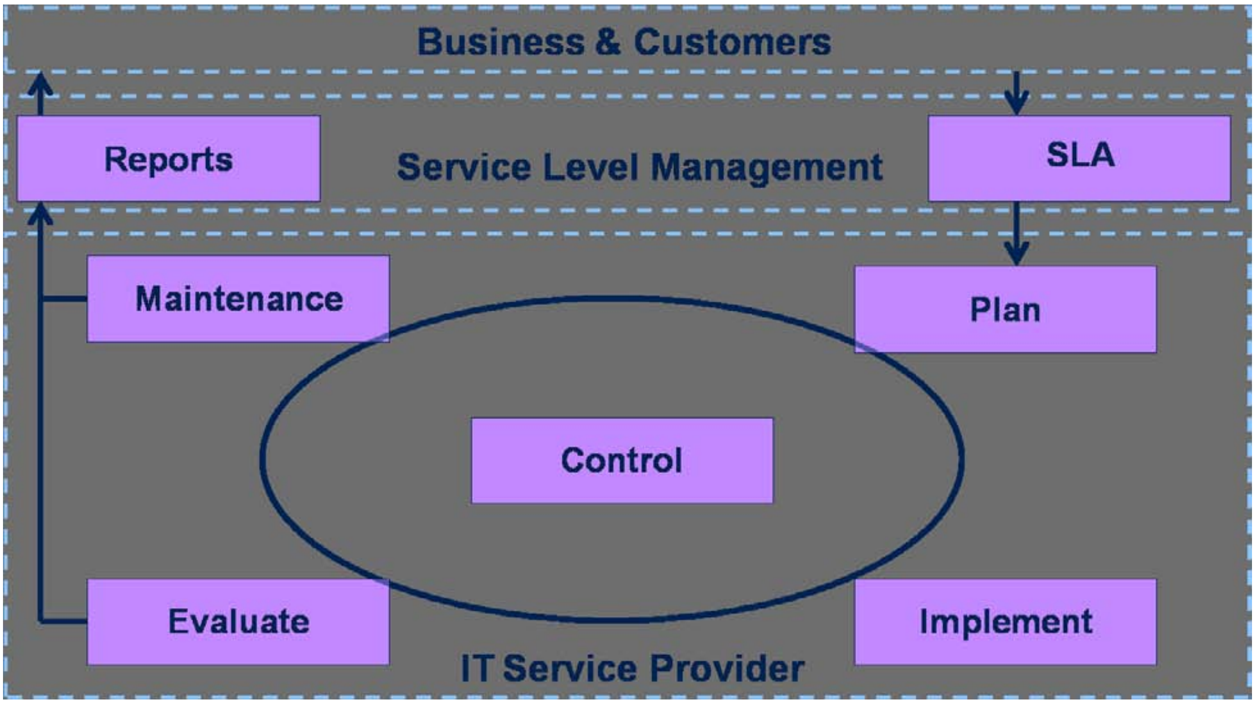
Information Security is a system of policies and procedures designed to identify, control and protect information and any equipment used in connection with its storage, transmission and processing.

In order to ensure that the confidentiality, integrity and availability of an organization's assets, information, data and IT services are maintained, Information Security Management must consider the following four perspectives:

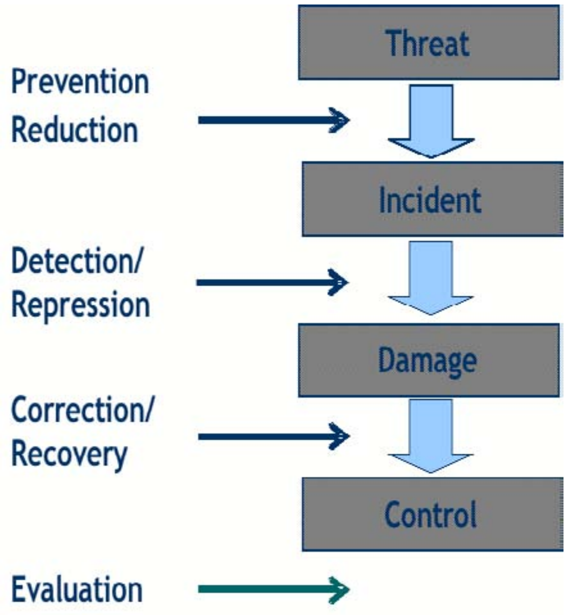
- Organizational
- Procedural
- Physical
- Technical

6.6.1 Information Security Management Activities

The diagram below shows the triggers for Information Security Management activities, from business and customer requirements are recorded in the SLAs. This initiates the security plan which is then assessed and evaluated. Any relevant maintenance or identified improvements will be carried out and a report handed back to Service Level Management to be discussed with the customer during Service Level meetings.



As shown on the previous page, control plays a pivotal role in Information Security Management as this is where Information Security is actually enforced. The process of control is examined below:



There are various security threats to our infrastructure and we want to prevent or reduce the damage of these as much as possible.

In the case that they do pass our prevention mechanisms, we need to have detection techniques to identify when and where they occurred.

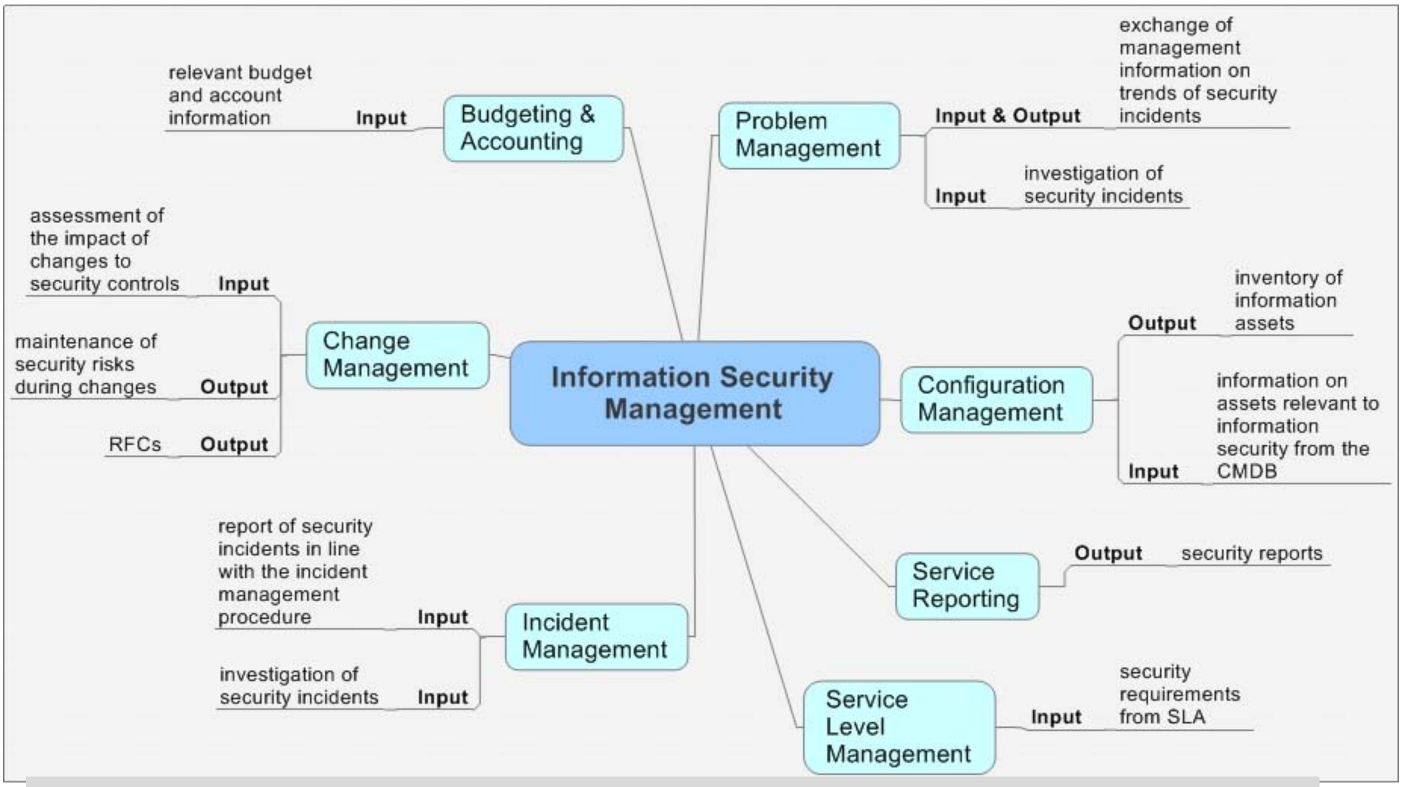
Once a security incident has occurred, we want to repress or minimize the damage associated with this incident.

We then want to correct any damage caused and recover our infrastructure to normal levels.

After this process we need to review how and why the breach occurred and how successful were we in responding to the breach.

Security measures do not need to be re-audited for ISO/IEC 20000 when ISO 27001 has already been achieved.

6.6.2 Interfaces with Other Processes


Information Security Management
Budgeting & Accounting
Input
relevant budget and account information
Problem Management
Input & Output
exchange of management information on trends of security incidents
Input
investigation of security incidents
Change Management
Input
assessment of the impact of changes to security controls
Output
maintenance of security risks during changes
Output
RFCs
Configuration Management
Output
inventory of information assets
Input
information on assets relevant to information security from the CMDB
Service Reporting
Output
security reports
Incident Management
Input
report of security incidents in line with the incident management procedure
Input
investigation of security incidents
Service Level Management
Input
security requirements from SLA

Examples of what Information Security management *shall* do:

- Management with appropriate authority approves an information security policy that is communicated to all relevant personnel and customers where appropriate.

- Security controls are documented and describe the risks to which the controls relate, and the manner of operation and maintenance of controls.

- All security incidents are reported and recorded in line with Incident Management.

- The impact of changes on control is assessed before changes are implemented.

Examples of what Information Security Management *should* do:

* The service provider's staff with specialist information security roles are conversant with ISO/IEC 17799.

* The service provider maintains an inventory of the information assets that are necessary to deliver services and classify each asset according to its criticality to the service, the level of protection it requires and nominate an owner to be accountable for providing that protection.

A complete overview of the requirements of Information Security Management can be found in Chapter 6.6, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 6.6, Part 2 of the ISO/IEC 20000 standard.

Please refer to module 9 in the online learning program for further information on service delivery processes.

6.6.3 Information Security Management Review Questions

1. What perspectives must be considered within Information Security Management?

   a) Organizational, procedural, physical and technical
   b) Procedural, physical, technical and financial
   c) Technical, financial, organizational, procedural
   d) Financial, organizational, procedural, physical

2. What of the following arrangements are based on formal agreement that defines all necessary security requirements?

   a) Internal
   b) External
   c) SLAs
   d) All of the above

3. Which of the following is NOT a requirement of Information Security Management?

   a) Security controls are documented
   b) Security incidents are reported and recorded in line with Incident Management
   c) All staff with specialist information security roles are conversant with ISO/IEC 17799
   d) The impact of changes on control is assessed before changes are implemented

4. Which of the following would assess the impact of a change to a service?

   a) Change Management
   b) Availability Management
   c) Security Management
   d) Service Continuity Management

5. What is the process of security control?

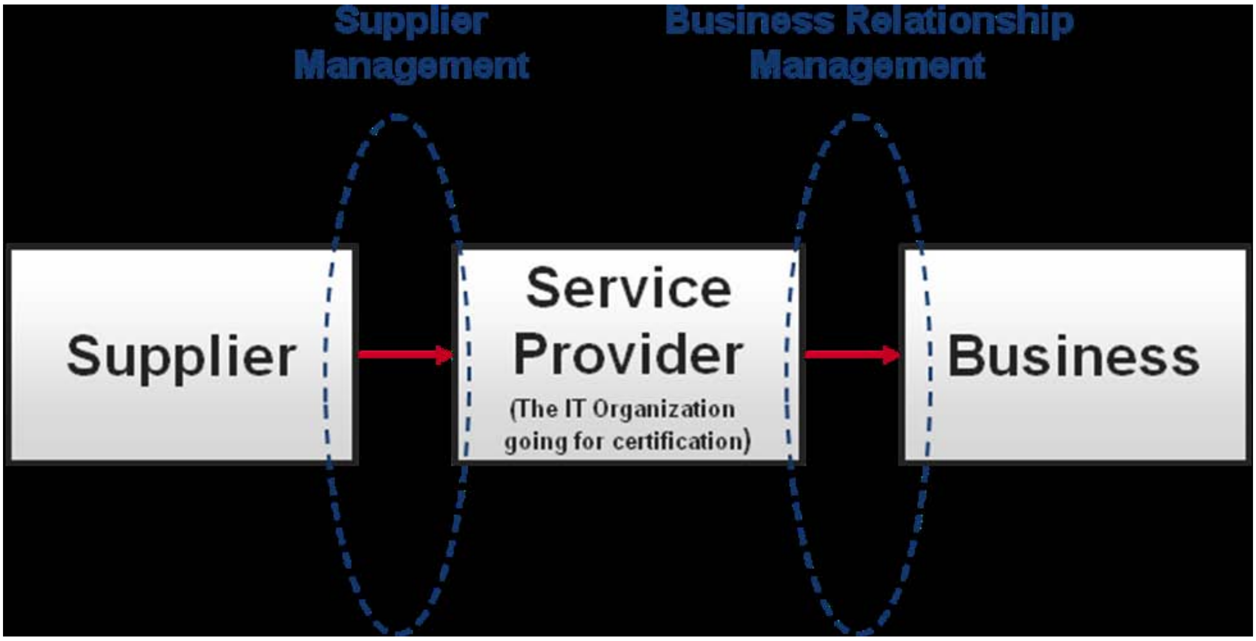
   a) Threat – Incident – Damage - Control
   b) Incident – Threat – Damage - Control
   c) Damage – Incident – Threat - Control
   d) Control – Threat – Incident – Damage

Answers to all questions can be found in Chapter 12.

This page intentionally
left blank.

7 Relationship Processes

There are two relationship processes outlined in the ISO/IEC 20000 standard. Supplier management deals directly with suppliers and the Service Provider while Business Relationship Management deals with the Service Provider and the business.


Supplier Management
Business Relationship Management
Supplier
Service Provider
(The IT Organization going for certification)
Business

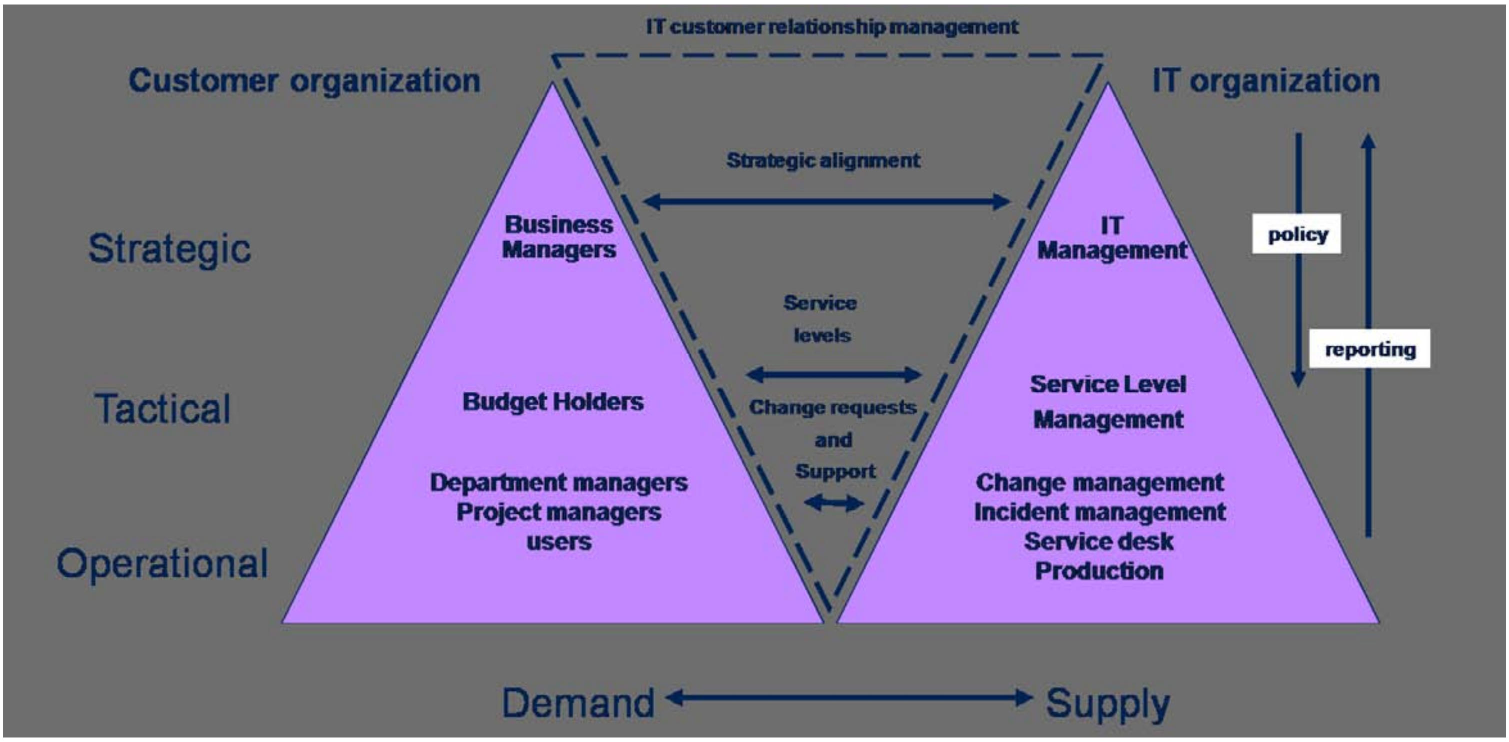
7.1 Business Relationship Management

OBJECTIVE: To establish and maintain a good relationship between the service provider and the customer based on understanding the customer and their business drivers.

The challenge of business relationship management is to ensure that there are effective relationships between the IT organization and the customer organization at all levels. This allows the IT organization to stay in touch with the customer and explore the options for linking the strategic objectives of both organizations.

The requirements of Business Relationship Management can be summarized as follows:

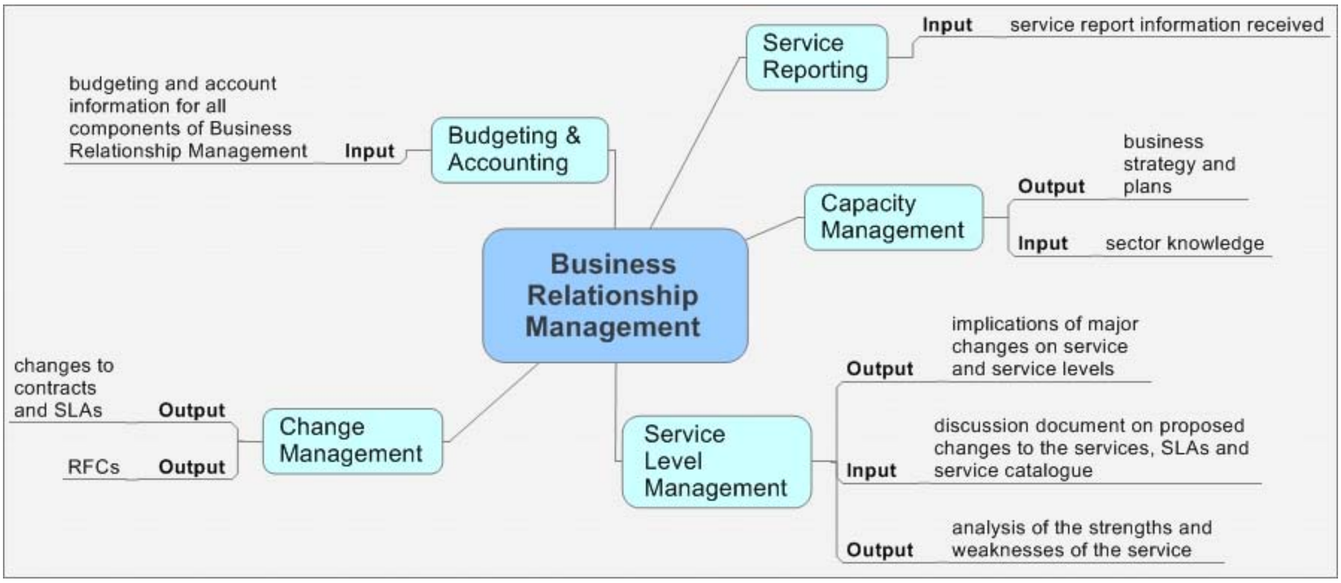
- Understanding the customer's organization, including both customers and stakeholders in order to develop a good relationship
- Understanding and discussing the business, plans and changes to the business or service needs with the customer
- Ensuring effective management of the contract or similar formal documented agreement
- Providing input to the service level management process on changes to business activity and services requiring changes to the SLAs
- Ensuring complaints are handled effectively
- Ensuring customer satisfaction is measured and managed and that a named individual is responsible
- Input provided to a plan for improving the service.



This diagram demonstrates the three levels of participation required to align the business and IT organization: Strategic, Tactical and Operational.

Supplier management deals with the relationship between the IT organization and sub-contractors. Supplier management ensures all underpinning contracts that are in place to support the SLAs agreed with customers are fulfilled in a qualitative and cost effective manner.

7.1.1 Interfaces with Other Processes


Business Relationship Management
Service Reporting
Input
service report information received
Budgeting & Accounting
Input
budgeting and account information for all components of Business Relationship Management
Capacity Management
Output
business strategy and plans
Input
sector knowledge
Change Management
Output
changes to contracts and SLAs
Output
RFCs
Service Level Management
Output
implications of major changes on service and service levels
Input
discussion document on proposed changes to the services, SLAs and service catalogue
Output
analysis of the strengths and weaknesses of the service

Examples of what Business Relationship Management *shall* do:

* The service provider identifies and documents the stakeholders and customers of the services.

* Any changes to contracts and SLAs that follow from these meetings are subject to the change management process.

* The service provider remains of aware of business needs and major changes in order to respond to those needs.

Examples of what Business Relationship Management *should* do:

* The service provider establishes a relationship with their customer, such that they would expect to be aware of business needs and major changes and able to prepare to respond to that need.

* Service providers periodically analyze the record of complaints to identify trends and report this analysis to customers.

* All compliments about the service are documented and reported to the service delivery team.

A complete overview of the requirements of Business Relationship Management can be found in Chapter 7.2, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 7.2, Part 2 of the ISO/IEC 20000 standard.

7.1.2 Business Relationship Management Review Questions

6. Any changes to contracts that follow meetings between the service provider and the customer are subject to which process?

   e) Service Level Management
   f) Business Relationship Management
   g) Configuration Management
   h) Change Management

7. The level of strategic alignment between IT and the business consists of:

   e) Business managers and IT managers
   f) Budget holders and Service Level Management
   g) Project Managers and Service Desk
   h) All of the above

8. What are the two relationship processes?

   e) Supplier Management and Business Relationship Management
   f) Supplier Management and Service Level Management
   g) Service Level Management and Business Relationship Management
   h) Business Relationship Management and Service Reporting

9. Which of the following is the objective of Business Relationship Management?

   a) To establish and maintain a good relationship between the service provider and the customer based on understanding the customer and their business drivers
   b) To manage suppliers to ensure the provision of seamless, quality services
   c) To define, agree, record and manage levels of service
   d) To manage information security effectively within all service providers

10. Service providers shall hold regular meetings to discuss which of the following?

    e) Service Level Agreements
    f) Contract of business needs
    g) Changes to service scope
    h) All of the above

Answers to all questions can be found in Chapter 12.

7.2 *Supplier Management*

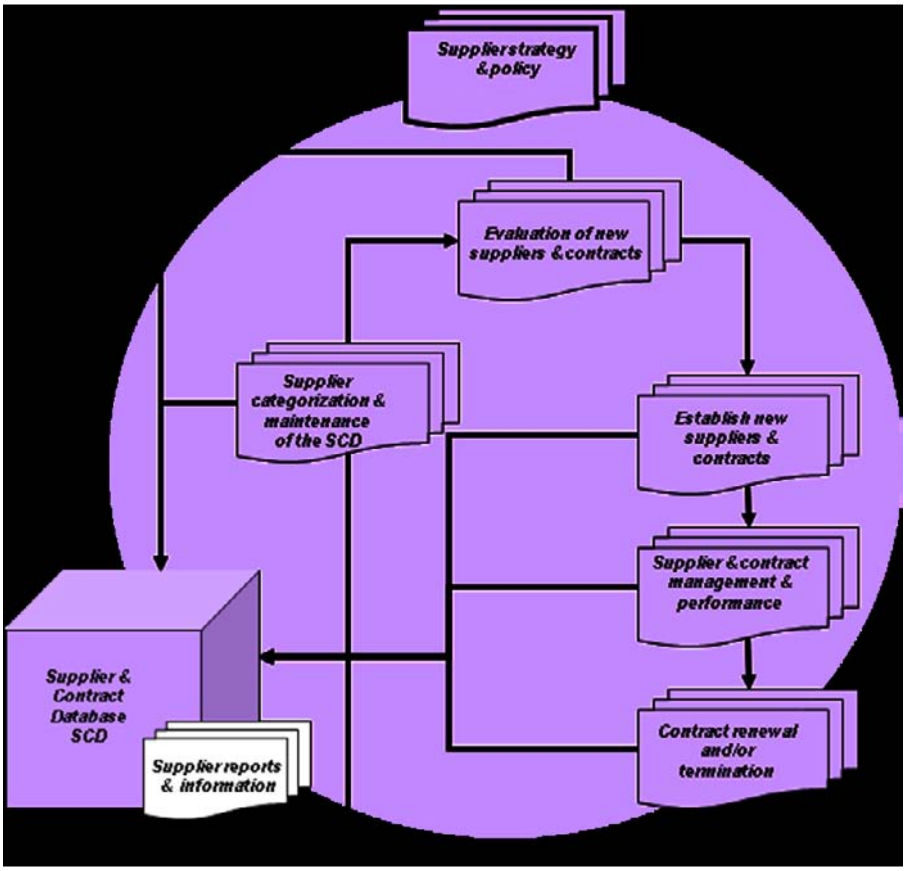
OBJECTIVE: To manage suppliers to ensure the provision of seamless, quality services.

Typical organizations will have many suppliers, most of which will provide service or products that the business uses as a commodity, supporting the business value chain, but under the control of the customer. Types of suppliers and their associated contracts will have a decisive impact on the organizational set-up and the whole SLA framework.

The relationships between suppliers, outsourcers, partners and organizations should always be underpinned by a contract, service level agreement or operational level agreement for internal suppliers.

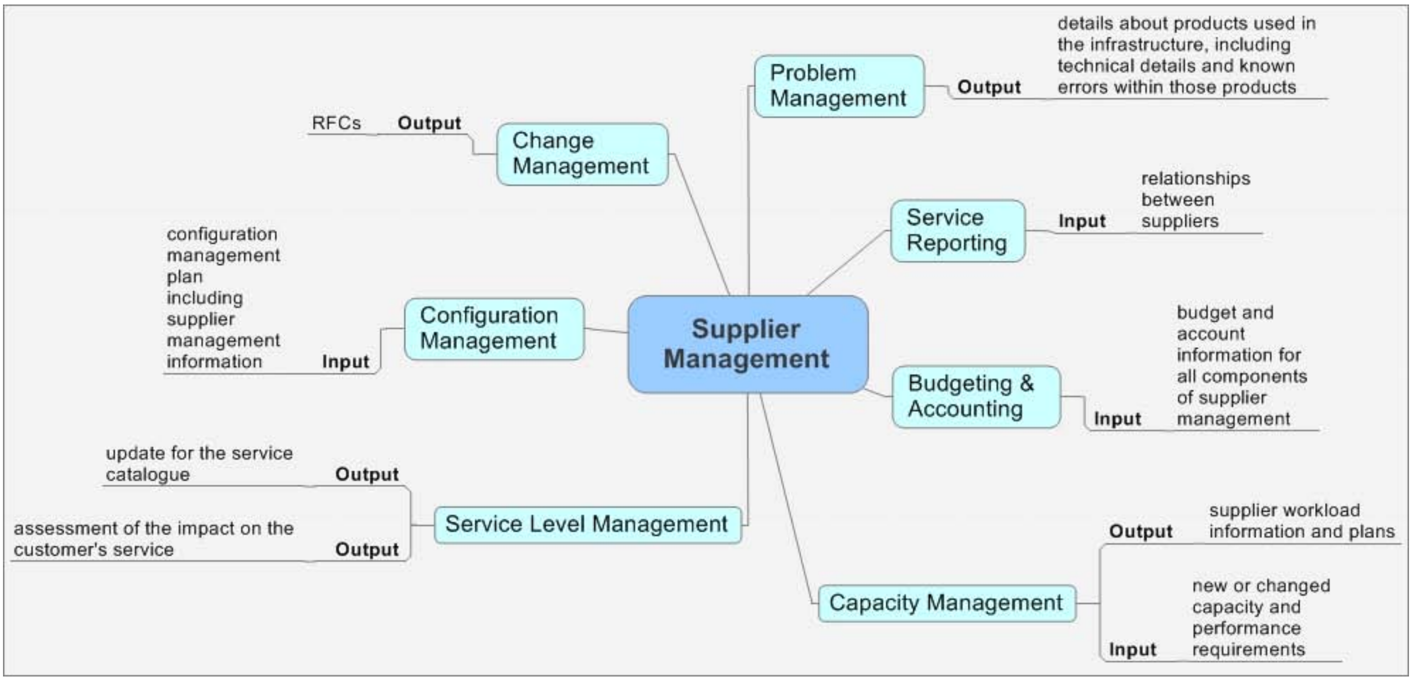
7.2.1 Supplier and Contract Database (SCD)

All Supplier Management process activities, as shown in the diagram below, should be driven by supplier strategy and policy. In order to achieve consistency and effectiveness in the implementation of the policy, a Supplier and Contract Database (SCD) should be established.


Supplier strategy & policy
Evaluation of new suppliers & contracts
Supplier categorization & maintenance of the SCD
Establish new suppliers & contracts
Supplier & contract management & performance
Contract renewal and/or termination
Supplier & Contract Database SCD
Supplier reports & information

Ideally the SCD should form an integrated element of a comprehensive CMS (Configuration Management System) or SKMS (Service Knowledge Management System), recording all supplier and contract details, together with the types of service, products etc provided by each supplier, and all the other information and relationships with other associated CIs(Configuration Items).

7.2.2 Interfaces with Other Processes


Supplier Management
Problem Management
Output
details about products used in the infrastructure, including technical details and known errors within those products
Change Management
RFCs
Output
Service Reporting
Input
relationships between suppliers
Configuration Management
configuration management plan including supplier management information
Input
Budgeting & Accounting
Input
budget and account information for all components of supplier management
Service Level Management
update for the service catalogue
Output
assessment of the impact on the customer's service
Output
Capacity Management
Output
supplier workload information and plans
Input
new or changed capacity and performance requirements

Examples of what Supplier Management *shall* do:

*	The service provider documents the supplier management processes and names a contract manager responsible for each supplier.

*	The requirements, scope, level of service and communication processes to be provided by the supplier are documented in SLAs or other documents and agreed by all parties.

*	Relationships and roles between lead and subcontracted suppliers are clearly documented and lead suppliers are able to demonstrate processes to ensure that subcontracted suppliers meet contractual requirements.

*	Review meetings are held at least annually for all contracts and formal agreements.

Examples of what Supplier Management *should* do:

* The service provider appoints a manager responsible for contracts and agreements with all suppliers.

* All supplier contracts contain a review schedule to assess whether the business objectives for sourcing a service remain valid.

* The lead supplier records the names, responsibilities and relationships with all sub-contracted suppliers and makes this available to the service provider if required.

A complete overview of the requirements of Supplier Management can be found in Chapter 7.3, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 7.3, Part 2 of the ISO/IEC 20000 standard.

Please refer to module 10 in the online learning program for further information on relationship processes.

7.2.3 Supplier Management Review Questions

1. How often shall contract renewal meetings be held?

   a) At least annually
   b) Bi-annually
   c) At the end of supplier contracts and before re-negotiation or termination
   d) As required

2. True or false?

   A service provider names a contract manager responsible for each supplier.

   T F

3. Which of the following is documented in SLAs for Supplier Management?

   a) Levels of service
   b) Scope
   c) Communication processes
   d) All of the above

4. The supplier management contract database should ideally form part of an overarching:

   a) SKMS
   b) CMDB
   c) SLM
   d) SLA

5. Which of the following is the objective of supplier management?

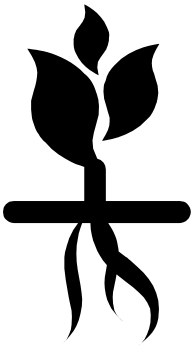
   a) To manage suppliers to ensure the provision of seamless, quality services
   b) To define, agree, record and manage levels of service
   c) To define and control the components of the service and infrastructure and maintain accurate configuration information
   d) To deliver, distribute and track one or more changes in a release into the live environment

Answers to all questions can be found in Chapter 12.

8 Resolution Processes

8.1 What is the difference between an Incident and a Problem?

A simple explanation of the difference between an Incident and a Problem is to think of a weed in a garden.



Describing the weed as an Incident: The weed is a nuisance and the gardener needs a 'quick fix' to remove it. The gardener may cut, rip, out or mow over the top of this weed to hide it from soil level. For the moment, the weed has gone, however it will grow back in time.

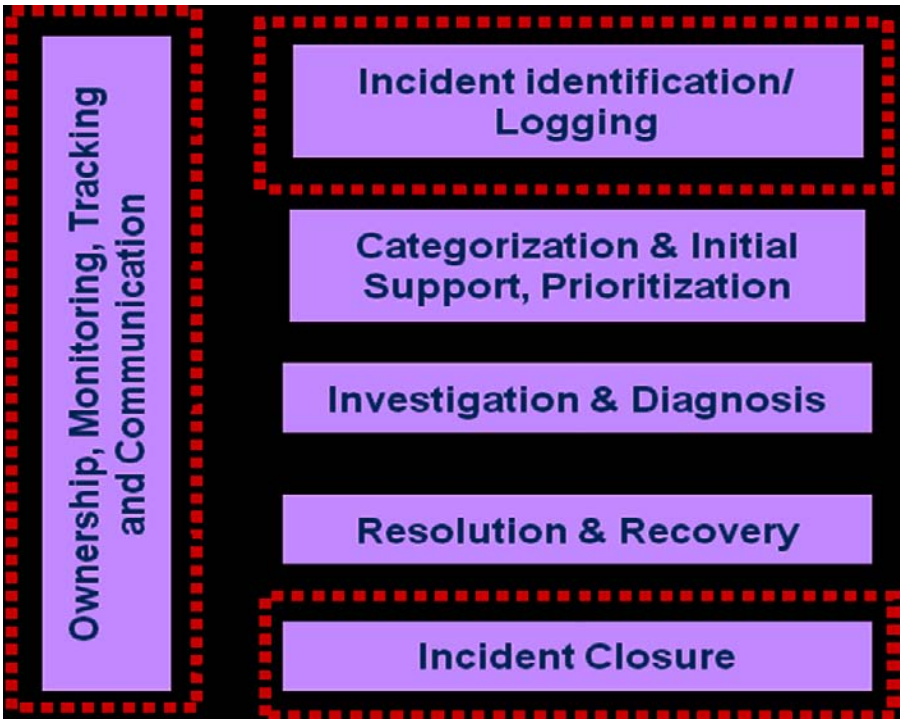
Describing the weed as a Problem: The weed must be removed so that it will never grow back. The gardener may poison, dig out, re-lawn, burn or concrete over the weed to ensure that it will not be a recurring issue.

8.2 Incident Management

OBJECTIVE: To restore agreed service to the business as soon as possible or to respond to service requests.

The incident management process may be delivered by a service desk, which acts as the day-to-day contact with users. This should be both a proactive and reactive process, responding to incidents that affect, or potentially could affect the service. Incident Management is concerned with the restoration of the customer's service; however it does not determine the cause. Here, incident management links closely with problem management.

8.2.1 Activities


Ownership, Monitoring, Tracking and Communication
Incident identification/ Logging
Categorization & Initial Support, Prioritization
Investigation & Diagnosis
Resolution & Recovery
Incident Closure

Ownership, Monitoring, Tracking & Communication

- Service Desk OWNS / is accountable for ALL Incidents
- Monitor progress, escalation of Incidents,
- Advise user and IT management

Incident identification and Logging

- Update/confirm Incident and user details

Categorization, Prioritization (Most critical activity), Initial Support

- Categorize so the exact type of call is recorded e.g. Desktop, Network, Email incident
- Assess urgency and impact to assign priority
- Match against existing Problems/Known Errors
- Match multiple Incidents and create new Problem record.
- Prioritization –taking into account the impact and urgency (how quickly an incident needs a resolution).

Investigation and Diagnosis

- Assess the Incident details and provide workaround (if available)
- Escalate to support areas (Functional) or IT management (Hierarchical)

Resolution and Recovery

- Resolve the Incident or raise a RFC

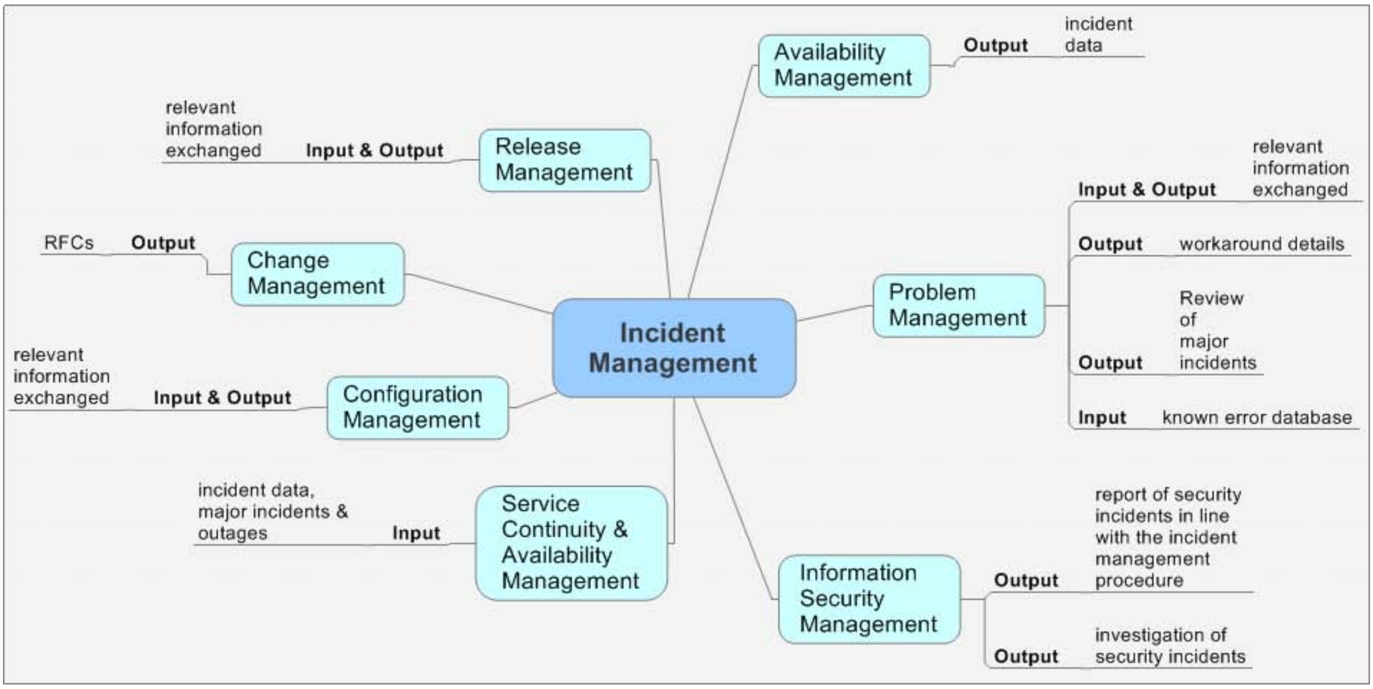
Incident Closure

- Update details of actions taken and classification of Incident.
- Confirm closure with User

8.2.2 Major Incidents

A major incident is the highest category or impact for an incident that results in significant disruption to the business. A separate process with shorter timescales and greater urgency should be used for major incidents. Problem Management looks further at major problem reviews.

8.2.3 Interfaces with Other Processes


Incident Management
Availability Management
Output
incident data
Release Management
Input & Output
relevant information exchanged
Change Management
Output
RFCs
Configuration Management
Input & Output
relevant information exchanged
Service Continuity & Availability Management
Input
incident data, major incidents & outages
Problem Management
Input & Output
relevant information exchanged
Output
workaround details
Output
Review of major incidents
Input
known error database
Information Security Management
Output
report of security incidents in line with the incident management procedure
Output
investigation of security incidents

Examples of what Incident Management *shall* do:

* All incidents are recorded and procedures are adopted to manage the impact of those incidents.

* The customer is kept informed of the progress of any reported incidents or service requests and alerted in advance if their service levels cannot be met and an action agreed.

Examples of what Incident Management *should* do:

* Incident Management is delivered by the Service Desk function.

* The recording of incidents occurs in a manner that allows relevant information to be retrieved and analyzed.

* Incident management staff have access to an up-to-date knowledge base holding information on technical specialists, previous incidents, related problems and known errors, workarounds and checklists that will help in restoring the service to the business.

A complete overview of the requirements of Incident Management can be found in Chapter 8.2, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 8.2, Part 2 of the ISO/IEC 20000 standard.

8.2.4 Incident Management Review Questions

1. True or False?

   Major incidents are classified and managed as part of the normal incident management process activities.

   T F

2. Which of the following is correct for an incident?

   a) Customers are kept informed of progress
   b) All shall be logged
   c) Closure is to be confirmed with the user
   d) All of the above

3. Which of the following is the correct formula for assessing priority?

   a) Prioritization and categorization
   b) Critically and impact
   c) Impact and urgency
   d) Urgency and categorization

4. Which of the following is the objective for Incident Management?

   a) To minimize disruption to the business by proactive identification and analysis of the cause of incidents and by managing problems to closure
   b) To manage information security effectively within all service providers
   c) To restore agreed service to the business as soon as possible or to respond to service requests
   d) To ensure that agreed service continuity and availability commitments to customers can be met in all circumstances

5. True or False

   All staff involved in incident management should have access to the known error database and the CMDB

   T F

Answers to all questions can be found in Chapter 12.

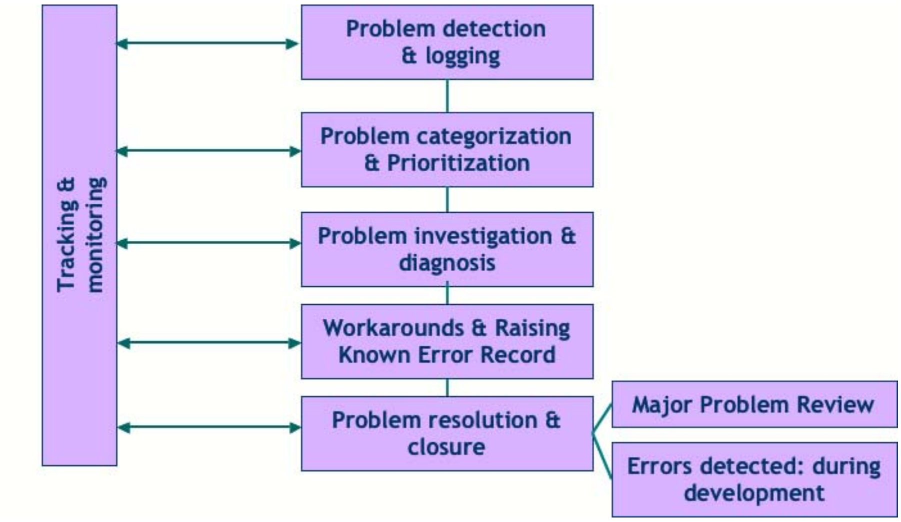
8.3 *Problem Management*

OBJECTIVE: To minimize disruption to the business by proactive identification and analysis of the cause of incidents and by managing problems to closure.

Problem management has interfaces with the change management process for managing the required changes. The incident management process and all other Service Management processes retrieve up-to-date information from the problem management process. The explicitly required documents in the problem management process are problem records and records of identified actions for improvement.

There are two sub-processes in Problem Management: Reactive and Proactive.

8.3.1 Reactive Problem Management


Tracking & monitoring
Problem detection & logging
Problem categorization & Prioritization
Problem investigation & diagnosis
Workarounds & Raising Known Error Record
Problem resolution & closure
Major Problem Review
Errors detected: during development

The activities of Reactive Problem Management are similar to those of Incident Management for the logging, categorization and classification for Problems. The subsequent activities are different as this is where the actual root-cause analysis is performed and the Known Error corrected.

Problems must be prioritized in the same way as incidents, but the frequency and impact of related incidents should be taken into account. In order to determine the root cause of a problem, the appropriate level of resources and expertise should be applied. It is often valuable to try to recreate the failure, so as to understand what has gone wrong, and then to try various ways of finding the most appropriate and cost-effective resolution to the problem. To do this effectively without causing further disruption to the users, a test system will be necessary that mirrors the production environment.

Workarounds can be used for any incidents caused by the problem. An example of a workaround may be a manual amendment made to an input file to allow a program to complete its run successfully and allow a billing process to complete satisfactorily. In this example, the reason for the file becoming corrupted in the first place must be determined and work on a permanent resolution continued.

Major Problem Review

After every major incident or problem, a review should be conducted to learn any lessons for the future. Specifically the review should examine:

- Those things that were done correctly
- Those things that were done wrong
- What could be done better in the future?
- How to prevent recurrence
- Whether there has been any third-party responsibility and whether follow-up actions are needed.

Such reviews can be used as part of training and awareness activities for staff – any lessons learned should be documented in appropriate procedures, working instructions, diagnostic scripts or Known Error Records.

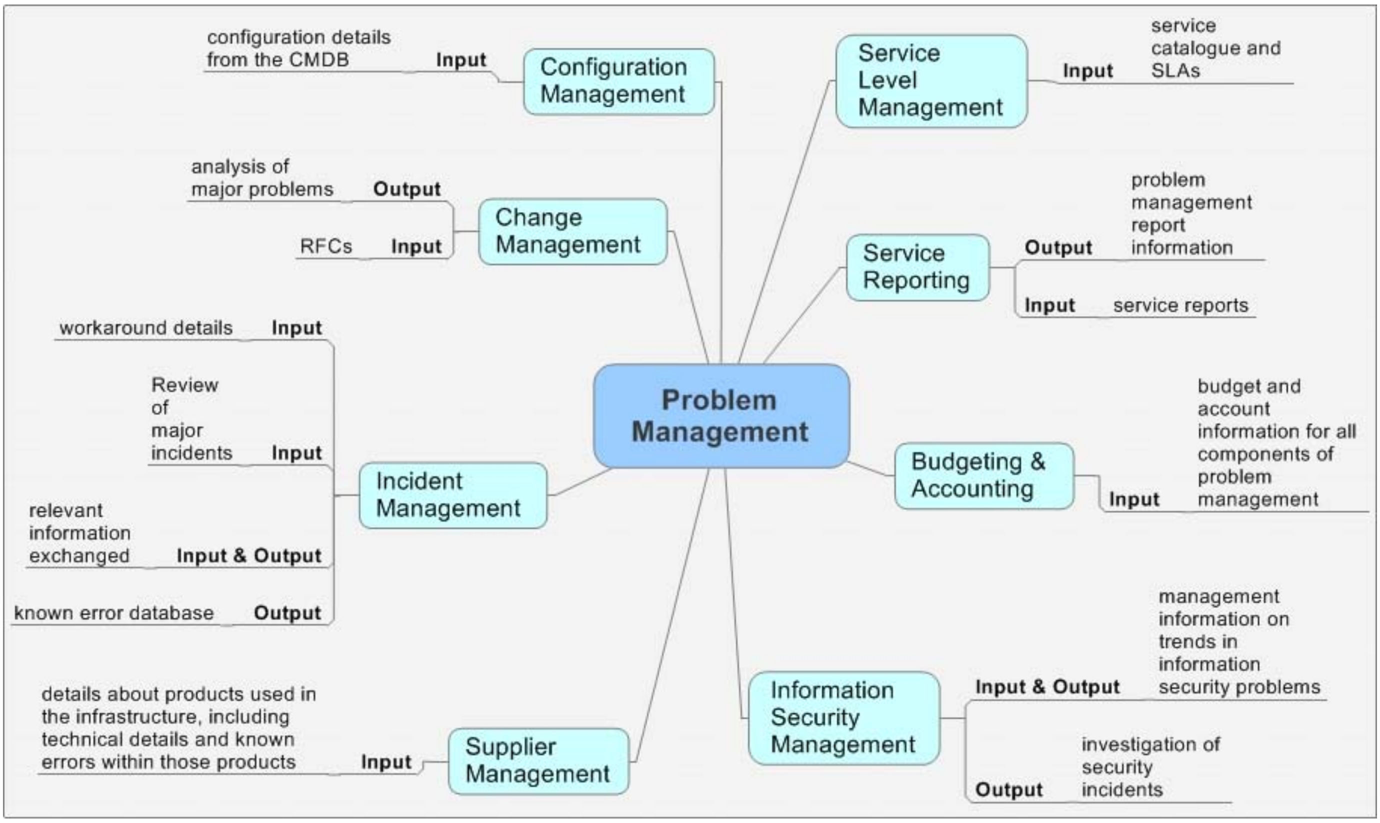
8.3.2 Proactive Problem Management

The two main activities of Proactive Problem Management are:

- **Performing a Trend Analysis**
  - Review reports from other processes (e.g. Incident, Availability Management)
  - Identify recurring Problems or training opportunities.

- **Targeting Preventative Action**
  - Perform a cost - benefit analysis of all costs associated with prevention
  - Target specific areas taking up the most support attention

8.3.3 Interfaces with Other Processes


Problem Management
configuration details from the CMDB
Input
Configuration Management
analysis of major problems
Output
RFCs
Input
Change Management
workaround details
Input
Review of major incidents
Input
relevant information exchanged
Input & Output
known error database
Output
Incident Management
details about products used in the infrastructure, including technical details and known errors within those products
Input
Supplier Management
Service Level Management
Input
service catalogue and SLAs
Service Reporting
Output
problem management report information
Input
service reports
Budgeting & Accounting
Input
budget and account information for all components of problem management
Information Security Management
Input & Output
management information on trends in information security problems
Output
investigation of security incidents

Examples of what Problem Management *shall* do:

* All identified problems are recorded and procedures adopted to identify, minimize or avoid the impact of incidents and problems. They define the recording, classification, updating, escalation, resolution and closure of all problems.

* Problem resolution is monitored, reviewed and reported on for effectiveness.

* Problem management is responsible for ensuring up-to-date information on known errors and corrected problems is available to incident management

Examples of what Problem Management *should* do:

* When the problem management investigation has identified the root cause of an incident and a method of resolving the incident, the problem is classified as a known error.

* Information on workarounds, permanent fixes or progress of problems is communicated to those affected or required to support affected services.

A complete overview of the requirements of Problem Management can be found in Chapter 8.3, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 8.3, Part 2 of the ISO/IEC 20000 standard.

Please refer to module 11 in the online learning program for further information on resolution processes.

8.3.4 Problem Management Review Questions

1. What is the difference between a problem and an incident?

   a) A problem deals with the underlying cause and an incident finds a solution as soon as possible
   b) An incident deals with the underlying cause and a problem find a solution as soon as possible
   c) A problem is a known error and an incident is a disruption to service
   d) An incident provides answers to service requests and a problem deals with recurring incidents only

2. True or False

   One of the activities of reactive problem management is performing trend analysis.

   T F

3. During a major problem review, which of the following will be addressed?

   a) How to prevent recurrence
   b) Things that were done well
   c) Lessons to be learned
   d) All of the above

4. Which of the following reactive activities follows problem detection and logging?

   a) Categorization and prioritization
   b) Workarounds
   c) Investigation and diagnosis
   d) Problem resolution and closure

5. When performing Trend Analysis, which of the following processes would problem management request reports from?

    a) Incident Management
    b) Availability Management
    c) Security Management
    d) All of the above

Answers to all questions can be found in Chapter 12.

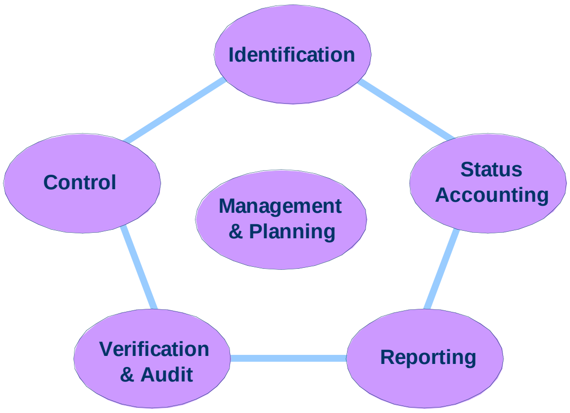
9 Control Processes

9.1 Configuration Management

OBJECTIVE: To define and control the components of the service and infrastructure and maintain accurate configuration information.

This process manages the service assets and Configuration Items in order to support the other Service Management processes. Configuration records and records of deficiencies are the required documents of configuration management.

9.1.1 Activities



Management & Planning

- Defining the strategy, policy, scope, objectives, processes and procedures.
- Roles and responsibilities of involved staff and stakeholders.
- Location of storage areas and libraries used to hold hardware, software and documentation.
- CMDB Design.
- CI naming conventions.
- Housekeeping including license management and archiving of Configuration Items.

Identification

The selection, identification, labeling and registration of Configuration Items. It is the activity that determine what CIs will be recorded, what their attributes are, and what relationships exist with other CIs. Identification can take place for:

- Hardware and Software – include OS
- Business systems – custom built
- Packages – off the shelf
- Physical databases
- Feeds between databases and links
- Configuration baselines
- Software releases
- Documentation

Control

Ensures that only authorized and identifiable CIs are recorded from receipt to disposal in order to protect the integrity of the CMDB. Control occurs anytime the CMDB is altered, including:

- Registration of all new CIs and versions
- Update of CI records and licence control
- Updates in connection with RFCs and Change Management
- Update the CMDB after periodic checking of physical items

Status Accounting

The reporting of all current and historical data concerned with each CI throughout its lifecycle. Provides information on:

- Configuration baselines
- Latest software item versions
- The person responsible for status change
- CI change/incident/problem history

Reporting

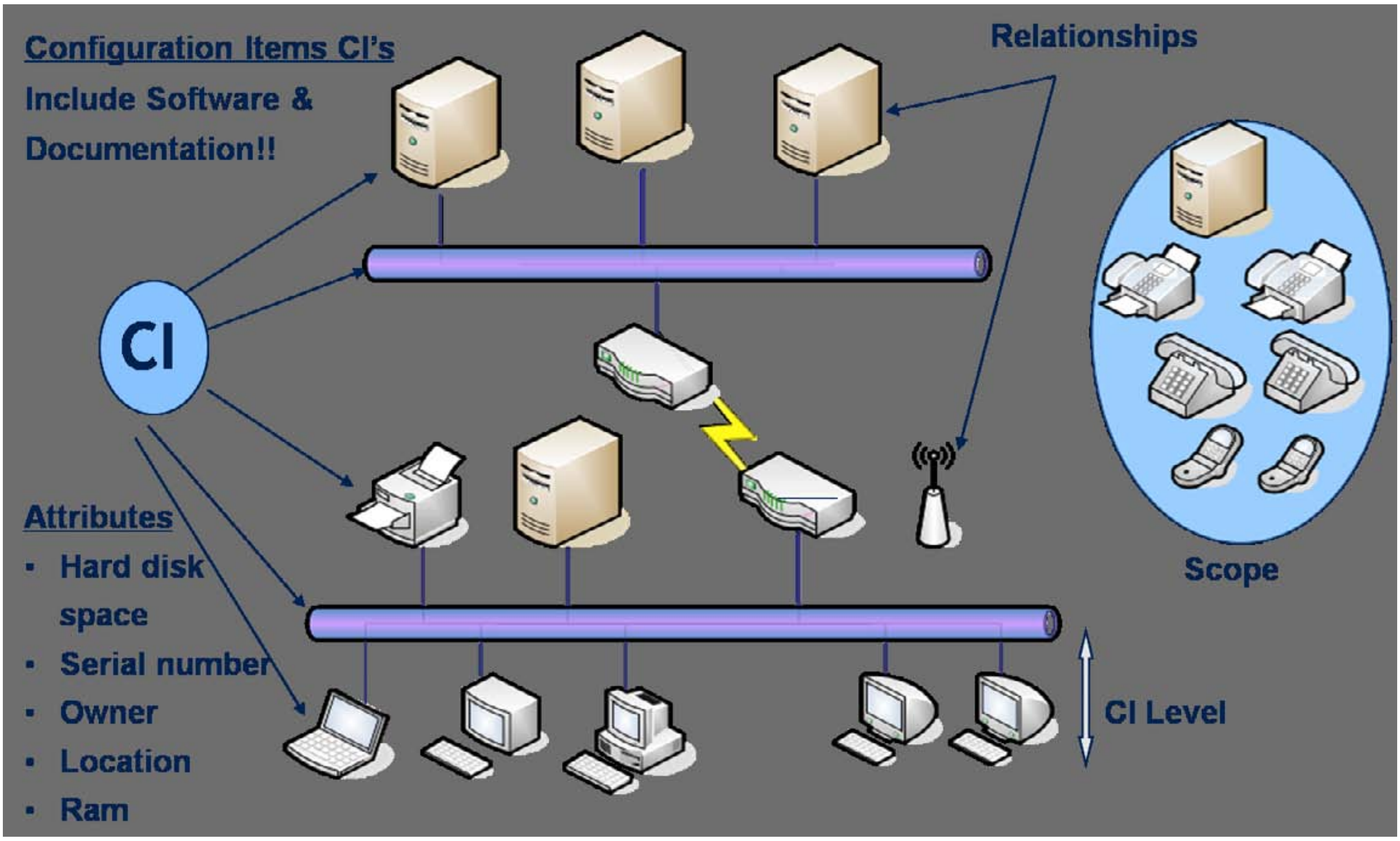
Reporting is the responsibility of the process manager. Configuration Management reports will be made available to the service level manager for the purpose of communicating feedback on service levels to the customer.

Verification and Audit

Reviews and audits verify the existence of CIs, checking that they are correctly recorded in the CMDB and that there is conformity between the documented baselines and the actual environment to which they refer.

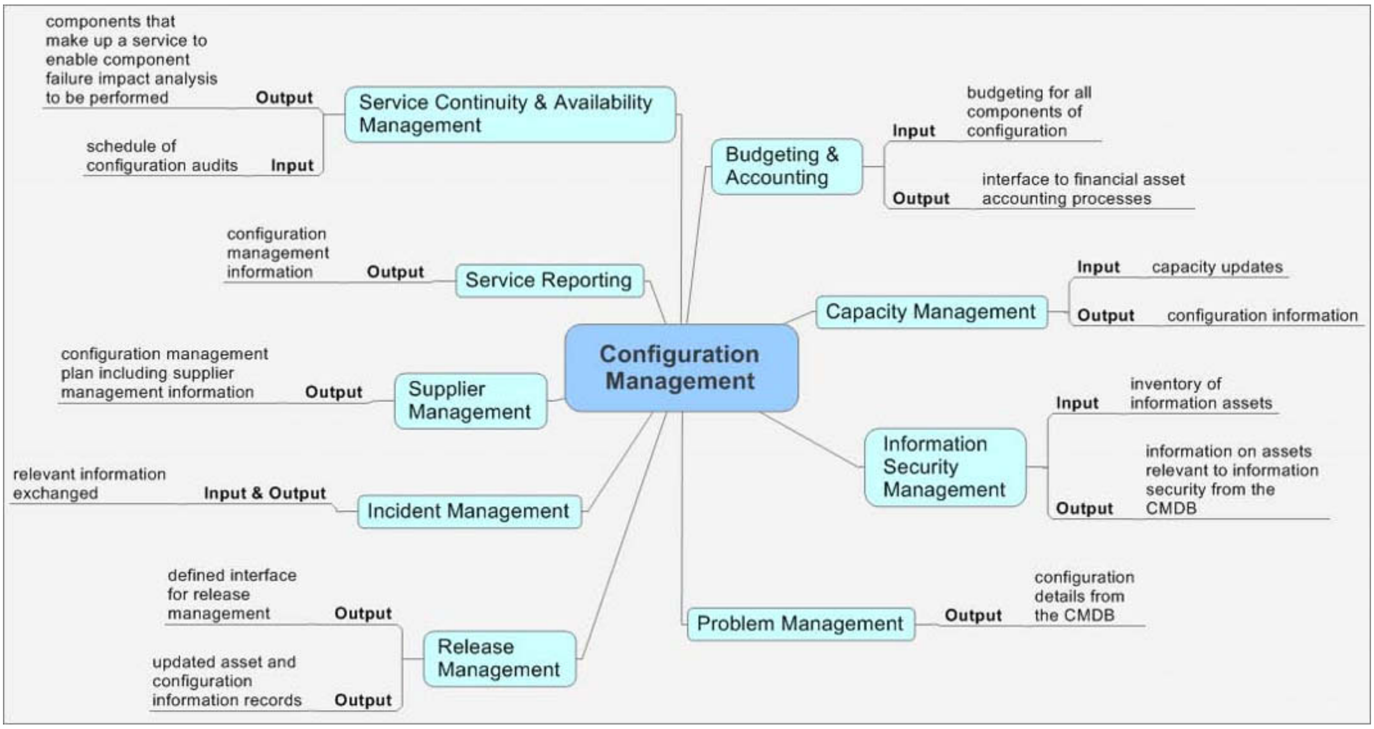
9.1.2 The Configuration Management Database (CMDB)

As demonstrated in the diagram below, the CMDB is a set of one or more connected databases and information sources that provide a logical model of the IT infrastructure. It captures Configuration Items (CIs) and the relationships that exist between them. Examples of CIs are shown below.



It is important to determine to what level the CMDB will record information about the IT infrastructure and to decide what is not covered within the scope of the CMDB. Components out of scope are typically those not under the control of Change Management e.g. telecommunication equipment.

9.1.3 Interfaces with Other Processes


Configuration Management
Service Continuity & Availability Management
Output
components that make up a service to enable component failure impact analysis to be performed
Input
schedule of configuration audits
Service Reporting
Output
configuration management information
Supplier Management
Output
configuration management plan including supplier management information
Incident Management
Input & Output
relevant information exchanged
Release Management
Output
defined interface for release management
Output
updated asset and configuration information records
Budgeting & Accounting
Input
budgeting for all components of configuration
Output
interface to financial asset accounting processes
Capacity Management
Input
capacity updates
Output
configuration information
Information Security Management
Input
inventory of information assets
Output
information on assets relevant to information security from the CMDB
Problem Management
Output
configuration details from the CMDB

Examples of what Configuration Management *shall* do:

* A policy exists on what is defined as a configuration item and its constituent components.

* The information to be recorded for each item is defined and includes the relationships and documentation necessary for effective service management.

* Configuration control procedures ensure that the integrity of systems, services and service components are maintained.

Examples of what Configuration Management *should* do:

* Configuration Management is planned and implemented with change and release management in order to ensure that the service provider can effectively manage its IT assets and configurations.

* Accurate configuration information is available to support the planning and control of changes, as new and updated services and systems are released and distributed.

A complete overview of the requirements of Configuration Management can be found in Chapter 9.1, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 9.1, Part 2 of the ISO/IEC 20000 standard.

9.1.4 Configuration Management Review Questions

1. CMDB stands for which of the following:

   a) Change management database
   b) Configuration management database
   c) Capacity management database
   d) Continuity management database

2. Which of the following activities is at the centre of the configuration management process?

   a) Identification
   b) Status accounting
   c) Control
   d) Management of planning

3. True or False?

   The information recorded for each item is to be defined and must includes relationships and documentation necessary for effective service management.

   T F

4. Which configuration management activity defines the strategy, policy, scope, objectives, processes and procedures?

   a) Identification
   b) Management & Planning
   c) Control
   d) Verification & Audit

5. The objective of Configuration Management is:

   a) To ensure all changes are assessed, approved, implemented and reviewed in a controlled manner
   b) To manage information security effectively within all service providers
   c) To minimize disruption to the business by proactive identification and analysis of the cause of incidents and by managing problems to closure
   d) To define and control the components of the service and infrastructure and maintain accurate configuration information

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

9.2 Change Management

OBJECTIVE: To ensure all changes are assessed, approved, implemented and reviewed in a controlled manner.

Change Management acts as the greatest contributor to the CMDB, as Changes to the CMDB must be assessed and authorized by Change Management first.

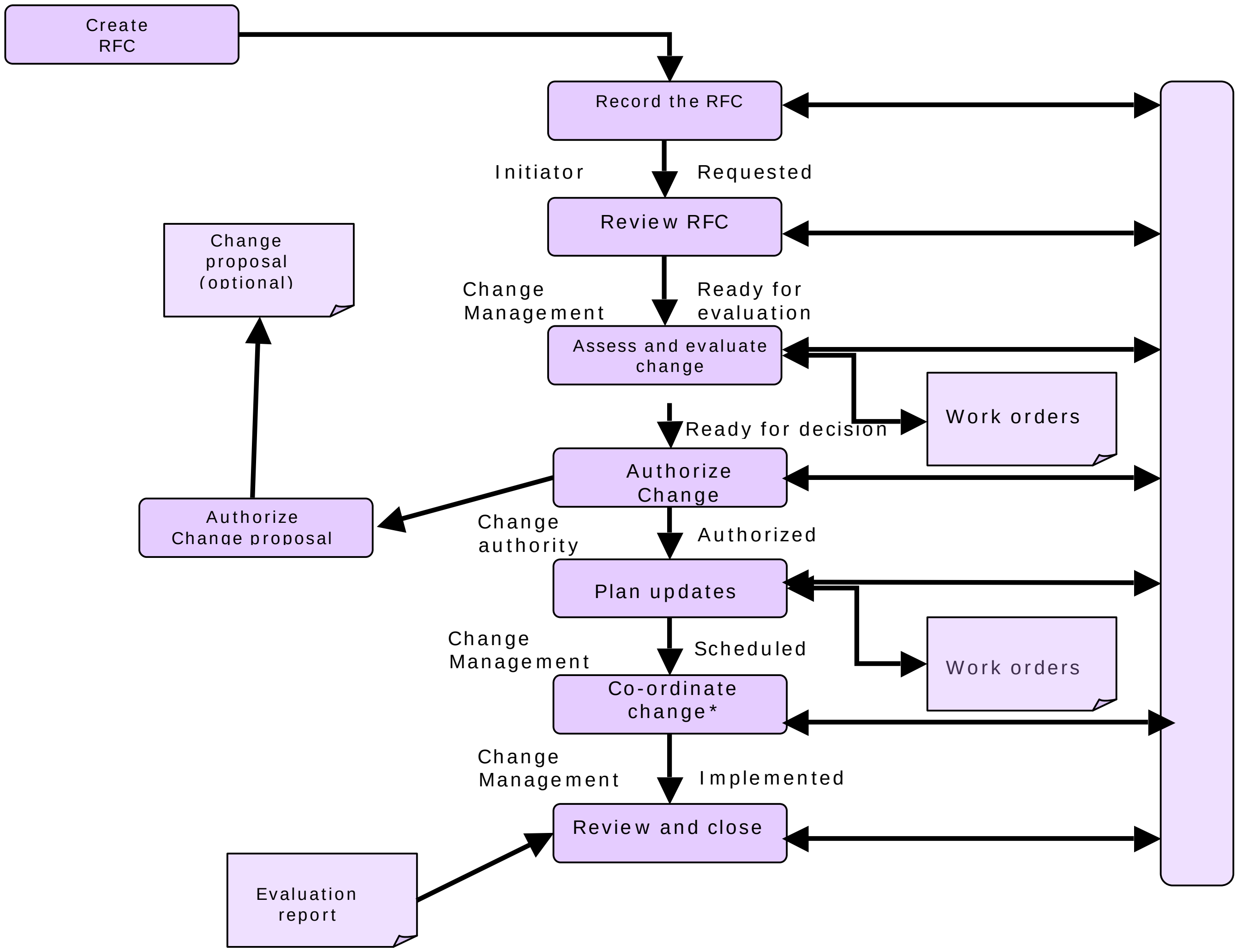
To work effectively, Change Management needs to remain impartial to the needs of any one particular IT group or customer, in order to make effective decisions that best support the overall organizational objectives.

To ensure that the Change Management process does not become a bottleneck, it is important to define what Change Models will be used to ensure effective and efficient control and implementation of RFCs.

9.2.1 Activities

The important steps, as demonstrated in the example Change Management process flow on the following page, are:

1. The RFC is logged:
2. An initial review is performed (filter RFCs)
3. The RFCs are assessed – may require involvement of CAB or ECAB.
4. This is authorized by the Change Manager
5. Work orders are issued for the build of the Change (carried out by other groups)
6. Change Management coordinates the work performed.
7. The Change is reviewed.
8. The Change is closed.



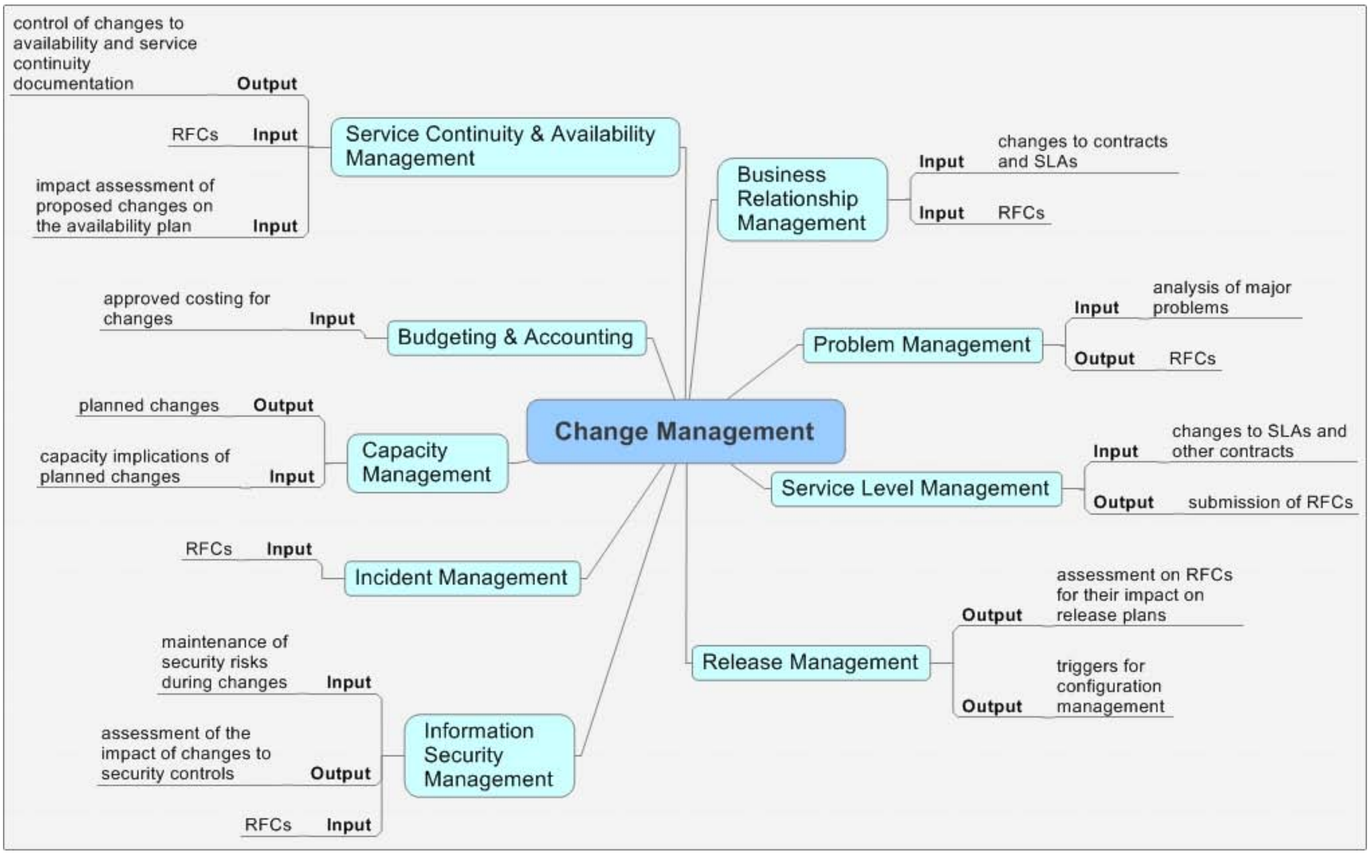
9.2.2 The 7Rs of Change Management

When assessing Changes, it is important to have answers to the following seven questions:

- Who RAISED the change?
- What is the REASON for the change?
- What is the RETURN required from the change?
- What are the RISKS involved in the change?
- What RESOURCES are required to deliver the change?
- Who is RESPONSIBLE for the build, test and implementation of the change?
- What is the RELATIONSHIP between this change and other changes?

These questions must be answered for ***all changes***. Without this information the impact assessment cannot be completed, and the balance of risk and benefit to the live service will not be understood. This could result in the change not delivering all the possible or expected business benefits or even of it having a detrimental, unexpected effect on the live service.

9.2.3 Interfaces with Other Processes


Change Management
Service Continuity & Availability Management
control of changes to availability and service continuity documentation
Output
RFCs
Input
impact assessment of proposed changes on the availability plan
Input
Budgeting & Accounting
approved costing for changes
Input
Capacity Management
planned changes
Output
capacity implications of planned changes
Input
Incident Management
RFCs
Input
Information Security Management
maintenance of security risks during changes
Input
assessment of the impact of changes to security controls
Output
RFCs
Input
Business Relationship Management
Input
changes to contracts and SLAs
Input
RFCs
Problem Management
Input
analysis of major problems
Output
RFCs
Service Level Management
Input
changes to SLAs and other contracts
Output
submission of RFCs
Release Management
Output
assessment on RFCs for their impact on release plans
Output
triggers for configuration management

Examples of what Change Management *shall* do:

*	Service and infrastructure changes have a clearly defined and documented scope.

*	All requests for change are recorded and classified. All changes are approved, checked and are implemented in a controlled manner. They are reviewed for success and action taken where necessary after implementation. The process includes the manner in which the change will be reversed or remedied if unsuccessful.

*	Changes recorded are analyzed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and other relevant information. The results and conclusions drawn from change analysis are recorded.

Examples of what Change Management *should* do:

*	The status of changes and scheduled implementation dates is used as the basis for change and release scheduling.

*	Scheduling information is made available to the people affected by the change and, where an outage can be caused during normal service hours, the people affected agree to the change before implementation.

A complete overview of the requirements of Change Management can be found in Chapter 9.2, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 9.2, Part 2 of the ISO/IEC 20000 standard.

Please refer to module 12 in the online learning program for further information on control processes.

9.2.4 Change Management Review Questions

1. All RFCs should be:

   a) Recorded
   b) Classified
   c) Approved and checked
   d) All of the above

2. Which of the following change management activities follows the assessment and evaluation of change?

   a) Planning updates
   b) Coordinating change
   c) Authorizing change
   d) Reviewing change

3. True or False?

   The change management process includes the manner in which the change will be reversed or remedial if unsuccessful.

   T F

4. The release process finds information on planned and approved change implementation from:

   a) The change schedule
   b) The CMDB
   c) SKMS
   d) Incident Management

5. Which of the following is the objective for change management?

a) To define, agree, record and manage levels of service
b) To minimize disruption to the business by proactive identification and analysis of the cause of incidents and by managing problems to closure
c) To deliver, distribute and track one or more changes in a release into the live environment
d) To ensure all changes are assessed, approved, implemented and reviewed in a controlled manner

Answers to all questions can be found in Chapter 12.

10 Release Processes

10.1 Release Management

OBJECTIVE: To deliver, distribute and track one or more changes in a release into the live environment.

Release Management refers to the implementation of a group of related and compatible CIs into a batch, known as a release. Circumstances where the process of release management may be advantageous include changes to a desktop build, application release or major upgrades.

The Change Management process governs each release through a request for change (RFC). This ensures that the group of changes in a release are authorized, scheduled and implemented correctly. The release management process also ensures that the groups of changes in each release are compatible with each other and that clashes with other unrelated changes do not occur.

10.1.1 Options for Release

Big Bang

The new or changed service is deployed to all user areas in one operation. This will often be used when introducing an application change and consistency of service across the organization is considered important.

The negative aspect of the Big Bang approach is that it increases the risk and impact of a failed Release.

Phased Approach

The service is deployed to a part of the user base initially, and then this operation is repeated for subsequent parts of the user base via a scheduled rollout plan.

This will be the case in many scenarios such as in retail organizations for new services being introduced into the stores' environment in manageable phases.

The Push Approach

This is used where the service component is deployed from the centre and pushed out to the target locations.

In terms of service deployment, delivering updated service components to all users, either in big bang or phased form is using the push approach, since the new or changed service is delivered into the users' environment at a time not of their choosing.

The Pull Approach

This is used for software releases where the software is made available in a central location but users are free to pull the software down to their own location at a time of their choosing or when a workstation restarts.

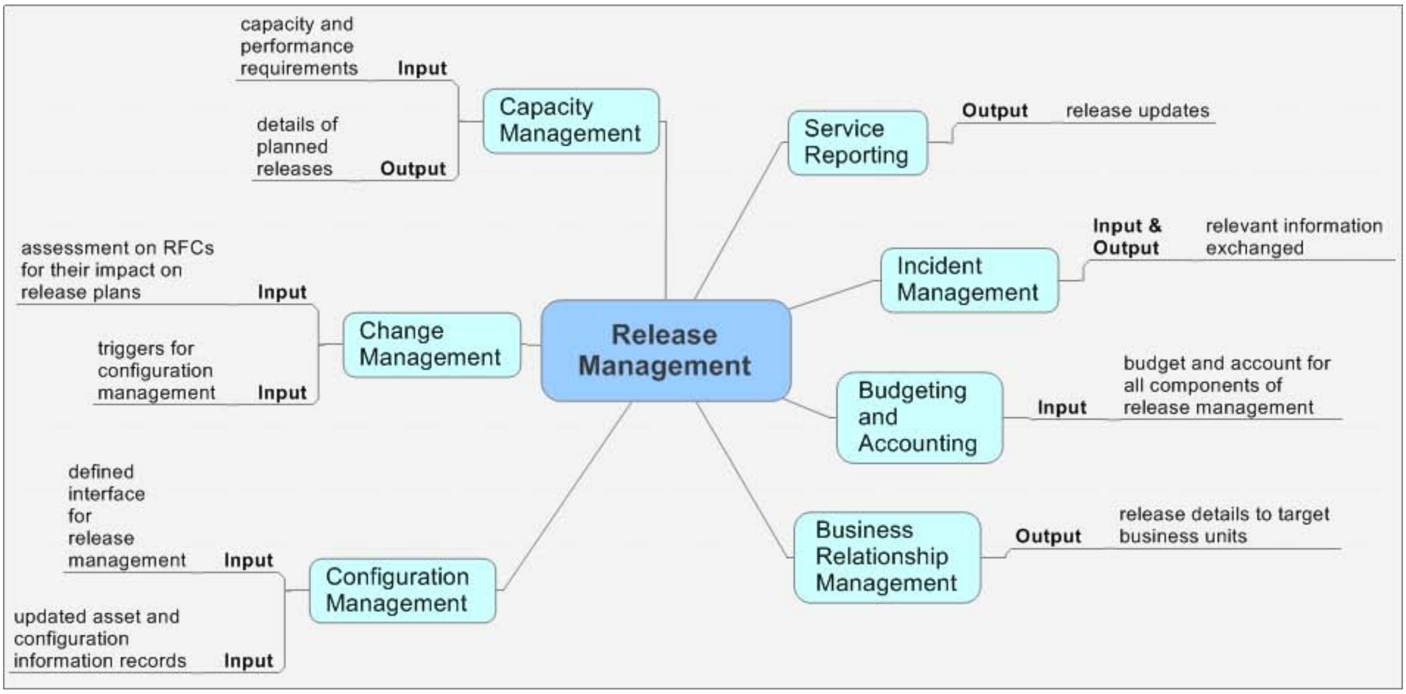
Automated

This option for release uses technology to automate releases. This helps to ensure repeatability and consistency. However, the time required to provide a well-designed and efficient automated mechanism may not always be available or viable.

Manual

This involves manual activities to distribute a release. It is important to monitor and measure the impact of many repeated manual activities as they are likely to be inefficient and error prone.

10.1.2 Interfaces with Other Processes


capacity and performance requirements
Input
details of planned releases
Output
Capacity Management
assessment on RFCs for their impact on release plans
Input
triggers for configuration management
Input
Change Management
defined interface for release management
Input
updated asset and configuration information records
Input
Configuration Management
Release Management
Service Reporting
Output
release updates
Incident Management
Input & Output
relevant information exchanged
Budgeting and Accounting
Input
budget and account for all components of release management
Business Relationship Management
Output
release details to target business units

Examples of what Release Management *shall* do:

* The release policy stating the frequency and type of releases is documented and agreed.

* The process includes the manner in which the release will be reversed or remedied if unsuccessful.

* Plans for release management record the release dates and deliverables and refer to related change requests, known errors and problems. The process passes suitable information to the incident management process.

Examples of what Release Management *should* do:

* Release management co-ordinates the activities of the service provider, suppliers and the business in order to plan and deliver a release across a distributed environment.

* The impact of all new or changed configuration items required to effect any authorized changes is assessed and the service provider ensures that both technical and non-technical aspects of the release are considered together.

A complete overview of the requirements of Release Management can be found in Chapter 10.1, Part 1 of the ISO/IEC 20000 standard. More guidance on best practices can be found in Chapter 10.1, Part 2 of the ISO/IEC 20000 standard.

Please refer to module 13 in the online learning program for further information on release processes.

10.1.3 Release Management Review Questions

1. The pull approach to release management is:

   a) When a service is deployed to a part of the user base initially, and then this operation is repeated for subsequent parts of the user base via a scheduled rollout plan
   b) When the new or changed service is deployed to all user areas in one operation
   c) Used where the service component is deployed from the centre and pushed out to the target locations
   d) Used for software releases where the software is made available in a central location but users are free to pull the software down to their own location at a time of their choosing or when a workstation restarts

2. Release Management is governed by which process?

   a) Service Level Management
   b) Configuration Management
   c) Change Management
   d) Service Continuity & Availability Management

3. True or False?

The big bang approach to release is used when the change is deployed to all user areas in one operation.

T F

4. What is the objective of Release Management?

   a) To deploy releases into production and establish effective use of the service
   b) To ensure all changes are assessed, approved, implemented and reviewed in a controlled manner
   c) To deliver, distribute and track one or more changes in a release into the live environment
   d) To define and control the components of the service and infrastructure and maintain accurate configuration information

5. A defined interface for release management is input by which process?

   a) Configuration Management
   b) Change Management
   c) Service Level Management
   d) Incident Management

Answers to all questions can be found in Chapter 12.

11 Management of ISO/IEC 20000

The objective of ISO/IEC 20000 management is to provide a management system, including policies and a framework to enable the effective management and implementation of all IT services.

An organization will need to develop and manage the roles and duty statements of all staff involved in provided IT service management.

Examples may be Position Statements or Performance Agreements where the role and expected work performance have been agreed and documented. In conjunction with this, individual learning plans should be developed. Regular reviews meetings should be conducted and the Position Statements and individual learning plans reviewed and updated as required.

Process roles such as the Problem Manager and Change manager can apply here, however these are ITIL® terms and are not referenced in the standard.

There are three components of management in the implementation of ISO/IEC 20000: Management responsibility, documentation requirements and competence, awareness and training.

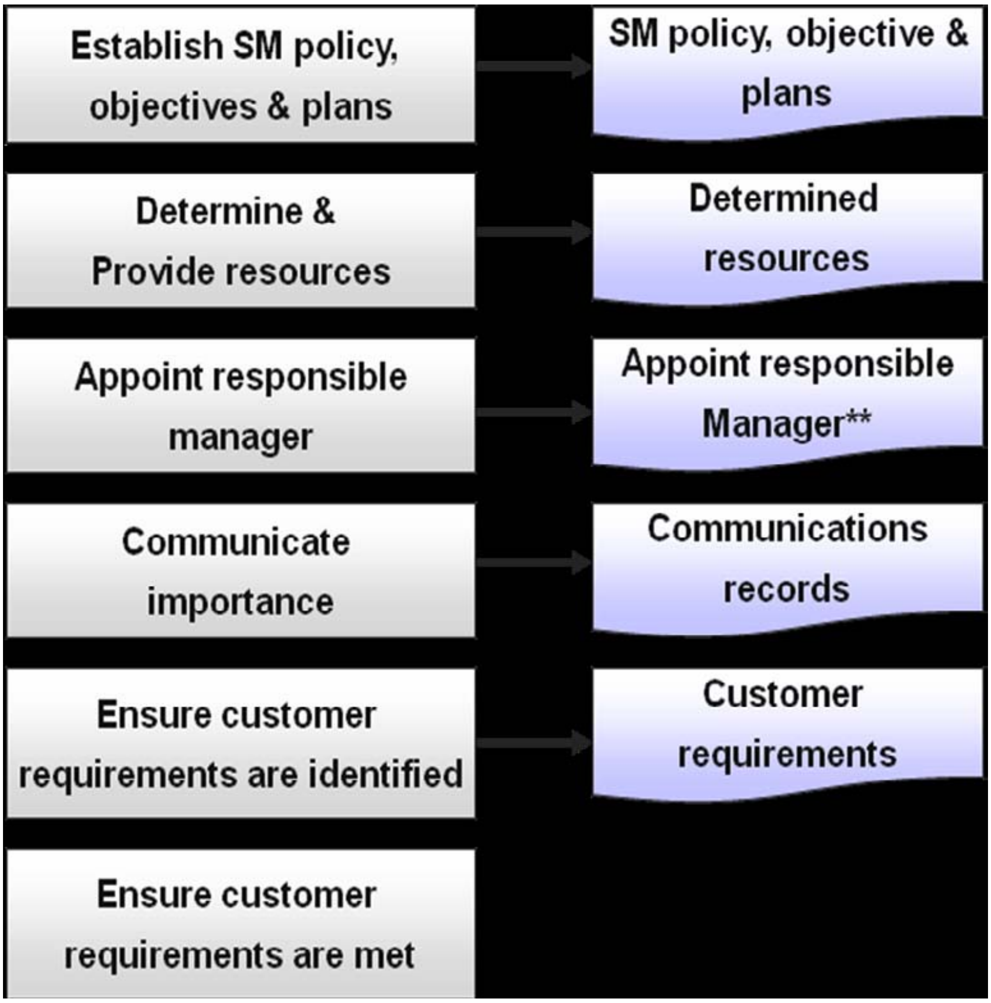
11.1.1 Management responsibility

Through leadership and actions, top/executive management is to provide evidence of its commitment to developing, implementing and improving its Service Management capability within the context of the organization's business and customer's requirements.

The concept of management commitment is essentially intangible and compliance to the management responsibility requirement can be shown only through documented leadership and actions for the development, implementation and improvement of its Service Management capability.

Documentation to demonstrate that commitment may include:

- Appointment records
- Written Service Management policies, objectives and plans
- Implementation results
- Communication records and meeting minutes
- Records of resource determination


Establish SM policy, objectives & plans
SM policy, objective & plans
Determine & Provide resources
Determined resources
Appoint responsible manager
Appoint responsible Manager**
Communicate importance
Communications records
Ensure customer requirements are identified
Customer requirements
Ensure customer requirements are met

The process flow above outlines the primary roles involved with the management of Service Management. These processes also include planned reviews and risk management through each of the Service Management processes.

11.1.2 Documentation Requirements

Documentation serves as a means to communicate information and also as a means of sharing knowledge. It facilitates the improvement of the organization's performance, and aids a common understanding across process fields.

Procedures must exist for the creation, review, approval, maintenance, disposal and control of all documents and records across all processes.

11.1.3 Competence, Awareness & Training

There are three quality management principles that apply when addressing competence, awareness and training. These are:

Leadership – the ability of the individual to influence, motivate and enable other to contribute toward the effectiveness and success of the organization

Involvement of People – the recognition of special talents and how each individual is made valuable to the organization

Continual Improvement – the competence and awareness of people is developed and enhanced continually

When organizing employees, the focus should not only be on obtaining a good match between the required and available competence, but also identify opportunities to develop competence, transfer expertise and learn skills.

Please refer to module 7 in the online learning program for further information on the management of service management processes.

11.1.4 ISO/IEC 20000 Management Review Questions

1. What documentation is needed to develop and manage the roles and duty statements of staff?

    a) Position Statements and Service Level Agreements
    b) Performance Statements and Service Level Agreements
    c) Position Statements and Performance Statements
    d) Performance Statements and Underpinning Contracts

2. True or False

    The objective of ISO/IEC 20000 management is to provide a management system, including policies and a framework to enable the effective management and implementation of all IT services.

    T F

3. Which of the following is CORRECT?

    a) Definition of ITIL® roles such as Problem Manager and Change Manager are requirements in the standard
    b) There are four components of management within the standard
    c) Compliance with management responsibility can only be shown through documented leadership and actions
    d) None of the above

4. What are the three quality management principles of Competence, Awareness and Training?

    a) Leadership, Involvement of People and Review Schedules
    b) Involvement of People, Leadership and Continual Improvement
    c) Continual Improvement, Review Schedules and Leadership
    d) Review Schedules, Involvement of People and Continual Improvement

5. Which of the following are examples of documentation to demonstrate commitment?

   a) Appointment records
   b) Implementation results
   c) Records of resource determination
   d) All of the above

Answers to all questions can be found in Chapter 12.

This page intentionally left blank.

12 Answers to Review Questions

Introduction

ANSWERS

1d, 2a, 3F, 4c, 5c

Planning and Implementation

ANSWERS

1c, 2d, 3b, 4T, 5a

Service Level Management

ANSWERS

1c, 2b, 3d, 4d, 5c

Service Reporting

ANSWERS

1c, 2a, 3c, 4d, 5d

Service Continuity & Availability Management

ANSWERS

1d, 2a, 3d, 4c, 5d

Budgeting & Accounting

ANSWERS

1b, 2d, 3a, 4c, 5b

Capacity Management

ANSWERS

1a, 2c, 3c, 4d, 5b

Information Security Management

ANSWERS

1a, 2d, 3c, 4c, 5a

Business Relationship Management

ANSWERS

1d, 2a, 3a, 4a, 5d

Supplier Management

ANSWERS

1a, 2T, 3d, 4a, 5a

Incident Management

ANSWERS

1F, 2d, 3c, 4c, 5F

Problem Management

ANSWERS

1a, 2F, 3d, 4a, 5d

Configuration Management

ANSWERS

1b, 2d, 3T, 4b, 5d

Change Management

ANSWERS

1d, 2c, 3T, 4a, 5d

Release Management

ANSWERS

1d, 2c, 3T, 4c, 5a

ISO/IEC 20000 Management

ANSWERS

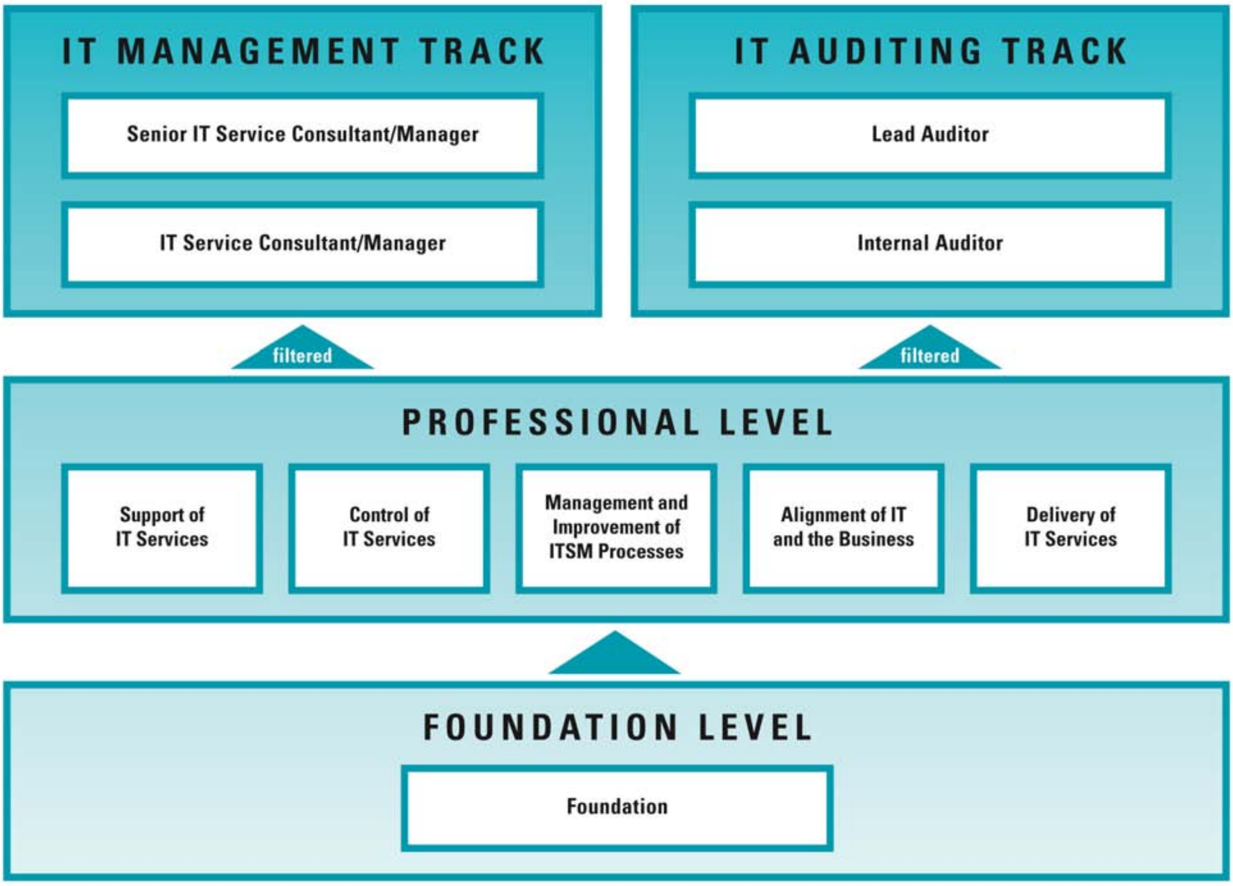
1c, 2T, 3c, 4b, 5d

This page intentionally
left blank.

13 Certification

13.1 ISO/IEC 20000 Certification Pathways

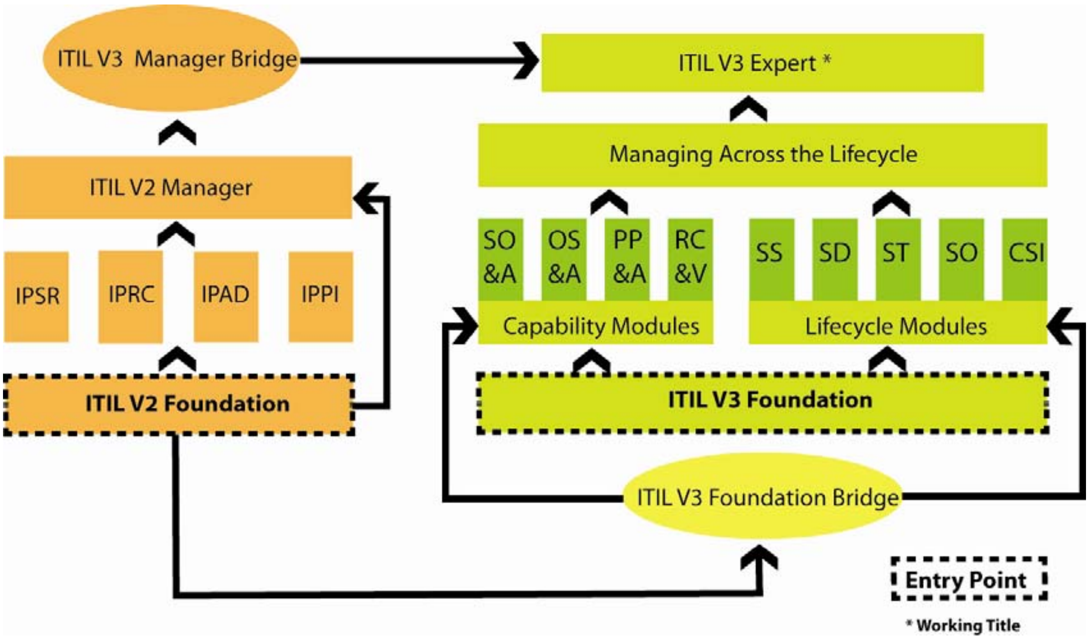
ISO/IEC 20000 Standard is becoming a basic requirement for IT Service providers and is fast becoming the most recognized symbol of quality regarding IT Service Management processes. ISO/IEC 20000 programs aim to assist IT professionals master and understand the standard itself and issues relating to earning actual standards compliance.



For more information on certification and available programs please visit our website http://www.artofservice.com.au

13.2 ITIL® Certification Pathways

There are many pathway options that are available to you within the ITIL® Certification scheme. Below illustrates the possible pathways that are available to you. Currently it is intended that the highest certification is the ITIL® V3 Expert, considered to be equal to that of Diploma Status.



For more information on certification and available programs please visit our website http://www.artofservice.com.au

14 ISO/IEC 20000 Foundation Exam Tips

Exam Details

- 40 questions
- The correct answer is only one of the four
- 60 minutes duration
- 26 out of 40 is a pass (65%)
- Closed book
- No notes

Practical Suggestions

- Read the question CAREFULLY
- At this level of exam the obvious answer is often the correct answer *(if you have read the question carefully!!)*
- Beware of being misled by the preliminary text for the question
- If you think there should be another choice that would be the right answer, then you have to choose the "most right"
- Use strategies such as *"What comes first?"* or "*What doesn't belong?"* to help with the more difficult questions.

Organising your Exam

EXIN facilitates the ISO/IEC 20000 Foundation exam. Please contact The Art of Service directly or visit http://www.exin-exams.com to arrange your examination. You can also take your exam at a Prometric Test Centre in your local area. By visiting http://www.prometric.com/default.htm, you will be able to access a full list of testing centres and book your exam online.

Make sure that you prepare adequately in the lead up to your exam by reviewing your notes, reading any available material and attempting the sample exams. We wish you luck in your exam and future ISO/IEC 20000 career!

Please refer to module 13 in the online learning program for further information on exam preparation.

This page intentionally left blank.

15 References

BSI (2005). *Information Technology – Service Management: Part1 Specification.*

BSI (2005). *Information Technology – Service Management: Part 2 Code of Practice.*

ITSMF International (2006). *Metrics for IT Service Management,* Zaltbommel, Van Haren Publishing

ITSMF International (2008). *ISO/IEC 20000: An Introduction.* Zaltbommel, Van Haren Publishing.

The Art of Service (2007) *ITIL® Factsheets*, Brisbane, The Art of Service

The Art of Service (2008) *CMDB and Configuration Management Creation and Maintenance Guide*, Brisbane, The Art of Service

The Art of Service (2008). *Introduction to ISO/IEC 20000*. United Kingdom, Emereo Pty Ltd.

The Art of Service (2008). *ISO/IEC 20000 Foundation Classroom Program Materials*. Brisbane, The Art of Service.

The Art of Service (2008) *IT Governance, Metrics and Measurements and Benchmarking Workbook*, Brisbane, The Art of Service

\The Art of Service (2008). *ITIL® V3 Foundation Complete Certification Kit*. United Kingdom, Emereo Pty Ltd.

The Art of Service (2008) *Risk Management Guide*, Brisbane, The Art of Service

www.artofservice.com.au

www.theartofservice.com

www.theartofservice.org