

ITIL Planning, Protection &Optimizati

Contents

1 Introduction to service management.....	6
1.1 Best practice.....	6
1.2 The ITIL frame work.....	6
1.3 Service management.....	6
1.4 Processes and functions.....	7
1.5 Roles	7
1.5.1 Process owner	7
1.5.2 Process manager	8
1.5.3 Process practitioner	8
1.5.4 Service owner.....	8
1.5.5 The RACI model	9
1.6 Planning, protection and optimization within the context of the service lifecycle	9
1.6.1 Service design value to the business.....	9
1.6.2 Planning, protection and optimization supporting the service lifecycle.....	9
2 Capacity management.....	11
2.1 Purpose and objectives	11
2.2 Scope	11
2.3 Value to the business	12
2.4 Policies, principles and basic concepts.....	12
2.5 Process activities, methods and techniques	13
2.5.1 Business capacity management	13
2.5.2 Service capacity management	14
2.5.3 Component capacity management	14
2.5.4 Capacity management – underpinning activities.....	14
2.5.5 Threshold management and control.....	15
2.5.6 Demand management.....	16
2.5.7 Modelling and trending.....	16
2.5.8 Application sizing.....	16

2.6 Triggers, inputs, outputs and interfaces	16
2.7 Information management	17
2.8 Critical success factors and key performance indicators	18
2.9 Challenges and risks	18
2.10 Roles and responsibilities	19
2.10.1 Capacity management process owner	19
2.10.2 Capacity management process manager	19
3 Availability management	20
3.1 Purpose and objectives	20
3.2 Scope	20
3.3 Value to the business	21
3.4 Policies, principles and basic concepts	21
3.5 Process activities, methods and techniques	22
3.5.1 Reactive activities of availability management	22
3.5.2 Proactive activities of availability management	24
3.6 Triggers, inputs, outputs and interfaces	25
3.7 Information management	26
3.8 Critical success factors and key performance indicators	26
3.9 Challenges and risks	26
3.10 Roles and responsibilities	27
3.10.1 Availability management process owner	27
3.10.2 Availability management process manager	27
4 IT service continuity management	29
4.1 Purpose and objectives	29
4.2 Scope	29
4.3 Value to the business	30
4.4 Policies, principles and basic concepts	30
4.5 Process activities, methods and techniques	30
4.5.1 Stage 1 – Initiation	30
4.5.2 Stage 2 – Requirements and strategy	31
4.5.3 Stage 3 – Implementation	32
4.5.4 Stage 4 – Ongoing operation	34

4.6 Triggers, inputs, outputs and interfaces	34
4.7 Information management	35
4.8 Critical success factors and key performance indicators	36
4.9 Challenges and risks	36
4.10 Roles and responsibilities	37
4.10.1 IT service continuity management process owner	37
4.10.2 IT service continuity management process manager	37
5 Information security management	38
5.1 Purpose and objectives	38
5.2 Scope	38
5.3 Value to the business	38
5.4 Policies, principles and basic concepts	38
5.4.1 Principles	38
5.4.2 Information security policy	38
5.4.3 Security framework	39
5.4.4 The information security management system	39
5.4.5 Information security governance	39
5.5 Process activities, methods and techniques	40
5.5.1 Security strategy	40
5.5.2 Security controls	40
5.5.3 Management of security breaches and incidents	41
5.6 Triggers, inputs, outputs and interfaces	41
5.7 Information management	42
5.8 Critical success factors and key performance indicators	42
5.9 Challenges and risks	42
5.10 Roles and responsibilities	43
5.10.1 Information security management process owner	43
5.10.2 Information security management process manager	43
6 Demand management	45
6.1 Purpose and objectives	45
6.2 Scope	45
6.3 Value to the business	45

6.4 Policies, principles and basic concepts	45
6.4.1 Supply and demand	45
6.4.2 Gearing service assets	45
6.4.3 Demand management through the lifecycle	46
6.5 Process activities, methods and techniques	46
6.5.1 Identify sources of demand forecasting	46
6.5.2 Patterns of business activity and user profiles	46
6.5.3 Activity-based demand management	47
6.5.4 Develop differentiated offerings	47
6.5.5 Management of operational demand	47
6.6 Triggers, inputs, outputs and interfaces	48
6.7 Information management	49
6.8 Critical success factors and key performance indicators	49
6.9 Challenges and risks	49
6.10 Roles and responsibilities	50
6.10.1 Demand management process owner	50
6.10.2 Demand management process manager	50
7 Technology and implementation	51
7.1 Generic requirements for IT service management technology	51
7.2 Evaluation criteria for technology and tools	52
7.3 Practices for process implementation	52
7.3.1 Business impact analysis	52
7.3.2 Service level requirements	53
7.3.3 Risks to the services and processes	53
7.3.4 Implementing service design	53
7.4 Challenges, critical success factors and risks	54
7.4.1 Challenges	54
7.4.2 Critical success factors	55
7.4.3 Risks	55
7.5 Planning and implementing service management technologies	56
7.6 Designing technology architectures and management architectures	56

1 Introduction to service management

1.1 Best practice

Organizations operating in dynamic environments need to improve their performance and maintain competitive advantage. Adopting best practices in industry-wide use can help to improve capability. Sources:

- Public frameworks and standards
- Proprietary knowledge of organizations and individuals

1.2 The ITIL frame work

- Vendor-neutral
- Non-prescriptive
- Best practice.

ITIL is successful because it describes practices that enable organizations to deliver benefits, return on investment and sustained success.

1.3 Service management

A set of specialized organizational capabilities for providing value to customers in the form of services

IT service: A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement (SLA). Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services.

The outcomes that customers want to achieve are the reason why they purchase or use a service. The value of the service to the customer is directly dependent on how well a service facilitates these outcomes.

Services can be classified as:

- Core services
- Enabling services
- Enhancing services

Service management enables service providers to:

- Understand the services they are providing
- Ensure that the services really do facilitate the outcomes their customers want to achieve

- Understand the value of the services to their customers
- Understand and manage all of the costs and risks associated with those services.

Service management is concerned with more than just delivering services. Each service, process or infrastructure component has a lifecycle, and service management considers the entire lifecycle from strategy through design and transition to operation and continual improvement.

IT service management (ITSM): The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.

1.4 Processes and functions

Processes have the following characteristics:

- Measurability
- Specific results
- Customers
- Responsiveness to specific triggers

An organization needs to clearly define the roles and responsibilities required to undertake the processes and activities involved in each lifecycle stage. These roles are assigned to individuals within an organizational structure of teams, groups or functions

1.5 Roles

A role is a set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process or function. One person or team may have multiple roles. Roles fall into two main categories

- generic roles
- specific roles

1.5.1 Process owner

The process owner role is accountable for ensuring that a process is fit for purpose, i.e. that it is capable of meeting its objectives; that it is performed according to the agreed and documented standard; and that it meets the aims of the process definition. This role may be assigned to the same person carrying out the process manager role. Key accountabilities include:

- Sponsoring, designing and change managing the process and its metrics
- Defining the process strategy, with periodic reviews to keep current, and assisting with process design
- Defining appropriate policies and standards for the process, with periodic auditing to ensure compliance
- Communicating process information or changes as appropriate to ensure awareness
- Providing process resources to support activities required throughout the service lifecycle

- Ensuring that process technicians understand their role and have the required knowledge to deliver the process
- Addressing issues with the running of the process
- Identifying enhancement and improvement opportunities and making improvements to the process.

1.5.2 Process manager

The process manager role is accountable for operational management of a process. There may, for example, be several process managers for one process in different locations. This role may be assigned to the same person carrying out the process owner role. Key accountabilities include:

- Working with the process owner to plan and coordinate all process activities
- Ensuring that all activities are carried out as required throughout the service lifecycle
- Appointing people to the required roles and managing assigned resources
- Working with service owners and other process managers to ensure the smooth running of services
- Monitoring and reporting on process performance
- Identifying opportunities for and making improvements to the process.

1.5.3 Process practitioner

A process practitioner is responsible for carrying out one or more process activities. This role may be assigned to the same person carrying the process manager role, if appropriate. Responsibilities typically include:

- Carrying out one or more activities of a process
- Understanding how his or her role contributes to the overall delivery of service and creation of value for the business
- Working with other stakeholders, such as line managers, co-workers, users and customers, to ensure that their contributions are effective
- Ensuring that the inputs, outputs and interfaces for his or her activities are correct
- Creating or updating records to show that activities have been carried out correctly.

1.5.4 Service owner

The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and is accountable to the IT director or service management director for the delivery of a specific IT service. The service owner's accountability for a specific service within an organization is independent of where the underpinning technology components, processes or professional capabilities reside. Service ownership is critical to service management and one person may fulfil the service owner role for more than one service. Key responsibilities include:

- Ensuring that the ongoing service delivery and support meet agreed customer requirements via effective service monitoring and performance

- Working with business relationship management to ensure that the service provider can meet customer requirements
- Ensuring consistent and appropriate communication with customers for service-related enquiries and issues
- Representing the service across the organization; for example, by attending change advisory board meetings
- Serving as the point of escalation (notification) for major incidents relating to the service
- Participating in internal and external service review meetings
- Participating in negotiating SLAs and operational level agreements (OLAs) relating to the service
- Identifying opportunities for, and making, improvements to the service.

The service owner is responsible for continual improvement and the management of change affecting the service under their care. The service owner is a primary stakeholder in all of the underlying IT processes which enable or support the service they own.

1.5.5 The RACI model

the RACI model or 'authority matrix' can be used to define the roles and responsibilities in relation to processes and activities.

- Responsible
- Accountable
- Consulted
- Informed

Only one person should be accountable for any process or individual activity, although several people may be responsible for executing parts of the activity.

1.6 Planning, protection and optimization within the context of the service lifecycle

1.6.1 Service design value to the business

- Improved alignment of IT service provision with the business's goals and its evolving needs
- Prioritization of all IT activities based on business impact and urgency
- Increased business productivity and profitability through the increased efficiency and effectiveness of IT processes
- Competitive advantage through the exploitation and innovation of IT infrastructure as a whole.

1.6.2 Planning, protection and optimization supporting the service lifecycle

The processes used within PPO operate across the entire service lifecycle. These processes must be linked together, with clearly defined interfaces, to manage, design, support and maintain services, IT infrastructures, environments, applications and data:

- Capacity management
- Availability management
- IT service continuity management (ITSCM)
- Demand management
- Information security management

Each of the above processes must interface with the design coordination process, which ensures that services, service management information systems, architectures, technology, processes, information and metrics are designed consistently to meet current and evolving business outcomes and requirements. The design coordination process coordinates all design activities, including resources and capabilities, across all projects, changes, suppliers and support teams, managing schedules and conflicts where necessary.

2 Capacity management

2.1 Purpose and objectives

The purpose of capacity management is to provide centrally coordinated management of all capacity- and performance related issues, for both services and resources.

The objectives of capacity management relate to both capacity and performance, and include:

- Production and maintenance of a capacity plan based on the current and future business needs, assessing the impact of proposed changes
- Providing advice and guidance to the business, IT and service management disciplines including incident, problem and change
- Ensuring that agreed performance targets for both services and resources are achieved or exceeded
- Assisting with the diagnosis and resolution of capacity- and performance-related incidents and problems
- Assessing the impact of all changes on the capacity plan
- Implementation of cost-justified proactive measures to improve service performance.

2.2 Scope

Capacity management is applicable at all stages of the service lifecycle and covers:

- Technological aspects of the IT infrastructure (e.g. network support, server support, operations management) for all supported environments, including both hardware and software. Note that day-to-day support is undertaken by the relevant technology function.
- Human resources (e.g. what skilled support staff are required to meet the agreed service level agreement (SLA) and operational level agreement (OLA) targets).
- Physical requirements including space planning and environmental systems capacity.
- Provision of end-to-end services to match the business requirements.

To achieve the provision of cost-effective services to the business, capacity management must understand:

- How the business currently operates, its requirements and the effect of patterns of business activity on the day-to-day operation of services
- Service strategy, the impact of new technology and its appropriate use in the provision of new or enhanced services; using information provided in the service portfolio on future business requirements and plans
- Service targets and the link with SLAs and standard operating procedures
- Capacity and performance capabilities in all areas of IT technology (infrastructure, data, applications and environment).

The capacity management process includes:

- Understanding and forecasting the agreed current and future levels of service provision, supported by the production of the capacity plan
- Monitoring and reporting on service usage and performance by considering PBA and service level plans and capturing statistics on performance, utilization and throughput for all components and areas of IT technology
- Proactively undertaking service and component improvements where cost-justifiable and, where necessary, influencing behaviour through demand management
- Increasing the efficiency of the existing technology by undertaking tuning activities
- Assisting other areas of service management (e.g. incident management) when performance issues occur.

Data gathered by capacity management gathers includes component statistics, end-to-end service performance and detailed future business requirements. This information is used to support cost-effective service provision by determining:

- Which components to upgrade (e.g. bandwidth, storage or processor power)
- When to upgrade; ideally not too early or too late
- What funding is required for upgrades, interfacing with the financial planning lifecycle.

Capacity management influences many other service management areas; its scope therefore includes good communication and interfaces with:

- Service strategy
- Change management
- Service level management (SLM)
- Incident and problem management
- ITSCM

2.3 Value to the business

Capacity management improves the performance and availability of the IT service the business needs by helping to reduce incidents and problems related to capacity and performance. It ensures that capacity is provided in the most cost-effective manner and improves budgeting through the use of a forward-looking capacity plan. Good capacity management also supports the efficient and effective design and transition of new or changed services.

2.4 Policies, principles and basic concepts

Capacity management supports the evolving business needs through the provision of cost-effective capacity. This is achieved by balancing:

- Costs against the resources required, ensuring money is not wasted on surplus capacity, and additional costs are not incurred because of the need for panic-buying
- Supply against demand, providing adequate capacity to satisfy the demand predictions or, in cases of excessive demand, influencing customer and user behaviour.

To ensure that the complete range of information required to support all aspects of service provision is available, capacity management is supported by three sub-processes:

- Business capacity management
- Service capacity management
- Component capacity management

A capacity management information system (CMIS) provides a set of tools, data and information gathered from the subprocesses to support capacity management. This information is used to create a capacity plan. The capacity plan documents a planned approach to the timing of upgrades, along with the technological requirements necessary to support the business over the next one to two years.

2.5 Process activities, methods and techniques

Proactive activities include:

- Pre-empting performance issues by monitoring current and predicted utilization, taking necessary action before issues occur and introducing improvements to service performance where cost-justifiable
- Planning the timely implementation of future upgrades and enhancements, based on trend analysis undertaken on component utilization data and the knowledge of component thresholds
- Reducing the risk of SLA or target breaches by planned, timely, budgeted upgrades and by maximizing the performance of existing infrastructure by tuning and optimizing activities

Reactive activities include:

- Reacting to and assisting with incidents and problems related to capacity or performance
- Monitoring, measuring, reporting and controlling current performance at both component and service levels
- Investigating and correcting capacity-related threshold events.

2.5.1 Business capacity management

The main objective of this sub-process is to understand the changing business needs.

Consideration should be given to new or changed services, to modifying existing service provision, to decommissioning obsolete services and to redeploying the additional capacity effectively.

In order to be successful capacity management needs to be involved at an early stage with all strategic and design activities; namely development of the service strategy, review and improvements to the IT strategy, and the technology architectures used.

Capacity management should be planned and has a significant part to play in the following activities:

- Assist with agreeing SLRs

- Design, procure and amend service configuration
- SLA verification and negotiation support

2.5.2 Service capacity management

The main objective of this sub-process is the continued delivery of end-to-end service in line with the agreed performance determined by the targets set in the SLAs and SLRs. This is achieved by:

- Establishing normal service levels using trend analysis techniques on data collected from service monitoring to ensure that the agreed capacity levels can be met.
- Monitoring and comparing actual end-to-end service performance against predicted workloads and transactions to enable proactive measures to be taken in a timely manner in order to avert failures. This is supplemented by the use of thresholds to provide alerts regarding potential future risks.
- Informing SLM of any near or actual service breaches by comparing normal service levels with exceptional conditions.
- Considering the impact of non-infrastructure-based issues related to poor design or coding of applications.

2.5.3 Component capacity management

This sub-process covers the individual components that are required to deliver the services and includes infrastructure, environment, data and applications.

The objective is that for every component, its performance, current utilization and capacity are understood, so allowing optimum usage of both hardware and software resources in line with the agreed service targets.

2.5.4 Capacity management – underpinning activities

There are several basic activities that underpin all of the three sub-processes; the only difference is the type of data being considered. Business capacity management requires a mapping of the transaction throughput rates that are translated into business volumes. Similarly, transaction throughput is used in conjunction with response times for service capacity management. Component capacity management looks at the utilization data for each individual component.

This underlying set of activities is broken down into four main elements which together safeguard the current operation and identify any changes that will be required in the future.

2.5.4.1 Monitoring

There are two main types of monitoring: utilization and response time.

Utilization is specific to the component and platform. Typical data includes processor, memory and disk utilization, input/output (IO) and transaction rates, queue lengths, response times, database usage and network traffic.

Response time is often included in SLA targets and accurate recording is difficult. This can be overcome by:

- The addition of a specific code within the client and server applications
- The use of robotic software with terminal emulation to provide indications of end-to-end responses
- The use of distributed agent monitoring software or specific passive monitoring systems (referred to as “sniffers”).

2.5.4.2 Analysis

The collected data can be analysed and compared with either a predetermined baseline or the normal utilization and service levels. This enables SLA breaches and near-misses to be identified so that they can be reported and corrective action taken.

Analysis should take into account the usage profile over several periods of time:

- Short term Usually a period of 24 hours
- Medium term One to four weeks
- Long term A period of a year.

2.5.4.3 Tuning

The results of the analysis activities can pinpoint areas in the configuration that may benefit from tuning to provide better utilization of the existing resources, therefore improving the performance of the component or the service. Techniques that can be used include:

- Balancing workload and traffic
- Balancing disk traffic, reducing contention between data by the use of striping
- Locking strategy, determining when and how locks should be applied
- Efficient memory use.

2.5.4.4 Implementation

Formal change management should be involved in any implementation of changes that are a result of the monitoring, analysis and tuning activities, as these types of change can have a serious impact on the provision of live services if they are incorrect or not proven.

2.5.5 Threshold management and control

The management and control of service and component thresholds is fundamental to the effective delivery of services to meet their agreed service levels. It ensures that:

- Service and component thresholds are maintained at appropriate levels, are monitored, and alerts and warnings are generated when breaches occur
- Analysis is carried out to enable remedial action to be taken, where justified, and to ensure that the situation does not occur again
- Potential future breaches can be predicted to allow action to be taken to avoid the breach.

All thresholds should be set below the level at which the component or service is over-utilized, or below the targets in the SLAs.

Workload management involves the optimization of infrastructure components and resources to maintain or improve performance. Actions include:

- Rescheduling of services or workload to utilize any additional capacity that is available during troughs in the service
- Balancing of utilization by moving a workload or service to a different part of the infrastructure
- Using 'virtualization' to allocate resources dynamically
- Applying demand management techniques.

2.5.6 Demand management

Demand management seeks to understand future demand for services in the form of PBA; these are then used by capacity management to understand the resulting demand for supporting services and underlying service assets. Demand management might be required to resolve:

- A short-term increase in demand as a result of partial failure of a critical resource
- A long-term solution when expensive upgrades are not cost-justifiable.

An understanding of the levels of resource utilization and scheduling is required before demand management can be applied.

2.5.7 Modelling and trending

Modelling provides accurate forecasts of future capacity requirements based on current utilization and the predicted growth. Different types of modelling include:

- Baselineing
- Trend analysis
- Analytical modelling
- Simulation modelling

2.5.8 Application sizing

This technique is used in the design stage for new or significantly enhanced services and predicts the resource requirements for the live operation of the service. It considers the SLRs and helps by advising on the appropriate technologies and products necessary to meet the levels of service required

The activity considers the potential impact of the design on any other existing services and SLAs. It also covers software that has been developed externally.

2.6 Triggers, inputs, outputs and interfaces

The capacity management process is triggered in a variety of ways, which include review and revision of:

- Strategies and plans (IT and business)
- Designs, SLAs, OLAs, contracts and agreements

- Current capacity and performance, together with future requirements
- Trends, models and exception reports.

Inputs include:

- Current and future business requirements, including the financial implications of changes
- Plans and budgets relating to service and IT strategies for all supported technologies
- Capacity and performance information on existing and new technologies provided from suppliers and manufacturers
- Specific capacity-related information held within the CMIS, including performance and workload information
- Service management information including performance issues identified in the incident and problem management processes, together with details of the services provided, to be found in the service portfolio, service catalogue, SLAs and SLRs
- Details from the configuration management system, and change management.

Outputs include:

- The CMIS, which is the repository for all capacity information
- Capacity plan
- Reports, including service performance, workload analysis and forecasts.
- Thresholds, alerts and events.

Key interfaces include:

- Availability management
- Service level management
- ITSCM
- Incident and problem management
- Demand management

2.7 Information management

The aim of the CMIS is to store the relevant capacity and performance information to support the capacity management process. These reports provide valuable information to many IT and service management processes, with the reports often being consolidated and held centrally (e.g. on an intranet site), so that they can be easily accessed. The reports should include:

- Component-based reports
- Service-based reports
- Exception reports
- Predictive and forecast reports

The CMIS should hold data from all areas of technology, and all components that make up the IT services, to enable analysis of technical and management reporting. The data types that should be stored within the CMIS include:

- Business data
- Service data
- Component data
- Financial data

2.8 Critical success factors and key performance indicators

- CSF Accurate business forecasts:
 - o KPI Timely incorporation of business plans into the capacity plan
 - o KPI Reduction in the number of variances from the business plans and capacity plans
- CSF Knowledge of current and future technologies:
 - o KPI Timely justification and implementation of new technology in line with business requirements (time, cost and functionality)
 - o KPI Reduction in the use of old technology
- CSF Ability to demonstrate cost-effectiveness:
 - o KPI Reduction in the over-capacity of IT
 - o KPI Reduction in business disruption caused by a lack of adequate IT capacity.

2.9 Challenges and risks

The major challenges are data-related:

- It can be difficult to obtain data from the business about future growth and new initiatives
- The diversity of data produced by the different tools monitoring the component capacity can be difficult to consolidate when trying to provide accurate forecasts
- The huge volume of data from the sub-processes increases the complexity of the analysis that is required.

Risks include:

- Lack of commitment and funding from business and senior management
- Concentration of information at the component level owing to the inability to obtain relevant business information, so distorting the overall process
- Too much technical data, with the resulting reports not being sufficiently business-focused to provide meaningful information
- Poor performance of services owing to inadequate knowledge of potential usage and pattern of demand or the lack of involvement of capacity management at the design stages
- Perception by customers that the service is unsuitable because of performance issues
- Inability to re-allocate surplus capacity because specific assets are being procured for each system and cannot be shared
- Dependencies on single parts of the infrastructure, causing overloading and reducing the ability to utilize components with spare capacity.

2.10 Roles and responsibilities

2.10.1 Capacity management process owner

- Carrying out the generic process owner role for the capacity management process
- Working with managers of all functions to ensure acceptance of the process for all capacity- and performance-related issues, regardless of the specific technology involved
- Working with other process owners to ensure an integrated approach to the design, transition and operation of capacity management, availability management, ITSCM and information security management
- Monitoring and reporting on capacity management process performance
- Making improvements to the capacity management process.

2.10.2 Capacity management process manager

- Carrying out the generic process manager role for the capacity management process
- Being aware of and exploiting new technology to improve the cost-justified provision of capacity and its monitoring to meet current and future business needs
- Understanding, assessing and, in conjunction with the service level manager, negotiating with the business the capacity requirements to support current, new, and enhanced services
- Coordinating the production of periodic reports on current usage, trends and forecasts for use by SLM, the business and IT management
- Maintaining an up-to-date knowledge of technology, its current and future use, and predicting upgrades and purchasing requirements for the organization, which are presented in the form of a capacity plan
- Promoting and using techniques such as optimization, tuning, application sizing and performance testing, to enable the provision of adequate capacity to meet the business needs
- Involvement with other service management processes (e.g. availability, change, incident and problem management).

3 Availability management

3.1 Purpose and objectives

The purpose of availability management is to ensure that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost-effective and timely manner. Availability management is concerned with meeting both the current and future availability needs of the business. The main objectives of availability management include:

- Delivery of business and customer benefits by proactively improving the IT infrastructure, services and support organization
- Measuring and monitoring to ensure the agreed levels of availability are consistently met or exceeded
- Producing and maintaining a plan for current and future availability requirements
- Assisting with the diagnosis and resolution of availability related incidents and problems
- Assessing the impact of all changes on the availability plan -Interacting with other service management areas, providing support and guidance on all availability-related issues (e.g. change, capacity, incident).

3.2 Scope

The availability management process covers all aspects of component and IT service availability from the business perspective throughout the complete lifecycle of the service. To accomplish this, availability management must consider and include:

- Design, implementation, measurement, management and improvement of IT service and component availability
- Current and future business processes, plans, priorities and their related service targets for availability
- Understanding of the IT infrastructure, data, applications and environment and how this relates to the current IT service operation and delivery.

The scope of the process covers:

- Monitoring of all aspects of availability, reliability and maintainability, including appropriate alarms, escalations and automatic recovery scripts
- Availability methods and techniques including risk assessment, availability calculation, measurement, reporting, and the testing of component resilience and failover mechanisms
- Understanding the levels of availability required by the business and influencing the design of services and components to meet those demands
- Producing an availability plan (to ensure services meet current SLAs and future SLRs) that identifies cost-justifiable improvements in the provision of availability to meet business needs
- Assisting in the identification and resolution of availability related incidents and problems.

3.3 Value to the business

The business requires that its IT services are both available and reliable in order to retain its market reputation and gain customer loyalty. Availability management is essential in the provision of the required levels of service availability to ensure quality of service and fulfil the business objectives.

3.4 Policies, principles and basic concepts

Availability management policies should consider both the reactive and proactive activities that are required to support the operational levels needed by the business.

The availability management process must be involved at all stages of the service lifecycle, to ensure that appropriate availability and resilience are designed into services and components from the initial design stages.

The following principles underpin the availability management process and its focus:

- Policies should be established regarding the criteria to be used to define availability and unavailability of a service or component and how each will be measured.
- There is a direct correlation between service availability and customer satisfaction, which is often influenced by the perceptions and expectations of the customers and users. How the service provider reacts to and handles failures is therefore important.
- The relationship between the IT services provided and the operation of the business should be clearly understood to facilitate improvements in availability.
- Eradication of weak components and single points of failure (SPOF) can increase the level of service availability.
- Service availability will be improved if a proactive approach is taken to reducing the risk of service failure. Involvement at the design stages for new or changed services not only provides cost-effective service availability but also reduces additional cost incurred by the later addition of extra resilience.

The basic concepts of availability management are:

- Reactive element
- Proactive element
- Component availability
- Service availability

The main aspects of a service (including service, component or configuration items (CIs)) that are reported on as a result of monitoring, measuring and analysis are:

- Availability
- Reliability
- Maintainability
- Serviceability

Types of availability that support IT services are:

- High availability
- Fault tolerance
- Continuous operation
- Continuous availability

The process covers the following key activities:

- Determining all the availability requirements for new and enhanced IT services, and identifying the VBFs in conjunction with the business and ITSCM
- Together with ITSCM, assessing the impact of component failure on the IT services and providing solutions to minimize business impact
- Defining, agreeing and documenting suitable targets for IT infrastructure components relating to IT service availability for inclusion in agreements
- Establishing measures, and reporting of availability, reliability and maintainability from the perspective of the business, user and IT support
- Monitoring and reviewing of availability, determining the cause of unacceptable levels, and predicting future impacts using trend analysis
- Production and maintenance of an availability plan.

3.5 Process activities, methods and techniques

The availability management process consists of both reactive and proactive activities and relies heavily on the ability to measure service and component availability to enable improvements to be made. The measurements obtained and assessed should take into account the following perspectives:

- Business
- User
- IT service provider

3.5.1 Reactive activities of availability management

The monitoring, measurement and analysis of availability is at the core of the process and data gathered day to day is assessed against the targets that have been set and agreed in the SLAs, OLAs and underpinning contracts. The measurements taken are presented in reports at the service level review meetings, enabling:

- Establishment of measures and agreement of targets with the business
- Monitoring of actual availability versus targets
- Identification of unacceptable levels of unavailability, impacting business and users
- Review of availability with the IT support organization
- Continual improvement activities to optimize availability.

Traditional measures of availability, developed from the IT service provider's perspective, concentrate on components and include:

- Percentage available
- Percentage unavailable
- Duration
- Frequency of failure
- Impact of failure

The user's perspective, considering frequency, duration and impact of downtime on a service, reflects how unavailability affects the business operation. Measures to achieve this are:

- Impact by user minutes lost
- Impact by business transaction

The business perspective needs measurements to highlight areas where unavailability has the highest impact on the business operation:

- Availability is assessed in relation to VBFs, enabling the consequences of failure on the business to be understood.
- Availability is reported in a way that promotes a common understanding, by the business and the service provider, of the measurements taken.

3.5.1.1 Unavailability analysis

- Investigation of incidents, with remedial actions implemented in the availability plan or the service improvement plan (SIP)
- Production of trends allowing further focus on areas of most impact or disruption
- Cost of unavailability balanced with the cost of availability (e.g. additional resilience) for VBFs
- Assessment of the ability of the IT service to deliver the required level of availability for new and enhanced services
- Provision of the costs of failure by the number of transactions impacted so as to be easily understood by both business and IT
- Financial investment supported by monetary cost of failure, includes tangible costs (e.g. lost revenue, lost user productivity) and intangible costs (e.g. loss of customers, damage to business reputation).

3.5.1.2 Expanded incident lifecycle

- Incident detection
- Incident diagnosis
- Incident repair
- Incident recovery
- Incident restoration

3.5.1.3 Service failure analysis

Service failure analysis (SFA) is a technique that uses a planned approach for identifying the causes of service outages and the areas (technical, process, procedural and employment of tools) that could be enhanced to reduce the risk of recurrence. The activity provides:

- A programme of improvement opportunities, including enhancement of availability levels, service quality and user perception
- Visible support to the business, cross-functional team working, increased in-house skills and competencies, and independent 'health checks'.

The structured approach includes the following stages:

- Select opportunity
- Scope assignment
- Plan assignment
- Build hypotheses
- Analyse key data
- Interview key personnel
- Findings and conclusions
- Recommendations
- Report
- Validation.

3.5.2 Proactive activities of availability management

Successful availability management is built upon the range and quality of proactive methods and techniques utilized by the process:

- Vital business function identification
- Designing for availability
- Base products and components
- Systems management
- Management processes
- High-availability design
- Special solutions with full redundancy
- Component failure impact analysis
- Single point of failure analysis
- Fault tree analysis
- Modelling
- Risk analysis and management
- Availability testing schedule
- Planned and preventive maintenance
- Production of the projected service outage document
- Continual review and improvement

3.6 Triggers, inputs, outputs and interfaces

Triggers include:

- New or changed business needs, services or targets within agreements
- Breaches and events, alerts and exception reports related to availability of the service or components
- Changes as a result of reviews and revisions to availability management forecasts, reports and plans; business and IT plans, designs and strategies
- Changes in risk or impact that affect business processes, VBFs, IT services or components
- Explanation of service achievements and setting of availability targets to support SLM.

Inputs include:

- Business information from strategies, current and future availability requirements, output from BIA for IT services and VBFs, and strategic and financial plans
- Risk register and previous risk analysis and assessment reports
- Service information from service portfolio, service catalogue, service targets (within SLAs, OLAs and contracts), service breaches and results from service reviews
- Information from other service management processes, including incidents, problems and details from financial, change, release and configuration management that can contribute to the availability management activities
- Technology information from the configuration management system (CMS) showing the components that contribute to each service, and details of the component's capability to support given availability requirements
- Availability management information system (AMIS) and measurements and achievements relating to past performance in the form of reports
- Information on unavailability and failures from incidents and problems.

Outputs include:

- AMIS, availability plan and projected service outage reports
- Schedules for planned preventive maintenance and testing
- Requirements for monitoring, management and reporting to allow the detection, appropriate action, recording and reporting of deviations
- Reporting of achievements against targets
- Reviews and reports relating to risk and an up-to-date risk register
- Details of proactive approaches used to prevent or minimize the adverse impact of component failure through extra resilience
- Availability design criteria and proposed targets for new or changed services
- Improvement actions to incorporate into a SIP.

Key interfaces include:

- Incident and problem management

- Capacity management
- ITSCM
- SLM

3.7 Information management

The availability management process should maintain an AMIS that contains the measurements and information required to provide appropriate information to the business on the level of IT service provided. It includes:

- Actual versus agreed levels of availability for IT services, as experienced by the business and users
- Activities to address shortfalls in availability for existing IT services, including associated costs and benefits where required
- Details of availability requirements for changes to existing IT services and for new IT services, including options and costs to meet these new requirements
- Details of service failure analysis assignments, to provide a forward schedule of these and to ensure that they are proactively improving the availability of IT services
- A technology futures section to provide an indication of the potential benefits and opportunities to exploit any planned technology upgrades.

3.8 Critical success factors and key performance indicators

- CSF Manage availability and reliability of IT service:
 - o KPI Percentage reduction in the unavailability of services and components
 - o KPI Percentage improvement in overall end-to-end availability of service
- CSF Satisfy business needs for access to IT services:
 - o KPI Percentage reduction of the cost of business overtime due to unavailable IT
 - o KPI Percentage reduction in critical time failures
- CSF Availability of IT infrastructure and applications provided at optimum costs:
 - o KPI Percentage reduction in the cost of unavailability
 - o KPI Reduced time taken to review system resilience.

3.9 Challenges and risks

The major challenges include:

- Meeting the expectations of customers, users and business and senior management; these often exceed the agreed service hours and require recovery of services within minutes, without considering the level of investment required to achieve this
- Convincing the business and senior management that investment is needed for proactive availability measures before a major outage
- Obtaining good-quality information regarding the current and future business needs for IT services
- Collecting and recording meaningful availability data within the AMIS, despite the fact that most organizations operate using many different technologies, tools and data formats.

Major risks include:

- Lack of commitment from the business to the availability management process, and the provision of information regarding future business strategies and plans
- The availability management process lacks commitment, resources and/or budget from senior management
- The process focuses too much on the technology, to the detriment of the end-to-end delivery of services to the business
- The detailed level of reporting makes it very labour-intensive
- The AMIS is maintained in isolation and data is not consistent or shared with related processes such as ITSCM, security management, and capacity management.

3.10 Roles and responsibilities

3.10.1 Availability management process owner

- Carrying out the generic process owner role for the availability management process
- Working with managers of all functions to ensure acceptance of the availability management process for all availability-related issues, regardless of the specific technology involved
- Working with other process owners to ensure an integrated approach is taken to the design, transition and operation of availability management, SLM, capacity management, ITSCM and information security management
- Monitoring and reporting on the performance of the availability management process
- Making improvements to the availability management process.

3.10.2 Availability management process manager

- Carrying out the generic process manager role for the availability management process
- Participating in the design and improvement of the IT infrastructure, ensuring that it can support the availability levels required by the business and agreed upon in the SLAs
- During the design for all types of changes (services or infrastructure design):
 - o Assessing the impact of the changes and attending change advisory board meetings where appropriate
 - o Ensuring that the agreed levels of availability can be delivered to the business
 - o Specifying the reliability, maintainability and serviceability requirements for components supplied by internal and external suppliers
 - o Creating appropriate availability and recovery design criteria
 - o Maintaining and implementing a schedule of availability testing, ensuring all major changes are tested
- Regularly reviewing the AMIS and availability plan, and setting up audits for the availability management process
- Monitoring and reporting the actual levels of availability compared with the SLA targets
- Assisting with other service management activities, including:
 - o Investigation and diagnosis of incidents and problems

- Specification of a new or enhanced event management system
- Working with financial management to ensure the cost-effective provision of availability
- Conducting risk assessments in conjunction with ITSCM and security management.

4 IT service continuity management

4.1 Purpose and objectives

The purpose of the IT service continuity management (ITSCM) process is to support the overall business continuity management (BCM) process by ensuring that, by managing the risks that could seriously affect IT services, the IT service provider can always provide the minimum agreed business continuity-related service levels.

In support of and alignment with the BCM process, ITSCM uses formal risk assessment and management techniques to reduce risks to IT services to agreed acceptable levels, and to plan and prepare for the recovery of IT services.

The objectives of ITSCM are to:

- Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets
- Maintain a set of IT service continuity plans and IT recovery plans that support the overall business continuity plans (BCPs) of the organization
- Complete regular BIA exercises to ensure that all continuity plans are maintained in line with changing business impacts and requirements
- Conduct regular risk analysis and management exercises, particularly in conjunction with the business and the availability management and security management processes, that manage IT services within an agreed level of business risk
- Provide advice and guidance to all other areas of the business, and IT on all issues relating to continuity and recovery
- Assess the impact of all changes on the IT service continuity plans and IT recovery plans
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so
- Negotiate and agree the necessary contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the supplier management process.

4.2 Scope

ITSCM focuses on those events that the business considers significant enough to be considered a 'disaster'. Less significant events will be dealt with as part of the incident management process.

The scope of ITSCM within an organization is determined by the organizational structure, culture and strategic direction (both business and technology) in terms of the services provided and how these develop and change over time. ITSCM primarily considers the IT assets and configurations that support the business processes.

The ITSCM process includes:

- Agreement of the scope of the ITSCM process and the policies adopted

- BIA to quantify the impact that loss of IT service would have on the business
- Risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality
- Production of an overall ITSCM strategy, integrated into the BCM strategy
- Production of an ITSCM plan, integrated with the overall BCM plans
- Testing the plans
- Ongoing operation and maintenance of the plans
- Providing strategic direction.

4.3 Value to the business

ITSCM provides an invaluable role in supporting the business continuity planning process. ITSCM should be driven by business risk as identified by business continuity planning, and ensures that the recovery arrangements for IT services are aligned with identified business impacts, risks and needs.

IT service continuity supports the business in limiting organizational damage to a minimum in the event of predictable as well as unpredictable crises.

4.4 Policies, principles and basic concepts

A lifecycle approach should be adopted for the setting up and operation of an ITSCM process, from initiation through to continual assurance that the protection provided by the plan is current and reflects all changes to services and service levels.

ITSCM is a cyclical process that occurs throughout the lifecycle to ensure that once service continuity and recovery plans have been developed, they are kept aligned with BCPs and business priorities.

The initiation and requirements stages are principally BCM activities. ITSCM should be involved in these stages only to support the BCM activities and to understand the relationship between the business processes and the impacts caused on them by loss of IT service. As a result of these initial BIA and risk strategy, and the first real ITSCM task is to produce an ITSCM strategy that underpins the BCM strategy and its needs.

The only way of implementing effective ITSCM is through the identification of critical business processes and the analysis and coordination of the required technology and supporting IT services.

4.5 Process activities, methods and techniques

4.5.1 Stage 1 – Initiation

The initiation process covers the whole organization and consists of the following activities:

- Policy setting
- Specifying terms of reference and scope
- Allocating resources
- Defining the project organization and control structure

- Agreeing project and quality plans

4.5.2 Stage 2 – Requirements and strategy

Ascertaining the business requirements for IT service continuity is critical in order to determine how well an organization will survive a business interruption or disaster and the costs that will be incurred.

4.5.2.1 Requirements – business impact analysis

The purpose of a BIA is to quantify the impact on the business that loss of service would have. The BIA identifies:

- The form that the damage or loss may take
- How and when the degree of damage or loss is likely to escalate after a service disruption
- The staffing, skills, facilities and services necessary to enable critical and essential business processes to continue operating at a minimum acceptable level
- The time within which minimum levels of staffing, facilities and services should be recovered
- The time within which all required business processes and supporting staff, facilities and services should be fully recovered
- The relative business recovery priority for each of the IT services.

4.5.2.2 Requirements – risk analysis

Risk analysis is a technique that can also be used to assess and reduce the chance of normal operational incidents occurring. It is used by availability management to ensure the required availability and reliability levels can be maintained. Risk analysis is also a key aspect of information security management.

Risk analysis is the assessment of the risks that may give rise to service disruption or security violation. Risk management is concerned with identifying appropriate risk responses or cost-justifiable countermeasures to combat those risks.

A standard methodology, such as the Management of Risk (M_o_R), should be used to assess and manage risks within an organization. The M_o_R process identifies four main steps which describe the inputs, outputs and activities that ensure that risks are controlled:

- Identify
- Assess
- Plan
- Implement

4.5.2.3 IT service continuity strategy

The results of the BIA and the risk analysis enable appropriate business and IT service continuity strategies to be produced in line with the business needs. The strategy will be an optimum balance of risk reduction and recovery or continuity options.

Preventive risk reduction efforts should be concentrated on those services that have been identified as high impact in the short term within the BIA.

Risk response measures

Most organizations will have to adopt a balanced approach where risk reduction and recovery are complementary and both are required.

As a general rule, invocation of a recovery capability should only be as a last resort. Ideally, an organization should proactively assess all of the risks to reduce the potential requirement to recover the business. Typical risk reduction measures include:

- Installation of an uninterruptible power supply (UPS) and backup power to computers
- Fault-tolerant systems for critical applications
- RAID arrays and disk mirroring for LAN servers
- Spare equipment and components to be used in the event of equipment or component failure
- The elimination of single points of failure, such as single access networks
- Resilient IT systems and networks
- Outsourcing services to more than one provider
- Greater physical and IT-based security controls
- Better controls to detect service disruptions
- A comprehensive backup and recovery strategy, including off-site storage.

ITSCM recovery options

An organization's ITSCM strategy is a balance between the cost of risk reduction measures and recovery options to support the recovery of critical business processes within agreed timescales.

- Manual workarounds
- Reciprocal arrangements
- Gradual recovery
- Intermediate recovery
- Fast recovery
- Immediate recovery

4.5.3 Stage 3 – Implementation

Once the strategy has been approved, the IT service continuity management plans need to be produced in line with the BCPs. The ITSCM plans are developed to enable the necessary information for critical systems, services and facilities to either continue to be provided or to be reinstated within an acceptable period to the business.

Generally the BCPs rely on the availability of IT services, facilities and resources. As a consequence of this, ITSCM plans need to address all activities to ensure that the required services, facilities and

resources are delivered in an acceptable operational state and are 'fit for purpose' when accepted by the business.

Management of the distribution of the plans is important to ensure that copies are available to key staff at all times. The plans should be controlled documents (with formalized documents maintained under change management and configuration management control) to ensure that only the latest versions are available and in use.

Additionally, plans that will need to be integrated with the main BCP are:

- Emergency response plan
- Damage assessment plan
- Salvage plan
- Vital records plan
- Crisis management and public relations plan
- Accommodation and services plan
- Security plan
- Personnel plan
- Communication plan
- Finance and administration plan

Finally, each critical business area is responsible for the development of a plan detailing the individuals who will be in the recovery teams and the tasks to be undertaken on invocation of recovery arrangements. Typically, a separate SLA with alternative targets is agreed if it is running at a recovery site following a disaster.

4.5.3.1 Organization planning

During the disaster recovery process, the organizational structure will inevitably be different from normal operation and will be based around:

- Executive
- Coordination
- Recovery

4.5.3.2 Testing

Experience has shown that recovery plans that have not been fully tested do not work as intended, if at all. There are four basic types of tests that can be undertaken:

- Walk-through tests
- Full tests
- Partial tests
- Scenario tests

4.5.4 Stage 4 – Ongoing operation

This stage consists of:

- Education, awareness and training
- Review
- Testing
- Change management

Invocation is the ultimate test of the business continuity and ITSCM plans. If all the preparatory work has been successfully completed, and plans have been developed and tested, then an invocation of the BCPs should be a straightforward process. The decision to invoke needs to take into account:

- The extent of the damage and scope of the potential invocation
- The likely length of the disruption and unavailability of premises and/or services
- The time of day/month/year and the potential business impact.

The ITSCM plan should include details of activities that need to be undertaken, including:

- Retrieval of backup tapes or use of data vaulting to retrieve data
- Retrieval of essential documentation, procedures, workstation images etc. stored off-site
- Mobilization of the appropriate technical personnel to go to the recovery site to commence the recovery of required systems and services
- Contacting and alerting telecommunications suppliers, support services, application vendors etc. who may be required to act or provide assistance in the recovery process.

Following invocation, once the recovery has been completed, a return to normal must be carefully planned and undertaken in a controlled fashion.

4.6 Triggers, inputs, outputs and interfaces

Triggers include:

- New or changed business needs or services
- New or changed targets within agreements, such as service level requirements (SLRs), SLAs, operational level agreements (OLAs) or contracts
- The occurrence of a major incident that requires assessment for potential invocation of either business or IT continuity plans
- Periodic activities such as the BIA or risk analysis activities, maintenance of continuity plans or other reviewing, revising or reporting activities
- Assessment of changes and attendance at change advisory board meetings
- Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component

- Initiation of tests of continuity and recovery plans.

Inputs include:

- Business information
- IT information
- A business continuity strategy and a set of BCPs
- Service information
- Financial information
- Change information
- Configuration management system (CMS)
- Testing schedules
- IT service continuity plans and test reports

Outputs include:

- A revised ITSCM policy and strategy
- A set of ITSCM plans, including all crisis management, emergency response and disaster recovery plans, together with a set of supporting plans and contracts with recovery service providers
- BIA exercises and reports, in conjunction with BCM and the business
- Risk analysis and management reviews and reports, in conjunction with the business, availability management and security management
- An ITSCM testing schedule
- ITSCM test scenarios
- ITSCM test reports and reviews. Forecasts and predictive reports are used by all areas to analyse, predict and forecast particular business and IT scenarios and their potential solutions.

ITSCM integrates and interfaces with all other processes. Key interfaces include:

- Change management
- Incident and problem management
- Availability management
- Service level management
- Capacity management
- Configuration management
- Information security management

4.7 Information management

ITSCM needs to record all of the information necessary to maintain a comprehensive set of ITSCM plans. The information held by ITSCM should include:

- Information from the latest version of the BIA
- A risk register, including risk assessment and risk responses
- The latest version of the BCM strategy and BCPs
- Details of completed tests and a schedule of all planned tests
- Details of all ITSCM plans and their contents, and all other plans associated with ITSCM
- Details of all existing recovery facilities, recovery suppliers and partners, recovery agreements and contracts, spare and alternative equipment
- Details of all backup and recovery processes, schedules, systems and media and their respective locations.

4.8 Critical success factors and key performance indicators

- CSF IT services are delivered and can be recovered to meet business objectives:
 - KPI Increase in success of regular audits of the ITSCM plans to ensure that, at all times, the agreed recovery requirements of the business can be achieved
 - KPI Regular, successful validation that all service recovery targets are agreed and documented in SLAs and are achievable within the ITSCM plans
 - KPI Regular and comprehensive testing of ITSCM plans achieved consistently
 - KPI Overall reduction in the risk and impact of possible failure of IT services
- CSF Awareness throughout the organization of the business and IT service continuity plans:
 - KPI Increase in validated awareness of business impact, needs and requirements throughout IT
 - KPI Increase in successful test results ensuring that all IT service areas and staff are prepared and able to respond to an invocation of the ITSCM plans.

4.9 Challenges and risks

One of the major challenges facing ITSCM is providing appropriate plans where there is no BCM process. If a BCM process is established, the challenge becomes one of alignment and integration.

Having achieved that alignment, the challenge becomes one of keeping them aligned by management and control of business and IT change. It is essential, therefore, that all documents and plans are maintained under strict change management and configuration management control.

Major risks include:

- Lack of commitment from the business to the ITSCM processes and procedures
- Lack of commitment from the business and a lack of appropriate information on future plans and strategies
- Lack of senior management commitment or a lack of resources and/or budget for the ITSCM process
- The processes focus too much on the technology issues and not enough on the IT services and the needs and priorities of the business

- Risk analysis and management are conducted in isolation and not in conjunction with availability management and security management
- ITSCM plans and information become out of date and lose alignment with the information and plans of the business and BCM.

4.10 Roles and responsibilities

4.10.1 IT service continuity management process owner

- Carrying out the generic process owner role for the ITSCM process
- Working with the business to ensure proper coordination and communication between business continuity management and ITSCM
- Working with managers of all functions to ensure acceptance of the ITSCM process as the single point of coordination for all IT service continuity-related issues, regardless of the specific technology involved
- Working with other process owners to ensure an integrated approach is taken to the design, transition and operation of ITSCM, information security management, availability management and business continuity management
- Monitoring and reporting on ITSCM process performance
- Making improvements to the ITSCM process.

4.10.2 IT service continuity management process manager

- Carrying out the generic process manager role for the ITSCM process and implementing and maintaining the ITSCM process
- Performing business impact analyses and risk assessment for all existing and new services
- Ensuring that all ITSCM plans, risks and activities underpin and align with all BCM plans, risks and activities, and are capable of meeting the agreed and documented targets under any circumstances
- Developing and maintaining the organization's continuity strategy, assessing potential service continuity issues and invoking the service continuity plan if necessary
- Developing and managing ITSCM plans to ensure that the recovery objectives of the business can be achieved; undertaking regular reviews of the plans and performing post-mortem reviews of service continuity tests and invocations; and instigating corrective actions where required
- Maintaining a comprehensive IT testing schedule, including testing all continuity plans in line with business requirements and after every major business change
- Communicating and maintaining awareness of ITSCM objectives within the business areas supported and IT service areas
- Negotiating and managing contracts with providers of third-party recovery services
- Assessing changes and attending change advisory board meetings when appropriate.

5 Information security management

5.1 Purpose and objectives

The purpose of the information security management process is to align IT security with business security and ensure that the confidentiality, integrity and availability of the organization's assets, information, data and IT services always match the agreed needs of the business.

The objective of information security management is to protect the interests of those relying on information (and the systems that process and deliver the information) from harm as a result of failures in:

- Confidentiality
- Integrity
- Availability
- Authenticity and non-repudiation

5.2 Scope

The scope of information security management must cover the establishment and maintenance of the information security management system (ISMS) to ensure effective governance of information security. The ISMS guides the development and management of a comprehensive information security programme to support business objectives.

5.3 Value to the business

- Providing assurance of business processes by enforcing appropriate security controls in all areas of IT
- Ensuring that the information security policy is maintained and enforced, and that it fulfils the needs of the business security policy and the requirements of corporate governance
- Managing IT risk in line with business and corporate risk management processes and guidelines
- Raising awareness of the need for security within all IT services and assets throughout the organization
- Managing all aspects of IT and information security across all areas of IT and service management.

5.4 Policies, principles and basic concepts

5.4.1 Principles

Information security must be closely aligned with business security and business needs. All of the IT organization's processes must take into account information security considerations.

5.4.2 Information security policy

Information security management activities should be focused on and driven by an information security policy. The policy should describe general information security requirements, objectives and specific policy statements addressing the following:

- Use and misuse of IT assets
- Access control
- Password control
- Email
- Internet
- Antivirus
- Information classification
- Document classification
- Remote access
- Supplier access
- Asset disposal.

Policies should be:

- Widely available to all customers and users
- Referenced in service level requirements (SLRs), SLAs, contracts and agreements
- Authorized by business and IT top executive management
- Endorsed by top management on a regular basis
- Reviewed and, if necessary, revised annually.

5.4.3 Security framework

The information security policy forms part of the security framework, which includes:

- Information security management system (ISMS)
- Comprehensive security strategy
- Effective security organizational structure
- Set of security controls to support the policy
- Monitoring processes
- Plans for security communications and training.

5.4.4 The information security management system

The ISMS is the framework to design, implement, manage, maintain and enforce security processes and controls systematically and consistently throughout the organization. The five elements within the ISMS framework are as follows:

- Control
- Plan
- Implement
- Evaluate
- Maintain

5.4.5 Information security governance

- Strategic alignment

- Value delivery
- Risk management
- Performance management
- Resource management
- Business process assurance

5.5 Process activities, methods and techniques

The key activities within the information security management process are:

- Production, review and revision of an overall information security policy and a set of supporting specific policies
- Communication, implementation and enforcement of the security policies
- Assessment and classification of all information assets and documentation
- Implementation, review, revision and improvement of a set of security controls, risk assessments and responses
- Monitoring and management of all security breaches and major security incidents
- Analysis, reporting and reduction of the volumes and impact of security breaches and incidents
- Scheduling and completion of security reviews, audits and penetration tests.

5.5.1 Security strategy

The information security management process, methods, tools and techniques constitute the security strategy. The security strategy identifies how good security practice will be embedded in every area of the business, through:

- Official training and ongoing communication to raise awareness of the overall security strategy
- Developing methods and process to enable the policies to be followed more easily.

The strategy also identifies how resources will be assigned to track developments in key enabling technologies to ensure the security strategy is maintained and aligned with these developments.

5.5.2 Security controls

Controls should be designed to support and enforce the information security policy and to minimize threats.

Controls are more cost-effective if they are included in the design of all services. This ensures the continued protection of all existing services and that new services are in line with the policy.

Controls are implemented by taking specific measures in response to a threat or incident. The measures can fall into the following categories:

- Preventive
- Reductive

- Detective
- Repressive
- Corrective

5.5.3 Management of security breaches and incidents

For all serious security breaches or incidents an evaluation is necessary to determine:

- What went wrong?
- What caused it?
- How can it be prevented in future?

5.6 Triggers, inputs, outputs and interfaces

Triggers include:

- New or changed business needs or services
- Periodic activities, such as reviewing, revising or reporting, including review and revision of information security management policies, reports and plans
- Service or component security breaches or warnings, events and alerts, including threshold events and exception reports
- New or changed business security policy, corporate governance guidelines or risk management processes
- Review and revision of business and IT plans, designs and strategies.

Inputs include:

- Business, service and IT information
- Risk analysis
- Security incidents and breaches
- Change information and configuration data
- Third-party access

Outputs include:

- An overall information security management policy, together with a set of specific security policies and an SMIS
- Revised security risk assessment processes and reports
- A set of security controls and security classifications, and a set of classified information assets
- Security audits and audit reports and also reviews and reports of security breaches and major incidents
- Security test schedules and plans, including security penetration tests and other security tests and reports
- Policies, processes and procedures for managing partners and suppliers and their access to services and information.

Key interfaces include:

- Incident and problem management
- ITSCM
- SLM
- Change management
- Configuration management
- Availability management
- Capacity management
- Financial management
- Supplier management
- Legal and human resources issues

5.7 Information management

All of the information required by information security management is contained within the SMIS, including all security controls, risks, breaches, processes and reports. This information covers all IT services and components and needs to be integrated and maintained in alignment with all other management information systems.

5.8 Critical success factors and key performance indicators

- CSF Business is protected against security violations:
 - KPI Percentage decrease in the impact of security breaches and incidents
 - KPI Percentage increase in SLA conformance to security clauses
- CSF The determination of a clear and agreed policy, integrated with the needs of the business:
 - KPI Decrease in the number of non-conformances of the information security management process to the business security policy and process
- CSF Security procedures that are justified, appropriate and supported by senior management:
 - KPI Increase in the acceptance and conformance of security procedures
 - KPI Increased support and commitment of senior management
- CSF Information security is an integral part of all IT services and all ITSM processes:
 - KPI Increase in the number of services and processes that conform with security procedures and controls.

5.9 Challenges and risks

One of the biggest challenges in establishing an appropriate information security policy is to ensure that there is adequate support from:

- The business
- Business security
- Senior management (both business and IT).

Once business support is ensured, the key challenge becomes one of alignment and integration. Information security management must ensure that accurate information is obtained from the business security process so that the information security management policies, information and plans can be aligned. When alignment is achieved, the challenge becomes one of maintaining that state. This requires ongoing dialogue between the business and IT.

Risks to the efficiency and effectiveness of the information security management process include:

- Lack of commitment from the business
- Lack of appropriate information from the business on future plans and strategies
- Lack of senior management commitment leading to a lack of resources or budget
- Too much focus by the information security management process on technology issues and not enough on the needs and priorities of the business
- The assessment and management of risk in isolation, and not in conjunction with availability management or ITSCM.

5.10 Roles and responsibilities

5.10.1 Information security management process owner

- Carrying out the generic process owner role for the information security management process
- Working with the business to ensure proper coordination and communication between organizational (business) security management and information security management
- Working with managers of all functions to ensure acceptance of the information security management process as the single point of coordination for all information security-related issues, regardless of the specific technology involved
- Working with other process owners to ensure an integrated approach is taken to the design, transition and operation of information security management, availability management, ITSCM and organizational security management
- Monitoring and reporting on information security management process performance
- Making improvements to the information security management process.

5.10.2 Information security management process manager

- Carrying out the generic process manager role for the information security management process, acting as a focal point for all security issues and promoting education and awareness of security
- Developing and maintaining the information security policy and a supporting set of specific policies and ensuring appropriate authorization, commitment and endorsement from senior IT and business management
- Communicating and publicizing the information security policy to all appropriate parties and ensuring that the information security policy is enforced and adhered to
- Identifying and classifying IT and information assets (configuration items) and the level of control and protection required and assisting with business impact analysis

- Performing security risk analysis and risk management
- Designing, maintaining and reviewing security controls and procedures for operating and maintaining security controls
- Monitoring, managing and reporting on all security breaches and handling security incidents and taking remedial action to prevent recurrence wherever possible
- Ensuring all changes are assessed and attending change advisory board meetings when appropriate
- Ensuring that the confidentiality, integrity and availability of the services are maintained at the levels agreed in the SLAs and that they conform to all relevant statutory requirements
- Ensuring that all access to services by external partners and suppliers is subject to contractual agreements and responsibilities.

6 Demand management

6.1 Purpose and objectives

The purpose of demand management is to understand, anticipate and influence customer demand for services and the provision of capacity to meet these demands. The objectives of demand management are to:

- Identify and analyse patterns of business activity (PBA) to understand the levels of demand that will be placed on a service
- Define and analyse user profiles (UPs) and ensure that the services are designed to meet the PBA
- Work with capacity management to ensure that adequate resources are available at the appropriate levels of capacity to meet the demand for services
- Anticipate and prevent or manage situations where demand for a service exceeds the capacity to deliver it
- Gear the utilization of resources to meet the fluctuating demands for services.

6.2 Scope

The scope of the demand management process is to identify and analyse the PBA that initiate demand for services, and to identify and analyse how different types of user influence the demand for services.

6.3 Value to the business

The main value of demand management is to achieve a balance between the cost of a service and the value of the business outcome it supports.

6.4 Policies, principles and basic concepts

6.4.1 Supply and demand

Strategically, demand management is about matching supply to demand. Therefore, a key element of demand management is to understand the potential demand, and its impact on the service assets. This allows capacity management to manage service assets (and investments) towards optimal performance and cost.

6.4.2 Gearing service assets

The balance of supply and demand is achieved by gearing the service assets to meet the dynamic patterns of demand on services not only by responding to demand as it occurs, but also by anticipating the demand, identifying the signals of increasing or decreasing demand and defining a mechanism to scale investment and supply as required. Managing service assets according to demand involves:

- Identifying the services through service portfolio management (SPM)
- Quantifying the patterns of business activity (PBA)
- Specifying the appropriate architecture for the type and quantity of demand

- Capacity and availability planning to ensure that the right service assets are available at the right time and are performing at the right levels
- Performance management and tuning service assets to deal with variations in demand.

6.4.3 Demand management through the lifecycle

To be fully effective, demand management needs to be active throughout the service lifecycle.

Activities include:

- Service strategy
- Service design
- Service transition
- Service operation
- Continual service improvement

6.5 Process activities, methods and techniques

6.5.1 Identify sources of demand forecasting

Demand management is based on a good understanding of business activity and how that activity impacts the demand for services. Demand management must therefore identify any documents, reports or information that can provide insight to these activities, and help to forecast the levels of demand. These sources will be used to define, monitor and refine the other components of demand management.

6.5.2 Patterns of business activity and user profiles

Customer assets (e.g. people, processes and applications) undertake business activities that are performed in patterns. PBA define the dynamics of a business, including interactions with customers, suppliers, partners and other stakeholders. As PBA generate revenue, income and costs, they account for most business outcomes. Once a PBA has been identified, its profile should be drawn up and details about it documented:

- Classification
- Attributes
- Requirements
- Service asset requirements

User profiles (UPs) for people are based on roles and responsibilities within organizations, while for processes and applications they are based on functions and operations. Processes may be automated and so consume their own services. Therefore, processes and applications can have UPs.

Each UP can be associated with one or more predefined PBA, allowing aggregation and relationships for PBA to be made. PBA and UPs provide the basis for managing demand for the service by:

- Enabling customers to understand their business activities better and view the activities as consumers of services and producers of demand
- Giving service providers the information they need to sort and serve demand with appropriately matched services, service levels and service assets.

PBA and UPs should be managed as part of normal change control procedures.

6.5.3 Activity-based demand management

An understanding of what creates demand patterns is key to IT service planners. Service demand is primarily driven by business processes, so PBA influence the service demand patterns.

Therefore, customer business patterns need to be identified, analysed and codified to provide input to capacity management, while looking at these patterns in terms of demand for supporting services and underlying service assets.

Demand patterns can occur at multiple levels, so activity-based demand management can daisy-chain demand patterns to ensure business plans are synchronized with service management plans.

Some of the benefits of analysing PBA are in the form of inputs to service management functions and processes, such as the following:

- Service design can optimize designs to suit demand patterns
- Capacity management translates the PBA into workload profiles so that the appropriate resources can be made available to support the levels of service utilization
- The service catalogue can map demand patterns to appropriate services
- SPM can approve investments in additional capacity, new services or changes to services
- Service operation can adjust allocation of resources and scheduling
- Service operation can identify opportunities to consolidate demand by grouping closely matching demand patterns together
- Financial management for IT services can approve suitable incentives to influence demand.

6.5.4 Develop differentiated offerings

When the PBA are analysed, it may become apparent that different levels of performance are required at different times, or different combinations of utility. In these cases, it is important to work with SPM to define service packages that meet the variations in PBA.

6.5.5 Management of operational demand

One of the activities of demand management during service operation is to manage or influence the demand where services or resources are being over-utilized. Typically this would occur in the following situations:

- PBA were inaccurate, resulting in over- or under-utilization of the services. Demand management could help by providing penalties or incentives for users to reduce service usage or use services during off-peak periods.

- The business environment changes, resulting in a change to PBA. This should be dealt with in conjunction with service level management (SLM) and capacity management to understand the new utilization patterns and to gear the resources and capabilities of the service provider appropriately.
- The service provider's forecast for resources was inaccurate and there is insufficient budget to increase capacity. This should be dealt with in conjunction with capacity management.

6.6 Triggers, inputs, outputs and interfaces

Triggers include:

- Requests from customers for a new service or a change to an existing service
- Creation of a new service to meet a strategic initiative
- A service model needs to be defined, and PBA and/or UPs must be defined
- Utilization rates are causing potential performance issues, or a potential breach of a service level target
- An exception has occurred to forecast PBA.

Inputs include:

- New or changed services from SPM or change management
- Service models need to be validated and associated PBA will need to be defined
- Customer portfolio, service portfolio and customer agreement portfolio, which all contain information about demand and supply for services
- Charging models, used to ensure that under- or over-recovery does not occur in internal service providers; or that pricing will be profitable for external service providers.

Outputs include:

- UPs
- Formally documented PBA
- Policies for management of demand when resources are over-utilized
- Policies for managing situations where service utilization is higher or lower than anticipated.

Major interfaces include:

- Strategy management for IT services
- SPM
- Financial management for IT services
- Business relationship management
- SLM
- Capacity management
- Availability management

- IT service continuity management
- Change management
- Service asset and configuration management
- Service validation and testing
- Event management

6.7 Information management

The documentation and information required for effective demand management includes:

- The service portfolio
- The customer portfolio to obtain information about customers and the opportunities that they represent
- The project portfolio to ensure that all projects include demand management as a component
- Minutes of meetings between business relationship managers and customers
- Service level agreements (SLAs) to baseline previous demand levels and to define limits and policies for future utilization
- The configuration management system to map service assets, customer assets and business outcomes.

6.8 Critical success factors and key performance indicators

- CSF The service provider has identified and analysed the PBA and is able to use these to understand the levels of demand that will be placed on a service:
 - KPI PBA are defined for each relevant service
 - KPI PBA have been translated into workload management by capacity management
- CSF The service provider has defined and analysed user profiles and is able to use these to understand the typical profiles of demand for services from different types of user:
 - KPI Documented user profiles exist and each contains a demand profile for the services used by that type of user
- CSF A process exists whereby services are designed to meet the PBA and business outcomes:
 - KPI Demand management activities are routinely included as part of defining the service portfolio
- CSF An interface with capacity management to ensure that adequate resources are available to meet the demand for services:
 - KPI Capacity plans include details of patterns of business activity and corresponding workloads
 - KPI Utilization monitors show balanced workloads.

6.9 Challenges and risks

Challenges include:

- The availability of information about business activities, especially if demand management is not included in the overall set of requirements and has to be collected separately
- Customers might find it difficult to break down individual activities that make sense to the service provider
- Lack of a formal service portfolio management process or service portfolio will make it difficult to understand the business requirements, relative value and priority of services.

Major risks include:

- Lack of, or inaccurate, configuration management information, making it difficult to estimate the impact of changing demand on the service provider's infrastructure and applications
- Service level management is not able to obtain commitments to minimum or maximum utilization levels and it is therefore difficult to commit to levels of service.

6.10 Roles and responsibilities

6.10.1 Demand management process owner

- Carrying out the generic process owner role for the demand management process
- Working with other process owners to ensure an integrated approach to the design, transition and operation of demand management
- Monitoring and reporting on demand management process performance
- Making improvements to the demand management process.

6.10.2 Demand management process manager

- Carrying out the generic process manager role for the demand management process
- Identifying and analysing PBA to understand the levels of demand that will be placed on a service
- Defining and analysing UPs to understand the typical profiles of demand for services from different types of user
- Helping to design services to meet the PBA and business outcomes
- Ensuring adequate resources are available at the appropriate levels of capacity to meet the demand for services
- Anticipating and preventing or managing situations where demand for a service exceeds the capacity to deliver it.

7 Technology and implementation

7.1 Generic requirements for IT service management technology

There are many tools and techniques that can be used to help with the design of services. They enable the following:

- Hardware design
- Software design
- Environmental design
- Process design
- Data design.

The tools and techniques are useful in:

- Speeding up the design process
- Ensuring standards are followed
- Prototyping, modelling and simulation
- Enabling 'What if?' analysis
- Enabling interfaces and dependencies to be checked
- Validating designs before development starts.

Developing service designs can be simplified by the use of tools that provide graphical views of the service and its constituent components. They can also be linked to auto-discovery tools to make the capture and maintenance of the relationships between all of the service components more efficient and accurate.

There is an opportunity to extend the use of these tools into day-to-day operation and, by linking to financial information, metrics and key performance indicators, they can be used to monitor and manage the service through all stages of its lifecycle.

The following generic activities are required to implement such an approach:

- Establish the generic lifecycle for IT assets (requirements, design and develop, build, test, deploy, operate and optimize, dispose) and define the principal processes, policies, activities and technologies within each stage of the lifecycle for each type of asset
- Formalize the relationships between different types of IT asset, and the relationships between IT asset acquisition and management and other IT disciplines
- Define all roles and responsibilities involved in IT asset activities
- Establish measures for understanding the (total) cost of ownership of an IT service
- Establish policies for the re-use of IT assets across services (e.g. at the corporate level)
- Define a strategy for the acquisition and management of IT assets, including how it should be aligned with other IT and business strategies.

Additional activities should be carried out for specific asset types; for example:

- Applications
- Data and information
- IT infrastructure and environmental
- Skills (people, competencies)
- Interfaces and dependencies.

7.2 Evaluation criteria for technology and tools

Some generic points that organizations should consider when selecting any service management tool include:

- Data handling, integration, import, export and conversion
- Data backup, control and security
- Ability to integrate multi-vendor components, existing and into the future
- Conformity with international open standards
- Usability, scalability and flexibility of implementation and usage
- Support options provided by the vendor, and credibility of the vendor and tool
- The platform the tool will run on and how this fits the IT strategy
- Training and other requirements for customizing, deploying and using the tool
- Costs: initial and ongoing.

It is generally best to select a fully integrated tool, but this must support the processes used by the organization, and extensive tool customization should be avoided.

Tool requirements should be categorized using MoSCoW analysis:

- M – MUST have this
- S – SHOULD have this if at all possible
- C – COULD have this if it does not affect anything else
- W – WON'T have this, but WOULD like in the future.

7.3 Practices for process implementation

The activities of implementing and improving service design need to be focused on the needs and desires of the customer and the business. Therefore these activities should be driven and prioritized by:

- Business needs and business impacts
- Risks to the services and processes.

7.3.1 Business impact analysis

A valuable source of input when trying to ascertain the business needs, impacts and risks is the business impact analysis (BIA). The BIA is an essential element of the overall business continuity process and will dictate the strategy for risk reduction and disaster recovery.

7.3.2 Service level requirements

As part of service level management, the service level requirements (SLRs) for all services will be ascertained and the ability to deliver against these requirements will be assessed. Finally the SLRs will be agreed in a formal service level agreement (SLA). For new services, the requirements must be ascertained at the start of the development process, not after completion. Building the service with SLRs uppermost in mind is essential from a service design perspective.

7.3.3 Risks to the services and processes

When implementing service design and IT service management (ITSM) processes, business-as-usual practices must not be adversely affected. This aspect must be considered during the production and selection of the preferred solution to ensure that disruption to operational services is minimized. This assessment of risk should then be considered in detail in the service transition activities as part of the implementation process.

7.3.4 Implementing service design

The process, policy and architecture for the design of IT services will need to be documented and utilized to ensure that appropriate innovative IT services can be designed and implemented to meet current and future agreed business requirements.

Implementation priorities should be set against the goals of a service improvement plan (SIP). Establish a formal process and method for implementation and improvement of service design, with the appropriate governance in place. This formal process should be based on the six-stage continual service improvement model:

- Step 1 What is the vision? Understand the vision by ascertaining the high-level business objectives. The 'vision-setting' should set and align business and IT strategies.
- Step 2 Where are we now? Assess the current situation to identify strengths that can be built on and weaknesses that need to be addressed. Perform an analysis of the current position in terms of the business, organization, people and process.
- Step 3 Where do we want to be? Develop the principles defined in the vision-setting and agree the priorities for improvement.
- Step 4 How do we get there? Detail the SIP to achieve higher-quality service provision.
- Step 5 Did we get there? Put in place measurements and metrics to show that the milestones have been achieved and that the business objectives and business priorities have been met.
- Step 6 How do we keep the momentum going? Ensure that the momentum for quality improvement is maintained.

The following are key elements for successful alignment of IT with business objectives:

- Vision and leadership in setting and maintaining strategic direction, clear goals, and measurement of goal realization in terms of strategic direction
- Acceptance of innovation and new ways of working
- A thorough understanding of the business, its stakeholders and its environment

- IT staff understanding the needs of the business
- The business understanding the potential of IT
- Information and communication available and accessible to everyone who needs them
- Separately allocated time for people to become familiar with the material
- Continuous tracking of technologies to identify opportunities for the business.

7.4 Challenges, critical success factors and risks

7.4.1 Challenges

7.4.1.1 Service design

- Ensuring alignment with current architectural directions, strategy and policies
- Understanding the implications of diverse and disparate technologies and applications
- Dealing with unclear or changing requirements from the business
- Clarifying business requirements and targets for services
- Ensuring appropriate planning to avoid unplanned initiatives and purchases.

7.4.1.2 Service transition

- Managing contacts, interfaces and relationships across a large customer and stakeholder group
- Lack of harmonization and integration of the supporting processes and disciplines; for example, finance, engineering and human resources
- Dealing with differences between legacy systems, new technology and the human elements related to them
- Balancing the need for a stable production environment with the need to be responsive to changing business requirements
- Creating an environment that fosters standardization, simplification and knowledge-sharing.

7.4.1.3 Service operation

- Lack of engagement with development and project staff
- Justifying funding on what are often seen as infrastructure costs
- Ensuring that the potential impact across all operational services is taken into account in each individual service design and transition
- Ensuring that a realistic assessment of true ongoing running costs, after transition, is taken into account in service design
- Ensuring service transition is effective in managing the transition from design to operation
- Understanding what and how to measure to demonstrate good performance
- Being increasingly involved in virtual or matrix teams can lead to confusion over who is accountable for ensuring specific activities are carried out.

7.4.2 Critical success factors

7.4.2.1 Service design

- Understanding business requirements and priorities and that they are taken into account when designing processes and services
- Ensuring good, ongoing communications with the affected individuals
- Involving as many people as possible in the design
- Gaining commitment from senior management as well as from all levels of staff.

7.4.2.2 Service transition

- Understanding the different stakeholder perspectives that underpin effective risk management and maintaining commitment
- Maintaining contact and managing all relationships
- Integrating with other lifecycle stages, processes and disciplines that impact service transition
- Automating processes to eliminate errors and reduce cycle time
- Maintaining new and updated knowledge in a format that can be found and used.

7.4.2.3 Service operation

- Ensuring senior management support; this is critical for maintaining the required funding and resources, as is visible support when new initiatives are launched
- Ensuring business units understand the role they play in adhering to policies, processes and procedures – such as using the service desk to log all requests
- Identifying champions who will lead others through their enthusiasm and commitment
- Understanding the number of staff required and planning to ensure required skills are retained
- Training service management staff to an appropriate level of understanding of the business, processes and tools
- Ensuring the suitability of and ongoing funding for tools
- Allowing sufficient time and effort to plan, design and execute the tests, ideally using independent testers
- Clearly defining how things will be measured and reported – to provide staff with targets to aim for and to allow IT and business managers to review progress and identify opportunities for improvement.

7.4.3 Risks

Many risks are simply the opposite of CSFs, but the ultimate risk to the business is the loss of critical IT services, with its subsequent adverse impact on employees, customers and finances.

7.4.3.1 Service design

- If any of the CSFs are not met, service design will not be successful
- If maturity levels for one process are low, it will be impossible to reach full maturity in other related processes

- Business requirements are not clear to IT staff
- Business timescales do not allow sufficient time for proper service design
- Policies and strategies are not available or are not clearly understood.

7.4.3.2 Service transition

- Changes in accountabilities, responsibilities and practices of existing projects that demotivate the workforce
- Alienation of some key support and operations staff
- Additional, unplanned costs to services in transition
- Resistance to change and circumvention of the processes due to perceived bureaucracy
- Lack of maturity and integration of systems and tools resulting in people 'blaming' technology for other shortcomings
- Poor integration between processes causing process isolation and a 'silo' approach to delivering ITSM.

7.4.3.3 Service operation

- Inadequate funding and resources available to maintain the infrastructure in a condition to guarantee ongoing service delivery
- Loss of momentum in the implementation of service management caused by day-to-day operational tasks taking priority
- Loss of key personnel, which can have a severe impact
- Resistance to change caused by a reluctance to take new things on board
- Lack of management support where middle managers may not gain the hands-on benefits that junior managers do, and may not see the overall vision.

7.5 Planning and implementing service management technologies

There are a number of factors to consider when deploying and implementing ITSM support tools:

- Licences
 - Dedicated licences
 - Shared licences
 - Web licences
 - Service on demand
- Deployment
- Capacity checks
- Timing of technology deployment
- Type of introduction

7.6 Designing technology architectures and management architectures

Good architectural design for service management will result in a simple and clear set of norms and standards that can be used:

- To ensure consistency in the creation of new services

- To guarantee maximum cohesion with the management systems and tools already in place to support the delivery of services.

Architectural design activities provide the blueprint for the IT infrastructure – a set of applications and data that satisfy the business needs. However, although the IT infrastructure underpins the delivery of quality IT services, it is also essential that the people, processes and partner or supplier aspects are taken into consideration. Architectures need to be developed in the following major areas:

- Service architecture
- Technology architectures:
 - Application architecture
 - Data and information architecture
 - IT infrastructure architecture
 - Environmental architecture
- Management architecture
 - Business: needs, requirements, processes, objectives and goals
 - People: scope, tasks and activities
 - Processes and procedures
 - Tools for management and support
 - Technology and IT products.

Management architectures need to be aligned with the business and not driven by technology.