ITIL 2011 FOUNDATION

ITIL 2011 Foundation:

ITIL2011 and Service Lifecycle:

Understanding ITIL and Service Management:

ITIL Overview:

ITIL (IT Infrastructure Library) is a set of guidelines and best practices outlining how IT Service Management (ITSM) can be implemented. It provides documentation in the form of 5 core publications each covering different aspects of ITSM.

ITIL was developed in the late 1980s

ITIL has become the leading framework for ITSM globally; the reasons for this include that

- It is **Non proprietary**
- It is **Non prescriptive**
- It provides **best practices**, and
- It provides **good practices**.

Non Proprietary:

- Means it is not owned by any organization and can be used by anyone.
- It is developed by **Office of Government Commerce (OGC)**, an independent office of British Treasury.
- It is a generic framework that is not based on any specific operating system, technology or industry.

Non Prescriptive:

- The framework is applicable in all types of organizations of any size

Best Practices:

- Provides best practices in ITSM that is followed by leading IT Service Providers. This means a new organization that follows ITIL will benefit from experience of Industry Leaders.

Good Practices:

- Provides good practices. These are practices that are adapted from other organizations and environments that were effective in achieving a particular benefit.

OGC works in conjunction with additional organizations to manage and provide ITIL. They are,

The Stationary Office (TSO):

- ✓ TSO is the largest publishing house in the UK.
- ✓ TSO is the official publisher for the OGC.

The APM Group or APMG:

- ✓ APMG is an accreditation, certification and qualification organization.
- ✓ OGC has appointed APMG as its official accreditor.

The Examination Institute for Information Science (EXIN):

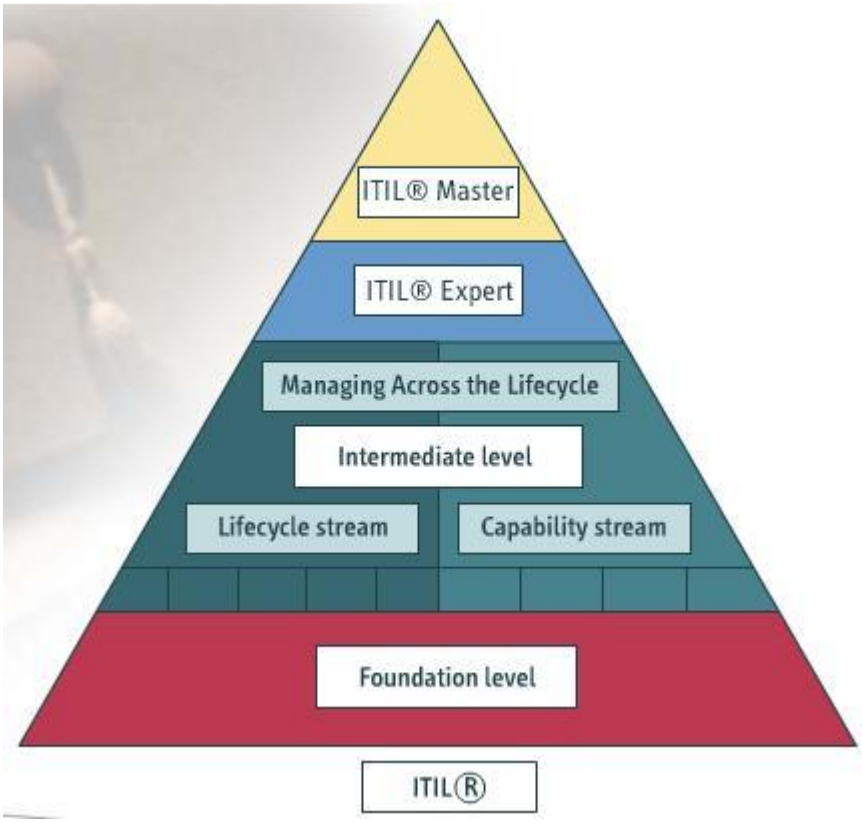
- ✓ EXIN is a global, independent examination provider.
- ✓ Develops and organizes official ITIL exams for all ITIL Qualifications.

Why should your organization adopt ITIL best practices for ITSM?

The reasons are,

- Improved quality and speed of IT Services.
- Improved customer relationships.
- Clear linking between IT Services and business Strategies.
- To narrow down gap between organization and their competitors.

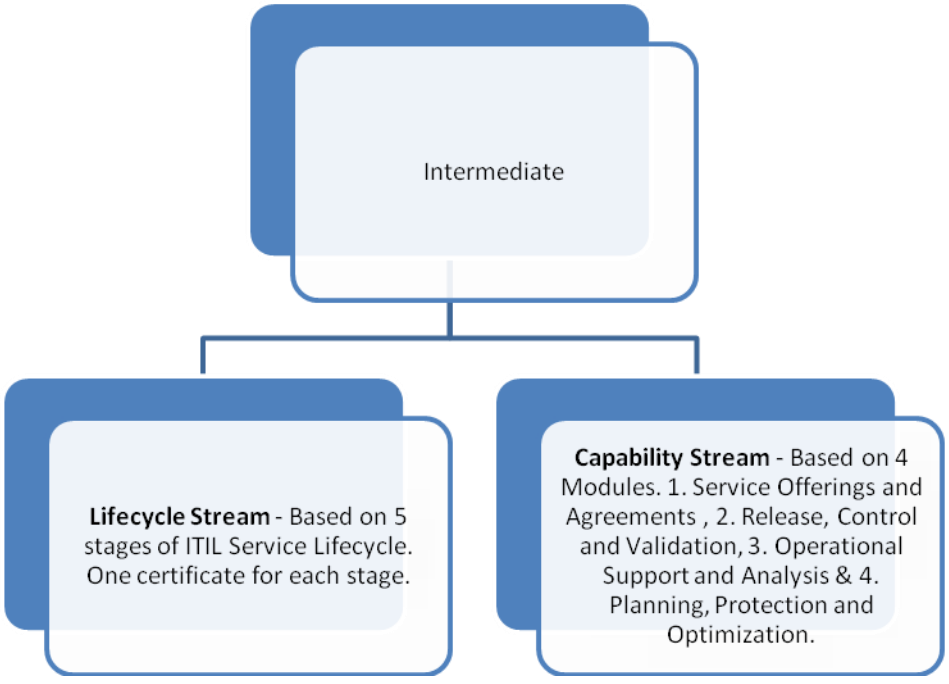
ITIL Qualification Scheme:



Foundation: Worth 2 credits

- Provides an introductory grounding in ITIL Concepts and covers basic concepts in ITIL framework.

Intermediate: Must acquire 15 credits to achieve:



Expert: Worth 5 credits

- Managing across lifecycle exam consolidates knowledge gained through foundation and intermediate modules.
- On completion and accumulation of 22 credits ITIL Expert Certification shall be awarded.

Master:

- ITIL Master Certification demonstrates an individual's proven ability to apply key ITIL methods and concepts to solve real world problems.

Basics of Service and Service Management:

Service:

A service is method of providing value to the customer by helping them achieve their objectives. "A service is a means of delivering value to customer by facilitating outcomes that customer want to achieve without the ownership of specific costs and risks"

Services are only successful if they provide value for customers. To add real value for customers, a service must have

- **Utility – be fit for purpose**
- **Warranty – be fit for use.**

Utility or fitness for purpose:

Utility is how useful a service is to customer. There are 2 ways to have increased utility,

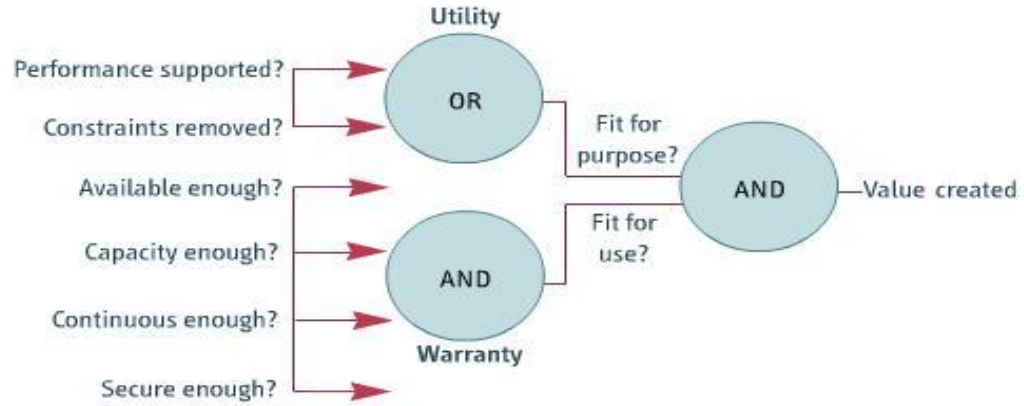
i. **Improve Performance:**
   - ✓ By improving skills of staffs
   - ✓ By providing the latest and best technology
   - ✓ By encouraging creativity and innovation

ii. **Relax or remove constraints on performance:**
   - ✓ Anything that limits the ability to provide a service is a constraint. A poor work environment, obsolete computers or a bureaucratic administration are few things that can constrain performance and limit utility.

Warranty or fitness for use:

Warranty refers to the guarantee that a service will meet its agreed requirements. Warranty has 4 characteristics,

1. **Availability** – a service must be available when it is required.
2. **Capacity** – a service must be provided at the right capacity or levels.
3. **Continuity** – a service must have continuity. An organization must consistently and continuously provide good service to maintain its reputation.
4. **Security** – a service must provide security, i.e.it must not involve any risk for the customers, and if a risk is unavoidable a service should at least minimize that risk.



Service Management:

Service Management is a set of specialized organization capabilities that can provide value to the customers in the form of services.

Service Management is a professional practice that has origins in the traditional service industries such as banking, airlines and hotels. Recently IT organizations have embraced a service oriented approach to managing IT processes.

Challenges to Service Management:

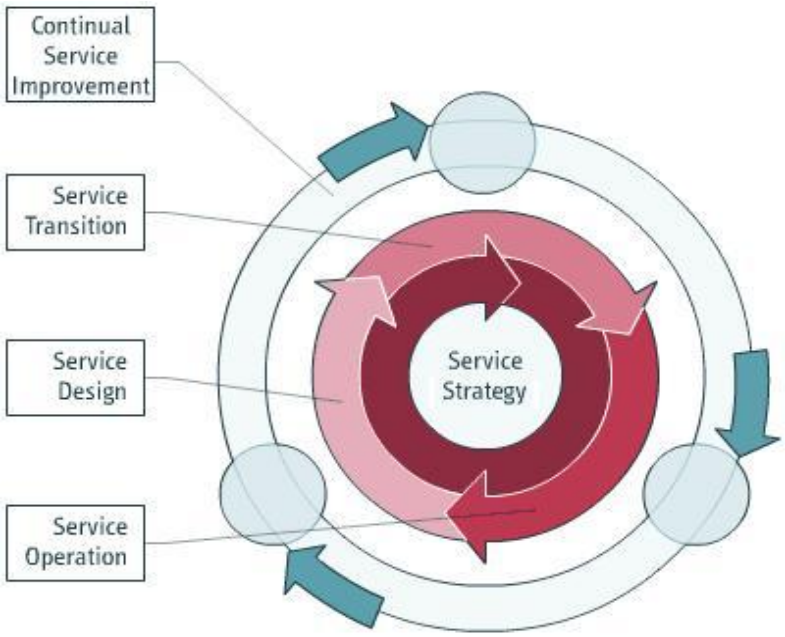
i. **The subjective nature of the output:**
   The main challenge of Service Management is that a good service is hard to identify, measure or control.

ii. **The demand is tied to customer's assets:**
   The demand for a service is integrally connected to a customer's assets. If the demand is high, the service provider is challenged to keep pace with the customer. If the demand is low the customer should be cautious of overusing their own assets to supply a service to customers with assets not in high demand.

iii. **The high levels of contact with customer:**
   Service providers work on the front line, often face-to-face and with high level of contact with the customer. As such there may be a buffer between the customer front office and back office.

iv. **The changing nature of demand:**
   The service provider needs to secure a steady supply of demand. This can only be done by offering value in the form of consistent quality.

The ITIL Service Lifecycle:



ITIL provides a framework and best practices guidelines for implementing, providing, managing and maintaining IT Services.

The core of ITIL is the ITIL Service Lifecycle – a comprehensive approach to service management.

The ITIL lifecycle is comprised of 5 key stages

1. Service Strategy (
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

Service Strategy:
This stage determines the underlying principles used for developing policies, objectives, guidelines and processes that are required throughout the progression of lifecycle. It also involves identifying business opportunities.

Service Design:
In this stage IT Services are designed and developed based on the principles founded during service strategy stage.

Service Transition:
Service Transition is the stage for creating a framework that will ensure that the designed services are effectively and efficiently implemented in the live environment. This stage includes determining risks, constraints and whether the services will meet requirements. This ensures that the expected performance is closely in line with actual performance.

Service Operation:
Service Operation is the stage in which all the required activities and processes for effectively running designed services are carried out; so that the framework developed in the Service Transition stage is effectively implemented.

Continual Service Improvement (CSI):
The Continual Service Improvement (CSI) stage is an overarching stage for maintaining the quality of services. This is done through learning and improving on processes involved in each stage of the ITIL Service Lifecycle. These continual Service improvements help ensue the effectiveness and efficiency of each stage.

Each stage in ITIL Service Lifecycle has specific objectives.

Objectives of Service Strategy Stage:
During Service Strategy stage, the primary objective is to create strategic goals and objectives that an organization hopes to achieve through the IT Services it delivers. Other objectives include,

- Turning Service Management into strategic assets to help service providing organizations achieve their goals.
- Determining the nature and the type of IT Services to offer and how they may differ from competing IT Services.
- Creating value for customers and stakeholders.
- Defining service quality and determining how to deliver and improve it.
- Determining how to allocate resources and creating a strategy for leveling over allocated resources.
- Determining where and when to make strategic investments.

Objectives of Service Design Stage:

The primary objective of Service Design stage is to design sound services and processes. The design of plans, processes, infrastructure, environments, applications and data resources must meet all objectives and business requirements such as quality, risk, compliance and security requirements. Further objectives of Service Design stage includes,

- Designing processes that ensure effectiveness, efficiency and good service management throughout the ITIL Service Lifecycle.
- Designing a stable IT Infrastructure that can be further expanded or developed without compromising time or cost constraints.
- Recognizing and controlling risks.
- Designing measurement methods to evaluate the success of the design processes.
- Assisting in creation of policies and standards through feedback about the design process.
- Ensuring that IT services do not need to be reworked once implemented.

Objectives of Service Transition Stage:

The purpose of service transition stage is to ensure that designed IT services are efficiently and effective transitioned into operation. This is done through packaging, building, testing and then deploying the services into live environment. The main objectives of Service Transition stage are,

- **Selecting resources and capacity:**
  An important objective of Service Transition stage is to select the resources and capacity that are required to establish IT services and to ensure that these resources are within the estimated budget, quality and time constraints.
- **Controlling visible errors and anticipating risks:**
  When IT services are transitioned into operation, it is important to ensure that the expected performance is closely in line with actual performance. This stage reduces and controls visible errors and anticipates risks so that there is little or no unanticipated impact on the lifecycle.
- **Meeting service requirements and constraints:**
  During Service Transition stage, operations and support must be able to meet service requirements and constraints that were specified during the service design and service strategy stage.
- **Meeting customer expectations:**
  Upon implementation of IT services performance, use and ability of the services must meet customer expectations. The customer, user and service provider must be satisfied with the methods of deployment, communication, and the accompanying data, training and knowledge handover.

Objectives of Service Operation:

During Service Operation stage the primary purpose is to ensure that the processes for effectively running the IT services are carried out properly. Objectives include,

- Continually maintaining any or all technology that accompanies the IT services.
- Ensuring that everyday operation of the processes is properly conducted and controlled.
- Ensuring efficient and effective management of the operational processes.
- Continually monitoring performance, conducting assessments and gathering information.

Objectives of Continual Service Improvement (CSI):

CSI concerned with overall improvement of all stages and processes that constitute an organization's delivered IT services. The purpose of the CSI is to identify areas that need improvement and ensure that those improvements are effectively and efficiently administered. Objectives of CSI stage include,

- Reviewing and improving aspects of each ITIL Service Lifecycle stage.
- Applying activities that improve overall IT service quality as well as IT Service Management processes.
- Ensuring customer satisfaction while ensuring cost effectiveness.
- Ensuring quality of the management methods used for the CSI process.

Scope and Value of Lifecycle stages:

Each stage of the ITIL service lifecycle performs specific activities to realize particular objectives. These activities are known as the scope of stage:

Scope of Service Strategy Stage: Determining Strategic Objectives

- determining strategic objectives
- defining resources
- providing guidance for growth
- prioritizing IT investments
- creating plans and actions and assigning them functions in Service Management
- defining the expected results so the success of Service Management can be evaluated at a later stage.

Scope of Service Design: creating a developed solution

- creating a developed solution that can meet the business requirements – such as the business strategies and constraints

Scope of Service Transition: packaging, building, testing and releasing

- packaging, building, testing and releasing the service
- ensure that all the customer requirement and expectations are met
- ensure incident management strategies are in place to ensure smooth transition.

Scope of Service Operation: running and supporting a service

- running and supporting a service
- performance of most service management processes
- management of technology required to deliver and maintain the service
- recognition of the people who are responsible for the demand, decisions and management of services.

Scope of Continual Service Improvement (CSI): maintaining the overall health of IT Service Management

- maintaining the overall health of ITSM
- continually aligning services with business needs
- monitoring the maturity of processes throughout the service lifecycle
- performing internal audits, gathering information on customer satisfaction, making recommendations, reviewing the service and deliverables for relevance and for further improvement opportunities.

Importance of Service Operation Stage:

- Generates value for the customer by applying the plans, designs, resources, and solutions developed during the other stages of the ITIL® Service Lifecycle.
- From the customer's perspective, Service Operation is the most valuable stage because it promotes effective and efficient service delivery and support.
- Uses tools, guidelines, and processes to ensure consistency and stability in operational activities. A stable IT operations environment makes it easier to implement changes and improvements in the design, scale, and scope of service offerings and service levels.
- Manages the technologies and activities required to support an IT service.
- Supports the provision of services, management of demand, and optimal use of organizational capacity.
- Assists in problem solving, scheduling operational activities, and implementing new IT models and architectures.

Value:

Each stage of the ITIL® Service Lifecycle intends to provide some kind of value to the business - benefits the organization can achieve if it adopts good practices.

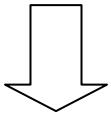
Value of Service Strategy:

- Can help organizations to develop and maintain the advantage of being the reliable and valuable IT Service Providers.

Value of Service Design:

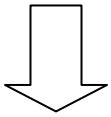
The value achieved by good service design can be observed when a good quality, cost – effective service is created according to business requirements. Some of the benefits of superior design practices are,

- **Reduced Total Cost of Ownership (TCO)**
  Good design practices = minimum Total Cost of Ownership (TCO)
- **Improved quality and consistency of IT services and ITSM**.
- **Effective IT service performance**
  This can be realized by including capacity, financial, availability and IT Service continuity plans.
- **Efficient implementation and better IT Service alignment**
  Good Service Design can ensure that IT services can be efficiently implemented and IT services align better to current and future business needs. This ensures that the IT services will meet Service Level Requirements (SLRs)
- **Improved IT Governance**
- **Better information and decision making**
  Creation of thorough and effective measurements and metrics



Will ensure

Information gathered is reliable and valuable



In turn ensures

Better decision making in service management processes.

Value of Service Transition:

The Service Transition stage is important for enabling an IT service provider to align services with business requirements and operations. Effective administering of Service Transition can ensure that an IT service provider is adaptable and has a competitive edge in being able to handle large amount of changes, improvements and releases for all its customers. The Service Transition stage can add value to a business by improving,

- A business' productivity, including staff productivity through the use of new or improved IT service.
- The ability to predict the service levels for IT services and to reduce high variances between expected and actual performance of IT service.
- Value to business operations through effective use of service by customers and users.
- The ability to meet business and governance compliance requirements.
- Skills in predicting risks and type of risks, so as to prevent service outages, disruptions or reworks.
- The administration of maintenance contracts so that cancellations or changes are timely and without problems.

Value of Service Operation:

- Culminates the value that each of the other stages of lifecycle provides.

Service Strategy	⇨	determines service value
Service Design	⇨	designs service
Service Transition	⇨	predicts and validates service
CSI	⇨	identifies areas that can be improved and optimized
Service Operation	⇨	ensures that these plans, designs and improvements are realized and monitored through IT Service Operation.

- Service Operation also provides value to the customer, as it is the stage where results of IT Services are most apparent. This means that its value can be readily determined.

Value of Continual Service Improvement (CSI):

The 4 terms that illustrates the value that CSI provides to a business are,

1. **Improvements**
   Results that show a positive difference when a process is applied.
2. **Benefits**
   Implementation of improvement yields a measurable result known as benefits.
3. **Return on Investment (ROI)**
   $$ROI = \frac{\text{Benefit – cost of benefit}}{\text{Cost of benefit}}$$
   In other words ROI will determine how much was saved in proportion to what was spent.
4. **Value on Investment (VOI)**
   VOI is defined as an additional value that is derived from benefits gained. This additional value can include non – monetary gains or gains that are realized over a longer time period.

Article: Lifecycle Functions and Processes

Introduction: There are various activities and behaviors that perform unique tasks throughout the IT Infrastructure Library (ITIL®) Service Lifecycle. These activities are linked, yet distinct in their nature and purpose, and can be divided into **processes** and **functions**.

Processes

- Business processes are systems that produce business outcomes according to constraints, objectives, and policies. The outcomes create value for the customer or stakeholder.
- In any given process, people apply their knowledge within a workflow infrastructure to complete specific tasks, monitor performance, and intervene when necessary. Within service management, processes focus the organization's cumulative skills and knowledge on particular service outcomes.
- For a process to be considered strategically useful, it must give the organization a competitive advantage and differentiate it in the market.
- Processes are particularly useful because they can cross organizational and geographic boundaries, and can incorporate suppliers and customers.
- IT systems – the applications and infrastructure – should make processes more transparent and dynamic, and align to organizational strategy.
- Communication between business and IT managers must be exceptionally good to facilitate the complex task of aligning information, applications, and infrastructure with business strategy.

A process is a structure or model that turns a defined input into a defined output through change and transformation. Processes are organized sets of dependent activities that are created to achieve a specific objective for a particular customer. The sequence of the activities is determined by the dependencies between the activities. Processes are closed-loop systems that use of feedback to self-reinforce and self-correct.

4 distinct characteristics of processes:

1. The first is that a process is measurable, and has an outcome that can be measured and reviewed for a particular reason (reason such as cost, quality, duration or productivity)
2. Second, a process is aimed at achieving a specific result, and the result must be identifiable and measurable.
3. Third, a process is aimed at supplying specific results to customers and stakeholders, according to their expectations.
4. Fourth, a process occurs because of a response to a specific event or trigger. This is regardless of the fact that a process may be ongoing.

Processes require control so that they can be repeated with consistent results. This involves careful definition and planning, and documentation, of all the steps and their dependencies, and the sequence of the steps. For a process to be considered effective, it must conform to the organization's operational norms and standards. And for it to be efficient, it must use the minimum resources.

Functions

Functions are specialized units or groups within an organization that perform a specific type of work and create specific results, through defined roles and responsibilities. Unlike processes, which are triggered by specific events, functions are established at a planning stage to fulfill organizational requirements. Functions generally carry out separate tasks or processes as required by their work. Functions are similar to processes in that they are also created for a specific purpose, but functions play a more specific role in doing a specific type of work.

Multiple functions in an organization are often coordinated through shared processes, which also tend to make them more productive.

Specialization and coordination across the lifecycle

At each stage of the Service Lifecycle – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement (CSI) – it is important to apply specialist functions and processes in order to achieve each stage's objectives. However, it is also important that there is coordination between these activities. There needs to be feedback and control between the functions and processes across the lifecycle.

In reality, an organization would need to adopt control methods in order to achieve effective management, and the ITIL® Service Lifecycle approach closely imitates this. There are two types of control perspectives that can be adopted – process-based control perspectives and lifecycle-based control perspectives. Process-based control perspectives are suited for those involved in the design, development, and improvement of processes for service management. Lifecycle-based control perspectives are suited to those involved in managing contracts, agreements, and services. These control perspectives both profit from systems thinking, and each can provide insights and patterns that might not be obvious in the other.

Service Strategy Fundamentals:

Service Strategy Concepts:

Service Strategy helps you to recognize how to use IT Services and Service automation to create added value to your organization.

Basic Concepts:

- Strategy
- Customers
- Services
- The Service portfolio
- Service provider
- Stakeholders

Strategy:

A strategy defines how a service provider will use services to enable customers achieve the business outcomes they require – and so in the process meet its own objectives.

Customers:

Customers are those who buy goods or services and establish service level targets. They may be internal or external.

Differences between internal and external customers:

Internal Customers	External Customers
Links with business strategy and Objectives: Internal customers share same overall organizational objectives and strategy as the service provider.	Service provider needs to determine what the customers' business objectives are in order to provide required levels of performance and functionality.
Cost of Service: The aim of providing service to the internal customers is to provide an optimal balance between cost and the quality of service, and so to support organization in achieving its objectives.	Actual cost is not disclosed to the external customer. The aim of service provider is to maximize profits while still remaining competitive with the pricing.
Involvement in Service Design: When customers are internal, services are	External Customers are typically less involved

designed based on enterprise policies, resource constraints and expected Return on Investment (ROI). Customers tend to be involved in generating detailed specification in terms of functionality and manageability of services.	in service design and service provider doesn't typically get involved in calculating customer's ROI.
Involvement in Service Transition and Operation: Internal customers get involved in building, testing and deploying services. Customers and IT Managers have to assess and authorize changes.	External customers are not generally involved in designing and testing of services and they may not be aware how these processes are managed.
Drivers for improvement: When customers are internal, objectives of the business units and the impact of services on these are the drivers for improvement. The aim is generally to optimize the balance between cost and quality.	When the customers are external, the need to retain customers and remain competitive drives improvement. The aim is to provide competitive service levels at reduced cost.

Services:

Services are means of delivering value to the customer. They facilitate outcomes that customer want achieve, while enabling them to pass on the risks and costs of designing and maintaining the services to an external service provider.

IT Services can be

- ✓ Internal, or
- ✓ External

Internal IT Service:

Internal IT services are delivered between departments or business units in the same organization. They support the business process that other internal business units manage.

External IT Services:

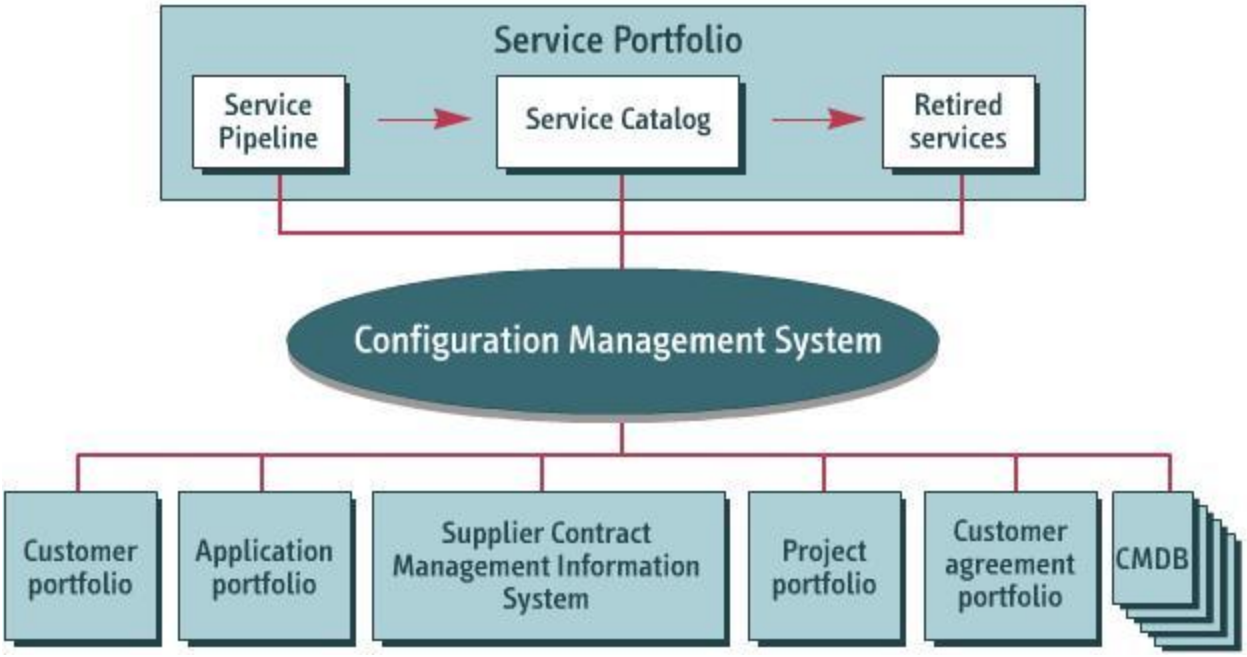
External IT Services are delivered to external customers. For example, an IT organization may provide public internet access at an airport.

Service Portfolio:

- ✓ A service portfolio is a complete set of services that a service provider manages.
- ✓ It records present contractual commitments, new service developments and ongoing service improvement plans.
- ✓ It also covers third party services which are integral part of service offerings to customers.

The Service Portfolio represents all the resources presently engaged or being released in various stages of the ITIL® Service Lifecycle. Each stage requires resources for completion of projects, initiatives, and contracts. This is a very important governance aspect of Service Portfolio Management.

The Service Portfolio should have the right mix of services in the Service Pipeline and Service Catalog to secure the financial viability of the service provider. The Service Catalog, however, is the only part of the portfolio that lists services that recover costs or earn profits.



Service Providers:

Service Providers supply IT Services to customers. They can be

- Internal Service provider
- Shared service unit
- External Service provider

Internal Service provider:

An internal service provider is embedded within an organization; there may be several internal service providers in an organization.

Shared service unit:

Shared service unit is a type of internal service provider that provides shared IT Services to more than one business unit.

External Service provider:

An external service provider provides IT services to external customers.

Stakeholders:

Stakeholders are those who have an interest in an IT Organization, its services, its targets, its policies, its projects, its activities, its resources and deliverables from Service Management.

External stakeholders may include customers, consumers, shareholders, partners, organizations, owners and suppliers.

Internal stakeholders are those within a service provider organization – include groups that deliver services and those that use them.

Create Value with Assets and Services:

A strategic perspective starts with understanding competitors and their services. This enables organizations to review their position and provide differentiated value to the customers.

Adding value to a service involves

- Providing differentiated value to the customers and
- Ensures that the organization does not become subject to competitive forces.

In some instances value can be quantified in financial terms. In other instances value is determined by a number of non financial factors such as,

Customer Perceptions:

Customers' preferences are influenced by perception. In turn customer perceptions are influenced by attributes of an IT Service such as

a. Value
b. Previous experience
c. Capabilities and capacity of competitors and their products.
d. Self image or position in the market.

Example for customer perception: Previous experiences the customers have had with a similar IT Service or service provider and its effect on their business outcomes.

Reference values: the reference value of a service

Customers' perceptions of value are influenced by their expectations. Customers base their perception of value added by a service on **reference values.** These reference values may be vaguely defined or actual facts. Therefore, it's important for an IT Service Provider to understand what their customers' reference values are. This can be achieved through dialog with customer or research and analysis of the market.

Examples for reference values:

1. The baseline cost that a customer would incur if they provide the service internally instead of obtaining it from an external service provider.
2. The level of service provided by a competitor.

The economic value of a service:

The economic value of a service to the customer = [Customer's reference value+ Net difference in value the customer associates with the service]

The positive difference comes from the service utility and warranty and negative difference comes from losses suffered by the customer as a result of utilizing the service.

Example of economic value of a service: Increased profit margin as a result of utilization of the service.

The 3 guidelines for uncovering key business outcomes that add value to customers are,

1. **To look from the customer's perspective**.
   Service providers need to look from customers' perspective to understand a customers' perception. To understand a customers' perspective an organization needs to ask the following questions,

   - What is our business?
   - Who are our customers?
   - What is it that customers value?
   - Who depends on our services?
   - How do customers use our services?
   - Why are our services valuable to customers?

2. **To recognize that value can be provided at different levels.**
   It is important for an organization to understand that value can be added at different levels.

   A service provider can differentiate itself from an equipment vendor through added value, even though it uses the vendor's equipments as assets.

3. **To understand the positive effect that customers perceive a service to have on their business outcomes.**
   To a service provider's customers, the outcomes that matters depends on the positive effect that customers perceive a service to have on their business outcomes and activities. The extent of this value depends on the customer's perception of fitness for use and fitness for purpose of a service.

One of the ways the service provider's can add value to a service is through the use of assets. There are 2 main types of assets,

1. **Resources**
2. **Capabilities**

Resources:

Resources are direct inputs into production or service delivery. There are 4 exclusive examples of resources

1. **Information:** data such as information about customers, contracts, services, events. Examples of information assets include records, messages and graphs.
2. **Infrastructure:** Infrastructure assets enable other assets to operate. Examples include servers, computers, storage systems, network devices, telecommunications equipments and monitoring systems.
3. **Applications:** Application assets are used to automate, codify, enable, enhance or mimic the properties, functions, and activities of other types of assets. They typically consume, produce and maintain other types of knowledge or information assets. Examples include accounting software, voicemail, encryption devices, inventory tracking, electronic design automation and bar code scanners.
4. **Financial Capital:** Financial Capital assets are required to support ownership and utilization of all other resources and capabilities. Example includes cash, cash equivalents, marketable securities and receivables that can be converted into cash.

Capabilities:

Capabilities are components that enable an organization to use and transform resources in way that adds value to services. Capabilities are often experience – driven, knowledge – intensive and information – based. They lie within an organization's people, processes and technologies. There are 4 exclusive examples of important capabilities, they are

1. **Organization:** The organization capability includes coordination of various other assets that carryout organizational activities. Examples include networks, storage systems, point-of-sale terminals, databases and hardware stores.
2. **Process:** The process capability comprises methods, procedures and routines for controlling an organization's activities. Process assets are often embedded in a software application and are very dynamic. Example include order fulfillment, account receivables, incident management and testing,
3. **Knowledge:** Knowledge capability is an accumulation of awareness, experience, information and intellectual property. It can be acquired through experience, observation and training. Examples include policies, plans, designs, architectures, configurations and process definitions.
4. **Management:** Management capability determines an organization's ability to coordinate all other assets. Examples include leadership, administration, performance measures and incentives.

People within an organization are both resource and capability. Capabilities are harder to acquire than resources and are typically developed over time. It is important for an organization to develop distinctive capabilities which can be enhanced through experiences gained from variety of customers, market spaces, contacts and services.

Automate Service Processes:

Service automation can have a direct impact on performance of service assets. These assets include the resources and capabilities that an organization uses to provide services and add value for customers.

When implemented correctly service automation can

- Improve quality of delivered service.
- Reduce costs.
- Reduce risks
- Resolve production trade-offs.

Examples of areas where service management can benefit from service automation

- Design and modeling
- Service cataloging
- Pattern recognition and analysis
- Classification, prioritization and routing
- Detection and monitoring
- Optimization

Advantages of service automation:

- **Adjusting capacity to demand:**
  Automated services can easily adjust capacity to demand, for example by responding to variation in demand volumes.
- **Handling capacity with fewer restrictions:**
  Automated resources can handle capacity with fewer restrictions on time of access – they can easily respond to demands and continue providing services across time zones and after hours.
- **providing a basis for measuring and improving service processes:**
  Automated resources that require limited and consistent human inputs provide a good basis for measuring and improving service processes. They can help determine how varying levels of knowledge and skills impact service quality.
- **enabling complex processes:**
  Service automation enables complex processes such as scheduling, routing and allocation of resources through the use of computing power. These processes may be beyond human capability or may be much less time consuming and more accurate as a result of automation.
- **providing a means for capturing knowledge:**
  Service automation provides a means for capturing knowledge required for monitoring, analyzing and improving a service process.

If service automation is implemented incorrectly then it can create more problem than it solves, so it's important for an organization to follow some basic guidelines to ensure service automation is implemented correctly. To ensure service automation is implemented correctly, an organization needs to

1. simplify service processes before automation
2. clarify the needed flow of activities
3. minimize users' contact with underlying processes
4. exercise caution when automating complex tasks and interactions

Service Strategy Processes:

Strategy management for IT Services:

Strategy management involves determining how to manage and maintain IT Services to optimize their value to your organization.

Objectives of Strategy Management:

- **ensure opportunities are recognized**
  Identify potentially beneficial opportunities through analysis of internal and external environments. Strategy plans can then be updated to capitalize on opportunities as they arise.

- **Identify and minimize constraints**
  Identify and minimize constraints that may prevent the achievement of business objectives or the delivery or management of IT Services.
- **Agree on the service provider's mission**
  Ensure that decision makers agree on the IT Service provider's vision and mission and these are regularly reviewed for continued relevance.
- **Define which services to deliver**
  A goal of Strategy Management is to define which IT Service to deliver – to which market spaces – in order to gain or maintain a competitive advantage.
- **Ensure all stakeholders are kept updated**
  Strategy Management should ensure that appropriate stakeholders are kept informed of information on relevant IT Service activities that they may require.
- **Translate strategic plans**
  Strategy Management should translate strategic plans into tactical and operational plans that an organization can put into action.
- **Manage strategy changes**
  Manage changes to IT strategies and related documents, as and when necessary, based on changes in a service provider's internal and external environments.

Executives set out plan and prioritize the objectives of IT Strategy Management. Planning Manager/Strategy Manager generally conducts the necessary assessments; drafts strategy documents, manages execution and reports the results of strategy management to either senior management or a board of directors.

Service Strategy focuses on what IT services and organization will offer and how they'll be delivered.

The main aim of a strategy is to define an organization's objective and how it will go about meeting these objectives. It should also be possible to determine when exactly these objectives have been met.

Advantages of Strategic management:

- **Ensure resources, capabilities and investments are matched to objectives**.
- **Ensures stakeholders are represented:**
  Strategy Management ensures that Stakeholders are represented and they agree on the organization's objectives and the way resources, capabilities and investments are prioritized.
- **Ensures service providers offer the appropriate set of services:**
- **Results in cost savings:** (as investments and expenditures matched to business objectives)
- **Leads to increased investments in valuable projects:** (cost savings help to invest more in projects that support its key objectives)
- **Helps organization to shift investment priorities when necessary**.

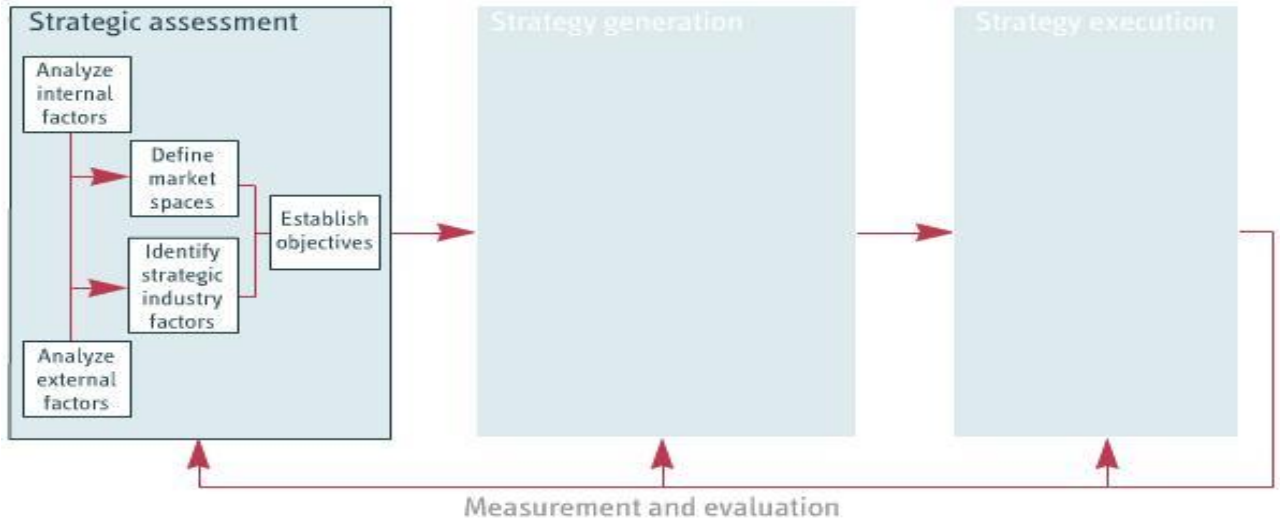
Strategy Management process for IT Services:

The Strategy Management for IT Services consists of 4 stages;

1. Strategic assessment
2. Strategy generation
3. Strategy execution
4. Measurement and evaluation

Strategic Assessment

The aim of strategic assessment is to produce a strategic objective that defines a result that an IT Service Provider wants to achieve. The strategic assessment stage include 5 activities

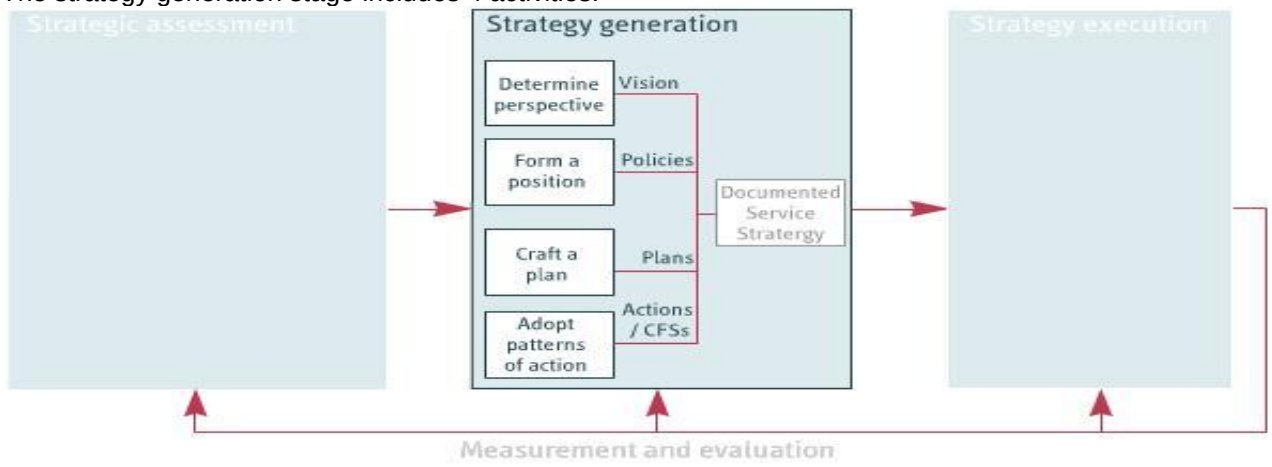


1. **Analyze internal factors: (strengths and weaknesses)**
   Analyze current environment and practices to identify organization's strengths and weaknesses. This information can be used in defining a strategy that leverages the organization's strengths and overcome its weaknesses.
2. **Analyze External factors: (opportunities and threats)**
   Analyze external environment to identify potential opportunities that can be exploited and identify threats that needed to be addressed.
3. **Define market spaces: (current markets and potential new markets)**
   Document all current market spaces and any new potential market spaces. This helps in deciding whether any changes are needed to retain a particular market space.
4. **Identify strategic industry factors: (customer need, competitors, technologies, etc)**
   IT Service providers needs to identify strategic industry factors that are influenced by customer needs, business trends, competition, regulatory environment, suppliers, standards, industry best practices and technologies.
5. **Establish objectives: (define targets for strategy)**
   It is necessary to establish objectives to define the targeted results for a specific strategy. Meaningful objectives are based on objectives customer wants to achieve. Objectives facilitate consistent decision making, minimize later conflicts, define priorities and serve as a standard.

<u>Strategy Generation:</u>

The output of strategy generation stage is a documented service strategy that specifies how the service provider will achieve the specified strategic objective.

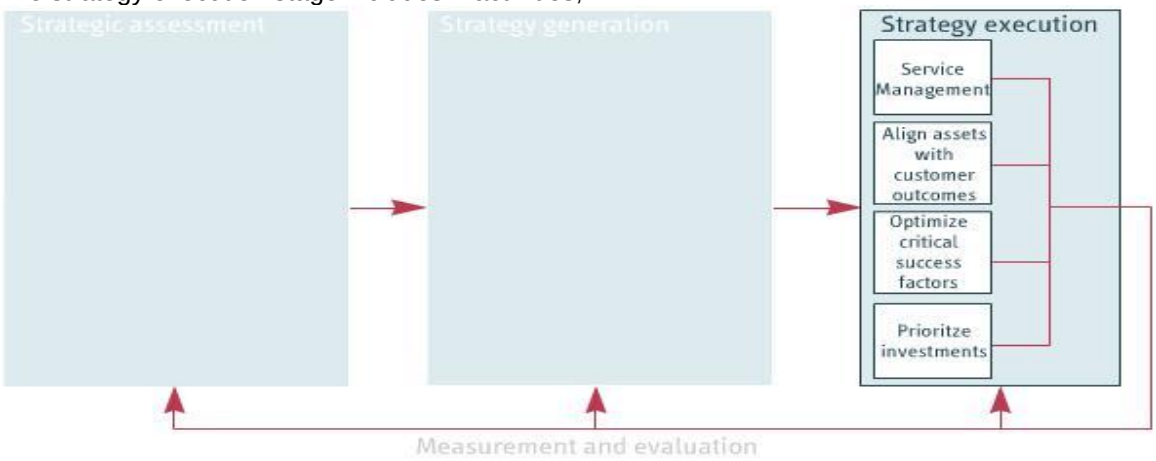
The strategy generation stage includes 4 activities:



1. **Determine perspective: (vision and mission statements)**
   Determining perspective involves the IT Service provider specifying it's overall direction, values, beliefs and purpose. It also defines how it intends to achieve these. The most common forms of perspective statements are vision and mission statement.
2. **Form a position: (differentiate from other providers)**
   The IT Service provider needs to define how it will differentiate itself from similar service providers by forming a position. An IT Service provider's position is often expressed through policies about what services will be provided, to what level and to which customers.
3. **Craft a plan: (plan a course of action)**
   IT service provider needs to craft a plan that defines a course of action required to achieve its objectives, vision and position. Plans often focus on financial budgets, services portfolio, new service developments, investments in service assets and improvements.
4. **Adopt patterns of action: (adopt best practices)**
   Adopt the patterns that are perceived to be an effective means of achieving the strategic objectives.

Strategy Execution:

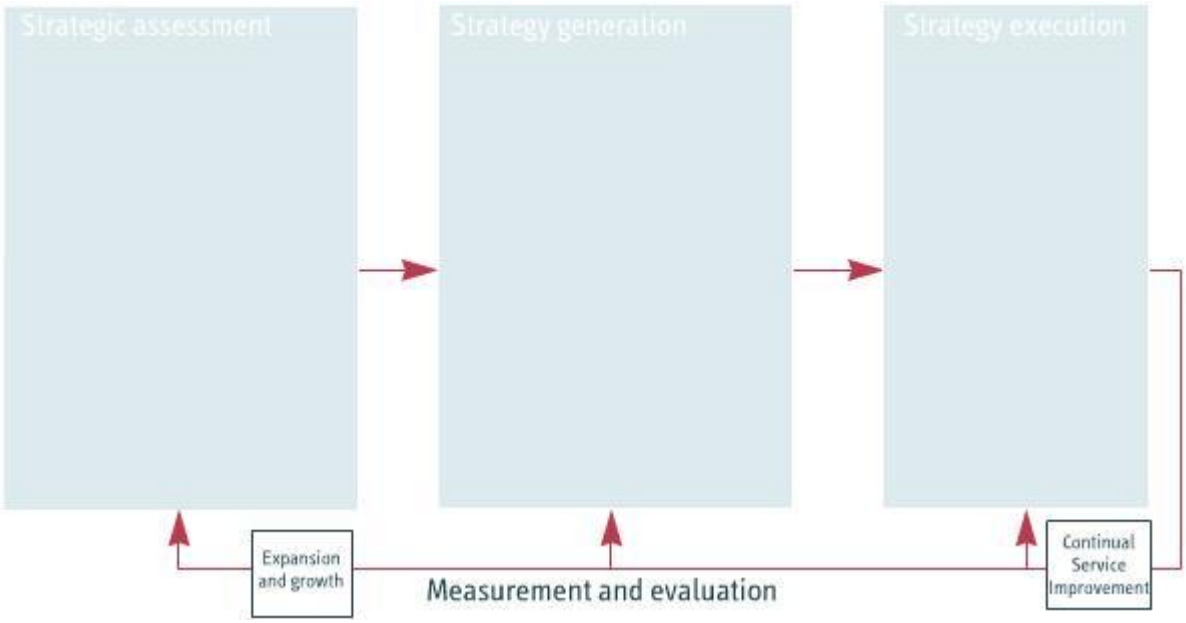
During this stage the IT Service Provider develops a tactical plan that defines what approaches and methods will be used to achieve the documented service strategy.
The strategy execution stage includes 4 activities,



1. **Service management: (to manage services)**
   IT Service provider defines an action plan that describes how it can best manage the IT Services that it provides.
2. **Aligning assets with customer outcomes: (deploy the assets for service delivery)**
   Ensure IT Service assets are coordinated, controlled and deployed so that the IT Service provider can provide the appropriate IT Services at the agreed levels.
3. **Optimize critical success factors (CSFs): (improve skills, tools, apps, etc for better Service Delivery)**
   Involves comparing IT Services, processes, skills and tools with identified strategic industry factors – or CSFs – to identify and address any potential shortcomings.
4. **Prioritize investments: (invest in services giving better ROI)**
   Involves analyzing each proposed new service or change to existing service to determine the level of investment it requires and the proposed return on investment (ROI).

Measurement and evaluation:

The final stage of strategy management process is measurement and evaluation. Includes 2 activities,



1. **Expansion and growth:**
   Successful expansion and growth involves leveraging existing service assets and customer portfolios to drive new growth and profitability in new market spaces.
2. **Continual service improvement:**
   CSI involves identifying areas that are performing below expectations and providing feedbacks to strategy generation and execution stages of the process so that these areas can be improved.

The strategy management may be conducted as part of annual planning cycle or it may be triggered by new business opportunities, changes to internal and external environment, or company merger or acquisition.

Inputs to strategy management include,

- Existing plans
- Research
- Vendor strategies and road maps
- Customer interviews and strategic plans
- The service portfolio
- Service reporting
- Audit reports

Outputs of strategy management are

- Strategic plans and service strategy
- Tactical plans for strategy execution
- Strategy review schedules
- Mission and vision statements
- Service design, operation and improvement policies
- Strategic requirements for new services

Strategy management interfaces include

- **The service portfolio**
  Service portfolio provides strategy management with information about the services currently in the service catalog and what strategic objectives they have been designed to meet.
- **Financial Management**
  Financial Management provides strategy management with financial information to enable strategy management to prioritize actions and plans.

- **Service design**
  Service design processes provide feedback to strategy management that enables measurement and evaluation of IT services being designed.
- **Service transition**
  Service transition identifies variation and provides feedback to strategy management so that the strategy can be reviewed.
- **Knowledge management**
  Knowledge management structures information so that it can be used to make strategic decisions.
- **Daily operations**
  Strategy management impacts daily operations in terms of execution of strategic priorities and adherence with strategy. Operations tools and processes must be aligned to strategic objectives and business outcomes.
- **Continual service improvement**
  Involves evaluating whether the strategy has been executed effectively and whether its meeting objectives. Any deviations are reported to those responsible for strategy management who can then improve the process or adjust strategy as required.

CSFs (Critical Success Factors) are the factors that must be in place if strategy management is to be successful. KPIs (Key performance indicators) are metrics used to evaluate CSFs.

CSFs (Critical Success Factors) for Strategy Management process include the ability to

- **Access information**
  KPI is accuracy of forecasts and findings from external research
- **Identify and overcome constraints**
  KPIs measuring the ability to manage constraints include the number of corrective actions taken to remove or reduce constraints and the results of those actions in terms of achieving
- **Clearly understand competitive positioning**
  KPI for understanding competitive positioning is whether each service in the service portfolio has a statement defining the business outcomes it's designed to meet and is measured in terms of these outcomes.
- **Produce, store, maintain and communicate strategy planning documents**
  Whether relevant stakeholders have access to appropriate and current planning documents is a KPI relating to the management of strategy planning documents.
- **Translate strategic plans into actionable plans**
  A KPI measuring the ability to translate strategic plans into actionable tactical and operational plans is whether the organization's unit leader can identify the plans for that unit and provide an overview of the relevant plan's contents.
- **Adjust strategies and related documents**
  The number of changes made to the strategy documents corresponding to the number of identified changes in the internal and external environments is an example of KPI measuring responsiveness to change.

Challenges to Strategy Management:

- Possibility of conducting the strategy management for IT Services at the wrong level in the organization.
- Lack of accurate information about external environments.
- Lack of support from stakeholders.
- Lack of appropriate tools or of knowledge about how to use them.
- Lack of appropriate document control mechanisms and procedures
- Failure to match operational targets to strategic objectives.

Risks involved in strategy management:
The success of strategy management may be compromised if

- A flawed governance model is used
- Short – term priorities override strategic directives
- Strategic decisions are made based on incomplete, incorrect or misleading information
- Wrong strategy is selected
- The metrics used by various business units don't align with those for the adopted strategy

Service Portfolio Management:

The service portfolio is the complete set of services managed by a service provider. It includes 3 categories

1. Service pipeline (proposed or in development)
2. Service catalog (live or available for deployment)
3. Retired services

The service portfolio describes the services in terms of their business values, defining the business needs and the services provider's response to those needs. A service portfolio helps answering the following strategic questions,

- Why should a customer buy services?
- Why should a customer buy services from us?
- What pricing or chargeback model should apply?
- What are our strengths, weaknesses, priorities and risks?
- How can our resources and capabilities be best allocated?

Service portfolio management is the process of managing a service portfolio including determining which IT services to include and how those services will be tracked throughout their lifecycles.

Objectives of service portfolio management:

- Ensure all services as well as the business needs they meet are clearly defined and linked to strategic objectives.
- Control which services are offered, under what conditions and at what level of investment.
- Analyze which services are no longer viable and when they should be retired.

Service Portfolio Management consists of 4 main phases of activity.

1. Define
2. Analyze
3. Approve
4. Charter

1. **Define:**

   The define phase involves ensuring that each proposed and existing service is clearly defined and has a documented business case. It also involves validating information about the business outcomes that IT Services can provide and the required investment in those services.

   During define phase you need to define new and existing IT services together with the

   - Targeted business outcomes for the services
   - Opportunities that the services exploit
   - Relevant warranty requirements and
   - Anticipated investment requirements for the services

What you can do in define phase?

- Ensure that all IT services are listed in a portfolio and create a business case for these services.
- Identify and categorize IT services.
- Identify new strategies or strategy adjustments and then identify stakeholders including all those who have an interest in the strategies or strategy changes.
- Establish and use a standard method for recording customer requests for new business. It may also highlight the potential for new IT Strategies.
- Identify ways to improve new and existing IT services. Improvement plans may relate to people, processes and tools that support the services.

2. **Analyze:**

The analyze phase involves evaluating the IT services in the service portfolio to determine whether they provide value and how supply and demand can be prioritized and balanced.

The concern of analyze phase is linking each service to a strategy to facilitate value proposition.

The analyze phase seeks to frame how the plan, perspective, position and patterns become actual service.

During analyze phase you should ask the following questions.

- Which services are most appropriate for achieving goals?
- What resources and capabilities are needed?
- What resources and capabilities are available?
- What services should be prioritized?

In the analyze phase you also align and prioritize IT services to balance supply and demand.

3. **Approve:**

The approve phase involves authorizing the level of investment required to deliver the targeted levels of service.

The objective of approve phase is to determine the feasibility of each proposed new IT service. If it's established that a service is feasible and will add value to the organization, it can be authorized and required resources can be assigned.

In the approve phase, the change proposal is

1) **submitted for investigation** (change proposal should include a description of the new service, a business case for it, information about relevant risks, alternatives and issues and a roster for implementation)
2) **assessed** (for feasibility, value added by new service)
3) **authorized or rejected** (If a change proposal is authorized by change management, service portfolio management will use the feedback to draft a service charter. If rejected, appropriate stakeholders should be informed and service portfolio should be updated)

4. **Charter:**

- A charter is a document that authorizes an IT service project and states its scope, terms and references. All services must be formally chartered and stakeholders must be updated about the investment decisions and resource allocations.
- In the charter phase, you create a new service charter for each new service that's approved.
- A service charter ensures that all relevant stakeholders, including development, testing and deployment staff members have a common understanding of what will be built, by when and the budget of the project.
- The charter also officially authorizes the allocation of resources for the new IT Service.

- The charter is an input for the project management process and initiates the design phase for the service.

The triggers for service portfolio management include

- **A change in strategy**
- **A request from a customer**
- **An identified improvement opportunity**
- **Feedback from staff** (about deviation from specifications like cost or release time. Service portfolio management will be involved in estimating the impact of this and defining corrective action if needed)
- **Service level management (SLM) reviews** (may indicate that particular services aren't providing the expected outcomes or aren't being used in the intended way)
- **Unexpected costs** (will affect expected ROI, so SPM is initiated)

Service portfolio management interfaces with several other functions and processes:

- **Service catalog management** (SPM decides which service to place in Service Catalog)
- **Strategy management for IT services**
- **Financial management for IT services** (helps SPM in ROI calculations and cost tracking)
- **Demand management** (provides info about PBAs to help determine utilization and expected ROI for each service)
- **Business relationship management (BRM)** (provides business info and customer requirements)

Examples of KPIs for evaluating service portfolio:

- Whether there is documented statement specifying the initial investment in each service
- The ongoing ROI for each service, based on the investment in the service in relation to the business outcomes it's generating
- Surveys indicating customers' level of satisfaction with the value they are receiving from a service
- Whether the risks associated with each service and corresponding risk responses are documented in the service portfolio.

Potential challenges and risks for Service Portfolio Management:

- **Insufficient access to customer and user information**
- **Lack of formal project or change management**
  Without formal project management it can be difficult to track services through design and transition stages and it's possible that service weaknesses or failures won't be detected
  Without formal change management, changes to services may be haphazardly, with little consideration of real value or cost of the changes.
- **Absence of project or customer portfolios**
  Without project portfolio it will be difficult to assess the impact of new initiatives on new services or proposed changes to services.
  Similarly without customer agreement portfolio it will be difficult to identify the objectives, use and ROI of services.
- **Failures to consider customers' required business outcomes**
- **Rushed or uninformed decisions**
- **Lack of defined metrics for measuring value**
  It's very difficult to calculate ROI of a service that hasn't been designed around a clear value proposition. In cost cutting situations, service providers may find themselves being forced to eliminate IT services that appear to be valuable, but for which no tangible returns can be demonstrated.

Service Strategy Processes:

Demand Management:

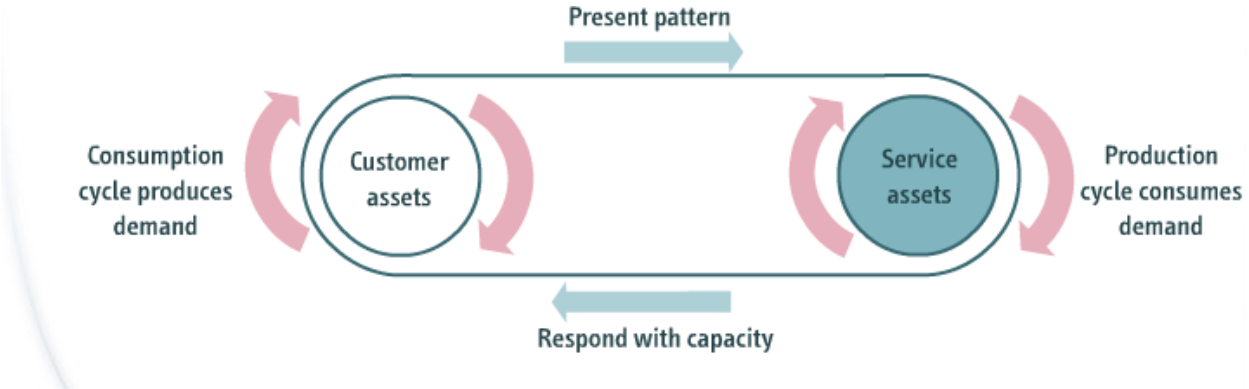
Demand Management involves interpreting and influencing customer demand for services, as well as providing capacity to meet those demands.

Challenges to Demand Management:

- **Idle capacity** (excess capacity which turns into idle capacity, doesn't generate returns or satisfy demands and is costly. For example, a help desk service offered to a customer at a per use cost)
  There are circumstances where a certain degree of **unused capacity** is required for service delivery and managing demand. The excess capacity is valuable because it enables a service provider to guarantee a higher level of service delivery. For example, a helpdesk service offered to a customer at a fixed cost.
  Unused capacity differs from idle capacity in that it serves a purpose associated with meeting demand.

- **Insufficient capacity** (affects service quality and hinders growth of a service)

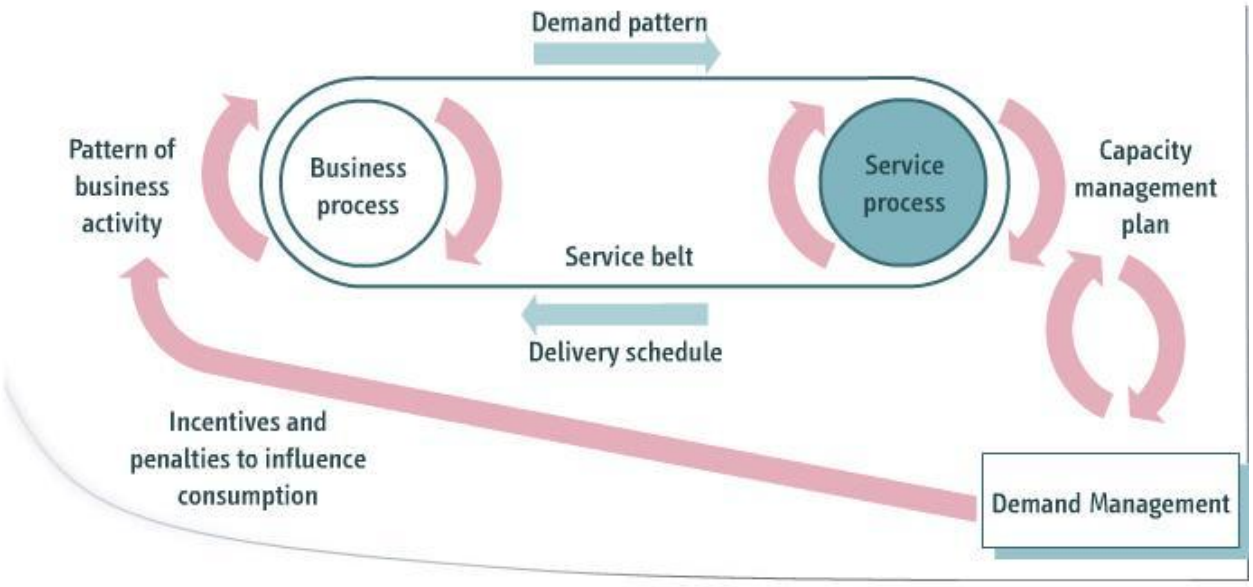
- **Synchronous production and consumption**
  Consumption of IT services produces demand and production of IT services consumes demand in a synchronized pattern. This makes predicting and providing for demand difficult.



  Demand is the factor that pulls capacity – demand does not exist merely because capacity does. Service production is therefore inextricably linked to service consumption, where consumption cycles stimulate production cycles.
  Demand Management activities aim to influence patterns of demand so that they are more predictable and service production can be more accurately aligned with demand. For example volume discounts, off-peak pricing and differentiated service levels are techniques used to influence patterns of demand.

- **Inability to manufacture services in advance**
  Services cannot be manufactured in advance and stockpiled in anticipation of demand. Demand and capacity are more closely linked in service systems due to the synchronous nature of production and consumption cycles.
  Although resources used in producing a service may be increased when demand increases and released when demand diminishes, it isn't possible to produce and stock service output before demand actually materializes.

Demand Management tries to influence patterns of demand so that they are more predictable and services can be provisioned accordingly.



How to overcome the challenges of managing demand?
At a strategic level, Demand Management involves analyzing **Pattern of Business Activity (PBA)** and **User Profile (UP)** to overcome the challenges of managing demand.

A PBA is a workload profile of one or more business activities. PBAs are used to help service providers understand and plan for different levels of business activity.

A UP is pattern of user demand for services. Each UP may include one or more predefined PBAs.

A customer's PBA is determined by its business processes and other assets, and on its interactions with its own customers, suppliers, partners and other stakeholders. For an IT service provider it is important to analyze the business of a customer to identify and codify its PBA.

In Demand Management, **a PBA links the business plan of a customer to the IT service provider's service management plan**. It enables the service provider to predict demand for services that support the customer's business activities. The PBA for a customer also provides a basis for Capacity Management – the process for ensuring that IT service providers have the capacity to deliver required service levels.

Codifying a customer's PBA involves determining attributes – such as frequency, location, volume and duration – associated with the customer's business processes and activities. It also involves identifying and categorizing customer requirements such as privacy, security and latency – or tolerance for delays.

Each PBA must significantly differ from other PBAs based on particular customer's business activities. A PBA must also be updated to reflect changes – for example when a customer organization alters its business processes, personnel, applications or infrastructure.
Once you have created PBAs, codifying them using criteria such as likeness and nearness allows for multidimensional analysis. This in turn enables IT service providers to develop robust and efficient service catalogs and to simplify and enhance service solutions.

Codifying Patterns of Business Activity (PBA)

A codifying table codifies the activity levels of a PBA as high (Hi) to low (Lo). Some business activities do not apply (N/a).

A codifying table (PBA No. 45F activities)

	Hi	3	2	1	Lo	N/a
Interact with customers remotely (frequency)			X			
Interact with customers onsite (frequency)				X		
Archive or handle customer information			X			
Process sensitive information (privacy)						X
Generate confidential information						X
Provide technical support (frequency)		X				
Seek technical assistance				X		
Network bandwidth requirements		X				
Data storage requirements (volume)		X				
Tolerance for delay in service response			X			
Seasonal variations in activity				X		
Print documents and images			X			
Mailing of documents using third-party systems			X			
Process transactions with wireless mobile device				X		
E-mail using wireless device			X			
Access work systems during domestic travel				X		
Access work systems during international travel						

A UP defines the roles and responsibilities of people and the functions and the operations of applications and processes within related organizations.

Examples of user profiles matched with patterns of business activity (example)

User profile	Applicable pattern of business activity (PBA)	PBA code
Senior executive (UP1)	Moderate travel - domestic and overseas; highly sensitive information; zero latency on service requests; high need for technical assistance; need to be highly available to the business	45F 45A 35D
Highly mobile executive (UP2)	Extensive travel - domestic and overseas; sensitive information; low latency on service requests; moderate need for technical assistance; high customer contact; need to be highly available to customers	45A 35D 22A
Office-based staff (UP3)	Office-based administrative staff; low travel - domestic; medium latency on service requests; low need for technical assistance; full-featured desktop needs; moderate customer contact; high volume of paperwork; need to be highly productive during work hours	22A 14B 3A
Payment processing system (UP4)	Business system; high volume; transaction-based; high security needs; low latency on service requests; low seasonal variation; mailing of documents by postal service; automatic customer notification; under regulatory compliance; need for low unit costs; need to be highly secure and transparent (audit control)	12F
Customer assistance process (UP5)	Business process; moderate volume; transaction-based; moderate security needs; very low latency on service requests; medium seasonal variation; mailing of replacement parts by express; automatic customer notification; need to be highly responsive to customers	24G 10G

Matching patterns between PBAs and UPs enables a systematic approach to understanding and managing customer demand. This leads to improved value for customers and service providers alike by helping eliminate waste and poor performance.

Types of services that organization provides includes,

- **Core services**
  Core services provide the basic outcomes desired by the customer and are the basis of the value proposition for the customer. They facilitate customer satisfaction and continued use of the IT service provider.
  Example: a core service provided by a bank could be providing customers with access to their basic account information online. To satisfy bank customers, the process of access must be timely and efficient.

- **Supporting services**
  Supporting services enable or enhance a core service. They meet the minimum requirement for the operation of a service. They may also enable service providers to provide services that differ from those offered by competing organizations.
  Example: a bank could offer supporting services such as the ability for customers to make changes to their accounts online rather than having to visit a bank branch.

- **Enabling services**
  Enabling services are supporting services that enable customers to use core services effectively. Customers expect enabling services to be offered without any additional charge.
  Example: a bank may offer the enabling services of a helpdesk to guide customers in accessing and using online account information or making changes.

- **Enhancing services**
  Enhancing services are supporting services that differentiate core services from the services provided by other organizations. Often enhancing services become enabling or even core services in time, depending on the changes to the market space.
  Example: as part of its online account services, a bank could provide customers the ability to pay different bills with different companies through their online bank account.

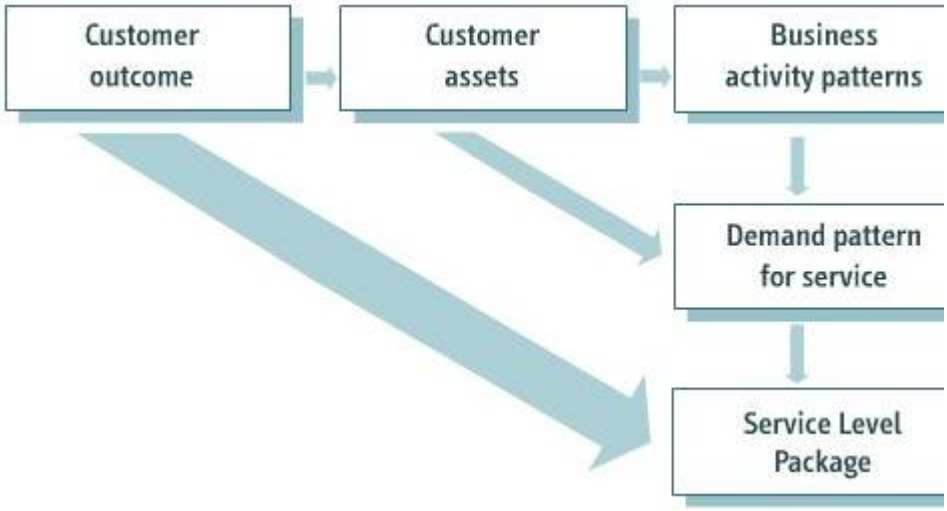
A service package is a detailed description of a set of related services that is available for delivery to customers. It is made up of one or more core services as well as supporting services. Bundling core services with supporting services is an essential aspect of a marketing strategy.

When making a decision to bundle services the following guidelines should be followed,

- **Conduct a thorough analysis of business environment** (to be aware of current business conditions, needs of customers they serve and alternative solutions that are available to those customers)
- **Take a long term view** (to sustain value of services for customers even if industry practices, norms, regulations and technologies change)
- **Consider implications for the design and operation of services (**decide whether to standardize core or supporting services in the package)

- **Devote sufficient attention to supporting services** (Customer satisfaction surveys indicate that supporting services are often a source of dissatisfaction, even when core services are being delivered)
- **Consider offering supporting services on their own (**a technical support or helpdesk service that usually form part of service packages can be offered as separate service)

A service package includes at least one **Service Level Package (SLP). An SLP is a defined level of utility and warranty for particular service package. Each SLP is designed to meet the needs of a particular PBA, although it may fulfill needs of more than one PBA. It helps to develop IT service packages according to the particular needs of a segment of users.**



SLPs are associated with a set of service levels, pricing policies and a Core Service Package (CSP).
A CSP is a detailed description of a core service that may be shared by two or more SLPs, providing a platform of utility for the SLPs.
CSPs offer the advantage of maintaining a tight control over core IT services. Each of multiple business units can develop SLPs to serve their own market spaces, but use centrally defined CSPs as the basis for providing core services within each service package.
SLPs combine with CSPs to build a Service Catalog with segmentation.
Service Catalogs are also made up of a collection of Lines of Service (LOS). These combine the most preferred utility and warranty for a segment of customers.
A LOS is a core service or supporting service that has multiple SLPs, each SLP designed to support a particular market segment.

Each LOS has one or more service offerings. In turn each service offering is made up of CSPs and SLPs.

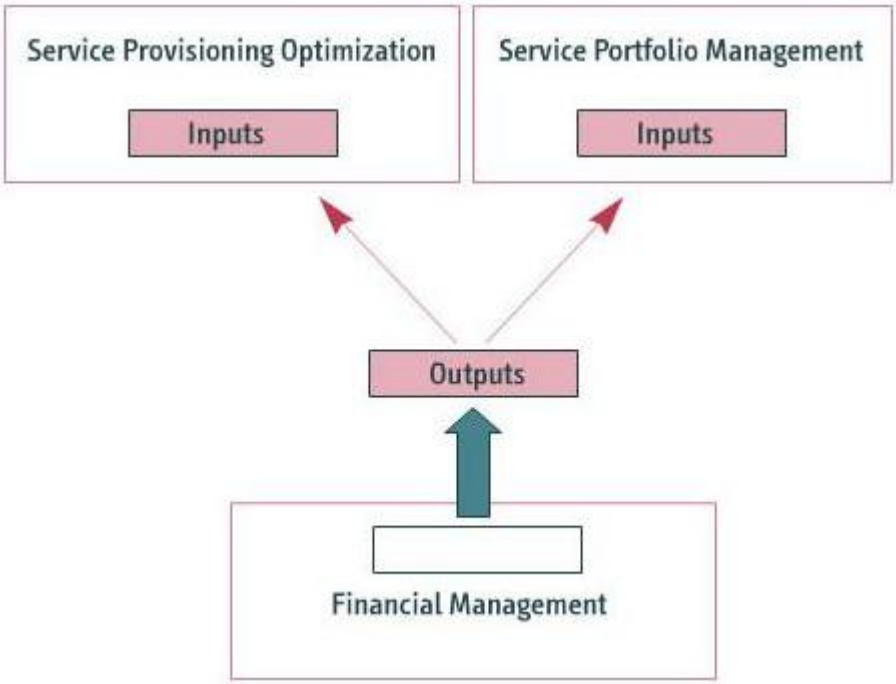
Financial Management for IT:
Financial Management involves managing an IT service provider's budgeting, accounting and charging requirements.
Benefits of Financial Management for IT:

- **Operational visibility, insight and superior decision making**
- **Use as a strategic tool** (to show financial visibility and accountability)
- **Ability to demonstrate the value of IT services** (value in financial terms, quantifies the value of assets underlying the provisioning of services)

Some of the concepts associated with Financial Management include

- **Service valuation** (quantifies a fiscal value for a service or service component)
- **Demand modeling** (Financial Management quantifies the fluctuations of funding that result from shifts in levels of demand)
- **Accounting** (to identify and keep track of service – oriented expenses or capital items)
- **Variable Cost of Dynamics (VCD)** (analyzes the many variables that affect service cost, how these elements may be affected by variability, and the related changes in value that result)

The outputs that result from Financial Management serve as inputs to other service strategy processes and tools, such as **Service Portfolio Management (SPM)** and **Service Provisioning Optimization (SPO)**



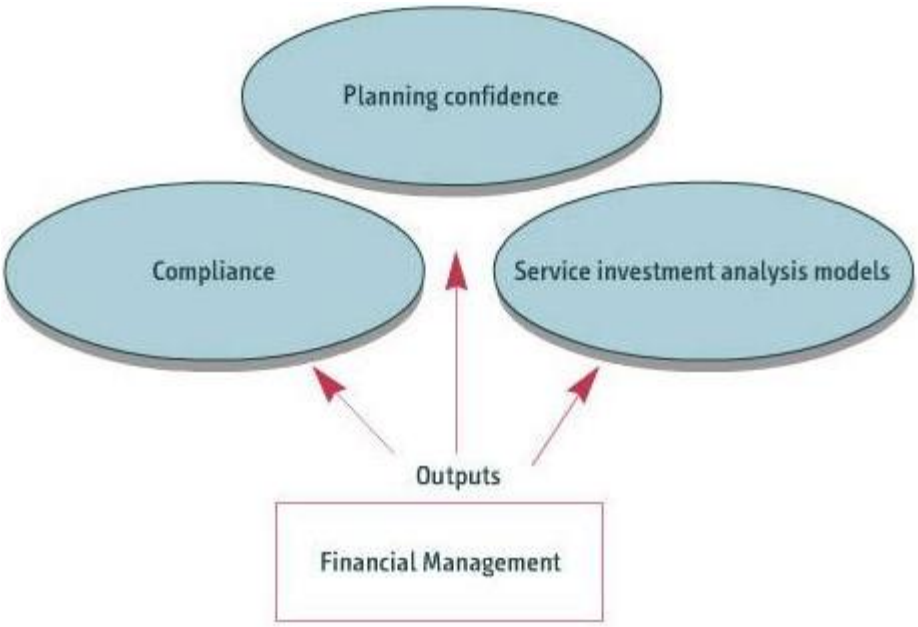
SPM uses **financial data** to understand the cost structures involved in the provision of a service, Organizations can benchmark the cost of a service against the cost offered by other service providers. This enables organizations to make decisions on whether it is cost effective to provide a service internally or whether it would be beneficial to outsource the service at a lower cost.

Financial Management provides inputs for **SPO**. SPO entails analyzing financial data relating to service components and delivery models to determine how to provide IT services at the best price and quality. Often, an IT service that has been proposed for removal from the Service Portfolio will be analyzed using SPO, to determine if it is worthwhile to retain the IT service.

Financial Management contains 3 outputs,

Planning Confidence:

Financial Management aims to ensure that there is sufficient funding available for the delivery and consumption of services. The financial data generated by Financial Management provides service providers with **planning confidence.** Planning facilitates the financial translation and qualification of forecasted future demand for services.



Compliance:
Financial Management procedures ensure the **compliance** of an organization with regulations and accepted business practices. Compliance ensures that proper and **consistent accounting practices are followed and documented**.

Service Investment Analysis Model: (used throughout an organization to assess the expected value of a service, derives an indication of value for the entire lifecycle of a service, based on the value received and the costs incurred during the service's lifecycle)

A business case is a decision support and planning tool that projects the likely consequences of a business action, such as a service management initiative. The consequences can have both qualitative and quantitative dimensions.

For example, a financial analysis provides quantitative information about likely financial consequences, and is often central to a business case. However, more qualitative consequences like improvements in an organization's market image may also be specified.
The structure of a business case for a service initiative includes five main components:

- an **introduction** that presents the business objectives addressed by the initiative
- a **methods and assumptions** section that defines the boundaries of the business action - such as time and cost limits - and assumptions on which the business case is based
- a **business impact** section that covers the projected financial and non-financial results of the initiative
- a **risks and contingencies** section, which allows for the probability that alternative results will emerge
- a **recommendations** section that proposes specific actions to be taken

All business cases include a detailed analysis of business impacts - the likely effects or benefits of business actions. Business impacts are in turn linked to business objectives.
A business objective is a goal that an organization sets for itself. It is a business-related reason for considering a service management initiative in the first place.

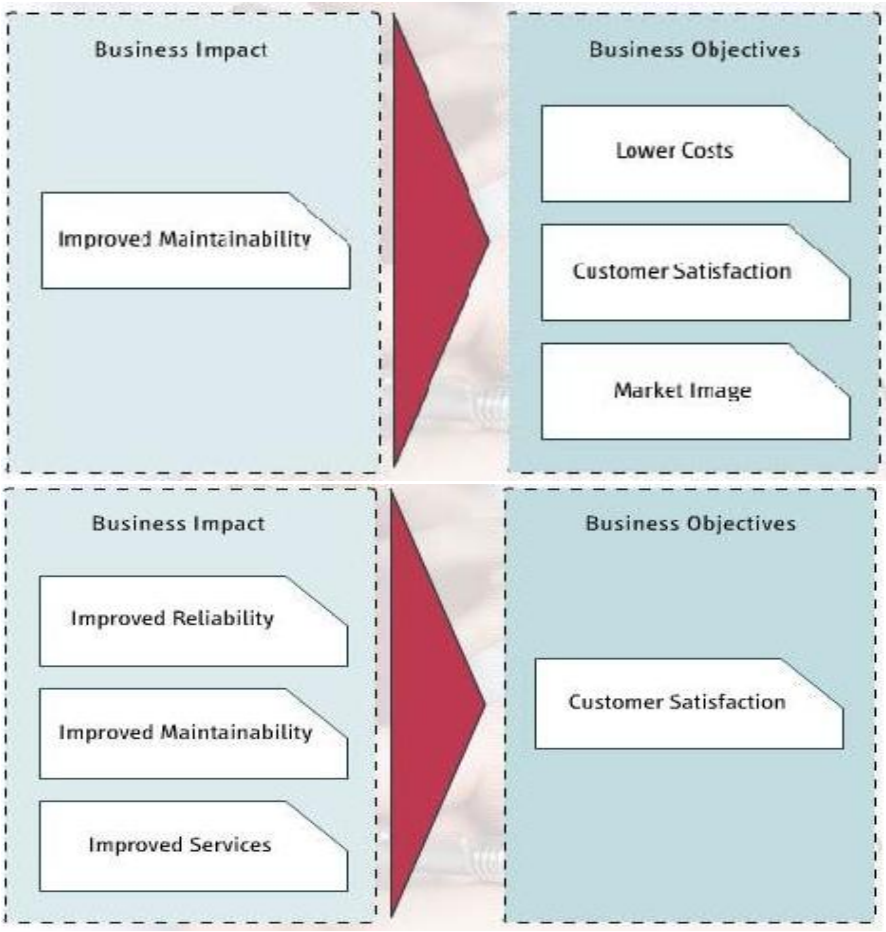
Objectives should be defined broadly in a business case. Commercial organizations' objectives are generally concerned with financial and organizational issues. The objectives of non-profit organizations usually focus on the people or membership served, as well as on financial and organizational issues.

Business Objectives usually fall into one of the 4 categories:

- **Operational Objectives** (with the day-to-day or short-term planning or delivery of a business process, an example is to increase productivity by a specified percentage)
- **Financial Objectives** (relate to improving profits, an example is to increase revenues by a specified margin)
- **Strategic Objectives** (deal with long-term planning to achieve the overall vision of an organization, an example improve professionalism of organization)
- **Industry objectives** (better branding and positioning of an organization in the marketplace, an example is to increase market share)

Ultimately a business impact won't have value for an organization unless it is linked to a business objective. However, business impacts and business objectives do not always have a one-to-one relationship.

A single business impact can affect multiple business objectives.
For example, the business impact of improved service maintainability may achieve the business objectives of lower costs, customer satisfaction, and improved market image.



Similarly, multiple business impacts may contribute to a single business objective.
For instance, the impacts of improved service reliability and maintainability and of improvements to service offerings may all contribute to the objective of improving customer satisfaction.

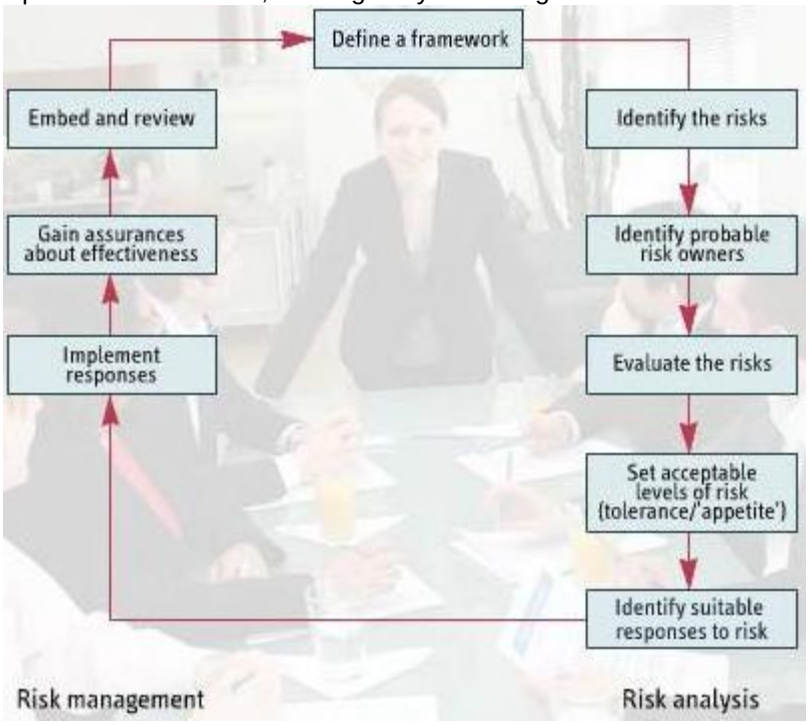
A business case argument usually rests on the basis of a cost analysis, although this is not the only aspect to consider when dealing with a service management initiative. The business case should focus on both financial and non-financial impacts, and it should link these impacts clearly to business objectives.

Risk is defined as uncertainty of outcome. It can take the form of positive opportunities or negative threats. **Risk Management** involves the identification and control of exposure to risks that may have an impact on the achievement of an organization's business objectives.

The purpose of Risk Management is to ensure that the organization makes cost-effective use of a risk framework that has a series of well-defined steps. The aim is to support better decision making through a good understanding of risks and their likely impacts. Risk Management includes two distinct phases -**risk analysis and the management of risk**.

Risk analysis is concerned with gathering information about exposure to risks so that an organization can make informed decisions and manage the risks appropriately. It also involves identifying and determining the level of the risks, based on the assessed values of assets and the levels of threats posed to those assets.

After risks have been analyzed, effective **Risk Management** involves determining and implementing appropriate risk responses. It also involves monitoring the risks to ensure the chosen responses are effective, and regularly reviewing risks to track their status.



Risk management forms an important aspect of many other areas of management, including

- business continuity management

- security management
- program and project risk management, and
- operational service management

All organizations need to take risks to achieve their objectives. So the main aim of Risk Management isn't to eliminate risks, but to manage them effectively in order to improve performance.

Effective management of risk helps improve performance by

- increasing certainty and lessening surprises
- improving service delivery and so protecting against client dissatisfaction and loss of market share
- resulting in more effective management of change in response to customer or market needs, and political or cultural changes
- resulting in more efficient use of resources
- improving management at all levels due to better decision making
- reducing waste and fraud, and increasing value for money
- encouraging innovation through new technologies so that opportunities can be exploited
- managing contingent and maintenance activities for dealing with any threats once they actually occur

Risk Management must be carried out with the issues of health and safety, security, and business continuity in mind.
Health and safety policy and practice is concerned with ensuring that the workplace is a safe environment.
Security deals with protecting an organization's assets - for example, its computer equipment, data, and buildings.
Business continuity ensures that an organization can continue to function in the event of major disasters such as fires, floods, or loss of service.

One purpose of risk management is finding weaknesses in supplier management that could pose a threat to an organization.

When working with suppliers, Risk Management focuses on threats to

- Customer Satisfaction
- Brand image
- Market share
- Share price
- Profitability
- Regulatory impacts or penalties that are industry dependant.

The nature of the relationship with a supplier determines the level of risk to an organization. Risks from an external supplier are generally greater and more difficult to deal with than those associated with using an internal supplier. Any risks that come out of the relationship need to be identified and managed appropriately. Prior to commencing any contract, a risk assessment should be done. Risks should also be re-assessed and monitored when changes occur to business needs, the operating environment, or contract scope.

A risk assessment should generally identify

- relevant risks, including threats and opportunities
- the likely impact of each threat
- the total impact of the risks
- the probability of each threat occurring

- possible actions or controls for managing each threat based on its impact or cost, and
- the person responsible for each risk and for implementing the chosen response

Business Relationship Management: BRM:

The Business Relationship Management (BRM) process involves maintaining a positive relationship with customers. It identities customer needs and ensures that an IT service provider can meet these needs with an appropriate catalog of services. It should also account for any changes in customers' needs overtime.

BRM can help an IT service provider articulate the value of a service and communicate this to customers, in order to align customers' expectations with what's being offered. BRM can also involve verifying that a service provider can meet customers' expectations before it agrees to deliver a service.

In addition, BRM can help organizations meet objectives in relation to

- **IT service delivery** (In the area of delivery, BRM helps IT service providers and customers work together to ensure that services meet customer requirements and add value)
- **Responsiveness** (BRM can improve an organization's responsiveness to changes in customers' needs. It may identify a need to introduce new services or change existing ones)
- **problem management** (When problems arise in the service provider-customer relationship, BRM helps establish formal processes that customers can use to register complaints and for the escalation of issues)

In terms of scope, BRM focuses on understanding and communicating

- the business outcomes that customers want
- the services currently being offered to customers and how they're being used
- how services are currently offered, including who's responsible for the services, agreed levels of service quality, and any anticipated changes in the services
- technology trends that may affect services or customers' requirements
- levels of customer satisfaction and current processes for addressing causes of any dissatisfaction
- how to optimize services for the future, and
- how customers perceive the service provider

BRM depends on a number of other service management processes and functions, including Service Portfolio Management, Configuration Management, Capacity Management, and Service Level Management. These complementary processes focus on what services to provide and the extent to which existing services meet stated requirements -whereas BRM focuses on customer relationships.

BRM and Service Level Management, or SLM, differ in terms of

BRM	SLM
Purpose: To ensure that a service provider meets customers' needs, in terms of utility and warranty.	To negotiate SLAs - and warranty terms with customers, and to ensure that all service management processes, OLAs, and underpinning contracts are appropriate for the agreed service level targets.
Focus: It focuses on the overall relationship between a service provider and customers.	It focuses on establishing required service levels and ensuring that the service provider meets these.
Primary Measure: BRM's primary measure is customer satisfaction.	The success of SLM is primarily measured based on how well a service provider meets agreed levels of service.

BRM can benefit IT service providers by clarifying customers' business needs. It creates a forum for ongoing, structured communication with customers. This helps ensure that customers' business needs are met. Over the long term, it also promotes better alignment of services with customer needs. The communication involved in BRM ensures that the service provider understands a customer's business better - and that the customer understands the service provider's capabilities and services.

Other benefits of BRM are that it

- helps ensure customers' expectations are realistic
- puts a human face on the service provider
- enables quick resolution of disagreements about what should be delivered - without speculation or mistrust
- facilitates higher levels of trust that the service provider is going to deliver value in future
- encourages service providers and customers to work together as strategic partners, and
- provides a more accurate measure of the real value that a service provider is adding to customers' businesses

The role of the business relationship manager isn't quite the same as the BRM process.
The main work of business relationship managers relates to the BRM process, but their high-level roles give them broad involvement across different processes. For example, gathering customer requirements feeds into the processes of Service Portfolio Management and Demand Management. Also, initiating communication with customers assists in the Project Management process.

Each business relationship manager makes use of a **Customer Portfolio**, which is a database or structured document that records information about all of an IT service provider's customers. The Customer Portfolio enables the IT service provider to quantify its commitments, investments, and risks relative to each customer.

It's useful to document information about customers in a Customer Portfolio for several reasons. For example, recording who has decision-making authority in the customer's organization can help protect against unauthorized personnel making demands on the service provider.

A Customer Portfolio also enables the service provider to document customer leads and follow up on these opportunities to expand its market share.

For each customer, a Customer Portfolio typically records specific information:

- the customer's name
- any authorized customer representatives
- the business relationship manager's name
- a description of the customer's business and required key business outcomes
- a list of services provided to the customer, along with any specific commitments for those services
- historic and projected revenue, along with margins - in the case of external service providers

For each customer, a Customer Portfolio may also include other details:

- a list of any meetings with the customer, with a list of the attendees and brief description of the meeting purpose and outcome
- a description of any reports that are produced, who receives those reports, and what action will be taken as a result of the reports
- a description of how and when the service provider's performance will be reviewed
- an overview of past performance, including any major issues or events for the customer, and how these were handled
- an outline of planned future IT services for the customer

- a schedule of agreement or contract reviews

The business relationship manager also makes use of a **Customer Agreement Portfolio** - which is a database or structured document used to manage service contracts, or agreements, with customers. The Customer Agreement Portfolio should list the contract or agreement that relates to each IT service delivered to each customer.

A goal of BRM is to ensure the alignment of IT services to these agreements. BRM directly influences customer satisfaction. It also involves measuring satisfaction levels, and comparing service provider performance with both customer satisfaction targets and previous scores.

According to the ITIL® Service Strategy volume, BRM promotes customer satisfaction by ensuring that the IT service provider understands the customer's objectives and overall requirements.

Information about customers is documented in a **Customer Catalogue**. BRM ensures that this information is appropriately linked to all potential services and agreements in the Service and Customer Agreement portfolios.

As agreement is reached about the type and level of service required, BRM initiates a Service Portfolio Management evaluation of whether that need will be met by a service currently in the Service Catalogue or pipeline.

At all stages in the service pipeline, through development and operation, BRM represents the customer's perspective and requirements. BRM also ensures that the customer is aware of the service provider's constraints and requirements.
The BRM process could be triggered by several incidents, including

- a new strategic Initiative
- initiation of a new service or a change to an existing service
- identification of a new opportunity
- chartering of a service by service portfolio managers
- customer requests, suggestions, or complaints
- scheduling of a customer meeting or of a customer satisfaction survey

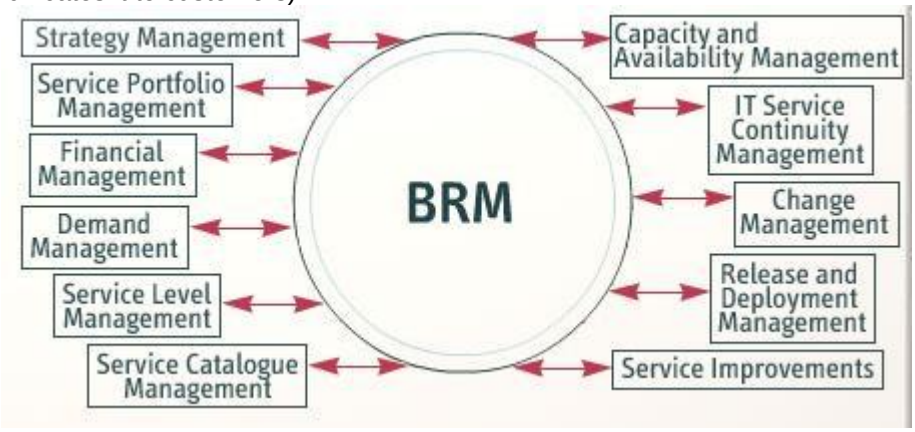
Inputs for BRM include all forms of feedback from customers, the IT service provider's strategy, the customer's strategy, and, when possible, the provider's IT Service Portfolio. They also include the Project Portfolio, SLAs, Requests For Change - or RFCs, patterns of business activity, and User Profiles defined by Demand Management that need to be validated through BRM.
The outputs of BRM include stakeholder definitions, defined business outcomes, payment agreements, the Customer Portfolio, service strategy, design, and transition requirements, customer satisfaction surveys, and the published results of these surveys. They also include schedules of customer activity in various Service Management process activities, a schedule of training and awareness events, and reports on customer perception of service performance.

BRM interfaces with many other management areas, including

- **Strategy Management** (involves working closely with BRM to identify market opportunities)
- **Service Portfolio Management** (SPM helps BRM with info about services available, BRM feeds into SPM helping identify suitable services based on customer requirements)
- **Financial Management** (BRM gives info about financial objectives of customers, also tells what price each customer is prepared to accept)
- **Demand Management** (BRM helps with PBAs and UP patterns, change in demands)
- **Service Level Management** (BRM provides info about customers' service requirements to SLM and ensures that SLAs are kept updated in the Customer Agreement Portfolio)
- **Service Catalogue Management** (provides BRM info about services moved to catalog from pipeline)

BRM also interfaces with

- **Capacity and Availability Management** (relies on information BRM provides about customers' IT service requirements)
- **IT Service Continuity Management** (BRM helps ensure that counter-measures, recovery plans, and tests take customers' real requirements into account)
- **Change Management** (BRM identify changes that will improve an IT service provider's ability to meet customers' needs, involves customer in Change Management process)
- **Release and Deployment Management** (BRM ensures the appropriate level of customer involvement in Release and Deployment Management and service validation and testing)
- **Service Improvements** (BRM identifies improvements that will meet customer needs and communicates it to customers)



Many Critical Success Factors, or CSFs, must be in place for BRM to function optimally. Each of these CSFs can be measured using Key Performance Indicators, or KPIs.
Commonly used CSFs for BRM relate to

- **requirements and outcomes**
  CSF: Ability to determine customers' key requirements and business outcomes**.**
  KPI: Whether all customers' requirements have been documented and signed off by the customers
- **customer satisfaction and follow-up**
  CSF: Customer satisfaction levels.
  KPI: How effectively the organization follows up on any indications of dissatisfaction.
- **environmental changes**
  CSF: Ability to identify environmental changes that may affect the types, levels, or utilization of services that customers require.
  KPI: Changes to services and strategy, resulting in improved customer satisfaction scores and increased revenue.

- **technology trends**
  CSF: Ability to identify technology trends that may affect customers' service requirements.
  KPI: Identification of opportunities leveraging new technologies. Each service opportunity's Return on Investment, or ROI, would be measured and a decision would be made to keep or retire the service, based on how effectively it met objectives.
- **service changes**
  CSF: Ability to establish and articulate business requirements for service changes, including changes to existing services or the introduction of new services.
  KPI: Whether a comprehensive set of requirements is defined for each service, and whether these have been signed off by both business and IT leadership at the Strategy, Design, and Transition stages
- **customer needs**
  CSF: Is BRM being able to measure that the service provider is meeting the business needs of the customer.
  KPI: One KPI is Service provider consistently being rated above a defined minimum level in a structured customer satisfaction survey. Another KPI would be service performance being matched to business outcomes, and reported to the customer. Deviations from expected achievements would be documented and - as appropriate - an improvement opportunity logged in the CSI Register, or a change initiated to the Service Portfolio.
- **Complaints**
  CSF: Having formalized complaints and escalation processes available to customers.
  KPI: Measurement and trending of the number of complaints and escalations - grouped by customer and time period

Challenges faced by BRM:
BRM also comes with several challenges.
The effectiveness of BRM can be compromised by an organization's history of poor service - which may make customers less willing to share requirements, feedback, and opportunities.

Also note that the role of the business relationship manager and the process of BRM shouldn’t be confused. Because business relationship managers often execute activities from other processes, it doesn’t mean those activities are parts of the BRM process.

Risks associated with BRM:
Risks associated with BRM are that it may

- **overlap with other processes**
  Because BRM is closely related to a number of other processes, confusion could arise about the boundaries between these processes. If these boundaries aren't clearly defined, the BRM process may overlap with other processes**.** This could result in unnecessary duplication of work, interference, or particular activities being neglected. For example, it's counter-productive for multiple processes to try to escalate the same incident in the same way.
- **fail to be properly integrated**
  Both customer-facing processes - such as BRM - and those focusing more on technology - such as Capacity Management - are critical for success, and need to be properly integrated. If there's a disconnect between these two areas and the processes aren't properly integrated**,** BRM is likely to be ineffective.

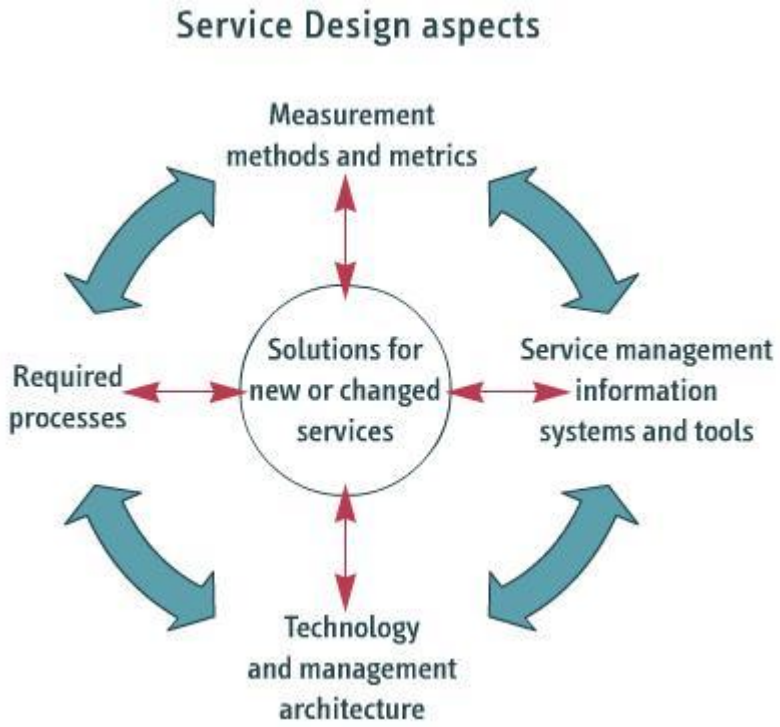
Service Design Fundamentals:
Introducing Service Design:
Aspects of Service Design:
Service Design involves identifying the requirements for new IT services or processes and defining the solutions that meet these requirements. The main purpose of Service Design is the design of new or changed services for introduction into the live environment.

There are five aspects of Service Design that need to be considered and that determine its scope. These include

- **solutions for new or changed services** (The new service should be aligned with company strategy and IT policies)
- **Service Management information systems and tools** (Existing Service Management information systems and tools should be capable of supporting the new service)
- **Technology and management architecture** (ensure that new service designed can function within existing technology and management architectures. Alternatively, these architectures may have to be revised)
- **Required processes** (A new service should be designed so that it can be supported and maintained by business processes. Those responsible must also have the authority and skills to operate the new service)
- **measurement methods and metrics** (existing measurement methods and metrics should be capable of producing the required performance information about the new service, or these systems and metrics must be revised)

Service Design requires that

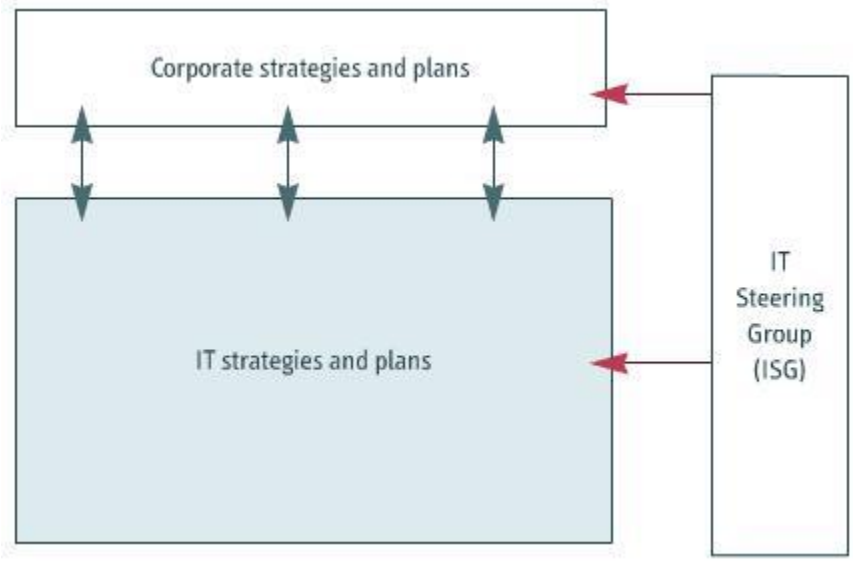
- Every time a new service solution is produced, it is checked against each one of the other Service Design aspects to ensure that it will integrate and interface with all of the services already in existence.



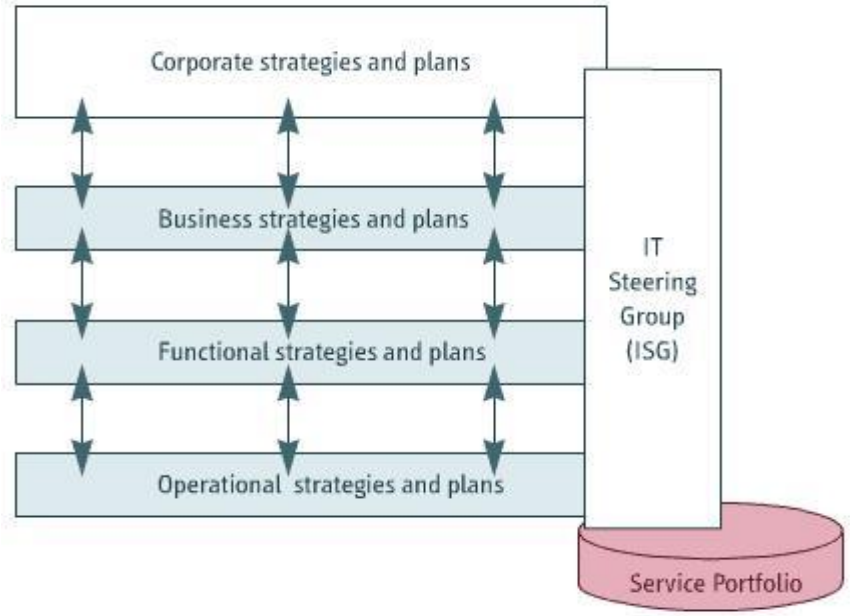
- results-driven approach be adopted for each of the Service Design aspects
- The desired business outcomes and planned results should be defined so that they meet customer expectations.

- Before implementing or changing any of the five aspects of Service Design, it's important to ensure that they align with business needs.
- Each new or changed IT service should be designed so that it integrates completely with the overall service and business strategy, and with the activities and processes that are internal and external to the business.

The IT Steering Group:
To ensure that Service Design aligns with business needs, many organizations set up a steering group - often referred to as the IT Strategy or Steering Group (ISG) - which facilitates cohesiveness between IT functionality and organizational plans and strategy.



The ISG reviews business and IT strategies, designs, plans, the Service Portfolio, IT architectures, and policies to ensure that IT functions and business needs are closely aligned.

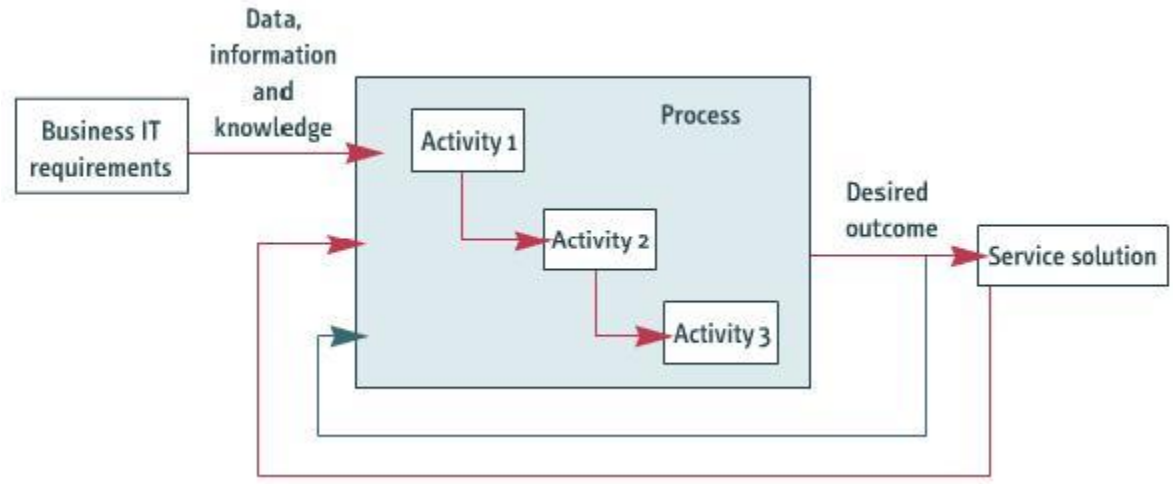


The ISG discusses all aspects of the business that involve IT services, as well as proposed or possible changes, at a strategic level.

The issues the ISG addresses may include

- **business and IT plans** (to identify any changes in either area that might trigger the need to create new or improve existing IT services)
- **demand planning** (to identify and plan for any changes in demand over the short and long term)
- **project authorization and prioritization** (Both business and IT Management should be satisfied with the projects that are authorized and with the prioritization of the projects)
- **Projects** (IT projects should be reviewed to ensure that their results contribute to the business and to verify that they are on schedule)
- **potential outsourcing** (The need for and the nature of potential outsourcing for provision of IT projects should be identified in relation to overall business needs)
- **business and IT strategy** (Major changes to business and IT strategy should be discussed to ensure alignment between the two)
- **business and IT service continuity** (Business and IT service continuity strategies must be aligned)
- **IT policies and standards** (IT policies and standard should be in place and should be aligned with overall corporate vision and objectives.)

Service Design should start with a new or changed set of business IT requirements and end with the development of a service solution designed to meet the needs of the business as a whole.



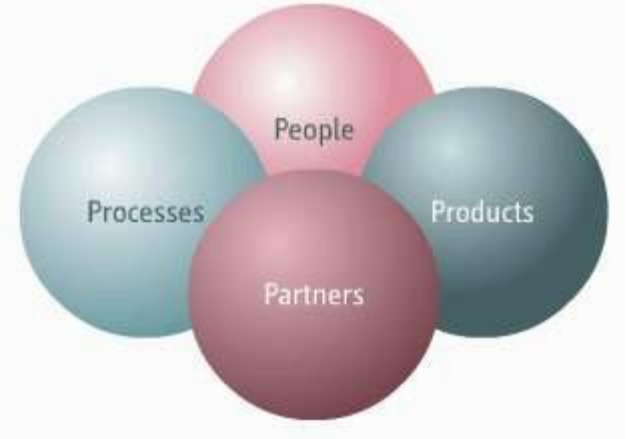
In case of a new or changed service, it is important to have properly performing design and planning processes if the desired outcome is a quality service.

With proper Service Design, it is possible to deliver quality services and to ensure that business requirements are being met.

Benefits of Service Design:
Good Service Design practice has the following benefits:

- **reduced risk** (when a service is well designed, it aligns with both IT and business strategies, meets customer requirements and reduces risk in the transition and operational stages)
- **project prioritization** (enables organizations to prioritize projects by establishing which projects, processes and services will have the greatest impact on, or benefit, to the organization)
- **alignment of requirements** (Good Service Design practice ensures that the new IT services align with overall business requirements)
- **improved quality, consistency, and scope for continuous improvement**

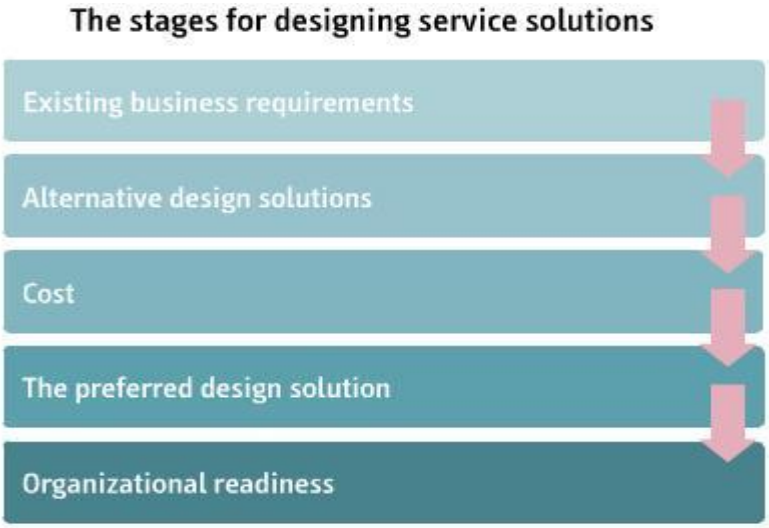
In some cases, a new service fails due to poor planning and management.
For all services, it helps to take the **"four P's"** into account.



1. **People** (managers and staff)
   The scope, tasks, activities, and skills of the people involved in the provision of IT services – managers and staff – are a critical factor in the success of these services.
2. **Products** (IT products, management support tools, technology used in Service Delivery)
   The success or failure of services depends in part on the IT products – including the management support tools and technology – used to manage the IT infrastructure and to deliver services and information to the right people, in the right place, at the right time.
3. **Partners** (Suppliers and Vendors)
   The capabilities and business interests of partners – including suppliers, manufacturers and vendors – help determine the likely success or failure of a service.
4. **Processes** (procedures, operations used to manage services)
   The processes and procedures used to manage IT services internally – to the organization and externally – to its customers – help determine the success or failure of services.

Aspect 1: Design Service Solution:
When designing service solutions, the following considerations should be included:

1. assessing existing business requirements
2. developing alternative design solutions
3. assessing the cost of design solutions
4. identifying the preferred design solution, and
5. assessing organizational readiness for implementing the preferred design solution

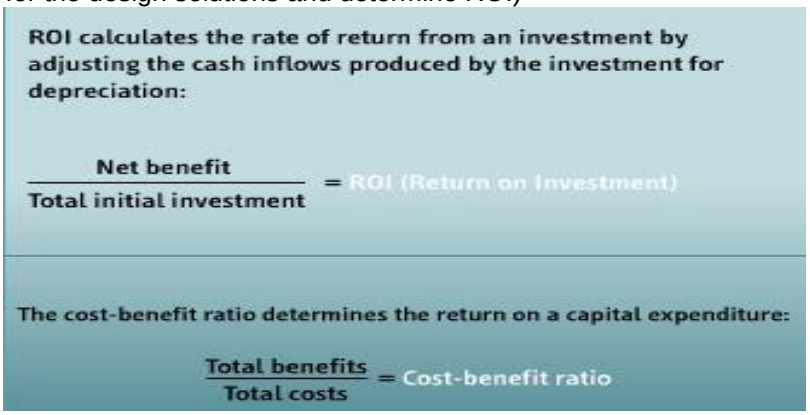


1. **assessing existing business requirements** (assess for new or changed requirements to ensure that service solutions are focused to fulfilling these requirements)

2. **developing alternative design solutions**
   Each proposed alternative must be developed with the following factors in mind:
   - the facilities and functionality required
   - the business processes supported
   - business cycles and seasonal variations
   - Service Level Requirements (SLR) and Service Level Targets
   - the timescales involved
   - the requirements for service testing

   When developing alternative design solutions, care should be taken to ensure that each proposed solution meet all the organization's Service Acceptance Criteria (SAC).

3. **assessing the cost of design solutions** (evaluate design in terms of its business benefits, potential advantages, disadvantages, and cost and reach on an agreement on budget and expenditure for the design solutions and determine ROI)



4. **identifying the preferred design solution** (Choose a design that aligns with existing corporate and IT strategies, and includes corporate and IT governance and security controls. All stakeholders must agree on the chosen design's planned outcomes and targets – its SLR)

5. **assessing organizational readiness for implementing the preferred design solution**
   Performing an organizational readiness assessment for an IT service involves assessing
   - **the commercial impact of the service on the organization** (include all costs -one-off projects as well as ongoing operational costs)
   - **associated risks and how they can be mitigated** (assess risks in terms of the operation, security, availability, and continuity of the service)
   - **the capability and maturity of the business** (ensure business has the capabilities to run the service and there is scope for maturity and growth of the new service)
   - **IT capability and maturity** (ensure that the business has the required IT capabilities and maturity to deploy the services)

     More specifically, the IT capability and maturity of the organization should be assessed in terms of
     - ✓ **the technology environment** (assess the impact of the new service on the existing technology environment - including IT infrastructure and services)
     - ✓ **IT organizational structure** (assess the impact of the new service on the IT organizational structure)
     - ✓ **IT processes** (assess existing IT processes to see if they can be applied to the new service)

- ✓ **staff capabilities** (determine whether IT resources have necessary skills to operate the new service and to identify training needs or the need to recruit more staff)
- ✓ **IT management processes** (determine whether existing IT management processes will support the new service)

  As well as assessing internal factors, the readiness assessment should consider supplier and supporting agreements that are necessary to maintain and deliver the service.

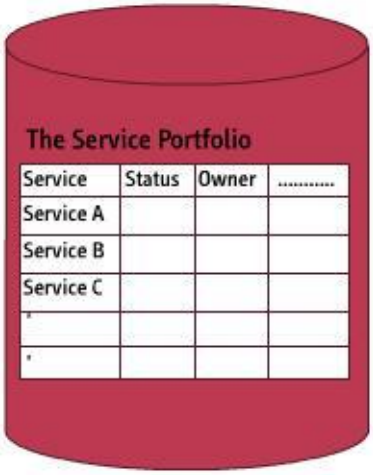
Finally a Service Design Package (SDP) should be assembled for the subsequent transition, operation and improvement of the new or changed service solution.

An SDP is a set of documents that defines all aspects of an IT service and its requirements through each stage of its lifecycle.

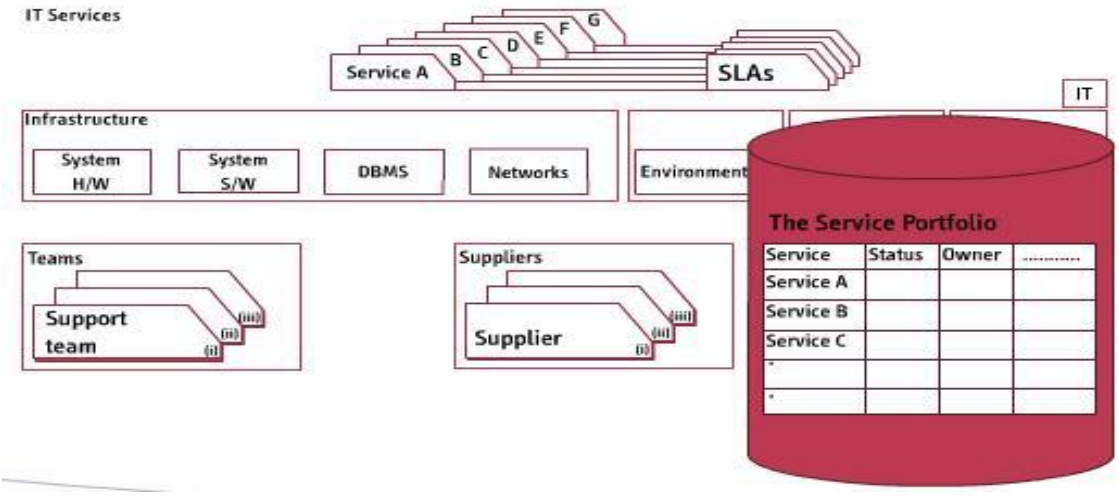
The contents of an SDP are divided into these categories;

- **Requirements** (includes agreed and documented business requirements, service contacts)
- **Service Design** (includes service functional requirements documented in SoR (Statement of requirements), planned outcomes, SLRs, service and operational management requirements, design, transition, implementation and operation plans)
- **Organizational Readiness Assessment** (report and plan)
- **Service Lifecycle Plan** (service program that details specific information for each stage of the lifecycle)
- **Service Transition Plan** (consists transition strategy, objectives, policies, risk assessment and plans)
- **Service Operational Acceptance Plan** (consists of interface and dependency management and planning, events, reports and service issues regarding the new service and final service acceptance)
- **Service Acceptance Criteria** (for progression through each stage of lifecycle)

Aspect 2: Service Portfolio:
Developing a Service Portfolio is part of the second aspect of Service Design - developing Service Management systems and tools.
The Service Portfolio acts as a central repository, with information relating to every existing or proposed service and its current status within the organization.



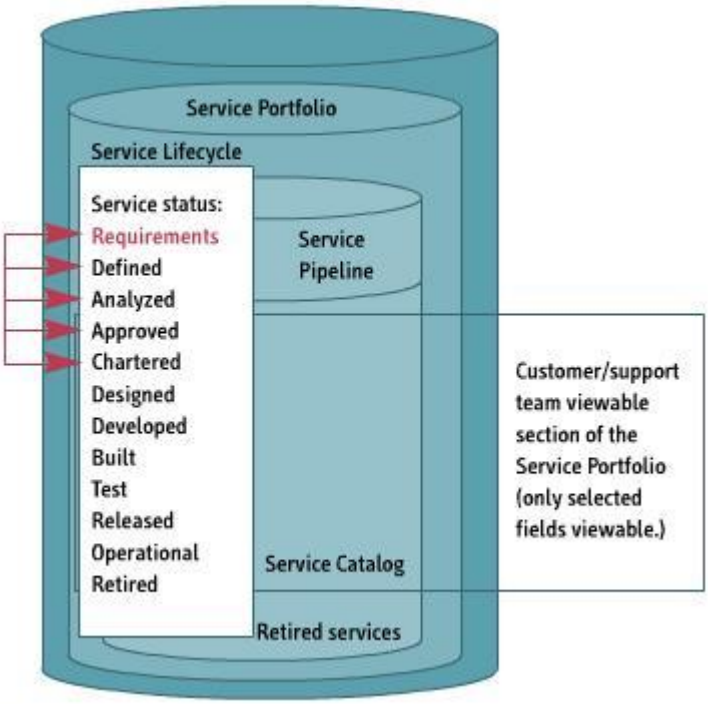
The Service Portfolio describes an IT service provider's services in terms of business value. Because business value relates to market value, the Service Portfolio provides a means for comparing the service competitiveness of different service providers.



A Service Portfolio should help to clarify the following strategic questions;

- Why should a customer buy these services?
- Why should the customer buy these services from your organization?
- What are the pricing or chargeback models for the services?
- What are the service provider's strengths and weaknesses, priorities, and risks?
- How should the organization's resources and capabilities be allocated?

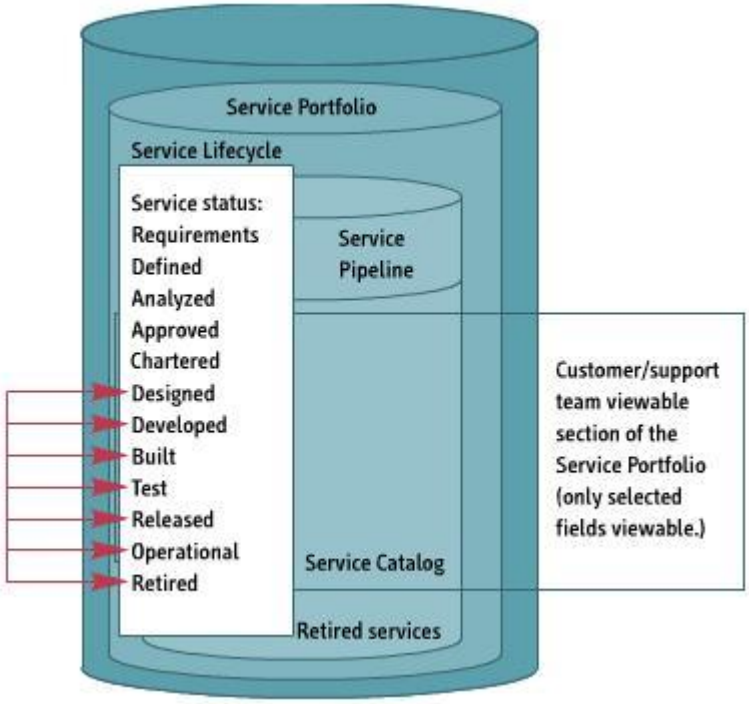
When you're formulating the set of requirements for a new service, the service may have one of five status options in the Service Portfolio.



- The **Requirements** status indicates that an outline of the requirements of a new service has been identified.
- The **Defined** status indicates that the requirements for the new service are being assessed, specified and documented and that the SLR's for the service are being produced.
- The **Analyzed** status option indicates that the requirements for the new service are still being evaluated and prioritized.

- The **Approved** status option indicates that the set of requirements for the new service have been finalized and authorized.
- The **Chartered** status option indicates that the set of requirements for the new service is being communicated and that resources and budgets are being allocated.

Once resources and budgets have been allocated to the new service, design work can commence. There are 7 status options for a new service once the design phase commences.



- The **Designed** status option indicates that the new service and its components are being designed.
- The **Developed** status option indicates that the new service and its components are being developed.
- The **Built** status option indicates that the new service and its components are being constructed.
- The **Test** status option indicates that the new service and its components are being evaluated.
- The **Released** status option indicates that the new service and its components are being delivered into the live environment.
- The **Operational** status option indicates that the new service and its components have been implemented and are functional within the live environment.
- The **Retired** status option indicates that the service and its components are no longer operational.

A new service may be allocated a particular overall status. However each constituent component of the service may be allocated a different status option.

Aspect 3: Design Technology and Management Architectures:

The design of technology and management architectures is the third aspect of service design.

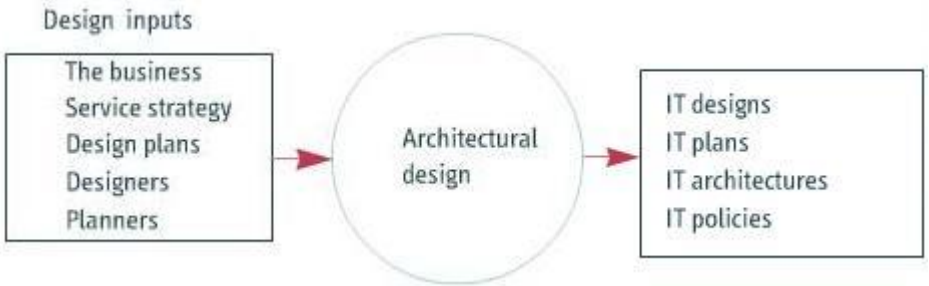
Architectural design can be defined as the development and maintenance of IT policies, strategies, architectures, designs, documents, plans, and processes. Architectural design is used for the deployment and subsequent operation and improvement of appropriate IT services and solutions throughout an organization.

Architectural design needs to ensure that the IT infrastructures, environments, data, applications, and external services serve the needs of the business, its products, and services.
This means that architectural design should include both the design of the technology components and the design of the systems that are used to manage them.

When designing architecture, it is important to obtain a balance between

- **Innovation** (Dynamic, continuous innovation that builds on existing architecture is less risky and costly than designing an entirely new architecture)
- **Risk** (Although the design of an entirely new architecture holds considerable risk as it might fail, it is even riskier not to innovate at all. Not working on innovative services can be costly to an organization in the long term when its competitors overtake it. A risk - benefit assessment should therefore be conducted)
- **Cost** (The cost of designing architecture should be determined in relation to the anticipated benefits from the innovation by obtaining the cost-benefit ratio)

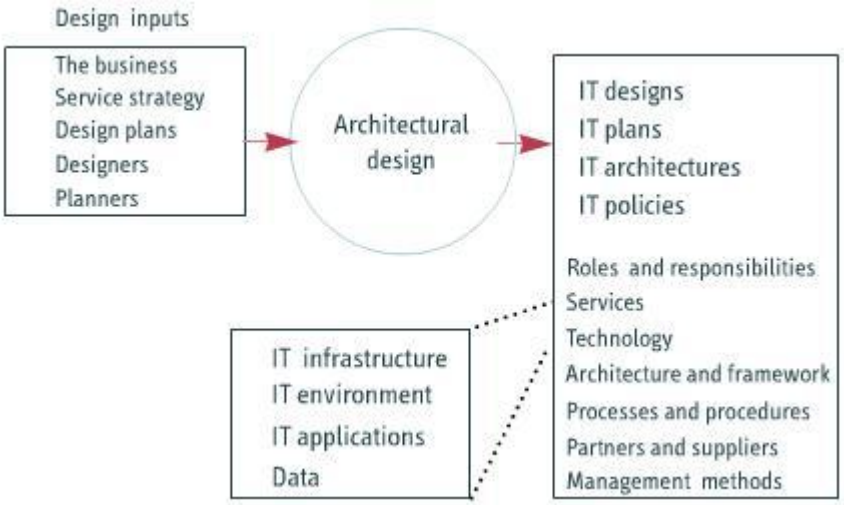
The inputs for architectural design come from the business, the Service Strategy, architectural design plans, designers, and planners. The outputs include IT designs, plans, architectures, and policies.



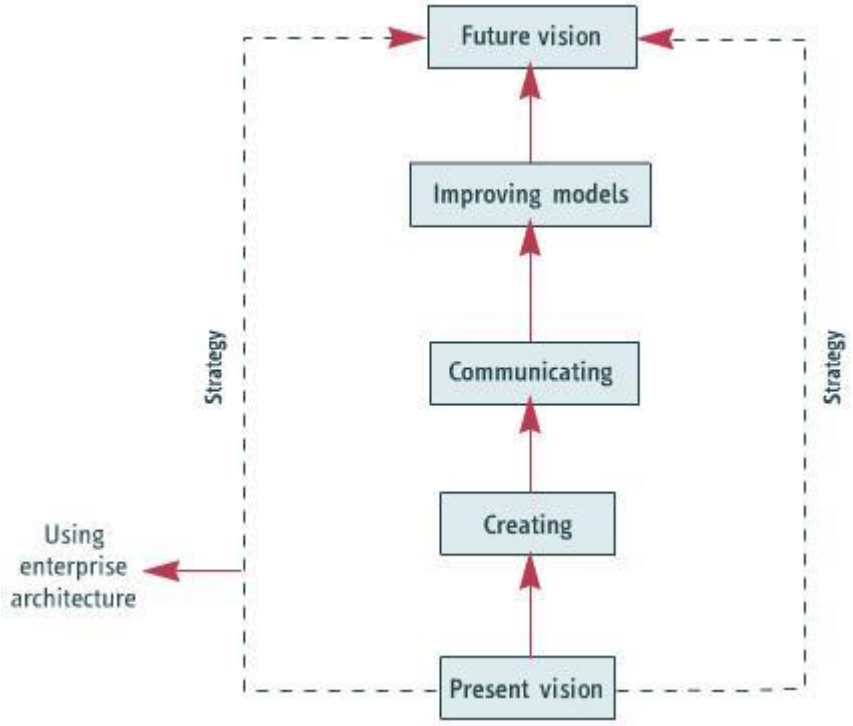
The designs, plans, architectures, and policies that result from architecture design should cover these aspects of IT:

- roles and responsibilities
- services
- technology
- architecture and frameworks
- processes and procedures
- partners and suppliers, and
- management methods

More specifically IT Technology refers to the IT Infrastructure, the environment, the applications and data.

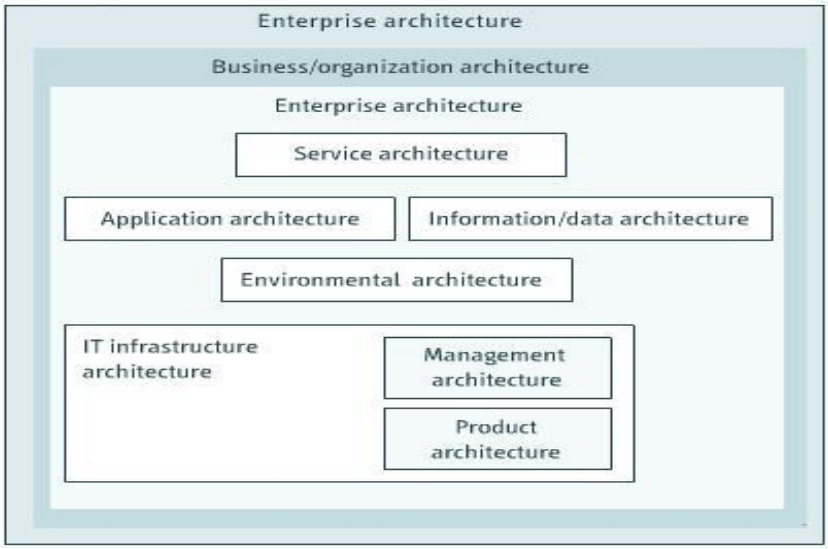


Enterprise architecture is defined as the process of translating business vision and strategy into effective enterprise change by creating, communicating, and improving key principles and models that describe the future state of the enterprise and enable its evolution.

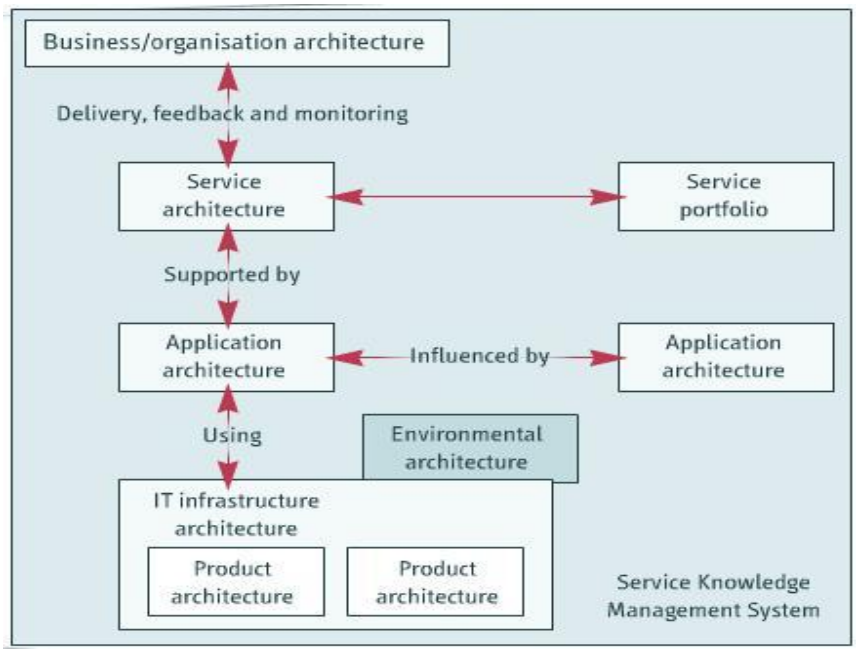


The enterprise architecture forms an integrated part of the business architecture. Its components are concerned with both the business of the organization and the information systems that support the business.

As an integrated part of the business architecture, the enterprise architecture includes five major areas.

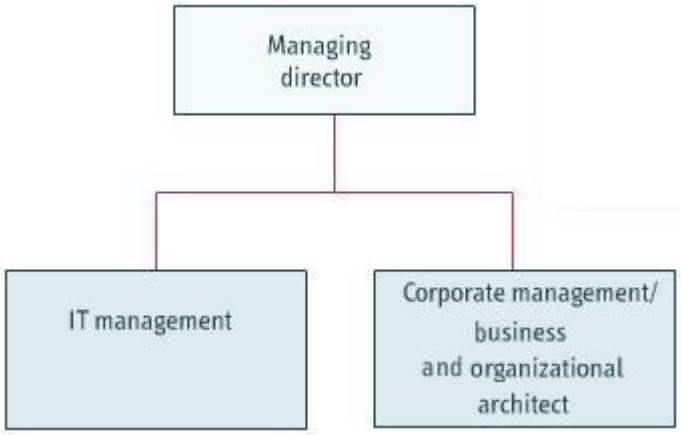


Service architecture – converts applications, infrastructure, and organization and support activities into a set of services
Application architecture – develops and deploys apps, ensures business and functional requirements mapped to applications.
Information and data architecture – manages logical and physical assets and data, manages information resources and shares it.
Environmental architecture describes all aspects, types and levels of environmental control and their management.
IT infrastructure architecture describes the structure, functionality, and geographical distribution of the hardware, software, and communications components - as well as the applicable technical standards - on which the overall architecture is based.

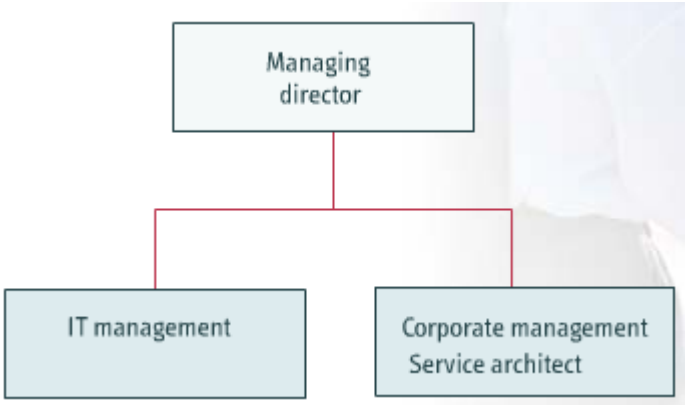


Organizations rely on key individuals to maintain architectural relationships and to drive the process forward. Most organizations will have these three roles:

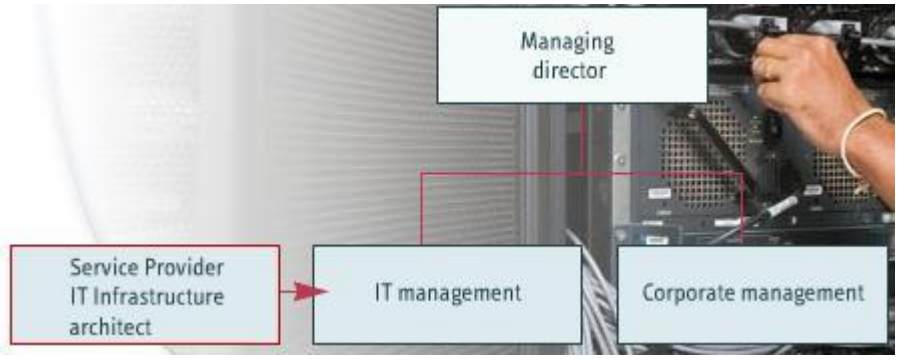
1. **business and organizational architect** (is concerned with business models, business processes, and organizational design - the structural and functional components of the organization and how these relate to each other)



2. **service architect** (is concerned with the architectures that support the business - the service, data, and application architectures - and the relationships and interfaces between them)



3. **IT infrastructure architect** (is concerned with the physical technology model and the infrastructure components that are required to support it. This includes the selection of the technologies, interfaces, protocols, and products required to implement the infrastructure.

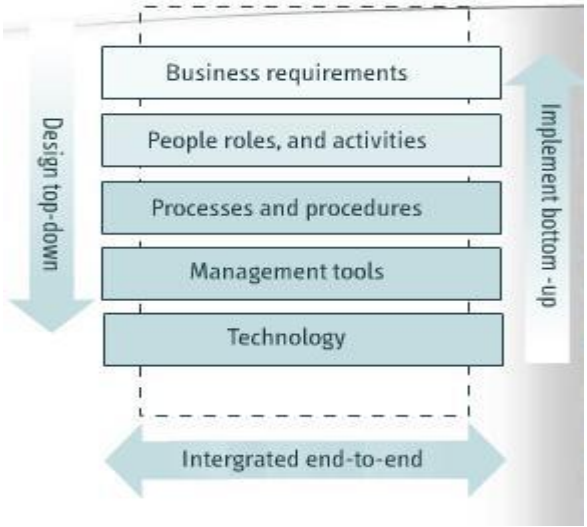


IT and business should work in partnership. IT needs should be aligned with business needs. It is useful to use a model to ensure that IT needs are aligned with business needs. The model includes five main areas that need to be considered.

- **Business requirements** include the needs, requirements, processes, objectives, and goals of the business units and managers within the organization.
- Considering **people, roles, and activities** involves considering the scope, tasks, and activities of the managers and staff involved in managing the provision of IT services.
- The **processes and procedures** used to manage the IT services that are provided to the business and its customers must align with business needs.
- The **management tools** and support tools required to manage the IT Infrastructure must align with business needs.
- The IT products and **technology** that are used to deliver services and information to the right people, in the right place at the right time, must align with business needs.

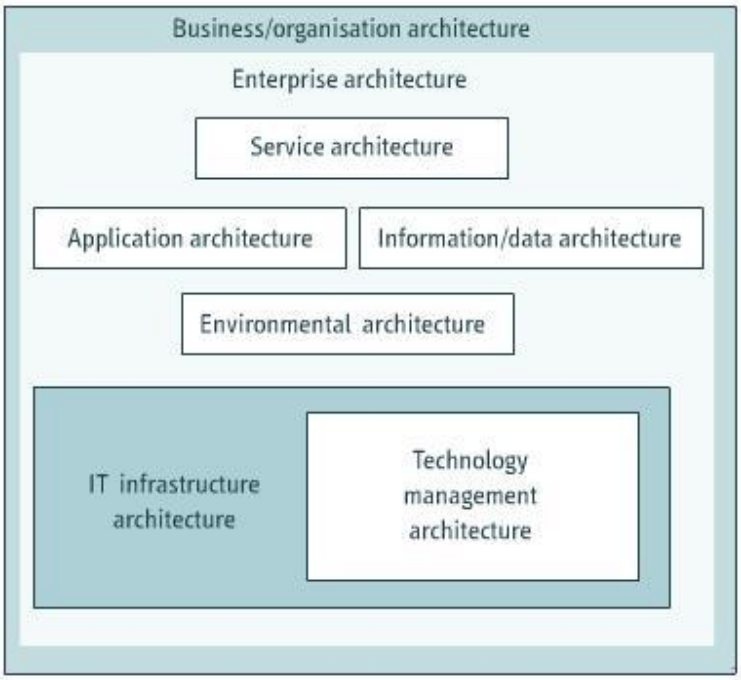
The model also enables an organization to follow a bottom-up and top –down approach when implementing the technology infrastructure. These approaches ensure that efficient and effective Service Management and Technology Management processes are fully integrated with the tools and technology in use within the organization.

The model should be used to ensure greater exploitation of tools in the management and support of technology and end-to-end processes.



To ensure that IT needs are aligned with the needs of the business, a strategic approach should be followed when planning the information technology for the design of the management architecture.

This calls for the creation of an architecture that provides a framework within which the technology will be managed over the long term. The technology management framework forms an integral part of the IT Infrastructure architecture and is one of the major areas of the enterprise architecture as a whole.



The benefits of using management architecture to integrate IT needs with business needs are that management systems become

- more focused on business needs
- more closely aligned to business processes
- less dependent on specific technology and more "service-centric"
- more integrated with other management tools and processes as management standards evolve
- incorporated in end-to-end management systems and processes
- more focused on providing quality customer services, and
- more flexible

Aspect 4: Design Required Processes:

One of the aspects of Service Design is the design of the processes that are required to operate, support, and maintain the new or changed service that is being designed.

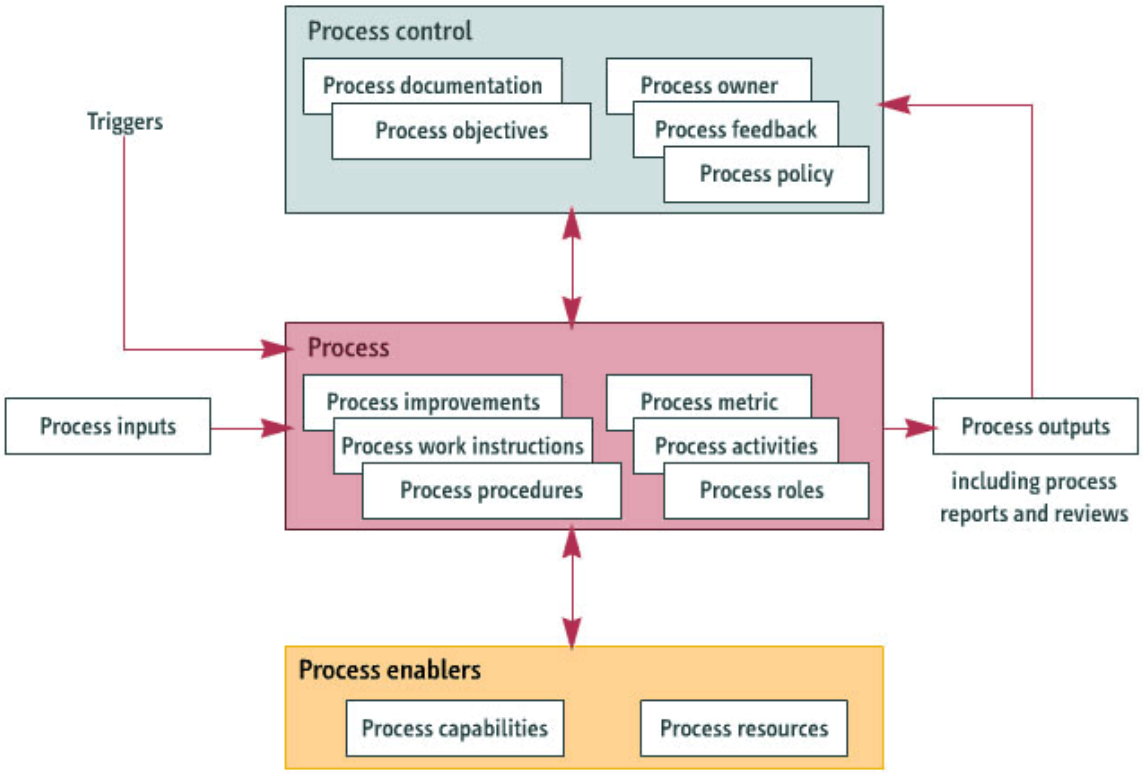
Each process should be described according to a clearly defined input, its activities, its procedures and roles, and the process output. The output needs to be measured regularly against a set of norms with the aim of optimizing the process.

Defining a process

A process can be defined as a structured set of activities that are designed to accomplish a specific objective. A process takes one or more inputs and uses roles, responsibilities, tools, and management controls to turn them into defined outputs.

Designing a process

A process is designed around its basic elements – the data that enters the process is processed to produce the output. The output is measured and the reviewed output is again used as input in order to improve the process until the design is optimized. In this way, a process is regulated to perform effectively, efficiently, and consistently.



The basic elements of designing a process
The aspects that need to be included in the design of a process are:

Process enablers (are the resources and the capabilities that enable the process to occur)
Process input (consists of data that needs to be carefully defined with the view of generating the desired output)
Process activities, procedures, and work instructions
Process output (should be driven by the process objectives and has to conform to the operational requirements that are derived from the objectives. The process output should also include reports containing measurements that can be used for the purpose of process control)
Process control (Process control is the responsibility of the process owner, who has to ensure that the process objectives are met and that the process is improved and optimized)

Aspect 5: Design Measurement Methods and Metrics:
The 5th aspect of Service Design is the design of measurement methods and metrics. Measurement methods and metrics are important for managing and controlling processes. The individual components of a process can be managed and improved upon only if they can be measured.

It's also important to select measurements and metrics that encourage people to meet all the objectives of a process. To be effective, measurement methods and metrics need to meet several requirements. They need to measure whether the design solution

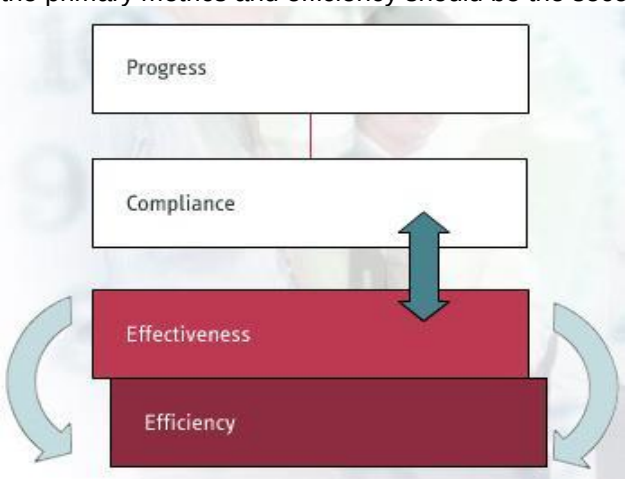
- i**s "fit for purpose"** (whether the design solution accomplishes what is set out in its objectives to establish its fitness for purpose)
- **has an appropriate level of quality** (whether the level of quality specified in the process objectives is achieved – the design solution should neither be over engineered nor under engineered)
- **works "right first time"** (whether the design solution works right first time and meets its expected targets.

- **minimizes the need for adjustments** (whether a design solution is capable of minimizing the need for adjustments or add-ons that have to be rapidly developed after the solution has been deployed)
- **is effective and efficient** (whether the design solution is effective and efficient from the perspective of business and its customers)

There are four types of metrics that can be used to measure the capability and performance of processes:

- **progress** (measure the capability of a process to reach milestones and to produce deliverables on time)
- **Compliance** (measure the compliance of a process to governance requirements and regulatory requirements. They also measure whether people comply with the way in which the process is meant to be used)
- **Effectiveness** (measure the accuracy and correctness of a process in terms of its objective – the ability of the process to deliver the right result)
- **Efficiency** (measure the productivity of the process and its speed, throughput and resource utilization)

Effectiveness should be the primary metrics and efficiency should be the secondary metrics.

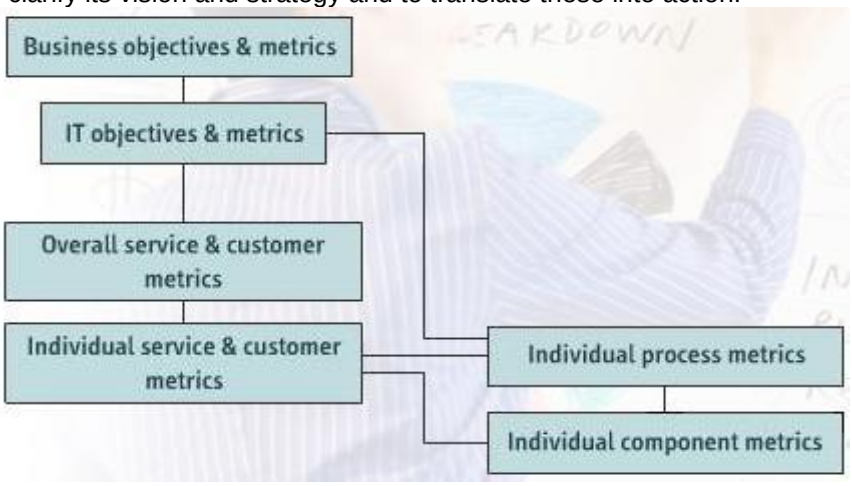


The Metrics Tree

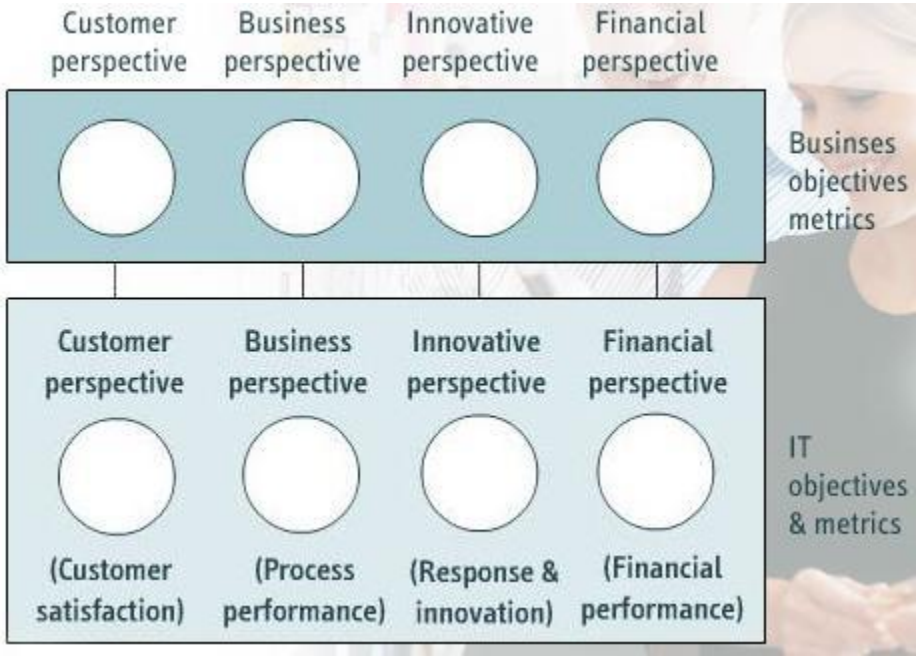
Organizations should attempt to develop automated measurement methods based on a form of metrics tree. A metrics tree is based on a typical balanced scorecard.

Note:

The balanced scorecard is a management and measurement system that enables an organization to clarify its vision and strategy and to translate these into action.

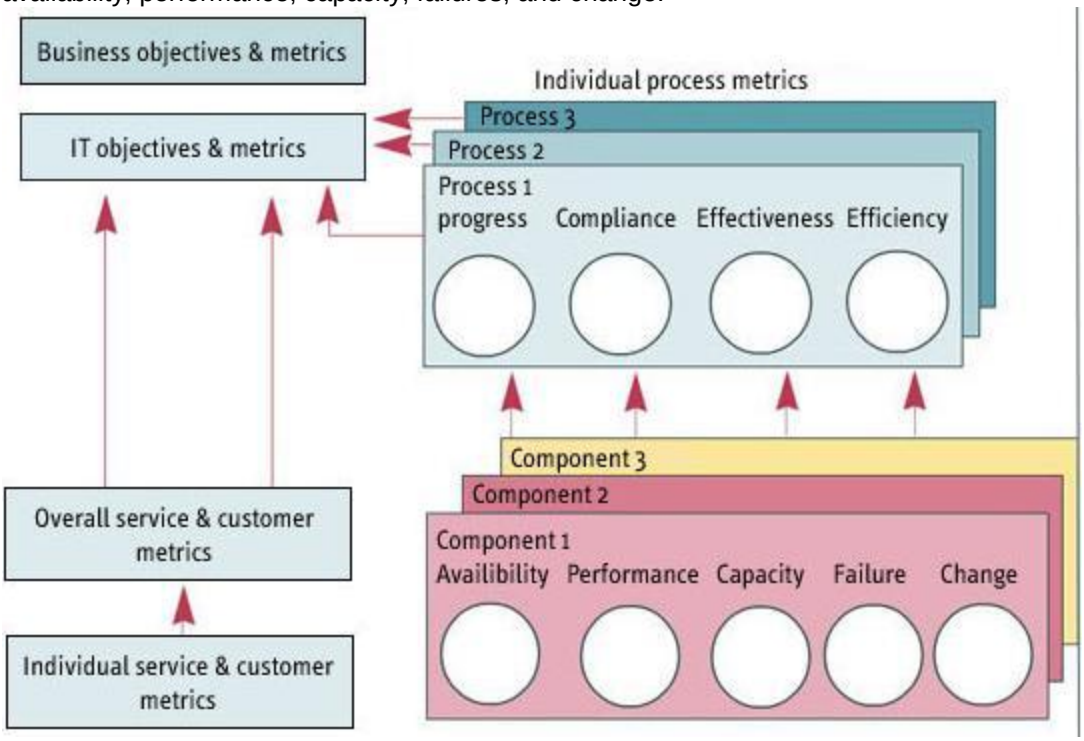


The metrics tree first links IT objectives and metrics with business objectives and metrics. In both cases, these objectives and metrics relate to the customer, business, innovation, and financial perspectives.



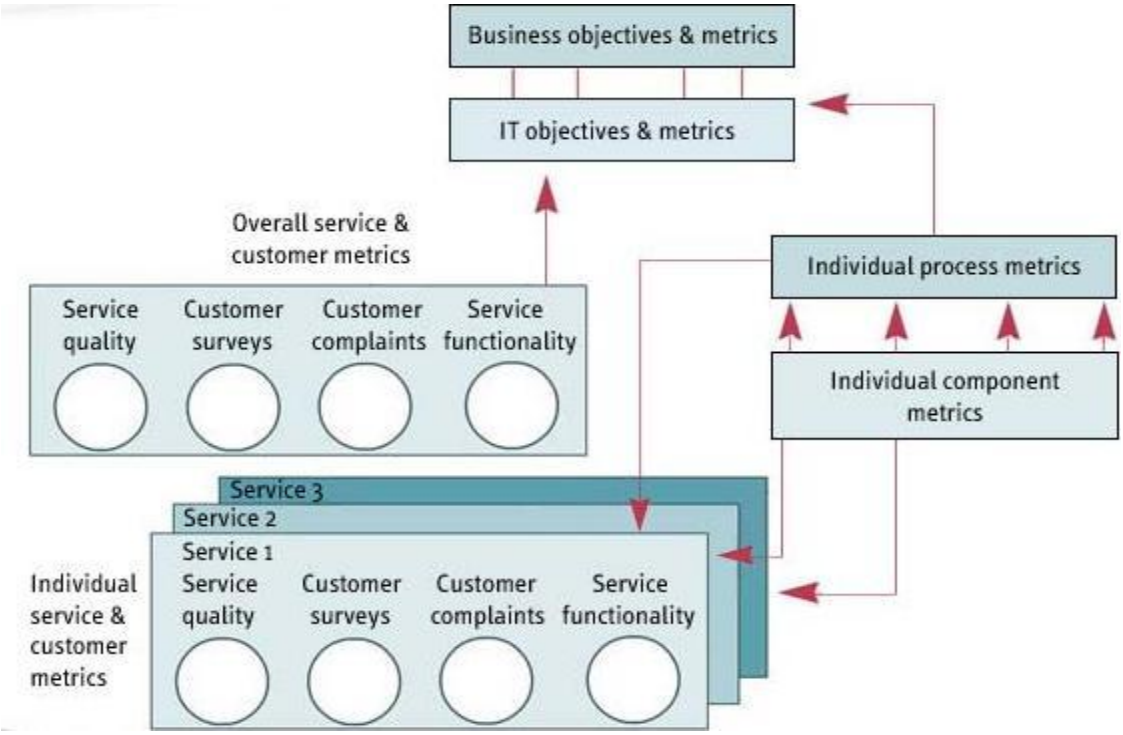
The metrics tree links the metrics for measuring individual internal business processes and individual process components with the business and IT objectives and metrics.

Individual business process metrics include those that measure progress, compliance, effectiveness, and efficiency. Individual process component metrics include those that measure availability, performance, capacity, failures, and change.

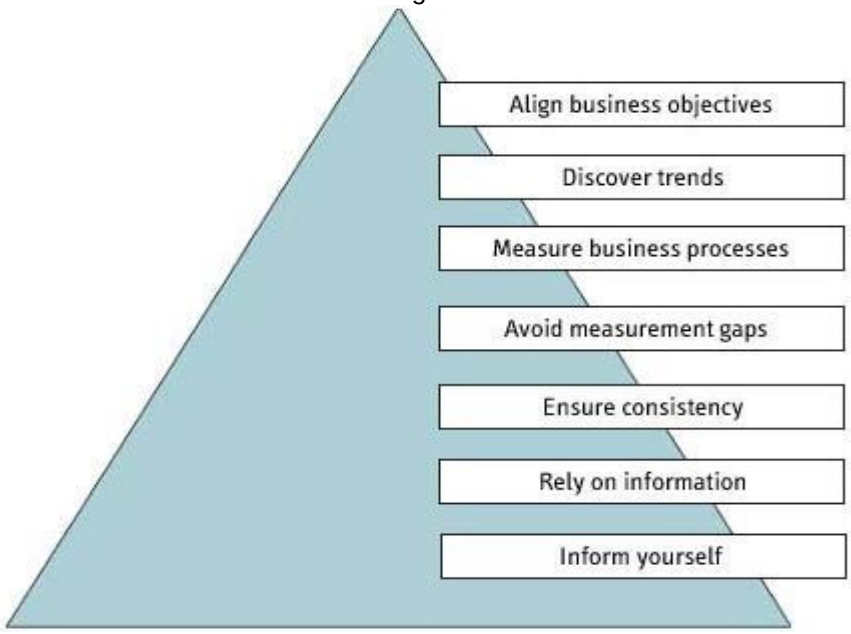


Finally, the metrics tree links overall and individual services - and their respective customer metrics, the processes external to the organization - to the business and IT objectives and metrics.

Overall and individual services and customer metrics include those for measuring service quality, customer feedback or surveys, customer complaints, and service functionality.



The metrics tree – or balanced scorecard – provides feedback on internal business processes and external outcomes with the aim of continually improving strategic performance and results. The use of a metrics tree has these benefits for an organization:



- measurements align with business objectives
- trends can be discovered overtime (For example, management may assess customer complaint metrics overtime to identify performance weaknesses)
- business processes are properly measured
- measurement gaps are prevented
- measurement, presentation, and calculation methods are consistent
- complete and accurate information is available (helps in deciding on strategies)
- picture of service performance is informative (people in an organization can obtain performance information that's relevant at the organizational levels they occupy)

Service Design Processes:

Introduction to Service Level Management (SLM):

The main purpose of Service Design Processes is to provide key information for design of new or changed service solutions. The output of Service Design processes should be the design of service solutions that meet both business and customer needs. Service Design includes 8 processes

Service Level Management (SLM) (involves negotiating SLAs (Service Level Agreements) and ensuring that they are adhered to. It also involves monitoring and reporting on service levels)

Design Coordination (involves ensuring the overall goals and objectives of the Service Design stage are met by providing and maintaining a single point of coordination and control for all activities and processes within the Service Design stage of the Service Lifecycle)

Service Catalog Management (involves maintaining an accurate, central set of information on all services provided by an organization. A Service Catalog usually details a service's status, interfaces, and dependencies)

Availability Management (involves ensuring reliable, stable service availability for customers)

Capacity Management (involves ensuring that the capacity and performance of IT systems and infrastructures meet business requirements in the most cost effective and timely way)

Supplier Management (involves ensuring that all contracted suppliers meet the needs of the organization and that they deliver on all contractual agreements on time)

Information Security Management (provides strategic direction for security activities. It ensures that information is secure and that assets are used appropriately)

IT Service Continuity Management (supports business continuity management processes by ensuring that IT infrastructure and facilities can be recovered after disaster within an agreed timescale)

The development of contracts is an important part of the Service Design process.

A contract is a legally binding commitment between a customer and a supplier. It sets out the obligations and responsibilities of each party, as well as the targets that must be met - during and sometimes even after the delivery of services.

Contracts may also include other agreed terms, such as

- security requirements
- business continuity requirements
- mandated technical standards
- migration plans
- disclosure agreements

Basic concepts that are central to SLM include the management of service levels in relation to

- **Suppliers** (third-party providing components, supplies, or services required to create and deliver a service to a customer. Suppliers are managed by underpinning contracts that ensure that the supplier meets the targets that are required to fulfill the SLA, SLM is responsible for defining, documenting, monitoring, and reporting associated service levels)

- **SLAs** (is an agreement between a service provider and a customer that defines the key service targets and responsibilities of both parties. SLM establishes SLAs to manage the service provided and customer expectations, and to meet agreed quality requirements)

- **Operational Level Agreements (OLAs)** (SLM is responsible for ensuring that all targets agreed in SLAs with an organization are supported by appropriate underpinning OLAs. An OLA is an agreement between the service provider and another area or department of the same organization that assists with the provision of services. An OLA should define the targets that support those agreed in the SLA. This ensures that targets will not be breached by failure of the supporting activity, department, or supplier.

Objectives of SLM:
The objectives of SLM are to ensure that

- the level of all IT services is defined, documented, agreed, monitored, measured, reported on, and reviewed
- relationships and communications with customers are improved at all levels within the business and customer community
- measurable targets exist for all services
- customer satisfaction is managed and improved with the level of service quality provided
- both IT service providers and customers have clear and unambiguous expectations of the level of service to be provided
- measures are taken to improve service levels where it is financially justifiable to do so

<u>Service Level Management Process Activities:</u>
Service Level Management (SLM) involves several key activities. These activities can be organized into four phases.

Negotiating Phase:
The negotiating phase of SLM involves designing SLA frameworks, determining, documenting, and obtaining agreement on requirements for new services, and developing and documenting contacts and relationships with the business, customers, and other stakeholders, in cooperation with the Business Relationship Management (BRM) process.

Designing SLA frameworks involves using the Service Catalog to design appropriate SLA structures which are based on business and customer needs.

There are three types of SLA structure,

A **service-based SLA** covers generic service requirements for a particular service and for all customers that make use of that service. This type of SLA is most appropriate when a broad range of customers or business areas share common service level requirements.
A **customer-based SLA** covers service agreements for all services that are used by a particular customer group. This type of SLA provides advantage for customers because it lists all their service level requirements within one document. Only one signatory is required.
A **multilevel SLA** usually comprises three levels - corporate, customer, and service. The corporate level covers the generic SLM requirements of every customer throughout the organization. The customer level covers SLM issues relevant to a customer group. The service level covers SLM issues relevant to the service, in relation to the customer group.

Producing SLRs is one of the earliest activities in the Service Design stage of the Service Lifecycle. An SLR is a customer requirement for an aspect of an IT service. SLRs are based on business objectives and are used to **negotiate agreed service level targets**

As a service progresses through its lifecycle, an SLR develops into an SLA. It is important to get customers involved at this stage, decide on performance targets and involve Capacity and Availability Management, to provide the input that is needed when determining realistic targets.

If there is any doubt about whether a target needs to be included, it should be included in a draft SLA. The draft SLA can then be monitored and adjusted throughout the service warranty period. The draft SLA is used during negotiations with the customer to finalize service targets, and with the service provider to ensure that the targets are achievable.

An important activity of SLM is **developing and documenting contacts and relationships** with customers. This ensures that the organization develops trust and respect with its customers.

The Service Catalog provides information that can help in the development of relationships with customers. It identifies the relationships between services and the customer business areas that depend on them. In addition, it should provide key contacts for each service.
There are several activities that take place during the SLM process to develop contacts and relationships. These activities include

- confirming stakeholders, managers in key business areas, and customers
- maintaining accurate information within the Service Catalog and Service Portfolio
- being flexible and responsive to the needs of the customer
- developing a full understanding of the customer, the customer's organization, and strategies
- regularly sampling the customer experience
- conducting customer surveys and acting on the results
- ensuring that the correct relationship processes are in place to achieve objectives

Other activities for developing relationships and contacts are

- marketing and exploiting the Service Portfolio and Service Catalog
- assisting with maintaining a list of outstanding improvements
- ensuring that the organization and customers understand their responsibilities
- facilitating the negotiation of SLRs and SLAs
- raising the awareness of the business benefits when using new technology
- promoting service awareness

- ensuring that IT provides the most appropriate levels of service

Monitoring Phase:
Monitoring service performance against SLAs helps ensure that services are operating optimally and meeting customer requirements.

Only specific targets that can be measured and monitored should be included in an SLA. The inclusion of targets that cannot be monitored can result in disputes and loss of faith in SLM.

An important activity in the SLM process is to **collate, measure, and improve customer satisfaction,** in cooperation with BRM. This requires monitoring service levels with an understanding of customers' perceptions of service delivery.

Existing monitoring capabilities within the organization should be reviewed and upgraded as necessary. Without monitoring each component of a service, it is hard to gain a complete picture of customer perception. Many organizations use service desk metrics to monitor customers' perception of service availability.

It is best to manage customer perceptions from the outset. This can be achieved by ensuring that appropriate service targets are set and by putting a process in place to manage customer expectations.

The aim should be to provide services that customers need and that are justified in terms of cost and strategy. However, senior business managers need to ensure that no customer group places unrealistic demands on the service provider.

Customer perception can be managed through
- periodic customer questionnaires and surveys
- customer feedback from review meetings
- feedback from a Post Implementation Review (PIR)
- user group and forum meetings
- analysis of customer complaints and compliments

Whatever method is used to manage customer perception, it is important to ensure that if customers provide feedback, the organization demonstrates a commitment to its customers by acting on this feedback.

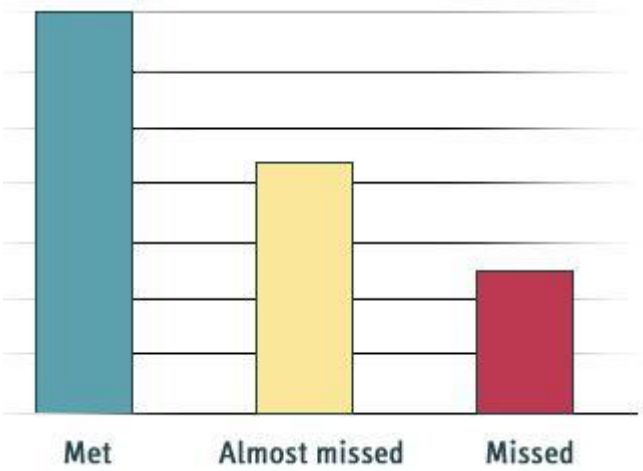
Reporting Phase:
Key **reporting activities** in the SLM process include producing service reports, and logging and managing customer complaints and compliments.

SLM is responsible for identifying reporting needs and automating production of the required reports. It should also ensure that the reports include information on past performance and trends, so that the impact of improvement actions can be measured and predicted. The results of monitoring must be used to produce **service reports.**

Periodic reports should include details of service performance and SLA targets. They may also include information about trends or actions that will improve the quality of the service.

Exceptional reports should be created whenever the SLA for a service is breached. Organizations should also create periodic reports based on their review cycles.

A Service Level Agreement Monitoring (SLAM) chart can also be used to assist in monitoring and reporting on actual achievements in relation to set targets. A SLAM chart is usually color coded to indicate whether each agreed target has been met, missed, or almost missed.



SLM should include procedures for logging and managing customer complaints and compliments. The service desk is usually responsible for logging complaints and compliments because it plays a key role in Incident Management. SLM should ensure that all complaints are managed and acted upon to the satisfaction of the customer. SLM should also define escalation procedures for complaints that are not acted upon appropriately or within predefined times. Reports should also be created to identify the types of complaints, trends, and the actions taken to resolve them. Similar reports should be created to monitor compliments.

Reviewing Phase:
SLM must review and revise underpinning agreements to ensure that they are comprehensive, kept up-to-date, and aligned with business needs.The results of this review can serve as inputs for Change and Configuration Management.

SLM includes conducting service reviews and implementing improvements regularly with customers. It also includes analyzing service performance in the previous period. This helps identify issues that might arise in the future.

Review meetings ensure that actions are taken by the customer and service provider to improve weak areas, where targets are not being met.

If it is decided that SLA targets are unachievable, new, achievable targets must be defined. If it is determined that the SLA breach is caused by failure of a third-party provider, underpinning agreements must be revised.

When utilizing external suppliers' contracts is mandatory, it is also useful to have agreements with internal support groups through Operational Level Agreements (OLAs). OLAs reflect the need to ensure that all targets within the agreement are aligned with the targets within the SLA.

Managing Key Service Design Processes:

Design Coordination:

The Service Design stage of ITIL Service Lifecycle involves many complex activities. The design coordination process helps IT service providers manage and organize these activities so that designs are created to support business outcomes.

Objectives of Design Coordination:
Design coordination has the following objectives:

- ensuring the consistent design of Service Management Information Systems, architectures, and technologies
- coordinating design activities across projects, and managing schedules, resources, and conflicts

- producing service design packages (SDPs) based on service charters and change requests
- planning and coordinating resources and capabilities required by Service Design
- managing the quality criteria and handover points between the Service Design stage, and Service Strategy and Service Transition stages

There are several other design coordination objectives:

- ensuring that all service models and solution designs meet requirements
- improving the effectiveness and efficiency of Service Design activities and processes
- monitoring and improving the performance of the Service Design Lifecycle stage
- ensuring a common framework of standards regarding activities, processes, and supporting systems

Scope of Design Coordination:

The scope of the design coordination process includes all design activity, such as service solutions, that need to be transitioned into, or out of, a live environment.

The scope of design coordination also includes

- assisting and supporting projects and changes through Service Design activities and processes
- maintaining policies, guidelines, budgets, models, and resources for activities and processes
- coordinating, prioritizing, and scheduling resources for Service Design
- planning and forecasting resources for future Service Design activities
- reviewing and improving the performance of Service Design activities and processes
- addressing the utility and warranty requirements of Service Design activities, and
- producing SDPs and handing them over to Service Transition

Design Coordination excludes activities and processes such as designing service solution details and producing individual parts for SDPs.

There are several reasons why design coordination is useful:

- it achieves services at acceptable risks and costs
- it minimizes rework and labor costs
- it increases customer and user satisfaction, and confidence in IT and IT services, and
- it ensures architectures are consistent and allows for data integration and exchange

Design coordination also

- focuses on service value and business, and customer outcomes
- improves the efficiency and effectiveness of Service Design activities and processes
- supports successful change delivery in a timely and cost-effective manner, and
- achieves greater agility and quality in designing service solutions

Policies and guidelines for Design Coordination:

Design coordination needs guidelines and policies to ensure a structured and holistic approach to design activities. These policies are defined by service providers because they decide how much attention or coordination design activities require. Policies should be in place to ensure design activities are properly documented. The design coordination process includes policies such as

- adherence to corporate standards and conventions
- standards for new or changed services such as documentation, training, and communications and marketing
- governance and regulatory compliance in all design activities, and
- criteria for how to resolve conflicting demands for Service Design resources

The main goal of policies is to create value and positive results. However, you shouldn't spend more time creating policies than implementing them.

As a guideline, the design coordination process must have balance in order to address all aspects of utility, warranty, and the needs of the service throughout its lifecycle.

Another guideline is to build on current practices and to continually search for ways to improve them. To do this, you can use the Continual Service Improvement (CSI) approach.

It's also important to limit the number of practices that are implemented, because too many new practices can disrupt design activities and lead to failure.

The Service Design Stage involves activities that are managed by the design coordination process. These activities include

- collecting, analyzing and engineering business, service provider, and technical requirements to ensure clear documentation, agreement, and alignment
- designing service solutions, technology, processes, information, and metrics
- producing and maintaining IT policies and design documents, and
- reviewing and revising the design and maintenance of process design documents

Other activities include

- planning deployment and implementation of IT strategies using roadmaps, programs, and project plans
- assessing and managing risk of all design processes and deliverables
- ensuring alignment with all corporate and IT strategies and policies, and
- producing service designs and SDPs for new or changed IT services

Design coordination activities fall into two categories. The first category relates to the overall Service Design stage.

1. **Define and maintain policies and methods**
   Defining and maintaining Service Design policies and methods produces consistent and accurate designs that meet the required business outcomes. Design coordination works collaboratively with all other Service Design processes to ensure a common framework of standard reusable processes, procedures, and systems to improve the effectiveness of the overall Service Design.

This includes agreeing on, using and managing the quality criteria, requirements, interfaces and hand-off points between the Service Design stage and other stages. The level of design coordination needed for different types of projects should also be defined. A set of architectural documents and principles for the design of service solutions and SDPs must also be maintained and revised by the design coordination process.

2. **Plan design resources and capabilities**
   Design Coordination does this by obtaining info from other processes in the Service Portfolio and Change Management. It also identifies and addresses gaps in current capabilities by providing training to staff, hiring new staff, automating design activities, enforcing requirements and standards, creating or improving procedures and capabilities, and developing knowledge and making it accessible.

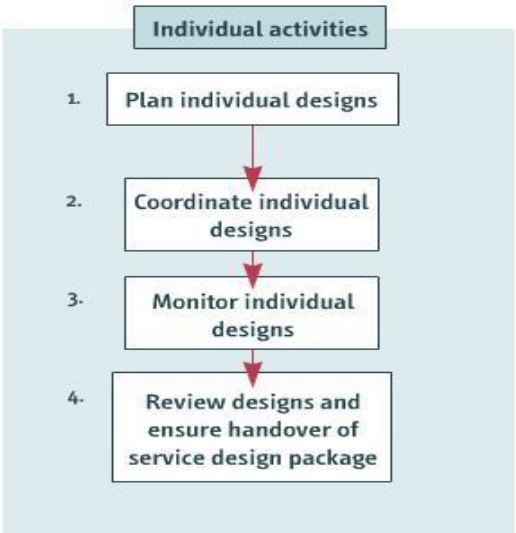
3. **Coordinate design activities**
   Design Coordination coordinates schedules, resources, and conflicts, and suppliers and support teams. Integrated approach (enterprise architecture) helps in effective coordination of design activities.

   To achieve an integrated design, the design coordination process needs to ensure good communication between design activities and parties concerned, that appropriate business and IT plans are available to designers, and that architectural documents, service models, service solution designs, and SDPs conform to architectural, governance, and other requirements. Lastly, there should be good communication and coordination with Service Transition processes to ensure proper handover.

4. **Manage design risks and issues**
   Managing design risks and issues by reducing them using risk assessment and management techniques is another activity. This activity monitors risks that occur in all design efforts as well as ones that occur in individual projects and change activities.

5. **Improve Service Design**
   This is accomplished by monitoring and measuring the Service Design stage's performance and then identifying improvement opportunities based on objective information. To do this, the CSI approach can be used for continual process improvement where ideas can be entered into the CSI register. Later, if accepted, these ideas can be added to service improvement plans (SIPs).

The second category that design coordination activities fall into relates to individual design activities.



1. **Plan individual designs**
   The first activity is planning individual designs using standards and templates that have already been created and tested. Design activities must ensure that the full design or SDP delivers the required business outcomes. This not only includes the IT service itself, but also the costs and schedules associated with the service. Design activities should therefore consider the functionality, warranty, the service's effectiveness, and the requirements to operate, maintain, and support the service.

2. **Coordinate individual designs**
   The second activity is coordinating the individual designs that will more than likely be carried out by a project manager who can draw upon the body of experience developed by the process from other designs. It's possible that as the Service Design stage progresses; some information may require strategic decisions to be revisited, such as the Service Portfolio Management process and other processes.

   Throughout the design activity, all requirements of service, business, and project change management should be adhered to and documented. Close attention must also be paid to scheduling both the service provider and customer resources to ensure accurate and complete designs.

3. **Monitor individual designs**
   Monitoring individual designs to ensure that the proper methods are followed and ensuring that there are no conflicts with other design efforts is the third activity. This ensures design milestones are met, and comprehensive designs that support the achievement of the required business outcomes are developed.

4. **Review designs and ensure handover of service design package**
   The final step is reviewing designs to ensure they comply with standards and conventions, and that SDP requirements have been completed. Completed SDPs can be handed over for service transition. All issues should be documented and a decision made on whether the issues should be addressed during the Service Design or Service Transition stages.

Design Coordination triggers:
The Design Coordination process can be triggered by various things such as requests for change, the need to create new programs, and projects, and the revision of overall IT strategy.

Inputs to Design Coordination:
Once triggered, design coordination obtains information from inputs such as’

- change requests and records, and service charters
- business and IT strategies
- business impact analysis
- Service Portfolios, Service Catalogs, and business requirements, and
- governance, corporate, legal, and regulatory policies and requirements

Other inputs include

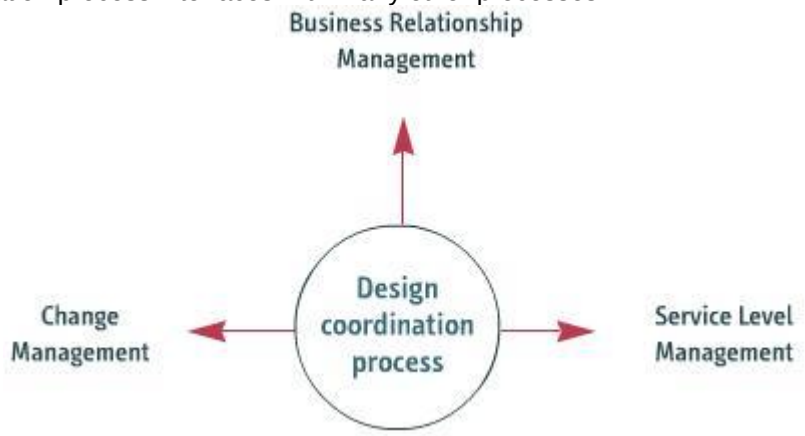
- program, project, and change schedules
- Configuration Management Systems (CMSs) and other management systems
- enterprise architectures, and
- measurement and metrics methods, and feedback from other processes

Outputs from Design Coordination:
The various design coordination process inputs produce outputs - for example, a set of service designs and SDPs, updates to change records, and enterprise architectures.

The outputs can also include revised management systems, processes, and measurement and metrics methods.

Design Coordination Interfaces:
The design coordination process within the Service Design stage interfaces with other stages of the Service Lifecycle and their processes, including the Service Strategy and the Service Transition stages

The design coordination process interfaces with many other processes.



Business Relationship Management interacts with the design coordination process by supplying it with information about desired business outcomes, and customer needs and priorities. It also acts as an interface between customers and the design coordination process

Change Management produces change requests and then interacts with the design coordination process by communicating what modifications the requests require - depending if it's within design coordination's scope. Change Management then authorizes and ensures the changes are carried out. Feedback is then provided, in the form of Post Implementation Reviews (PIRs), stating areas that the design coordination process needs to improve.

Service Level Management (SLM), along with the design coordination, defines the service level requirements for new or changed services. It focuses mainly on the warranty levels that the solution design and design coordination activities require. This ensures the service solution design and SDP are appropriately addressed.

The Design Coordination process interfaces with several other processes.

- Service Portfolio Management
- Financial Management for IT services
- Transition Planning and Support
- Strategy Management for IT services
- Supplier, Release, and Deployment Management
- Service Validation and Testing, and
- Availability, Capacity, IT Service Continuity, and Information Security Management processes

Challenges to Design Coordination:
The design coordination process has certain challenges that need to be closely monitored.

One of the major challenges is trying to maintain consistent quality across the Service Design stage, as a result of the work being carried out by different individuals, such as process owners, managers, and project managers.

The design coordination process also has to develop standards and practices and integrate them into the organization's project management methodology to ensure high-quality consistency.

Another challenge is ensuring that enough time and resources are allocated to activities, and that individuals and groups are assigned the appropriate responsibilities to complete the job

Lastly, the design coordination process should ensure that there is a balance in bureaucracy and autonomy.

Design Coordination potential risks:
The design coordination process also faces potential risks, such as

- a potential lack of skills and knowledge
- a reluctance of business involvement
- inadequate direction and strategy
- insufficient information on business priorities and impacts, and
- poorly defined requirements and desired outcomes

Other risks that the design coordination process may face include

- project managers who communicate poorly or refuse to involve themselves in activities
- relevant stakeholders like customers, users, and support and other operations staff refusing involvement
- other Service Lifecycle stages not interacting or offering input into the design coordination process, and
- poor designs that require more changes later due to efforts to try and save time and money

Service Catalog and Availability Management:
The Service Catalog is produced and maintained by the **Service Catalog Management** process, which is one of the Service Design processes.

The objective of Service Catalog Management is to ensure that there is a central, accurate, and consistent source of data about all operational services and about all services being transitioned to the live environment.

The Service Catalog is an important part of the overall Service Portfolio. It provides a key, customer-facing view of the services on offer.

A newly created Service Catalog characteristically consists of a matrix, a table or a spreadsheet.

Once a service has the chartered status -indicating that it's being developed for use by customers - Service Design produces the specifications for the service. It is at this point that the service should be added to the Service Catalog.

The Service Catalog should summarize the characteristics of the service, and contain details of its customers and maintainers.

The Service Catalog has two aspects

- the Business Service Catalog, and
- the Technical Service Catalog

The **Business Service Catalog** contains details of all the IT services delivered to customers, including the relationships of the services to business units and details of the business processes that depend on the services. This is the customer view of the Service Catalog.

For each IT service, the **Technical Service Catalog** details relationships to the supporting services, shared services, elements, and Configuration Items (CIs) necessary to provide the service to the organization. The Technical Service Catalog should support the Business Service Catalog, and is not a part of the customer view of the Service Catalog.

In Service Design, the **Availability Management** process focuses on ensuring that all operational services meet the agreed availability targets.

Objectives of Availability Management:
These are the objectives of the Availability Management process:

- to produce and maintain an appropriate and up-to-date Availability Plan that accurately reflects current and future needs of the organization
- to offer advice and guidance to all other areas of the organization and IT on availability-related issues
- to ensure that availability achievements meet or exceed targets
- to assist with the diagnosis and resolution of availability-related incidents and problems
- to evaluate the influence of any changes on the Availability Plan and on the performance and capacity of all services and resources, and
- to ensure that all cost-effective measures to improve the availability of services are implemented

The success of the Availability Management process relies on the measurement, monitoring, analysis, and reporting of three aspects of a service:

- The **availability** of a service refers to the ability of a service to fulfill its agreed purpose at the correct time. Service availability is usually measured as a percentage.
- The **reliability** of a service refers to duration for which it can perform its function without interruption.
- The **maintainability** of a service refers to how quickly and effectively the service returns to the normal after a failure.

The Availability Management process incorporates two main elements, namely reactive activities and proactive activities.

Reactive activities involve actions such as monitoring, measuring, analyzing and managing all occurrences and problems regarding unavailability. These activities are primarily related to operational roles.

Proactive activities refer to the planning, design and improvement of availability that is carried out proactively. These activities are predominantly concerned with the roles of planning and designing.

The Availability Management process focuses on both overall service availability and component availability.

If components aren't readily available, this will impact the overall service that incorporates them. So it's important to manage component availability to ensure that service availability and unavailability can be managed effectively.

As well as managing service and component availability, the Availability Management process focuses on serviceability. This refers to the ability of a third-party supplier to meet the terms and conditions of a contract.

Contract terms may include agreed reliability, maintainability, and availability levels for both services and their supporting components.

To measure the availability of a service, you can subtract the amount of downtime from the Agreed Service Time (AST), divide the result by the AST, and then multiply this number by 100 to obtain a percentage.

$$\text{Availability\%} = \frac{\text{AST} - \text{Downtime}}{\text{AST}} \times 100$$

Suppose your IT organization provides an antivirus software service. The service has an AST of 8,760 hours per year. In the course of a year, the service has had four hours of downtime
To calculate the availability of the service, you subtract 4 from 8,760, divide the result by 8,760, and then multiply by 100. This gives the service an availability of 99.95%.

The reliability of a service can be measured in either of these units:
• Mean Time between Service Incidents (MTBSI), or
• Mean Time between Failures (MTBF)

To calculate the reliability of a service in MTBSI you divide the available time in hours by the number of breaks in service availability.

$$\text{Reliability (MTBSI in hours)} = \frac{\text{Available time in hours}}{\text{Number of breaks}}$$

For example, your organization's antivirus software has 8,760 hours of time available. A total of four breaks have occurred.

$$\text{Reliability (MTBSI in hours)} = \frac{8{,}760}{4}$$

To calculate the reliability of this service in MTBSI, you divide 8,760 by 4. This gives you the reliability of 2,190 hours MTBSI.

$$2{,}190 = \frac{8{,}760}{4}$$

To calculate the reliability of a service in MTBF, you subtract the total downtime in hours from the available time in hours, and divide the result by the number of breaks.

$$\text{Reliability (MTBF in hours)} = \frac{\text{Available time in hours} - \text{Total down time in hours}}{\text{Number of breaks}}$$

Say the antivirus service had four hours downtime within the available time of 8,760 hours, and a total of four breaks.

$$\text{Reliability (MTBF in hours)} = \frac{8{,}760 - 4}{4}$$

To calculate the reliability of the antivirus service in MTBF, you subtract 4 from 8,760 and divide the result by 4. This gives the service a reliability of 2,189 hours MTBF.

$$2{,}189 = \frac{8{,}760 - 4}{4}$$

The maintainability of a service is usually measured in Mean Time to Restore Service (MTRS). You calculate the MTRS for a service by dividing the total downtime in hours by the number of service breaks.

$$\text{Maintainability (MTRS in hours)} = \frac{\text{Total downtime in hours}}{\text{Number of service breaks}}$$

The antivirus service had four hours downtime and four breaks.

$$\text{Maintainability (MTRS in hours)} = \frac{4}{4}$$

To calculate the maintainability of this service, you divide 4 by 4 - giving a maintainability value of one hour.

$$1 = \frac{4}{4}$$

The quality of the Service catalog and Availability Management processes depends greatly on the role by the respective managers.

It is typically the responsibility of the Service Catalog manager to produce and maintain the Service Catalog. The duties of the Service Catalog manager are to ensure that

- all relevant services are recorded in the Service Catalog
- the information in the Service Catalog is accurate and up-to-date
- the information in the Service Catalog Is consistent with that of the Service Portfolio, and
- the information in the Service Catalog is protected and backed up

The Availability manager is typically responsible for ensuring that all the specified aims of Availability Management are met. The responsibilities of the availability manager include

- ensuring that all services deliver the levels of availability established in Service Level Agreements (SLAs)
- ensuring that all new services are designed to deliver the levels of availability required by the organization
- validating that final designs meet the minimum required levels of availability
- assisting with the exploration and diagnosis of all incidents and problems that cause availability issues or unavailability of services or components
- participating in IT infrastructure design, including establishing the availability requirements for hardware and software, and
- establishing the reliability, maintainability, and serviceability requirements for supplied components

Capacity Management and Supplier Management:

Capacity Management:

Capacity Management is first supported in the Service Strategy stage. During this stage capacity considerations affect Patterns of Business Activity (PBA), Line of Service (LOS) and Service Level Package (SLP) development.

Capacity Management is a process that extends throughout the Service Lifecycle. However, this process is an important consideration in the Service Design stage.

Objectives of Capacity Management

These are some of the objectives of Capacity Management:

- ensuring that cost-justifiable IT capacity aligns with agreed business needs in all areas of IT
- providing a point of focus and management for all capacity and performance-related issues
- producing and maintaining an appropriate and up-to-date capacity plan that portrays business needs, and
- providing advice and guidance for all capacity and performance-related issues

Additional aims of the Capacity Management process are to ensure that service performance achievements meet their agreed performance targets, and to assist with the diagnosis and resolution of performance and capacity-related incidents and problems.

Capacity Management strives to measure the effect that any change has on the capacity plan, and on the performance and capacity of all services and resources. It also ensures that deliberate

measures to improve the performance of services are implemented as long as its costs can be justified.

A capacity plan records levels of utilization of resources as well as performance of service. Once the service strategy and plans have been reviewed, the capacity plan can then also be used to anticipate future requirements for IT resources. The plans should include any proposals that have been measured in relation to required resource, cost, benefits and impact.

A capacity plan typically consists of current services, technology and resources, the levels of capacity within an organization and any identified problems relating to over-or-under capacity. It also includes the extent to which service levels are reached and any changes since the last copy of the plan.

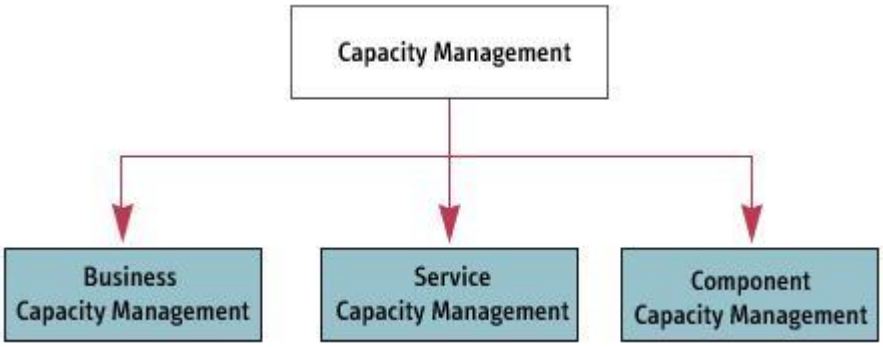
Capacity Management relies on a delicate balance of

- costs against resource needs
- supply against demand

Capacity Management needs to balance **cost against resource needs**. Any purchased processing capacity should be cost-justifiable in terms of business needs, and resources should be put to use most efficiently.

Capacity Management needs to ensure a balance between **supply and demand** for IT capacity. The available supply of IT processing power should match current and future business demands. It may be necessary to manage or influence the demand for a particular resource.

Capacity Management can be a very technical, complex, and demanding process. In order for this process to succeed in reaching its objectives, three supporting sub processes are needed.



Business Capacity Management turns business needs and plans into requirements for service and IT infrastructure. This ensures that future business requirements for IT services are quantified, designed, planned, and implemented in a timely fashion.

Future requirements come from the detail of new processes and service requirements, changes, improvements, and growth in the existing services outlined in the Service Strategy and Service Portfolio.

Future requirements can be forecasted, modeled, trended or predicted by using existing data on the current resource utilization of various services and resources.

Service Capacity Management aims to manage, control, and predict the end-to-end performance and capacity of operational IT service usage and workloads.

It also ensures that the performance of all services is monitored and measured, and that the collected data is recorded, analyzed, and reported. Automated thresholds are used where possible to identify breached or threatened Service Level Agreements (SLAs).

When necessary, employees with knowledge of technology used in the delivery of end-to-end IT service should perform proactive and reactive actions to ensure that service performance meets the agreed targets.

Component Capacity Management focuses on the management, control, and prediction of the performance, utilization, and capacity of IT technology components.

It ensures that the components of the IT infrastructure that have limited resources are monitored and measured. Collected data from these components should be recorded, analyzed, and reported.

Here too, automated thresholds should be used to manage all components. This ensures the speedy identification of breached or threatened component usage or performance so that cost-effective solutions can be implemented.

Supplier Management:

In Service Design, the Supplier Management process aims to ensure that suppliers meet the terms, conditions, and targets of their contracts and agreements. It's also implemented as a means to attain a higher value for money from suppliers and the services they offer.

The Supplier Management process is driven by a supplier strategy and policy identified during the Service Strategy stage. The consistent and effective implementation of Supplier Management depends on the establishment of a Supplier and **Contract Database (SCD)** as well as on clearly defined roles and responsibilities.

The SCD should record all supplier and contract details, including the types of services or products provided by each supplier. It then serves as a comprehensive reference for use across all Supplier Management procedures and activities.

A comprehensive SCD provides information in the areas of

- supplier categorization
- establishment of new suppliers, their assessment, and the establishment of associated contracts
- contract renewal and termination, and
- management of supplier and contract performance

Supplier Management aims to manage all suppliers and contracts needed to support the provision of IT services. Its objectives are to

- secure good value for money from suppliers and contracts
- align contracts with suppliers to business needs and targets
- manage relationships with suppliers
- manage supplier performance, and
- maintain the organization's supplier policy and supporting SCD

The Supplier Management aims to negotiate and agree on contracts with suppliers and to manage these contracts through their lifecycles.

The contracts managed by the Supplier Management process are - like all contracts -legally-binding agreements between two or more parties.

A formal contract should be used when an organization has external supply arrangements that make a significant contribution to the delivery and development of the business. This type of contract is also used for high-value and strategic relationships.

The elements of a basic contract include

- basic terms and conditions
- service description and scope
- service standards, and
- management information

The **basic terms and conditions** of a contract outline the duration of the contract, the parties and locations involved, and the scope of the contract, as well as definitions and the commercial basis of the contract.

The **service description and scope** section of the contract details the functionality of the provided services and the extent of the agreement. It also considers all constraints -such as performance, availability, capacity, technical interface, and security constraints - on service delivery. Service functionality may be explicitly defined, or - in the case of well-established services - included by reference to other established documents like the Service Portfolio or the Service Catalog.

The **service standards** outlined in the contract define the minimum acceptable standards and service measures regarding performance and quality.

Management information is all the information about operational performance that must be reported by the supplier. Management information should concentrate on the most important - or headline - reporting measures on which the relationship will be assessed. Key Performance Indicators (KPIs) and balanced scorecards may form the core of reported performance information.

A basic contract contains workload ranges, which are the volume limits within which service standards apply or for which specific pricing rules apply.

The responsibilities and dependencies described in the contract depict the obligations of the organization and the supplier regarding communication, contacts, and escalation.

The service levels outlined in the contract must be realistic, measurable, and aligned to the organization's needs. The contract should also support the targets agreed on in Service Level Requirements (SLRs) and SLAs.

Maintaining the SCD forms an integral part of the Supplier Management process. Supplier Management is responsible for recording all supplier and contract details, as well as details of the type of service or product provided by each supplier, in the SCD. It is also responsible for recording the relationships of contracted services or components with other associated Configuration Items (CIs).

The SCD assists with the following integral Supplier Management activities:

- categorization of suppliers
- evaluation and setup of new suppliers and contracts
- establishment of new suppliers
- management of supplier and contract performance, and
- contract renewal and termination

The Capacity and Supplier Management processes are the responsibility of the Capacity and Supplier manager respectively. The responsibilities of the capacity manager include

- identifying capacity requirements with the service level manager
- understanding the existing use of IT infrastructure and services, as well as the maximum capacity of each component

- performing sizing on all suggested new services and systems to determine capacity requirements, and
- predicting future capacity requirements

Other responsibilities of the capacity manager include ensuring that there is adequate IT capacity to meet required levels of service, that senior IT management is appropriately guided on how to match capacity and demand, and that the use of existing capacity is optimized.

The capacity manager is also responsible for the production, regular review, and revision of the capacity plan, and for identifying current usage and predicted requirements during the period covered by the plan.

The supplier manager is responsible for ensuring that all the objectives of Supplier Management processes are met. The responsibilities of the supplier manager include

- supporting the development and review of SLAs, contracts, agreements, and any other documents for third-party suppliers
- ensuring good value for money from all IT suppliers and contracts
- ensuring that all IT supplier processes are consistent and interface with supplier strategies, processes, and standard terms and conditions
- maintaining and reviewing the SCD
- regularly performing a review and risk analysis of all suppliers and contracts, and
- ensuring that any supporting contracts, agreements, or SLAs developed align with those of the organization

Information Security Management and ITSCM:

In Service Design, Information Security Management (ISM) provides the focus for all aspects of IT security. It involves management activity within the corporate governance framework. It provides strategic direction for security activities and ensures that all objectives are achieved.

It also ensures that information security risks are managed appropriately and that enterprise information resources are responsibly used.

Objectives of Information Security Management: ISM:

The objectives of ISM are to

- ensure that agreed levels of service availability are supported
- protect the confidentiality of data and systems
- protect the integrity of information, and
- ensure authenticity and non repudiation of transactions and information

ISM aims to ensure that agreed levels of service **availability** are supported. It helps do this by ensuring that usable information is provided when required and that the providing systems can resist relevant attacks and recover from or prevent failures.

ISM aims to protect **confidentiality** of data and systems. This is accomplished by ensuring that information is disclosed only to those people who have a right to see and use it.

ISM aims to protect **integrity** of information. This is done by ensuring that information is complete, accurate and protected from unauthorized modification.

ISM aims to ensure **authenticity** and non repudiation of all business transactions and information trades between enterprises or with partners to ensure that organization is deemed trustworthy.

It is important to have a comprehensive ISM policy because, to be effective, information security must align closely with business security and business needs. The necessary security measures for monitoring and enforcing the ISM policy should also be in place.

Effective ISM entails managing security risks, monitoring processes to ensure compliance, and providing feedback on effectiveness. It should also include developing a communications strategy and providing any necessary training on security policies and measures.

An effective ISM process and framework should include the following components:

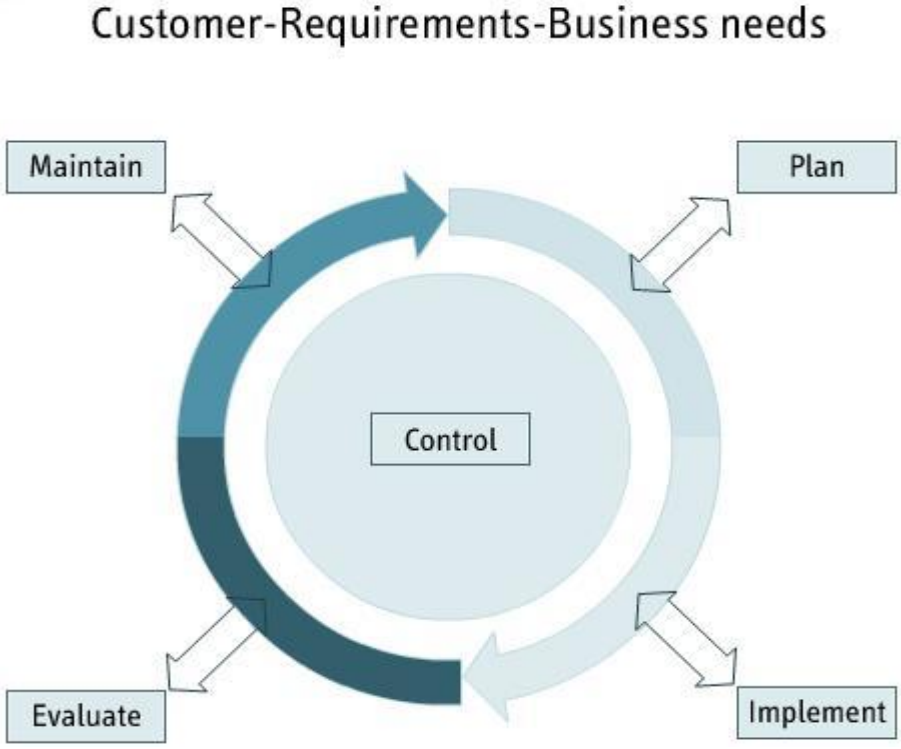
- an information security policy
- an Information Security Management System (ISMS)
- a comprehensive security strategy that aligns to business objectives, strategies, and plans
- an effective security organizational structure
- security controls to support the information security policy
- monitoring processes aimed at ensuring compliance and providing feedback on efficacy
- a communications strategy, and
- a security training plan

The information security policy should consider all elements of a security strategy, and must align with business needs. It may include several more specific security policies.

Because the information security policy defines the entire organization's attitude towards security matters, it should apply across the organization. The policies it includes must be appropriate and supported by senior management. Some examples of what the information security policy may include are

- an overall policy for securing information
- a policy defining the difference between appropriate and inappropriate use of IT assets
- an access control policy
- a password control policy, and
- an e-mail policy

The **ISMS** provides a system for creating a cost-effective information security program that aligns with business objectives. It contains standards, management procedures, and guidelines that support the information security policy. ISMS consists of five main elements



The **plan** element of the ISMS aims to identify and create the appropriate security measures, based on knowledge of organizational needs. To determine organizational security needs, you gather information from sources such as business and service risk assessments, plans, and strategies, Service Level Agreements (SLAs), and Operational Level Agreements (OLAs). You also need to consider the legal, moral, and ethical responsibilities associated with information security, the amount of funding available, prevailing organization culture, and attitudes to security.

The **implement** element of ISMS aims to implement the appropriate procedures, tools, and controls to underpin the information security policy. This involves managing awareness and training in security needs, accounting for assets and classifying information, establishing personnel, physical, and system security, managing access rights, and implementing procedures for handling security incidents. This element should also include a mechanism for ensuring continual improvement in ISM.

The **evaluate** element of ISMS aims to supervise and check compliance with the information security policy. This involves performing regular audits of the technical security of IT systems, and providing required information to external auditors and regulators.

The **maintain** element of the ISMS strives to improve the implementation of security measures and controls and specified security agreements.

The **control** element of ISMS aims to establish a management framework that can manage information security in the organization. It aims to establish an organizational structure to prepare, approve and implement information security policy. It also allocates responsibility and establish control.

The outcomes of ISM that is properly implemented are

- strategic alignment between IT and the business
- value delivery
- improved risk management
- improved performance management
- improved resource management, and
- business process assurance

IT Service Continuity Management (ITSCM):
The IT Service Continuity Management (ITSCM) process supports the overall Business Continuity Management (BCM) process by ensuring that the required IT technical and service facilities can recommence within required business timescales.

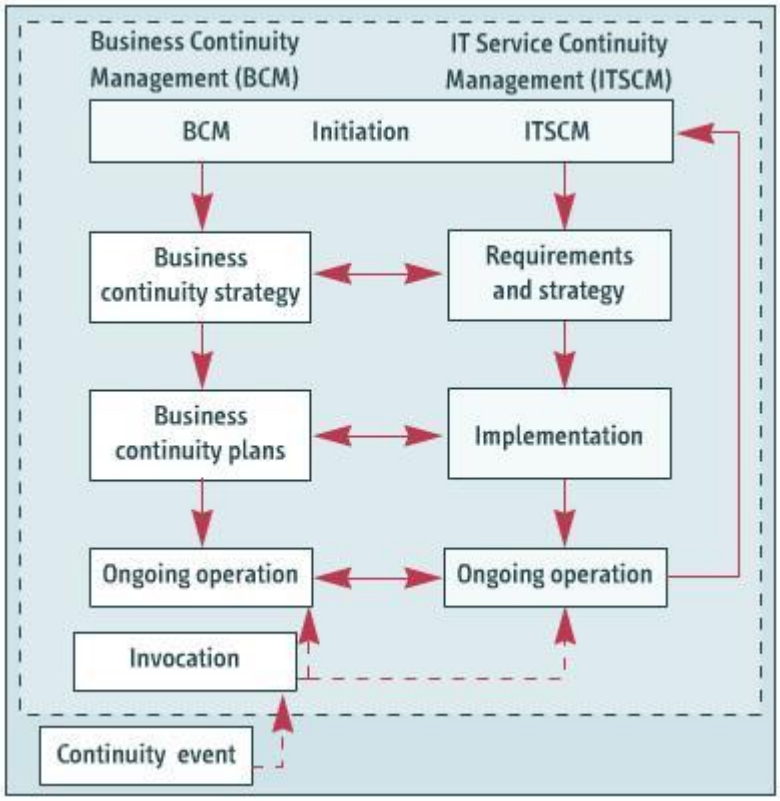
Objectives of ITSCM:
The objectives of ITSCM are to

- maintain IT Service Continuity and recovery plans that support overall Business Continuity Plans (BCPs)
- complete regular Business Impact Analysis (BIA) exercises to ensure that all continuity plans align with changing business requirements
- perform regular risk analysis and management exercises, especially together with the business and the Availability Management and Security Management processes
- give advice and guidance to other business and IT areas on all continuity and recovery-related issues, and
- ensure that appropriate continuity and recovery mechanisms are in place to meet agreed business continuity targets

ITSCM aims to assess the effect of any changes on the IT service continuity plans and IT recovery plans. It also strives to ensure that cost-justifiable, proactive measures to improve service availability are implemented.

Furthermore, it aims to establish the necessary contracts with suppliers - in alignment with the Supplier Management process - to provide the recovery capability needed to support all continuity plans.

ITSCM is a cyclic process that should occur throughout the Service Lifecycle, to ensure that newly developed service continuity and recovery plans are kept aligned with BCPs and business priorities.



The ITSCM lifecycle includes four stages

1. initiation
2. requirements and strategy
3. implementation, and
4. ongoing operation

Initiation is the first stage of the lifecycle. It applies to the whole organization and includes activities such as policy setting, specifying terms of reference, allocating resources, defining the project organization and control structure, and agreeing on project and quality plans.

Setting business **requirements and strategy** is the second stage of the Lifecycle. Business Impact Analysis (BIA) and risk assessment are also performed in this stage, and required risk reduction measures and recovery options are recorded.

Implementation is the third stage of the lifecycle, in which the strategy has been approved and the IT service continuity plan is produced in alignment with the BCP. The activities in this stage include developing ITSCM plans that ensure that the necessary information for critical systems, services, and facilities will still be provided or will be reinstated within a reasonable period after a failure.

Ongoing operation is the final stage of the lifecycle. Its activities include raising awareness through education and training, performing reviews and testing, and Change Management.

The initiation and requirement stages are BCM activities during which the ITSCM process provides support. These initial activities result in a business continuity strategy that focuses on business processes and associated issues.

An ITSCM strategy is produced after the business continuity strategy, once the role of IT services within the strategy has been determined. Both strategies support each other.

The activities in the implementation stage depend on the extent to which continuity facilities have been applied within the organization. For example, certain parts of the business could have established their own BCPs.

Successful implementation of ITSCM relies on identifying critical business processes, and on the analysis and coordination of required technology and supporting IT services.

The Change Management process, which forms part of the ongoing operation stage, should ensure that all changes are assessed to determine their potential impact on the ITSCM plans.

The security manager and IT service continuity manager are respectively responsible for ISM and ITSCM.

Responsibilities of Security Manager:
These are some of the responsibilities of the security manager:

- developing and maintaining the information security policy and supporting policies
- ensuring appropriate authorization, commitment to, and approval of policies by senior IT and business management
- communicating and publicizing the information security policy to all the appropriate areas
- ensuring that the information security policy is enforced and abided by, and
- identifying and classifying IT and information assets, as well as the necessary level of protection

Responsibilities of ITSCM Manager:
These are some of the responsibilities of the IT service continuity manager:

- performing BIAs for all services
- implementing and maintaining the ITSCM process to ensure that agreed targets are met
- ensuring that all ITSCM plans, risks, and activities support and align with BCM plans, risks, and activities, and
- performing risk assessment and management to prevent failures whenever practical and cost-justifiable

The IT service continuity manager is also responsible for developing and maintaining the ITSCM strategy and assessing any possible service continuity problems and, if necessary, using the service continuity plan.

Service Transition:

Service Transition Processes and Policies:

The Scope and Policies of Service Transition:

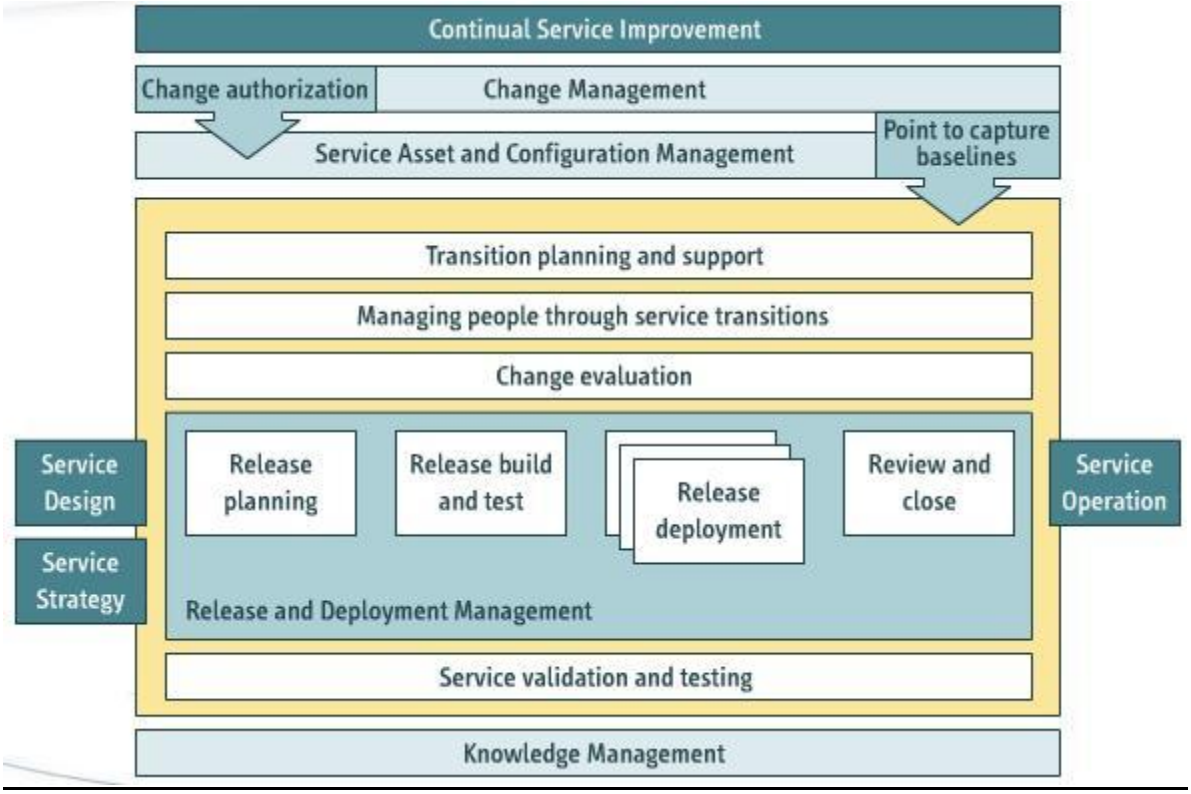
Service Transition ensures that new or modified services meet the business expectations documented in the Service Strategy and Service Design stages of the lifecycle.

Processes included in the Service Transition stage are transition planning and support, Change Management, Service Asset and Configuration Management (SACM), Release and Deployment Management, service validation and testing, change evaluation, and Knowledge Management.

Objectives of Service Transition:

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 appropriate expectations** about the performance and use of new or changed IT services
- ensure that service changes create the expected **business value**, and
- **provide accurate information** about services and service assets



Scope of Service Transition:

The scope of Service Transition includes

- managing the complex changes to services and Service Management processes
- introducing new services or making changes to existing services
- decommissioning and discontinuing services, applications, or service components when relevant

- transferring services to and from other IT service providers - for example, due to changes in outsourcing, use of co-sourcing, or company mergers

Benefits to organization by Service Transition:
Adopting and implementing consistent approaches during the Service Transition stage can help organizations to

- estimate project costs more accurately
- adopt changes more readily
- increase confidence that new or changed IT services can be delivered to specification
- improve control of service assets and configurations
- reduce delays, and
- enable more efficient resource sharing

Policies of Service Transition:
ITIL® provides 14 policy examples that can guide organizations in adopting best practices for the successful transition of IT services. Each policy has associated principles and best practices.

Policy 1: Define and implement a formal policy for Service Transition

- The appropriate management team should define, document, and approve a formal policy for Service Transition. It should also be communicated to all relevant stakeholders.
- The policy should clearly state the objectives and should be aligned with the overall governance framework.
- The policy should also demonstrate the commitment of sponsors and senior management to deliver predicted outcomes from any changes in IT services.
- The policy should outline processes that integrate teams while maintaining clear lines of accountability and responsibility. They should also specify how changes are delivered - as releases, for example.

Policy 2: Implement all changes to services through Service Transition

- All service changes should be managed through the Service Transition stage, with the exception of standard changes that follow procedures defined during the stage.
- Service changes should be managed from a single focal point and their scope must be documented.
- Access and permissions for changes should be restricted, and all updates to changes and releases should be recorded against service assets or Configuration Items in the Configuration Management System (CMS).
- Standardized methods and procedures should be used to ensure efficient and prompt handling of all changes. Late requests for changes that can't be properly managed shouldn't be accepted.

Policy 3: Adopt a common framework and standards

- Service Transition should be based on a common framework of standard re-usable processes and systems. This will improve integration of the parties involved in Service Transition and reduce variations in the processes.
- Best practices for this policy are to gain buy-in for standardization, and to support consistent processing through the use of automation and a clear framework within which the work is carried out. The framework should also be controlled using Change Management and SACM processes.

Policy 4: Maximize re-use of established processes and systems

- New processes are developed with re-use in mind.
  Principles:
- Re-use established protocols wherever possible
- develop re-usable standard Service Transition models to build up experience and confidence,

- implement industry best practices for standardization and integration
- Capture data and information from the original source to reduce errors and aid efficiency.

Best Practices:

- Integrating Service Transition into overall Service Management using the organization's project management practices and existing communication channels and processes. Service Transition models should be designed to enable easy customization to suit specific circumstances.

Policy 5: Align Service Transition plans with business needs to maximize the value of the change.

- Manage the resources required to package, build, test, and deploy a release successfully.
- Provide clear and comprehensive plans that enable the customer and business to align their change activities with the Service Transition plans.

Principles:

- set customer and user expectations about how a service can be used effectively to enable business change
- provide information and establish processes to enable integration of a release into business processes and services
- ensure that the transitioning service can be used in accordance with the specified requirements and constraints to improve satisfaction
- transfer knowledge to customers and other stakeholders to increase their capability to use the new or changed service
- monitor and measure the use of the service and underlying technology, during deployment and early life support, and
- compare actual to predicted performance of the service to reduce variations in service capability and performance

Policy 6: Establish and maintain relationships with stakeholders throughout Service Transition to set expectations about the new or changed IT service.

- Set expectations about service performance and how the service will enable business change.
- Communicate changes to stakeholders and ensure good quality information about the transition is readily available.

Best Practice:

- An associated best practice is validation from stakeholders that the new service can be used according to requirements and constraints.
- Share plans with stakeholders, build relationships with them, and gain commitment from key suppliers during and following transition.

Policy 7: Establish effective controls and disciplines throughout the Service Lifecycle

Associated principles and best practices relate to

- general management of service assets and configurations throughout the lifecycle
- definition of roles and responsibilities
- Regular configuration and process audits to monitor the change lifecycle

Policy 8: Provide systems for knowledge transfer and decision support.

- As best practices, you need to provide easy access, presentation, and reporting tools for the SKMS and CMS.
- After each Service Transition is complete, it's useful to document a summary of the predicted and unpredicted effects of the change in terms of capability, performance, and risk.
- Principles associated with providing systems for knowledge transfer include providing quality data, information, and knowledge at the right time to the right people to reduce effort spent waiting for decisions and consequent delays.

- Ensure that there is adequate training and that the quality of the data and documentation is acceptable.
- Also establish a definitive source of knowledge and share this information with relevant stakeholders across the Service Lifecycle. It's helpful to provide consolidated information to enable change and effective decisions.

Policy 9: Plan release packages in ways that provide the agreed levels of traceability in a cost-effective and efficient way.

- Ensure relevant stakeholders approve the release policy and that the policy is planned well in advance.
- Planned release and deployment mechanisms should ensure component integrity during installation, handling, packaging, and delivery.
- Resource use should be coordinated during release and optimized to reduce costs.
- The risks of a failed release should be included in the plans, and assessed and managed.
- Emergency releases should be planned and managed in line with emergency change procedures.

Policy 10: anticipate and manage course corrections:

- Train employees to identity, make, and manage course corrections, and to apply necessary variations to original Service Transition plans within prescribed and understood limits.
- Encourage stakeholders to expect changes and understand that these are necessary and beneficial.
- Predict future changes and use end-of-transition debriefing sessions to inform others.

Policy 11: proactively manage resources across Service Transition:

To manage resources proactively, you need a capable team to implement the change through all lifecycle stages. You should establish shared, dedicated, and specialist resources across Service Transition activities to eliminate delays and optimize the use of resources.

Automate repetitive and error-prone processes to improve the effectiveness and efficiency of key activities.

Policy 12: ensure early involvement in Service Lifecycle:

By ensuring early involvement in the Service Lifecycle, you can maximize early detection of potential faults or weaknesses, and of changes that won't deliver the expected benefits. This generally results in much lower costs than if you identify problems only later on.

Policy 13: provide assurance of the quality of new or changed service:

- Verify that the proposed changes can meet specified business requirements and deliver the anticipated business benefits.
- Identify risks and measure and reduce known errors.
- Test design and execution should be managed and delivered independently from the service designer or architect and developers. Additionally, test environments need to reflect live environments to the greatest degree possible to allow for relevant results.

Policy 14: Quality Improvement Policy:

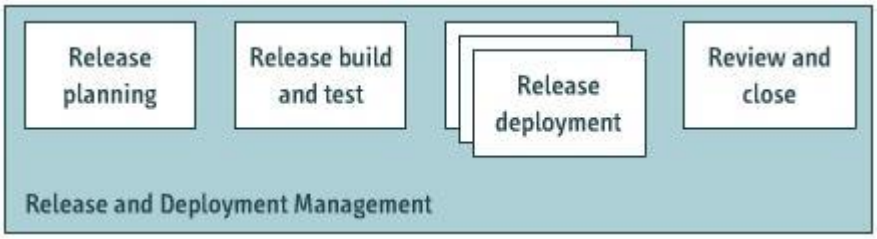
The final policy proposed by ITIL® is to improve quality proactively during the Service Transition stage. Three principles are associated with implementing this policy:

- detecting and resolving issues during the transition stage to reduce the likelihood of errors occurring during the Service Operation stage
- managing and reducing issues and errors during Service Transition to reduce costs and the need for re-work, and

- aligning Incident and Problem Management with the Service Operation processes to help measure and manage their impact

Release and Deployment Management in Service Transition:

Release and Deployment Management process guides the planning, scheduling, building, testing, and deployment of releases.



Objectives of Release and Deployment Management:

- Define and sign off Release and Deployment Management plans with stakeholders
- Create and test packages that are compatible with Configuration Items (CIs).
- maintain the integrity of a release and all of its associated components
- deploy release packages from the definitive media library (DML) to the live environment in line with agreed plans and schedules
- ensure that all release packages can be tracked, installed, tested, verified, and canceled if appropriate
- ensure that change is properly managed during service release and deployment
- ensure that any new or changed service can deliver the agreed utility and warranty
- record and manage deviations and risks, and take necessary corrective action, and
- ensure knowledge transfer to keys stakeholders to optimize the use of new or changed IT services

Scope of Release and Deployment Management:

The scope of Release and Deployment Management includes the processes, systems, and functions required to package, build, test, and deploy releases into live environments.

It also includes those processes needed to establish IT services and formally hand them over to the Service Operation functions.

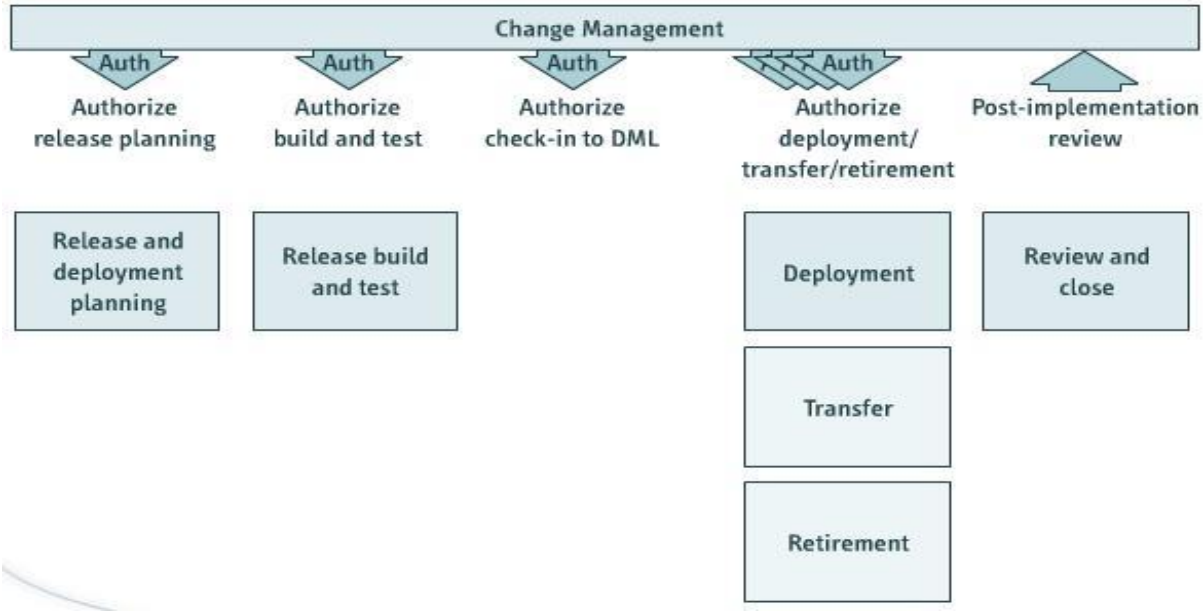
The scope of the Release and Deployment Management process also includes all CIs. Examples Include

- physical assets, such as a server or network
- virtual assets, such as a virtual server or virtual storage
- applications and software
- training for users and IT staff, and
- services, including all related contracts and agreements

The 4 Phases of Release and Deployment Management:

The Release and Deployment Management process has 4 phases –

1. release and deployment planning
2. release build and test
3. deployment, and
4. review and close



Phase 1: Release and Deployment Planning:

- The plans for creating and deploying a release are generated in the release and deployment planning phase.
- This phase starts with Change Management authorization to plan a release, and ends with Change Management authorization to create the release.

The release and deployment plan for a release should specify

- the scope and content of the release
- associated risks
- stakeholders affected by the release
- the team responsible for the release
- the deployment schedule for the release
- the delivery and deployment strategy for the release
- resources required for the next phase, and
- the pass or fail criteria for the release

Activities that take place during release and deployment planning:

- Developing build plans, design specifications, and environment configuration requirements.
- Establish release logistics and schedules
- Define a configuration baseline for the build environment
- Test the build and related procedures, and
- Assign resources, roles, and responsibilities for performing key activities.

Phase 2: Release build and test:

- During the release build and test phase, a release package is built, tested, and checked into the DML.
- The phase starts with Change Management authorization to build a release and ends with Change Management authorization for the base lined release package added into the DML by Service Asset and Configuration Management (SACM).

Activities that take place during release build and test:

- Manage the build and test environments. This includes controlling access rights to physical and technology components and managing environmental issues - such as cooling, fire precautions, accessibility, and safety measures.
- Manage and document build and test activities, such as those related to version control, baseline management, test report generation, and output control.

Other activities associated with this phase include

- verification activities - for example, checking that prerequisites are met before a build or test begins
- preparation activities - preparing and controlling the service release ready for deployment to the live environment, and
- promotion activities - promoting or handing over the service release to the next stage or team

Phase 3: Deployment:

- The deployment phase starts with Change Management authorization to deploy a release package to one or more target environments. It ends with handover to the Service Operation functions and early-life support.

Activities that take place during deployment:

- Develop a detailed implementation plan, including details of who is responsible for each aspect of implementation.
- Make sure deployment stakeholders are sufficiently confident in a service release to deploy it, own their aspects of deployment, and be committed to the deployment.

Phase 4: Review and close:

When reviewing a deployment, you need to capture experiences and feedback about customer, user, and service provider satisfaction.

You need to check that any problems, known errors, and workarounds are documented and accepted by the affected stakeholders.

You should also highlight quality criteria that weren't met and ensure that required actions, necessary fixes, and changes are complete.

Before closing the Release and Deployment Management process, you need to ensure that there isn't any remaining capability, resource, capacity, or performance issues to address. To do this, it's useful to review performance targets, achievements, and the risk register.

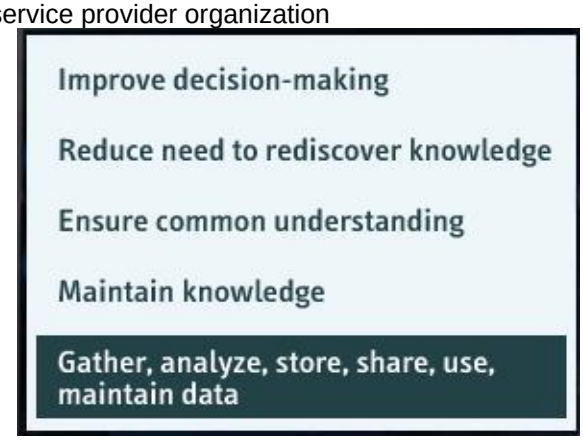
You also need to ensure that any redundant assets have been removed, and make final checks to ensure the service is ready for transition from early-life support into operation.

So in this phase, experience and feedback are captured, performance targets and achievements are reviewed, and lessons are learned.

Knowledge Management in Service Transition:
The Knowledge Management process involves sharing perspectives, data, ideas, experience, and information, and ensuring that these are available in the right place and at the right time. This enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge.

Objectives of Knowledge Management:
Knowledge Management has several objectives:

- to improve management decision-making by ensuring reliable and secure knowledge, information, and data is available throughout the Service Lifecycle
- to reduce the need to rediscover knowledge, thereby improving efficiency, quality of service, and customer satisfaction, and reducing the cost of service
- to ensure that employees have a clear and common understanding of the value that IT services provide to customers and users, and the ways in which that value is realized
- to maintain a Service Knowledge Management System (SKMS) that provides controlled access to appropriate knowledge, information, and data for the intended audience, and
- to gather, analyze, store, share, use, and maintain knowledge, information, and data throughout the service provider organization



SKMS – Service Knowledge Management System:
An SKMS is a set or tools and databases used to manage knowledge, information, and data, with the aim of improving the overall efficiency and effectiveness of all stages of the Service Life cycle.

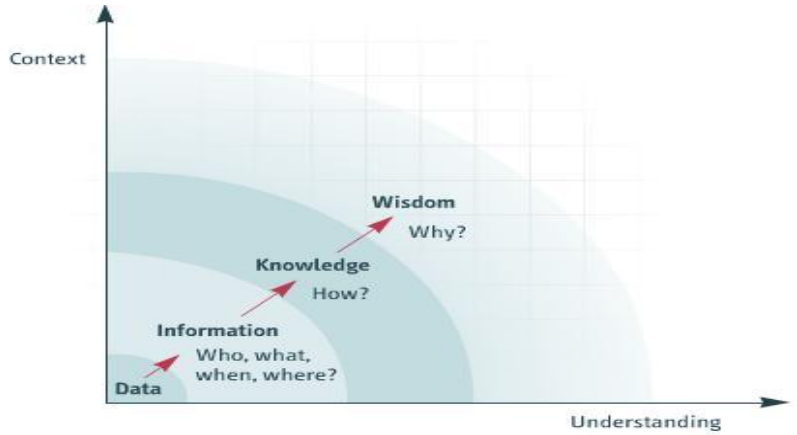
An SKMS enables people to benefit from the knowledge and experience of others, supports informed decision-making, and improves the management of IT services.

Knowledge that's especially important during the Service Transition stage includes the identities of stakeholders affected by new or changed IT services, acceptable risk levels, service performance expectations, and available resources and timescales.

The ability to deliver a quality service or process relies strongly on the ability of those involved to respond appropriately in different circumstances. In turn, this ability depends on people's understanding of each situation, and of the relevant service or process in that context.

The quality and relevance of stakeholders' knowledge depends on the accessibility, quality, and continued relevance of the information that's made available via an SKMS.

DIKW Structure:
Data-to-information-to-Knowledge-to-Wisdom (DIKW) is a structure that can help you understand and implement effective Knowledge Management processes.
The DIKW structure includes 4 elements.



Data:
Data refers to discrete facts. Most organizations capture large amounts of data in highly structured databases. These may include Service Management, service asset, and Configuration Management databases.

The key Knowledge Management activities associated with data are identifying relevant data, capturing the data accurately, analyzing and synthesizing the data, maintaining data integrity, and storing data to ensure an optimal balance between its availability and the use of resources.

Information:
Information is data to which context has been added to improve understanding. Information is typically stored in semi-structured media such as documents or e-mail.

The key Knowledge Management activity associated with information is ensuring that information is easy to capture, query, find, re-use, and learn from. This helps ensure that mistakes aren't repeated and that work isn’t duplicated.

Knowledge:
Knowledge is dynamic and context-based, and serves to facilitate decision-making. It's composed of the tacit experiences, ideas, insights, values, and judgments of individuals. People gain knowledge from their own and their peers' experiences, and through the analysis of both data and information. Through the synthesis of these elements, new knowledge is created.

In Service Transition, this knowledge isn't based solely on the transition in progress. Instead, it's also based on experiences of previous transitions, and awareness of recent and anticipated changes - which experienced employees accumulate unconsciously overtime

Wisdom:
Wisdom refers to the application of knowledge and strong common sense in given contexts to create value. It’s illustrated in well informed decisions.

Example for DIKW process:
As an example, the DIKW process may begin with gathering **data** such as the date and time at which an incident was logged.

This data can be transformed into **information** by combining the start time, end time, and priority of many incidents to find the average time it takes to close incidents of the same priority.

Using this average time information, you can develop **knowledge**. For example, you might analyze the information and find that the average time to close incidents with the given priority has increased by about 10% since a new version of a service was released.

From this, **wisdom** can be attained. For example, wisdom may involve recognizing that the increase in the time it takes to close the incidents is due to poor-quality documentation for the new version of the service. You can then decide how best to improve the documentation.

Asset Transition, Service Support and Testing:
The Service Asset and Configuration Management (SACM) process ensures that the assets required to deliver IT services are properly controlled, and that accurate and reliable information about those assets is available when and where it's needed.

This information includes details of how the assets have been configured and the relationships between assets.

To better understand the scope and purpose of Asset and Configuration Management, it's useful to distinguish between

- a service asset, and
- a Configuration Item (CI)

A service asset is any resource or capability that could contribute to the delivery of an IT service. Examples of service assets are a virtual server, a physical server, a software license, information stored in a Service Management system, or knowledge held by a senior manager.

A CI is a service asset that has to be managed to deliver an IT service. All CIs are service assets, although service assets aren't all CIs. Examples of CIs are servers and software licenses.

Every CI must be under the control of Change Management. Information that's stored but that isn't under the control of Change Management may be a very valuable asset, but it isn't a CI.

Objectives of SACM:
SACM has several objectives

- to ensure that assets are identified, controlled, and properly cared for throughout their lifecycle
- to ensure the integrity of CIs by establishing and maintaining an accurate and complete Configuration Management System (CMS)
- to identify, control, record, report, audit, and verify services and other CIs, including versions, baselines, constituent components, and service attributes and relationships
- to maintain accurate configuration information about the historical, planned, and current state of services and other CIs, and
- to support efficient and effective Service Management processes by providing information that allows for effective decision-making

SACM ensures that CIs are identified, base lined, and maintained, and that changes to them are controlled.

So its scope includes management of the complete lifecycle of every CI. For example, a virtual server will be used in providing in house access to company policies. The asset is identified, its baseline performance is measured, the system is maintained through the transition, and its performance is reviewed once the service is tested.

SACM is responsible for ensuring releases into controlled environments and operational uses are formally authorized. It also provides a configuration model of services and service assets by recording the relationships between **CIs.**

Asset types covered by SACM include

- non-IT assets, and
- fixed assets

SACM may cover non-IT assets, work products used to develop the services and CIs required to support the service that would not be classified as assets by other parts of the business.

The scope includes interfaces to internal and external service providers where there are assets and CIs that need to be controlled - for example, when assets are shared.

Most organizations use a fixed Asset Management process to track and report the value and ownership of fixed assets throughout their lifecycles.

Fixed Asset Management involves maintaining an asset register that records financial information about an organization's fixed assets. It isn't usually under the control of the same business unit that manages IT services. However, the SACM process should be applied for fixed assets under the control of IT, and there should be well-defined interfaces between SACM and fixed Asset Management.

Data from the asset register may also be integrated with the CMS to provide a more complete view of the CIs.

Transition Planning and Support:
The purpose of transition planning and support process is to provide overall planning for Service Transition processes and to coordinate the resources that they require.

Objectives of Transition Planning and Support:
The objectives of transition planning and support are to monitor and improve the performance of the Service Transition stage and to

- coordinate resources to achieve objectives
- coordinate activities to run transition planning smoothly
- establish new or changed IT services
- Establish new systems, tools, processes and measurement methods to measure Service Design requirements are being met.
- ensure the adoption of a common framework
- provide clear plans, and
- identify, manage and control risks

Scope of Transition Planning and Support:
The scope of transition planning and support includes

- maintaining policies – RACI Matrix
- guiding changes
- Coordinating activities so that multiple transitions can happen simultaneously.
- planning resource requirements, and
- reviewing and improve planning and support activities

Service Validation and Testing:
The service validation and testing process provides quality assurance within the Service Transition domain. It verifies that a new or changed IT service is fit for purpose and fit for use.

Service validation and testing is the last process in Service Transition. Once this process completes, the IT service is moved into a live environment.

Objectives of Service Validation and Testing:
Purpose - To ensure that a new or changed IT service matches its design specification and will meet business needs. Objectives are,

- quality assurance for a release, its constituent service components, the resultant service, and the service capability delivered by a release
- validation that a service is "fit for purpose" -or will deliver the required utility
- assurance that a service is “fit for use" - or will deliver the agreed warranty
- confirmation that customer requirements for the new or changed service are correctly defined
- planning and implementation of a structured validation and testing process, and
- ongoing review that identifies, assesses, and addresses issues, errors, and risks throughout the Service Transition stage

Testing directly supports the Release and Deployment Management process by ensuring that appropriate levels of testing are performed during Release and Deployment Management activities.

It evaluates the detailed service models to ensure that they are fit for purpose and fit for use before being authorized to enter Service Operation, through the service catalogue.

The output from testing is used by the change evaluation process to provide information on whether the service is formally judged to be delivering the service performance with an acceptable risk profile.

Testing can be classified according to the end user of a service product.

- Customer Service Testing
- Testing of in-house services

With **customer service testing**, a Service Level Agreement (SLA) guides testing and aims to ensure that the service provider takes responsibility for delivering, operating, and maintaining customer or service assets at the agreed levels.

Service validation and testing can be applied throughout the Service Lifecycle to quality assure any aspect of a service and the service providers' capability, resources, and capacity to deliver a service or service release successfully.

When validating and testing an end-to-end service, the interfaces to suppliers, customers, and partners are important.

Testing is as important for **in-house services** as for services provided to external customers.
It includes testing of new or changed IT services or service components, and examines the behavior of these in the target business unit, service unit, deployment group, or environment

This environment could include aspects outside the control of the service provider - for example, public networks, user skill levels, or customer assets.

Change Management for IT Services:
Change in relation to the IT function refers to the addition, modification, or removal of anything that could have an effect on IT services. This includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and Configuration Items (CIS).

Changes may be made proactively - for example, when organizations are actively seeking business benefits such as reduction in costs, improved services, or increased ease and effectiveness of support.

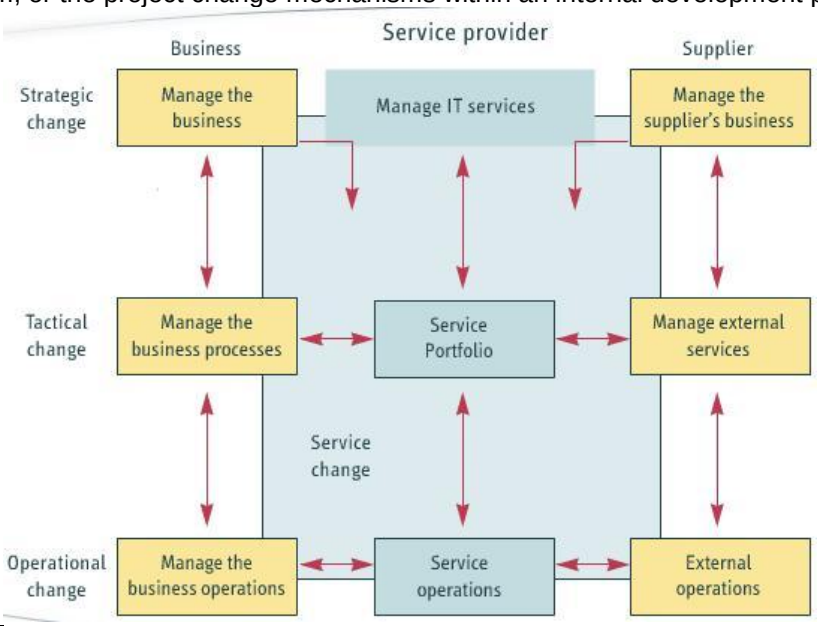
Alternatively, changes may be made reactively, in order to respond to errors that occur or adapt to changing circumstances.

Change Management is the process in the Service Transition stage that's responsible for controlling the lifecycle of all changes to IT services. Its primary purpose is to ensure that only beneficial changes are made and that these result in minimal disruption.

Objectives of Change Management:
The purpose of the Change Management process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimal disruption to IT services. To accomplish this, Change Management aims to

- maximize value
- align services (align IT services with business needs)
- control and document changes, and
- optimize risk (implement only changes with acceptable risk)

Change Management must interface with business Change Management and with the supplier's Change Management. This may be an external supplier within a formal Change Management system, or the project change mechanisms within an internal development project.



Typically all changes are initialed via a documented request of some kind. The level of detail and the type of authorization required generally depends on the nature of the change.

Changes are often categorized as major, significant, or minor - depending on the level of cost and risk involved, and on the scope of a change and its relationship to other changes.

The way a change is categorized may be used to identify an appropriate change authority.

A best practice is for an organization to predefine change models and apply them to appropriate changes when they occur, based on their own environment and needs.

A change model defines an agreed sequence of steps and support tools for handling a particular type of change. It helps ensure that changes are handled consistently and in alignment with predefined timescales.

As well as outlining steps for handling a particular type of change, a change model should define any dependencies among the steps or required co-processing. It should also include a list of responsibilities, the people to whom these are assigned, and timescales and thresholds for completion of the defined steps.

Finally, a change model should define an appropriate escalation procedure, identifying who should be contacted and when.

The three main informational documents associated with initiating and controlling Change Management are

1. change proposals
    - Submitted by Service Portfolio Management process or program or project management to Change Management before chartering new or changed IT services.
    - Gives a high-level description of the proposed change, including business outcomes to be supported, and utility and warranty to be provided.
    - Should also include a schedule and a full business case including risks, alternatives, and budget and financial expectations.
    - Authorization of the change proposal doesn't authorize implementation of the change but simply allows the service to be chartered so that Service Design can commence.

2. RFCs
    - An **RFC** is a formal and documented - either written or electronic - proposal for a change to be made. It includes details of the proposed change.
    - RFCs are only used to submit requests. They are not used to communicate the decisions of Change Management or to document the details of the change.
    - RFCs could include a service desk call, a project initiation document, or a specific RFC template.

3. change records
    - A **change record** is a record that documents the lifecycle of a single change, and is used to manage the lifecycle of that change.
    - A change record is created for every RFC, including those that are subsequently rejected.
    - A change record should reference the CIs affected by the proposed change, and all the required information about a change, including information from the RFC.
    - Change records may be stored in the CMS or elsewhere in the Service Knowledge Management System (SKMS).

Change proposals are generated by various processes such as Service Portfolio Management, Continual Service Improvement, Service Level Management, and Service Catalog Management

The Change Management now reviews each change proposal and the current change schedule, identifies any potential conflicts or issues, and authorizes the proposed change or documents the issues that need to be resolved.

Once a change proposal is authorized, the change schedule should be updated to include an outline of implementation dates for the change.

After the new or changed service is chartered, RFCs are used to request authorization for specific changes. These RFCs should be associated with the change proposal so that Change Management has a view of the overall strategic intent and can prioritize and review the RFCs appropriately.

The three basic types of service changes are

- standard
- emergency, and
- normal

A **standard change** is a pre-approved change, with authorization effectively given in advance.

A defined trigger initiates a standard change. An example could be a request from a user to reset a password, or to increase the size of the user's mailbox in an e-mail application. A standardized procedure should exist for implementing the change, which occurs commonly or is expected.

Standard changes typically involve low risks and costs, and low levels of effort to implement.

An **emergency change** has to be implemented as soon as possible - for example, to resolve a major incident or implement a security patch when a high-risk threat is detected.

Emergency changes should be designed carefully and tested as much as possible before they're implemented, or the impact of the changes themselves may be worse than that of the original incident. However, there may be minimal time available for implementing these types of changes. Details of emergency changes may also be documented retrospectively.

A **normal change** is any service change that isn't a standard or emergency change. So this type of change isn't associated with a pre-approved, standardized process, but also isn't categorized as an emergency.

For example, an organization knows that one of its network software monitoring systems will have to be updated if it's to continue to support network traffic at optimal levels in the future. As a proactive measure, the organization decides to perform the update before performance issues occur. This is a normal change in that it should go through the formal and complete Change Management process.

No change should be authorized without a **remediation plan** (what to do if the change isn't successful). It outlines the actions needed to recover after a failed IT change- or release.

Remediation may include back-out plans, invocation of service continuity plans, or other actions designed to enable business processes to continue.
A back-out plan is typically the ideal remediation response. It specifies how to restore the organization to its initial state, often through the reloading of a base lined set of CIs - especially for software and data.

However, not all changes are reversible, so an alternative approach to remediation may be required. This could include revising the change itself in the event of failure, or - if the impact of a failure is severe, even invoking the organization's business continuity plan.

Change Management Interfaces:
Change Management interfaces with

- Transition planning and support to ensure that there's a coordinated approach to managing Service Transitions.
- Release and Deployment Management
- Supplier Management, where changes affect or may be affected by suppliers.

- Business change processes.
- Business program and business project management teams.
- Program and project management to ensure that the change schedule is effective and that all changes are well managed.

Changes to any business or project deliverables that don't impact services or service components may be subject to business or project Change Management procedures, rather than to IT Change Management procedures. In these cases, however, IT Change Management is still involved in

- managing changes to configuration baselines
- Liaising with project teams to ensure smooth implementation and consistency within the changing environments.
- Handling change proposals to ensure that potential conflict for resources or other issues are identified.

The Change Management process also interfaces with change evaluation.

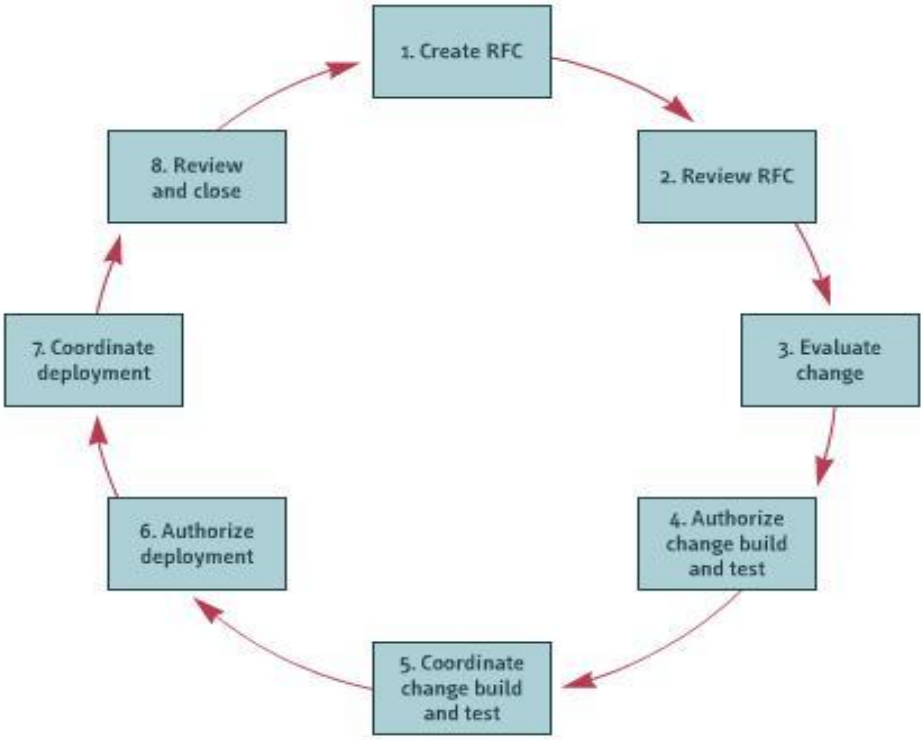
Change Management provides the trigger for change evaluation, and the evaluation report must be delivered to Change Management in time for the change authority to use it to assist in decision-making.

The three remaining key interfaces with Change Management are

- Stakeholder Change Management – to manage organizational changes
- sourcing and partnering – to manage vendor and supplier relationships
- Service Management – needs Change Management for implementing process improvements and service changes.

Normal and Emergency Changes in Change Management:

ITIL defines the normal change lifecycle as including eight steps. Following these 8 steps can help ensure effective Change Management.



1. Create RFC
2. Review RFC

3. Evaluate Change
4. Authorize Change build and test
5. Coordinate Change build and test
6. Authorize deployment
7. Coordinate deployment
8. Review and close

The first four steps in the normal change lifecycle focus on assessment and authorization for building and testing changes.

Create RFC:
The individual or group proposing a change creates the Request for Change (RFC).
All RFCs received should be logged and allocated identification numbers in chronological sequence. If a change request is submitted in response to a trigger, such as a resolution to a problem record, the reference number of a document about the triggering event should also be recorded.

Review RFC:
Change Management should ensure that RFCs include all required information. Incomplete or impractical RFCs should be returned, together with brief details of why they've been rejected -and the status of the RFCs should be logged. If an RFC is accepted, it will move onto the next step.

Evaluate Change:
Changes considered to be significant - based on well-defined criteria - should be subject to the formal change evaluation process. A formal request for evaluation should be submitted to trigger this process.
When formal change evaluation isn't required, a proposed change may be assessed more informally.

Authorize Change build and test:
Formal authorization for any change should be obtained from a suitable change authority, which may be an individual or a group of people. The levels of authorization required for a particular type of change should be based on the type, size, risk, and potential business impact of the change.

Where disputes arise over change authorization or rejection, there should be a right of appeal to an authority at a higher level. Changes that have been rejected should be formally reviewed, documented, and closed.

Example:
Consider an example. First the IT Department in an organization receives an RFC from the Sales Department, requesting that a secure server be set up for e-commerce purposes. This is passed to the IT Change Management team.

The team then reviews the **RFC,** checking that it contains all required information.

As the third step, the Change Management team assesses and evaluates the proposed change, using a set of **seven "R" questions**:

- Who **raised** the change?
- What is the **reason** for the change?
- What **return** is required from the change?
- What **risks** are involved in the change?
- What **resources** are required to deliver the change?
- Who is **responsible** for the build, test and implementation of the change?
- What is the **relationship** between this change and other changes?

As the fourth step in the normal change lifecycle, the proposed change - which is judged to be of value - is formally authorized by the members of a Change Advisory Board (CAB).

Steps 5 to 8 are the final four steps in the normal change lifecycle.

Coordinate Change build and test:
If an authorized change is part of a release, then packaging the change into a release and building and testing it is coordinated through the Release and Deployment Management process. For simple changes that aren't part of a release, the Change Management process coordinates building and testing.

Change Management is also responsible for ensuring that changes are thoroughly tested. Where emergency changes haven't been fully tested, special care needs to be taken during implementation.
Testing may continue in parallel with initial deployment of a service into the live environment so that further corrective action can be taken if necessary.

Authorize deployment:
The design, build, and testing of a change should be evaluated to ensure that risks have been managed and that actual performance meets business requirements.

The change evaluation process generates an interim evaluation report for any significant changes. For smaller changes, the Change Management process carries out suitable checks. The result of this evaluation should be forwarded to the appropriate change authority for formal authorization to deploy the change.

If authorization isn't given at this stage, the change authority may request changes to the design or to the deployment schedule.

Coordinate Deployment:
The Change Management process coordinates deployment for simple changes that aren't part of a release. Change Management's responsible for ensuring that changes are deployed and scheduled when the least impact on live operations is likely. Support staff should be on hand to deal quickly with any incidents that might arise.

Each deployment must be authorized. This may require that multiple RFCs be submitted. Alternatively, some organizations use a single RFC with multiple authorization stages.

Also, remediation procedures should be prepared and documented in advance in case errors occur. Authority and responsibility for invoking remediation should be specifically defined in change documentation.

Review and Close:
Before closing a change, it must be assessed in terms of its performance and to ensure that the change didn't introduce any unacceptable risks. The evaluation should also assess any associated incidents. If an external provider manages the change, details of any contractual service targets will be required.

For significant changes, the change evaluation process generates an evaluation report. For smaller changes, suitable checks are conducted as part of the Change Management process.

If the evaluation of a change is favorable, the change is presented as completed for change stakeholder agreement. Lessons learned should be recorded so they inform future changes.

Example Continued:
In the case of the request for a new e-commerce server, work orders for authorized changes are sent to hardware, security, and applications teams during the fifth step of the normal change lifecycle. These work orders are tracked and linked to the original RFCs. During Change Management the process is overseen to ensure that the server is thoroughly tested.

Once testing is complete, a change authority reviews the interim evaluation report to ensure that the server can perform as required. It then formally authorizes deployment of the requested server.

The Change Management team coordinates the deployment and monitors deadlines to ensure that all goes as scheduled.

Finally, the team assesses whether the new server is meeting the requirements of the Sales Department and overall organization.

Emergency Changes:
The number of emergency changes proposed should be kept to an absolute minimum because these types of changes tend to be disruptive and prone to failure. So as much as possible, all changes likely to be required should be anticipated and planned, bearing in mind the availability of resources to build and test the changes.

Also, when a change is needed urgently -because of poor planning or sudden changes in business requirements - it's preferable if it can be treated as a normal change but given the highest priority.

However, emergency changes may sometimes be required. It's important to have procedures in place for handling these quickly, but without sacrificing important management controls.

An emergency change procedure should generally be reserved for changes intended to repair errors in IT services that are having a significant, negative impact on a business's users or customers.

Changes intended to introduce urgently required business improvements should be handled as normal changes, but assigned the highest urgency.

The emergency change lifecycle is basically the same as the normal change lifecycle. However, due to the time constraints in an emergency situation, some of the steps may be handled slightly differently.

Normal and emergency change procedures may differ in four basic areas.

Authorization:
Often in an emergency, a full CAB meeting can’t be held. In cases where CAB authorization is required, an emergency CAB (ECAB) may then be established according to the organization's procedures for this.

Predictable emergency changes - such as server failures - are unlikely to need an ECAB. Instead, the authority to authorize these changes may be delegated to Service Operation functions, Technical Management, or Application Management.

Such delegation should be limited to actions that don’t change the specification of service assets and don’t attempt to correct software errors. With software incidents, it's best to revert to the previous trusted state or version, rather than attempting an unplanned and potentially dangerous change.

Testing:
Emergency changes should be designed carefully and tested as much as possible before use, or the impact of the emergency change may be greater than the original incident.

Completely untested changes shouldn't be implemented if this is at all avoidable. The less a change is considered likely to fail, the more reasonable it may be to reduce the degree of testing in an emergency.

When only limited testing is possible, then testing should be focused on aspects of the service that will be used immediately, or elements that could cause the most short-term inconvenience or errors once live in the environment.

Review:
If a change fails to rectify the urgent outstanding error, Iterative attempts at fixes may be necessary. Change Management should ensure that business needs remain the primary concern and that each iteration is controlled. Change Management should ensure that ineffective changes are swiftly backed out.

If too many attempts at an emergency change are ineffective, you need to consider whether the error has been correctly diagnosed, the resolution has been adequately tested, and the solution has been correctly implemented.

In such circumstances, it may be better to provide a partial service to allow the change to be thoroughly tested, or perhaps to suspend the service temporarily and then implement the change.

Documenting:
It may not be possible to update all change records at the time that urgent actions are being completed. For example, these changes may occur overnight or during the weekend.

It is, however, essential that temporary records are made during such periods, and that all records are completed retrospectively, at the earliest possible opportunity.

An agreed time for completing these updates should be documented when the change is authorized.

Example:
Suppose an organization has multiple reports coming in of clients not able to log into their payroll systems Through Problem Management procedures, it's discovered that a server has failed.

This requires an emergency change. The server hardware has to be repaired or replaced, and a small change in the server's configuration may be required. The change in this case can be authorized by operational staff, rather than requiring authorization by an ECAB.

Because of time constraints, only daily entry features for the payroll are tested. End-of-month routines are not tested at this point.

The team implementing the change documents who gave authority for it and keeps detailed notes on how the change is implemented. The notes state that full reports will be completed within three working days.

Change Evaluation:
The purpose of the change evaluation process is to provide a consistent and standardized means of determining the performance - or value - of a proposed IT service change, to facilitate a decision about whether to authorize the change.

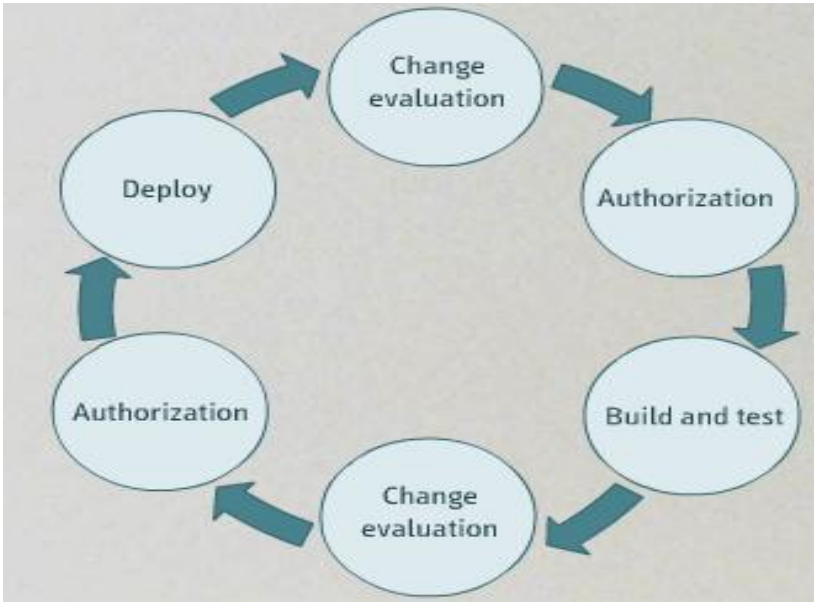
It involves identifying and assessing the likely impacts of a proposed change on business outcomes, and on existing and proposed services and IT infrastructure.

It also involves identifying associated risks and issues.

The objectives of change evaluation are to

- Set stakeholder expectations – ensure realistic stakeholder expectation by providing information about all the likely effects of the changes and associated risks.
- evaluate the effects of a proposed change
- Provide high-quality outputs – or information which helps in deciding whether or not to authorize the changes.

For example, the results of evaluation may guide decisions about whether to authorize building and testing of an IT service change, and about whether to authorize deployment of the new or altered service to the live environment.



Each organization needs to decide which changes should be subject to formal change evaluation and which can be evaluated more simply as part of the Change Management process.

This decision is normally documented in the change model used to manage each type of change.

For the change evaluation process to be effective, it should involve assessing a proposed change objectively. It should also include consistent reporting methods.

The evaluation team should provide an evaluation report, or interim evaluation report, to Change Management to facilitate decision-making at each point where authorization is required.

Effective change evaluation establishes how and whether a proposed service change will be of value to the organization, given the required resources, the likely effects of the change, and any potential or real associated risks.

In turn, it helps ensure a focus on value in Change Management -with decisions to authorize changes based on what value they'll contribute.

In addition, the results of change evaluation can feed into and support Continual Service Improvement (CSI). For example, weaknesses associated with proposed service changes can be addressed and resolved, informing future improvements in service offerings and delivery.

Challenges to Change Evaluation:
However, the change evaluation process is subject to several challenges. These include

- developing and using appropriate evaluation measures (for example it can be difficult to measure in ways that demonstrate less variation in predictions during and after transition)
- understanding stakeholders' perspectives
- Balancing risks (understanding, and being able to assess, the balance between managing risk and taking risks is a challenge).
- communicating risks (encourage Risk Management culture)

Factors that can prevent change evaluation from being effective include

- a lack of clear criteria for when change evaluation should be used
- unrealistic expectations of the time required for change evaluation
- change evaluation personnel with insufficient experience or organizational authority to influence change authorities, and
- projects and suppliers estimating delivery dates inaccurately and causing delays in change evaluation activities

Service Operation:

Scope and Responsibilities of Service Operation:

The purpose of the Service Operation stage is to coordinate and carry out the activities and processes required to deliver and manage services at agreed levels to business users and customers. So the Service Operation stage ensures that services are delivered as promised

The Service Operation stage is also responsible for ensuring that the necessary technology is managed properly to support this service delivery.
Service Operation is a critical stage in the Service Lifecycle because it ensures that daily operations function smoothly. The organization's strategic objectives are ultimately achieved during the Service Operation stage.

When operations run smoothly, you can gather the baseline data needed to plan improvements, or to find inspiration for a better design for services.
People working within Service Operation processes need to approach work with a broad view of the entire operation and delivery mechanisms. If they approach work with only their specific process or tasks in mind they may not be in a good position to detect any threats or failures in overall service quality.

This end-to-end view may include suppliers, customers, and after-sales care. So when needed, processes and tools used to manage cross-organizational workflows should be deployed.
The area of Service Operation is broad – its scope encompasses all processes, functions, and tools needed to deliver and support services. This scope includes

- Services – activity or service related task carried out by your organization, an external supplier, or the user or customer of the service.
- Managing Service Management processes (example, managing Change Management Core activities)
- Managing technology (example, Managing IT Infrastructure that helps daily operations in Service Delivery)
- Managing people involved in Service Delivery.

To successfully fulfill the scope of Service Operation responsibilities, you need to consider and strive toward these goals:

- deliver IT services and support of these services effectively and efficiently
- ensure IT services are provided only to those authorized to receive the service, and
- reduce the impact of service outages in daily operations

As part of the **ITIL© Service Lifecycle,** the Service Operation stage is responsible for executing and performing processes to optimize the cost and quality of services within the Lifecycle.

Another responsibility is to provide the business with capacity to meet its objectives.

The remaining responsibilities within the Service Operation stage include

- the technology used to deliver and support service, and
- the overall functioning of the business itself (cost efficiency and SLA adherence)
- Ensuring user satisfaction with the IT services.

When Service Operation works effectively and achieves a balance between a focus on detail and on the broader context, businesses are able to benefit from their IT investments.
So Service Operation is the stage at which the business receives value for an IT investment, which makes this stage of the Service Lifecycle critical.

The Role of Communication in Service Operation:

Communication – means people or groups of people exchange information, verbally or in writing.

In Service Operation, good communication can prevent problems or mitigate issues that may lead to problems.

Bad communication can worsen situations by failing to prevent problems from escalating.

Good communication is necessary at all levels. Service Operation teams, IT Teams, users, and both internal and external customers need to communicate regularly and effectively.
These are some of the best practices you should keep in mind;

- identify the relevant stakeholders
- be aware of the types of communication typical in Service Operation
- express the intended purpose of each communication clearly, and
- agree on an appropriate mode of communication

Some examples of different types of communication that may be required in Service Operation include

- routine operational communication
- communication between shifts
- performance reporting
- communication in projects, and
- training on new or changed processes and service designs

Through **routine operational communication,** stakeholders can summarize events and present new issues, and highlight the need for any follow-up on past issues.

Communication between shifts may be required to update incoming staff about any incidents or problems that occurred during the previous shift.

All team members may play a role in **performance reporting**. For example, team members may be asked to report on the health of any major systems and to inform other staff of any issues that may affect IT service operations in the near future.

Communication in projects is needed to ensure that all relevant stakeholders are aware of any problems or incidents that need to be dealt with, and that action plans are devised for attending to outstanding issues.

It's important that relevant stakeholders communicate any necessary information about **training on new or changed processes and service designs**. This ensures that staff members are available to participate in any relevant training, and prevents training from disrupting operations.

Further examples of different types of communication needed in Service Operation include communication related to

- changes
- exceptions
- emergencies, and
- strategy, design, and transition to service operation teams

It's important to communicate **changes** to affected parties. Communications may be scheduled to discuss changes that are expected and potential incidents that may occur as a result, and to devise a plan of action for dealing with the relevant incidents.

If there are operational **exceptions**, they need to be communicated to the staff, including any anticipated impact the exceptions may have on operations.

In case of operational **emergency** such as a major network failure, staff may need to meet to discuss the problem, find solutions and settle on a plan of action.

General information **on IT strategy, design, and IT services being transitioned** to relevant stakeholders in service operation must also be communicated.

In addition to meetings, communication may be delivered in many ways including e-mail, social media and micro blogging services, instant messaging and web-based chat, pagers, Voice over Internet Protocol (VoIP) utilities, teleconference and virtual meeting utilities, and document-sharing utilities.

Although ITIL® does not specify a particular medium for communication or communication frequency; organizations should determine and document their own communication policies based on their organizational needs and preferences.

It's important that all stakeholders know how and when communication is to take place.

Meetings, when executed properly, are a very beneficial medium for communication. The purpose of holding a meeting is to exchange information on common issues and objectives with a group. Meetings should always remain focused on a common agenda with the aim of driving action.

These are some of the factors that can help ensure a successful meeting:

- establishing a clear agenda (A clear agenda can help ensure that the participants stay focused and that the meeting objectives are met)
- recording issues that are not on the current agenda (so that details of these issues can be addressed at a later time)
- ensuring that rules for participation are understood (so that meeting runs smoothly)
- keeping minutes, and
- encouraging appropriate levels of participation (that certain participants do not take over the meeting)

Face-to-face meetings between stakeholders in Service Operation may be required periodically, but aren't always the best solution.

It's better if relevant information can be shared just as effectively by other means, such as e-mail.

It's also important not to develop a culture in which work takes place or management consults with staff only during meetings.

Face-to-face meetings can be expensive and potentially disruptive. They require people to set time aside from their usual activities and to travel to a meeting place. In addition, venues need to be booked and refreshments may have to be supplied.

So organizers should always weigh the benefits of face-to-face meetings with the costs involved.

The 3 types of meetings commonly held Include

- operations meetings (meeting chaired by Ops head, attended by reps from various Ops units, IT Ops issues will be discussed/highlighted)
- group meetings (similar to Ops meetings except that they include only the members of a particular department, group, or team)
- customer meetings (meeting between management and customers to review service delivery and expectations, and to address any service-related issues)

Service Desk Roles and Objectives:

A function comprises the measures and the people that carry out a defined process or activity. This may be represented by a single organizational unit or a diverse group of teams and departments.

There are four main Service Operation functions, which have the overall purpose of managing a "steady state" operational IT environment.

The **service desk** is the primary point of contact for users when there is a service disruption, for service requests, or even for some categories of Requests for Change (RFC).

Technical Management provides detailed technical skills and resources needed to support the ongoing operation of the IT Infrastructure - such as servers, networks, and desktops. Technical Management also plays an important role in the design, testing, release, and improvement of IT services.

IT Operations Management is the function responsible for the daily operational activities needed to manage the IT Infrastructure. It incorporates IT operations control and Facilities Management IT operations control ensures that routine operational tasks are carried out. Facilities Management refers to the management of the physical IT environment -usually data centers or computer rooms.

Application Management is responsible for managing applications throughout their lifecycle. The Application Management function supports and maintains operational applications and also plays an important role in the design, testing, and improvement of applications that form part of IT services.

The above 4 Service Operation functions ensure that IT systems, software and facilities operate efficiently and consistently.

Service Desk:

A service- desk is a functional unit made up of a dedicated number of staff responsible for dealing with a variety of service events.

These events are reported via telephone calls or a web interface, or are automatically reported infrastructure events.

The service desk is the single point of contact for IT users on a day-to-day basis.

Service desks generally handle all incidents and service requests, and usually make use of specialist software tools to log and manage all such events.

The primary aim of the service desk is to restore service to normal for users as quickly as possible. The Service Desk also helps to improve customer service, and to enhance IT operations.

Benefits of Service Desk:

The benefits of an effective service desk are that it

- improves customer service, through better handling and faster turnaround of customer or user requests
- increases accessibility through a single point of contact
- improves infrastructure and control
- improves the use of IT support resources, through improved teamwork and communication
- reduces the negative business impact of service disruptions by increasing the productivity of business personnel, and
- provides an excellent grounding for employees who wish to pursue a career in Service Management

There are a range of possible structure and location options for service desks. The optimal solution for a service desk structure and location is dependent on your organization's needs.

Some service desks may also need to be customized with specialist service desk groups.

The two most basic organizational structures for service desks are

- local, and
- centralized

A **local service desk** is located within or close to the user community it serves. This often aids communication and gives the service desk a visible presence. However, a local service desk can be inefficient and expensive to resource, particularly when call volumes are relatively low. You may need to maintain a local service desk even where call volumes alone do not justify this. This may be due to specialized or high-status user groups; language, cultural, or time zone differences; or the existence of customized or specialized services that require specialist knowledge.

A **centralized service desk** has staff located in one or more centralized service desk structures. This can be more efficient and cost-effective than using local service desks because fewer staffs are needed in order to handle a higher volume of calls. This structure also encourages higher skill levels because staffs tend to have to deal with a large number of specific events. Maintaining some form of local presence may still be necessary in order to handle physical support requirements, but such staff can be controlled and deployed from the central service desk.

Other organizational structures for service desks make use of technology and business globalization.

Using technology such as the Internet and corporate support tools, it is possible to give the impression of a single, centralized service desk when in fact personnel are located across any number or type of geographical or structural locations. This is the role of a **virtual service desk**. Virtual service desks provide the option of home working, secondary support groups, off shoring, or outsourcing - or any combination of these options. However, there needs to be consistency and uniformity in service quality and cultural terms, which can be difficult to achieve with a virtual service desk.

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 desk**. This provides 24-hour coverage at relatively low cost because no desk has to work more than a single shift. For example, a service desk in the Asia-Pacific region may handle calls during its standard office hours and, at the end of this period, hand over responsibility for any open incidents to a European-based service desk.

All service desks need to share common processes, tools, and database information. The issue of culture and language also needs to be addressed for this approach to succeed.

Some organizations find it beneficial to create **specialist service desk groups** within the overall service desk structure. Incidents relating to particular IT services are routed directly to the group best equipped to handle them. This enables faster resolution of these incidents, through greater familiarity and specialist training

You can set up automatic telephone scripts to route users through to the relevant specialist service desk group. For example, "If your call is about the wireless service, please press 1 now; otherwise please hold for a service desk analyst." Or alerts for a particular service type can be routed directly to the associated service group.

The available selections should not be overcomplicated, so specialist service groups should be considered only for a very small number of key services, where call volumes for these services are high.

Regardless of the service desk structure that you select for your organization, you need to ensure that users know who they need to contact and how to contact the appropriate service desk.

A single telephone number, e-mail address, and web page - or one for each group if separate service desks are chosen - should be provided and well publicized.

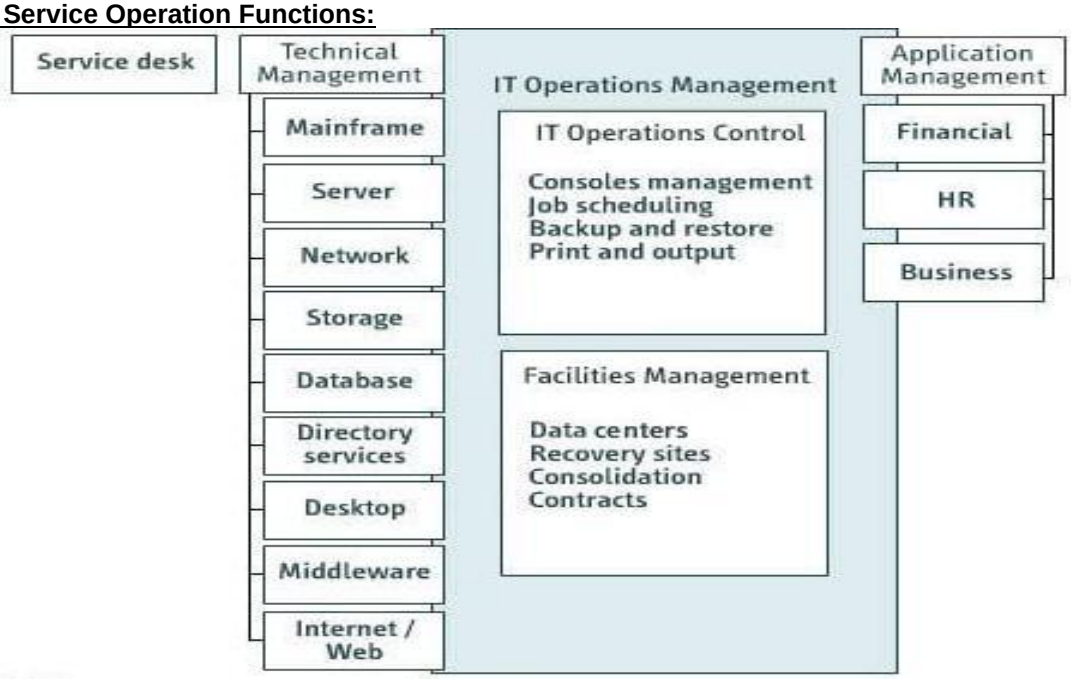
Points of contact can be advertised in various ways to ensure that users know what number to call, which web site to go to, or what e-mail address to use.

You can place contact information on hardware, telephones, notice boards, or corporate gifts such as pens or mugs.

You can use a customized background or desktop that contains the service desk contact details, together with information read from the system that will be needed when calling - such as Internet Protocol (IP) address and operating system (OS) build number.

You can also place contact details prominently on service desk Internet or intranet sites, add them to e-mail correspondence with users, or provide users with calling cards.

Other Service Operation Functions:



In addition to the service desk, Service Operation functions include

- Technical Management
- IT Operations Management, and
- Application Management

Technical Management assists in the planning, implementation, and maintenance of a stable technical infrastructure to support the organization's business processes.

Technical infrastructure should be maintained through the adequate and timely use of technical skills and techniques to diagnose and resolve any technical failures that do occur.

IT Operations Management include maintaining stability in the organization's daily processes and activities, improving service at reduced cost through regular analysis, and using operational skills to diagnose and resolve any IT operations failures that occur.

Application Management aims to support an organization's business processes by managing the application software. It assists in the design, deployment, maintenance, and improvement of cost-effective applications. It is also expected to diagnose and resolve technical failures.

Technical Management:
Technical Management refers to the groups, departments, or teams that provide technical expertise and overall management of the IT Infrastructure.

The Technical Management function focuses on the management of IT hardware. Within this context, it plays a dual role:

- it holds technical knowledge and expertise (to manage organization's IT infrastructure)
- it provides technical resources to support the IT Service Management (ITSM) Lifecycle

Technical Management ensures the use of appropriate human resources to manage the technology required to support business objectives.

An important aspect of carrying out this role effectively is the ability to balance the skill levels available, the use of resources, and the cost of these resources.

For example, if you hire a very experienced technician and then use the technician's skills for only a small percentage of the time, you have not used wage resources optimally. In this scenario, it may be better to hire a contractor for the task.

Larger organizations may leverage specialist staff out of central pools for specific technical tasks. This helps to ensure economies of scale and reduces the need to hire contractors for technical work. This type of resource use is particularly effective for project teams and problem resolution.

Technical Management is expected to provide guidance to IT operations about how best to carry out the ongoing operational management of technology.

This role is carried out in the Service Design process, as well as during ongoing communications with IT Operations Management.

IT Operations Management:
IT Operations Management is the function responsible for the ongoing maintenance and management of organizations' IT infrastructure. It is defined by the daily activities needed to ensure that the infrastructure operates optimally.
In turn, IT Operations Management allows an organization to meet its business objectives through the use of its IT infrastructure.
IT Operations Management has two sub functions - Operations Control and Facilities Management.

Operations Control oversees the execution and monitoring of the activities and events in the IT infrastructure. This is carried out using an operations bridge or network operations center - the physical location in which the IT network is monitored and managed.

In addition to executing routine tasks in all technical areas, Operations Control performs the following specific tasks:

- managing consoles (Console Management is a central observation and monitoring capability used to monitor and control operational activities)
- job scheduling (managing routine batch jobs or scripts)

- performing backups and restores
- managing print and electronic output, and
- performing maintenance activities

The **Facilities Management** sub function of IT Operations Management involves the management of the physical IT environment. This includes data centers and computer rooms, as well as necessary power and cooling equipment.

In cases where the management of a data center is outsourced, Facilities Management is responsible for managing the outsourcing contract.

Facilities Management is also responsible for coordinating large-scale consolidation projects, such as server consolidation projects.

As with many IT Service Management processes and functions, IT Operations Management plays a dual role:

- keeping current activities and processes running optimally (maintaining the stability of the IT infrastructure and the consistency of IT Services)
- adapting to changes in business requirements and demand (It must ensure that operations and events support a changing environment)

Because the two roles of IT Operations Management are at some level contradictory, IT Operations Management needs to create a balance between maintaining the status quo and changing the status quo to meet new challenges.

To achieve this balance, IT Operations Management needs to generate two sets of metrics - to report to the business on the achievement of service objectives, and to report to IT managers on the efficiency and effectiveness of IT operations.

IT Operations Management must develop a cost strategy aimed at balancing the requirements of different business units with the cost savings available through optimization of existing technology or investment in new technology.

This strategy needs to be founded on a value-based – rather than a cost-based - Return on Investment (ROI) approach to investments.

To achieve balance between its two roles, the IT Operations Management function requires a clear understanding of both technological and service needs.

To ensure this, it needs to outline procedures and manuals that outline the role of IT operations in both the management of technology and the delivery of IT services.

It also needs to build an understanding of how technology is used to provide IT services and the relative importance and impact of those services on the business.

So all IT operations staff need to understand how the performance of technology affects the delivery of IT services.

Application Management:
Application Management plays a role in managing all applications, whether purchased or developed in-house. It is also responsible for informing decisions about whether to buy or build needed applications.

The dual role that Application Management plays is to provide

- technical knowledge and expertise (to manage applications

- resources needed to support the ITSM Life cycle (In this role, it ensures that application staffs are trained and that sufficient resources are deployed throughout the ITSM Lifecycle)

Application Management's two roles help to ensure a balance between skill levels and the cost of application resources, in support of the organization's business objectives.

In addition to its two high-level roles, Application Management performs the following specific roles:

- providing guidance to IT service operation (**to IT service operation** about how to manage applications effectively)
- integrating the Application Management Lifecycle with each stage of the ITSM

Service Operation Processes:

Incident Management:

The Scope and Principles of Incident Management:

In the ITIL Service Lifecycle, the Service Operation stage includes five processes. One of these is incident management.

In ITIL terminology, an incident is defined as an unplanned interruption in, or reduction of the quality of an IT service.

An incident can also include a Configuration Item (CI) failure, if service is interrupted.

Incident Management is the process for managing the lifecycle of all incidents.

You maybe alerted to incidents in different ways

- through reports from technical staff
- as a result of using event monitoring tools
- as a result of users' communication with service desk staff, or
- through reports from suppliers or business partners

Efficient Incident Management has clear

- purpose, and
- objectives

The **purpose** of incident Management is to ensure that IT services are provided at the levels agreed to in a Service Level Agreement (SLA). The focus of Incident Management is on maintaining or restoring service in the event of an incident, and on minimizing the negative effects of any interruptions on customers, users, and business operations.

The **objectives** of Incident Management are to ensure standardization in incident response, reporting, analysis, and documentation. It should increase visibility and communication of incidents to business and IT support staff. It should also focus on a positive portrayal of IT services through efficient incident response and communication, maintaining user satisfaction through good quality IT services, and aligning all Incident Management activities with organizational goals and priorities.

Service interruptions are often communicated directly by users, either through the service desk or Incident Management reporting or tracking tools.

An organization's Incident Management policy should specify how users can report incidents. It should also specify how technical staff should report, log, and respond to incidents.

It's important to distinguish between reported incidents and regular service requests. Service requests are logged like incidents, but rarely cause any kind of service interruption.

For example, a user may contact an IT service desk for a password reset request or with an account change request. These are examples of a service request rather than an incident

because, although the event inconveniences the user, it doesn’t cause a service interruption nor does it impact other users.

An example of an Incident would be a number of users reporting an inability to connect to the company network. IT service for those users is interrupted, and the service desk must implement steps to resolve the connection issues.

Each organization's process for managing incidents may differ depending on the organization's needs and circumstances. However, it's important to apply certain general principles for Incident Management to be effective.
These principles include

- Setting timescales for incident response (**set reasonable timescales** and targets for handling incidents. These are typically specified in SLAs, and should reflect targets set in the operational level agreements (OLAs) and underpinning contracts (UCs))
- creating incident models (Many types of incidents tend to recur, so it's generally useful to define **incident models** and apply them to relevant incidents when they occur)
- Planning special responses to major incidents (There should he a **specific model or set of steps for dealing with major incidents**. An organization may define what constitutes a major incident, although typically it's any incident that interrupts critical services and takes considerable time to repair)
- Tracking incident status (following each incident through the stages of its lifestyle, using status codes. This maintains efficiency in handling and reporting processes)
- Dividing the incident lifecycle into clear stages (like detection, diagnosis, repair, recovery, and restoration. This can result in better understanding and handling of an incident)

An SLA, may establish a timescale for completing each stage of the Incident Management process.

Alternatively, an automated process may be used to establish appropriate timescales for incident response. This can also help determine the severity of an incident, and whether it has escalated in severity since first being detected.

All IT employees and support staff should be aware of the agreed timescales and respond accordingly when dealing with incidents. For example, they should know which types of incidents to prioritize.
An incident model defines the steps that should be taken to deal with any incident that matches the model.

This helps ensure that standard incidents are handled in a standardized way, and within predefined timescales.

An incident model may be useful even for managing incidents that require specialized handling. For example, it may outline steps for identifying the nature of the incidents and for redirecting those that require special handling to the appropriate people or departments.

Each incident model should include specific information:

- the required steps for handling an incident of the relevant type
- the order of the required steps, including any extra tasks
- the designated employees or units responsible for each step
- any precautions - such as making backups or implementing other safety measures -that should be taken before the specified steps are implemented
- timescales and thresholds for completion of the steps
- who to contact if an incident requires escalation, and
- any steps required to collect and secure evidence for use if legal action is taken

A plan for responding to a major incident may identify a dedicated team that can provide the time and resources required to implement a quick resolution.

A distinction should be made between the person managing a major incident and the general incident manager. This ensures that other, less serious incidents aren't neglected, while major incidents receive sufficient attention.

Incident tracking helps ensure that incidents aren't overlooked at any point in their lifecycles, and that those responsible for managing incidents can prioritize resources appropriately.
Some of the common incident status tracking codes includes

- open, for recently discovered incidents
- in progress, for incidents that have been assigned and are currently being dealt with
- resolved, for incidents that have been resolved but before regular service is resumed, or
- closed, for once regular service has resumed

The Incident Management Process:

Effective Incident Management helps ensure that an IT service provider can provide services at the levels outlined in a Service Level Agreement **(SLA).** It does this by restoring normal service as quickly as possible after incidents occur and minimizing any impacts they cause.

The Incident Management process includes a defined sequence of steps;

1. incident identification
2. incident logging
3. incident categorization
4. incident prioritization
5. initial diagnosis
6. incident escalation
7. investigation and diagnosis
8. resolution and recovery, and
9. incident closure and if necessary, incident re-opening

Step1: Incident Identification:

The first step is to identify an incident when it occurs. This may happen only when a user contacts the IT service desk with a problem.
However, it's best if you can identify incidents before they inconvenience users, instead of only once services have been significantly disrupted.

To identify the nature of an incident, service desk staff or other IT personnel may question the affected users. They may also run remote diagnostic tests.

Step2: Incident Logging:

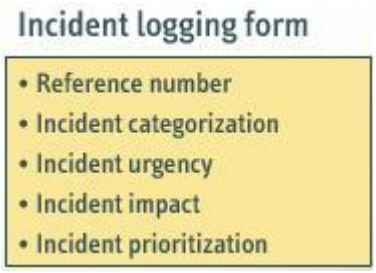
Once you've identified an incident, it's important to begin incident logging - which then continues throughout the lifecycle of the incident.

You should log information about each incident's

- category and impact
- nature and occurrence, and
- resolution

In a log, you should assign each incident a unique reference number for tracking purposes. You should also identify its **category, the urgency of resolving the incident, its impact on users, and its priority level.**

The way you categorize an incident will depend on your organization's system for doing this. Top-level categories may also be broken down into sub-categories.



In the log, you should Include information such as the date and time the Incident was recorded, the name or ID of the employee recording the incident, how the incident was identified, and the contact details for the department to which the user who reported the incident belongs. You should also include a description of symptoms, the incident status, related Configuration Items (CIs), and the support group responsible for resolving the incident.

Once an incident has been resolved, you should update the log with any related problems or known errors associated with the incident, the activities taken to resolve the incident, the resolution date and time, the updated incident category, and the closure date and time.

- Related problem / known error
- Resolution activities
- Resolution date and time
- Closure category
- Closure date and time

If a service desk doesn't operate 24 hours a day, other groups, such as those involved in IT operations or network support, can log incidents outside service desk hours.

As further actions to resolve an incident are taken, the incident log should be updated so that a full history is maintained.

For example, this might include changing the categorization or priority of an incident based on the results of further diagnosis or escalation activities.

Step3: Incident Categorization:
During initial incident logging, it's important to categorize incidents based on their type. Different organizations define incident categories differently depending on their needs. However, it's important for organizations to develop and use a standard set of codes for this purpose.

To develop an appropriate set of incident categories, you can

1. conduct a brainstorming session (define categories)
2. use trial categories (after defining the categories use these for a trial period)
3. review and adjust the categories (make necessary changes however try to keep categories stable unless changes are genuinely required)

It's common to categorize incidents at multiple levels - usually to three or four levels of granularity. For example, an incident may be categorized based on the location, service, system, and application it affects.

It's worth noting that sometimes the details available at the time an incident is logged may be incomplete, misleading, or incorrect. So it's important that the categorization of an incident is checked and updated if necessary.

Step4: Incident prioritization:
Another important aspect of incident logging is to allot an appropriate prioritization code. This will determine how the incident is prioritized.

As an IT service provider, you should determine a priority coding system and be sure all staffs are clear on the associated policies.

Priority coding system

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Priority code	Desciption	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

To determine the priority of an incident, you take its urgency and level of business impact into account. An indication of impact is often the number of users being affected, although if a single affected user is key to business, the consequences can be just as dire as an incident that impacts many users.

Other factors that help determine the impact of an incident include physical risk, number of affected services, potential financial loss, potential damage to an organization's business reputation, and legal implications.

There are also occasions in which the normal priority system is overridden, due to a user request or specific impact on a business.

As an example, it may be appropriate to assign an application crash that prevents affected users from performing all work duties a priority code of 2, where the code indicates high priority.

In this case, the priority code maps to a target resolution time of 5 hours. So this is the time within which a team should resolve the incident.

Step5: Incident Diagnosis:
Each incident may be subject to two possible diagnoses - an initial diagnosis when it's first reported and a second diagnosis if the incident requires further investigation.

When a user initially reports an incident to a service desk, a service desk analyst tries to diagnose the incident by asking relevant questions. The analyst may then use software and currently available information to resolve the incident immediately.

If the incident can't be resolved immediately, the analyst should inform the user, it may also be appropriate to give the user an incident reference number, which is typically generated from electronic incident log applications.

When a user first reports a possible application crash, for example, a service desk analyst asks the user questions to try to determine the cause and nature of the incident.

The service desk analyst performs remote diagnostic testing on the user's computer and discovers possible operating system instability. The analyst can't handle the incident from the service desk, so the appropriate support staffs are notified.

Some types of incidents occur regularly, so the appropriate resolution actions for these incidents are typically known. However, it's important to follow a procedure for matching data about an incident to the appropriate classification.

Successful matching will ensure that the response to an incident is appropriate and efficient. It also minimizes the need for escalation.

Step6: Incident Escalation:
When it becomes clear that the service desk is unable to resolve the incident, the incident must be escalated immediately for further support. Types of escalation include

- functional escalation, and
- hierarchic escalation

Functional escalation occurs when an incident is escalated one level at a time. If the service desk can't resolve the incident, it's escalated to the next appropriate support group, such as a tier 2 support group. If this group also can't resolve the incident, it's escalated further up the support chain. Some incidents may be escalated to multiple support groups, or even to third parties such as software suppliers or hardware manufacturers.

In the case of **hierarchic escalation**, an incident is escalated directly to a higher level within the organization, like the next level of management, for example, so that it receives the immediate attention of an appropriate person with required authority. Hierarchic escalation is also used if the investigation, diagnosis, and resolution and recovery steps are taking too long.

Hierarchic escalation should continue up the management chain as needed so that appropriate management personnel can approve or direct necessary action, such as allocating additional resources or involving suppliers for resolving the incident.

Step7: Investigation and Diagnosis:
If an incident is escalated, it will go through a second stage of investigation and diagnosis.

The actions taken at this point, including details of any actions taken to try to resolve or re-create the incident, should be fully documented in the incident log to ensure it provides a complete Incident history.

Where possible, Investigation and diagnosis should be performed in parallel to reduce the overall time it takes to resolve an incident. Support tools should be designed or selected to allow this as much as possible.
Investigating an incident is likely to involve

- establishing exactly what has gone wrong or is being sought by the user
- determining the chronological order of events that occurred
- confirming the full impact of the incident, including the number and range of users affected
- identifying any events that could have triggered the incident, and
- searching incident records or known error databases for previous knowledge gained as a result of similar incidents

The support group, investigating the application crash, performs tests on the affected systems and determines a potential resolution involving rebooting a server. The group's investigation reveals that the initial crash was a result of a failed automatic reboot.

Step8: Resolution and Recovery:
Once a potential resolution to an incident has been identified, it should be applied and tested. Various people may be involved in implementing measures to resolve an incident. These include

- Users (perform certain activities on their own workstations or remote equipment to help resolve an incident. For example, you could ask a user to run a virus scan)
- Service desk staff (may use central methods, like rebooting a server, to help resolve an incident. They may also address incidents remotely, for example using software to take control of a user's desktop and implement a resolution)
- Members of support groups (You can ask **specialist support groups** to implement specific recovery actions. For example, you could ask a third-party task team to reconfigure a router to maintain network stability)
- third-party suppliers (ask a **third-party supplier** or service provider to resolve an incident For example; you might ask a supplier to replace a faulty configuration on a router that's causing network failure)

If multiple support groups are involved in applying a resolution, it’s important to coordinate their activities and liaise with all parties involved.

The dedicated IT support group, for example, implements the proposed resolution of using software to repair the operating system, registry, and e-mail software on the user's computer.

With an incident like a damaged operating system, the group then needs to test the computer repeatedly to verify that the incident has been successfully resolved and service restored.

Step9: Incident Closure:
After the incident has been resolved, it can be closed.
As part of the closure step, service desk staff should confirm that

- the initial incident categorization was correct (to maintain accurate incident record)
- users are satisfied with the resolution (call users or use email survey to verify that **users are satisfied with the resolution** that has been applied)
- documentation has been updated
- the incident's root cause has been addressed (if root cause not identified, it's possible the incident will recur, so raise a new problem record in conjunction with the Problem Management process so that preventive action is initiated)

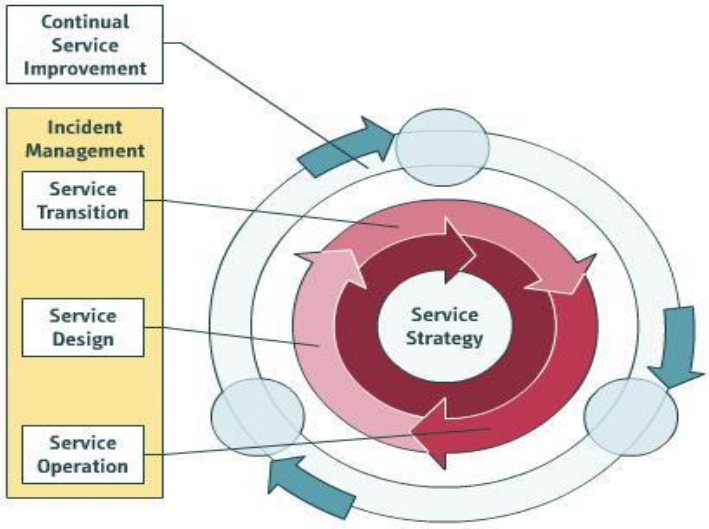
Some organizations choose to apply an automatic closure period for specific, or even all, incidents. For example, an organization's policy may specify that any incident will be closed after two days if no further user contact has occurred.
Regardless of the duration, you can formally close an incident once you're certain it has been fully addressed and shouldn't recur.

Even with adequate management, there will be occasions when incidents recur despite being closed. The decision can then be made to re-open the incident - the optional final phase of the Incident Management process.

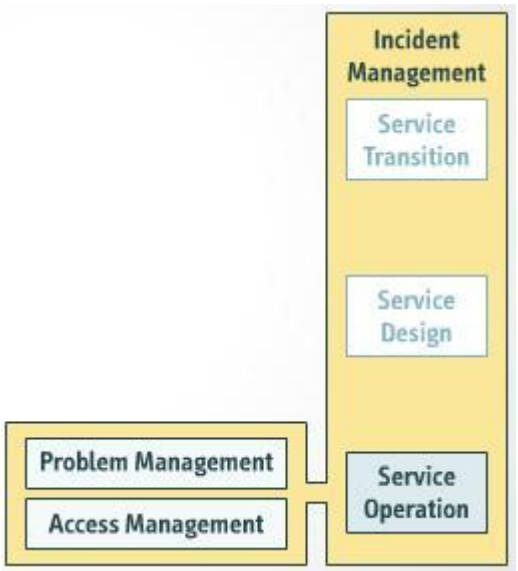
It's wise to have predefined rules about if and when an incident can be re-opened.

It might make sense, for example, to agree that if an incident recurs within one working day of being closed, it can be re-opened - but that beyond this point, a new incident must be logged, but linked to the previous incident.

Incident Management Interfaces:
Incident Management interfaces with various processes in the Service Transition, Service Design, and Service Operation stages of the Service Lifecycle.



Within the Service Operation stage, Incident Management interfaces with two processes - Problem Management and Access Management.

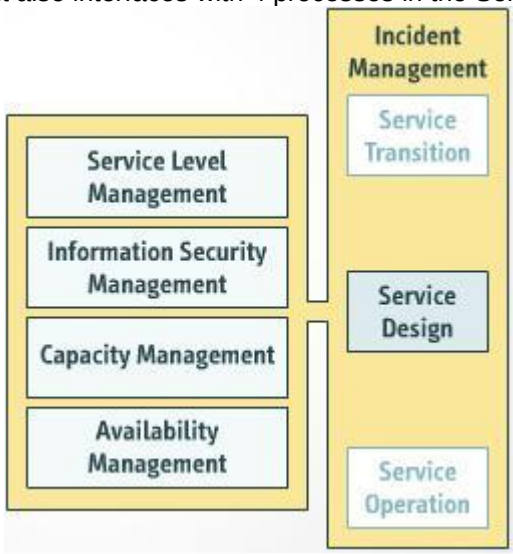


It's sometimes necessary to involve **Problem Management** in investigating and resolving the underlying causes of incidents. Problem Management, in return, provides information about existing problems and known issues that could be the causes of incidents. This information can facilitate faster incident resolution.

For example, a group of employees can't access their e-mail. While trying to restore their e-mail access, Incident Management interfaces with Problem Management to help determine why the employees have lost e-mail access.Problem Management identifies certain known issues that affect the e-mail service, and provides a permanent fix that can be used to restore the employees' e-mail access.

Incident Management interfaces with **Access Management** when incidents relate to unauthorized access attempts or other types of security breaches.Access Management may use historical incident records from Incident Management to review access controls.Similarly, Incident Management may use information from Access Management to help resolve incidents that involve access breaches.

Incident Management also interfaces with 4 processes in the Service Design Stage.



Incident Management enables **Service Level Management (SLM)** to define measurable responses to service disruptions. It also assists with determining where services are at their

weakest, so that SLM can define actions as part of the service improvement plan. SLM defines the acceptable levels of service within which Incident Management works. It defines incident response times, impact definitions, target resolution times, service definitions, rules for requesting services, and expectations for providing feedback to users.

For example, a number of incidents that involve an application crashing are reported. SLM defines an uptime of this application of 99.5%, with a 60-minute resolution time for any downtime to the application.

Incident Management provides **Information Security Management** with incident information as needed to support Service Design activities and enable evaluation of the effectiveness of overall security measures.

For example, the Incident Management process might provide Information Security Management with a report of all unauthorized e-mail access incidents. Information Security Management would then use this information to evaluate current e-mail security measures.

Incident Management alerts **Capacity Management** to performance-related incidents. These may trigger performance monitoring and capacity changes. In turn, Capacity Management may help Incident Management resolve incidents - for instance by increasing the capacity that's available.

For example, employees continuously report that access to e-mail is unusually slow during peak times. Incident Management informs Capacity Management of the incident so that it can be monitored and further steps taken if necessary to increase the capacity of the network.

Availability Management uses Incident Management data to determine the actual availability of IT services. This can be compared to the required availability levels. Availability and Incident Management may then work together to improve service availability as necessary.

For example, Availability Management might use incident records created during the Incident Management process to determine the availability of an e-mail service. It could also interface with Incident Management to develop a plan to improve the service's availability.

Within the Service Transition stage, Incident Management interfaces with the Service Asset and Configuration Management (SACM) and Change Management processes

One of the uses of the **Configuration Management System (CSM)** is to identify faulty equipment and to assess the impact of associated incidents.

Incident Management can provide SACM with information about faulty Configuration Items (CIs). It can also help SACM assess the infrastructure of supporting services to help identify the cause of an incident and resolve it.

For example, SACM may identify a faulty router and determine that it could be contributing to incidents involving loss of e-mail access. Incident Management maintains information about the status of the router, which is fed back to the SACM process. It also uses information from SACM to help resolve the incident related to e-mail access.

Where a change is required to implement a workaround or resolution, this will need to be logged as a Request for Change (RFC) and handled through Change Management.

In turn, Incident Management detects and resolves incidents that arise from failed changes.

For example, an RFC may involve replacing an e-mail server. Once the change is approved and implemented, Incident Management would need to monitor the change closely to identify and resolve any incidents involving e-mail access that could arise as a result.

Problem, Event, Request and Access Management:
The Scope and Principles of Problem Management:
ITIL defines a problem as an underlying cause of one or more incidents.
Problem Management is the process for managing problems throughout their lifecycles. It forms part of the Service Operation stage of the ITIL® Service Lifecycle.

The purpose of Problem Management is to identify, document and resolve problems.

The Problem Management process covers several objectives:

- proactively prevent problems and associated incidents from occurring
- eliminate recurring incidents by identifying and resolving their root causes, and
- minimize the impact of problems that can't be prevented

Scope of Problem Management:
The scope of Problem Management includes diagnosing the root causes of incidents and determining resolutions.

Implementing resolutions through the appropriate control procedures, especially Change Management and Release and Deployment Management, is also included in Problem Management's scope.

Another aspect in Problem Management's scope is maintaining and documenting information about problems and appropriate workarounds and resolutions.

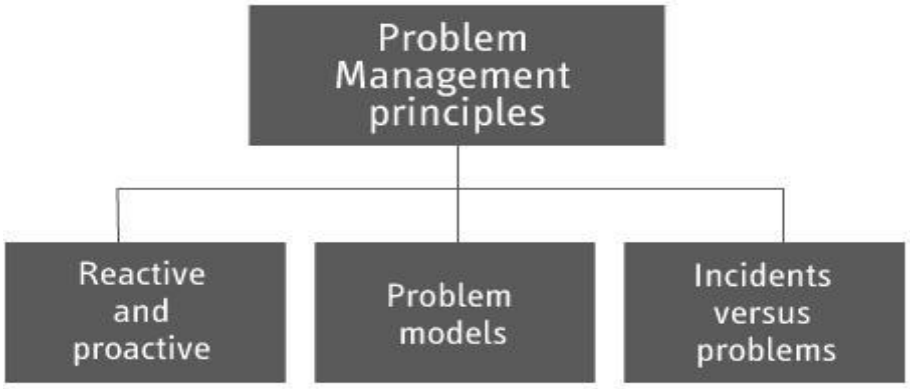
The purpose of a workaround is to reduce the number or severity of associated incidents until the underlying problem can be resolved – or to provide an alternative solution when it's not possible to eliminate the problem completely.

Several other activities fall within the scope of Problem Management:

- conducting periodic scheduled reviews of incident records to find patterns and trends that may indicate errors in the infrastructure
- conducting major incident reviews
- conducting periodic scheduled reviews of operational logs and maintenance records to identify patterns and trends in activities

- conducting periodic scheduled reviews of event logs to identify patterns and trends -for example, in warning and exception events records
- conducting brainstorming sessions to identify trends, and
- using check sheets to collect data on service or operational quality issues

Principles of Problem Management:
Effective Problem Management depends on three important principles. It should include both reactive and proactive approaches, it should make use of problem models, and it shouldn't be confused with Incident Management.



The difference between reactive and proactive Problem Management lies in how the Problem Management process is triggered.

Reactive Problem Management activities are triggered by incidents that have already occurred. These activities complement Incident Management activities by focusing on finding and resolving the underlying causes of incidents, and identifying workarounds when necessary.

The goal of improving overall service quality or delivery drives **proactive Problem Management**. It involves seeking out problems and resolving them before they cause incidents, or before incidents are directly linked to them. For example, trend analysis of historical incident records may suggest an underlying problem, which can then be investigated.

Proactive Problem Management complements Continual Service Improvement (CSI) activities. Both contribute to ongoing improvements in IT services - and problems identified through proactive Problem Management may be recorded in the CSI register as improvement opportunities.

Proactive Problem Management redirects the efforts of an organization from reacting to incidents to preventing incidents. This enables the organization to provide better service to its customers and make more effective use of available IT resources.

Another principle of effective Problem Management is to use **problem models**. Problem models are sequenced steps to follow when resolving specific types of problems, which increases efficiency in dealing with problems when they actually occur.

Problem models and workarounds for known errors should be recorded in a Known Error Database (KEDB) so they can be easily retrieved when they're needed.

A final principle for effective Problem Management is to avoid confusing it with incident management.

Incident Management and Problem Management focus on different areas.

An Incident is an unplanned interruption to an IT service or a reduction in the quality of an IT service. The cause may be an underlying problem. Users losing access to their e-mail is an example of an incident. Incident Management activities focus on restoring services to their normal state as soon as possible after service disruptions occur.

A problem is an actual or potential cause of incidents. A faulty e-mail server is an example of a problem. This could result in one or more incidents in which users lose access to e-mail services. Problem Management activities focus on finding ways to prevent incidents from occurring.

Although the two processes differ, they're obviously related - and Incident Management activities may invoke Problem Management activities. For example, one or more incidents handled through Incident Management may indicate an underlying problem, which is then recorded and handled through Problem Management.

The rules for invoking Problem Management during an incident may vary among different organizations.

It may be appropriate to invoke Problem Management during an incident in various circumstances:

- Problem Management may have information about existing problems and known errors that could be contributing to one or more incidents
- trend analysis of logged incidents suggests an underlying problem
- Problem Management activities can help identify the root cause of the incident
- a support group, a supplier, or other IT functions identify that a problem condition exists, or
- the service desk has resolved an incident but hasn't determined a definitive cause and suspects it's likely to recur

The Problem Management Process:

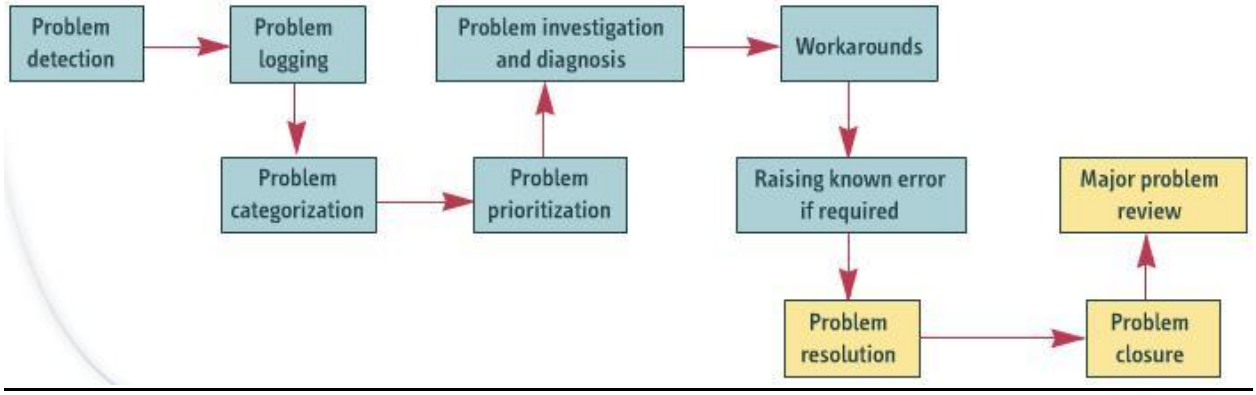
The Problem Management process, as outlined by ITIL©, consists of ten steps. First a problem is detected. Then it's logged, categorized, and prioritized.

The problem is investigated and diagnosed, and, if possible, a workaround is developed to address the problem temporarily.

If relevant, a known error record is then raised.

Finally, to resolve the problem, you typically follow these three steps:

- implement the solution to the problem
- close the problem record, and
- if the problem was classified as major, review the problem and its resolution



Step1: Problem Detection:
Problem Management personnel typically detect a problem in one of two ways:

- reactively, or
- pro actively

The Problem Management process may be triggered in **response** to a problem that has already been reported. For example, a problem maybe reported by a service desk if it appears to be the cause of certain incidents. A problem may also be identified by a technical support group that analyzes an incident, by an automated system, or by a supplier or contractor.

A problem may be detected as a result of **proactive** activities, designed to identity problems before they have serious negative effects on customers or users. For example, a problem may be identified through regular quality of service improvement activities.

For example, a service desk receives reports from several regional sales representatives, who can't access the company virtual private network (VPN) to upload their daily sales orders.

After logging each of the reported incidents, the service desk opens a problem report - because the incidents indicate an underlying problem.

Step2: Problem Logging:
Once a problem has been detected, its details should be recorded. This ensures that the problem can be adequately tracked and managed, and that the organization accumulates an historical record of all problems.

The initial problem record should be updated throughout the remainder of the problem's life cycle.

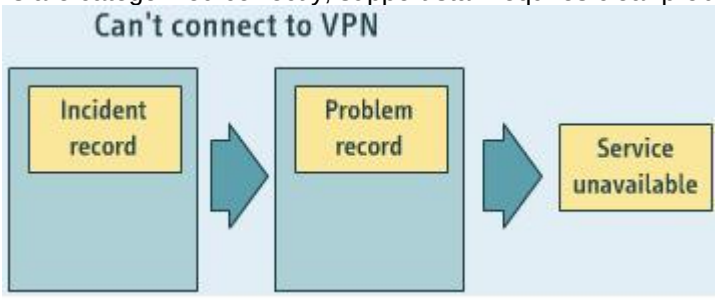
Some of the details that should be logged in a problem record are

- details of the individual reporting the problem
- the date and time the problem was initially logged
- service and equipment details
- priority and categorization details
- information about any incidents thought to be associated with the problem, including incident record numbers, and
- details of all diagnostic or attempted recovery actions taken

Step3: Problem Categorization:
Next a problem should be categorized, using the same coding system that was used to categorize any associated incidents.

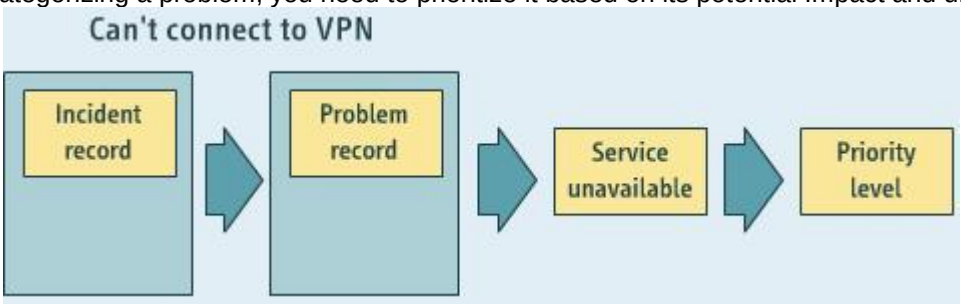
For example, incidents and associated problems may be categorized as "service unavailable" or" slow performance"

To ensure problems are categorized correctly, support staff requires clear problem definitions.



Step4: Problem Prioritization:

After categorizing a problem, you need to prioritize it based on its potential Impact and urgency.



Each problem should be assigned an appropriate priority code level, which may be mapped to a corresponding target resolution time.

For instance, the VPN access problem that's preventing sales orders from being uploaded may be assigned a medium level of impact and a high level of urgency. Using a simple coding system, the problem can then be assigned the code 2 - which is associated with a target resolution time of 8 hours.

Priority coding system

Urgency	Impact: High	Impact: Medium	Impact: Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

Priority code	Desciption	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

Step5: problem investigation and diagnosis:
Once a problem has been prioritized, it should be investigated and diagnosed, with the aim of uncovering its root cause.

The speed and nature of this investigation will vary depending on the priority assigned to the problem and the associated target resolution time.

Some of the problem-solving techniques you can use to investigate and diagnose a problem include

- brainstorming
- the "5-Whys" technique
- fault isolation
- affinity mapping
- hypothesis testing
- technical observation post
- Ishikawa diagram, and
- Pareto analysis

During a **brainstorming** session, a group generates as many ideas as possible about the causes of a problem and resolutions. The group then narrows down its ideas, agrees on actions, and documents the results.

The **5-Whys technique** is a simple but effective method of getting to the root cause of a problem you start by describing the problem and then ask "Why did this happen?" Each response is then followed up by another "Why?" question. It often takes five questions to determine the root cause of a problem.

To **isolate a fault**, it's usually necessary to replicate the events that led to the problem. You then investigate the Configuration item (CI) at the start of the event, followed by each subsequent CI, until you find the fault. If the fault can't be recreated, you investigate the healthy state of each CI involved in the event.

Affinity mapping is commonly done during brainstorming sessions with key support staff. Possible solutions are recorded on individual cards and then grouped according to similar characteristics. A "header" is assigned to each group for future identification and examined for a root cause.

When using **hypothesis testing**, a team generates a list of possible root causes based on educated guesses. It then determines which are true and which are false.

The **technical observation post** enables specialist technical support staff from within the IT support organization to monitor events in real time, in order to catch problems as they occur, and potentially identify possible causes of the problem.

An **Ishikawa diagram** is usually developed during a brainstorming session, during which a problem is discussed in order to increase understanding and identity the source of a problem. The main trunk of the diagram charts the problem. Possible causes are represented by the trunk's branches, and secondary factors are added as stems.

Pareto analysis is a statistical method used to determine the most important, or frequently occurring, potential failures. It's based on the Pareto principle, or the 80-20 rule, which states that 80% of problems are caused by 20% of the causes.

You can use the Configuration Management System (CMS) to help diagnose the exact point of a failure.

You can also use the Known Error Database (KEDB) and problem-matching techniques, such as keyword searches, to establish if a problem has occurred before and to check for a predefined resolution.

You may want to re-create the failure in a test environment that mirrors the live environment to find out the cause of the problem and then to find the most appropriate and cost-effective resolution. A test environment enables you to investigate and diagnose the problem without causing further disruptions to users.

When the problem of offsite agents being unable to upload sales orders is investigated, logs reveal that similar incidents happened on two separate occasions. In both cases, the incidents were reported after the configuration of the same router was updated.

It's then established that the root cause is a corrupt line of code that was introduced during a router configuration update.

A viable solution to the problem then is to reconfigure the router to remove the faulty coding.

Step6: Workaround:
A workaround is a temporary method of overcoming the difficulties that a problem has introduced. Even if a workaround exists, it's important to continue working toward a permanent resolution. It's also important to document the details of a workaround and keep the problem record open.

Sometimes multiple workarounds exist, and each helps reduce the impact and urgency of a problem - with the result that its priority level may be reduced.

For example, it may be possible to establish a connection between offsite sales agents and a company server by reconfiguring a backup router. It may also be possible to let all agents fax their sales orders rather that submit electronically until the problem is resolved.

Step7: Raising known error if required:
A known error is defined as a problem with a documented root cause and workaround.

A known error record should be opened, or raised, as soon as a problem has been diagnosed and a workaround has been found, if one exists. The record should then be entered in the KEDB for future reference.

Sometimes it's necessary to raise a known error record even before problem diagnosis is complete and a workaround is found. For example, this might be done for information purposes or to identify a root cause or workaround that appears to address a problem, but that hasn't been confirmed.

A known error record should

- identity the problem record to which it relates
- document the status of actions being taken to resolve the problem
- identify the root cause, and
- document the workaround

Step8: Problem Resolution:
Once a solution to a problem has been determined, it can be applied.

During this step, it's vital that safeguards are introduced to ensure the resolution doesn't create further difficulties. If any change in functionality is required, a Request for Change (RFC) - a formal proposal for a change - should be raised and authorized before the resolution is applied.

If the problem is serious and an urgent fix is needed for business reasons, an emergency RFC should be raised. The resolution should be applied only once the change has been authorized and scheduled for release. In the meantime, the KEDB should be used to help resolve any further occurrences of the problems that may occur.

If the resolution to a problem can’t be justified -for example, because its cost is too high - a decision may be taken to leave the problem record open and to rely on a workaround.
The priority of the problem may also then be reduced, based on the effect of the workaround
In the case of sales agents who can’t use a VPN to upload their sales orders, a resolution might be to install a dedicated router, to eliminate or reduce the introduction of errors in configuration updates. This would require an RFC because it involves a change to the network infrastructure.

If the organization decides not to install a dedicated router, any future router configuration updates should be amended to include testing the functionality of the sales submission software before it goes live.

Step9: Problem Closure:
Once a final resolution has been applied, the problem record is checked to ensure it is fully updated. The problem record and any related incident records that are still open are then closed.

Also, the status of any related known error record is updated to show that the resolution has been applied.

Step10: Major Problem Review:
As the final step in Performance Management, major problems - as defined based on an organization's priority system - should be reviewed so the organization can learn any lessons for the future.
The review should examine

- things that were done correctly
- things that were done wrong
- what could be done better in the future
- how to prevent similar problems from recurring, and
- whether there was any third-party responsibility for the problems and whether follow-up actions are needed

The results of a major problem review should be used to

- train staff and raise awareness
- provide input to proactive Problem Management, and
- inform service review meetings

The results of a major problem review should be used as part of **training and awareness** activities for support staff. Any lessons learned should be documented in appropriate procedures, work instructions, diagnostic scripts, or known error records. The problem manager should facilitate the session and document any agreed actions.

The results of major problem review can help indicate potential causes of other problems, or of problems that may occur in the future.

The results should be incorporated into a **service review meeting** with the customer or user groups. This is done to ensure that the customer is aware of the actions taken and of the plans to prevent future major incidents from occurring. It helps to improve customer satisfaction and assure the business that Service Operation is handling major incidents responsibly and actively working to prevent their future recurrence.

The lesson learned from the router configuration update that resulted in sales agents not being able to upload their sales orders is to implement more thorough beta testing of router configuration updates, at least for systems and software that are deemed critical.

Problem Management Interfaces:
The Problem Management process is responsible for dealing with all problems that may occur in the ITIL® Service Lifecycle stages. To do this effectively, it has to interface with various processes in each of the lifecycle stages.

Problem Management Interface with Service Strategy:
In the Service Strategy stage, Problem Management interfaces with the Financial Management for IT services process. Problem Management provides information that supports Financial Management because it assists in assessing the impact - including the financial impact - of proposed workarounds and solutions.

So Problem Management can provide Financial Management for IT services with information about the costs of resolving and preventing problems. This information can then be used as input into budgeting and accounting systems, and in Total Cost of Ownership (TCO) calculations.

In turn, Financial Management for IT services may provide Problem Management with useful information, including the results of pain value analysis. This type of analysis identifies the areas

of the IT infrastructure in which problems and incidents could have the most severe impact on the business.

Problem Management Interface with Service Design:
Problem Management interacts with four Service Design processes:

- Availability Management
- Capacity Management
- IT Service Continuity Management, and
- Service Level Management (SLM)

Availability Management helps determine how to maximize the availability of IT services - or to ensure that the availability levels defined in Service Level Agreements (SLAs) are provided. Problem Management supports this process by providing information about problems that may reduce availability, and by resolving these problems or generating appropriate methods for working around them.

Some problems, like those Involving performance issues, may require investigation by **Capacity Management** teams. Both Capacity Management and Problem Management may cooperate to diagnose and resolve these problems. Capacity Management also plays a role in taking proactive measures to prevent problems from occurring.

During capacity planning, Problem Management may provide information that affects capacity-related decisions. For example, it may identify problems that could be solved by increasing an organization's hardware or bandwidth capacity.

Problem Management acts as an entry point into **IT Service Continuity Management** in situations where a significant problem isn't resolved before it starts to have a major impact on business.

For example, a router that supports a key business process is faulty but the manufacturer can't deliver a replacement for a few days. Problem Management would interface with IT Service Continuity management so a temporary process or fix can be implemented, to ensure service continues with as little interruption or loss as possible to users and customers.

Problem Management contributes to improvements in the service levels that are agreed and monitored through the **SLM** process. The information it provides may also determine the Service Level Agreement (SLA) review components used by SLM.

In turn, SLM provides the parameters that Problem Management works within by defining service level targets.

SLM also reviews service levels, potentially helping identify problems that should be resolved through Problem Management.

Problem Management Interface with Service Transition:
Problem Management interfaces with various processes in the Service Transition stage. One of the most important of these is Change Management.

Problem Management is responsible for ensuring that any changes to Configuration Items (CIs) that are needed to resolve problems are submitted to Change Management for approval, in the form of Requests for Changes (RFCs).

Change Management processes help to monitor the progress of these changes. The outcomes are then filtered into Problem Management processes which are responsible for correcting all failed changes.

Problem Management also interfaces with the Service Asset and Configuration Management (SACM) process in the Service Transition stage.

Problem Management uses the Configuration Management System (CMS) that's set up and maintained through SACM to identity faulty CIs and to determine the impacts of problems and resolutions.

Problem Management also interacts with Knowledge Management - another process in the Service Transition stage. It uses the Service Knowledge Management System (SKMS) as the basis of the Known Error Database (KEDB), which can hold or integrate with problem records.

A final Service Transition process that interacts with Problem Management is Release and Deployment Management, which is responsible in-deploying problem fixes into the live environment.

This process also helps ensure that the associated known errors are transferred from the development KEDB into the live KEDB.

In turn, Problem Management helps to resolve any problems that are caused by faults during the Release and Deployment Management process.

Problem Management also interfaces with the Continual Service Improvement (CSI) lifecycle stage. The occurrence of incidents and problems provides 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 or customer satisfaction.

Event, Request and Access Management:

In addition to Incident Management and Problem Management, three other processes occur during the Service Operation Stage of the ITIL Service Lifecycle.

These processes are

- Event Management
- Request Fulfillment, and
- Access Management

An **event** is any change of state that has significance for the management of a Configuration Item (CI) or IT service. The purpose of Event Management is to manage events throughout their lifecycles. Associated activities include detecting events, making sense of them, and determining and coordinating the appropriate control actions.

A service request is any request or demand that a user makes to an IT organization. Many of these requests are for common or minor actions involving low risk and low costs, or for simple information. **Request Fulfillment** is the process responsible for managing the lifecycles of all service requests.

Access Management is the process of granting specific authorized users the rights to use services, while also preventing unauthorized users from gaining access to them. It involves executing the policies and actions defined through Information Security Management.

Event Management:

Event Management is focused on generating and detecting meaningful notifications about the status of an organization's IT infrastructure and services.

It's also the basis for operational monitoring and control. If events are programmed to communicate operational information, warnings, and exceptions to the IT Department, they can be used as a basis for automating many routine operations and management activities.

Examples are executing scripts on remote devices, submitting jobs for processing, or dynamically balancing the demand for a service across multiple devices to enhance performance.

Objectives of Event Management:
The objectives of the Event Management process ate to

- detect all changes of state that have significance for the management of a CI or IT service
- determine the appropriate control action for events and ensure these are communicated to the appropriate functions
- provide the trigger, or entry point, for the execution of many Service Operation processes and operations management activities
- provide the means to compare actual operating performance and behavior against design standards and Service Level Agreements (SLAs), and
- provide a basis for service assurance and reporting, and service improvement

Event Management can be applied to any aspect of IT Service Management that needs to be controlled and that can be automated. This includes events associated with

- CIs
- environmental conditions
- software licensing
- security, and
- normal IT activity

Some CIs may be included in the scope of Event Management because they need to stay in a constant state. For example, a switch on a network may need to stay on. Tools may confirm that the switch does stay on by monitoring responses to pings.
Other CIs may be included because their status needs to change frequently and Event Management can be used to automate this process - for example, using a script to perform routine updates to a file server.

Environmental conditions ranging from temperature fluctuations to natural disasters like earthquakes can generate events, and these fall within the scope of Event Management.

For example, Event Management may include responding to alerts indicating that the controls for regulating temperature in a server room have failed.

Software license monitoring - to ensure optimum and legal use of software licenses - falls within the scope of Event Management.

For example, an event monitoring system may raise alerts when the licenses on specific software is about to expire.

Security events fall within the scope of the Event Management process. For example, Event Management software installed on a LAN may raise an alert if any unauthorized attempt at network access is detected.

Normal IT activity often falls within the scope of Event Management. For example, Event Management may involve using software to track the use of a particular application or the performance of a server.

Request Fulfillment:

Request Fulfillment plays an important role in maintaining end user satisfaction by ensuring that users' requests are satisfied as promptly and efficiently as possible.

To ensure common types of requests are fulfilled within a reasonable time, it's important to have documented processes in place for handling these requests.

This prevents minor requests from congesting the normal Incident Management and Change Management processes, and negatively impacting overall service delivery.

Objectives of Request Fulfillment:
The objectives of the Request Fulfillment process are to

- maintain user and customer satisfaction through efficient and professional handling of all 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, and
- assist users by providing general information and handling complaints

The process needed to fulfill a request will vary depending on the request, but it can usually be broken down into a set of activities.

For each type of request, these activities should be documented in a request model.

For example, think of a manager who requires reminders of login details for a rarely used work e-mail account and approaches the IT Department with a request.

In the manager's organization, a dedicated IT team follows the model that lists the appropriate Request Fulfillment steps. These involve identifying the request, consulting the appropriate expert, and finally fulfilling the request.

The team then logs the request and liaises with network administrative staff to recover the forgotten login details. The team then communicates the information to the manager.

The Request Fulfillment process is handled differently in different organizations. For example, service requests may be treated as

- a separate work stream
- incidents, or
- the responsibility of an expanded service desk

In an organization that deals with varied requests that may require specialist knowledge, service requests maybe dealt with as a separate work stream. This is essential if a requests and incidents are handled by different groups of employees. In the example of the manager requesting login details, the separate work stream is a dedicated IT team that fulfills the request.

Some organizations handle service requests through the Incident Management process. Service requests are then handled as a particular type of planned incident - unlike regular incidents, which are unplanned.

In some organizations, an expanded service desk handles all employees' service requests. For example, this type of service desk may handle requests to service a photocopier or even requests associated with building management issues, such as replacing a light fitting or repairing a leak in the plumbing.

Access Management:

The purpose of Access Management is to grant specific users rights to use specific services. Some organizations may refer to this process as Rights Management or Identity Management.

The objectives of the Access Management process are to

- manage access to services based on policies and actions defined in Information Security Management
- respond efficiently and appropriately to requests for granting access to services, changing access rights, or restricting access, and
- oversee access to services and ensure that the assigned rights are properly used

The Access Management process executes the policies defined through Information Security Management. For example, it may implement a policy that allows only specified managers in a Human Resources Department to access a payroll application.

By implementing information security measures, Access Management enables an organization to manage the confidentiality, availability, and integrity of its data, including intellectual property.

Although Access Management ensures that users are given the appropriate rights to use a service, it's Availability Management that ensures that this access is available at all agreed times. Access Management is usually included in all technical and application management functions. However, it's usually coordinated through a single control point - such as IT operations management or a service desk.

A service request may initiate Access Management - for example, if an employee requests rights to specific information or services on an office network.

ITIL 2011 Foundation: Module 9: Continual Service Improvement:

CSI Scope:

According to ITIL®, Continual Service Improvement (CSI) is the stage of the Service Lifecycle that involves identifying and implementing improvements to IT services that support business processes. In this way, it helps ensure that IT services are aligned with ever-changing business needs.

CSI draws on principles, practices, and methods from processes like Quality Management, Change Management, and Capacity Management, combining these to improve performance throughout all the stages of the Service Lifecycle.

Throughout the CSI stage, the performance of an IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure where necessary. This can result in improved IT service quality, operational efficiency, and better cost efficiency.

Objectives of CSI:

CSI has several objectives:

- review, analyze, prioritize, and make recommendations for improvements in the lifecycle stages
- review and analyze service level achievements
- identity and implement activities to improve IT service quality
- improve the efficiency and effectiveness of the processes that enable the provision of IT services
- improve cost effectiveness of IT services without negatively impacting customer satisfaction
- ensure that appropriate quality management methods are used to support improvement activities
- ensure that processes have clearly defined objectives and that progress toward achieving these can be measured

The CSI stage should use a "closed loop" feedback system that's based on the **Plan-Do-Check-Act (PDCA)** cycle.

Through this feedback system, the output or feedback from any stage in the Service Lifecycle can be used to identify improvement opportunities for any other stage. For example, outputs from the Problem Management process - which is part of the Service Operation stage -may point to the need for an improvement in the Service Design or Service Transition stages.

All CSI initiatives

- Should have clearly defined goals and objectives.
- Should also ensure that the success of each service improvement initiative can be properly measured in terms of its success or failure in meeting the specified goals.
- Ensure that resources aren’t wasted on improvement initiatives that aren't really needed.

Another important consideration when implementing CSI is that it's critical to understand what to measure and why, as well as what the successful outcome of an improvement initiative should be.

Without this understanding, the conclusions you reach about what improvements are needed, and about the success or failure of these improvements once they've been implemented, maybe invalid.

CSI provides best-practice guidance in four main areas.

First it provides guidance on the overall health of IT Service Management as a discipline.

It also provides continual alignment of the IT Service Portfolio with service users' current and future business needs.

CSI also provides guidance for the maturity and capability of the IT service provider and its supporting management, processes, and people.

Last it provides guidance for the continual improvement of all aspects of IT services and the service assets that support them.

CSI depends on ten supporting activities. The first five activities include

- reviewing management information and trends to ensure that IT services are meeting the agreed service levels
- reviewing management information and trends to ensure that the output of the enabling processes are achieving the desired results
- conducting maturity assessments to demonstrate areas for improvement, as well as areas of concern
- conducting internal audits to verify employee and process compliance, and
- reviewing existing deliverables for appropriateness

The remaining five supporting activities include

- proposing recommendations for improvement opportunities
- conducting customer satisfaction surveys
- reviewing business trends and changed priorities to keep ahead of business projections
- conducting external and internal service reviews to identify CSI opportunities, and
- measuring and identifying the value created by CSI improvements

Benefits for organization adopting best CSI practices:
For an organization, adopting and implementing standard and consistent approaches for CSI has several benefits:

- it leads to continual improvements in service quality and customer satisfaction
- it ensures that IT services are aligned with business needs
- it increases the cost effectiveness of service provisioning by reducing costs or enabling an organization to handle more work at the same cost
- it uses monitoring and reporting to identify potential opportunities for improvement in all lifecycle stages, and
- it identifies opportunities for improvements in an organization's structure, resourcing capabilities, partners, technology, staff skills and training, and communications

The CSI Register:
An important activity in the Continual Service Improvement (CSI) stage of the Service Lifecycle is recording all improvement opportunities and their details in a CSI register.

A CSI register is a database or structured document used to record and manage improvement opportunities throughout their lifecycles.

The CSI register serves four main purposes:

- it is a tool to record all improvement opportunities (provides CSI with a structured approach for recording, monitoring, and reviewing service improvement efforts across an organization)
- it is a tool to categorize improvement opportunities (categorization helps make it clear how best to prioritize improvement initiatives and allocate resources and also to change priorities when necessary)
- it is a tool to catalog the benefits that can be achieved by implementing improvement initiatives
- it provides a coordinated, consistent view of all improvement activities

Ideally a dedicated CSI manager should be responsible for the production and maintenance of a CSI register. This helps ensure that a consistent approach is used and that the need to update the register isn't overlooked.

The CSI register contains important information for service providers and so should be regarded as part of an organization's overall Service Knowledge Management System (SKMS).

The SKMS is the set of tools and databases that an IT service provider uses to manage the knowledge, information, and data required to manage the full lifecycle of all IT services.

Like other components of the SKMS, such as the Configuration Management System (CMS), the CSI register should be properly updated and maintained.

Another best practice is to ensure that for each recorded improvement initiative, suitable Key Performance Indicators (KPIs) are also identified in the CSI register. These are metrics for measuring whether an initiative is providing the desired key benefits.

For example, a KPI for an initiative that involves increasing the total bandwidth available to network users might be the average speed of data transmission on the network. The KPI provides a concrete and objective way to gauge the success or failure of the initiative.

The use of KPIs can help improve and quantify the overall performance of CSI.

A final best practice is to define the interface between the CSI register and other processes in the Service Lifecycle. The information recorded in the register should inform processes in other lifecycle stages.

Similarly, the outputs of processes like Change Management, Problem Management, and Capacity Management should trigger the entry of new improvement opportunities in the register when it makes sense.

The results of service reviews are also likely to result in improvement requirements that should be recorded in the CSI register.

ITIL® doesn't provide strict rules about how the CSI register should be formatted or about exactly what information it should include.
Instead, each organization should evaluate its own requirements and create a CSI register that suits its own purposes.

A CSI register typically takes an electronic format. For example, it may be a database or a spreadsheet. However, smaller organizations may keep a paper register.

Although each organization should determine the layout and format of the CSI register it uses, certain types of information should generally be included.

Opportunity no.	Date raised	Size (small, medium, large)	Timescale (short, medium, long)
1	01/04	Small	Short

The **opportunity number** is a reference number that's assigned to an entry in the CSI register. Ideally it should identify the order of records in the register based on when they were entered.

The **date raised** is the date when an improvement opportunity or initiative was first entered in the CSI register. Alternatively, it may indicate when the issue requiring improvement was first identified.

The **size** refers to the scale of a needed improvement or initiative, based on how much work and effort it will require. Generally, an entry in the register is categorized just as small, medium, or large.

In a **timescale** field, you record the estimated time it will take to complete an improvement or initiative, or to resolve a specified issue. Often an improvement initiative is categorized simply as being of short-, medium-, or long-term duration.

The CSI register should include a **description** of each improvement opportunity or issue and, when possible, of its likely causes.

Description
A number of failures have occurred when implementing new or updated applications. This has been caused by the testing procedure in release and deployment using out-of-date test data. The requirement is to update the test data in repository test 4371.

Information derived from Change Management, Problem Management, or Capacity Management may also be mentioned here to indicate which processes are required or are involved in the issue.

A **priority** field should indicate how urgently an improvement is required to be implemented. For example, using a code from 1 to 4, with 1 indicating urgent and 4 indicating the lowest priority. This helps ensure that the most serious issues are recognized and dealt with first, given limits on available resources.

A **KPI metric** field should list one or more appropriate KPIs for measuring the success of each improvement initiative,

It's also useful to provide a **Justification** field for explaining the choice of a particular KPI metric - or for justifying the need for a particular improvement initiative based on the benefits it will have.

Priority (urgent, 1, 2, 3, 4)	KPI metric	Justification	
1	*n*% reduction in failures	Significant reduction in failures after transition and resulting business impact.	

Three further fields are useful to include in the CSI register.

It's useful to **record the name of the person who first raised the improvement initiative**. For example, this might be an employee who discovered a way a system could function better.

It's important to specify **who's responsible for ensuring that each improvement is implemented**, to ensure that needed improvements aren't overlooked or put aside.

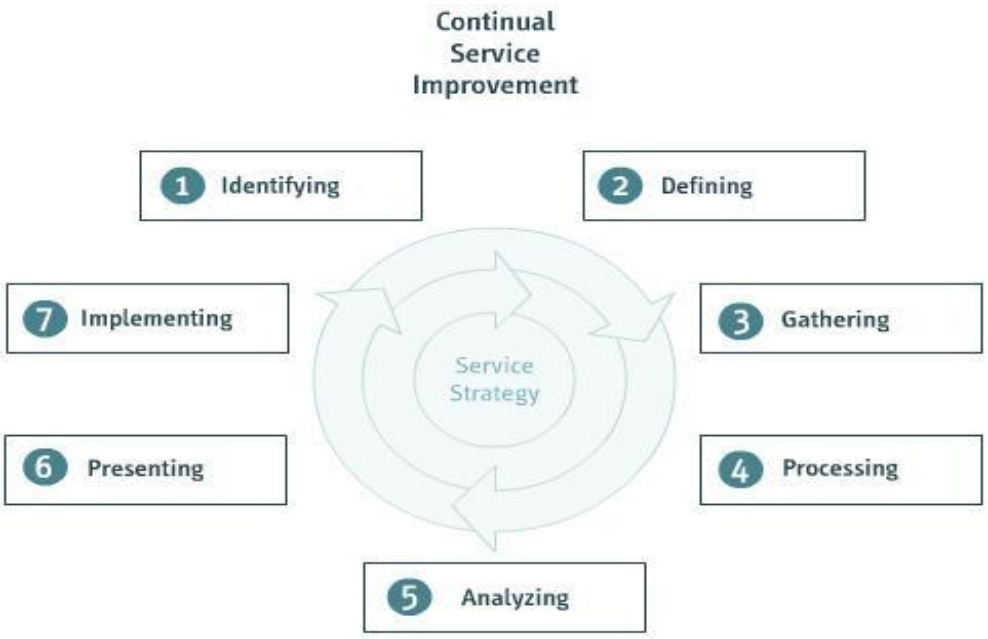
When relevant, a CSI register should **record the date by which an improvement must be completed implemented**, or an issue fully resolved.

Raised by	To be actioned by	Date required by
E. King	R. Bergman	01/14

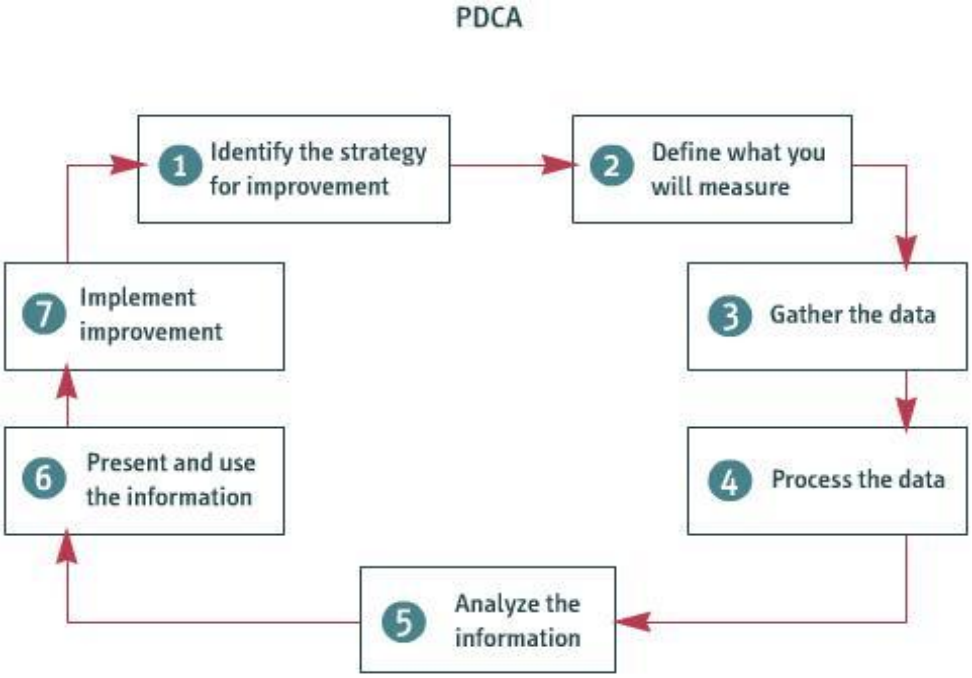
Introduction to CSI Process:

Many activities have to be completed to ensure effective Continual Service Improvement (CSI) across the Service Lifecycle.

ITIL® prescribes a seven-step improvement process for incorporating these activities. The process involves **identifying, defining, gathering, processing, analyzing, presenting,** and then **implementing** the service improvements.

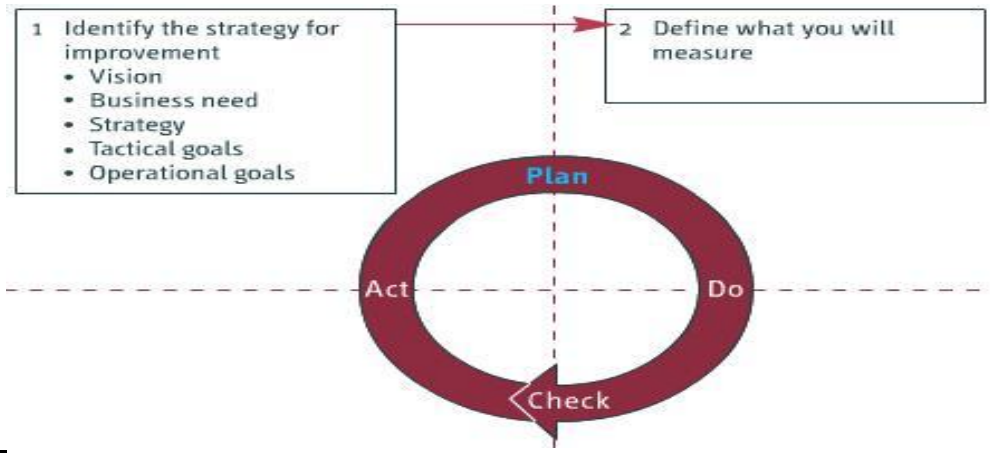


This process integrates with the **Plan-Do-Check-Act (PDCA) cycle** to provide reliable, ongoing service improvements.

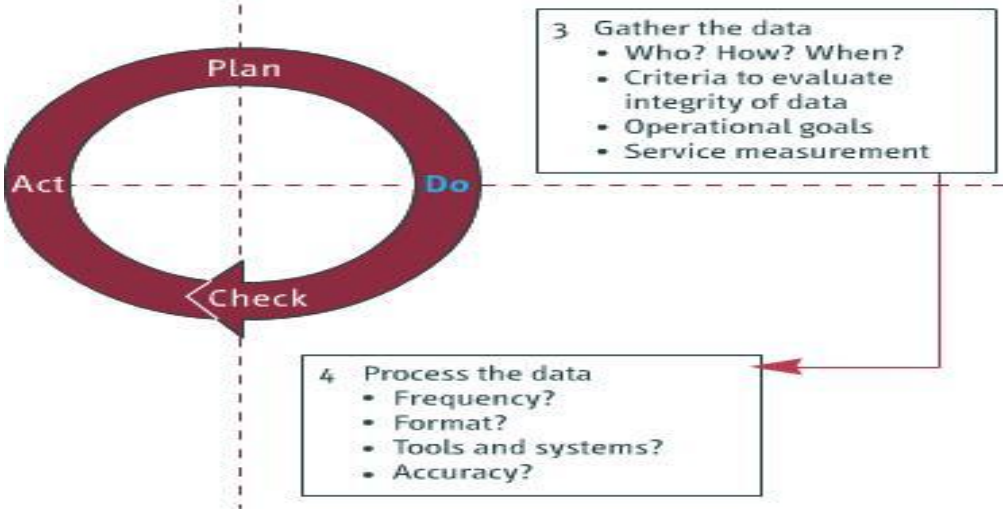


The PDCA cycle includes four steps, each of which maps to specific CSI activities in the seven-step improvement process.

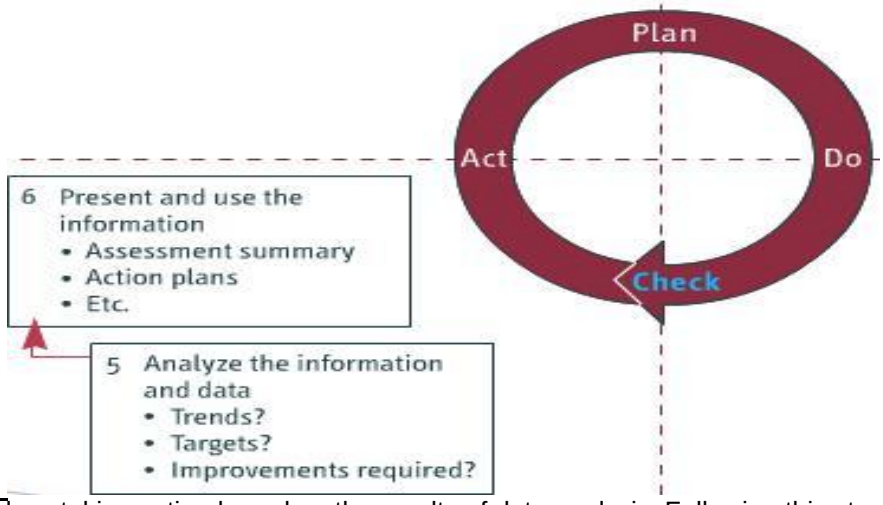
The Plan step involves identifying the vision, business need, and operational and strategic goals driving the need for improvements. Once these are in place, you can identify opportunities for specific improvements and their associated Key Performance Indicators (KPIs) for measurement.



The Do step involves collecting raw data from service operations and then processing this data, using Critical Success Factors (CSFs) to ensure that all of it is evaluated in the same context.



The Check step involves analyzing the prepared data to reveal business trends and the success or failure of the strategy determined in the Plan step. You can then communicate the analyzed data and conclusions about the effectiveness of service improvement efforts to stakeholders.



The Act step involves taking action based on the results of data analysis. Following this step, an organization establishes a new baseline and the PDCA cycle can begin again.

Objectives of CSI Process:
The objectives of the CSI process are to

- identify opportunities for improving services (example improved bandwidth or connectivity)
- reduce the cost of providing services
- identify what needs to be measured (example include measuring the bandwidth provided to customers compared to the price paid by the provider, and the stability of different types of customer connection technology)
- continually review service achievements (to ensure that they remain aligned with business requirements)
- understand what to measure (for example the bandwidth transfer rates of different technology, and the cost versus effectiveness of different types of broadcast technologies and strategies)

Every potential improvement opportunity should be accompanied by a business case, or justification, to show how it will benefit a business overall.

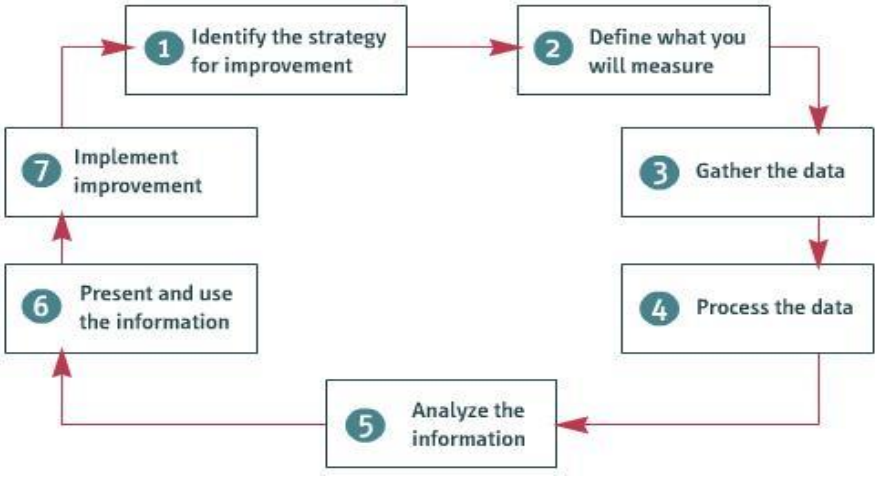
Although cost reduction is a clear objective, it should be achieved without sacrificing quality. Similarly, improvements in quality shouldn't be implemented unless the costs of making the improvements are warranted.

It's important to note that the seven-step improvement process isn't independent. It will achieve the desired outcomes only when applied to technology, services, processes, the organization, and its partners.

The Scope of CSI Seven Step Improvement Process:
The scope of the CSI seven-step improvement process includes

- service analysis (analyzing the performance and capabilities of services, processes throughout the lifecycle, organizational partners, and technology)
- service alignment (continual **alignment** of the IT Service Portfolio with the current and future business needs of service users)
- service technology (make best possible use of existing technology and exploit new technology)
- Organizational structure and personnel (The process can be used to assess and improve **organizational structure** and the capabilities of personnel. For example, you can use it to determine whether people are working in appropriate functions and roles, and if they have the required skills)

<u>The CSI Seven-Step Improvement Process:</u>
The Continual Service Improvement (CSI) process includes seven steps.



The aim of the process is to ensure ongoing improvement of IT services so that these services meet business needs and support the desired business outcomes.

Step1: Identify the strategy for improvement:
To start the CSI process, you need to ask pertinent questions to help identity an appropriate strategy for improvement. For example, what are the organization's business and IT strategies and plans for the coming months and years? And what do these plans indicate you should focus on improving?

The strategy you formulate should be designed to enable the business to perform optimally, with as few constraints as possible posed by the quality or costs of IT services.

To identify an appropriate strategy, you assess the organization's

- technical operational goals and strategic goals, and
- upcoming business and IT plans

An **organization's strategic goals** will help you determine its overall IT service needs, and so help shape the focus of service improvement efforts. For example, if an organization's strategic goal is to provide customers with a service at a lower cost than its competitors, IT service improvements may focus on improving efficiency and cutting operating costs.

Technical operational goals will give you more specific requirements for IT service improvements. For example, a goal of reducing the time it takes to complete a particular process may depend on specific improvements in the performance of an IT system or in data transfer rates.

Upcoming business and IT plans may have implications for the improvement strategy you choose. For instance, business expansion plans may require a focus on increasing network capacity. Plans to upgrade a company's information management system may create a corresponding need for higher-bandwidth network connections.

Among the questions you can ask to help identify a strategy for improvement are "What are the organization's business objectives?" "What effects do poor internal IT services have on profits?" and "How can improvements in IT services help the organization achieve its business objectives?"

An organization's business objectives help reveal its strategy.

And improvements in IT services can help support a business objective point to suitable technical operational goals.

Step2: Define what will you measure?
Once you've identified the strategy for improvement, you need to decide how progress will be measured.
In this step, you

- define what you should measure
- define what you can actually measure
- conduct a gap analysis, and
- finalize a measurement plan

To define what you'll measure to track service improvements, you should assess

- service elements (break service or service management in to service elements so you can determine which elements it's possible to measure)
- Performance indicators (how are performance, availability, and quality currently measured - and how could they be measured?)

- the goals of the target audience (so that you don't waste time and money on improvements that your internal or external customers consider unnecessary)

Accordingly, once you've identified an improvement strategy, you should establish metrics designed to measure service elements that customers and users consider important, or that are key to customers achieving their own business goals.

During the CSI stage, it may be relevant to measure

- customer and user levels of satisfaction with existing IT services
- the business impact of IT service disruptions
- the performance of third-party suppliers, and
- market performance, to establish whether IT services are in line with or superior to those offered by other service providers

Step3: Gather the data:
Gathering data involves monitoring the service or Service Management processes using application, system, monitoring tools or, in certain cases, a manual monitoring process.

Typically you focus on monitoring quality, or the effectiveness and efficiency, of a service, process, tool, or Configuration Item (CI) and identify where improvements can be made. So monitoring for CSI tends to focus on detecting exceptions and tracking resolutions.
However, you shouldn't focus only on monitoring for exceptions or weaknesses. If a Service Level Agreement (SLA) is consistently met over time, you should focus on determining whether that level of performance can be sustained at a lower cost - or whether the targeted service levels need to be adjusted due to changing business requirements.

You won't need or be able to cope with the vast quantities of data produced by all monitoring activities, so the focus in the CSI process will be on a specific subset of monitoring at any given time.

When a new IT service is being designed or an existing one changed, this is a perfect opportunity to ensure that the service requirements contain what CSI needs to monitor.

To support CSI, you typically need to collect

- technology metrics (performance and availability of IT service components, apps)
- Process metrics (CSFs, KPIs, activity metrics for the Service Management processes. These metrics can help determine the overall health of a process)
- service metrics (measure the overall effectiveness or output of an end-to-end IT service)

Step4: Process the data:
The next step is to process the gathered data. Through processing convert the data that has been gathered into a usable format that can be interpreted and analyzed.

Data processing may be automated or manual. Automated data gathering and processing is less vulnerable to errors than manual processing, so it's good practice to automate as much as possible.

Where manual processing is required, it's vital for employees to document their compliance activities, and to keep logs and records updated. For instance, you may need certain employees to log the time it takes to upload specific types of files.

Step5: Analyze the information:
This step involves transforming the data you've processed into useful information, including information about improvement opportunities.

During analysis, you assess the extent to which the measured service or Service Management process is meeting specified goals and objectives. You also document your observations and conclusions clearly.

When analyzing data, it's important to ask questions such as

- Are operations running according to plan?
- Are targets defined in SLAs or the Service Catalog being met?
- Are there underlying structural problems that can be identified?
- Are improvements required?
- Are there any trends, and if so, what are the trends showing and are they positive or negative?
- What is leading to or causing the trends?

It's good practice to review trends over a period of time. Just a snapshot view of data about a service or Service Management process is unlikely to be very informative. Instead, it's useful to ask "How did we do this month compared with last month, this quarter compared with last quarter, this year compared with last year?"

If you detect an anomaly, verify that it's not actually part of a trend - and investigate its possible causes.

Similarly, investigate trends - or changes in trends - to determine their underlying causes

Step6: Present and use the information:
The sixth step in the CSI process is to present the analyzed data - in reports, action plans, reviews, evaluations, and identified improvement opportunities - to relevant stakeholders and target audience in a way they will find it easy to understand.

It's important to include only information that's of value to your particular target audience. You should note exceptions and identify benefits that were revealed during the monitored time period.

The information you present should differ depending on whether your audience consists of

- **Customers** (inform whether targeted service levels were provided and, in the case of weaknesses, what improvements are being implemented to improve the situation)
- **Senior management** (CSFs, KPIs, customer satisfaction levels, actual performance Vs planned performance, costing, revenue targets. This will help senior management in making strategic decisions on investment, implementing improvements, enhance customer satisfaction levels, etc)
- **internal IT personnel** (provide info about KPIs activity metrics so they can plan, coordinate, schedule, and identify incremental improvement opportunities)
- **Suppliers** (KPIs and activity metrics related to suppliers' services and performance. Suppliers may also be targeted with improvement initiatives)

Step7: Implement Improvement:
The final step in the CSI process is implementing the improvements that have been identified.

However, the CSI process may identify many opportunities for improvement, and it may not be feasible to implement all of them. As a result, organizations need to prioritize improvement opportunities.

Once a decision is made to improve a particular IT service or Service Management process, the Service Lifecycle continues.

The seven steps in the CSI process can be described as a "knowledge spiral" rather than a simple cycle.

Each lime the process is completed, organizational knowledge is gained. This can then be used to inform future service improvements.

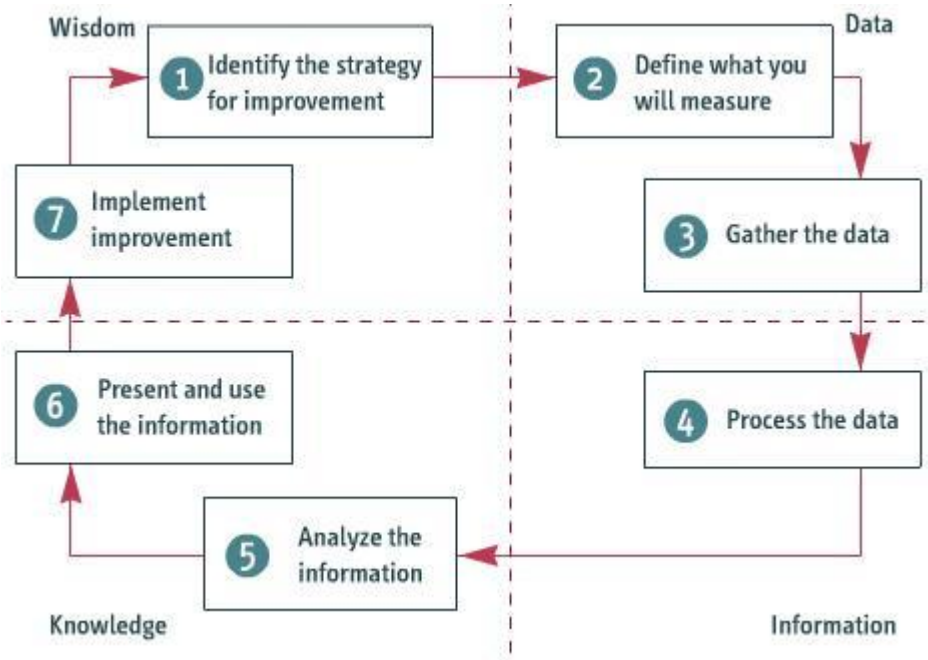
Each step in the seven-step improvement process correlates to the sequence of elements in the Data-Information-Knowledge-Wisdom (DlKW) model.

Data:
Data represents the raw facts that are dealt with in steps two and three of the CSI process, which involve determining what to measure and gathering data.

Information:
Information is used in step four of the CSI process, which involves processing the data that has been collected. When data is processed, it's given contextual meaning and is thereby converted into information.

Knowledge:
Knowledge is generated and used in steps five and six of the CSI process, which involve analyzing, and presenting and using the information that has been processed. Knowledge is information that's placed in a context and that equips the holder to act upon and use that information.

Wisdom:
Wisdom is used in the seventh step of the CSI process and feeds back into the ongoing CSI cycle. Wisdom is the accumulation of data, information, and knowledge that leads to an informed state of understanding in which the knowledge holder can act effectively and add value to an organization.



For CSI to truly succeed, it has to be fully integrated with each stage in the Service Lifecycle, and with the processes in each of these stages.