Table of Contents

Chapter 1: Introduction to ITIL

What is ITIL?

- As described by the officials, "ITIL is the most widely adopted approach for IT Service Management in the world. It provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business."
- It simply is a set of best practices in the field of IT Service Management.
- ITIL advocates that IT services must be aligned to the needs of the business and underpin the core business processes. It provides guidance to organizations on how to use IT as a tool to facilitate business change, transformation and growth.
- ITIL Best Practices also underpin the foundations of ISO/IEC 20000 (previously BS15000), the International Service Management Standard for organizational certification and compliance. Organizations can therefore implement ITIL to achieve organizational certification.

Trainer Note: *ITIL has been adopted by thousands of organizations worldwide, such as NASA, the UK National Health Service (NHS), HSBC bank and Disney™. ITIL is also supported by quality services from a wide range of providers including examination institutes, accredited training providers and consultancies, software and tool vendors and well known service providers such as IBM, Telefonica, HP and British telecom (BT).*

Best Practice

- Organizations operating in dynamic environments need to improve their performance and maintain competitive advantage.
- There are several sources for these best practices, e.g.:
  - Public frameworks and standards
    - validated across diverse environments
    - knowledge is widely distributed among professionals
    - there is publicly available training and certification
    - Acquisition of knowledge through the labour market is easier, as is collaboration and coordination across organizations.
  - Proprietary knowledge of organizations and individuals
    - This is customized for the local context and specific business needs
    - may only be available under commercial terms

The ITIL Framework

The ITIL framework is a source of best practice in service management. It is:

- 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, enabling organizations to:

ITIL ® is a registered trade mark of the Cabinet Office, United Kingdom

- Deliver value for customers through services, improving customer relationships
- Integrate the strategy for services with the business strategy and customer needs
- Measure, monitor and optimize IT services and service provider performance and reduce costs
- Manage the IT investment and budget, risks, knowledge, capabilities and resources to deliver services effectively and efficiently
- Enable adoption of a standard approach to service management across the enterprise
- Change the organizational culture to support the achievement of sustained success.

ITIL has been deployed successfully around the world for morethan 20 years.

Service Lifecycle

An approach to IT service management that emphasizes the importance of coordination and control across the various functions, processes and systems necessary to manage the full lifecycle of IT services. The service lifecycle approach considers the strategy, design, transition, operation and continual improvement of IT services.

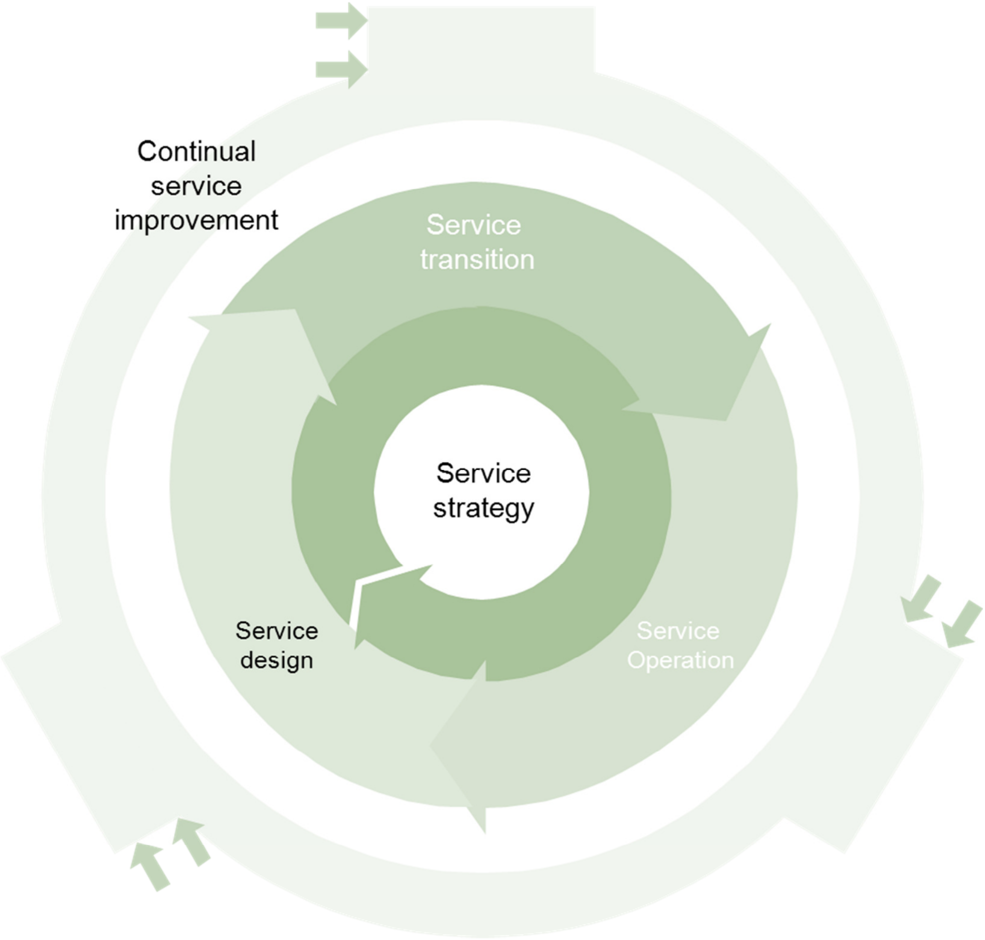


Figure: The ITIL service lifecycle

Overview of ITIL Certifications:

ITIL Foundation

The Foundation Level is the entry level qualification which offers delegates a general awareness of the key elements, concepts and terminology used in the ITIL Service Lifecycle, including the linkages between Lifecycle stages, the processes used and their contribution to Service Management practices.

This qualification is primarily aimed towards:

- those who require a basic understanding of the ITIL framework
- those who need understanding of how ITIL can be used to enhance the quality of IT service management within an organization
- IT professionals or others working within an organization that has adopted and adapted ITIL who need to be informed about, or contribute to an ongoing service improvement programme.

The ITIL qualification is open to any individuals who may have an interest in the subject.

The ITIL Foundation qualification is not intended to enable the holders of the qualification to apply the ITIL practices for Service Management without further guidance.

ITIL Intermediate Level

ITIL Intermediate level has a modular structure with each module holding a different focus. Delegates can take as few or as many Intermediate qualifications as they require, and to suit their needs. The Intermediate modules go into more detail than the Foundation level, and are an industry-recognised qualification.

Delegates who are seeking a management/team leader role in their company that requires a broad management focus of ITIL practice areas and work across teams or manage multiple capability areas, the Service Lifecycle modules will be of interest to them:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

For delegates who are looking to gain intense, specialized, process-level knowledge in one or more process, with focus on the day-to-day execution of ITIL practices, the Service Capability modules will be of interest:

- Service Offerings and Agreements
- Release, Control and Validation
- Operational Support and Analysis
- Planning, Protection and Optimization

Some individuals may wish to concentrate on one stream of modules, however delegates may also choose to select modules from both Service Lifecycle and Service Capability streams to gain a holistic view of an entire stage from both a high level management level and the detailed, technical perspective.

To be eligible for any of the Intermediate exams delegates need to complete mandatory accredited training.

ITIL Managing Across the Lifecycle Qualification

The ITIL Managing Across the Lifecycle (MALC) qualification is a capstone qualification which is the final required module that a candidate must take prior to achieving ITIL Expert Level.

The learning outcomes of MALC module are intended to bring a candidate from ITIL content knowledge to ITIL content application and integration knowledge, and to provide skills that can be used in the workplace in a tangible way.

This module is aimed at individuals who are interested in achieving the ITIL Expert Level, for which this module is a key requirement.

ITIL Expert Level

The ITIL Expert level of qualification is aimed at those individuals who are interested in demonstrating a superior level of knowledge of the ITIL Scheme in its entirety.

Achieving this level of ITIL qualification will benefit a candidate in both their personal and professional development, by aiding career advancement and progression within the IT Service Management field.

Candidates who achieve ITIL Expert level will also satisfy the prerequisite entry criteria for the ITIL Master Level; the highest level qualification within the ITIL scheme.

ITIL Master Qualification

The ITIL Master Qualification Certificate validates the capability of the candidate to apply the principles, methods and techniques from ITIL in the workplace.

To achieve the ITIL Master Qualification the candidate must be able to explain and justify how they selected and individually applied a range of knowledge, principles, methods and techniques from ITIL and supporting management techniques, to achieve desired business outcomes in one or more practical assignments.

For more details, please visit www.itil-officialsite.com.

SERVICE MANAGEMENT

To understand what service management is, we need to understand what services are, and how service management can help service providers to deliver and manage these services.

Service

A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. The term 'service' is sometimes used as a synonym for core service, IT service or service package.

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. 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.

Outcome

The result of carrying out an activity, following a process, or delivering an IT service etc. The term is used to refer to intended results as well as to actual results.

Services can be classified as:

- **Core services:** Deliver the basic outcomes desired by one or more customers
- **Enabling services:** Needed for a core service to be delivered
- **Enhancing services:** Added to core services to make them more appealing to the customer.

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.

PROCESSES AND FUNCTIONS

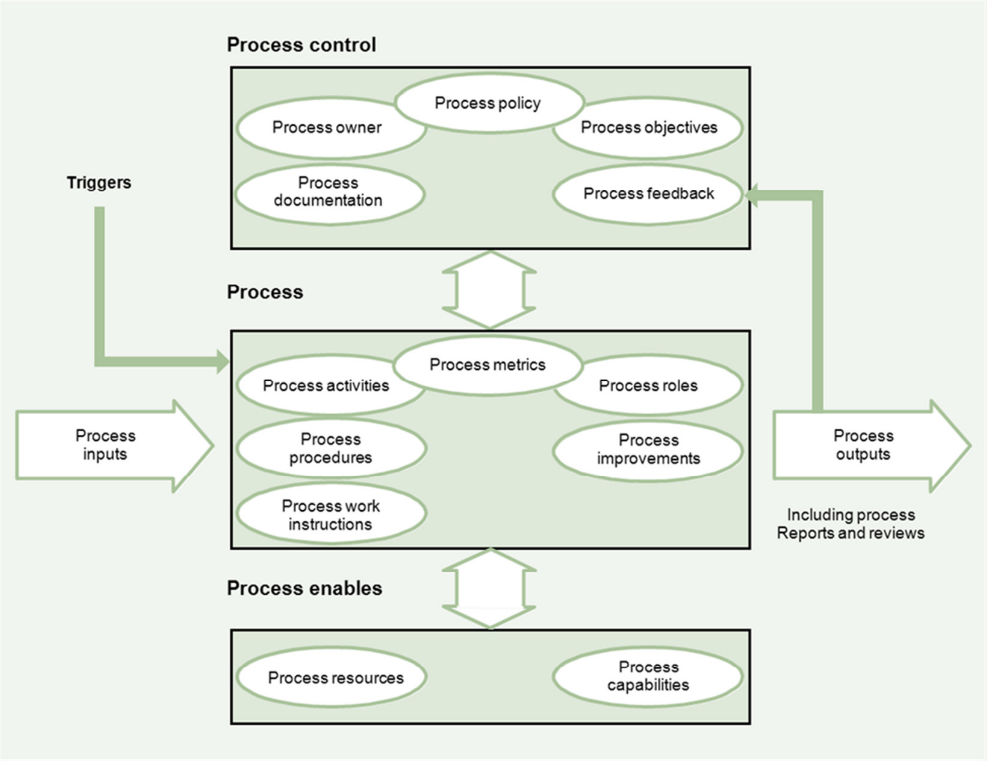
Process

A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. It may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions if they are needed.

Processes define actions, dependencies and sequence. Processes have the following characteristics:

- **Measurability** Processes can be measured and performance driven, in management terms such as cost and quality, and in practitioner terms such as duration and productivity
- **Specific results** Processes exist to deliver a specific result that is identifiable and countable
- **Customers** Processes deliver their primary results to a customer or stakeholder, either internal or external, to meet their expectations
- **Responsiveness to specific triggers** Processes may be ongoing or iterative, but should be traceable to a specific trigger.

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 organization structure of teams, groups or functions.



© Crown copyright 2013 Reproduced under licence from OGC

Figure: Process Model

Function

A team or group of people and the tools or other resources they use to carry out one or more processes or activities – for example, the service desk.

- Functions are self-contained with capabilities and resources necessary for their performance and outcomes. They provide structure and stability to organizations. Coordination between functions through shared processes is a common organizational design.
- ITIL Service Operation describes the service desk, technical management, IT operations management and application management functions in detail, with technical and application management providing the technical resources and expertise to manage the whole service lifecycle.

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 (e.g. process owner) and specific roles that are involved within a particular lifecycle stage or process.

Some of the generic roles are described below, whilst specific roles are covered in the relevant lifecycle chapters of the core ITIL publications.

Service manager

The term is commonly used to refer to a business relationship manager, a process manager or a senior manager with responsibility for IT services overall. A service manager is often assigned several roles such as business relationship management, service level management and continual service improvement (CSI).

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.

Process manager

The process manager role is accountable for operational management of a process. There may be several process managers for one process, for example for different locations.

The process manager role is often 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.

Process practitioner

A process practitioner is responsible for carrying out one or more process activities. The process practitioner role may be combined with the process manager role, if appropriate.

Responsibilities typically include:

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

Service owner

The service owner is responsible to the customer for the initiation, transition and ongoing maintenance and support of a particular service and accountable to the IT director or service management director for the delivery of a specific IT service.

Service ownership is critical to service management and a single 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 customer(s) for service-related enquiries and issues
- Representing the service across the organization, including in change advisory board (CAB) 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 service level agreements (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.

The RACI model

RACI model supports the idea of defining roles and responsibilities in relation to processes and their component activities, which run through an entire organization.

RACI is an acronym for:

- **Responsible** The person or people responsible for correct execution - for getting the job done
- **Accountable** The person who has ownership of quality and the end result. Only one person can be accountable for each task
- **Consulted** The people who are consulted and whose opinions are sought. They have involvement through input of knowledge and information
- **Informed** The people who are kept up to date on progress. They receive information about process execution and quality.

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

Chapter 2: Service Strategy

- Successful organizations tend to have a clear set of overall objectives, and a clear business strategy associated with those objectives.
- An IT strategy typically covers multiple aspects, including the IT technology strategy and the IT service strategy. The IT service strategy explains how IT services will be used to enable IT to achieve its objectives, and how IT services underpin the overall business strategy.

PURPOSE, OBJECTIVES, SCOPE AND VALUE OF SERVICE STRATEGY

Purpose and objectives

The purpose of the service strategy stage in the ITIL service lifecycle is to define the perspective, position, plans and patterns that a service provider needs to consider in order to be able to meet its organization's desired business objectives (the four Ps of service strategy).

A service strategy must identify:

- How the service provider intends to become, and remain, uniquely valuable to its customers
- The service provider's intended unique approach to creating and delivering value to its customers
- Its objectives in terms of the business outcomes it intends to enable
- The constraints the service provider must work within, including the competitive alternatives within which the service provider operates.

The objectives of the service strategy stage of the ITIL lifecycle include providing the service provider with:

- An understanding of what strategy is
- The necessary processes to:
  - Define its service strategy
  - Identify which services it needs to provide to achieve its strategy
  - Predict what levels of service demand it should expect as a result of its strategy
  - Determine what level of investment is required to achieve its strategy
  - Enable a working relationship between the service provider and its customers
- A clear definition of its services and the customers that use them
- A clear articulation of how services will be created, delivered and funded, who they will be delivered to and how each service delivers value
- Understanding of the organizational capability required to deliver the service strategy
- Clarity on which of its service assets are used to deliver each service and how the performance of these service assets can be optimized.

Scope

ITIL Service Strategy is intended for use by both internal and external service providers.

Two aspects of strategy are covered in ITIL Service Strategy.

- Defining a strategy whereby a service provider will deliver services to meet a customer's business outcomes
- Defining a strategy for how to manage those services.

Value to business

Any investment by a service provider in service strategy must deliver business value in return. The typical benefits gained from adopting and implementing service strategy best practice include:

- A greater ability to understand and articulate the links between the service provider's IT service assets, its activities and the critical outcomes its customers achieve as a result of using its services
- The service provider being seen by its organization and its customers to be contributing to value, not just to cost
- A more flexible and timely ability to adapt its IT services to pre-empt and meet changing business needs – ensuring increased competitive advantage over time
- A maintained portfolio of qualified services
- Improved use of IT investments, where service development investment is driven by business priorities and clear return on investment (ROI) analysis.

KEY PRINCIPLES

Utility and warranty

Customer perception of value from an IT service is influenced by the combination of two aspects of that service:

- utility (its fitness for purpose) and,
- warranty (its fitness for use).

Both utility and warranty must exist for an IT service to provide **value** to the customer.

Utility

Utility is the functionality offered by a product or service to meet a particular need. Utility can be summarized as 'what the service does', and can be used to determine whether a service is able to meet its required outcomes, or is 'fit for purpose'. The business value of an IT service is created by the combination of utility and warranty.

Warranty

Warranty is the assurance that a product or service will meet agreed requirements. This may be a formal agreement such as a service level agreement or contract, or it may be a marketing message or brand image. Warranty refers to the ability of a service to be available when needed, to provide the required capacity, and to provide the required reliability in terms of continuity and security.

Value creation through services

A physical product generally has some form of intrinsic value - its resale value. But the value of a service comes from what it enables someone to do, not from what the service is made from. Therefore, the value of a service is not determined by the service provider, but by the customer - whoever receives that service

Characteristics of value

The value of a service can be characterized in the following terms:

- Value is defined by the customer ***Trainer Note:*** *Irrespective of a service provider's suggested value for their service.*
- Affordable mix of features ***Trainer Note:*** *based upon which service offering has the most effective mix of features at a price they are willing to pay*
- Achievement of objectives ***Trainer Note:*** *from services that associate with business objectives*
- Value changes over time and circumstance

Trainer Note: *perception of what is valuable to them is likely to differ over time*

Creating value

It can be relatively simple to quantify the financial value of a service if it can be directly related to business outcomes that are also measured in financial terms. However, it is more difficult to evaluate the value of a service when related business outcomes are not directly linked to a monetary value.

There are additional factors that influence customer perception of value, in addition to just the ability of the service to enable the customer to achieve business outcomes. These additional contributory factors are the customer's preferences and the customer's perceptions.

Perception of value

A customer's perception of a service provider and of the value of the services from that service provider is influenced by:

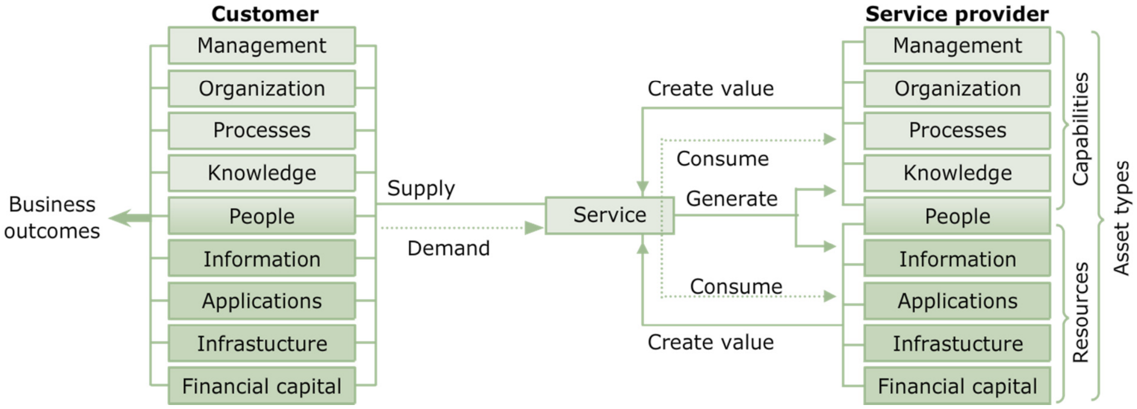
- The attributes of the services delivered
- The customer's present and prior experience of similar attributes. ***Trainer Note:*** *the supplier and the supplier's competitors and peers*
- The relative capability of the service provider's competitors
- The customer's self-image and position in its market. ***Trainer Note:*** *does the customer position itself as an innovator or as a low-risk option?*

Service providers need to understand, articulate and measure how effective their services are in enabling their customers to achieve their desired outcomes and consider any potential differences between what the customer perceives as valuable and what the service provider believes it provides.

The economic value is the total value that the customer perceives the proposed service will deliver, including the reference value. This is the overall measure of the customer's perception of their ability to meet their desired outcomes when using the proposed service.

Assets, resources and capabilities

Any IT service provider would have a set of assets that it uses to create IT services for its customers.



© Crown copyright 2013 Reproduced under license from OGC

Figure: The interaction of service provider and customer assets

Assets

Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.

Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure or financial capital.

Customer asset: Any resource or capability used by a customer to achieve a business outcome.

Service asset: Any resource or capability used by a service provider to deliver services to a customer.

Resource

This is a generic term that includes IT infrastructure, people, money or anything else that might help to deliver an IT service. Resources are considered to be assets of an organization.

Capability

The ability of an organization, person, process, application, IT service or other configuration item to carry out an activity. Capabilities are intangible assets of an organization.

Key differences between Resources and Capabilities	
Resources	Capabilities
Can be acquired any time, as per the need.	Can typically only be developed over time.
Are the basic direct inputs to the production of a service	Represent the organization's ability to effectively coordinate, control and deploy its resources to produce value
Relatively easy to acquire	reflect the organization's ability to embed its experience and knowledge into its people, processes and technologies

Patterns of business activity

A workload profile of one or more business activities. Patterns of business activity are used to help the IT service provider understand and plan for different levels of business activity.

Business activity is performed by the customer's assets, and this activity tends to be performed in distinct patterns, these being known as 'patterns of business activity' (PBA).

PBA definitions typically include:

- **Classification:** An indication of the type of PBA, such as where the activity originates (user or automated), the type and impact of the outcomes, and the type of workload.
- **Attributes:** The frequency, volume, location and duration of the activity.
- **Requirements:** Aspects such as the performance, security, availability and tolerance for delays.
- **Service asset requirements:** A utilization profile for the PBA, describing what assets it uses, when and in what quantity.

Service portfolio

The service portfolio describes services currently being considered and being developed by the service provider, along with its present contractual commitments, on-going service improvement plans (SIPs), and retired services those services that the service provider no longer provides).

A service portfolio also includes any third-party services that are used by the service provider as an integral component of its service offerings to its customers.

Service Portfolio

The complete set of services that is managed by a service provider. The service portfolio is used to manage the entire lifecycle of all services, and includes three categories: service pipeline (proposed or in development), service catalogue (live or available for deployment), and retired services.

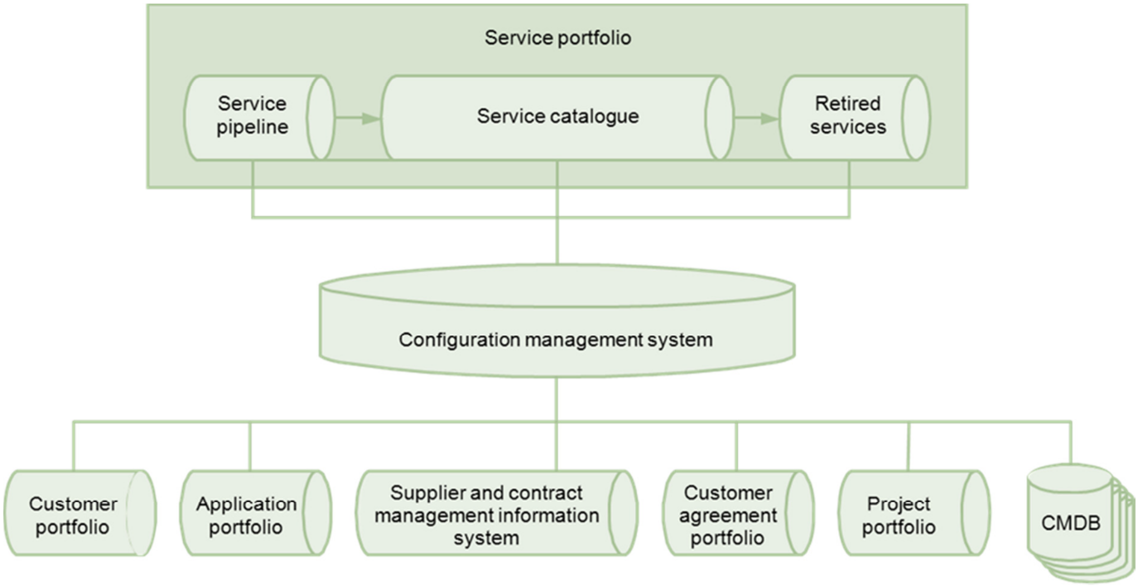


Figure: The service portfolio

Governance

Ensures that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

Trainer Note: *It defines the overall common direction, policies and rules that both the business and IT use to conduct business. The international standard for corporate governance of IT is ISO/IEC 38500*

Business case

Justification for a significant item of expenditure. The business case includes information about costs, benefits, options, issues, risks and possible problems.

A business case is typically required whenever a major investment decision needs to be taken. It is a decision support and planning tool that explains the objectives of a proposed initiative and the specific business impacts (costs, risks and benefits) that the initiative is expected to generate.

A business case for investment in a new service generally includes the following elements:

- Introduction
- Business impacts
- Risk and contingencies
- Recommendations

Risk management

The process responsible for identifying, assessing and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in 'risk assessment and management'. Risk management is relevant across the entire service lifecycle.

Planning for risk management essentially involves:

- Identifying the risks
- **Analysing the risks:** Once a list of potential risks has been compiled, the impact and probability of each risk can be assessed. The impact is the effect on the project if the risk becomes reality. ***Trainer Note:*** *This analysis describes the consequences (used to define how to deal with risks) and impacts along with some form of associated numeric value (used to rank the risks).*
- Once the project risks have been identified and analysed, a risk management **plan** is built to **control** and address these risks. The risks and the plan then need to be regularly reviewed to check that appropriate actions have taken place and have been successful.

A core principle of risk management is the recognition that project risks may become more or less probable over the duration of a project, and their potential impact may also change as the project progresses.

Service providers

To successfully execute against its service strategy, a service provider must achieve a real understanding of who its customers are, who its target customers should be and what business outcomes it wants to enable.

In short, a Service Provider is any organization supplying services to one or more internal customers or external customers. Service provider is often used as an abbreviation for IT service provider. Similarly, an IT service provider is any organization supplying services to one or more internal customers or external customers. Service provider is often used as an abbreviation for IT service provider.

Service providers fall into three broad categories:

- **Type I - internal service provider:** Exists within a business unit solely to deliver IT services to that one specific business unit. There could be multiple Type I service providers in an organization.
- **Type II - shared services unit:** An internal service provider delivering IT services to multiple business units in the same organization.
- **Type III - external service provider:** Provides IT services to external customers.

Stakeholders in service management

Service providers have many different internal stakeholders, including the functions, groups and teams that deliver the services. External stakeholders include:

- **Customers:** Those who buy goods or services. For an IT service provider, this is the person or group who defines and agrees the service level targets.
- **Users:** Those who use the service on a day-to-day basis, as distinct from a customer who may not use the IT service directly. Users may not necessarily be within the customer organization.
- **Suppliers:** Third parties responsible for supplying goods or services required to deliver IT services.

Internal and external customers

- **Internal customers:** People or departments who work for the same organization as the IT service provider.
- **External customers:** People who work for a different organization or organizations that are separate legal entities from the IT service provider and purchase services via a legally binding contract or agreement.

Both internal and external customers must be provided with the agreed level of service, with the same levels of customer service. However, the way that services are designed, transitioned, delivered and improved is often different.

Differences between internal and external customers include:

- Funding and accounting
- Links to business strategy and objectives
- Involvement in service design, transition and operation
- Drivers for improvement.

Internal and external services

Internal services are delivered between departments within the same organization, whereas **external services** are delivered to customers outside of the service provider's overall organization.

By classifying its services into 'supporting', 'internal' and 'external' categories, a service provider can differentiate between services that support an internal activity from services that actually achieve business outcomes for external customers:

- **Supporting services:** Services not directly used by the business or external customers, enabling the IT processes and services used by the IT service provider to provide other services. The performance of supporting services is managed by OLAs.
- **Internal customer-facing services:** Services directly supporting one or more business processes that are managed by an internal customer. These services are managed by Service Level Agreements(SLA) and are underpinned by supporting services.
- **External customer-facing services:** Services that are supplied directly from IT to external customers. These services are provided to enable the overall organization to meet certain strategic objectives, and as such, are business services in their own right. These services are managed through contracts.

Service model

A model that shows how service assets interact with customer assets to create value. Service models describe the structure of a service (how the configuration items fit together) and the dynamics of the service (activities, flow of resources and interactions). A service model can be used as a template or blueprint for multiple services.

PROCESSES AND ACTIVITIES

Process 1: Service portfolio management

Purpose and objectives

- The purpose of service portfolio management is to ensure that a service provider has the right mix of services to meet its overall service strategy.
- It is the governance process of the service portfolio - the process by which a service provider manages its investments across the service lifecycle, considering each service in terms of the business value it provides.

The objectives of service portfolio management include:

- Enabling a service provider to investigate and make decisions on which services to provide and which to retire, based on an analysis of the risk and potential return
- Management of a definitive portfolio of services, including a clear articulation of the business needs that each service addresses and the business outcomes it supports
- Evaluation of the degree to which each of its services enables the service provider to achieve its service strategy
- Control of which services are offered, under what conditions and at what level of investment
- To track each investment in service throughout the lifecycle of each service.

Scope

The scope of service portfolio management encompasses:

- Services that are planned to be delivered
- Services that are currently being delivered
- Services that have been withdrawn from service (retired).

An internal service provider's execution of service portfolio management requires them to work closely with each business unit in the organization to assess service investment and returns.

External service providers tend to be able to evaluate the value of each service more overtly, as each service should either directly generate profit or support services that are profit generating.

Process 2: Financial management for IT services

Purpose and objectives

The purpose of financial management for IT services can be summarized as:

- To secure the appropriate level of funding to design, develop and deliver the IT services required to support the service strategy
- To ensure that the IT service provider does not commit to services that it is unable to deliver
- To identify the balance between service cost and quality, and supply and demand.

Objectives include:

- Define and maintain a framework to:
    - Secure funding to manage the provision of services
    - Identify, manage and communicate the cost of providing services
    - Recover costs of service provision (and required profit, in the case of external service providers)
- Evaluate the financial impact of new or changed strategies
- Execute enterprise and IT service provider specific financial policies and practices
- Account for the money spent in the development, delivery and support of services
- Forecast the financial requirements for the service provider.

Scope

It has three core aspects, each of which generally has an annual planning cycle and a monthly operational monitoring and reporting cycle:

- **Accounting:** Mechanisms by which the IT service provider accounts to its overall organization for the way its money was spent.
- **Budgeting:** Predicting and controlling the service provider's income and expenditure. Achieved through periodic negotiation cycles in which budgets are typically set annually and actual financial performance against these budgets is reported monthly.
- **Charging:** How the IT service provider bills its customers for services supplied.

Process 3: Business relationship management

Purpose and objectives

Business relationship management is the process that enables business relationship managers (BRMs) to provide effective links between the service provider and its customers, so that the service provider can understand the business requirements of their customers and provide services that meet the needs of their customers.

The purpose of the business relationship management process includes:

- Enabling effective business relationships between the service provider and its customers.

- Identifying customer needs and ensuring that the service provider continues to recognize and understand each customer and their individual business needs as they change over time.
- Assisting the customer to understand the value of the service(s) provided and ensuring customer expectation does not exceed what they are willing to pay for.
- Ensuring that the service provider fully understands the customer requirement and is able to meet the customer's expectations before agreeing to deliver the service.

Business relationship management objectives include enabling the service provider to:

- Prioritize its services and service assets to meet their customers' perspective of service requirements
- Sustain high levels of customer satisfaction
- Establish and maintain constructive business relationships with its customers
- Identify changes in its customers' environments and technology trends that could impact the services to individual customers
- Establish and articulate its customers' business requirements for services
- Mediate in situations where there are conflicting requirements for services from different customers
- Establish formal complaints and escalation procedures for each of its customers.

Scope

The scope of business relationship management for internal service providers focuses on the alignment of objectives of the various business units with the activities of the IT service provider.

The business relationship management process focuses on understanding and communicating:

- Business outcomes that the customer wants to achieve
- Services currently provided to the customer
- How services are currently delivered
- Technology trends that may impact current services, and the nature of the potential impact upon each customer
- Customer satisfaction, and the status of any plans to address dissatisfaction
- How the service provider is represented to the customer.

Business relationship management focuses on a more strategic level - to ensure the service provider is meeting the customer's overall needs, while SLM focuses on ensuring agreed levels of service are provided to the customer and users.

TECHNOLOGY CONSIDERATIONS

Service automation

Service automation can improve the utility and warranty of services, providing advantages such as:

- It is easier to adjust the capacity of automated resources in response to changes in demand volumes and patterns
- Automated resources make it easier to respond to changes in requirements, and enable greater flexibility to serve demand across time zones and out of normal business hours
- Automated systems produce high degrees of consistency
- Scheduling, routing and allocation of resources is complex and time consuming and an ideal candidate for automation
- Automation enables effective capture, codification and distribution of knowledge throughout the service provider's organization in a consistent and secure manner, and reduces the risk of knowledge being lost through staff movement.

Automation of service processes can significantly contribute to improved service quality and reduced service costs and risks.

Service management can particularly benefit from automation in the areas of:

- Design and modelling
- Service catalogue
- Pattern recognition and analysis
- Classification, prioritization and routing
- Detection and monitoring
- Optimization.

Service analytics and instrumentation

Service analytics techniques are used throughout service management to apply context and understanding to service data captured from multiple sources.

Instrumentation techniques include:

- **Asynchronous capture:** Passive listeners scanning for alerts
- **External source:** Compilation of data from external sources such as service desk tickets, supplier notifications and enterprise resource planning systems
- **Manual generation:** Manually create or alter an event
- **Polling:** Monitoring systems actively interrogate functional elements on a regular basis
- **Synthetic transactions:** Simulation of end-user experience through known transactions.

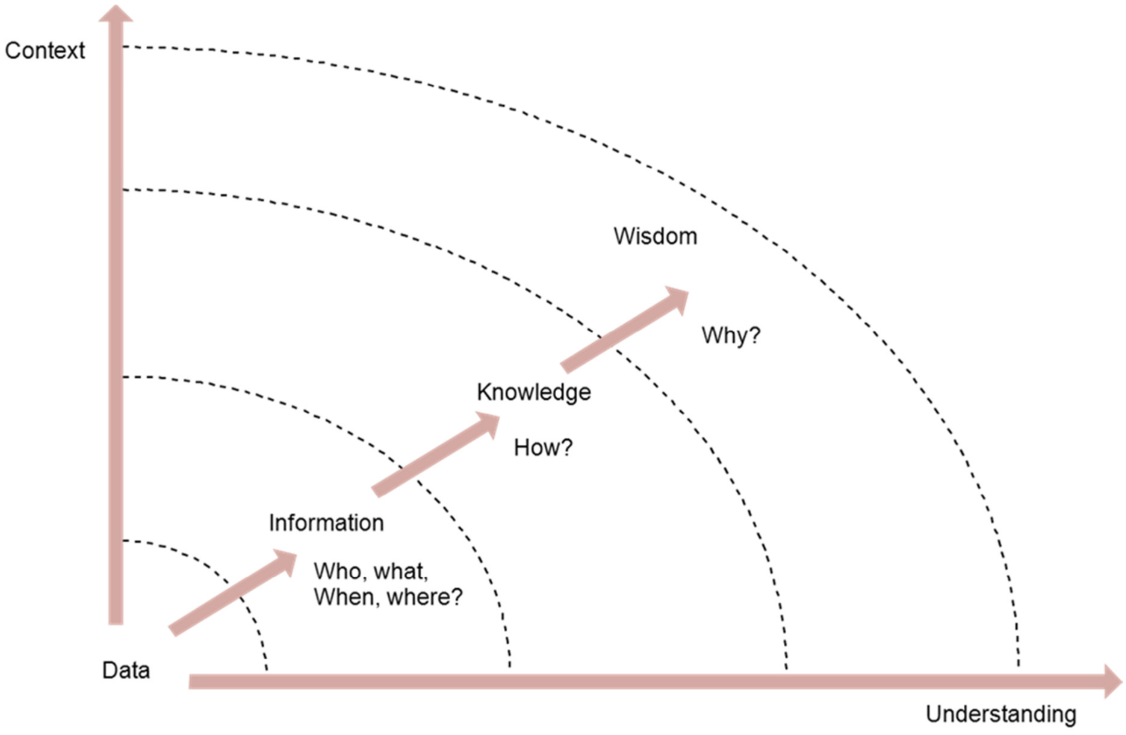


Figure: The flow from data to wisdom

Service analytics and instrumentation are critical to event management, where usable and actionable information is produced from monitoring data. Common event management techniques include:

- **Compression:** Consolidation of multiple identical alerts into a single alert
- **Correlation:** Analysis to identify if multiple alerts from various sources happening during a short period of time have any relationship
- **Filtering:** Applying rules to a single alert source over some period of time
- **Intelligent monitoring:** Applying adaptive instrumentation that automatically tunes the monitoring techniques according to system status
- **Roll-up:** Compression of alerts through the use of hierarchical collection structures
- **Verification:** Active confirmation of an actual incident.

Chapter 3: Service design

For services to provide true value to the business, they must be designed with the business objectives in mind. Service design is the stage in the lifecycle that turns a service strategy into a plan for delivering the business objectives.

PURPOSE, OBJECTIVES, SCOPE AND VALUE OF SERVICE DESIGN

Purpose and objectives

The purpose of service design is to:

- Design IT services, governing IT practices, processes and policies
- Realize the service provider's strategy
- Facilitate the introduction of services
- Ensure quality service delivery, customer satisfaction and cost-effective service provision.

The objective is to:

- Design IT services so effectively that minimum improvement during their lifecycle will be required
- Embed continual improvement in all service design activities to ensure that solutions become even more effective over time
- Identify changing trends in the business that may offer improvement opportunities.

Scope

Service design starts with a set of new or changed business requirements and ends with the development of a service solution designed to meet those requirements.

There are five aspects to service design, covering the design of:

- Service solutions for new or changed services
- Management information systems and tools
- Technology architectures and management architectures
- The processes required
- Measurement methods and metrics.

Value to business

A standard and consistent service design approach:

- Reduces total cost of ownership (TCO)
- Improves the quality, consistency and performance of service
- Eases the implementation of new or changed services
- Improves alignment with business needs and with customer values and strategies
- Improves IT governance
- Improves effectiveness of service management and IT processes
- Improves information and decision-making.

KEY PRINCIPLES

The four Ps of service design

It is key to recognize the importance of the four Ps to successful service provision:

- People
- Processes
- Products (services, technology and tools)
- Partners (supplier, manufacturers and vendors).

Many designs, plans and projects fail through a lack of preparation and management. The implementation of ITSM as a practice is about preparing and planning the effective and efficient use of the four Ps.

The five design aspects

Service design takes into consideration five major aspects of service provision (as discussed earlier in "Scope", Page 23) for which the design activities must be carried out.

Designing service solutions

A formal and structured approach is required to produce a service with the right balance of functionality and cost within agreed timescales.

The areas to be considered include:

- Analyse the business requirements
- Explore opportunities for re-use
- Produce service solution designs
- Create and maintain the service acceptance criteria (SAC)
- Evaluate and cost alternative designs
- Agree the expenditure, budgets and timelines through to deployment of the service
- Re-evaluate and confirm the business benefits
- Agree the preferred solution and its planned outcomes and targets
- Ensure the solution is in line with strategies, policies, architecture and make proposals for change if not
- Ensure corporate and IT governance and security controls are taken into account
- Complete an organizational readiness assessment
- Identify requirements for suppliers and supporting contracts
- Assemble the service design package (SDP).

Designing management information systems and tools

The most effective way of managing all aspects of services through their lifecycle is by using appropriate management systems and tools, including:

- Service portfolio
- Service knowledge management system (SKMS)
- Configuration management system (CMS)
- Capacity management information system (CMIS)

- Availability management information system (AMIS)
- Security management information system (SMIS)
- Service continuity management information system.

Designing technology architectures and management architectures

Architectural design within an IT organization provides the strategic blueprints for the development and deployment of an IT infrastructure that will satisfy the needs of the business. It involves the development and maintenance of:

- IT policies
- Strategies
- Architectures
- Designs
- Plans
- Processes.

An Architecture for any system should consider its constituent components; their relationship to each other and how they interact; the relationship between the system and its environment; the design principles that inform, guide and constrain its structure and operation, as well as its future development.

The five areas to consider when designing a suitable management architecture are:

- Business requirements
- People, roles and activities
- Processes and procedures
- Management tools
- Technology.

Management architectures need to be business-aligned, not technology-driven.

Designing processes

A process model enables understanding and helps to articulate the distinctive features of a process.

Each process is owned by a process owner, who is accountable for the process, its improvement and for ensuring it meets its objectives.

Process outputs are expected to conform to operational norms, and where this is the case, the process can be considered to be effective.

Designing measurement methods and metrics

To effectively manage processes and their outcomes they have to be measured. The measurements and metrics selected need to reflect the goals and objectives of the process being measured.

Where possible, metrics need to be driven by organizational goals and developed to operate in a hierarchical way – a metrics tree - so that detailed technical operational and process metrics, at the lowest levels, can be aggregated and reported at a higher level to demonstrate service performance against SLAs.

The balanced scorecard is an example of a tool that can be used to develop a set of organizational metrics and measures in this way.

The service design package

Document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. A service design package is produced for each new IT service, major change, or IT service retirement.

The service design package is assembled using the output from the various processes, methods and techniques employed throughout service design, and is the foundation document supporting the subsequent transition, operation and continual improvement of the new or changed service.

At a high level the SDP includes the following:

- Requirements
- Service design
- Organizational readiness assessment
- Service lifecycle plans including programme, transition and
- operational acceptance plans
- Service acceptance criteria (SAC).

PROCESSES AND ACTIVITIES

Process 1: Design coordination

Purpose and objectives

The purpose of design coordination is to ensure the goals and objectives of the design stage are met. It provides a single point of coordination and control for all activities and processes within this stage of the service lifecycle.

The objectives of the design coordination process are to:

- Ensure the consistent design of appropriate services, service management information systems, architectures, technology, processes, information and metrics to meet current and evolving business needs and requirements
- Plan and coordinate all design activities
- Produce SDPs based on service charters and change requests
- Ensure that appropriate service designs are produced and that they are handed over to service transition as agreed
- Manage the interfaces with service strategy and service transition
- Improve the efficiency and effectiveness of service design activities and processes.

Scope

The scope of design coordination includes all design activity. Some design efforts will be part of a project and others will be managed through the change process alone, without a formally defined project. Typically, major changes require the most attention from design coordination but any change that could benefit from design coordination may be included. Each organization should define criteria to determine the level of attention to be applied in design coordination for each design.

Process 2: Service level management

Purpose and objectives

The purpose of the service level management (SLM) process is to ensure that all current and planned IT services are delivered to agreed achievable targets.

The objectives of SLM are to:

- Define, document, agree, monitor, measure, report and review the level of IT services provided
- Improve the relationship and communication with the business and customers
- Ensure that specific and measurable targets are developed
- Monitor and improve customer satisfaction
- Ensure a clear and unambiguous expectation of the level of service to be delivered
- Ensure continual improvement to the levels of service, even when all agreed targets are met.

Scope

SLM acts to represent the service provider to the business and the business to the service provider.

It manages the expectations and perceptions of the business, customers and users, and ensures that the service provided is in line with those expectations. Its focus extends beyond currently delivered services to involvement in the design of new or changed services, producing and agreeing the service level requirements for these services.

Principles and basic concepts

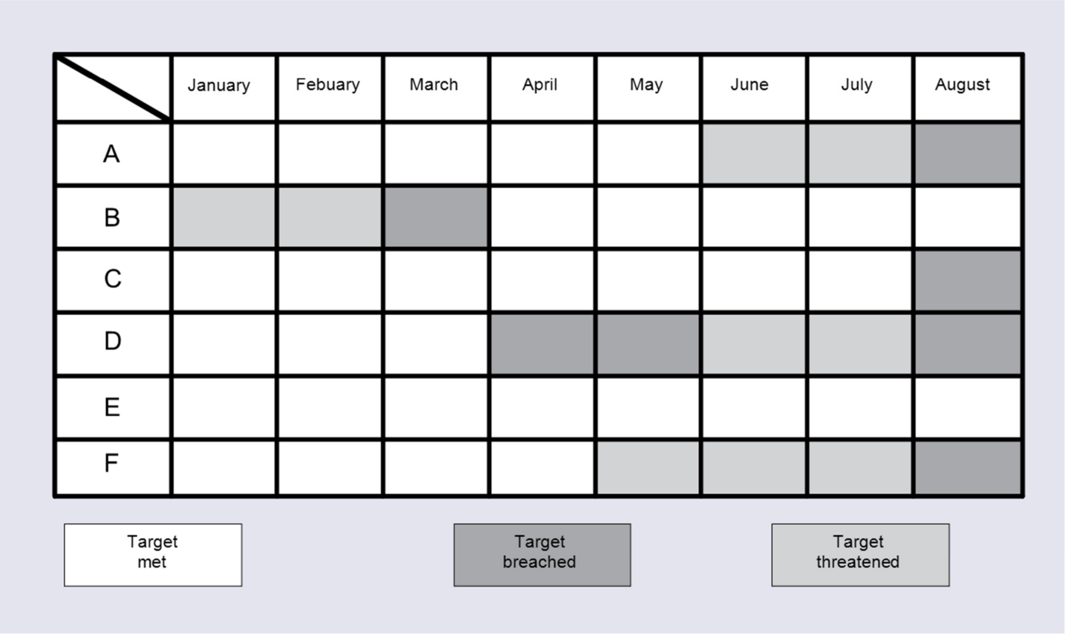
Service level requirements

An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers.

SLAs provide the basis for managing the relationship between the service provider and the customer. Whereas, SLM develops SLAs for all services and ensures the service continues to be delivered in line with the agreements made in the SLA.

Service level agreement monitoring (SLAM) chart

A service level agreement monitoring (SLAM) chart monitors and reports achievements against service level targets. Such a chart is typically colour-coded to show whether each agreed service level target has been met, missed or nearly missed during each of the previous 12 months.



	January	Febuary	March	April	May	June	July	August
A	□	□	□	□	□	▨	▨	■
B	▨	▨	■	□	□	□	□	□
C	□	□	□	□	□	□	□	■
D	□	□	□	■	■	▨	▨	■
E	□	□	□	□	□	□	□	□
F	□	□	□	□	▨	▨	▨	■

□ Target met
■ Target breached
▨ Target threatened

Figure: SLA monitoring (SLAM) chart

Service level agreement frameworks

When designing SLA frameworks, options available include:

- **Service-based SLAs:** The SLA describes a specific IT service to be delivered.
- **Customer-based SLAs:** All IT services delivered to a specific customer are described.
- **Multi-level SLAs:** For example, from corporate down through customer to service, where the agreements at each level are inherited by those at the next. This helps with ongoing maintenance, making the SLAs easier to work with. The information at the higher levels is subject to less frequent change and is not repeated in every lower-level SLA.

Where service delivery relies on supporting services provided either by other departments or by external suppliers, SLM ensures that operational level agreements (OLAs) and contracts are in place to underpin the service delivery targets in the SLA.

Operational Level Agreement (OLA)

An agreement between an IT service provider and another part of the same organization. It supports the IT service provider's delivery of IT services to customers and defines the goods or services to be provided and the responsibilities of both parties.

Underpinning contract

A contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The underpinning contract defines targets and responsibilities that are required to meet agreed service level targets in one or more service level agreements.

Service review

This constitutes meetings held on a regular basis with customers (or their representatives) to review the service achievement in the previous period and to preview any issues for the coming period. The customer and provider should be actioned as appropriate to improve weak areas where targets are not being met. Analysis of the cost and impact of service breaches provides valuable input and justification of service improvement plan (SIP) activities and actions.

Service improvement plan

A formal plan to implement improvements to a process or IT service.

Service level management and business relationship management

While SLM focuses on ensuring agreed levels of service are provided to the customer and users, business relationship management focuses on a more strategic level - to ensure the service provider is meeting the customer's overall needs.

Process activities, methods and techniques

The key activities for SLM are:

- Design SLA frameworks
- Determine, document and agree requirements for new services and produce SLRs
- Negotiate, document, agree, monitor and report on SLAs for operational services
- Conduct service reviews and instigate improvements within an overall SIP
- Collate, measure and improve customer satisfaction
- Review and revise SLAs, OLAs, service scope and underpinning agreements.

Triggers, inputs, outputs and interfaces

Triggers

- Changes in the service portfolio
- New or changed SLRs, SLAs, OLAs or contracts
- Service breaches or threatened breaches
- Periodic activities - reviewing, reporting and customer satisfaction surveys
- Changes in strategy or policy.

Inputs

- Business requirements
- Strategies, policies and constraints from service strategy
- The service portfolio and the service catalogue
- Customer and user feedback
- Improvement opportunities from the CSI register.

Outputs

- Service reports
- Service improvement opportunities
- SIP
- SLRs, SLAs, and OLAs.

Interfaces

- Business relationship management ***Trainer Note****: Provides a full understanding of the needs and priorities of the business. Ensures customers are appropriately involved and represented.*
- Service catalogue management ***Trainer Note:*** *Provides information about services and their interfaces and dependencies. Identifies customers/business units that need to be engaged by SLM.*
- Incident management ***Trainer Note:*** *Provides data to demonstrate performance against SLA targets. Ensures incidents are resolved in line with SLA targets.*
- Supplier management ***Trainer Note:*** *Ensures supplier and contractual targets align with SLAs.*
- Availability, capacity, IT service continuity and information security management (ISM) ***Trainer Note:*** *Support definition of service level targets related to the specific area of responsibility.*
- Design coordination ***Trainer Note:*** *Ensures that the overall service design activities are completed successfully.*

Process 3: Service catalogue management

Service catalogue

A database or structured document with information about all live IT services, including those available for deployment. The service catalogue is part of the service portfolio and contains information about two types of IT service: customer facing services that are visible to the business; and supporting services required by the service provider to deliver customer facing services.

Purpose and objectives

The service catalogue is a single source of consistent information on all of the agreed services. The objective of service catalogue management is to manage the information contained within the service catalogue and to ensure that it is accurate and current.

Scope

The scope is to provide and maintain accurate information on all services that are being transitioned, or have been transitioned, to the live environment.

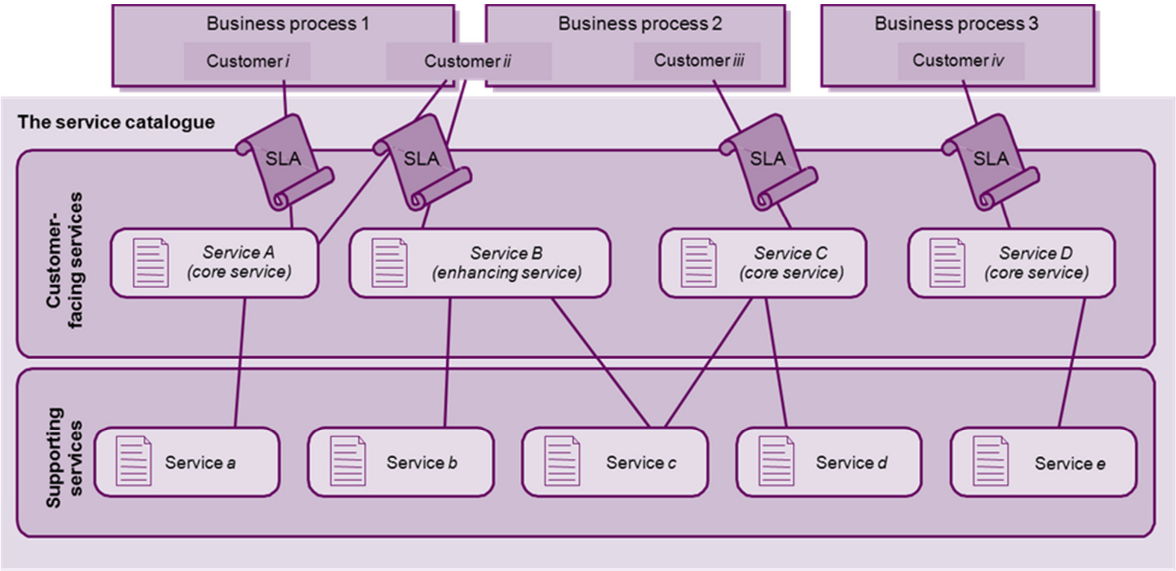
Principles and basic concepts

The service catalogue is part of the service portfolio. The service catalogue contains details of all services from the point they are 'chartered' as part of the service strategy stage. It contains details of services as they progress through the design, transition and operation stages of the service lifecycle.

It is recommended that a service provider defines two different views of the service catalogue. This is referred to as a **two-view service catalogue**:

- Business / customer service catalogue: Contains details of the IT services delivered to the customers (customer-facing services), links to the business units and the business processes they support and provides the customer view of the service catalogue.
- Technical/supporting service catalogue: Contains details of the supporting IT services delivered, links to the customer facing services and configuration items (CIs) and other supporting services necessary to deliver the service.

The number of views defined depends on the audiences to be addressed and the uses to which the catalogue will be put.



© Crown copyright 2013 Reproduced under licence from OGC

Figure: Two-view service catalogue

Trainer Note: *a three-view service catalogue may be created to distinguish the customer-facing services available to different customers, or different types of customer, e.g. wholesale versus retail customers.*

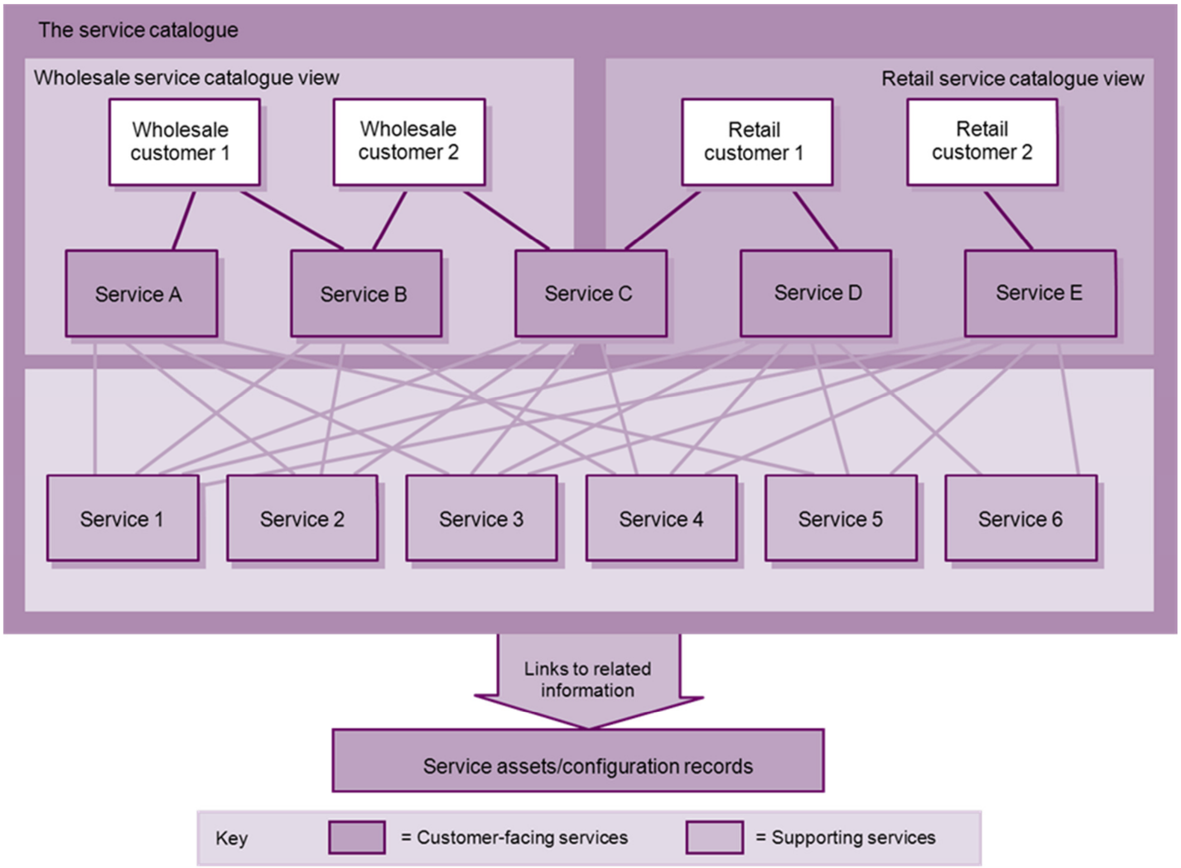


Figure: Three-view service catalogue

Process 4: Availability management

Availability management

Purpose and objectives

Availability management ensures that the level of availability delivered in all IT services meets the agreed availability needs in a cost-effective and timely manner. It is concerned with meeting both the current and future availability needs of the business.

The objectives of availability management are to:

- Produce and maintain the availability plan, reflecting the current and future needs of the business, and to provide guidance to the business and IT on availability-related issues
- Ensure that availability achievements meet or exceed targets and, where they do not, assist with the diagnosis and resolution of related incidents and problems
- Assess all changes for their impact on the availability plan and proactively improve availability, where cost-justifiable to do so.

Scope

Availability management covers the design, implementation, measurement, management and improvement of IT service and component availability. It commences as soon as the availability requirements are clear and is an on-going process, finishing only when the IT service is decommissioned or retired.

Principles and basic concepts

Availability

Ability of an IT service or other configuration item to perform its agreed function when required. Availability is determined by reliability, maintainability, serviceability, performance and security. Availability is usually calculated as a percentage. This calculation is often based on agreed service time and downtime. It is best practice to calculate availability of an IT service using measurements of the business output.

Availability management is completed at two interconnected levels:

- **Component availability:** Involves all aspects of component availability
- **Service availability**: Involves all aspects of service availability and the actual, or potential, service impact of component availability.

Availability management focuses on the following key aspects, which influence the overall availability and the business perception of unavailability:

- **Availability:** The ability to perform an agreed function when required
- **Reliability:** How long an agreed function can be performed without interruption
- **Maintainability**: How quickly and effectively agreed functionality can be returned after a failure
- **Serviceability:** The ability of a third-party supplier to meet the terms of its contract, including agreed levels of availability, reliability and maintainability for a supporting service or component.

Availability management identifies **vital business functions (VBFs)** and takes these into account when making design recommendations.

Process 5: Information security management

Purpose and objectives

Information security management (ISM) is a governance activity within the corporate governance framework. It provides the strategic direction and is the focal point for all security activities.

The purpose of ISM is to align IT security with business security and to ensure it matches the agreed needs of the business.

The objective is to protect the interests of those relying on information, and the systems and communications that deliver the information, from harm as a result of failures of confidentiality, integrity and availability.

Scope

ISM needs to understand:

- Business security policy and plans

- Current business operation and its security requirements
- Future business plans and requirements
- Legislative requirements
- Obligations and responsibilities with regard to security contained within SLAs
- Business and IT risks and their management.

ISM raises awareness across the organization of the need to secure all information assets.

Principles and basic concepts

Information security policy

The information security policy should have the full support and commitment of top executive IT and business management, covering all areas of information security and appropriate to meet the ISM objectives.

ISO/I EC 27001 is the formal standard against which organizations may seek independent certification of their ISMS.

Process 6: Supplier management

Purpose and objectives

The purpose of supplier management is to obtain value for money from suppliers and to provide seamless quality of service to the business.

The objectives of supplier management are to:

- Obtain value for money from all suppliers and contracts
- Ensure that underpinning contracts (UCs) and agreements with suppliers are aligned with business needs, and support and align with agreed targets
- Manage supplier performance and relationships with the suppliers
- Negotiate and agree contracts with suppliers and manage them throughout their lifecycle
- Maintain a supplier policy and a supporting supplier and contract management information system (SCMIS).

Scope

The supplier management process includes the management of all suppliers and contracts needed to support the IT services. The process recognizes the supplier's value contribution and builds and manages a relationship that sustains that contribution.

Principles and basic concepts

Supplier categorization

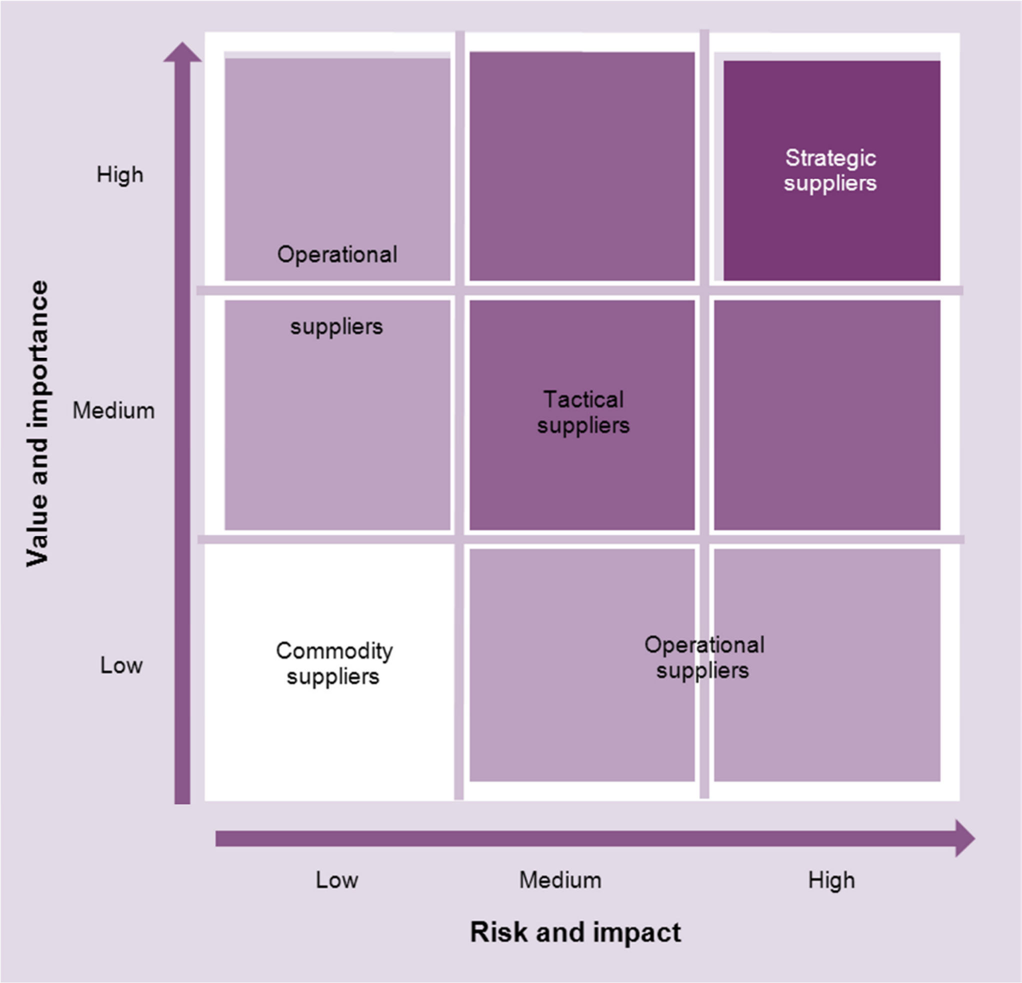
Managers should spend more time and effort managing key suppliers than less important suppliers. Suppliers can be categorized based on:

- Assessing the risk and impact associated with using the supplier
- The value and importance of the supplier and its services to the business.

The time and effort spent can then be appropriate to the supplier's categorization:

- **Strategic:** For significant 'partnering' relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans

- **Tactical:** For relationships involving significant commercial activity and business interaction
- **Operational:** For suppliers of operational products or services
- **Commodity:** For suppliers providing low value and/or readily available products or services.



© Crown copyright 2013 Reproduced under licence from OGC

Figure: Supplier categorization

Process 7: Capacity management

Purpose and objectives

The purpose of capacity management is to ensure that the capacity of IT services and the IT infrastructure meets the agreed capacity and performance-related requirements in a cost-effective and timely manner.

The objectives of capacity management are:

- Produce and maintain an accurate capacity plan, and provide advice and guidance on all capacity and performance related issues
- Ensure service performance achievements meet their agreed targets, and assist with diagnosis and resolution of incidents and problems

- Assess the impact of all changes on the capacity plan and proactively improve performance, where cost-effective.

Scope

Capacity management is a process that extends across the whole service lifecycle. A key factor in managing capacity is ensuring it is considered in service design. The capacity management process provides a focal point for the management of all IT performance and capacity issues.

Capacity management seeks to understand current and future business and IT needs relating to capacity and performance, and also to understand and take account of current capability and future opportunities presented by advances in technology.

Capacity management ensures that IT resources are planned and scheduled to deliver a consistent level of service, matched to the agreed current and future needs of the business.

Principles and basic concepts

Capacity management is essentially a balancing act:

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

Capacity management is a complex and demanding process. To deliver results it relies on three sub-processes:

- **Business capacity management:** Translating business needs and plans into requirements for IT services and infrastructure
- **Service capacity management:** Predicting, managing and controlling the end-to-end performance of the operational IT services and their workloads
- **Component capacity management:** Predicting, managing and controlling the performance, utilization and capacity of individual IT components.

A capacity plan is used to manage the resources required to deliver IT services. The plan contains details of current and historic usage of IT services and components plans for the development of IT capacity to meet the needs in the growth of both existing services; any agreed new services and any issues that need to be addressed (including related improvement activities).

Process 8: IT service continuity management

Purpose and objectives

The purpose of IT service continuity management (ITSCM) is to support the overall business continuity management (BCM) process by ensuring that the IT service provider can always provide minimum agreed business continuity related service levels.

The objectives of ITSCM are to:

- Maintain a set of IT service continuity plans and IT recovery plans that support the overall business continuity plans (BCPs) and, in support of this, to carry out regular BIA, risk analysis and management activities
- Provide advice and guidance on continuity and recovery related issues

- Ensure that appropriate continuity mechanisms are in place to meet or exceed the agreed business continuity targets
- Assess the impact of all changes on the IT service continuity plans
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable
- Negotiate and agree contracts with suppliers for the provision of the necessary recovery capability.

Scope

ITSCM serves to underpin the activities of the BCM process and focuses on those events that the business considers to be a 'disaster'. It does not cover minor technical faults which are addressed through the incident management process. These 'minor' issues are also covered by the availability management process in the design of services for availability and recovery.

Additionally, ITSCM does not usually directly address longer term risks such as those from changes in business direction, diversification and restructuring, when there is generally time to evaluate the risks and address them through an IT change management programme.

Principles and basic concepts

Business continuity plan (BCP)

A business continuity plan defines the steps required to restore business processes following a disruption. It also identifies triggers for invocation, people to be involved, communications etc. IT service continuity plans form a significant part of BCPs.

Business impact analysis (BIA)

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

- The form that the damage or loss may take
- How the degree of loss or damage is likely to escalate after a service disruption
- The staffing, skills, facilities and services (including the
- IT 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 relative business recovery priority for each of the IT services.

Risk assessment

This is an assessment of the level of threat and the extent to which the organization is vulnerable to that threat.

Chapter 4: Service Transition

ITIL Service Transition moves services and service changes into operational use. Service transition achieves this by receiving a new or changed service design package (SDP) from the service design stage, testing it to ensure it meets the needs of the business, and deploying it within the production environment.

ITIL Service Transition also introduces the service knowledge management system (SKMS), which can support organizational learning and help to improve the efficiency and effectiveness of all stages of the service lifecycle. This enables people to benefit from the knowledge and experience of others, support informed decision-making, and improve the management of services.

PURPOSE, OBJECTIVES, SCOPE AND VALUE OF SERVICE TRANSITION

Purpose and objectives

The purpose of the service transition stage of the service lifecycle is to ensure that new, modified or retired services meet the expectations of the business as documented in the service strategy and service design stages of the lifecycle.

The objectives of service transition are to:

- Plan and manage service changes efficiently and effectively
- Manage risks relating to new, changed or retired services
- Successfully deploy service releases into supported environments
- Set expectations on the performance and use of new or changed services
- Ensure that service changes create the expected business value
- Provide knowledge and information about services and service assets.

Scope

The scope of ITIL Service Transition includes the development and improvement of capabilities for transitioning new and changed services into supported environments, including release planning, building, testing, evaluation and deployment. It also includes service retirement and transfer of services between service providers.

Value to business

Effective service transition provides the following benefits:

- Better estimation of cost, timing, resource requirement and risks
- Higher volumes of successful change
- Reduce delays from unexpected clashes and dependencies
- Reduced effort spent on managing test and pilot environments
- Improved expectation setting for all stakeholders

- Increased confidence that new or changed services can be delivered to specification without unexpectedly affecting other services or stakeholders
- Ensure that new or changed services will be maintainable and cost-effective
- Improved control of service assets and configurations.

PROCESSES AND ACTIVITIES

Process 1: Transition planning and support

Purpose and objectives

The purpose of the transition planning and support process is to provide overall planning for service transitions and to coordinate the resources that they require.

The objectives of transition planning and support are to:

- Plan and coordinate service transition resources within IT and across projects, suppliers and service teams where required
- Establish new or changed services within predicted cost, quality and time
- Establish new or modified management information systems and tools, technology and management architectures, service management processes, and measurement methods and metrics to meet agreed requirements
- Provide plans that enable business change projects to align with service transition
- Identify, manage and control risks
- Monitor and improve the performance of the service transition lifecycle stage.

Scope

The scope of transition planning and support includes:

- Maintaining policies, standards and models for service transition
- Guiding major changes through service transition processes
- Prioritizing and coordinating resources needed to manage multiple transitions at the same time
- Planning service transition budget and resources
- Reviewing and improving the performance of transition planning and support.
- Transition planning and support is not responsible for detailed planning for changes or releases.

Process 2: Change management

Purpose and objectives

The purpose of change management is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

The objectives of change management are to:

- Respond to changing business requirements while maximizing value and reducing incidents, disruption and re-work
- Respond to RFCs that will align services with business needs
- Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner
- Optimize overall business risk.

Scope

The scope of change management covers changes to all configuration items (CIs) across the whole service lifecycle, whether these CIs are physical assets such as servers or networks, virtual assets such as virtual servers or virtual storage, or other types of asset such as agreements or contracts. It also covers all changes to any of the five aspects of service design:

- Service solutions
- Management information systems and tools
- Technology architectures and management architectures
- Processes
- Measurement systems, methods and metrics.

Principles and basic concept

Types of change request

Changes are categorized as standard, emergency or normal changes:

- **Standard change:** A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction - for example a password reset or provision of standard equipment to a new employee. RFCs are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request.
- **Emergency change:** A change that must be introduced as soon as possible, for example to resolve a major incident or implement a security patch. The change management process normally has a specific procedure for handling emergency changes.
- **Normal change:** Any change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process.

Changes are often categorized as major, significant and minor, depending on the level of cost and risk involved, and on the scope and relationship to other changes. This categorization may be used to identify an appropriate change authority.

Changes & RFCs

The terms 'change', 'RFC' and 'change record' are often used inconsistently, leading to confusion. The usage in ITIL Service Transition is as follows:

- **Change:** The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other CIs.

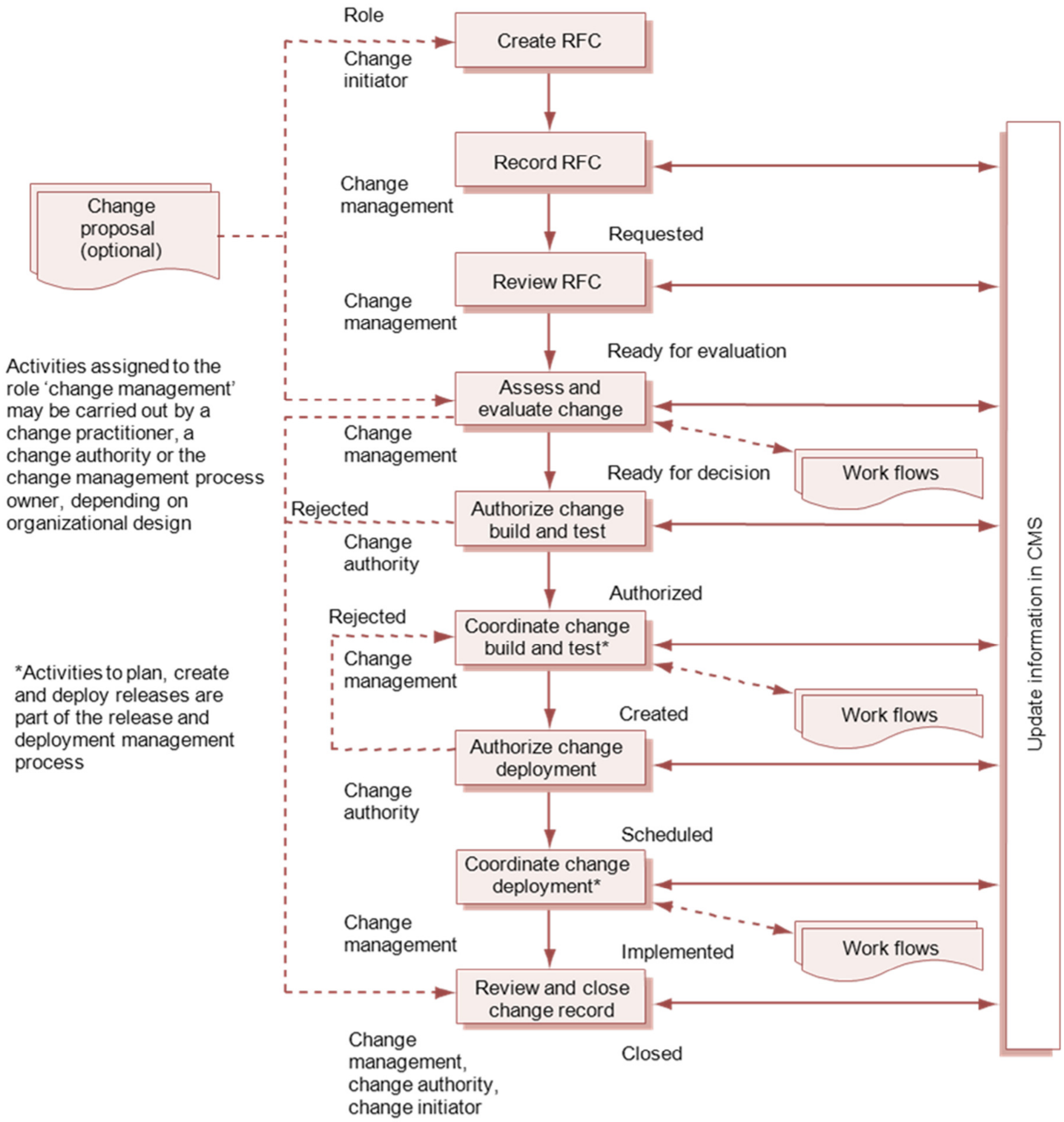
- **RFC:** A request for change - a formal proposal for a change to be made. It includes details of the proposed change, and may be recorded on paper or electronically.

Change models

A change model is a repeatable way of dealing with a particular category of change. It defines specific agreed steps that are followed for a change of this category. These models are often input to change management support tools that automate handling, management, reporting and escalation.

Each change model includes:

- Steps that should be taken to handle the change, including escalation procedures for issues and unexpected events
- Responsibilities for each step, including identification of change authorities
- Timescales and thresholds for completion of actions.


Role
Create RFC
Change initiator
Record RFC
Change management
Change proposal (optional)
Requested
Review RFC
Change management
Ready for evaluation
Activities assigned to the role 'change management' may be carried out by a change practitioner, a change authority or the change management process owner, depending on organizational design
Assess and evaluate change
Change management
Work flows
Ready for decision
Rejected
Authorize change build and test
Change authority
Authorized
Rejected
Coordinate change build and test*
Change management
Work flows
*Activities to plan, create and deploy releases are part of the release and deployment management process
Created
Authorize change deployment
Change authority
Scheduled
Coordinate change deployment*
Change management
Work flows
Implemented
Review and close change record
Change management, change authority, change initiator
Closed
Update information in CMS

© Crown copyright 2013 Reproduced under license from OGC

Figure: Lifecycle of a normal change

Change advisory board (CAB)

A CAB is a group of people that supports the authorization of changes and assists change management in the assessment, prioritization and scheduling of changes.

CABs should:

- Be composed according to the changes being considered and vary in make-up even across the range of a single meeting
- Involve suppliers when useful
- Reflect both users' and customers' views
- Include the problem manager, service level manager and customer relations staff for at least part of the time.

Emergency change advisory board (ECAB)

For emergency change there may not be time to convene the full CAB, so it is necessary to identify a smaller board with authority to make emergency decisions - this is called an emergency change advisory board (ECAB).

Change proposals

Major changes that involve significant cost, risk or organizational impact are usually initiated through the service portfolio management process, and a change proposal is used to communicate a high-level description of the change.

Trainer Note: *After the new or changed service is chartered, RFCs are used in the normal way to request authorization for specific changes. These RFCs are associated with the change proposal so that change management has a view of the overall strategic intent and can prioritize and review these RFCs appropriately.*

Remediation planning

No change should be authorized without a plan for what to do if it is not successful. Ideally, there is a back-out plan, but if the change is not reversible then an alternative approach is required. In some cases this may even require invoking the organization's business continuity plan.

Every change implementation plan should include milestones and other triggers for remediation to ensure there is sufficient time for this to occur.

Process activities, methods and techniques

The key activities of change management are:

- Planning, controlling and scheduling changes
- Understanding the impact of change
- Change decision making and change authorization
- Change and release scheduling (working with release and deployment management)
- Communication with stakeholders
- Ensuring that there are remediation plans

- Measurement, control and management reporting
- Continual improvement.

Process 3: Service asset and configuration management

Purpose and objectives

The purpose of the service asset and configuration management (SACM) process is to ensure that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed.

The objectives of SACM are to:

- Ensure that assets are identified, controlled, managed and protected throughout their lifecycle
- Identify, control, record, report, audit and verify services and other CIs, including their attributes and relationships
- Ensure the integrity of CIs and configurations by maintaining accurate configuration information on their historical, planned and current state in a CMS
- Support efficient and effective service management by providing accurate configuration information.

Scope

Service assets that need to be managed in order to deliver services are known as configuration items (CIs).

The scope of SACM includes management of the complete lifecycle of every CI. The scope also includes interfaces to internal and external service providers where there are assets and CIs that need to be controlled, e.g. shared assets.

Fixed asset management is not usually under the control of the same business unit as the IT services, but the SACM process must provide proper care for the fixed assets under the control of IT.

Principles and basic concepts

Configuration items (CIs)

It is important to distinguish between service assets, CIs and configuration records, as these concepts are often confused:

- A service asset is any resource or capability that could contribute to the delivery of a service. Examples of service assets include a virtual server, a physical server, a software licence, or knowledge in the head of a manager.
- A configuration item (Cl) is any service asset that needs to be managed in order to deliver a service. All CIs are service assets, but many service assets are not CIs. Examples of CIs are a server or a software licence.
- A configuration record is a set of attributes and relationships about a Cl. Configuration records are stored in a configuration management database (CMDB) and managed with a CMS.
- The service knowledge management system (SKMS) is a set of tools and databases that are used to manage knowledge, information and data. Many CIs are stored in the SKMS – for example, a service level agreement (SLA), a report template or a definitive media library (DML).

Configuration Management System (CMS)

A set of tools, data and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analysing and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes and releases. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.

Definitive Media Library (DML)

One or more locations in which the definitive and authorized versions of all software configuration items are securely stored. The definitive media library may also contain associated configuration items such as licences and documentation. It is a single logical storage area even if there are multiple locations. The definitive media library is controlled by service asset and configuration management and is recorded in the configuration management system.

Process 4: Release and deployment management

Purpose and objectives

The purpose of the release and deployment management process is to plan, schedule and control the build, test and deployment of releases, and to deliver new functionality required by the business while protecting the integrity of existing services.

The objectives of release and deployment management are to:

- Define and agree release and deployment management plans

- Create and test release packages, stored in a definitive media library (DML) and recorded in the CMS
- Deploy release packages from the DML following the agreed plan
- Ensure that organization and stakeholder change are managed
- Ensure that the new or changed service can deliver the agreed utility and warranty
- Ensure that there is knowledge transfer to customers, users and IT.

Scope

The scope of release and deployment management includes the processes, systems and functions to package, build, test and deploy a release into live use, establish the service specified in the SDP, and formally hand the service over to the service operation functions.

The scope of release and deployment management does not include carrying out testing, or authorizing changes, but the process must ensure that these activities have been carried out.

Principles and basic concepts

Release

One or more changes to an IT service that are built, tested and deployed together. A single release may include changes to hardware, software, documentation, processes and other components.

Release policy

Release and deployment management policies should be in place to help the organization achieve the correct balance between cost, service stability and agility.

Process activities, methods and techniques

The four phases of release and deployment management are:

- **Release and deployment planning:** Plans for creating and deploying the release are created. This phase starts with change management authorization to plan a release and ends with change management authorization to create the release.
- **Release build and test:** The release package is built, tested and checked into the DML. This phase starts with change management authorization to build the release and ends with change management authorization for the baselined release package to be checked into the DML. This phase only happens once for each release.
- **Deployment:** The release package in the DML is deployed to the live environment. This phase starts with change management authorization to deploy the release package to one or more target environments and ends with handover to the service operation functions and early life support. There may be many separate deployment phases for each release.
- **Review and close:** Experience and feedback are captured, performance targets and achievements are reviewed and lessons are learned.

Early-life support

Once a new or changed service has been deployed into the production environment, service transition may provide early life support for a limited period of time. During early-life support the service levels and monitoring thresholds are reviewed and additional resources may be provided for incident and problem management.

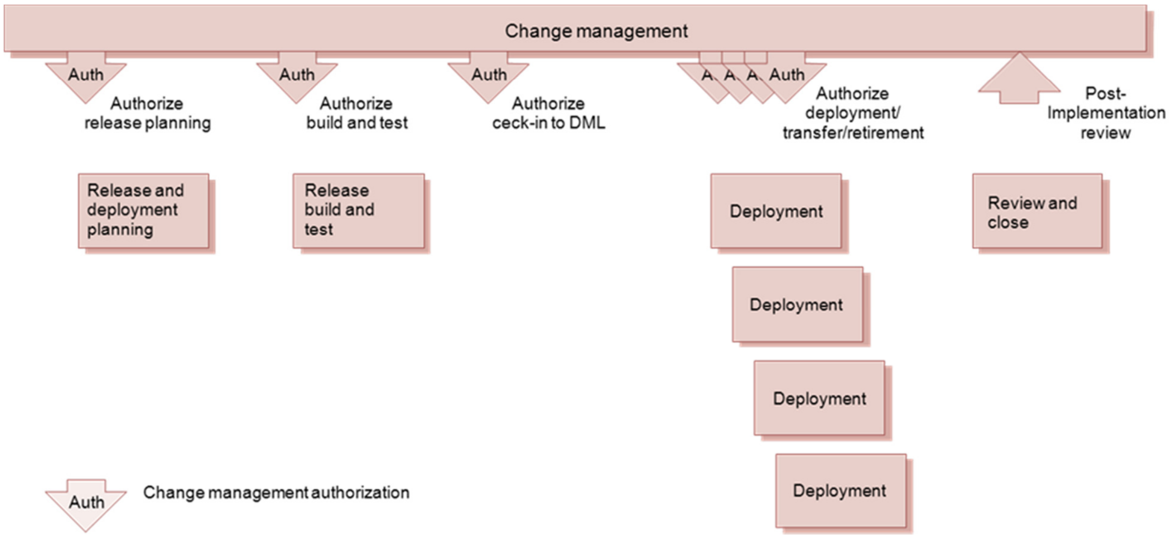


Figure: Three-view service catalogue

Process 5: Knowledge management

Purpose and objectives

The purpose of the knowledge management process is to share perspectives, ideas, experience and information; to ensure that these are available in the right place at the right time to enable informed decisions; and to improve efficiency by reducing the need to rediscover knowledge.

The objectives of knowledge management are to:

- Improve management decision-making by ensuring that reliable and secure knowledge, information and data are available
- Enable the service provider to be more efficient and improve quality of service, increase satisfaction and reduce the cost of service
- Maintain an SKMS that provides controlled access to appropriate knowledge, information and data
- Gather, analyse, store, share, use and maintain knowledge, information and data throughout the service provider organization.

Scope

Knowledge management is a whole lifecycle-wide process in that it is relevant to all lifecycle stages and hence is referenced throughout ITIL from the perspective of each publication.

Principles and basic concepts

Data-to-Information-to-Knowledge-to-Wisdom (DIKW)

Knowledge management uses the DIKW hierarchy to help create value.

Data is a set of discrete facts. An example of data is the date and time at which an incident was logged.

Information comes from providing context to data. An example of information is the average time to close priority 2 incidents.

Knowledge is composed of the tacit experiences, ideas, insights, values and judgements of individuals. An example of knowledge is that the average time to close priority 2 incidents has increased by about 10% since a new version of the service was released.

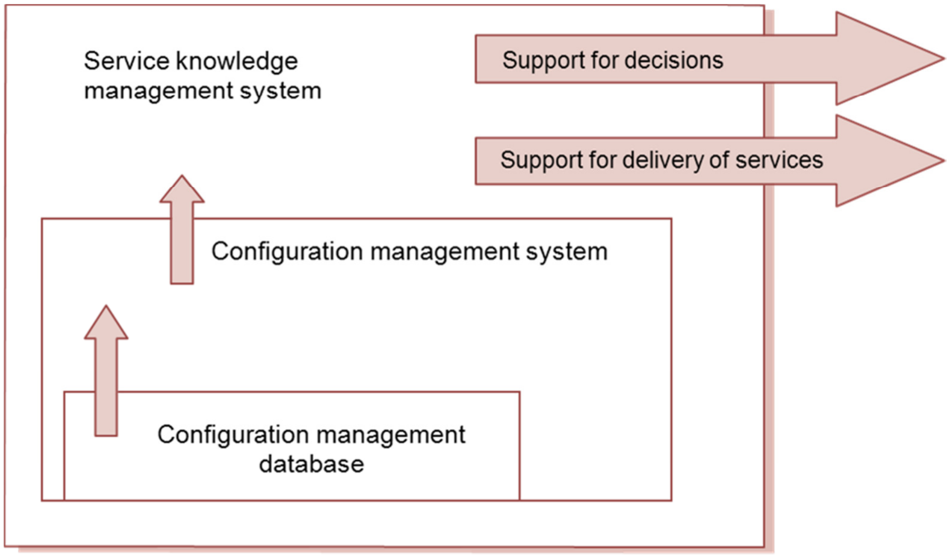
Wisdom makes use of knowledge to create value through correct and well-informed decisions. An example of wisdom is recognizing that the increase in time to close priority 2 incidents is due to poor-quality documentation for the new version of the service.

Service knowledge management system (SKMS)

A set of tools and databases that is used to manage knowledge, information and data. The service knowledge management system includes the configuration management system, as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analysing and presenting all the knowledge, information and data that an IT service provider will need to manage the full lifecycle of IT services.

The SKMS supports delivery of the services and informed decision-making, and is underpinned by the CMS, but it should also contain many other things, for example:

- The service portfolio
- The DML
- SLAs, contracts and OLAs
- The CSI register and service improvement plans (SIPs)
- The capacity plan and capacity management information system
- Project plans from previous projects
- Skills register, and typical and anticipated user skill levels
- Web-based training courses.


Service knowledge management system
Support for decisions
Support for delivery of services
Configuration management system
Configuration management database

© Crown copyright 2013 Reproduced under license from OGC

Figure: Relationship of the SKMS, the CMS and the CMDB

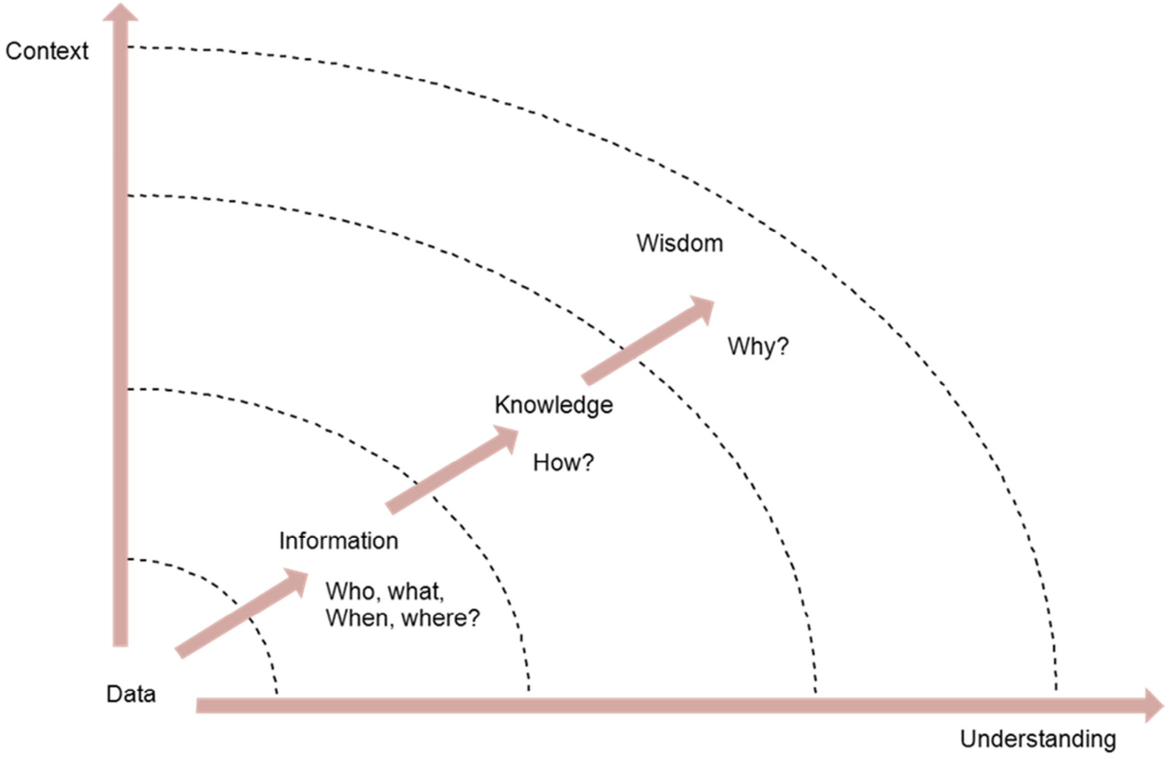


Figure: Data-Information-to-knowledge-to-Wisdom

Chapter 5: Service Operation

PURPOSE, OBJECTIVES, SCOPE AND VALUE OF SERVICE OPERATION

Purpose and objectives

The purpose of the service operation stage of the service lifecycle is to coordinate and carry out the activities and processes required to deliver and manage services at agreed levels to business users and customers. Service operation is also responsible for the ongoing management of the technology that is used to deliver and support services.

Service operation is a critical stage of the service lifecycle. Well planned and well implemented processes are to no avail if the day-to-day operation of those processes is not properly conducted, controlled and managed.

The objectives of service operation are to:

- Maintain business satisfaction and confidence in IT through effective and efficient delivery and support of agreed IT services
- Minimize the impact of service outages on day-to-day business activities
- Ensure that access to agreed IT services is only provided to those authorized to receive those services.

Scope

Service operation describes the processes, functions, organization and tools used to underpin the ongoing activities required to deliver and support services and includes:

- **Services:** Activities that form part of a service are included in service operation, whether it is performed by the service provider, an external supplier or the user or customer of that service.
- **Service management processes:** The ongoing management and execution of the many service management processes that are performed in service operation. Even though a number of ITIL processes (such as change and capacity management) originate at the service design or service transition stage of the service lifecycle, they are in use continually in service operation.
- **Technology:** All services require some form of technology to deliver them. Managing technology is an integral part of the management of the services.
- **People:** People drive the demand for the organization's services and products; decide how this will be done; manage the technology, processes and services. Failure to recognize this will result (and has resulted) in the failure of service management activities.

Value to business

Service operation is the stage in the lifecycle where the plans, designs and optimizations are executed and measured. Service operation is where actual value is seen by the business.

Adopting and implementing standard and consistent approaches for service operation:

- Reduces the duration and frequency of service outages, which will allow the business to take full advantage of the value created by the services they are receiving and reduce unplanned costs and resource usage
- Provides operational results and data to provide justification for investing in ongoing service improvement activities and supporting technologies
- Meets the goals and objectives of the organization's security policy by ensuring that IT services will be accessed only by those authorized to use them
- Provides quick and effective access to standard services which business staff can use to improve their productivity or the quality of business services and products
- Provides a basis for automated operations, thus increasing efficiencies and allowing expensive human resources to be used for more innovative work, such as designing new or improved functionality or defining new ways in which the business can exploit technology for increased competitive advantage.

KEY PRINCIPLES

Communication in service operation

Effective communication in service operation ensures that all teams and departments are able to execute the standard activities involved in delivering IT services and managing the IT infrastructure, including:

- **Routine operational communication:** To coordinate the regular activities of service operation and ensure staff are aware of scheduled activities and any changes
- **Communication between shifts:** To ensure that any handover between shifts is effective
- **Performance reporting:** IT service performance and service operation team or department performance
- **Communication in projects:** To manage communication between projects and the involvement of service operation staff
- **Communication related to changes:** Information required to assess the impact of and successfully implement or back-out changes
- **Communication related to exceptions:** Information around any occurrence that is outside expected activity or performance
- **Communication related to emergencies:** To allow effective investigation and management of emergency situations
- **Communication with users and customers:** A focus on customer or user requirements and concerns.

PROCESSES AND ACTIVITIES

Process 1: Incident management

Purpose and objectives

The purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. 'Normal service operation' is defined as an operational state where services and configuration items (CIs) are performing within their agreed service and operational levels.

The objectives of the incident management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align incident management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services.

Scope

Incident management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by users, either through the service desk, through an interface from event management to incident management tools or incidents reported and/or logged by technical staff.

Although both incidents and service requests are reported to the service desk, this does not mean that they are the same. Service requests do not represent a disruption to agreed service, but are a way of meeting the customer's needs and may be addressing an agreed target in a service level agreement (SLA). Service requests are dealt with by the request fulfillment process.

Principles and basic concepts

Incident

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident - for example, failure of one disk from a mirror set.

Impact

Impact is a measure of the effect of an incident, problem or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.

Urgency

A measure of how long it will be until an incident, problem or change has a significant impact on the business. For example, a high-impact incident may have low urgency if the impact will not affect the business until the end of the financial year. Impact and urgency are used to assign priority.

Priority

A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken.

Trainer Note: *For example, the service level agreement may state that Priority 2 incidents must be resolved within 12 hours.*

Timescales

Timescales must be agreed for all incident handling activities, based upon the overall incident response and resolution targets agreed within SLAs, operational level agreements (OLAs) and underpinning contracts (UCs). All support groups should be made fully aware of these timescales.

Incident models

An incident model is a way of predefining the steps that should be taken to handle a particular type of incident in an agreed way.

Major incidents

A major incident is often confused with a problem. In reality, an incident remains an incident for ever - it may grow in impact or priority to become a major incident, but an incident never 'becomes' a problem.

A definition of what constitutes a major incident must be agreed so that they are dealt with through a separate major incident procedure. Where necessary this procedure should include the establishment of a separate major incident team under the leadership of the incident manager, to concentrate on this major incident alone to ensure that adequate resources and focus are used to find a speedy resolution.

Incident status and tracking

Incidents should be tracked throughout their lifecycle to support proper handling and reporting on the status of incidents. Within the incident management system, status codes may be linked to incidents to indicate where they are in relation to the lifecycle.

Trainer Note: *Examples include: open, in-progress, resolved and closed.*

Expanded incident lifecycle

The expanded incident lifecycle can be used to help understand all stages and activities involved in the incident lifecycle and their impact on the resolution of incidents and their subsequent improvement.

Process activities, methods and techniques

The key activities for incident management are:

- **Incident identification:** Incidents may be detected by event management, by calls to the service desk, from web or other self-help interfaces, or directly by technical staff.
- **Incident logging:** All incidents must be logged and timestamped, regardless of how they are received. The log must include sufficient data to enable the incident to be managed.

- **Incident categorization:** Categories are used to identify the type of incident and to identify service requests so they can be passed to the request fulfilment process. Categories are also checked when the incident is closed
- **Incident prioritization** A priority code is assigned based on impact and urgency. Priorities are dynamic and may be changed during the life of the incident
- **Initial diagnosis:** If possible, the incident should be resolved while the user is on the telephone. Sometimes the service desk analyst will continue to work on the incident and contact the user when it has been resolved
- **Incident escalation:** 'Functional escalation' is transferring the incident to a technical team with a higher level of expertise; 'hierarchic escalation' is informing or involving more senior levels of management.
- **Investigation and diagnosis:** All actions taken by support groups should be recorded in the incident record.
- **Resolution and recovery:** The resolution must be fully tested and documented in the incident record, before the incident is passed back to the service desk for closure.
- **Incident closure:** Check and confirm the incident categories, carry out a user satisfaction survey, ensure all incident documentation is up to date, check to see if a problem record should be raised and then close the incident with the appropriate closure categorization.
- **Rules for reopening incidents:** Despite all adequate care, there will be occasions when incidents recur even though they have been formally closed. Because of such cases, it is wise to have predefined rules about if and when an incident can be reopened.

Interfaces

- **Service level management (SLM):** Requires a process capable of resolving incidents in a specified time which can also provide information and reports that enable SLM to review services and identify service weaknesses and improvements.
- **Information security management (ISM)**: Requires information on security incidents to measure the effectiveness of security measures and support service design activities.
- **Capacity management:** Requires performance monitoring and information on performance issues and problems.
- **Availability management:** Requires information on the availability of IT services and the improvement of the incident lifecycle.
- **Service asset and configuration management (SACM)**: Provides data to identify and progress incidents, identify faulty equipment and to assess the impact of an incident.
- **Change management:** The implementation of a workaround or resolution is logged as an RFC and progressed through change management. Incident management needs to detect and resolve incidents arising from failed changes.
- **Problem management:** Provides known errors and workarounds for faster incident resolution and also the investigation and resolution of the underlying cause of incidents preventing or reducing the impact of recurrence.
- **Access management:** Requires information on unauthorized access attempts and security breaches.

Process 2: Problem management

Purpose and objectives

The purpose of problem management is to manage problems through their lifecycle from first identification through investigation, documentation and eventual resolution and closure.

Problem management seeks to minimize the adverse impact of incidents and problems on the business caused by underlying errors within the IT Infrastructure, and to proactively prevent recurrence of incidents related to these errors.

The objectives of the problem management process are to:

- Prevent problems and resulting incidents from happening
- Eliminate recurring incidents
- Minimize the impact of incidents that cannot be prevented.

Scope

Problem management includes the activities required to diagnose the root cause of incidents and to determine the cause and resolution of the underlying problems. It is also responsible for ensuring resolutions are implemented through the appropriate procedures, especially change management and release and deployment management.

Problem management maintains information about problems, workarounds and resolutions, enabling reductions in the number and impact of incidents over time, requiring a strong interface with knowledge management, and tools such as the known error database (KEDB).

Principles and basic concepts

Problem

A problem is the cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.

Known Error

A known error is a problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers.

Workaround

A workaround is a way of reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available. ***Trainer Note:*** *for example, by restarting a failed configuration item.* Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

Known Error Database (KEDB)

A database containing all known error records. This database is created by problem management and used by incident and problem management. The known error database may be part of the configuration management system, or may be stored elsewhere in the service knowledge management system.

Reactive and proactive problem management activities

Both reactive and proactive problem management activities raise problems, manage them through the problem management process, find the underlying causes of the incidents and prevent future recurrences of those incidents. The difference is how the problem management process is triggered:

- **Reactive problem management** Triggered in reaction to an incident that has taken place, complementing incident management activities by focusing on the underlying cause of an incident to prevent its recurrence and identifying workarounds when necessary
- **Proactive problem management** Triggered by activities seeking to improve services, such as trend analysis activities, complementing CSI activities by helping to identify workarounds and improvement actions that can improve the quality of a service.

Problem models

Many problems will be unique and require handling in an individual way. However some incidents may recur because of dormant or underlying problems (for example, where the cost of a permanent resolution will be high and a decision has been taken not to go ahead with an expensive solution but to 'live with' the problem).

As well as creating a known error record in the KEDB to ensure quicker diagnosis, a problem model can be created for handling such problems in the future.

Incidents versus problems

An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. A problem presents a different view of an incident by understanding its underlying cause. Incidents do not 'become' problems. While incident management activities are focused on restoring services to normal state operations, problem management activities are focused on finding ways to prevent incidents from happening. It is quite common to have incidents that are also problems.

Situations where it may be desired to invoke problem management during an incident include:

- Incident management cannot match an incident to existing problems and known errors
- Trend analysis of logged incidents reveals an underlying problem might exist
- A major incident has occurred where problem management needs to identify the root cause
- An incident is resolved but no definitive cause has been identified and it is likely to recur
- Analysis of an incident reveals that an underlying problem exists, or is likely to exist.

Process activities, methods and techniques

The key activities for problem management are:

- **Problem detection** By the service desk, technical support, event management, notification by a supplier, or from incident trend analysis.
- **Problem logging** All details must be recorded, including links to related incidents.
- **Problem categorization** Usually uses the same categorization codes as incidents.
- **Problem prioritization** Differs from incident prioritization in that this is based on frequency and impact of linked incidents, plus severity of the incident (impact on the infrastructure, cost to fix, time to fix).

- **Problem investigation and diagnosis** Determine root cause using techniques such as chronological analysis, pain value analysis, Kepner-Tregoe, brainstorming, Ishikawa diagram and Pareto analysis.
- **Workarounds** A workaround to the related incidents can reduce the impact of the problem until full resolution is achieved.
- **Raising a known error record** For use by the service desk to identify the symptoms and restore service quickly, using the workaround if one exists. Create when diagnosis is complete, but can raise earlier if useful.
- **Problem resolution** Usually requires a change request. If the resolution is not cost-effective, then the problem may be left open and the workaround should continue to be used.
- **Problem closure:** After the change has been successfully reviewed - review related incident records, update known error records, check problem data and formally close.
- **Major problem review:** A review of every major problem should be conducted to learn lessons for the future. Major problem is defined by the priority system.

Interfaces

Problem management provides a wealth of information and reports on the volumes and types of information to all other areas and processes, including:

- **Financial management for IT services:** Assists in assessing the impact of proposed resolutions or workarounds, as well as pain value analysis, with problem management providing management information about the cost of resolving and preventing problems, which is used as input into the budgeting and accounting systems and total cost of ownership calculations.
- **Availability management:** Uses proactive problem management to determine howto reduce downtime.
- **Capacity management:** Assists with the investigation of some problems (e.g. performance issues), and with assessing proactive measures. Problem management provides management information relative to the quality of decision making during the capacity planning process.
- **ITSCM:** Problem management acts as an entry point into ITSCM where a significant problem is not resolved before it starts to have a major impact on the business.
- **SLM:** Problem management contributes to improvements in service levels by analysing incidents and problems affecting the level of service, and its management information is used as the basis of SLA reviews. SLM also provides parameters within which problem management works, such as impact information and the effect on services of proposed resolutions and proactive measures.
- **Change management:** Involves problem management in rectifying the situation caused by failed changes and problem management also ensures that all resolutions or workarounds that require a change to a Cl are submitted through change management.
- **SACM:** Provides the CMS which assists problem management to identify faulty CIs and also to determine the impact of problems and resolutions.
- **Release and deployment management:** Is responsible for deploying problem fixes out into the live environment. It also assists in ensuring that the associated known errors are

transferred from development into the live KEDB. Problem management also helps to resolve problems caused by faults during the release process.

- **Knowledge management:** Provides the SKMS, which can be used to form the basis for the KEDB and record or integrate with the problem records.
- **Seven-step improvement process:** Incidents and problems provide a basis for identifying opportunities for service improvement and adding them to the CSI register. Proactive problem management activities may also identify underlying problems and service issues that if addressed, can contribute to increases in service quality and end user/customer satisfaction.

Process 3: Event management

Purpose and objectives

The purpose of event management is to manage events throughout their lifecycle. This lifecycle of activities to detect events, make sense of them and determine the appropriate control action is coordinated by the event management process.

The objectives of the event management process are to:

- Detect all changes of state that have significance for the management of a Cl or IT service
- Determine the appropriate action for events and ensure communication to the appropriate functions
- Provide the trigger for the execution of many processes and operations management activities
- Provide comparison of actual operating performance against design standards and SLAs
- Provide a basis for service assurance and reporting and service improvement.

Scope

Event management can be applied to any aspect of service management that needs to be controlled and which can be automated. This includes:

- Monitoring and control of the status of CIs
- Environmental conditions
- Software license monitoring to ensure optimum/legal license utilization and allocation
- Security
- Normal activity.

Principles and basic concepts

Event

A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool.

Types of events include:

- Informational For example, notification that a scheduled task has completed or a user has logged in
- Warning Typically generated when a threshold has been reached, enabling someone to react before things go wrong

- Exception A service or device is operating abnormally and action is required.

Alert

An alert is a notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.

Process 4: Request fulfillment

Purpose and objectives

Request fulfilment is the process responsible for managing all service requests from the users through their lifecycle.

The objectives of the request fulfilment process are to:

- Maintain user and customer satisfaction through efficient and professional handling of service requests
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services
- Assist with general information, complaints or comments.

Scope

Some organizations handle service requests through their incident management process (and tools), with service requests being handled as a particular type of 'incident'. However there is a significant difference between an incident, usually an unplanned event, and a service request, which is something that should be planned. The process needed to fulfil a request varies depending upon exactly what is being requested, but can usually be broken down into a set of activities that have to be performed.

Therefore, in an organization where large numbers of service requests have to be handled, and where the actions to be taken to fulfil those requests are very varied or specialized, it may be appropriate to handle service requests as a completely separate work stream. Ultimately it is up to each organization to decide and document which service requests it handles through the request fulfilment process and which have to go through other processes.

Principles and basic concepts

Service Request

A service request is a formal request from a user for something to be provided - ***Trainer Note:*** *for example, a request for information or advice; to reset a password; or to install a workstation for a new user.* Service requests are managed by the request fulfillment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request.

Process 5: Access management

Purpose and objectives

The purpose of access management is to provide the right for users to be able to use a service or group of services. It is therefore the execution of policies and actions defined in ISM.

The objectives of the access management process are to:

- Manage access to services based on policies and actions defined by ISM
- Efficiently respond to requests for granting access to services, changing access rights or restricting access, ensuring that the rights being provided or changed are properly granted
- Oversee access to services and ensure rights being provided are not improperly used.

Scope

Access management is effectively the execution of the policies in ISM, in that it enables the organization to manage the confidentiality, availability and integrity of the organization's data and intellectual property.

ORGANIZING FOR SERVICE OPERATION

Function 1: Service desk function

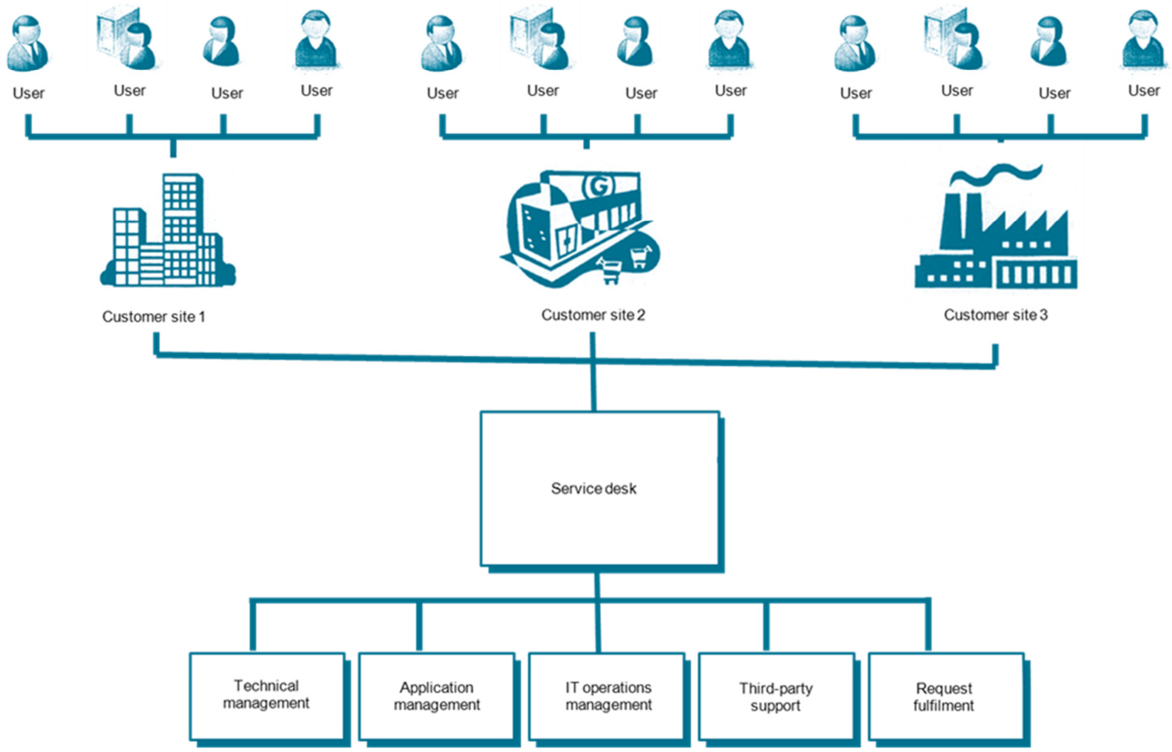
The service desk is a vitally important part of an organization's IT department and is the single point of contact for IT users on a day-by-day basis. The service desk is key to the implementation of the request fulfilment and incident management processes.

A good service desk is often able to compensate for deficiencies elsewhere in the IT organization, but an ineffective service desk can give a poor impression of an otherwise very good IT organization.

Justification and role of the service desk

The benefits of a good service desk include:

- Improved customer service, perception and satisfaction
- Single point of contact, communication and information
- Better quality and faster turnaround of customer or user requests
- Improved usage of IT support resources and increased productivity of users
- More meaningful management information for decision support.



© Crown copyright 2013 Reproduced under license from OGC

Figure: Three-view service catalogue

Service desk objectives

The service desk provides a single central point of contact for all users of IT. The service desk usually logs and manages all incidents, service requests and access requests and provides an interface for all other service operation processes and activities.

The primary aim of the service desk is to restore normal service as quickly as possible.

Trainer Note: *This may involve fixing a technical fault, fulfilling a service request, or answering a query - anything that is needed to allow the users to return to normal working.*

The specific responsibilities include:

- Logging all incidents and requests, categorizing and prioritizing them
- First-line investigation and diagnosis
- Managing the lifecycle of incidents and requests, escalating as appropriate and closing them when the user is satisfied
- Communicating with users, keeping them informed of incident progress
- Conducting customer/user satisfaction callbacks/surveys
- Updating the CMS under the direction and approval of configuration management if so agreed.

Service desk organizational structure

There are many ways of structuring and locating service desks - the correct solution varies for different organizations. The primary options are detailed below and a combination of these may be needed in order to fully meet the business needs:

- **Local service desk:** Co-located within or physically close to the user community it serves. This often aids communication, gives a clearly visible presence, and can support local language and cultural differences, but can often be inefficient and expensive to resource as the volume and arrival rate of calls may not justify the minimum staffing levels required.
- **Centralized service desk:** The number of service desks can be reduced by merging them into a single location or a smaller number of locations. This can be more efficient and cost effective, allowing fewer staff to deal with a higher volume of calls. It might still be necessary to maintain some 'local presence', but such staff can be controlled and deployed from the central desk.
- **Virtual service desk:** Through the use of technology, particularly the Internet, and corporate support tools, it is possible to give the impression of a single, centralized service desk when in fact the personnel may be in any number or types of locations. This gives the option of 'home working', offshoring or outsourcing - or any combination necessary to meet user demand.
- **Follow the sun:** Some global or international organizations may combine two or more of their geographically dispersed service desks to provide a 24-hour follow-the-sun service. This can give 24-hour coverage at relatively low cost, as no desk has to work more than a single shift. However, common processes, tools, a shared database of information, and robust handover procedures are needed for this to be successful.
- **Specialized service desk groups:** Some organizations find it beneficial to create specialist groups within the overall service desk structure, so that incidents relating to a particular IT service can be routed directly to the specialist group, allowing faster resolution of these incidents, through greater familiarity and specialist training.

Function 2: Technical management function

Technical management role

Technical management plays a dual role:

- It is the custodian of technical knowledge and expertise related to managing the IT infrastructure. In this role, technical management ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined
- It provides the actual resources to support the service lifecycle. In this role technical management ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

Part of the role is also to ensure a balance between the skill level, utilization and cost of these resources.

Technical management objectives

The objectives of technical management are to help plan, implement and maintain a stable technical infrastructure to support the organization's business processes through:

- Well designed and highly resilient, cost-effective technical topology

- The use of adequate technical skills to maintain the technical infrastructure in optimum condition
- Swift use of technical skills to speedily diagnose and resolve any technical failures that do occur.

Function 3: IT operations management function

IT operations management role

The role of IT operations management is to execute the ongoing activities and procedures required to manage and maintain the IT infrastructure so as to deliver and support IT services at the agreed levels.

As with many ITSM processes and functions, IT operations management plays a dual role and must achieve the right balance between the two roles:

- The stability of the IT infrastructure and consistency of IT services is a primary concern of IT operations
- IT operations must also continually adapt to new and changing business requirements and demand.

IT operations management includes two functions:

- **IT operations control:** Staffed by shifts of operators who carry out routine operational tasks. They provide centralized monitoring and control, usually from an operations bridge or network operations centre. Specific activities include:
  - Console management - defining and operating a central observation and monitoring capability
  - Job scheduling - the management of routine batch jobs or scripts
  - Backup and restore - on behalf of all technical and application management teams and departments and often on behalf of users
  - Print and output management
  - Maintenance activities - on behalf of technical or application management teams or departments.
- **Facilities management:** Responsible for the management of data centers, computer rooms and recovery sites together with their power and cooling requirements. Facilities management also coordinates large-scale projects, such as data center consolidation or server consolidation.

IT operations management objectives

The objectives of IT operations management include:

- Achieving stability of the organization's day-to-day processes and activities
- Continual improvements to improve service at reduced costs, while maintaining stability
- Rapid diagnosis and resolution of any IT operational failures that occur.

Function 4: Application management function

Application management role

Application management is responsible for managing applications throughout their lifecycle. This differs from application development as application management covers the entire ongoing lifecycle of an application, including requirements, design, build, deploy, operate and optimize.

Application management activities are performed in all applications, whether purchased or developed in-house. One of the key decisions that they contribute to is the decision of whether to buy an application or build it. Once that decision is made, application management has several roles:

- It is the custodian of technical knowledge and expertise related to managing applications. In this role application management, working together with technical management, ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined
- It provides the actual resources to support the service lifecycle. In this role, application management ensures that resources are effectively trained and deployed to design, build, transition, operate and improve the technology required to deliver and support IT services.

By performing these roles, application management is able to ensure that the organization has access to the right type and level of human resources to manage applications and thus to meet business objectives. Application management also performs other specific roles:

- Providing guidance to IT operations about how best to carry out the ongoing operational management of applications
- Integration of the application management lifecycle into the service lifecycle.

Application management objectives

The objectives of application management are:

- To support the organization's business processes by helping
- identify functional and manageability requirements for application software
- To assist in the design and deployment of applications and the ongoing support and improvement of those applications.

These objectives are achieved through:

- Designing applications that are resilient and cost-effective
- Ensuring that the required functionality is available to achieve the required business outcome
- Organizing technical skills to maintain operational applications in optimum condition
- Using technical skills to speedily diagnose and resolve technical failures that occur.

Application development versus application management

Often, application development and management teams and departments have acted as autonomous units. Each one manages its own environment in its own way and each has a separate interface to the business.

Application development will become more accountable for the successful operation of applications they design, while application management will move towards greater involvement in the development of applications.

Table 5.6 Application development versus application management

	Application development	Application management
Nature of activities	One-time set of activities to design and construct application solutions	Ongoing set of activities to oversee and manage applications throughout their entire lifecycle
Scope of activities	Performed mostly for applications developed in-house	Performed for all applications, whether purchased from third parties or developed in-house
Primary focus	Utility focus Building functionality for their customer What the application does is more important than how it is operated	Both utility and warranty focus What the functionality is as well as how to deliver it Manageability aspects of the application, i.e. how to ensure stability and performance of the application
Managementmode	Most development work is done in projects where the focus is on delivering specific units of work to specification, on time and within budget. This means that it is often difficult for developers to understand and build for ongoing operations, especially because they are not available for support of the applicationonce they have movedon to the next project	Most work is done as part of repeatable, ongoing processes. A relatively small number of people work in projects. This means that it is very difficult for operational staff to get involved in development projects, as that takes them away from their ongoing operational responsibilities
Measurement	Staff are typically rewarded for creativity and for completing one project so that they can move on to the next project	Staff are typically rewarded for consistency and for preventing unexpected events and unauthorized functionality (e.g. 'bells and whistles' added by developers)
Cost	Development projects are relatively easy to quantify because the resources are known and it is easy to link their expenses to a specific application or IT service	Ongoing management costs are often mixed in with the costs of other IT services because resources are often shared across multiple IT services and applications
Lifecycles	Development staff focus on software development lifecycles, which highlight the dependencies for successful operation, but do not assign accountability for these	Staff involved in ongoing management typically only control one or two stages of these lifecycles - operation and improvement

Chapter 6: Continual service improvement

ITIL Continual Service Improvement provides guidance on creating and maintaining value for customers through better strategy, design, transition and operation of services. It combines principles, practices and methods from quality management, change management and capability improvement.

ITIL Continual Service Improvement describes best practice for achieving incremental and large-scale improvements in service quality, operational efficiency and business continuity, and for ensuring that the service portfolio continues to be aligned to business needs. A closed loop feedback system, based on the Plan-Do-Check-Act (PDCA) cycle, is established. Feedback from any stage of the service lifecycle can be used to identify improvement opportunities for any other stage of the lifecycle.

PURPOSE, OBJECTIVES, SCOPE AND VALUE OF CONTINUAL SERVICE IMPROVEMENT

Purpose and objectives

The purpose of the CSI stage of the lifecycle is to align IT services with changing business needs by identifying and implementing improvements to IT services that support business processes. CSI is always seeking ways to improve service effectiveness, process effectiveness and cost effectiveness.

The objectives of CSI are to:

- Review, analyze, prioritize and make recommendations on improvement opportunities in each lifecycle stage
- Review and analyze service level achievement
- Identify and implement specific activities to improve IT service quality and improve the efficiency and effectiveness of the enabling processes
- Improve cost effectiveness of delivering IT services without sacrificing customer satisfaction
- Ensure applicable quality management methods are used to support continual improvement activities
- Ensure that processes have clearly defined objectives and measurements that lead to actionable improvements
- Understand what to measure, why it is being measured and what the successful outcome should be.

Scope of CSI

ITIL Continual Service Improvement provides guidance in four main areas:

- The overall health of ITSM as a discipline
- The continual alignment of the service portfolio with the current and future business needs
- The maturity and capability of the organization, management, processes and people utilized by the services
- Continual improvement of all aspects of the IT service and the service assets that support them.

ITIL ® is a registered trade mark of the Cabinet Office, United Kingdom

Value to business

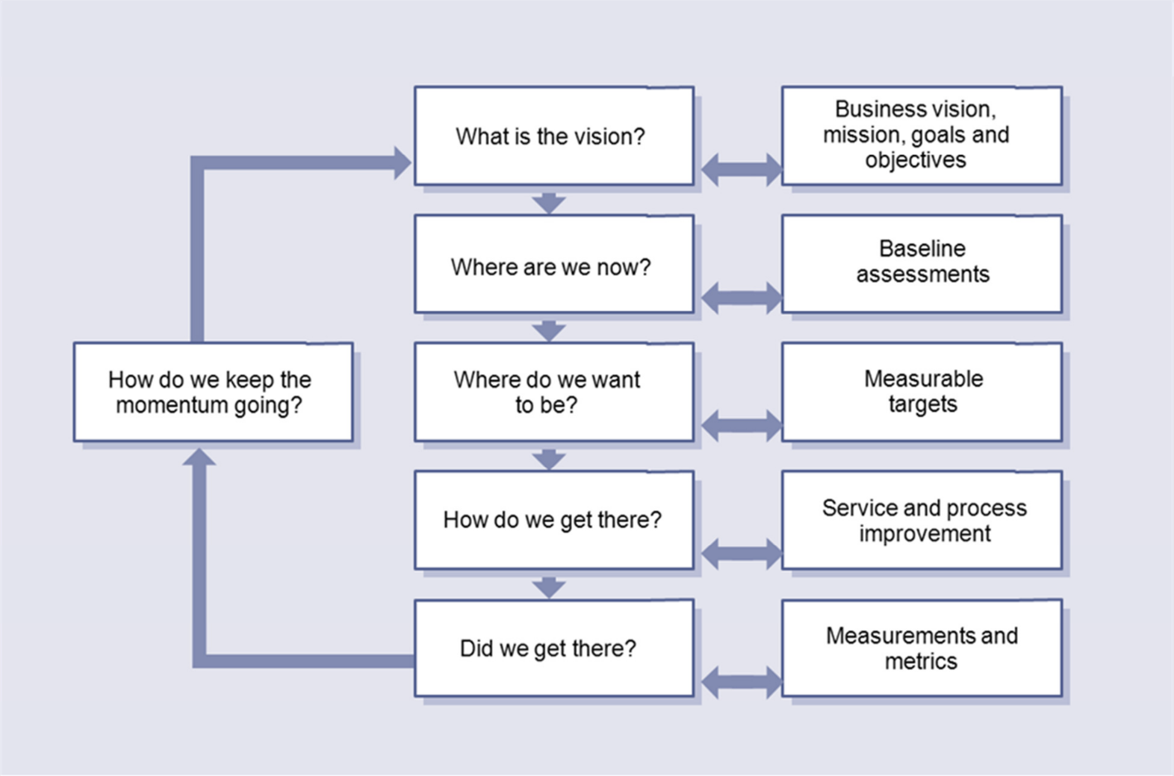
Adopting and implementing standard and consistent approaches for CSI:

- Leads to a gradual and continual improvement in service quality, where justified
- Ensures that IT services remain continuously aligned to business requirements
- Results in gradual improvements in cost effectiveness through a reduction in costs and/or the capability to handle more work at the same cost
- Uses monitoring and reporting to identify opportunities for improvement in all lifecycle stages and in all processes
- Identifies opportunities for improvements in organizational structures, resourcing capabilities, partners, technology, staff skills and training, and communications.

KEY PRINCIPLES

Service improvement must focus on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT service management (ITSM) processes. The only way to do this is to ensure that improvement opportunities are identified throughout the entire service lifecycle.

Continual service improvement approach



© Crown copyright 2013 Reproduced under license from OGC

Figure: Continual service improvement approach

The figure shows an overall approach to CSI and illustrates a continual cycle of improvement. This approach to improvement can be summarized as follows:

- **What is the vision?** Understand high-level business objectives and align business and IT strategies.
- **Where are we now?** Assess the current situation to obtain an accurate, unbiased snapshot of where the organization is now, including the business, organization, people, process and technology.
- **Where do we want to be?** Understand and agree on the priorities for improvement based on the vision. The full vision 260 Continual service improvement may be years away but this step provides specific goals and a manageable timeframe.
- **How do we get there?** Detail the CSI plan to achieve higher quality service provision by implementing or improving ITSM processes.
- **Did we get there?** Verify that measurements and metrics are in place and that the milestones were achieved, process compliance is high, and business objectives and priorities were met.
- **How do we keep the momentum going?** Ensure the momentum for quality improvement is maintained by assuring that changes become embedded in the organization.

Continual service improvement register

Many initiatives or possibilities for improvement may be identified and it is recommended that a CSI register is kept to record all improvement opportunities. Each opportunity should be categorized into small, medium or large undertakings and also categorized into initiatives that can be achieved quickly, or in the medium term or longer term.

Each improvement initiative should also show the benefits that will be achieved by its implementation. With this information a clear prioritized list can be produced. The CSI register contains important information for the overall service provider and should be held and regarded as part of the service knowledge management system (SKMS). The CSI manager should have accountability and responsibility for the production and maintenance of the CSI register.

The Deming Cycle/PDCA cycle

The Deming Cycle (Plan-Do-Check-Act or PDCA cycle) is widely used as the foundation for quality improvement activities across many types of organization.

- **Plan** Clearly document the target state and the intended steps to get there
- **Do** Execute the plan
- **Check** Monitor and measure outcomes to determine actual achievements against the plan
- **Act** Identify gaps against expectations and opportunities for further improvement.

The PDCA cycle is critical at two points in CSI: implementation of CSI, and for the application of CSI to services and service management processes. At implementation, all four stages of the PDCA cycle are used. With ongoing improvement, CSI draws on the check and act stages to monitor, measure, review and implement initiatives.

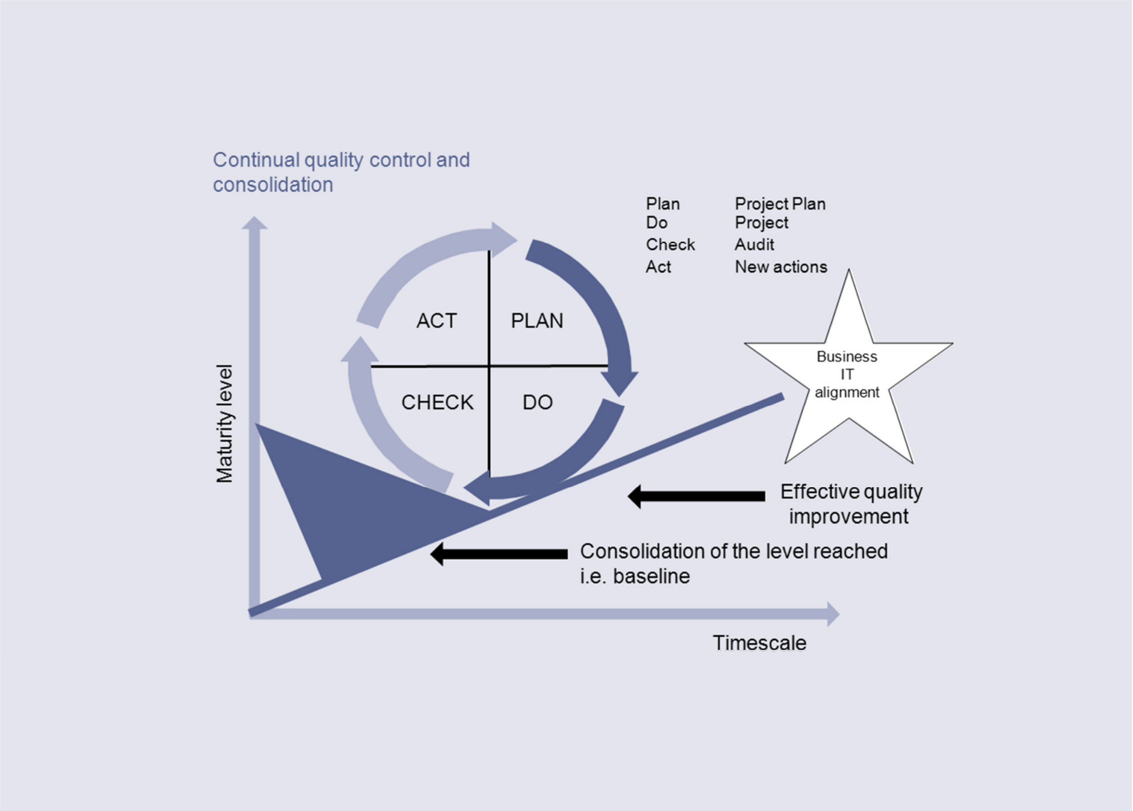

Continual quality control and consolidation
Plan
Do
Check
Act
Project Plan
Project
Audit
New actions
ACT
PLAN
CHECK
DO
Business IT alignment
Maturity level
Effective quality improvement
Consolidation of the level reached i.e. baseline
Timescale

Figure: The Deming Cycle

Service measurement

Baselines

An important starting point for any improvement activity is establishing a baseline. In the context of CSI, a baseline provides the current state of a configuration item (Cl), process or any other data recorded at a specific point in time, and is used as a reference point for future comparisons.

Trainer Note: *For example, an ITSM baseline can be used as a starting point to measure the effect of a service improvement plan (SIP);* a performance baseline can be used to measure changes in performance over the lifetime of an IT service.

It is essential to collect baseline data at the outset, even if the integrity of the data is in question. It is better to have baseline data to question than to have no baseline data at all.

Metrics, KPIs and CSFs

Metrics

Something that is measured and reported to help manage a process, IT service or activity. There are three types of metrics that an organization needs to collect to support CSI and other activities:

- **Technology metrics:** These metrics are often associated with component and application-based metrics such as performance, availability etc.

- **Process metrics:** These metrics are captured in the form of critical success factors (CSFs), KPIs and activity metrics for service management processes. They can help determine the overall health of a process and focus on quality, performance, value and compliance.
- **Service metrics:** These metrics are a measure of the end-to-end service performance. Individual technology and process metrics are used when calculating the end-to-end service metrics.

In general, a metric is a scale of measurement defined in terms of a standard, i.e. a well-defined unit.

Critical success factor (CSF)

Something that must happen if an IT service, process, plan, project or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor.

Trainer Note: *For example, a critical success factor of 'protect IT services when making changes' could be measured by key performance indicators such as 'percentage reduction of unsuccessful changes', 'percentage reduction in changes causing incidents' etc.*

Key performance indicator (KPI)

A metric that is used to help manage an IT service, process, plan, project or other activity.

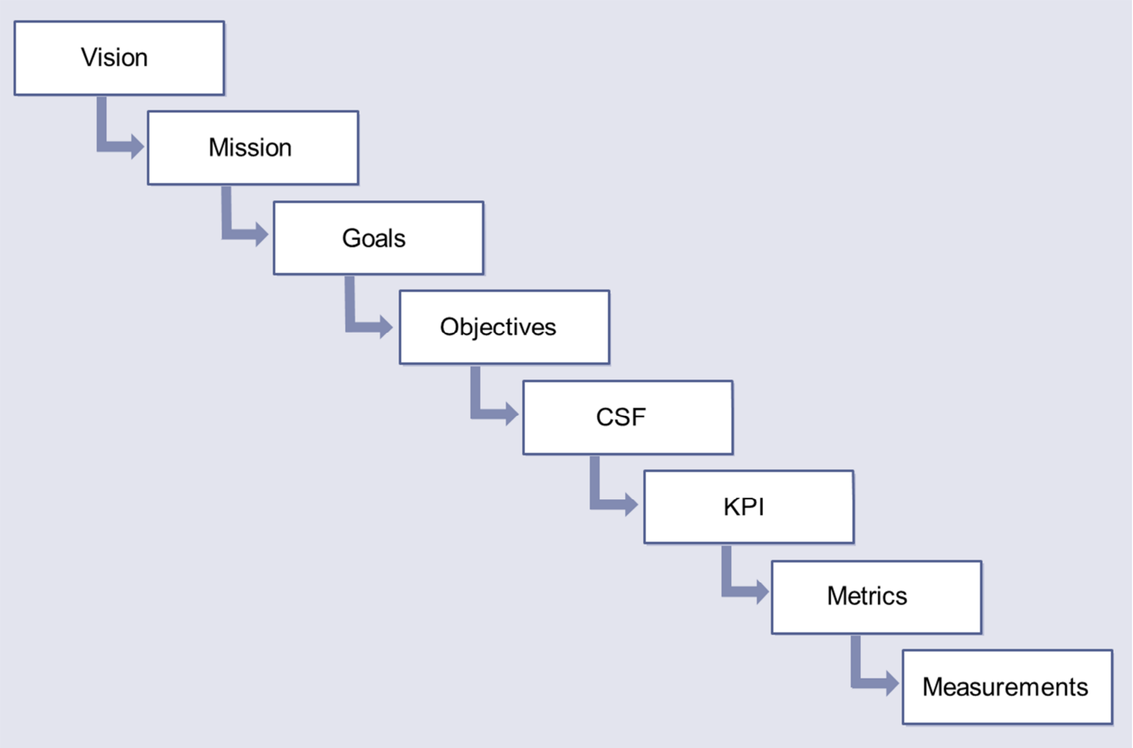
There are two basic kinds of KPI, qualitative and quantitative. Qualitative KPIs relate to the quality or character of something, whereas quantitative KPIs relate to size or quantity.

It is recommended that in the early stages of a CSI initiative only two to three KPIs for each CSF are defined, monitored and reported on. As the maturity of a service and service management processes increase, additional KPIs can be added.

Relationship between CSF and KPI:

Key performance indicators are used to measure the achievement of each critical success factor**.** For example, a critical success factor of 'protect IT services when making changes' could be measured by key performance indicators such as 'percentage reduction of unsuccessful changes', 'percentage reduction in changes causing incidents' etc. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity.

From vision to measurements



© Crown copyright 2013 Reproduced under license from OGC

Figure 6.2 From vision to measurements

To help illustrate this relationship, here are two examples of how metrics, KPIs and measurements are used to support CSFs, and ultimately the vision.

Qualitative example

- CSF: Improving IT service quality
- KPI: 10% increase in customer satisfaction rating for handling incidents over the next six months.

Metrics required:

- Original customer satisfaction score for handling incidents
- Ending customer satisfaction score for handling incidents.

Measurements:

- Incident-handling survey score
- Number of survey scores.

Quantitative example

- CSF: Reducing IT costs
- KPI: 10% reduction in the costs of handling printer incidents.

Metrics required:

- Original cost of handling printer incidents

- Final cost of handling printer incidents
- Cost of the improvement effort.

Measurements:

- Time spent on the incident by first- and second-level operatives and their average salaries
- Time spent on problem management activities by second-level operatives and their average salary

Service reporting

Service reporting is a set of activities that produce and deliver reports of achievement and trends against service levels. The format, content and frequency of reports should be agreed with customers.

PROCESSES AND ACTIVITIES

The seven-step improvement process

The purpose of the seven-step improvement process is to define and manage the steps needed to identify, define, gather, process, analyse, present and implement improvements.

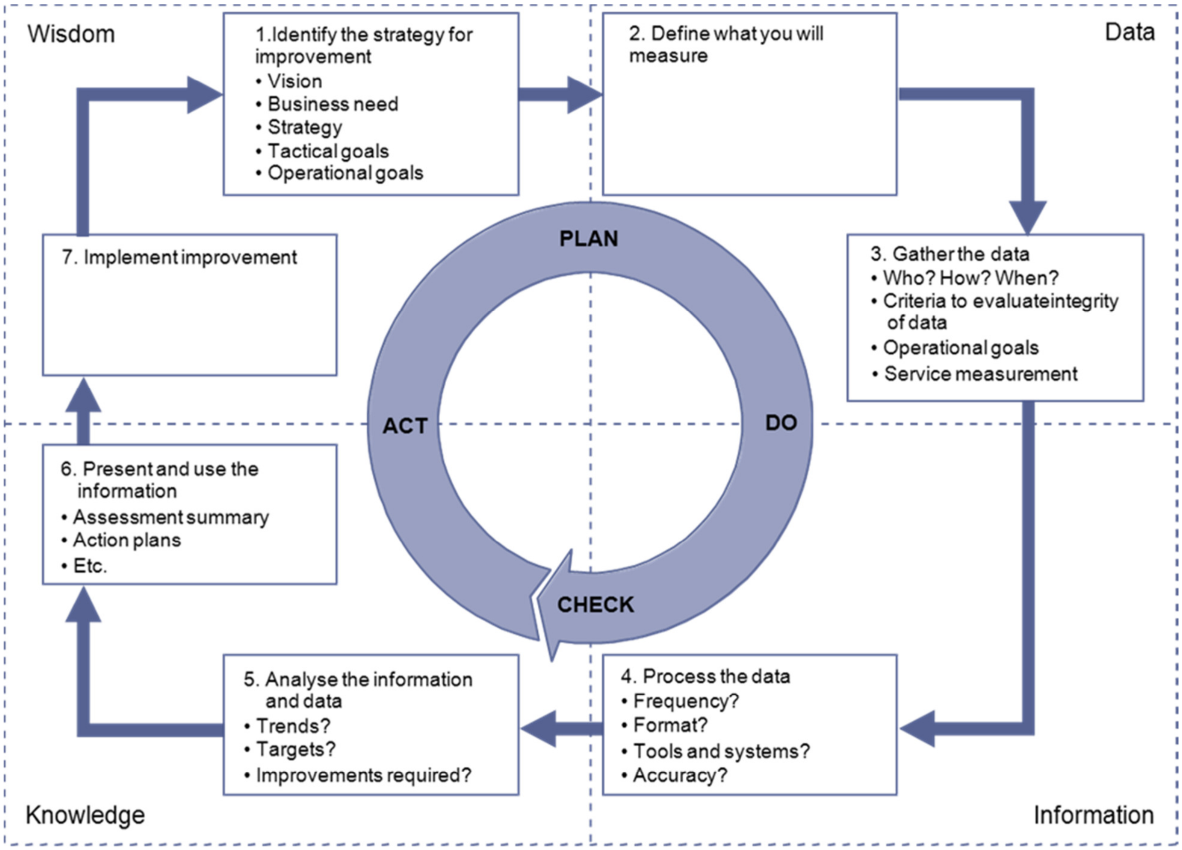


Figure: Seven-step improvement process

Figure above shows the seven-step improvement process and its interaction with the PDCA cycle and the CSI approach. The figure also shows how each of these elements aligns with the Data-to-Information-to-Knowledge-to-Wisdom (DIKW) structure of knowledge management.

The objectives of the seven-step improvement process are to:

- Identify opportunities for improving services, processes, tools etc.
- Reduce the cost of providing services and ensuring that IT services enable the required business outcomes to be achieved
- Identify what needs to be measured, analysed and reported to establish improvement opportunities
- Continually review service achievements to ensure they remain matched to business requirements; continually align and re-align service provision with outcome requirements
- Understand what to measure, why it is being measured and carefully define the successful outcome.

Scope

The seven-step improvement process includes analysis of the performance and capabilities of services, processes throughout the lifecycle, partners and technology. It includes the continual alignment of the portfolio of IT services with the current and future business needs as well as the maturity of the enabling IT processes for each service.

It also includes making best use of the technology that the organization has and looks to exploit new technology as it becomes available where there is a business case for doing so. Also within the scope are the organizational structure, the capabilities of the personnel, and asking whether people are working in appropriate functions and roles, and if they have the required skills.

Process activities, methods and techniques

While these seven steps appear to form a circular set of activities, in fact they constitute a knowledge spiral. Knowledge gathered and wisdom derived from the knowledge at one level of the organization becomes a data input to the next: from operational management, to tactical management, to strategic management.

Step 1 - Identify the strategy for improvement

What are we trying to achieve for the business and how can the IT organization contribute through improvements? Take into account current and future plans.

Step 2 - Define what you will measure

Compare what you should ideally measure with what you can actually measure, identify gaps, and develop a realistic measurement plan to support the improvement strategy. Take into account the current capabilities of tools and processes.

Step 3 - Gather the data

Use monitoring to gather the data. Monitoring can be undertaken using technology and tools or can be a manual process.

Step 4 - Process the data

Convert the data gathered into the required format for the intended audience. This can be seen as converting metrics into KPI results, and turning data into information.

Step 5 - Analyse the information and data

Combine multiple sources of data and transform the information into knowledge. Develop an understanding of the real meaning of identified patterns and trends. Answer questions such as:

- Is this good or bad?
- Is this expected and in line with targets?

Step 6 - Present and use the information

Communicate the information at the right level of detail for the audience and in a way that is understandable, provides value and supports informed decision making. Section 6.2.11 discusses reporting further and includes an example output.

Step 7 - Implement improvement

Use the knowledge gained and combine it with previous experience to make informed decisions about the improvements that should be made. These improvements should focus on optimizing and correcting services, processes, tools etc.