ITIL – Introducing service design

The objectives of service design

The main objective of the service design stage can be defined as:

The design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.

There are five individual aspects of service design. These are:

- New or changed services
- Service management systems and tools, especially the service portfolio, including the service catalogue
- Technology architecture and management systems
- The processes required
- Measurement methods and metrics

The service design stage of the lifecycle starts with a set of new or changed business requirements and ends with the development of a service solution designed to meet the documented needs of the business. This developed solution is then passed to service transition to evaluate, build, test and deploy the new or changed service.

Other objectives include:

- Design services to satisfy business objectives, based on the quality, compliance, risk and security requirements, delivering more effective and efficient IT and organisation solutions and services aligned to organisational needs
- Design services that can be easily and efficiently developed and enhanced within appropriate timescales and costs and, wherever possible, reduce, minimise or constrain the long term costs of service provision
- Design efficient and effective processes for the design, transition, operation and improvement of high quality IT services, together with the supporting tools, systems and information, especially the service portfolio, to manage services through their lifecycle
- Design secure and resilient IT infrastructures, environments, applications and data/information resources, and capability, that meet the current and future needs of the organisation
- Design measurement methods and metrics for assessing the effectiveness and efficiency of the design processes and their deliverables
- Produce and maintain IT plans, processes, policies, architectures, frameworks and documents for the design of quality IT solutions, to meet current and future agreed organisation needs
- Assist in the development of policies and standards in all areas of design
- Develop the skills and capability within IT by moving strategy and design activities into operational tasks, making effective and efficient use of all IT service resources
- Contribute to the improvement of the overall quality of IT service within the imposed design constraints, especially by reducing the need for reworking and enhancing services, once they have been implemented in the live environment

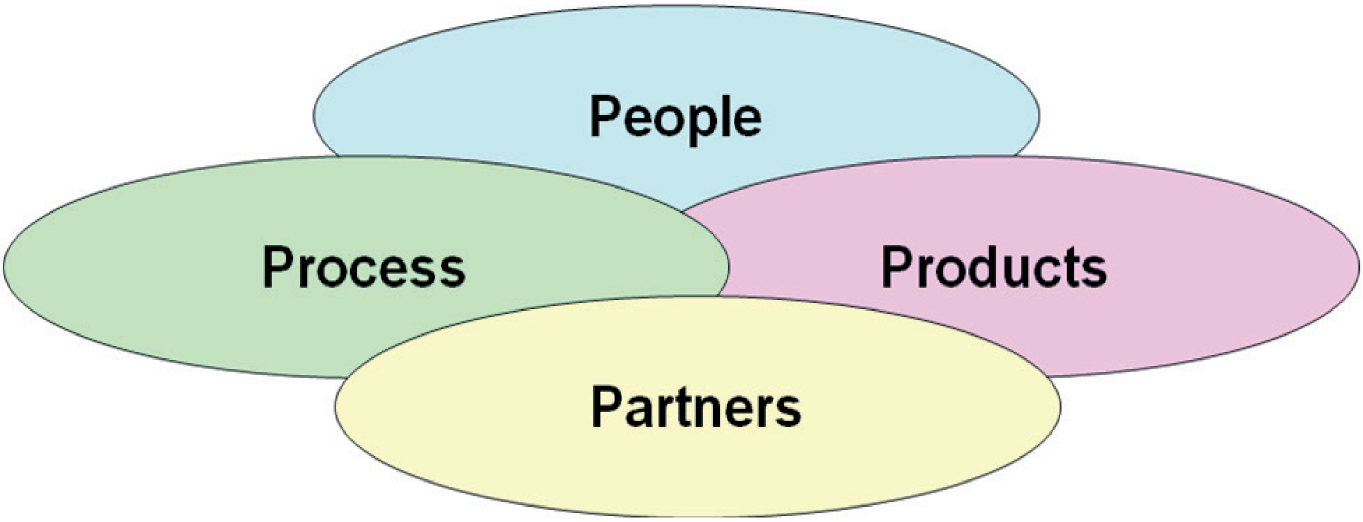
Value to the organisation of service design

- Agreeing service targets across the whole organisation, ensuring critical business processes receive most attention
- Measuring IT quality in these business terms, reporting what is relevant to users (e.g. customer satisfaction, business value)
- Appropriate mapping of the IT infrastructure to the business processes
- Providing *end to end* business focused performance monitoring and measurement
- Periodic reporting against targets

- Reduced Total Cost of Ownership (TCO)
- Improved quality of service
- Improved consistency of service
- Easier implementation of new or changed services
- Improved service alignment
- More effective service performance
- Improved IT governance
- More effective service management and IT process
- Improved information and decision making

The four Ps of service design

ITIL, in particular service design, is built primarily upon the four Ps.



In order to deliver the benefits of service management and ITIL, these 4 *Ps* need to overlap each other, a popular misconception is that 1 *P* will fix all the rest, and many organisations believe this is the *product*. There has to be a balance of all 4 Ps to ensure the right *mix* for the appropriate design.

Many designs, plans and projects fail through a lack of preparation and management. The implementation of ITIL service management as a practice is about preparing and planning the effective and efficient use of the four Ps: the People, the Processes, the Products (services, technology and tools) and the Partners (suppliers, manufacturers and vendors).

Service design processes

- Service level management
- Capacity management
- Availability management
- IT service continuity management
- Information security management
- Service catalogue management
- Supplier management

Service level management

Why have service level management?

As organisations become increasingly dependent on IT, they demand a higher quality of service. By creating an IT service management strategy, organisations are able to maximise end user productivity, improve operational effectiveness and enhance overall business performance. Additionally, the effort creates a forum for communication between the IS organisation and the business units. Also an ITSM strategy provides the basis for integrating IT measurement into operational and strategic IT management. In most cases, however, service management is not well defined or not defined at all.

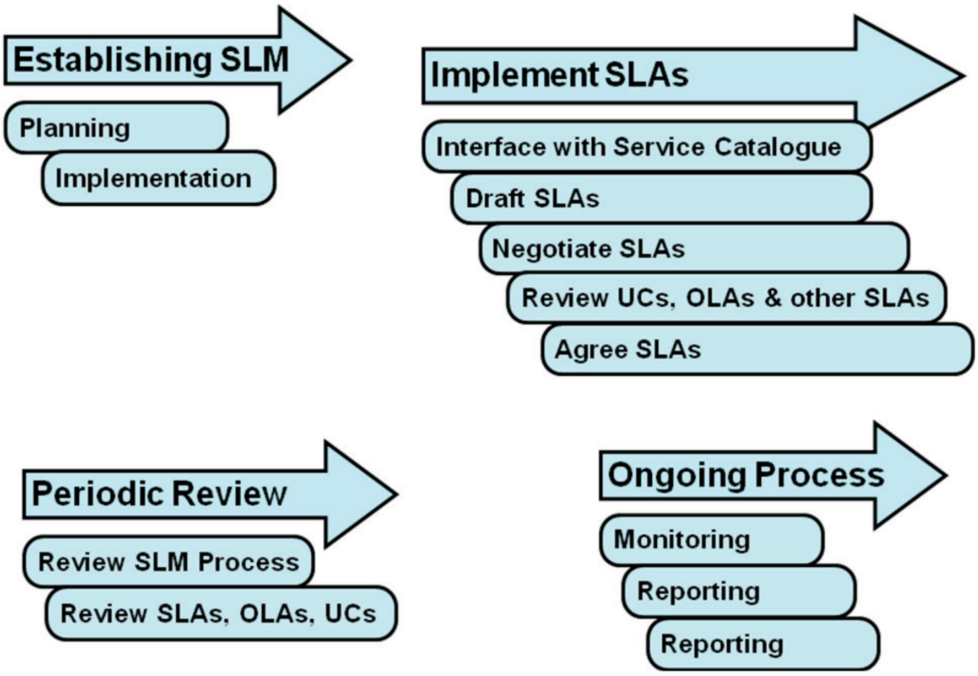
Service level management principles form the basis on how to contribute to an ITSM culture to ensure that the right services with the appropriate quality are delivered, at the right cost to end users.

Although Service Level Management (SLM) is focused heavily on CSI, this process also plays a major part in the service design book, especially its involvement in service catalogue management and supplier management.

The objectives of service level management

To maintain and improve IT service quality, through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and instigation of actions to eradicate poor service – in line with business or cost justification. Through these methods, a better relationship between IT and its customers/users can be developed.

- Define, document, agree, monitor, measure, report and review the level of IT services provided
- Provide and improve the relationship and communication with the business/customer
- Ensure that specific and measurable targets are developed for all IT services
- Monitor and improve customer satisfaction
- Ensure that IT and the customers have a clear and unambiguous understanding of the level of service to be delivered
- Ensure that improvements to the levels of service are implemented wherever the service is failing, and the that these improvements are cost justified



The activities of service level management

Identification

- Analysing current services and service level requirements
- Recording the current service provision in a service catalogue

Definition

Matching and customising (with the customer) of the right service provision against the right costs:

- Service catalogue
- Demands of the customer (service level requirements)

Agreement (defining and signing SLAs)

- Service Level Agreements, supported by: Operational Level Agreements (OLA's) and underpinning contracts

Monitoring

- Measuring the actual service levels against the agreed service levels

Reporting

- Reporting on the service provision (to the customer and the IT organisation)

Evaluation (review)

- Evaluate the service provision with the customer
- Match and customise: adjust service provision if required? (service improvement plan/programme, service quality plan)
- Match and customise: adjust SLA if required?

The Terminology of service level management

SLR (Service Level Requirements)

- Detailed recording of the customers' needs
- Blueprint for defining, adapting and revising of services

Service spec sheets (service specifications)

- Connection between functionality (externally/customer focused) and technicalities (internally/IT organisation focused)

Service catalogue

Service level management must ensure that a service catalogue is produced, maintained and contains accurate information on all operational services and those ready for deployment. A service catalogue is a written statement of all current and available IT services, default levels and options.

SLA (Service Level Agreement)

The written agreement between the provider and the customer (organisation representative).

Service level achievements

The service levels that are realised.

SIP (Service Improvement Plan)

This is a formal plan or program that is developed when the IT service provider is not currently delivering a service that meets the legitimate Service Level Requirements (SLR's) of the business representative or when greater cost effectiveness is achievable. The SIP should include clear milestones, which will enable the business representative to judge whether or not timely progress is being made.

SQP (Service Quality Plan) – not specifically an SLM term, but strategically linked

This plan underlies the service strategy, detailing the internal targets to be achieved within an agreed period, typically one to two years, to improve agreed service levels and the business perception of service quality:

- Management information for steering the IT organisation
- Process parameters of the service management processes and the operational management
- Key performance indicators:
    - Incident management – resolution times for levels of impact
    - Change management – processing times and costs of routine changes

OLA (Operational Level Agreement)

A written agreement with another internal IT department to support the SLA.

UC (Underpinning Contract)

A written agreement with an external IT supplier.

Capacity management

Why have capacity management?

Every application makes its own demands on the IT environment. Some are unavoidable, such as the continuing spread of applications for Enterprise Resource Planning (ERP), supply chain management or human resources management. Also, new applications are emerging (e.g. those employing multimedia content) that will impact IT with their heavy demands for bandwidth. Finally, additional applications are required to support the growing IT infrastructure of an organisation (e.g. remote storage of back up data).

Failure to consider these issues will lead to negative effects on the business, as the capacity of the IT environment simply does not match the requirements of the business.

- Balancing costs and supply against demand
- Balancing costs against resources needed

The objectives of capacity management

The capacity management process understands the business requirements (the required service delivery), the organisation's operation (the current service delivery) and the IT infrastructure (the means of service delivery). It ensures that all the current and future capacity and performance aspects of the business requirements are provided cost effectively.

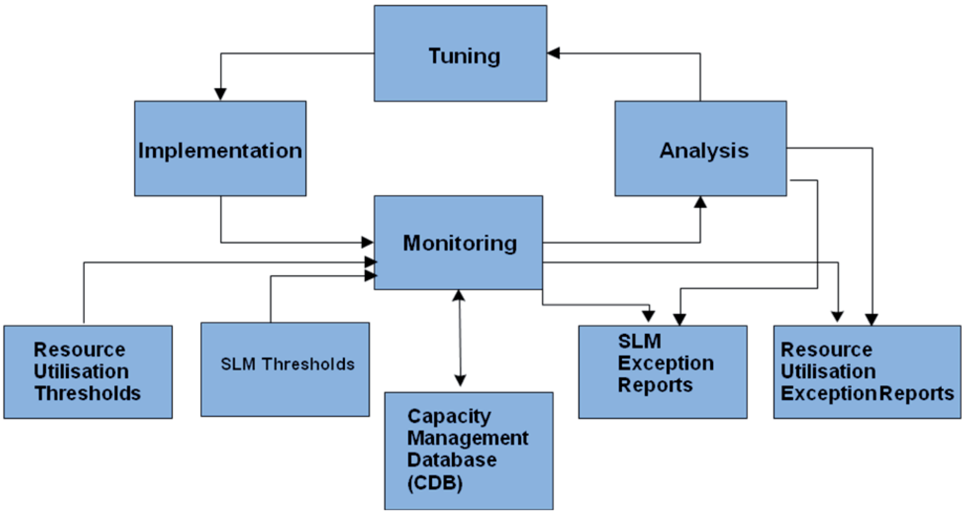
The activities of capacity management

Business capacity management: This sub-process is responsible for ensuring that the future business requirements for IT services are considered, planned and implemented in a timely fashion. This can be achieved by using the existing data on the current resource utilisation by the various services to trend, forecast or model the future requirements. These future requirements come from business plans outlining new services, improvements and growth in existing services, development plans etc.

Service capacity management: The focus of this sub-process is the management of the performance of the live, operational IT services used by the customers. It is responsible for ensuring that the performance of all services, as detailed in the targets in the SLAs and SLRs, are monitored and measured, and that the collected data is recorded, analysed and reported. As necessary, action is taken to ensure that the performance of the services meets the business requirements. This is performed by staff with knowledge of all the areas of technology used in the delivery of end to end service, and often involves seeking advice from the specialists involved in resource capacity management.

Component capacity management: The focus in this sub-process is the management of the individual components of the IT infrastructure. It is responsible for ensuring that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analysed and reported. As necessary, action must be taken to manage the available resource to ensure that the IT services that it supports meet the business requirements.

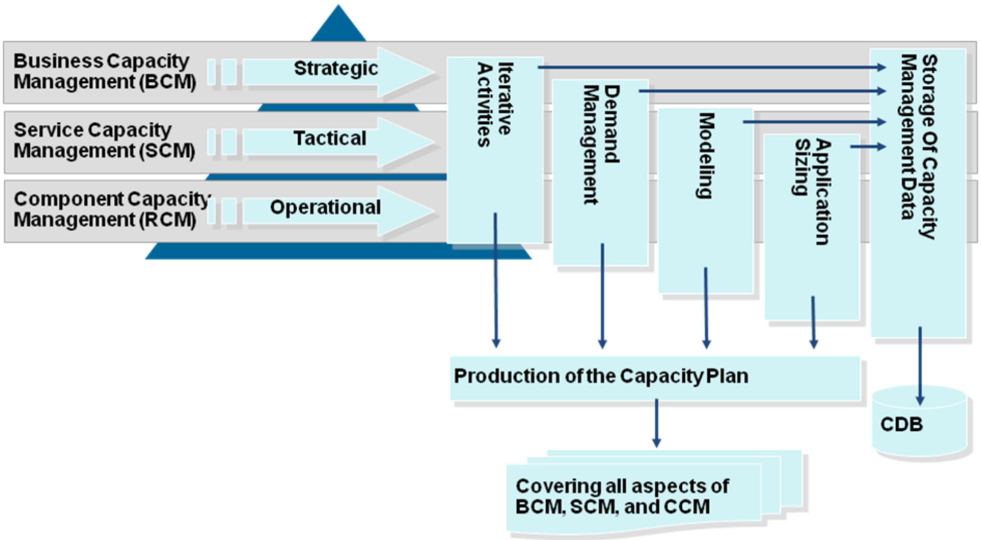
Iterative activities (performance management)


Tuning
Implementation
Analysis
Monitoring
Resource Utilisation Thresholds
SLM Thresholds
Capacity Management Database (CDB)
SLM Exception Reports
Resource Utilisation Exception Reports

- Analysis
- Tuning – Modifications made for better utilisations of current infrastructure (under the control of change management)
- Implementation
- Monitoring

Other capacity activities

- Demand management – Aims to influence the use of capacity, perhaps by incentive or penalty, in circumstances where unmanaged demand is likely to exceed the ability to deliver. Demand management is achieved by assigning resources according to priorities.
- Application sizing – Determining the service level, resource and cost implications of any new application or any major addition or enhancement to an existing application.
- Modelling – A set of tools and techniques used to predict the performance of a specified system under a given volume and variety of work. Modelling is used to predict the availability and performance of services.
- Capacity management database – Used by all activities in the process for storage of capacity data e.g. technical, business, financial, service and utilization data.
- Capacity plan – development and maintenance – the capacity plan predicts demand for IT services and outlines the resources needed to meet this. It will contain costed possible scenarios for IT services together with a recommended option.


Business Capacity Management (BCM)
Strategic
Service Capacity Management (SCM)
Tactical
Component Capacity Management (RCM)
Operational
Iterative Activities
Demand Management
Modeling
Application Sizing
Storage Of Capacity Management Data
Production of the Capacity Plan
CDB
Covering all aspects of BCM, SCM, and CCM

Availability management

Why have availability management?

Gartner research shows that people and/or process failures directly cause an average of 80% of mission critical application service downtime. The other 20% is caused by technology failure, environmental failure or a disaster. The complexity of today's IT infrastructure and applications makes *high availability* systems management difficult. Applications requiring high levels of availability must be managed with operational disciplines (including network monitoring, systems management activities etc.) to avoid unnecessary and potentially devastating outages.

The objectives of availability management

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

The activities of availability management

Proactive activities

- Ensure that appropriate design and planning of availability takes place for all new services
- Planning, design and improvement of availability
- Providing cost effective availability improvements that can deliver business and customer benefits
- Ensuring agreed level of availability is provided
- Produce and maintain an availability plan

Reactive activities

- Monitoring, measuring, analysis and management of all events, incidents and problems involving unavailability
- Continually optimise and improve availability of IT infrastructure services
- Assisting security and ITSCM in the assessment and management of risk
- Attending CAB as required

Determining availability requirements

Input from service level management. The Service Level Manager discusses with the client what their needs for service are (service level requirements). Based on these requirements, the Availability Manager can determine the availability requirements.

Determining vital business functions (VBF's)

Some organisation's processes are more critical than others. IT systems that support VBFs should have higher availability expectations and the appropriate systems and support to achieve and sustain these higher levels at critical times which have been agreed and documented in the SLA.

Business impact analysis

A formal analysis of the affect on the business, if a specific set of IT services are not available. It will also identify the minimum set of services that an organisation will require to continue operating.

- Risk analysis management (input for IT service continuity management) – this activity involves trying to identify the impact to the business of service unavailability. It is part of our risk analysis and risk management activities. The outcomes of these activities are utilised in various processes: availability management, IT service continuity management and information security management.

Defining availability, reliability and maintainability targets

Input for Service Level Agreements (SLAs) and other contracts. Based on the first three steps, we are now ready to create the achievable and sustainable availability targets. In order to do this, we need to get input from all technical areas within the IT group. (as well as suppliers).

Monitoring and trend analysis

- MTBF (Mean Time between Failures)
- MTBSI (Mean Time between System Incidents)
- MTRS (Mean Time to Restore Services)
- Planned downtime, unscheduled downtime, extended (excess) downtime
- Frequent (scheduled) backups

Root cause analysis of low availability

- Relationship with the problem management process

Producing and maintaining an availability plan – This plan has to be updated at least once every year!

Reporting

The techniques of availability management

- SOA – Service Outage Analysis
- SPOF Analysis – Single Point of Failure Analysis
- CFIA – Component Failure Impact Analysis
- TOP – Technical Observation Post
- CRAMM – CCTA Risk Analysis Management Method
- FTA – Fault Tree Analysis

The terminology of availability management

Availability: Key indicator of the service provided. It should be defined in the Service Level Agreement.

Reliability: Reliability of the service is made up out of the reliability of service components and the resilience of the IT infrastructure.

Serviceability: Contractual arrangements with third parties in regards to maintenance.

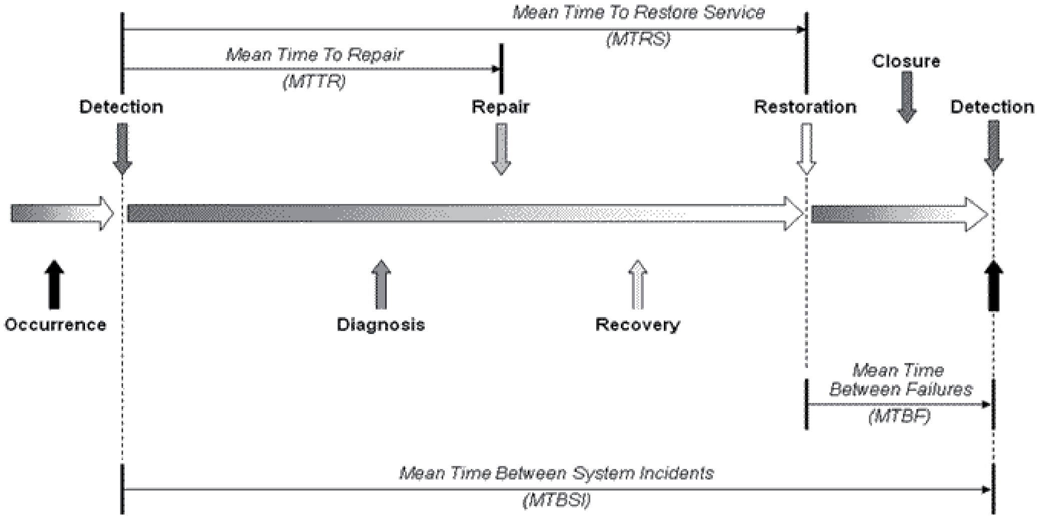
Maintainability: The ability of the IT group to maintain the IT infrastructure in operational state and available according to the agreed service levels.

Security: Confidentiality, Integrity and Availability (CIA) of *data*.

Resilience: The ability of individual components to absorb or be flexible in times of stress.

Availability relationship with other processes

The connection between incident management (detection), problem management (diagnosis), change management (repair time) and availability management is shown in the following diagram:



The following metrics are commonly used in availability management:

- Mean Time to Restore Services – MTTRS: average time between the occurrence of a fault and service recovery (or the downtime)
- Mean Time Between Failures – MTBF: mean time between the recovery from one incident and the occurrence of the next incident
- Mean Time Between System Incidents – MTBSI: mean time between the occurrences of two consecutive incidents. The MTBSI = MTTR + MTBF

The ratio of MTBF to MTBSI shows if there are many minor faults or just a few major faults. Availability reports may include the following metrics:

- Rate of availability (or unavailability) in terms of MTRS, MTBF and MTBSI
- Over all uptime and downtime, number of faults
- Additional information about faults which actually, or potentially, result in a higher than agreed unavailability

IT service continuity management

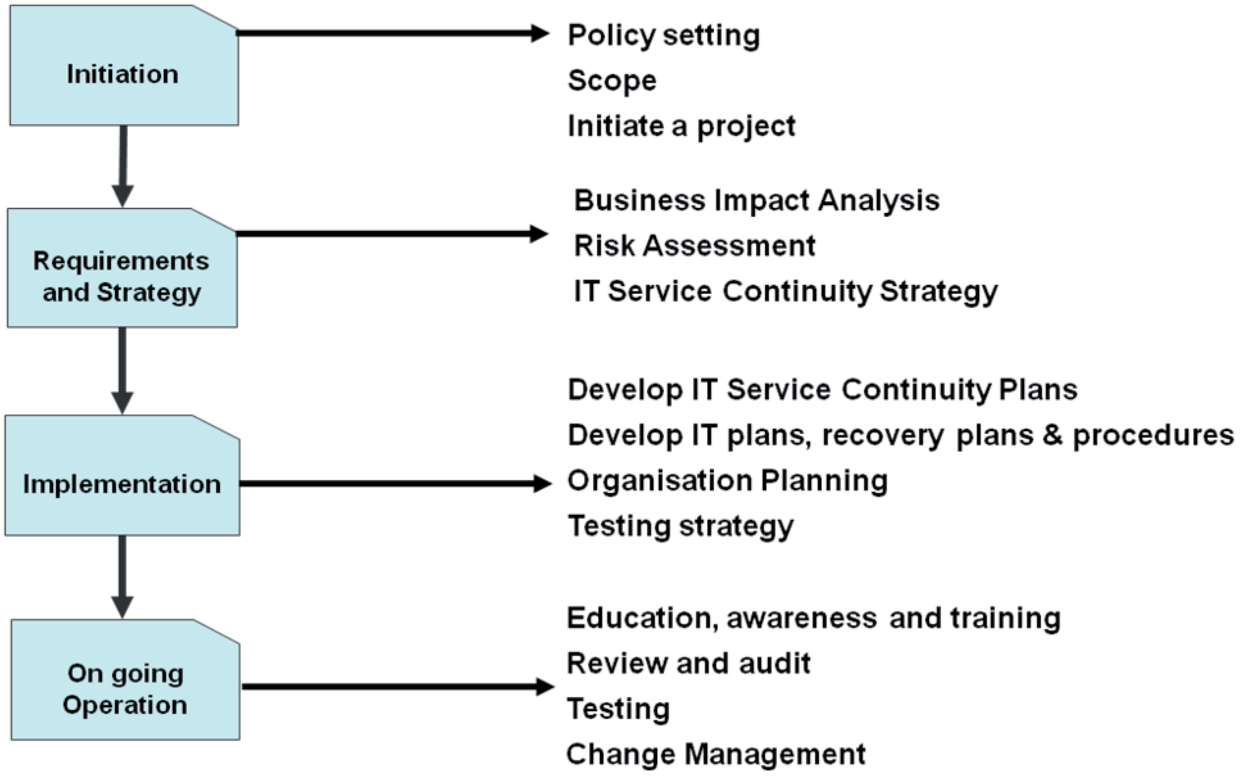
Why have IT service continuity management?

As technology is a core component of most business processes, continued or high availability of IT is critical to the survival of the organisation as a whole. This is achieved by introducing risk reduction measures and recovery options. Like all elements of ITSM, successful implementation of ITSCM can only be achieved with senior management commitment and the support of all members of the organisation. Ongoing maintenance of the recovery capability is essential if it is to remain effective. The purpose of ITSCM is to maintain the necessary ongoing recovery capability within the IT services and their supporting components.

The objectives of IT service continuity management

The objective for ITSCM is to support the overall business continuity management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required, and agreed, business timescales.

The activities of IT service continuity management



The diagram, on the previous page, shows the four stages of ITSCM, incorporating each of the activities that take place to ensure that IT organisations are as prepared and organised as possible in the event of a disaster situation. Stage 1 is really an activity that has to be done by the business, so IT can figure out what it is that BCM do? The IT organisation has to provide details with how they will support this BCM by the continuation of delivery of IT services in times of crisis and disaster.

Two of the major data sources for ITSCM are developed within requirement and strategy, including business impact analysis and risk assessment.

Stage 1: initiation

- Link with business continuity plan
- Policy setting
- Terms of reference and scope
- Allocate resources

Stage 2: requirements and strategy

- Input from availability management and security management (risk assessment)
- Business impact analysis
- Discuss recovery options (link to SLM)

Stage 3: implementation

- Write continuity plans, including:
  - Emergency response plan
  - Damage assessment plan
  - Salvage plan
  - Crisis management and PR plan
- Implement standby arrangements
- Implement recovery options
- Test the plans
- Develop and implement procedures and working instructions

Stage 4: operational management

- Link ITSCM to change management to keep plans and recovery options up to date
- IT staff need to be aware and trained to use the plans
- Continuous improvement of the process through review and testing

Risk analysis technique

Risk Analysis and Management Method (CRAMM) – a phased approach:

- Identify components
- Analyse the threats
- Assess the vulnerabilities
- Evaluate threats and vulnerabilities to provide an estimate of the risks

The terminology of IT service continuity management

Recovery options:

Do nothing: sometimes the business can function without this service.

Manual work around: administrative actions, takes lot of resource to enter data back into systems.

Reciprocal arrangements: agree to use the infrastructure of another organisation, especially for batch processing.

Gradual recovery (*cold standby*): an empty room available (in house or outsourced service), mobile or fixed, where IT infrastructure can be rebuilt. (Takes longer than 72 hours to recover).

Intermediate recovery (*warm standby*): a contract with a third party/supplier recovery organisation to use their infrastructure in a contingency situation. Backup tapes should be available at the crisis site at all times. (Takes 24 to 72 hours to recover).

Fast recovery (*hot standby*): this option (sometimes referred to as *hot standby*) provides for fast recovery and restoration of services, and is sometimes provided as an extension to the intermediate recovery provided by a third party recovery provider.

Where there is a need for a fast restoration of a service, it is possible to *rent* floor space at the recovery site and install servers or systems with application systems and communications already available, and data mirrored from the operational servers. In the event of a system failure, the customers can then recover and switch over to the backup facility with little loss of service. (This typically involves the re-establishment of the critical systems and services within a 24 hour period).

Immediate recovery (also known as *hot standby*): a full duplication of system (minus components) for instantaneous recovery. This option (also often referred to as *hot standby*, *mirroring*, and *load balancing* or *split site*) provides for immediate restoration of services, with no loss of service. For business critical services, organisations requiring continuous operation will provide their own facilities within the organisation, but not on the same site as the normal operations. Sufficient IT equipment will be *dual located* in either an owned or hosted location to run the complete service from either location in the event of loss of one facility, with no loss of service to the customer. The second site can then be recovered whilst the service is provided from the single operable location. This is an expensive option, but may be justified for critical business processes or VBFs where non-availability for a short period could result in a significant impact, or where it would not be appropriate to be running IT services on a third party's premises for security or other reasons. The facility needs to be located separately and far enough away from the home site, that it will not be affected by a disaster affecting that location. However, these mirrored servers and sites options should be implemented in close liaison with availability management, as they support services with high levels of availability.

Information security management

Why have information security management?

ISM needs to be considered within the overall corporate governance framework. Corporate governance is the set of responsibilities and practices exercised by the board and executive management, with the goal of providing strategic direction, ensuring the objectives are achieved, ascertaining the risks are being managed appropriately and verifying that the enterprise's resources are used effectively. Information security is a management activity within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It further ensures that the information security risks are appropriately managed and that enterprise information resources are used responsibly. The purpose of ISM is to provide a focus for all aspects of IT security and manage all IT security activities.

The term *information* is used as a general term and includes data stores, databases and metadata. The objective of information security is to protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.

The objectives of information security management

The goal of the information security management process is to align IT security with organisation security and ensure that information security is effectively managed in all service and service management activities.

Security objectives in most organisations are met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures availability
- Information is observed by, or disclosed, to only those who have a right to know (confidentiality)
- Information is complete, accurate and protected against unauthorised modification (integrity)
- Business transactions, as well as information exchanges between partners, can be trusted (authenticity and non-repudiation)

Security controls

Preventive

- Preventing security incidents from occurring

Reductive

- Taking action to reduce the damage caused by security incidents

Detective

- Detecting security incidents quickly

Repressive

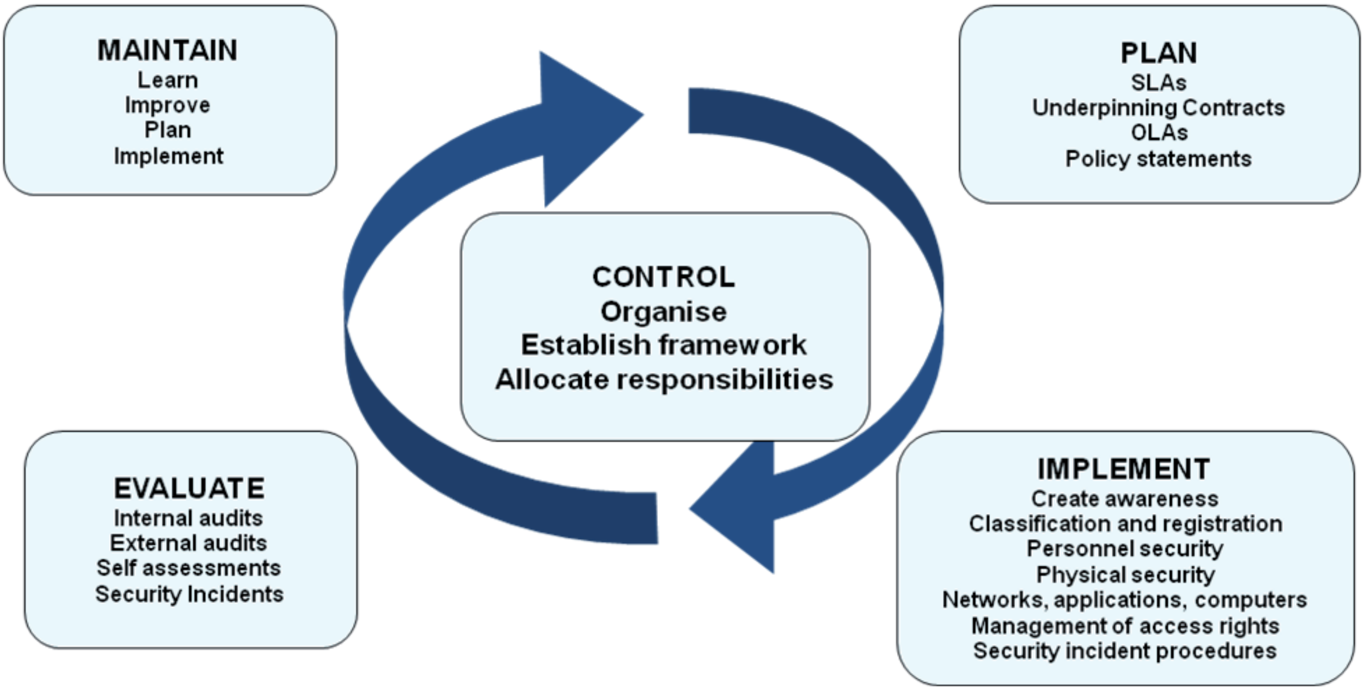
- Preventing further occurrences of a specific security incident

Corrective

- Having tested plans to recover from security incidents

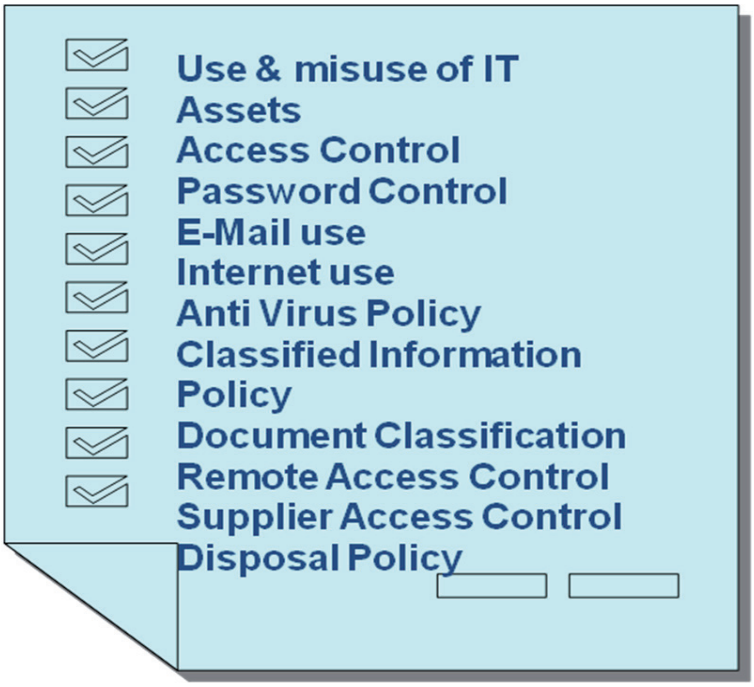
The activities of information security management

- 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 clarification of all information assets and documentation
- Implementation, review, revision and improvement of a set of security controls and risk assessment and responses
- Monitoring and management of all security breaches and major security incidents
- Schedule and completion of security reviews, audits and penetration tests



The information security policy

- This covers all areas of security, including:



Use & misuse of IT
Assets
Access Control
Password Control
E-Mail use
Internet use
Anti Virus Policy
Classified Information
Policy
Document Classification
Remote Access Control
Supplier Access Control
Disposal Policy

- This must be followed by everyone!

Information security management terminology

Confidentiality – protecting information against unauthorised access and use.

Integrity – accuracy, completeness and timeliness of the information.

Availability – the information should be accessible at any agreed time. This depends on the continuity provided by the information processing systems.

Security baseline – The security level adopted by the IT organisation for its own security, and from the point of view of good *due diligence*.

Security incident – any incident that may interfere with achieving the SLA security requirements; materialisation of a threat.

Verifiability – ability to verify that information is used correctly and that security measures are effective.

Security baseline – the security level adopted by the IT organisation for its own security and from the point of view of good *due diligence*.

Information security management relationship with other ITIL processes

- Information security management sets policy for all other processes
- Availability management performs risk assessment for Confidentiality, Integrity and Availability (CIA) on Data. Security management uses this information for IT security
- Change management and release management implement changes regarding security measures and security policy
- Service level management has security measures as part of a service catalogue, SLAs and other SLM documents
- Access management helps to protect the confidentiality, integrity and availability (CIA) of assets; therefore it is the execution of policies and actions defined in information security and availability management

Supplier management

Why have supplier management?

The supplier management process ensures that suppliers and the services they provide are managed to support IT service targets and organisation expectations.

It is essential that supplier management processes and planning are involved in all stages of the service lifecycle, from strategy and design, through transition and operation, to improvement. The complex organisation demands require the complete breadth of skills and capability to support provision of a comprehensive set of IT services to a business. Therefore, the use of value networks and the suppliers (and the services they provide) are an integral part of any end to end solution. Suppliers and the management of suppliers and partners are essential to the provision of quality IT services.

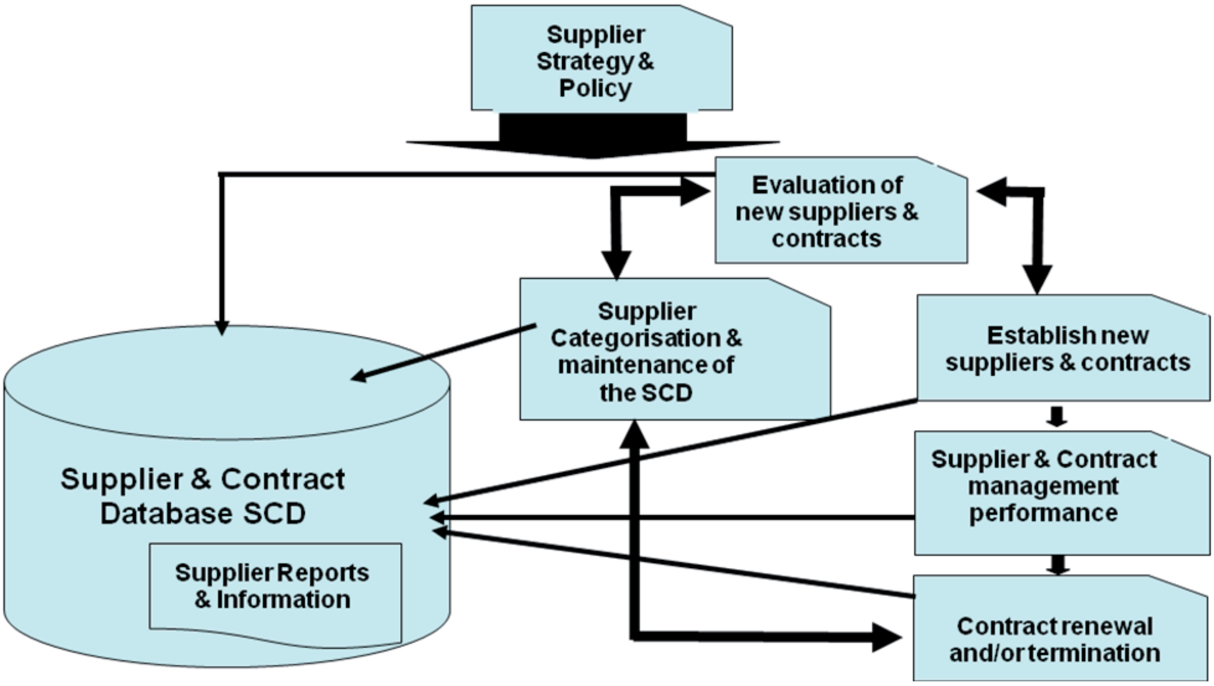
The purpose of the supplier management process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts.

The objectives of supplier management

The goal of the supplier management process is to manage suppliers and the services they supply, to provide seamless quality of IT service to the organisation, ensuring value for money is obtained.

The main objectives of the supplier management are to:

- Obtain value for money from suppliers and contracts
- Work with SLM to ensure UCs support and are aligned with business needs, SLRs and SLAs
- Negotiate and agree UCs and manage through their lifecycle
- Manage supplier relationships and performance
- Maintain a supplier policy and a Supplier and Contract Database (SCD)

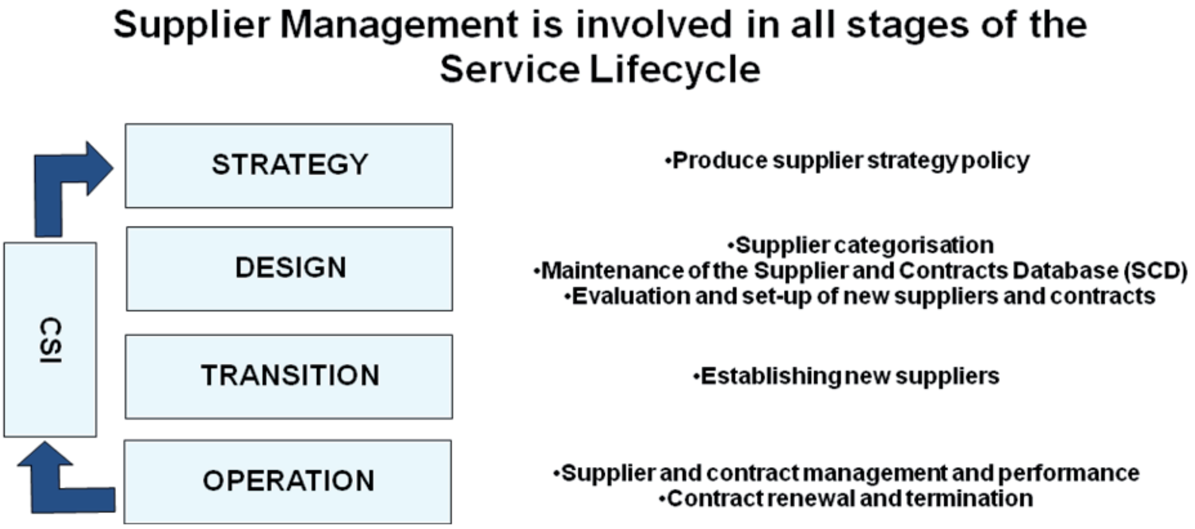

Supplier Strategy & Policy
Evaluation of new suppliers & contracts
Supplier Categorisation & maintenance of the SCD
Establish new suppliers & contracts
Supplier & Contract management performance
Contract renewal and/or termination
Supplier & Contract Database SCD
Supplier Reports & Information

The activities of supplier management

All supplier management process activity should be driven by service strategy and policy. In order to achieve consistency and effectiveness in the implementation of the policy, a Supplier and Contract Database (SCD) should be established.

Ideally, the SCD should form an integrated element of the larger service knowledge management system, recording all suppliers and contract details, together with the types of service, products etc provided by each supplier, and all the other information and relationships with other associated CIs.

This will also contribute to the information held in the service portfolio and service catalogue. The information within the SCD will provide a complete set of reference information for all supplier management procedures and activities.



Supplier Management is involved in all stages of the Service Lifecycle

•Produce supplier strategy policy

•Supplier categorisation
•Maintenance of the Supplier and Contracts Database (SCD)
•Evaluation and set-up of new suppliers and contracts

•Establishing new suppliers

•Supplier and contract management and performance
•Contract renewal and termination

Although supplier management is firmly placed within the service design Phase of the lifecycle, some of the activities are carried out in the other lifecycle phases too.

- Supplier categorisation and maintenance of the SCD (occurs within the service design phase)
- Evaluation and setup of new Suppliers and contracts (occurs within the service design phase)
- Establishing new suppliers (occurs within the service transition phase)
- Supplier and contract management and performance (occurs within the service operation phase)
- Contract renewal and termination (occurs within the service operation phase)

The terminology of supplier management

UC: Underpinning Contract.

SCD: Supplier and Contract Database.

SLR: Service Level Requirements.

SLA: Service Level Agreement.

SSIP: Supplier Service Improvement Plans – used to record all improvement actions and plans agreed between suppliers and service providers.

Supplier service reports: feedback gathered from all individuals that deal directly with suppliers. Results are collated and reviewed by supplier management, to ensure consistency in quality of service provided by suppliers in all areas. These can also be published in league tables to encourage competition between suppliers.

Shared risk and reward: e.g. agreeing how investment costs and resultant efficiency benefits are shared, or how risks and rewards from fluctuations in material costs are shared.

Supplier and contract review meetings: all details are recorded in meeting minutes.

Supplier and contract performance reports: used as input for the supplier and contract review meetings to manage the quality of the service provided by suppliers and partners. This should include information on shared risk, when appropriate.

Service catalogue management

Why have service catalogue management?

This process ensures that a service catalogue is produced, maintained and contains accurate information on all operational services and those being developed.

The purpose of service catalogue management is to provide a single source of consistent information on all of the agreed services, and ensure that it is widely available to those who are approved to access it.

The objectives of service catalogue management

- To ensure that a service catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally
- To manage the information contained within the service catalogue, and to ensure that it is accurate and reflects the current details, status, interfaces and dependencies of all services that are being run, or being prepared to run, in the live environment

The value to the business of a service catalogue

The service catalogue provides a central source of information on the IT services delivered by the service provider. This ensures that all areas of the organisation can view an accurate, consistent picture of the IT services, their details and their status. It contains a customer facing view of the IT services in use, how they are intended to be used, the organisation processes they enable, and the levels and quality of service the customer can expect for each service.

The activities of service catalogue management

The service catalogue management activities should include:

- Definition of the service
- Production and maintenance of an accurate service catalogue
- Interfaces, dependencies and consistency between the service catalogue and service portfolio
- Interfaces and dependencies between all services and supporting services within the service catalogue and the CMS
- Interfaces and dependencies between all services, and supporting components and Configuration Items (CIs) within the Service Catalogue and the CMS

The service catalogue has two aspects:

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

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

The terminology of service catalogue management

SLA: Service Level Agreements

SLR: Service Level Requirements

OLA: Operational Level Agreements

BIA: Business Impact Analysis

CI: Configuration Items