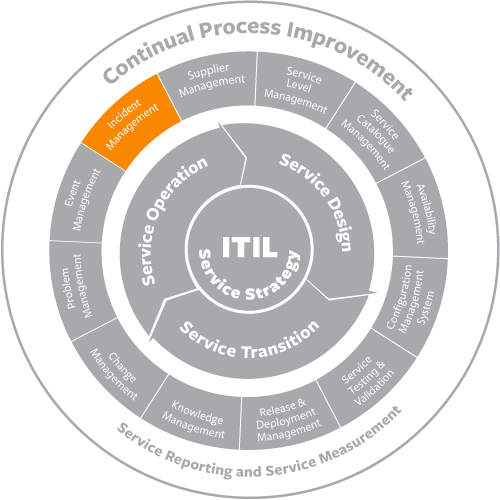
**ITIL Incident Management 101**

Incident management is typically closely aligned with the service desk, which is the single point of contact for all users communicating with IT. When a service is disrupted or fails to deliver the promised performance during normal service hours, it is essential to restore the service to normal operation as quickly as possible. Also any condition that has the potential to result in a breach or degradation of service ought to trigger a response that prevents the actual disruption from occurring. These are the objectives of incident management.



Service desk personnel usually are identified as level 1 support, which includes the following

* Incident identification
* Incident logging
* Incident categorization
* Incident prioritization
* Initial diagnosis
* Escalation, as necessary, to level 2 support
* Incident resolution
* Incident closure
* Communication with the user community throughout the life of the incident

Incident management is not expected to perform root cause analysis to identify why an incident occurred. Rather, the focus is on doing whatever is necessary to restore the service. This often requires the use of a temporary fix, or workaround. An important tool in the diagnosis of incidents is the known error database (KEDB), which is maintained by problem management. The KEDB identifies any problems or known errors that have caused incidents in the past and provides information about any workarounds that have been identified.

Another tool used by incident management is the incident model. New incidents are often similar to incidents that have occurred in the past. An incident model defines the following:

* Steps to be taken to handle the incident, the sequence of the steps, and responsibilities
* Precautions to be taken prior to resolving the incident
* Timescales for resolution
* Escalation procedures
* Evidence preservation

Incident models streamline the process and reduce risk.

Incident management has close relationships with and dependencies on other service management processes, including:

* Change management. The resolution of an incident may require the raising of a change request. Also, since a large percentage of incidents are known to be caused by implementation of changes, the number of incidents caused by change is a key performance indicator for change management.
* Problem management. Incident management, as noted above, benefits from the KEDB, which is maintained by problem management. Problem management, in turn, depends on the accurate collection of incident data in order to carry out its diagnostic responsibilities.
* Service asset and configuration management. The configuration management system (CMS) is a vital tool for incident resolution because it identifies the relationships among service components and also provides the integration of configuration data with incident and problem data.
* Service level management. The breach of a service level is itself an incident and a trigger to the service level management process. Also, service level agreements (SLAs) may define timescales and escalation procedures for different types of incidents.

**What is an Incident?**

ITIL defines an incident as an unplanned interruption to or quality reduction of an IT service. The service level agreements (SLA) define the agreed-upon service level between the provider and the customer.   
  
Incidents differ from both problems and requests. An incident interrupts normal service; a problem is a condition identified through a series of multiple incidents with the same symptoms. Problem management resolves the root cause of the problem; incident management restores IT services to normal working levels. Requests for fulfillment are formal requests to provide something. These may include training, account credentials, new hardware, license allocation, and anything else that the IT service desk offers. A request may need approvals before IT fulfills it.   
  
Incidents interrupt normal service, such as when a user’s computer breaks, when the VPN won’t connect, or when the printer jams. These are unplanned events that require help from the service provider to restore normal function.

**What is ITIL Incident Management?**

When most people think of IT, incident management is the process that typically comes to mind. It focuses solely on handling and escalating incidents as they occur to restore defined service levels. Incident management does not deal with root cause analysis or problem resolution. The main goal is to take user incidents from a reported stage to a closed stage.   
  
Once established, effective incident management provides recurring value for the business. It allows incidents to be resolved in timeframes previously unseen. For most organizations, the process moves support from emailing back and forth to a formal ticketing system with prioritization, categorization, and SLA requirements. The formal structures take time to develop but results in better outcomes for users, support staff, and the business. The data gathered from tracking incidents allows for better problem management and business decisions. Incident management also involves creating incident models, which allow support staff to efficiently resolve recurring issues. Models allow support staff to resolve incidents quickly with defined processes for incident handling. In some organizations, a dedicated staff has incident management as their only role. In most businesses, the task is relegated to the service desk and its owners, managers, and stakeholders. The visibility of incident management makes it the easiest to implement and get buy-in for, since its value is evident to users at all levels of the organization. Everyone has issues they need support or facilities staff to resolve, and handling them quickly aligns with the needs of users at all levels.   
  
Operational incident management requires several key pieces:

1. A service level agreement between the provider and the customer that defines incident priorities, escalation paths, and response/resolution time frames
2. Incident models, or templates, that allow incidents to be resolved efficiently
3. Categorization of incident types for better data gathering and problem management
4. Agreement on incident statuses, categories, and priorities
5. Establishment of a major incident response process
6. Agreement on incident management role assignment

Number five in the list above is important to incident management. The incident manager is tasked with handling incidents that cannot be resolved within agreed-upon SLAs, such as those the service desk can’t resolve. In many organizations, this person may be an IT operations manager or an IT technical lead.

**Incident Management’s Main Function: The Service Desk**

Incident management involves several functions. The most important is the service desk. The service desk is also known as the “help desk”. The service desk is the single point of contact for users to report incidents. Without the service desk, users will contact support staff without the limitations of structure or prioritization. This means that a high-priority incident may be ignored while the staff handles a low-priority incident. Low-priority incidents, such as fixing a bad docking station, might not get resolved for weeks while the IT support staff handles the most pressing issues presented to them at that moment. The structure of the service desk enables support staff to handle everyone’s issues promptly, encourages knowledge transfer between support staff, creates self-service models, collects IT trend data, and supports effective problem management.   
  
A service desk is divided into tiers of support. The first tier is for basic issues, such as password resets and basic computer troubleshooting. Tier-one incidents are most likely to turn into incident models, since the templates to create them are easy and the incidents recur often. For example, a template model for a password reset includes the categorization of the incident (category of “Account” and type “Password Reset”, for example), a template of information that the support staff completes (username and verification requirements, for example), and links to internal or external knowledge base articles that support the incident. Low-priority tier-one incidents do not impact the business in any way and can be worked around by users.   
  
Second-tier support involves issues that need more skill, training, or access to complete. Resetting an RSA token, for example, may require tier-two escalation. Some organizations categorize incidents reported by VIPs as tier two to provide a higher quality of service to those employees. Tier-two incidents may be medium-priority issues, which need a faster response from the service desk.  
  
Correct assignment of tiers and priorities occurs when most incidents fall into tier one/low priority, some fall into tier two, and few require escalation to tier three. Those that require urgent escalation become major Incidents, which require the “all-hands-on-deck” response. Major Incidents are defined by ITIL as incidents that represent significant disruption to the business. These are always high priority and warrant immediate response by the service desk and often escalation staff. In the tiered support structure, these incidents are tier three and are good candidates for problem management.

**The Incident Process**

In ITIL, incidents go through a structured workflow that encourages efficiency and best results for both providers and customers. ITIL recommends the incident management process follow these steps:

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization
5. Incident response
   * Initial diagnosis
   * Incident escalation
   * Investigation and diagnosis
   * Resolution and recovery
   * Incident closure

The incident process provides efficient incident handling, which in turn ensures continual service uptime.   
  
The first step in the life of an incident is incident identification. Incidents come from users in whatever forms the organization allows. Sources of incident reporting include walk-ups, self-service, phone calls, emails, support chats, and automated notices, such as network monitoring software or system scanning utilities. The service desk then decides if the issue is truly an incident or if it’s a request. Requests are categorized and handled differently than incidents, and they fall under request fulfillment.   
  
Once identified as an incident, the service desk logs the incident as a ticket. The ticket should include information, such as the user’s name and contact information, the incident description, and the date and time of the incident report (for SLA adherence). The logging process can also include categorization, prioritization, and the steps the service desk completes..  
  
Incident categorization is a vital step in the incident management process.   
  
Categorization involves assigning a category and at least one subcategory to the incident. This action serves several purposes. First, it allows the service desk to sort and model incidents based on their categories and subcategories. Second, it allows some issues to be automatically prioritized. For example, an incident might be categorized as “network” with a sub-category of “network outage”. This categorization would, in some organizations, be considered a high-priority incident that requires a major incident response. The third purpose is to provide accurate incident tracking. When incidents are categorized, patterns emerge. It’s easy to quantify how often certain incidents come up and point to trends that require training or problem management. For example, it’s much easier to sell the CFO on new hardware when the data supports the decision.   
  
Incident prioritization is important for SLA response adherence. An incident’s priority is determined by its impact on users and on the business and its urgency. Urgency is how quickly a resolution is required; impact is the measure of the extent of potential damage the incident may cause.

1. **Low-priority incidents** are those that do not interrupt users or the business and can be worked around. Services to users and customers can be maintained.
2. **Medium-priority incidents** affect a few staff and interrupt work to some degree. Customers may be slightly affected or inconvenienced.
3. **High-priority incidents** affect a large number of users or customers, interrupt business, and affect service delivery. These incidents almost always have a financial impact.

Once identified, categorized, prioritized, and logged, the service desk can handle and resolve the incident. Incident resolution involves five steps:

1. **Initial diagnosis**: This occurs when the user describes his or her problem and answers troubleshooting questions.
2. **Incident escalation**: This happens when an incident requires advanced support, such as sending an on-site technician or assistance from certified support staff. As mentioned previously, most incidents should be resolved by the first tier support staff and should not make it to the escalation step.
3. **Investigation and diagnosis**: These processes take place during troubleshooting when the initial incident hypothesis is confirmed as being correct. Once the incident is diagnosed, staff can apply a solution, such as changing software settings, applying a software patch, or ordering new hardware.
4. **Resolution and recovery**: This is when the service desk confirms that the user’s service has been restored to the required SLA level.
5. **Incident closure**: At this point, the incident is considered closed and the incident process ends.

**Incident Statuses**

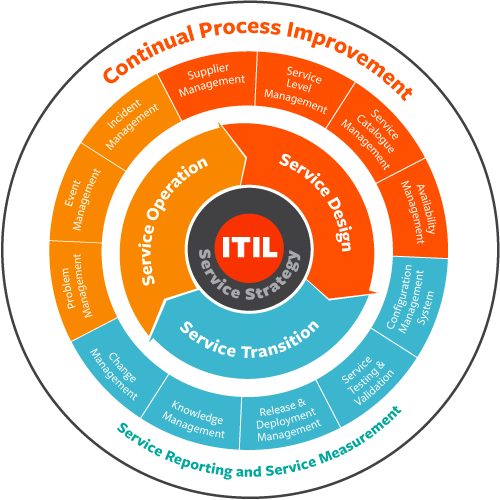
Incident statuses mirror the incident process and include:

* New
* Assigned
* In progress
* On hold or pending
* Resolved
* Closed

The **new** status indicates that the service desk has received the incident but has not assigned it to an agent.  
  
The **assigned** status means that an incident has been assigned to an individual service desk agent.

The **in-progress** status indicates that an incident has been assigned to an agent but has not been resolved. The agent is actively working with the user to diagnose and resolve the incident.  
  
The **on-hold** status indicates that the incident requires some information or response from the user or from a third party. The incident is placed “on hold” so that SLA response deadlines are not exceeded while waiting for a response from the user or vendor.  
  
The **resolved** status means that the service desk has confirmed that the incident is resolved and that the user’s service has restored to the SLA levels.  
  
The **closed** status indicates that the incident is resolved and that no further actions can be taken.   
  
Incident management follows incidents through the service desk to track trends in incident categories and time in each status. The final component of incident management is the evaluation of the data gathered. Incident data guides organizations to make decisions that improve the quality of service delivered and decrease the overall volume of incidents reported. Incident management is just one process in the service operation framework. Read on to learn about ITIL continual service improvement (CSI).

## New to ITIL? Start here!

Most organizations consider their people, capabilities, processes, and technologies to be strategic assets. These assets help deliver and support the company’s vision and mission. Efficient and effective alignment of capabilities and resources of services and products can help create a strategic advantage in the markets that organizations serve. This is where ITIL®, the Information Technology Infrastructure Library, comes into play. ITIL is the most widely accepted approach to IT service management in the world. It helps individuals and organizations use IT to realize business change, transformation and growth.

The ultimate goal of ITIL is to improve how IT delivers and supports valued business services. ITIL is not just technology management or process management. It also focuses on improving the capabilities of people, processes, and technology. ITIL provides value for an organization, its resources and capabilities, including employees and customers.

Adoption of the ITIL framework can be the foundation for success of other initiatives such as DevOps, cybersecurity, cyber-resilience, Internet of Things (IoT), and other emerging trends and technologies.

**How to use this guide**

This online guide presents the following:

* Overview of the principles of ITIL
* Advantages of adopting the ITIL framework
* Descriptions of each ITIL stage
* Links to useful resources for further learning

As you page through this online guide, you’ll have opportunities to read blog posts associated with ITIL, learn about BMC ITIL-compliant solutions, download free ITIL best practice books, visit the ITIL and CMDB community, and sign up for ITIL Certification and Training. Check back often to keep up with the latest ITIL information available from BMC.

**ITIL Processes from ITIL V3 2011**

The guide covers the following processes:

* [ITIL Service Strategy ›](http://www.bmcsoftware.uk/guides/itil-service-strategy.html)
* [ITIL Service Design ›](http://www.bmcsoftware.uk/guides/itil-service-design.html)
* [ITIL Service Transition ›](http://www.bmcsoftware.uk/guides/itil-service-transition.html)
* [ITIL Service Operation ›](http://www.bmcsoftware.uk/guides/itil-service-operation.html)
* [Continual Service Improvement ›](http://www.bmcsoftware.uk/guides/itil-continual-service-improvement.html)

**What is ITIL?**

ITIL is a set of IT Service Management practices that focuses on aligning IT services with the needs of business.

Every organization delivers a service or product. For every service or product, the ITIL framework helps manage delivery, industrialization, support, and consumerization from inception to retirement. The five stages of the ITIL framework include:

* Service Strategy
* Service Design
* Service Transition
* Service Operation
* Continual Service Improvement

Each stage in this service lifecycle supports all the other stages.

ITIL does not tell any particular organization all the capabilities that it needs. But for any IT organization making roadmap decisions it gives practical guidance on strategy and services.

ITIL also complements other industry best practices. For example, if an organization also needs guidance for project management, then that organization can augment the ITIL framework foundation with a project management best practice.

**Who uses ITIL?**

Large, medium, and small organizations all over the world use ITIL to help them improve the value of their services. ITIL helps organizations in all industries and sectors solve business issues as well as improving IT capability. Organizations use ITIL as a guide to improve or implement a capability that provides business value.

Since ITIL is a set of best practices and not a standard, organizations are free to adopt as much of the ITIL framework as they see fit.

**What are the benefits and advantages of ITIL?**

Organizational benefits of adopting ITIL best practices include:

* Stronger alignment between IT and the business
* Improved service delivery and customer satisfaction
* Reduced costs through improved use of resources
* Greater visibility of IT costs and assets
* Better management of business risk and service disruption or failure
* More stable service environment to support constant business change

More detailed benefits and advantages of the ITIL framework are documented in each of the stages and in the 26 ITIL process areas defined in the [core books](http://www.bmc.com/forms/ESM_TL_ITIL_ReferenceBooks_BMCcom_EN_Apr2012_V2.html). Essentially, the benefit lies in aligning process area with desired business outcome. The goal is to improve the specialized capability of the process, people, suppliers and technology which supports the business service.

**Why BMC?**

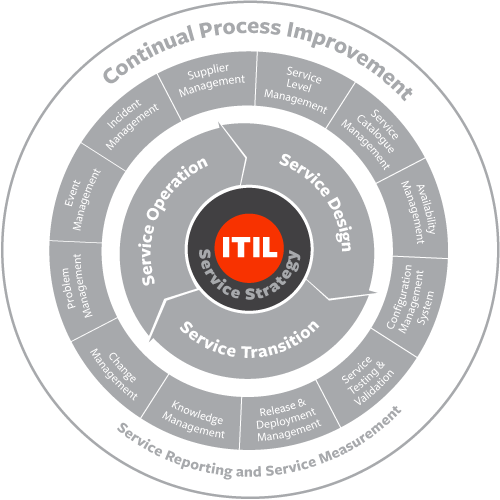
BMC builds ITIL-compliant solutions and supports those solutions with ITIL training, services, and resources. Our Centers of Excellence and industry-leading technologies help organizations all over the world define and execute their IT Service Management (ITSM) strategies for traditional and digital services.

Whether transforming or evolving service maturity, BMC has helped organizations worldwide achieve high-performing service business value. BMC helps organizations achieve value from all of the ITIL process areas.

BMC also provides:

* ITIL PinkVerify Certified Technology
* ITIL industry contributors
* Industry-leading education offerings
* Transformation practice for ITIL prescriptive guidance
* Industry partner collaboration
* ITIL synergies with other best practices
* [ITIL Service Strategy Processes](http://www.bmcsoftware.uk/guides/itil-service-strategy.html)
* [**Service Portfolio Management**](http://www.bmcsoftware.uk/guides/itil-service-strategy.html#portfolio) **|** [**Financial Management**](http://www.bmcsoftware.uk/guides/itil-service-strategy.html#financial) **|** [**Demand Management**](http://www.bmcsoftware.uk/guides/itil-demand-management.html) **|** [**Business Relationship Management**](http://www.bmcsoftware.uk/guides/itil-service-strategy.html#business) **|** [**Strategy Management**](http://www.bmcsoftware.uk/guides/itil-service-strategy.html#strategy)

**What is ITIL Service Strategy?**



ITIL Service Strategy helps organizations understand the merits of using a market-driven approach. To succeed organizations must deliver and support services and products that their customers need. Service Strategy helps them to do this by encouraging a practice of service management for managing IT services.

No organization acts in a vacuum. Customers always have alternatives. Even government and nonprofits where social services compete for tax dollars and contributions.

Competitive forces demand that an IT organization do its job better than the alternatives. What service strategy is about is positioning your organization as non-optional.

Service Strategy process areas include:

* service portfolio management
* financial management for IT services
* demand management
* business relationship management
* strategy management for IT services

## Service Portfolio Management

Service portfolio management (SPM) is a means by which you can dynamically and transparently govern resource investment. The goal of SPM is to maximize value to the business while managing risks and costs. We do this by ensuring that the content of the service portfolio is in line with the organization’s service management strategy.

In cooperation with the change management process it evaluates proposed services. As well as major changes to existing services.

Service Portfolio Management is a cradle to grave process.

It monitors services in the pipeline. First as they proceed through funding, then through design, development, testing, and deployment. Once operational it monitors to ensure we are achieving expected returns. And finally, when the service has reached the end of its useful life, it works with Service Transition processes to ensure an orderly retirement and preservation of essential records and assets.

**Financial Management for IT Service**

Financial management for IT services ensures we track and associate IT investment and spending with the services provided.

Why do we need to do this? We want to deliver the best quality service at the lowest possible cost. We want to create business value and increase the opportunity to take on extra projects that result in even greater value to the business.

The three major activities which take place within financial management for IT services are:

* **A**ccounting
* **B**udgeting
* **C**harging

(the “ABCs” of financial management).

Accounting involves applying cost accounting principles to IT spending. We do this to answer the question, “What does it cost to provide each service?”

We use Budgeting to show the funding required to support the defined services at a given level of business activity. The budget assures that IT Service Management will have adequate funding to deliver promised services.

Charging is the process of assuring that IT Service Management will “capture” value. That is, that the consumers of services are aware of the cost of providing services to them.

**Demand Management**

[ITIL Demand Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-demand-management.html)

**Business Relationship Management**

ITIL business relationship management works closely with service portfolio management and strategy management. It helps IT services to inform and implement the strategy and service selection.

Participants in this process seek to form a relationship with customers to understand their needs for service. This involves:

* ensuring that services provided are delivering the value expected by the customer
* understanding the customer’s environment well enough to identify opportunities for new services or new applications of existing services
* being aware of changes in the customer’s business environment which may impact service needs

The most important key performance indicator (KPI) for business relationship management is customer satisfaction.

**Strategy Management for IT Services**

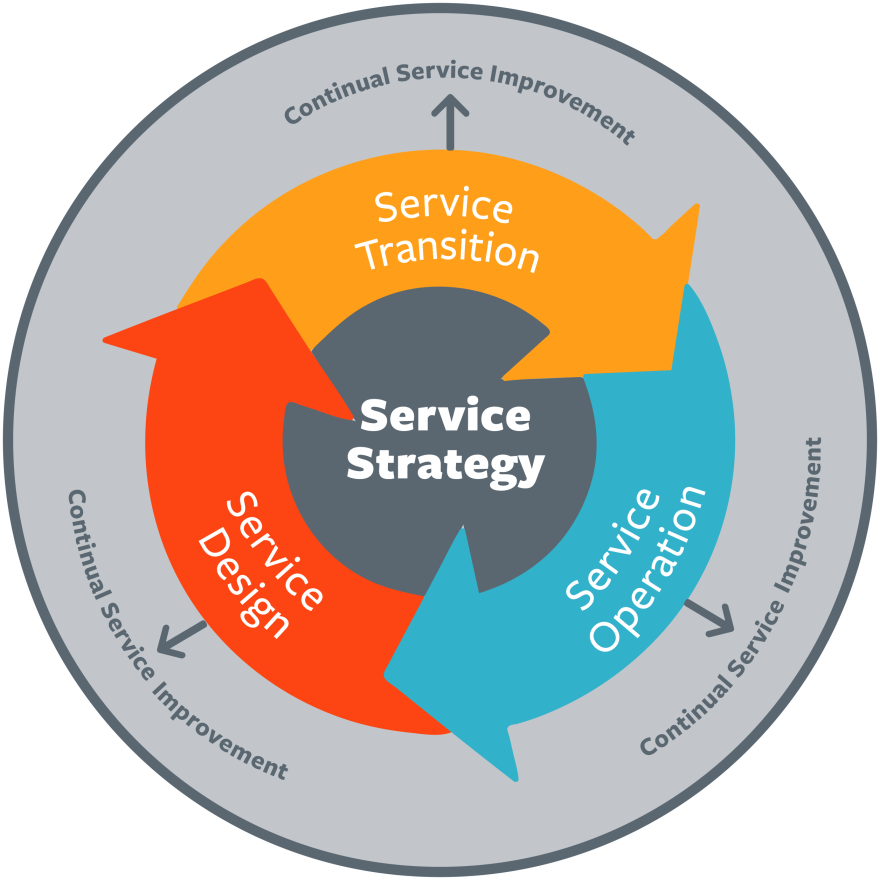
ITIL strategy management for IT services seeks to enable IT Service Management to become a strategic asset to the organization. It’s not enough to align IT with the business; IT should also *integrate* with the business.

Any service provider, to be successful, must have a thorough understanding of the market space in which they operate. They must know what their strengths and weaknesses as a provider are, as well as what opportunities are available. Strategy management for IT services seeks to answer questions such as the following:

* Who are our customers?
* What business outcomes do they need?
* How do the services we provide support those outcomes?
* How can we position ourselves to be the only logical provider of these services?
* What market spaces do we operate in?
* Are there ways to expand our current service offerings into new markets?
* Are there unmet needs in our current market spaces for which we can develop services?

ITIL Demand Management 101

At some point during the service design or service strategy phase, someone may ask what services your organization actually needs and uses. Or perhaps the statement of work is coming up for renewal, requiring a new service level agreement (SLA). Reevaluating your services is also important when an organization has been financially burdened by inadequately planning for an influx of tickets or service usage. To determine "how much" service is enough, decisions should be based on data rather than gut feeling. Fortunately, ITIL has defined the IT service management strategies needed to identify, analyze, and plan for changes in usage patterns.  
  
This process is called demand management.



**What is ITIL Demand Management?**

ITIL Demand Management helps a business understand and predict customer demand for services. Every business is subject to cyclical behavior. This means that demand for services can grow or shrink with the business cycle. In deciding whether to provide a service, IT Service Management must understand the patterns of business activity (PBAs) related to the service. While it is important to avoid having inadequate capacity, excess capacity is also a business risk, involving expense which typically cannot be recovered, since customers cannot be expected to pay for capacity they are not using.

PBAs are typically thought of in terms of transaction volumes. ITIL suggests other factors be considered as well, such as the source of the demand, special needs such as enhanced security, and tolerance for delay. The job of demand management is to identify appropriate PBAs and to associate them with user profiles (UPs). This becomes important input to the capacity management process in the Service Design lifecycle phase.

According to ITIL, the purpose of demand management is to understand, anticipate, and influence customer demand for services. As a process, it is part of the [ITIL service strategy](http://www.bmc.com/guides/itil-service-strategy.html) stage of the ITIL lifecycle. Service strategy determines which services to offer to prospective customers or markets. The decisions that are made in the service strategy stage affect the service catalog, the business processes, the service desk, the required capacity, and the financial requirements of the service provider.  
  
As part of the service strategy stage, demand management rationalizes and optimizes the use of IT resources. It ensures that the amount of technical and human resources that has been budgeted matches the expected demand for the service. If the prediction is too low, the agreed-upon service levels may not be delivered. If the predictions are too high, resources will have been allocated to a service that will not be used (or paid for). Demand management bridges the gap between service design, capacity management, and business relationship management to ensure that the predictions are accurate.  
  
Demand management is a process within ITIL that is more supportive of other processes than a self-contained process. Unlike incident management, for example, the activities inside demand management are not visible to the customer. When service demand is not properly balanced, it affects nearly every part of the ITIL lifecycle.

**Demand Management Roles**

Like every process within the ITIL framework, demand management has a chain of responsibility and ownership. Here, the owners are called **business relationship managers**. Business relationship management creates and grows the connection between the customer and the service provider.

**Demand Management Objectives and Activities**

The purpose of demand management is to **detect and influence the demand that customers have on IT services**. This process involves three main actions:

1. **Analyzing current customer usage of IT services**: The easiest way to do this is to analyze service desk data regarding incidents, requests, and problems. Network usage and uptime can be measured via a service dashboard, such as the kind used in a network operations center (NOC) environment.
2. **Anticipating future customer demands for IT services**: Here, the business relationship manager comes into play. He or she may speak with the customer directly about forecasted needs, will analyze trends in usage or tickets, and will make educated projections about future usage based on similar customers trends.
3. **Influencing consumption as necessary by financial or technical means**: For example, if a customer uses more service than anticipated in the SLA, a service provider may charge fees for the excessive consumption to offset the costs of the unforeseen demand. Demand management also makes sure that the appropriate costs are included in the service design. Formally, this involves two processes:

**Demand Prognosis**

In demand prognosis, the business relationship manager analyzes IT service consumption. This individual will also forecast future consumption based on known information, such as consumption trends and service-quality feedback from the customer. Sometimes, the customer will directly indicate when more capacity or a great number of services are needed. In ITIL, this is called the **Pattern of Business Activity** (PBA). According to ITIL, the PBA is a workload profile of one or more business activities that helps service providers establish usage patterns.

The pattern of business activity measures the following aspects of customer service usage:

* **Frequency**
* **Volume**
* **Duration**
* **Location**

The **duration of usage** is how long the pattern of business usage lasts. Does peak database usage occur only during business hours, for example, or only during certain months? How long ago did the increase or decrease in usage begin?  
  
The **volume of usage** is the amount of activity. For example, this could be the number of transactions processed or a service desk ticket number. Volume can increase or decrease.  
  
The **frequency of usage** is how often the volume of usage occurs.   
  
The **location of usage** is where the business usage occurred. Is it in the service desk or the sales department, for example?  
  
The PBA also includes a **user profile**, which is a pattern of service usage that is tied to a type of user. For example, developers may have a higher database usage pattern than business users.

**Demand Control**

Demand control is the way that providers control IT service consumption. This can be done through technical means (such as network throttling) or financial means (such as increased charges for usage higher than the agreed-upon levels). The control is implemented until the capacity for greater demand is implemented into the service catalog.

Developing differentiated offerings and service packages also controls demand. Differentiated offerings and service packages control demand and cost while providing the customer with the services they use and value most.

**The ITIL Demand Management Communication Flow**

Unlike other processes within the ITIL lifecycle, demand management relies on communication between different processes rather than on a self-contained set of procedures. Unlike some other processes, demand management interfaces with the other service strategy lifecycle processes. On one side, demand management receives customer feedback from the business relationship manager and the PBA. On the other side, demand management informs many other processes based on the information obtained and the conclusions drawn.

Demand management is seen in **service strategy** when the pattern of business activity is used alongside service portfolio management to invest in new services and increased capacity.  
  
It is seen in **service transition** when the data collected is used to validate that the new service catalog meets the projected needs of the pattern of business activity.  
  
It is used in **service operation** as the end point for feedback from the service desk. The service desk detects trends in service usage and sends that information to demand management, which alerts capacity management to increase or decrease resources as needed.  
  
Finally, demand management is seen in **continual service improvement** (CSI) when the data from demand management and the PBA is used to proactively improve services based on usage forecasts.

**Why is ITIL Demand Management So Important?**

Demand management is essential for one simple reason: It is impossible to adequately plan for and meet service demands based on gut check alone. Predicting how much service will increase based on what you think you remember about current demand versus the demand of other similar customers results in inaccurate data at best and expensive overstaffing at worst. Accurate planning requires analyzing the data gathered and client feedback, as seen in the **demand prognosis** process. Inaccurate estimates have negative impacts on:

* SLA metrics
* KPIs
* Customer satisfaction
* Financial management
* Incident management
* Business relationship management
* Service strategy

Poorly managed service demand is a huge risk for organizations. Inadequately planning for increases in service usage could mean missed service levels and poor service quality across the entire service catalog. For businesses, that could mean anything from financial implications to lost business altogether.

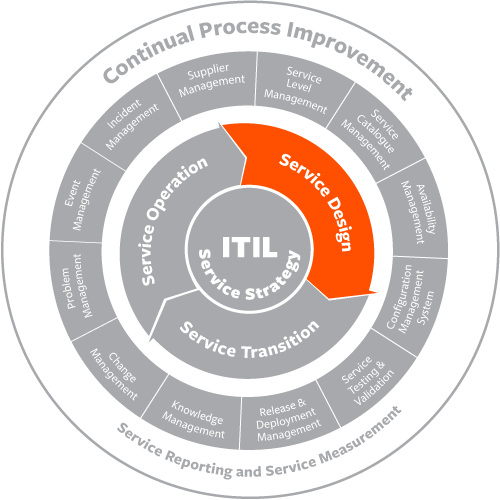
**Related ITIL Stages and Processes**

Demand management interfaces with many ITIL processes. As a part of [service strategy](http://www.bmc.com/guides/itil-service-strategy.html) stage, it is closely aligned with [service portfolio management](http://www.bmc.com/guides/itil-service-strategy.html#portfolio), [financial management for IT services](http://www.bmc.com/guides/itil-service-strategy.html#financial), and [business relationship management](http://www.bmc.com/guides/itil-service-strategy.html#business). This is because the question of "how much" service is enough is integral to those processes. In financial management, for example, the question of how much of a service to provide directly impacts the IT budget and the costs passed on to the service customer. In service portfolio management, demand directly impacts which services are offered in the customer service catalog. service operations is thus also impacted, since it relies on the service catalog for its range of services, as well as on the associated capacity and asset management of operations.   
  
Demand management is a small but important component within ITIL. Getting demand management wrong impacts the entire organization and the services rendered. Read on to learn about the other processes within service strategy.

**What is Service Design?**

Service Design covers the fundamentals of designing services and processes. It provides a holistic design approach to help an organization deliver better services.

Designing a service to meet an organization’s strategic and customer needs requires coordination and collaboration.  Aim for high service maturity when designing services rather than the completion of an IT project. The higher the service maturity the higher customer and user satisfaction will be.



The five key aspects of Service Design are:

1. Designing the service solution
2. Management information systems and tools
3. Technology
4. Processes
5. Measurements and metrics

Approach all aspects with service oriented thinking and decision making.

**Video: ITIL Service Design Capabilities**

This video addresses capabilities needed for effectively consuming, designing and building services and systems. Relationship to service strategy, customer service focus, demand management, cloud computing and business intelligence to enable organization collaborative design capabilities are discussed. (11:46)

**Service Level Management**

The service level management (SLM) process focuses on researching and understanding requirements. Areas include:

* defining, negotiating, agreeing upon and documenting IT service targets
* monitoring, measuring and reporting on how well the service provider delivered the agreed upon targets

When targets are appropriate and met, then the business and IT have a better chance of becoming aligned.

Agreed upon targets are often spelled out in service level agreements (SLAs). Monitoring, measuring and reporting on SLA's in this way provides close links to Continual Service Improvement (CSI).

SLAs are agreements to provide specific services at a defined level of quality (warranty) for a specific price. SLAs typically need negotiation of agreements with other internal organizations (OLA's) or external suppliers (Underpinning Contracts).

Negotiating SLAs to ensure service commitments are met, service level management works with the following warranty processes:

* capacity management
* availability management
* security management
* service continuity management

Service level management is accountable for monitoring conformance to the SLAs and take action if there is a breach of the SLA. This means working with the service desk, incident management, and problem management.

Customer satisfaction is not determined only by SLA performance. Therefore service level management should meet with customers face-to-face on a regular basis. This helps to maintain a positive relationship address any concerns the customer may have.

* [**Atrium Service Level Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-service-design.html)

**Atrium Service Level Management**

[](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

Atrium Service Level Management gives you the tools you need to define, track, and report service levels. Real-time insight helps you identify risks, prioritize resources, and deliver the quality of service the business demands.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/atrium-service-level-management.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

**Service Catalog Management**

Service catalog management ensures that an accurate and up-to-date service catalog is available to all parties authorized to see it. All parts of IT Service Management, as well as customers and users, use the service catalog. Accuracy and availability are essential.

Service catalog management must work closely with service portfolio management as new services move from the pipeline into the catalog and older services are retired. It also helps define how services can be requested and what options are available (gold/silver levels, for instance). The service catalog should document all defined services.

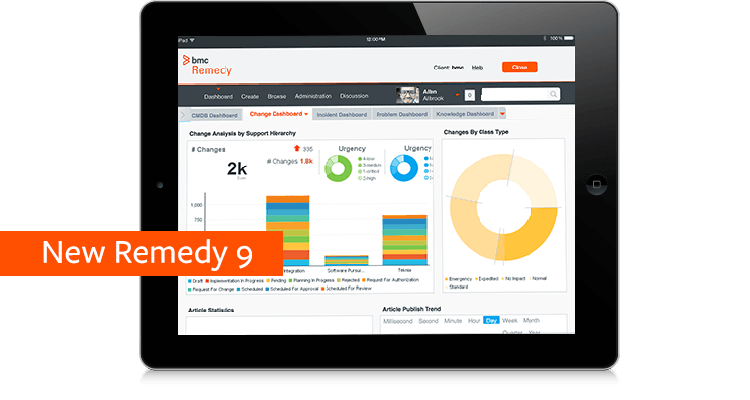
The service catalog generally comprises two views:

* a business service view that is visible to the customer
* a technical service view that is visible only to IT personnel.

This enables the customer to choose services based on their business requirements. At the same IT personnel can use their view to determine what technical services they need to support a given business service.

* [**Remedy IT Service Catalog: Free Trial**](http://www.bmcsoftware.uk/guides/itil-service-design.html)

**Remedy IT Service Catalog**

[](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

BMC provides ITIL®-compliant service catalog management solutions that help you improve user satisfaction, streamline service management, and increase opportunities for self-service automation.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/it-service-catalog.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

**Capacity Management**

[ITIL Capacity Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-capacity-management.html)

**Availability Management**

Availability Management ensures that infrastructure, tools, roles etc. are appropriate for the agreed targets. It also works with the design teams to ensure that availability is designed into services.

Part of the process is to identify vital business functions (VBFs) which IT services support. This will help clarify which approach to availability to take:

* prevention (making sure, as far as possible, that unavailability never happens)
* recovery (developing plans to restore service rapidly in the event of an outage).

Availability management views availability from the user’s perspective, from end to end. This means identifying single points of failure and designing resilience into any infrastructure supporting the service. Availability management serves as a focal point for all issues in IT Service Management related to availability.

Availability management handles specifying which metrics to use to measure availability. And, monitors availability to ensure that the SLA targets are met.

**IT Service Continuity Management**

IT service continuity management (ITSCM) focuses on supporting the overall continuity of the business. We define ITSCM as the process responsible for managing risks that could seriously impact IT services.

Risks so serious they could threaten the very survival of the business.

This activity is often referred to as disaster recovery (DR). But, the use of the term ITSCM should show that there is a corresponding business continuity management (BCM) process. ITSCM supports the BCM process.

ITSCM must work closely with BCM to perform risk analysis and business impact analysis (BIA). This analysis determines how different types of disruptions impact the business. The business areas determined to suffer the greatest impact need the most focus from the service continuity teams.

ITSCM is responsible for development and deployment of the service continuity plan. This includes regular testing and training of all personnel associated with the plan. ITSCM also works with change management to ensure that continuity plans are updated as the operational model changes.

**Information Security Management**

The information security management (ISM) process focuses on aligning IT security with business security. Information security is an activity that happens as part of corporate governance.

We use information security to protect data stores, databases, and metadata. It protects the interests of people who rely on this information, and it protects the systems that deliver the data.

Information security management works closely with service level management to ensure that the business’s needs for security are documented in service level agreements.

Information security measures include the following:

* Preventive: Preventing security breaches. This is primarily accomplished via access controls.
* Reductive: Minimizing the impact of potential security incidents using measures such as taking regular back-ups.
* Detective: Ensuring instantaneous awareness of security breaches which do occur.
* Repressive: Preventing further damage as the result of a breach such as by quarantining servers that are compromised.
* Corrective: Repairing any damage done, such as by restoring from a backup

**Supplier Management**

Supplier management works with third parties, such as suppliers, to negotiate contracts for products or services.  Supplier management monitor conformance to the contract conditions and address any breaches. At renewal, supplier management will determine whether to renew, renegotiate, or end the contract.

The objectives of supplier management is to ensure alignment of contracts with the needs of the business. It is also responsible for ensuring suppliers are meeting their commitments. The supplier and contract management information system (SCMIS) holds supplier and contract details.

**Design Coordination**

The central principles in design coordination are balance, prioritization and integration with project management. Balance and prioritization address the utility and warranty of a service, as well as the needs of the service throughout its lifecycle.

Design coordination oversees all activity in the Service Design phase of the service lifecycle. Its aim is to ensure that a holistic, integrated approach is taken to the design of services. This is necessary because of the variety of disciplines involved in Service Design and the need to take a consistent approach.

Design coordination is accountable for the production of the service design package (SDP). The SDP is a comprehensive description of how a new or changed service is to be designed, built, tested, deployed, and operated. The SDP is the handoff from the Service Design phase to the Service Transition phase.

Design coordination handles managing resources needed by the Service Design phase of the lifecycle. This includes:

* planning to ensure that adequate resources are available
* scheduling access to resources among the many projects that may be in this phase at any one time

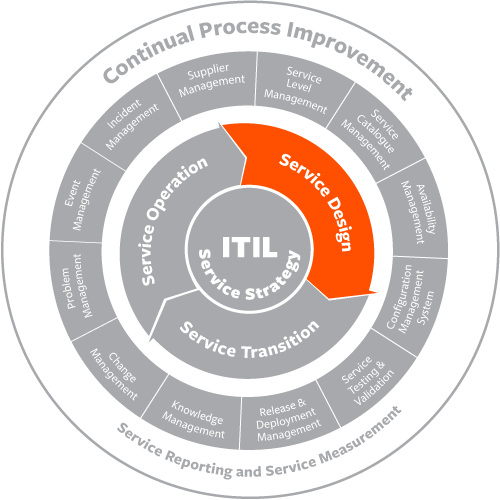
It is accountable for the performance and improvement of the Service Design phase of the lifecycle.

**Video: ITIL Service Design Management**

This video focuses on managing the development of a service product. Design coordination, cloud computing, other best practices are discussed as a component of an overall service management framework. (08:50)

## What is Capacity Management?

ITIL capacity management is responsible for ensuring that adequate capacity is available at all times to meet the agreed needs of the business in a cost-effective manner. The capacity management process works closely with service level management to ensure that the business’ requirements for capacity and performance can be met. Capacity management also serves as a focal point for any capacity issues in IT Service Management. Capacity management supports the service desk and incident and problem management in the resolution of incidents and problems related to capacity.



Successful capacity management requires a thorough understanding of how business demand influences demand for services, and how service demand influences demand on components. This is reflected by the three subprocesses of capacity management: business capacity management, service capacity management, and component capacity management. It is required that capacity management develop a capacity plan, which addresses both current capacity and performance issues, as well as future requirements. The capacity plan should be used throughout IT Service Management for planning and budgeting purposes.

Capacity management is responsible for defining the metrics to be captured during service operation to measure performance and use of capacity. This includes monitoring tools, which can provide input to the event management process. Capacity management may be called upon to perform tactical demand management, which involves using techniques such as differential charging to change users’ behavior so that demand does not exceed supply. Other activities of Capacity management include sizing (working with developers to understand capacity requirements of new services) and modeling (building statistical representations of systems).

**Capacity Management Definitions**

Before implementing capacity management, it’s important everyone is on the same page. One way for an organization to accomplish this is to learn and own the definition. Capacity management introduces new ideas and terms that should be discussed before they are implemented, including **component**, **capacity plan**, **capacity report**, **capacity management information system**, and **performance**.  
  
A **component** is the underlying structure behind a service. For example, it is the database behind the application or the server underneath the website. It is a component that must be purchased, built, maintained, and monitored. Improving performance often involves a replacement, upgrade, or load balancing of the individual component.  
  
The **capacity plan** contains different scenarios for predicted business demand and offers costed options for delivering the service-level targets as specified. This plan allows service designers to make the best choices about how to provide quality service at an affordable price point.   
  
The **capacity report** is a document that provides other IT management with data regarding service and resource usage and performance. This is used to help other managers make service-level decisions or decisions regarding individual components.  
  
The **capacity management information system (CMIS)** is the virtual repository used to store capacity data. Dashboards are one way to store and report on capacity data.  
  
**Performance** is how quickly a system responds to requests. For example, how quickly an application processes data and returns a new screen is one indicator of its performance.

**The Purpose of Capacity Management**

The purpose of capacity management is to determine *how much* capacity should be provided based on the information from demand management regarding *what* should be provided. In particular, capacity management is concerned with speed and efficiency. If IT capacity forecasts are accurate and the amount of IT capacity in place meets business needs, the capacity management process is a success.

**Capacity Management Activities**

This process involves constant measurement, modeling, management, and reporting. More specifically, these activities include:

* Designing a service so that it meets service-level agreement (SLA) objectives once implemented
* Managing resource performance so that services meet SLA objectives
* Assisting with the diagnosis of performance-related incidents and problems
* Creating and maintaining a capacity plan that aligns with the organization’s budget cycle, paying particular attention to costs against resources and supply versus demand
* Continually reviewing current service capacity and service performance
* Gathering and assessing data regarding service usage, and documenting new requirements as necessary
* Guiding the implementation of changes related to capacity

In practice, implementing this from scratch would involve the same steps as for other projects. For example, implementation might follow these broad steps:

**1. Gather the data**

Work with business to determine the service-level need. Determine what this means relative to service availability and service capacity. Identify the individual components necessary. Work with demand management resources to predict demand based on user roles. Work with the financial management team to determine the costs.

**2. Design a service and reach agreement**

Once you've identified the services and the level of performance needed, the cost, and the expected demand, you'll be able to work with ITIL service level management to build an SLA that everyone can agree to. You will also have designed a service at this point.

**3. Build the service**

The next step is to build the service. This involves purchasing the components and building the IT infrastructure, processes, and documentation necessary to support the new service/s. Capacity management should continue to monitor the business needs and any new data to ensure that the service being built will have the necessary capacity for quality performance. Financial management will be involved at this stage to facilitate purchasing of components and other resources.

**4. Operation**

Once you have built the service, and everyone agrees it will meet demand, capacity, and availability requirements, it's go-live time. This is when service operation takes over. Capacity management then supports service operation to deliver services that meet targets.

Monitoring and managing services and their individual components are most easily done via monitoring dashboards that provide data on multiple components in one location. Gathering the data manually from each service or component adds to the total time it takes to produce service-capacity reports.

**Capacity Management Processes**

This process is built on several sub-processes, including **business capacity management**, **service capacity management**, **component capacity management**, and **capacity management reporting**. These processes share common activities, such as modeling, workload management, analysis, and optimization.

**Business capacity management** is the sub-process that turns the needs of the business into IT service requirements. It is involved in service strategy and service design, reviewing the data to ensure that there will be not be any changes in demand before the IT service is implemented. This sub-process works with demand management to ensure that the service is meeting business needs. Other sub-processes make sure that the service meets service-level targets; this sub-process ensures that the service-level targets meet the business needs. A thorough understanding of the business and the service-level agreements is necessary to effectively perform the activities in this sub-process.  
  
**Service capacity management** is the sub-process that focuses on the operation of the service. Unlike component capacity management, this process focuses solely on the service itself. It ensures that the end-to-end service provided meets agreed-upon service-level targets. For example, this process would monitor, control, and predict a ticketing system to ensure it was up and running efficiently.   
  
**Component capacity management** focuses on the technology that provides the performance and capacity to the IT service. Components are things like hard disks, phones, and databases. This sub-process requires knowledge of how each component individually contributes to service performance. It manages, controls, and predicts performance usage and capacity of individual components rather than the service as a whole (as seen in service capacity management). The goal of this sub-process is to reduce the total amount of service downtime by monitoring current performance and predicting future performance. Component capacities are designed around service capacities and not the other way around.   
  
**Capacity management reporting** is the final sub-process. It gathers and then provides other stages with the data related to service capacity, service usage, and service performance. The output of this sub-process is the *service capacity report*.

**Capacity Management and Other ITIL Processes**

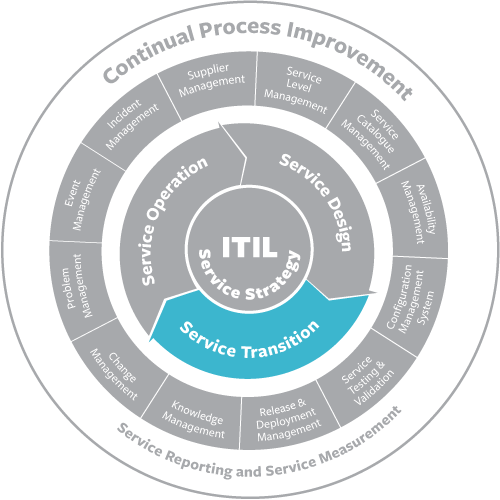
Capacity management must interface with other processes within ITIL, including demand management, availability management, service-level management, and financial management. When the business has a service need, it comes from demand management. It's then relayed to the business continuity management team, which then translates it into an SLA and capacity terms. Service-level management helps with this. Once the service is deployed, service capacity management and component capacity management come in to keep everything at peak performance. Availability management works hand-in-hand with capacity management to keep services running and prevent downtime. Financial management comes into play when individual components must be estimated, purchased, maintained, and replaced. Not working closely with financial management can result in either untimely drops in uptime or organizational budget losses.

**Takeaways**

ITIL capacity management is an important one. With it, your organization can save costs by having the data necessary to make decisions regarding service performance. Rather than being based on gut decisions and guesses, you can use gathered component data to make business cases that win over financial management. What's more, this process can identify where performance tuning is a better choice than upgrading, thereby saving the organization money. Other barriers, such as performance bottlenecks and early indicators of performance issues, are identified before they become problems. This maintains uptime and increases customer and end-user satisfaction.

## What is Service Transition?

ITIL service transition helps plan and manage the change of state of a service in its lifecycle. Managing risk for new, changed and retired services protects the product environment. This helps the business deliver value to itself and its customers.



Curating service knowledge helps all stakeholders make informed, reliable decisions and support challenges with service delivery. Both managing service risk and curating service knowledge are integral to service transition.

During service transition, the following organizational elements need support:

* Service Strategy
* People
* Process
* Technology
* Suppliers of the service
* Organizational culture
* Governance
* Risk

No change is without risk. In fact, change can create extra risk. When transitioning services, focus on communication planning for awareness and compliance. One of the biggest challenges in service transition is changing people’s behavior to accommodate a new or different service. People have a psychological need to feel safe and comfortable with changes to them and around them.

**Change Management**

[ITIL Change Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-change-management.html)

**Video: ITIL Service Transition Capabilities**

This video addresses capabilities needed to enhance the customer’s service experience, organizational specializations and service validations needed for service excellence. BSM, Knowledge management systems, project management, application development relationships with service management and capabilities for service performance are discussed. (11:06)

**Change Evaluation**

ITIL change evaluation analyzes Changes before they move to the next phase in their lifecycle. The lifecycle of a change includes several points at which a go/no-go decision needs to be made:

* Authorization to build and test
* Authorization to check software into the definitive media library (DML)
* Authorization to deploy

We should evaluate all changes. But, for significant changes a formal evaluation process should be invoked. Each organization must define for itself what “significant change” is.

The evaluation should include:

* Evaluating the intended effects of the change
* As far as possible, anticipating any unintended effects of the change
* Identifying risks
* Presenting a recommendation to change management on whether to proceed to the next stage

The change management process can make the go/no-go decision on proceeding to the next stage.

**Release and Deployment Management**

Release and deployment management handles designing and building packages of approved changes. It also deals with deployment into the live environment and the planning thereof. The aim is to implement approved changes with minimal disruption to the live environment.

Release and deployment management creates and enforces a release policy. Below are some of the items contained in a typical policy:

* Release naming and numbering conventions
* Roles and responsibilities at each stage of the process
* Expected frequency for each release type
* Exit and entry criteria for acceptance into each service transition phase

An important resource for release and deployment management is the definitive media library (DML). This is a physical repository containing the master (or gold) copy of the installation media for all approved software. The purpose of the DML is to serve as the source for all software media to be deployed to the live environment. The DML typically also contains license information and the master copy of software documentation.

The steps involved in the release and deployment process are as follows:

*Release and deployment planning*

The starting point for this activity is the service design package (SDP) provided by the design coordination process. The SDP provides guidelines for packaging and deployment. We add to these the scope and content of the release, who the stakeholders are, roles and responsibilities for the release, and a deployment schedule.

*Release build and test*

This starts with the authorization by change management to build and test the release. It concludes with the authorization by change management to check the software into the DML. Release packages are built in this step and tested according to the criteria identified in the previous step. Actual testing is carried out by the service validation and test process.

*Deployment*

This step starts with the authorization by change management to deploy the release. Activities vary depending on the scale of the release, but may include the following:

* Notification of stakeholders to ensure they are aware of, and agree to, the deployment plans
* Knowledge transfer. This includes training of the service desk and user community as well as input to problem management on any known errors included in the release
* Capturing a baseline (snapshot) of the current state of configuration items affected by the release
* Deployment to the live environment
* Invocation of the back-out plan, if necessary
* Documentation of any deviation from the planned cost, effort, or results
* Updates to the configuration management system (CMS)
* Early life support monitoring of performance in the first days and weeks after deployment. This ensures that we can resolve unexpected incidents and problems rapidly
* Review and close. Capture any learning and feedback. Review results achieved versus planned.

**Service Validation and Testing**

Testing can take place at any point in the service lifecycle but, it generally occurs during Service Transition. The service validation and testing process plans, conducts and reports on tests of new or changed services. The results of testing go to the change evaluation process to support a decision on whether to proceed.

The service design package (SDP) outlines the tests to perform.

Working with change evaluation, service validation and testing will:

* Work with transition planning and support to plan the resources required for testing
* Plan and design tests
* Schedule tests
* Prepare the test environment
* Perform the tests
* Evaluate exit criteria and report
* Clean up and close tests

Service validation and test will perform different types of tests, as called for in the service design package. Types of tests include:

* Utility testing. Does the service deliver the required functionality?
* Warranty testing. Will the service deliver required levels of availability, capacity, security, and continuity?
* Usability testing. Will the service be usable by all potential users, including those with restricted abilities?
* Contract and regulation testing. Will the service conform to applicable regulatory and contract requirements?
* Operational readiness testing. Are the support functions, including the service desk, staffed and trained to support the new or changed service?

**Service Asset and Configuration Management**

What is service asset and configuration management? Successful service delivery requires a large number of assets of different types such as computers, network equipment etc. In addition, various artifacts created during service management, such as policies, service level agreements, and the service catalog, are required for successful administration and delivery of services.

ITIL refers to such assets as configuration items (CI's). Service asset and configuration management creates one or more configuration management databases (CMDBs) to maintain accurate information about CIs, including:

* Current state
* Ownership
* Relationships with other CIs
* Audit trail

To maintain the currency and accuracy of a CMDB, service asset and configuration management relies on change management to ensure that only authorized changes occur and that the results of change are accurately recorded.

Service asset and configuration management maintains the configuration management system (CMS). The CMS comprises the following:

* Data layer. CMDBs and related databases, such as the problem database, change database, request database etc.
* Integration layer. Tools to integrate the items in the data layer so that they can be treated as one logical database.
* Knowledge processing layer. Tools to analyze, model, and report on the contents of the integrated database.
* Presentation layer. Tools to provide customized views of the database for the different user communities. All parts of service management have a need to view the contents of the database, but each has its own specific needs.
* [**Step-by-Step Guide To Building a CMDB**](http://www.bmcsoftware.uk/guides/itil-service-transition.html)

**Download The Free Guide**

[](http://www.bmcsoftware.uk/forms/ITSM-Remedy-CMDB-StepbyStepGuide-PaidSearch.html)

In this Step-by-Step Guide to CMDB, fully updated for ITIL® V3, you’ll learn a common-sense, step-by-step approach to deliver a comprehensive, effective, and useful CMDB for your organization.

[Download The Free Guide ›](http://www.bmcsoftware.uk/forms/ITSM-Remedy-CMDB-StepbyStepGuide-PaidSearch.html)

**Knowledge Management**

[ITIL Knowledge Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-knowledge-management.html)

**Service Transition Planning and Support**

At any time, there will be several projects passing through the service transition phase of the lifecycle. It is the responsibility of transition planning and support to coordinate service transition activities for all these projects.

Specifically, the responsibilities of transition planning and support include:

* Work with capacity management to ensure that adequate resources are available
* Where there is contention for resources, develop a schedule that meets the requirements of the stakeholders
* Ensure that all parties use a standard, reusable process framework.
* Monitor and improve the performance of the Service Transition lifecycle phase.

**Video: ITIL Service Transition Management**

This video focuses on risk and knowledge management benefits within the service lifecycle for service outcomes. Cloud computing, BSM, SKMS, DIKW, management of organizational environment, governance and business impact management to meet business service delivery objectives are discussed. (14:48)

## ITIL Change Management 101

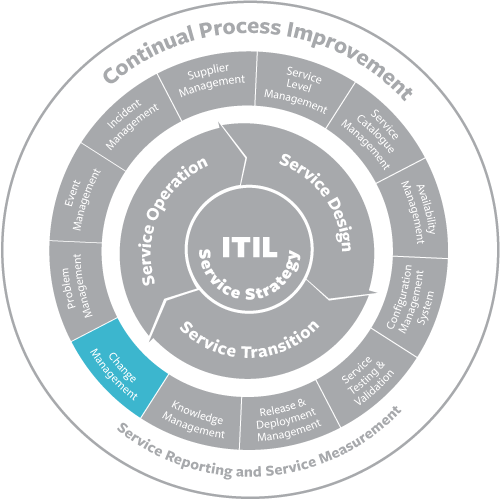
Every IT landscape must change over time. Old technologies need to be replaced, while existing solutions require upgrades to address more demanding regulations. Finally, IT needs to roll out new solutions to meet business demands. As the Digital Age transforms many industries, the rate of change is ever-increasing and difficult for IT to manage if ill prepared.

The Information Technology Infrastructure Library (ITIL) provides a set of best practices for change management that makes it easier for IT professionals to roll out and prioritize changes efficiently, without negatively impacting customers or agreed-upon service levels. To stay competitive and avoid the stress of implementing changes without direction, it’s important to understand these guidelines.

Note that ITIL is not very prescriptive when it comes to how to implement IT processes. Many companies augment ITIL best practices with their own policies and processes, which reflect their own interpretation of the ITIL framework. This is specifically true for the IT change management process. Some of these policies and process may be borrowed from other best practice frameworks or regulations.

## What is ITIL Change Management?

ITIL change management is a process designed to understand and minimize risks while making IT changes. Businesses have two main expectations of the services provided by IT:



* The services should be stable, reliable, and predictable.
* The services should be able to change rapidly to meet evolving business requirements.

These expectations are in conflict. The objective of change management is to enable IT service management to meet both expectations—to enable rapid change while minimizing the possibility of disruption to services.

Although change management is a process in the Service Transition phase of the lifecycle, the decision about whether to approve a proposed change is sometimes a strategic one, and therefore it is expected that the change management process will work closely with the portfolio management process as necessary.

Change management applies a formal process to accomplish change and therefore is sometimes thought of as making change more difficult by adding “red tape.” But a properly implemented change management process can enable a greater volume of useful change than would be possible without it. It does so in the following ways:

* By assuring that all proposed changes are evaluated for their benefits and risks, and that all impacts are considered.
* By prioritizing changes so that limited resources are allocated to those changes that produce the greatest benefit based on the business need.
* By requiring that all changes are thoroughly tested and that each deployment includes a back-out plan to restore the state of the environment in the event that the deployment fails.
* By ensuring that the configuration management system is updated to reflect the effect of any changes.

The change manager must always be aware of opportunities to make the change management process more efficient. There are two important tools for accomplishing this:

* Change models. It is extremely rare that a proposed change is not similar to changes made in the past. The change manager can develop a change model to standardize the procedure for implementing a specific type of change. This streamlines the process and reduces the risk of change.
* Standard changes. A standard change is a special case of a change model and applies to routine changes involving little risk. Standard changes are pre-approved, meaning that they do not have to be reviewed by change management and are typically treated as service requests by the service desk.

In deciding whether to authorize changes, the change manager is assisted by the change advisory board (CAB), which comprises experts in IT technology, finance, and the business.

* [**Remedy Change Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-change-management.html)

**ITIL Change Management Overview**

ITIL defines the best practices that IT organizations use to deliver value to customers via the concept of “services.” Companies and individual IT professionals who use ITIL are able to standardize the way they plan, deliver, and support IT services to their internal or external customers. One of the benefits of using a standardized best-practice framework is in ensuring that employees understand their roles and the procedures that they must follow to deliver services and provide a high level of customer support. Employee knowledge and performance tend to improve with the use of ITIL, and customer satisfaction is higher when customers know what to expect from service.  
  
The ITIL framework is also intended to give IT support providers a more interactive role in businesses. Instead of providing support in the background, IT departments that utilize this framework are part of the businesses’ overall structure.

**IT Change Management Mission**

The mission of the IT change management process is to implement changes in the most efficient manner, while minimizing the negative impact on customers when changes are implemented.

Key performance indicators (KPIs) for tracking the success of the IT change management process are:

* **Successful changes**: The number of changes that have been completed successfully compared to the total number of completed changes. The higher the percentage of successful changes, the better.
* **Backlog of changes**: The number of changes that are not yet completed. While this absolute number depends on the size of the organization, it should not grow over time.
* **Emergency changes**:  The number of completed “emergency” changes. This absolute number is depends on the size of the organization and should not increase over time.

**Change Management Scope**

The scope of the IT change management process is limited to change implementations that will cause:

* A service to become unavailable or degraded during service hours
* The functionality of a service to become different
* The CMDB to require an update

Other IT changes don’t usually require formal change management. Instead, they can be tracked as standard IT activities.

**IT Change Management Procedures**

The IT change management process typically consists of different procedures:

* **Request for change review**: Change coordinators use this procedure when they are dealing with requests for change.
* **Change planning**: Change coordinators and specialists employ this process to prepare the implementation plans for changes.
* **Change approval**: The change manager and approvers (e.g., customer representatives and service owners) follow this procedure to approve planned changes.
* **Change implementation**: Specialists use this process to implement infrastructure changes.
* **Change closure**: Specialists follow this procedure when they perform production tests after changes have been implemented, and change coordinators employ it when they close out changes.

These procedures vary slightly for different types of IT changes and risk levels.

Wherever possible, IT organizations should standardize and automate the way that they process requests.

**Types of IT Changes**

There are different types of change requests, or change classes, that are typically managed in different ways:  
  
• **Standard changes** are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront. These changes are managed according to policies that are the IT organization already has in place. Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don’t require approval from a risk management perspective.  
  
• **Normal changes** are those that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.  
  
• **Emergency changes** arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately.

Latent changes, expedited changes, and no-impact changes are classes that BMC Remedy® ITSM software handles, though they are typically not listed in ITIL documentation.

**Change Management Roles**

Before you begin utilizing ITIL procedures, you will need to assign the following roles to your team:

* The **change initiator** recognizes and identifies the need for change. Your change initiator should be someone who works directly with support services tools. Members of your team who provide support services to customers may be best suited for this position due to their frequent interaction with the system.
* The **change coordinator** assesses requests for change that originate from incident management, problem management, release management, or continuity management. The change coordinator registers changes as needed to handle requests for change or receives change requests from other change initiators; determines the risk and impact for requested changes; prepares implementation plans by creating tasks; and monitors the progress of changes.
* The **change manager** is generally needed in mid-sized and larger organizations. If your IT department is part of a larger company, you will need to pick one or multiple persons to perform the role of change manager. These individuals are responsible for managing change procedures, receiving and prioritizing change requests, evaluating the risk level associated with requests, and keeping thorough records of the outcome of each change.
* The **change advisory board** is responsible for authorizing changes and further evaluating requests when the change manager determines that there is a high risk associated with these requests. The board takes into account the impact that a requested change may have on all affected parties. When these high-risk changes are brought to the attention of the change advisory board, the board will schedule a meeting with a detailed agenda to determine how to proceed.
* The **approver** decides whether to approve or reject changes.
* The **change implementation team** consists of the **specialists** on your team who are responsible for actually making changes. You will likely be part of this team and employees directly under you may also be assigned to implement changes. As an IT manager, you will often be responsible for overseeing changes.

**ITIL Change Management Process**

This section reviews the various procedures that are part of the ITIL change management process. Once you understand the course, you will be able to proceed through the process without having to stop to determine what comes next.

**Creating a Request for Change**  
  
If you are creating a request for change, you are responsible for documenting details that will help others understand what change needs to be implemented and why you are making the request. The initial change request submission often includes details about the risk and implementation steps, if the initiator already knows this information. However, this is not required information at this time.

Details that may be found in a change request include:

* Incidents that necessitate the change
* Description of how the change would be implemented
* The impact that the change would have on all associated systems
* A risk assessment
* Contact information for everyone involved in the change
* An outline of who will need to approve the request
* A backup plan to follow in case the change is not successful

**Reviewing and Assessing a Request for Change**

If you are responsible for reviewing a request for change, you will need to evaluate the request based on its practicality and priority. Your job is to determine whether the request is reasonable and to give feedback related to the request. If requests relate to problems that have already been addressed or are not practical to implement, they will be set aside.   
  
Practical requests will be evaluated according to the originator of the request, the impact that making a change would have on the company, the estimated return on any investment made in relation to the request, and the resources that are needed to fulfill the request. You will also determine who would be responsible for fulfilling the request, and the implementers’ ability to dedicate time to making the change.  
  
**Planning the Change**

Once a change request is made, you will need to plan the change as if it is going to occur. A change plan outlines the course that the change will take, the resources that are needed to complete the change, and a timeline for implementation.   
  
**Testing the Change**

If a change relates to debugging software or otherwise changing a system, you may need to test the change before it is approved. A small-scale test will demonstrate the procedure to be followed in case the change request is approved. Testing the change also gives you the opportunity to work out any problems in the procedures that you have developed.  
  
**Creating a Change Proposal**

A change proposal outlines the type of change, the priority associated with a change request, and the outcomes that could occur if the change is not made. Your proposal will be given to the person empowered to authorize the change, so it is important that you provides a thorough explanation of why a change needs to be made. For example, a change with a high-priority level may result in outages that will affect customers and result in revenue losses. The people who authorize changes must be aware of the severity of the impact if you do nothing.

**Implementing Changes**

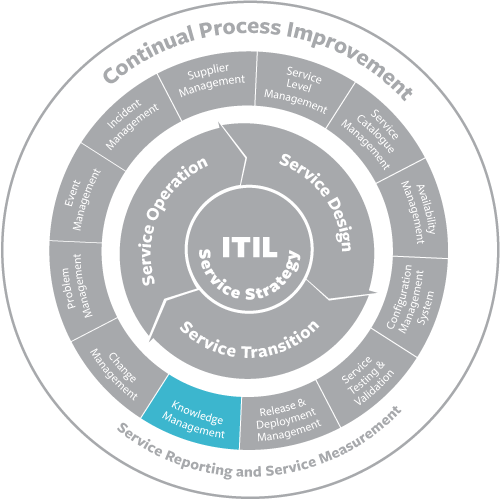
Implementing a change is not a simple process. The change has to be built during the planning process, and implementation is just one step in the change management process. Once the change has been made, tests must be done to determine whether the desired results have been achieved. If the change is not successful, remediation methods may be used to determine what went wrong and to implement a backup plan to alleviate the issues that necessitated the change request.  
  
**Reviewing Change Performance**

The post-implementation review is an essential part of the change management process. As an IT professional, you want to understand whether your change procedures are working as expected. This includes reviewing records to determine whether the change was successful or failed, and recording details about the time and expense of the change to determine the accuracy of estimates that were made before a request was fulfilled. Reviewing change performance gives you the opportunity to fine-tune your change management process for better results in the future.  
  
**Closing the Process**

Once the change process is complete, you must be sure that the entire process has been documented in a database that all stakeholders can access. Once this documentation has been made, the process is closed out.

## What is ITIL Knowledge Management?

Knowledge management is responsible for maintaining the service knowledge management system (SKMS), which represents the total body of knowledge within the service management organization. In order to deliver service successfully, it is necessary that knowledge be captured, organized, and made available to all with a need to know. The SKMS contains all of the other data stores used by service management, including:

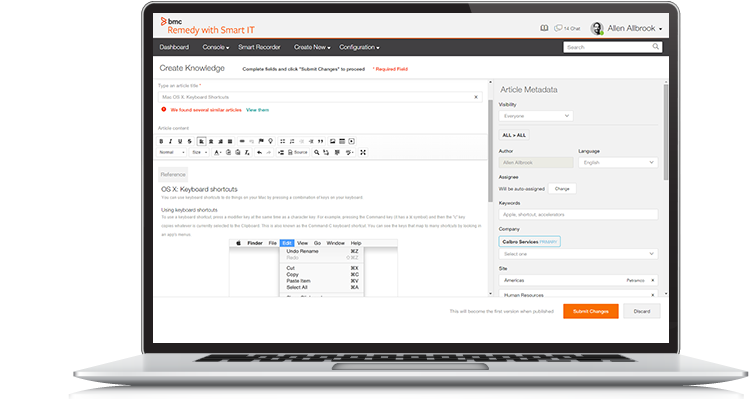


* Service portfolio
* CMS
* Supplier and contract management information system (SCMIS)
* Availability, capacity, and security management information systems (CMIS, AMIS, and ISMIS)
* CSI register

Knowledge can be categorized according to the data-information-knowledge-wisdom (DIKW) structure as follows:

* Data (often called “raw data”) represents discrete facts or numbers. By themselves, data items have little meaning. The responsibility of knowledge management with respect to data is to capture data, identify relevant data, maintain its integrity, and archive or purge data when it is no longer needed.
* Information is generated when data is viewed in context. This typically involves the use of statistics such as averages or peak and minimum values. The responsibility of knowledge management with respect to information is to manage content in a way that allows users to query and analyze it.
* Knowledge combines information with experience. Knowledge can be used as a basis for decision-making or taking an action. The responsibility of knowledge management with respect to knowledge is to support the tools that allow users to spot trends, or determine that a threshold has been exceeded.
* Wisdom can be created by taking advantage of all the knowledge available, such as recognizing that a recent deterioration of service performance coincided with the adoption of a new procedure. The responsibility of knowledge management with respect to wisdom is to make available the tools needed to identify these associations.
* [**Remedy Knowledge Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-knowledge-management.html)

## Remedy Knowledge Management

[](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

Create articles from scratch, share existing knowledge, or import knowledge from external sources and make it available to both your IT and business users. Remedy Knowledge Management is a complete framework to give your workforce the information they need.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/remedy-knowledge-management.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

As you manage your IT team, you want to be sure that every employee has access to accurate and reliable information. Knowledge is key when it comes to successfully completing tasks and ensuring that your team can provide effective services, so how do you manage the flow of information in an IT team? Information Technology Infrastructure Library (ITIL) knowledge management helps keep team members informed, knowledgeable, and ready to assist customers.

## ITIL Knowledge Management Defined

ITIL knowledge management is aimed at helping you and your team make decisions throughout the service process by controlling and managing the flow of information. When you use knowledge management, you are able to ensure that the knowledge that is being distributed to employees is accurate, reliable, and trustworthy. Improving the quality of information prepares employees to make effective decisions, and the end result is a more efficient team.

## The Benefits of Knowledge Management

By implementing knowledge management practices in the workplace, IT managers can improve their teams and provide better service. Consider these benefits:  
  
• Decreases the amount of time that must be spent on training employees. Since your team will constantly receive accurate and up-to-date information, they will require fewer formal training sessions to continue to meet and exceed performance expectations.  
  
• Reduces the number of errors that are made by team members. If your team has the knowledge that they need to make decisions, they are far less likely to make mistakes.   
  
• Reduces the need to complete steps in the service process more than once. When everyone is informed about the process, it is less likely that a step will be performed incorrectly. By implementing knowledge management, you give your team the power to reduce service process time by eliminating the need to repeat steps.  
  
• Allows IT professionals to respond to customer needs faster and more effectively. Your employees will know how to answer customer questions more often, so you will not have to intervene or respond to negative feedback about team members’ lack of knowledge.

## The Stages of Knowledge Management

As with other ITIL concepts, knowledge management must be understood before it can be implemented. There are four stages of knowledge management.

### Data

Raw data consists of the facts that are available in databases that you and your IT team use on a daily basis. When this data is processed, it becomes information that can be distributed to team members.

### Information

Once the raw data has been given context, it becomes information. To create information, the data is sorted according to type. In other words, it answers "who, what, where, when, and why" questions. The translated information can then be relayed via documents, email, and formal reports to establish relevant information.

### Knowledge

When you and your team members analyze information while taking your own experiences into consideration, knowledge is formed. Your insights into the information that is translated from raw data turn basic information into real knowledge. Once the facts have reached this stage, you can start to use knowledge to make decisions.

### Wisdom

When you have knowledge, you will use these facts to put them into context in IT service situations. You and your team are responsible for using personal judgment, experience, and expertise to properly apply knowledge in a way that allows it to reach the wisdom stage of knowledge management.

## Knowledge Management Activities

The process of knowledge management is also broken down into key activities that must be performed to complete the process.

### Knowledge Management Strategy

As an IT manager, you need to create a strategy for identifying the information that should be processed through knowledge management. Many organizations identify feedback from customers, repeated incident reports, and the costs associated with providing and managing support systems as key data that needs to be translated into facts to be distributed across the team. Your strategy should determine the types of information to target for processing through knowledge management. You’ll need to document your strategy to ensure that everyone on the team understands what is expected.

### Knowledge Transfer

Once you have your strategy in place, you will have to decide how knowledge will be transferred among team members and between departments. The first step in knowledge transfer is determining where gaps are located to ensure that you have a plan for getting knowledge to the appropriate people in the organization. By taking the time to identify gaps, you can eliminate them. It is helpful to create a communication plan for disseminating information across channels during this activity.

### Information Management

Information can only become knowledge if it is properly managed and distributed across your team. Access to information is essential to the knowledge management process. Information management is part of the process that involves gathering data, managing information, and determining how this information will be translated to become knowledge. Policies and procedures can be created using information, but you must first establish a process to organize this information into a procedure and record it in a manual your team members can access as needed.

### SKMS

The Service Knowledge Management System (SKMS) is a group of systems, tools, and databases required for successful knowledge management. As an IT manager, you will use the system to store, update, and manage data on a regular basis. Team members can access information through the system at any time of the day, so utilizing such a system is of the utmost importance for teams that include members across time zones.   
  
There are two key portions of the SKMS:  
  
• The Configuration Management System (CMS) manages all configuration information that is entered into the system. Incident reports, established errors, and feedback are all part of this system.  
  
• Configuration Management Databases (CMDBs) contain key pieces of configuration data that have been entered into the database.   
  
The Service Knowledge Management System also contains several layers that allow information to be processed as knowledge and made available to team members and other people in the organization through tools and databases. There are four layers:  
  
• The Presentation Layer allows users to access information. In this layer, users are presented with visual materials that allow them to search, browse, and update information they find in the system. Users may also be given the opportunity to collaborate to improve the knowledge base and ensure that edits are made as needed.   
  
• The Knowledge Processing Layer allows users to report information that can be analyzed. Performance management is also a part of this layer and can be used to determine whether your team members are meeting performance goals. You can monitor scorecards in this layer to help improve the productivity of your team.  
  
• The Information Integration Layer integrates all of the information from relevant portions of the organization in one place. If your organization has partners, information related to these partners may also be found in this layer.   
  
• The Data Integration Layer integrates the data that must be managed for a successful Knowledge Management process by managing applications, documents, and files. The data sources are found in this layer, as well as the tools team members can use to properly apply data as knowledge.

## Who Uses Knowledge Management?

In one form or another, knowledge management is used by everyone in your organization. Your job as an IT manager is to ensure that data is properly processed into information,which is stored in a location that is accessible to the people who require specific knowledge to successfully complete job tasks. Your team will run more efficiently if you use knowledge management properly.  
  
At your team's level, knowledge management creates knowledge and access to this knowledge when necessary. All of your team members will be responsible for identifying the need to translate information into knowledge, while you will need to manage the databases and manuals that are available to your team members.  
  
Outside of your IT team, knowledge needs to be available to users through self-service portals. To improve the efficiency of your team, basic knowledge should be available to users who are willing to troubleshoot their own problems. When users can find solutions on their own, your team has opportunity to focus on escalated issues that require special skills and knowledge that is not available to those who are not familiar with IT applications, processes, and knowledge.

## Keys to Knowledge Management Success

If you are just starting to implement knowledge management in your organization, it may be difficult to get everyone else on board with the idea. While knowledge management is a significant undertaking, it is one that yields tangible benefits. To ensure that your efforts are successful, you need to involve everyone affected by the changes. You will also need to establish methods to manage the problems that may arise.

### Involving Members of the Organization

Unless you own your own business or are working in a small or mid-sized company, you will probably need to find someone at the executive level to advocate for implementing knowledge management. To ensure that you have a strong advocate, take the time to explain the benefits of knowledge management to high-level managers. Not only will a high-level manager be able to gain approval for your plan, but involving such a professional will give you the benefit of in-house support throughout the process.  
  
To get everyone on the same page, you will need to proactively educate them about the reasons for implementing knowledge management. Be sure to explain how implementation will help improve customer service and allow people to find solutions for their issues on their own when the incidents do not have to be reported and processed.   
  
As you implement knowledge management, be sure to monitor progress to report to associated members of the organization. Gaining support for knowledge management is often a matter of showing that the process creates a positive outcome.

### Being Proactive about Managing Problems

Knowledge management is partially about successfully managing problems that your IT team may encounter. These problems may even be related to the knowledge management process itself. To avoid delays in implementation and efforts to update knowledge databases, it is important for you to establish roles and dictate how problems will be resolved before implementation.   
  
The most essential part of avoiding problems with knowledge management is to both assign roles and assure that team members understand their roles. If everyone knows the part that they play in the knowledge management process, your team will be better able to collaborate.

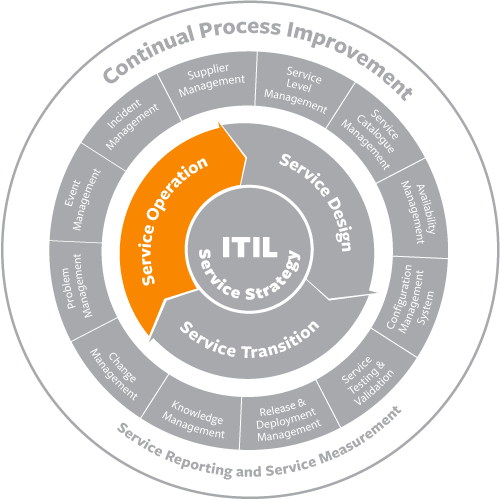
## The Relationship between Knowledge Management and Other Processes

Knowledge management affects all processes that your IT team encounters. When you and your team members collaborate to establish procedures, these procedures are then used to handle everything from incident reporting to managing databases. Managing knowledge for your IT team allows other processes to flow smoothly by ensuring that there are established procedures available for your team members to follow.

## Conclusion

Your IT team can be more efficient and effective when everyone on the team collaborates to create knowledge resources. ITIL knowledge management offers a guideline for recording data, processing information, and creating a knowledge database that can be accessed by your team members as needed. The end result is a more knowledgeable and effective team that can promptly process incident reports to provide superior customer service.

## What is Service Operation?



Service operation encompasses the day-to-day activities, processes, and infrastructure responsible for delivering value to the business through technology.

In Service Strategy, Service Design, Service Transition and Continual Service Improvement, we create value. But, no service is consumed and no business activity is experienced. Because users can access the service during Service Operation, we need high support levels to keep service consumption at high-levels. No customer wants to pay for a service that does not perform as needed or is not available for usage.

Consumerization and service experience is a key factor in Service Operation. The goal of Service Operation is to maintain day-to-day services to the point that there are no issues. When issues do occur Service Operation principles dictate response based on business priority. Service feedback from Service Operation throughout the ITIL service lifecycle enables continual service improvement.

## Incident Management

[ITIL Incident Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-incident-management.html)

## Video: ITIL Service Operation Capabilities

This video addresses new capabilities and resources needed in service operation for social media, cloud computing and business agility. Agility, security, changing business model, governance, service chain complexities and IT asset utilization are discussed related to being service management capable. (11:30)

**Request Fulfillment**

The service desk’s aim is to be the single point of contact for all communications between users and IT service management. As noted above, this includes the reporting of incidents by users. Yet, there are other reasons for users to contact IT service management. These include:

* password resets
* requests for information or usage help
* standard changes as described under change management

We know these types of requests as service requests.

The request fulfillment process handles logging, categorizing, prioritizing, scheduling, and satisfying service requests. Request fulfillment is not required to satisfy requests that are infeasible or lacking proper justification.

Typically, service requests do not affect configuration items (CIs). An exception is a standard change. This is a low-risk, routine change that is pre-approved by change management. Any other request that affects one or more CIs we refer to change management.

It is advisable to document frequent occurring requests in a request model. This will help to ensure consistent handling and documentation. We should document standard services, particularly those for which there is a charge, in the service catalog.

An evolving trend in request fulfillment is the increasing use of self-help tools. These allow users to make requests such as password resets or downloads of approved software.

**Event Management**

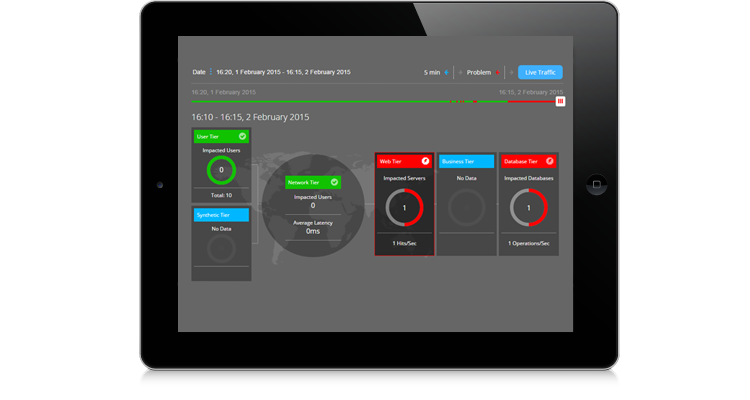
Events are generated by operating systems, database management systems, middleware, applications, and monitoring tools. Most events generate during normal operations and need no response other than logging. Yet a small percentage of events state an actual or potential failure of a CI. This will necessitate the opening of an incident.

Event management handles recognizing events as they occur. It then makes sense of them, and determines the appropriate control action. Since events can generate in large volumes, event management cannot be successful without a software tool. As far as possible, the tool should provide for an automatic response, such as opening an incident record. Incidents with known and straightforward resolutions should automatically invoke procedures to resolve the incident. Where this is not possible, an alert in the form of a page, email or popup window, should generate to notify support personnel of the incident.

Integrated management software suites can provide built-in capabilities for communicating events to the event management tool. Most event-generating software can communicate events via “traps”. These are defined in the simple network management protocol (SNMP). The event management tool can be configured to parse the information in the traps.

* [**TrueSight Event and Impact Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-service-operation.html)

**TrueSight Event and Impact Management**

[](http://www.bmcsoftware.uk/forms/TrueSight-ITDataAnalytics-Trial.html)

Simplify and consolidate event and impact management, improve service performance and availability, reduce operational costs, and minimize business risk. Drive business value by automating ITIL processes and workflows across BMC and third-party solutions.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/truesight-event-impact-manager.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/TrueSight-ITDataAnalytics-Trial.html)

**Access Management**

[ITIL Access Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-access-management.html)

**Problem Management**

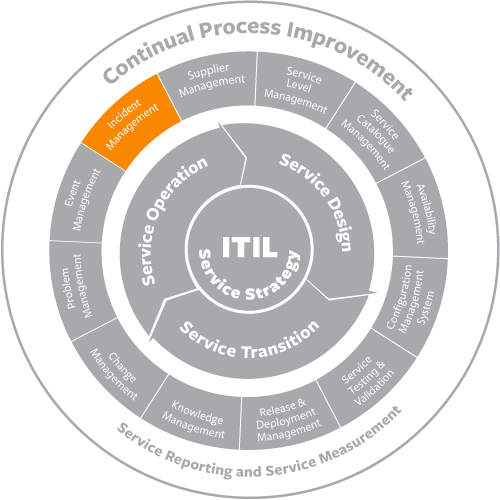
[ITIL Problem Management Processes & Best Practices ›](http://www.bmcsoftware.uk/guides/itil-problem-management.html)

**Video: ITIL Service Operation Management**

This video focuses on managing service operation for value, quality and higher-performance. Cloud computing and the service lifecycle’s dynamic relationship to service operation’s value realization, innovation and business strategy are discussed. (09:42)

**ITIL Incident Management 101**

Incident management is typically closely aligned with the service desk, which is the single point of contact for all users communicating with IT. When a service is disrupted or fails to deliver the promised performance during normal service hours, it is essential to restore the service to normal operation as quickly as possible. Also any condition that has the potential to result in a breach or degradation of service ought to trigger a response that prevents the actual disruption from occurring. These are the objectives of incident management.



Service desk personnel usually are identified as level 1 support, which includes the following activities:

* Incident identification
* Incident logging
* Incident categorization
* Incident prioritization
* Initial diagnosis
* Escalation, as necessary, to level 2 support
* Incident resolution
* Incident closure
* Communication with the user community throughout the life of the incident

Incident management is not expected to perform root cause analysis to identify why an incident occurred. Rather, the focus is on doing whatever is necessary to restore the service. This often requires the use of a temporary fix, or workaround. An important tool in the diagnosis of incidents is the known error database (KEDB), which is maintained by problem management. The KEDB identifies any problems or known errors that have caused incidents in the past and provides information about any workarounds that have been identified.

Another tool used by incident management is the incident model. New incidents are often similar to incidents that have occurred in the past. An incident model defines the following:

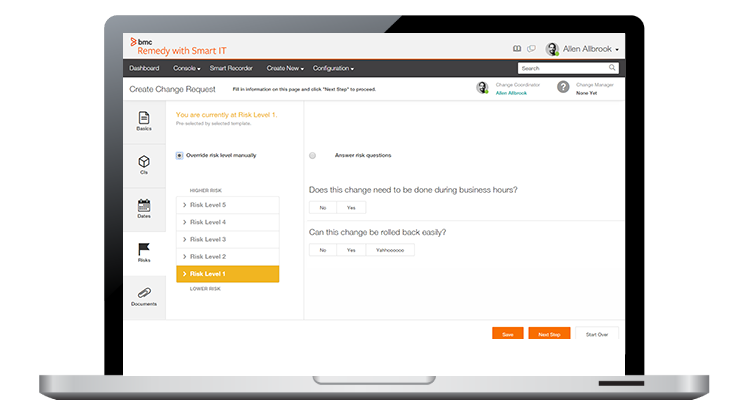
* Steps to be taken to handle the incident, the sequence of the steps, and responsibilities
* Precautions to be taken prior to resolving the incident
* Timescales for resolution
* Escalation procedures
* Evidence preservation

Incident models streamline the process and reduce risk.

Incident management has close relationships with and dependencies on other service management processes, including:

* Change management. The resolution of an incident may require the raising of a change request. Also, since a large percentage of incidents are known to be caused by implementation of changes, the number of incidents caused by change is a key performance indicator for change management.
* Problem management. Incident management, as noted above, benefits from the KEDB, which is maintained by problem management. Problem management, in turn, depends on the accurate collection of incident data in order to carry out its diagnostic responsibilities.
* Service asset and configuration management. The configuration management system (CMS) is a vital tool for incident resolution because it identifies the relationships among service components and also provides the integration of configuration data with incident and problem data.
* Service level management. The breach of a service level is itself an incident and a trigger to the service level management process. Also, service level agreements (SLAs) may define timescales and escalation procedures for different types of incidents.
* [**Remedy Incident Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-incident-management.html)

**Remedy Incident and Problem Management**

[](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

Based on ITIL® best practices, Remedy Incident and Problem Management capabilities give IT comprehensive visibility into the vital connections between IT infrastructure and business services.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/remedy-incident-management.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

**What is an Incident?**

ITIL defines an incident as an unplanned interruption to or quality reduction of an IT service. The service level agreements (SLA) define the agreed-upon service level between the provider and the customer.   
  
Incidents differ from both problems and requests. An incident interrupts normal service; a problem is a condition identified through a series of multiple incidents with the same symptoms. Problem management resolves the root cause of the problem; incident management restores IT services to normal working levels. Requests for fulfillment are formal requests to provide something. These may include training, account credentials, new hardware, license allocation, and anything else that the IT service desk offers. A request may need approvals before IT fulfills it.   
  
Incidents interrupt normal service, such as when a user’s computer breaks, when the VPN won’t connect, or when the printer jams. These are unplanned events that require help from the service provider to restore normal function.

**What is ITIL Incident Management?**

When most people think of IT, incident management is the process that typically comes to mind. It focuses solely on handling and escalating incidents as they occur to restore defined service levels. Incident management does not deal with root cause analysis or problem resolution. The main goal is to take user incidents from a reported stage to a closed stage.   
  
Once established, effective incident management provides recurring value for the business. It allows incidents to be resolved in timeframes previously unseen. For most organizations, the process moves support from emailing back and forth to a formal ticketing system with prioritization, categorization, and SLA requirements. The formal structures take time to develop but results in better outcomes for users, support staff, and the business. The data gathered from tracking incidents allows for better problem management and business decisions. Incident management also involves creating incident models, which allow support staff to efficiently resolve recurring issues. Models allow support staff to resolve incidents quickly with defined processes for incident handling. In some organizations, a dedicated staff has incident management as their only role. In most businesses, the task is relegated to the service desk and its owners, managers, and stakeholders. The visibility of incident management makes it the easiest to implement and get buy-in for, since its value is evident to users at all levels of the organization. Everyone has issues they need support or facilities staff to resolve, and handling them quickly aligns with the needs of users at all levels.   
  
Operational incident management requires several key pieces:

1. A service level agreement between the provider and the customer that defines incident priorities, escalation paths, and response/resolution time frames
2. Incident models, or templates, that allow incidents to be resolved efficiently
3. Categorization of incident types for better data gathering and problem management
4. Agreement on incident statuses, categories, and priorities
5. Establishment of a major incident response process
6. Agreement on incident management role assignment

Number five in the list above is important to incident management. The incident manager is tasked with handling incidents that cannot be resolved within agreed-upon SLAs, such as those the service desk can’t resolve. In many organizations, this person may be an IT operations manager or an IT technical lead.

**Incident Management’s Main Function: The Service Desk**

Incident management involves several functions. The most important is the service desk. The service desk is also known as the “help desk”. The service desk is the single point of contact for users to report incidents. Without the service desk, users will contact support staff without the limitations of structure or prioritization. This means that a high-priority incident may be ignored while the staff handles a low-priority incident. Low-priority incidents, such as fixing a bad docking station, might not get resolved for weeks while the IT support staff handles the most pressing issues presented to them at that moment. The structure of the service desk enables support staff to handle everyone’s issues promptly, encourages knowledge transfer between support staff, creates self-service models, collects IT trend data, and supports effective problem management.   
  
A service desk is divided into tiers of support. The first tier is for basic issues, such as password resets and basic computer troubleshooting. Tier-one incidents are most likely to turn into incident models, since the templates to create them are easy and the incidents recur often. For example, a template model for a password reset includes the categorization of the incident (category of “Account” and type “Password Reset”, for example), a template of information that the support staff completes (username and verification requirements, for example), and links to internal or external knowledge base articles that support the incident. Low-priority tier-one incidents do not impact the business in any way and can be worked around by users.   
  
Second-tier support involves issues that need more skill, training, or access to complete. Resetting an RSA token, for example, may require tier-two escalation. Some organizations categorize incidents reported by VIPs as tier two to provide a higher quality of service to those employees. Tier-two incidents may be medium-priority issues, which need a faster response from the service desk.  
  
Correct assignment of tiers and priorities occurs when most incidents fall into tier one/low priority, some fall into tier two, and few require escalation to tier three. Those that require urgent escalation become major Incidents, which require the “all-hands-on-deck” response. Major Incidents are defined by ITIL as incidents that represent significant disruption to the business. These are always high priority and warrant immediate response by the service desk and often escalation staff. In the tiered support structure, these incidents are tier three and are good candidates for problem management.

**The Incident Process**

In ITIL, incidents go through a structured workflow that encourages efficiency and best results for both providers and customers. ITIL recommends the incident management process follow these steps:

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization
5. Incident response
   * Initial diagnosis
   * Incident escalation
   * Investigation and diagnosis
   * Resolution and recovery
   * Incident closure

The incident process provides efficient incident handling, which in turn ensures continual service uptime.   
  
The first step in the life of an incident is incident identification. Incidents come from users in whatever forms the organization allows. Sources of incident reporting include walk-ups, self-service, phone calls, emails, support chats, and automated notices, such as network monitoring software or system scanning utilities. The service desk then decides if the issue is truly an incident or if it’s a request. Requests are categorized and handled differently than incidents, and they fall under request fulfillment.   
  
Once identified as an incident, the service desk logs the incident as a ticket. The ticket should include information, such as the user’s name and contact information, the incident description, and the date and time of the incident report (for SLA adherence). The logging process can also include categorization, prioritization, and the steps the service desk completes..  
  
Incident categorization is a vital step in the incident management process.   
  
Categorization involves assigning a category and at least one subcategory to the incident. This action serves several purposes. First, it allows the service desk to sort and model incidents based on their categories and subcategories. Second, it allows some issues to be automatically prioritized. For example, an incident might be categorized as “network” with a sub-category of “network outage”. This categorization would, in some organizations, be considered a high-priority incident that requires a major incident response. The third purpose is to provide accurate incident tracking. When incidents are categorized, patterns emerge. It’s easy to quantify how often certain incidents come up and point to trends that require training or problem management. For example, it’s much easier to sell the CFO on new hardware when the data supports the decision.   
  
Incident prioritization is important for SLA response adherence. An incident’s priority is determined by its impact on users and on the business and its urgency. Urgency is how quickly a resolution is required; impact is the measure of the extent of potential damage the incident may cause.

1. **Low-priority incidents** are those that do not interrupt users or the business and can be worked around. Services to users and customers can be maintained.
2. **Medium-priority incidents** affect a few staff and interrupt work to some degree. Customers may be slightly affected or inconvenienced.
3. **High-priority incidents** affect a large number of users or customers, interrupt business, and affect service delivery. These incidents almost always have a financial impact.

Once identified, categorized, prioritized, and logged, the service desk can handle and resolve the incident. Incident resolution involves five steps:

1. **Initial diagnosis**: This occurs when the user describes his or her problem and answers troubleshooting questions.
2. **Incident escalation**: This happens when an incident requires advanced support, such as sending an on-site technician or assistance from certified support staff. As mentioned previously, most incidents should be resolved by the first tier support staff and should not make it to the escalation step.
3. **Investigation and diagnosis**: These processes take place during troubleshooting when the initial incident hypothesis is confirmed as being correct. Once the incident is diagnosed, staff can apply a solution, such as changing software settings, applying a software patch, or ordering new hardware.
4. **Resolution and recovery**: This is when the service desk confirms that the user’s service has been restored to the required SLA level.
5. **Incident closure**: At this point, the incident is considered closed and the incident process ends.

**Incident Statuses**

Incident statuses mirror the incident process and include:

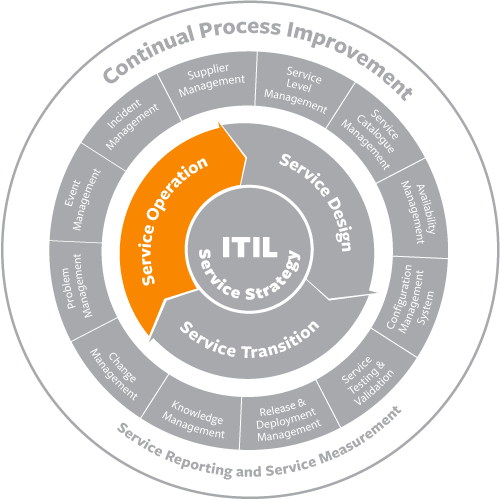
* New
* Assigned
* In progress
* On hold or pending
* Resolved
* Closed

The **new** status indicates that the service desk has received the incident but has not assigned it to an agent.  
  
The **assigned** status means that an incident has been assigned to an individual service desk agent.

The **in-progress** status indicates that an incident has been assigned to an agent but has not been resolved. The agent is actively working with the user to diagnose and resolve the incident.  
  
The **on-hold** status indicates that the incident requires some information or response from the user or from a third party. The incident is placed “on hold” so that SLA response deadlines are not exceeded while waiting for a response from the user or vendor.  
  
The **resolved** status means that the service desk has confirmed that the incident is resolved and that the user’s service has restored to the SLA levels.  
  
The **closed** status indicates that the incident is resolved and that no further actions can be taken.   
  
Incident management follows incidents through the service desk to track trends in incident categories and time in each status. The final component of incident management is the evaluation of the data gathered. Incident data guides organizations to make decisions that improve the quality of service delivered and decrease the overall volume of incidents reported. Incident management is just one process in the service operation framework. Read on to learn about ITIL continual service improvement (CSI).

**What is Access Management?**

Access management works closely with information security management to ensure that the access provisions of the information security policy are enforced. Requests for access may be initiated as service requests and be handled by the service desk, or may be routed to a security group for fulfillment.



A major part of information security management is controlling access to applications or data. Access management is responsible for dealing with requests from users for access. This process involves username and password control, but also includes the creation of groups or roles with defined access privileges, and then controlling access by defining group membership.

In addition to granting rights, access management revokes rights when a user’s status changes through transfer, resignation, or termination. Also, access management should periodically review the roles or groups used to control access to ensure that only necessary rights are being granted and that there are no rights conflicts among the roles or groups.

Access management is also known as **identity management** or **rights management**. Its role is to make sure that the individuals in an organization are able to use the systems that help them do their job, but only have as much access to them as they really need. This process runs on the information security principle of “least privilege” (or “least authority”), which states that each user must only be able to access the information or resources necessary to their job. While it may seem like a burden to have to deny access to those users who want it, it's important for everyone to follow the process. Access management enables the organization to maintain a secure environment that not only prevents unauthorized usage, but also averts data breaches that can erode customer trust and incur financial penalties.

**Access Management Definitions**

* **Access** is the level or extent of an application's functionality that a user is allowed to use. For example, in a file server or content management system, access is whether a user can read a file, read and write a file, edit a file, or delete a file.
* **An access request** is the way in which a user requests to be able to access a service. This is usually a request for a login via a service request from the service desk.
* **The information security policy** is the document that provides the rules that access management then implements. The information security management process builds and maintains this policy.**Identity** is the information needed to tell you who a user is. It is used to verify a user's status within an organization and define his or her access levels. An identity is unique to the user.
* **Rights,** also known as privileges, are the settings that you provide to a user along with their access. For example, a user may have access to view an internal wiki but may not be allowed to edit or delete anything in the wiki.&
* **Service groups** are similar sets of services. These services might perform similar or interrelated functions, such as a ticketing system and a call center system. This is implemented when users are added to a specific group that then grants similar access across multiple systems.

**Access Management Activities**

ITIL is very clear about the hierarchy of access decision-making, stating that access should be granted according to the rules set by the information security policy. Access management should not dictate any of the security policies. The activities of access management, therefore, respond according to the rules that have already been set.

**Request Access**

This is the first step in implementing access management. Requests can come from the service desk via a service request (in service operation) or from a request for change (in service transition). Access can involve going from not having access to having access, or from having one level of access to another level. Ideally, the service catalog should include processes for responding to requests. This activity should define who can request access, what information is required, and how the request will go through the system.

**Verification**

This activity verifies that an individual who requests access is qualified to ask for it. The user must prove their identity and that they have a legitimate business reason for the request. Different levels of access may include different amounts of verification. For example, access to view and edit financial reports should require much different approval requirements than the verification required to create a new user with default permissions.

**Providing Rights**

Once the individual has been verified, it's time to provide access. This involves adding the user to a new group, if needed. Credentials may need to be created in each system that a user requests to access. It is the job of access management to ensure that the access provided does not interfere with any other access rights already granted. Building the catalog of user roles and access profiles helps keep the different groups straight.

**Monitoring Identity Status**

Identity status changes are vitally important, especially for large organizations. This is where having a repository of access that has already been given is vital. If there are too many people processing access change requests, there is a chance that access could be granted that could conflict with other access granted. Automatically monitoring security changes also ensures that access is only being granted according to policy.

**Logging and Tracking Access**

By logging and tracking access changes, your organization ensures that the access being granted is only used as intended. Tracking changes also protects the organization from security gaps and risks. Events such as unauthorized access, unusual application activity, and excessive incorrect login attempts should be evaluated for security breaches.

**Removing or Restricting Rights**

This activity involves removing access once it has been granted or restricting access based on user roles. This occurs when users change roles over the course of their employment, working in different departments or on different systems. Whether a user is terminated, dies, changes roles, moves departments, or changes physical locations, there should be a process in place for granting them the access their role should allow.These activities are the foundation of a solid information security policy. Processes should exist for each activity as it applies to each user role.

**Access Management Processes**

Access management has two sub-processes:

1. **Maintaining a catalog of user roles and access profiles**: This process involves building and maintaining an active repository of all of the user roles and access profiles within the organization. User roles are defined listings and hierarchies of all the roles in an organization, including types of users, such as service desk agent, business user, sales person, etc. It is important to review these roles periodically, particularly when requests come in for access changes that don't seem to correspond to the role. The access given to roles should also be evaluated when new software is purchased or decommissioned. This allows you to grant and remove access based on the process rather than by one-off requests.
2. **Provisioning user access requests**: This sub-process is where access management activities come into play. Access management verifies the user, provides access rights, monitors the identity status, removes or restricts access, and logs and tracks access. The success of this sub-process depends maintaining an accurate user profile and access repository.

**Access Management and Other ITIL Processes**

Access management interfaces with many other stages, such as:

* Component management inside capacity management when there is a license limit that would inhibit the creation of new logins
* Financial management when adding an additional user would impose a financial cost
* Service design and service strategy when services and components are discussed and the number of logins needed must be agreed upon
* Other service operation processes when the service desk sends a request to access management

Access management is the sole process responsible for implementing security policies. As the guardian of the organization's systems, it is as vital to the health of the organization as the locks on the front door. Unfortunately, it is often one of the last formal processes to be fully fleshed out in the service operation stage of the ITIL lifecycle.

**What is Problem Management?**

Problem management is one aspect of ITIL implementation that gives many organizations headaches. The difficulty lies in the similarity between incident management and problem management. The two processes are so closely aligned that differentiating the activities can become difficult for ITIL novices. At what point does one turn into the other? In some organizations, the two processes aret so closely related they are combined altogether. The differences are important, however, since they are not the same and have different objectives.

The term “problem” refers to the unknown cause of one or more incidents. A useful metaphor for understanding the relationship between problems and incidents is to think of the relationship between a disease and its symptoms. In this metaphor, the disease is the problem and the symptoms are the incidents. Just as a doctor uses the symptoms to diagnose the disease, so problem management uses the incidents to diagnose the problem.

When incidents occur, the role of incident management is to restore service as rapidly as possible, without necessarily identifying or resolving the underlying cause of the incidents. If incidents occur rarely or have little impact, assigning resources to perform root-cause analysis can’t be justified. However, if an individual incident or a series of repeated incidents causes significant impact, problem management is tasked with diagnosing the underlying cause of the incidents and, ultimately, to identify a means to remove that cause.



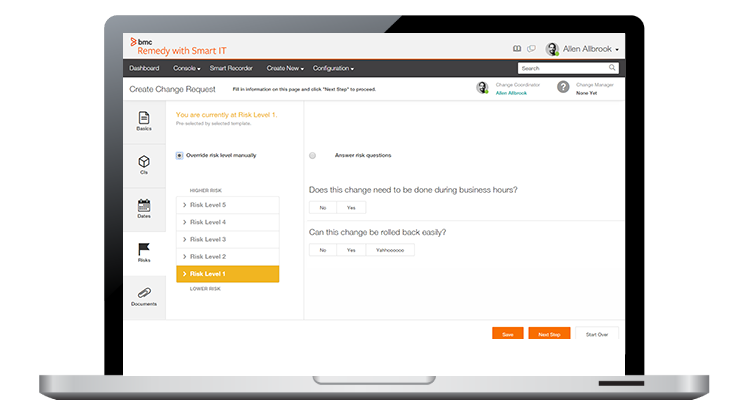
Problem management’s first activity is to diagnose the problem and validate any workarounds. Problem management uses a problem database to track problems and to associate any identified workarounds with them. Once the problem has been diagnosed and a workaround identified, the problem is referred to as a “known error.” These are documented in the known error database (KEDB), which may be the same physical database as the problem database. The KEDB is a significant tool for incident management in resolving incidents caused by known errors.

After the known error has been identified, the next step is to determine how to fix it. This will typically involve a change to one or more CIs, so the output of the problem management process would be a request for change, which would then be evaluated by the change management process, or included in the CSI register.

Problem management is thought of as a reactive process in that it is invoked after incidents have occurred, but it is actually proactive, since its goal is to ensure that incidents do not recur in the future, or if they do, to minimize their impact.

* [**Remedy Problem Management: Free Trial**](http://www.bmcsoftware.uk/guides/itil-problem-management.html)

**Remedy Incident and Problem Management**

[](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

Based on ITIL® best practices, Remedy Incident and Problem Management capabilities give IT comprehensive visibility into the vital connections between IT infrastructure and business services.

[Learn More ›](http://www.bmcsoftware.uk/it-solutions/remedy-incident-management.html) [Free Trial ›](http://www.bmcsoftware.uk/forms/remedy-itsm-trial.html)

**Problem Management 101**

Problem management is a step beyond incident management in the ITIL service operation lifecycle. Incident management handles any unplanned interruption to or quality reduction of an IT service, whereas problem management handles the root causes of incidents. Or in clearer terms, incident management restores service whereas problem management eliminates the cause of failed services.  
  
A **problem** is defined by ITIL as the cause of one or more incidents. Some incidents, such as a malfunctioning mouse at a user’s workstation, are not indicative of a problem. Other incidents, such as repeated network outages, create a problem investigation due to their frequency. In this case, problem management is reactive. Proactive problem management involves addressing the state of hardware, software, and processes, and preemptively addressing issues before they cause excessive incidents. Neither incident management nor request management has the ability to be proactive like problem management.

**The Purpose of Problem Management**

When users continue to face the same incidents without resolution, they lose trust in the service desk’s ability to resolve any problem. Hence the primary objective of problem management is to identify, troubleshoot, document, and resolve the root causes of repeated incidents. Incident information filters up to problem management and problem management, in turn, provides the service desk with the known error and workaround information necessary to mitigate problems in the short term.

Problems include issues such as failing hardware or an inadequately configured database query. Problem management reduces incidents over the long term. Incident reduction decreases the load on the service desk, improves end-user satisfaction, and decreases the long-term costs associated with user and service downtime. When problems cannot be resolved, problem management works with the service desk to mitigate the impact of the related incidents. The end goal of problem management should always be to reduce the overall quantity of preventable incidents and thereby increase the quality of service provided.

**The Scope of Problem Management**

Problem management has a very limited scope and includes the following activities:

• Problem detection  
• Problem logging  
• Problem categorization  
• Problem prioritization  
• Problem investigation and diagnosis  
• Creating a known error record  
• Problem resolution and closure  
• Major problem review

**The Main Function of Problem Management**

While problem management involves several functions, the most important is the **service desk**. While it is also known as a help desk, this is not the ITIL-preferred term and should be avoided. In ITIL, this function acts as the single point of contact for service customers to report incidents and submit service requests. Without a single point of contact, users may contact staff and expect immediate service without prioritization limitations. Unfortunately, this means that urgent incidents could be ignored while incidents that don't impact the business get handled first. Another common scenario is that important but low-priority incidents are not handled for weeks while the IT support staff take care of the most pressing issues on their desks, leaving no time for smaller issues. The service desk allows the service provider to address everyone’s issues promptly and sequentially. It also encourages knowledge transfer between departments, collects data on IT trends, and feeds problem management.   
  
This function can be divided into separate support levels called tiers. The first tier is for basic issues. This includes low-priority issues such as basic computer troubleshooting. Tier one incidents are the most likely to be turned into incident models, since these are easy to solve and recur often. Tier-one incidents do not impact the business or other users. They can always be worked around until the service desk resolves them. For example, a Microsoft® Outlook® error can be worked around by using the web-based email application instead.

Then there's tier two. The second-tier support level handles issues that have some impact on the user but not on the business as a whole. Usually these incidents require more skill or access to resolve. Tier-two incidents are medium priority, and require a more immediate response and higher level of access or training than tier-one incidents.   
  
Tier-three incidents affect the entire organization and many users. Sometimes, a VIP may fall into a tier-two or tier-three categorization to provide a faster response time for these users. Often, these incidents fall into the Major Incident Response (MIR) process. These incidents are defined by ITIL as those that cause significant disruption to the business. These are always high priority. Incidents that require MIR are good candidates as potential problems, since they affect the business and likely have a different root cause than regular incidents.  
  
You'll know that you've accurately assessed tiers and priorities when most incidents fall into tier one/low priority, fewer fall into tier two, and only a few require escalation to tier three.   
  
The service desk interfaces with the problem management team in several ways. The first interaction is when a potential problem is raised. This often happens when an incident is deemed unresolvable at the service desk and must be escalated. This also happens when an incident occurs repeatedly despite normal troubleshooting and resolution steps. Finally, when the problem management or continual service improvement team identifies problems proactively, they may contact the service desk for more information or incident statistics.

**The Problem Management Process**

The ITIL problem management process has many steps, and each is vitally important to the success of the process and the quality of service delivered.  
  
The first step is to **detect the problem**. A problem is raised either through escalation from the service desk, or through proactive evaluation of incident patterns and alerts from event management or continual service improvement processes. Signs of a problem include incidents that occur across the organization with similar conditions, incidents that repeat despite otherwise successful troubleshooting, and incidents that are unresolvable at the service desk.

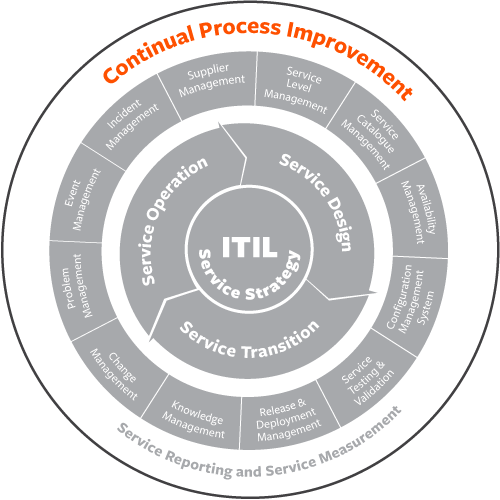
The second step is to **log the problem**. In an ITIL framework, problems are logged in a problem record. A problem record is a compilation of every problem in an organization. This can be accomplished via a ticketing system that allows for problem ticket types. Pertinent problem data, such as the time and date of occurrence, the related incident(s), the symptoms, previous troubleshooting steps, and the problem category all help the problem management team research the root cause.  
  
The third step is to **categorize the problem**. Problem categorization should match incident categorization. Incident [and problem] categorization involves assigning a main and secondary category to the issue. This step is beneficial in several ways. One benefit is that it allows the service desk to sort and model incidents that occur regularly. The modeling allows for automatic assignment of prioritization. The third and most important benefit is the ability to gather and report on service desk data. This data allows the organization to not only track problem trends, but also to assess its effect on service demand and service provider capacity.   
  
The fourth step is to **prioritize the problem**. A problem’s priority is determined by its impact on users and on the business and its urgency. Urgency is how quickly the organization requires a resolution to the problem. The impact is a measure of the extent of potential damage the problem can cause the organization. Prioritizing the problem allows an organization to utilize investigative resources most effectively. It also allows organizations to mitigate damage to the service level agreement (SLA) by reallocating resources as soon as the issue is known.  
  
The fifth step is a two-part process, which involves **investigating and diagnosing the problem**. The speed at which a problem is investigated and diagnosed depends on its assigned priority. High-priority issues should always be addressed first, as their impact on services is the greatest. Correct categorization helps here, since identifying trends is easier when problem categories correlate to incident categories. Diagnosis usually involves analyzing the incidents that lead to the problem report as well as further testing that may not be possible at the service desk level, such as advanced log analysis.  
  
The sixth step is to **identify a workaround for the problem**. A workaround should always be indicated, because problems are not resolved at the incident level. A workaround enables the service desk to restore services to users while the problem is being resolved. A problem can take anywhere from an hour to months to resolve, therefore a workaround is vital. A problem is considered open until resolved, so a workaround should only be considered a temporary measure.  
  
Step seven is to **raise a known error record**. Once the workaround has been identified, it should be communicated to staff within the organization as a known error. It’s good practice to record a known error in both an incident knowledge base and what ITIL calls a known error database (KEDB). Documenting the workaround allows the service desk to resolve incidents quickly and avoid further problems being raised on the same issue.   
  
Step eight is to **resolve the problem**. Problems should be resolved whenever possible. Resolution resolves the underlying cause of a set of incidents and prevents those incidents from recurring. Some resolutions may require the change management board, as they may affect service levels. For example, a database switchover may cause slowness during the switchover period. All risks should be evaluated and accounted for before implementing the resolution. Document the steps taken to resolve the problem in the organization’s knowledge base.   
  
The ninth step is to **close the problem**. This step should only occur after the problem has been raised, categorized, prioritized, identified, diagnosed, and resolved. While many organizations stop at this step, it isn't the last according to ITIL.  
  
The final step is to **review the problem**. This is also known as a major problem review. The major problem review is an organizational activity that prevents future problems. During the review, the problem management team evaluates the problem documentation and identifies what happened and why. Lessons learned, such as process bottlenecks, what went wrong, and what helped should be discussed. This is where having a complete problem log will help. A completed log will work much better than trying to pull the details from memory. This problem review should result in improved processes, staff training, or more complete documentation.

**How Problem Management Fits into ITIL**

Problem management is only one component of the ITIL service management lifecycle. Within ITIL, it exists in the [service operation](http://www.bmc.com/guides/itil-service-operation.html) main process. As a process, it interfaces with many other parts of ITIL. Due to its relationship with the service desk, it is directly affected by and affects [incident management](http://www.bmc.com/guides/itil-incident-management.html). It also interfaces with financial management, since the financial impact of a problem is considered during the prioritization and resolution stages. It interfaces with[service design](http://www.bmc.com/guides/itil-service-design.html) when past and potential problems are considered during the IT design process. It interfaces with knowledge management when known issues are recorded. Finally, it interfaces with [continual service improvement](http://www.bmc.com/guides/itil-continual-service-improvement.html) when problem management is proactive, since both have the goal of improving the quality of service delivered to internal and external customers.  
  
This process is one that is integral to long-term service delivery success and therefore should not be ignored when designing a robust IT service, whether it's internally or externally facing. Read on to discover more about the ITIL lifecycle.

# What is Continual Service Improvement?

Continual Service Improvement (CSI) uses a metrics-driven approach to identifying opportunities for improvement and to measure the impact of improvement efforts. Although CSI is a phase of the lifecycle and is documented in a separate ITIL publication, CSI can be effective only if it is integrated throughout the lifecycle, creating a culture of continual improvement. CSI should ensure that all participants in service delivery understand that identifying opportunities for improvement is their responsibility.



An important task for CSI is to identify which metrics out of the thousands that are created daily should be monitored. This is done by identifying, for each service or process, what the critical success factors (CSFs) are. CSFs must be present if a process or service is to succeed. It is recommended that each process or service have identified no more than three to five CSFs (one or two in the early life of a service or process).

To determine whether CSFs are present, it is necessary to identify key performance indicators (KPIs) that represent the degree to which the CSF is present. Again, it is recommended that each CSF be measured by no more than three to five KPIs (one or two in the early life of a service or process). It’s important to keep in mind that, although most KPIs are quantitative, qualitative KPIs, such as customer satisfaction, need to be considered as well.

CSI is based on the Plan-Do-Check-Act approach developed by W. Edwards Deming. This is implemented in the CSI approach, as follows:

* What is the vision? What is our long-term objective?
* Where are we now? What are the current values of our KPIs?
* Where do we want to be? What are the desired KPI values?
* How do we get there? What’s the plan?
* Did we get there? Do the KPI values after implementation of the plan meet our objectives?
* How do we keep up the momentum? Let’s go back to the beginning.

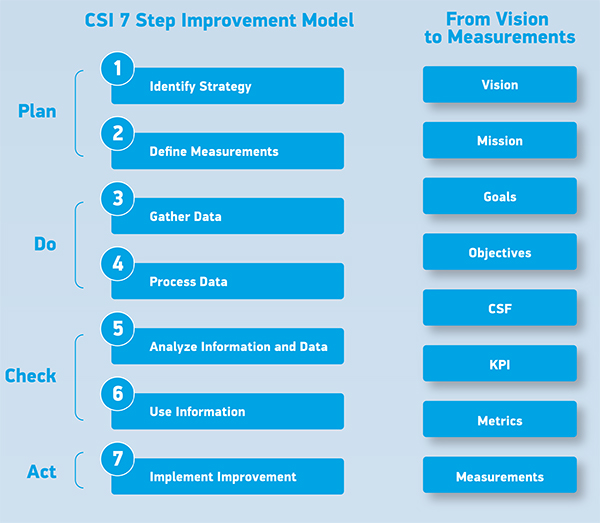
CSI uses a 7-step process to guide how data is collected and used:

* Define the objectives.
* Determine what to measure.
* Collect the data.
* Process the data.
* Analyze the data.
* Present and use the information.
* Implement improvement.

If CSI is performing its role properly, there will be improvement suggestions arising from all parts of service delivery. The organization is unlikely to have enough resources to implement all of the suggestions, so it is necessary to capture the improvement opportunities, understand their impact, scope, and resource requirements, and prioritize their implementation. CSI uses the CSI register as a tool to document, analyze, and plan for improvements.

# 7-step Improvement Process

The 7-step improvement process in ITIL is integrated with the Deming Cycle and the DIKW (Data-Information-Knowledge-Wisdom) model. Improvement can be made across the ITIL lifecycle with each stage of the lifecycle support giving feedback to the other stages for collaborative coordinated improvements.



1. Identify the strategy for improvement
2. Define metrics
3. Gather data
4. Process data
5. Analyze data
6. Use the data for improvement decisions
7. Implement improvements

Special attention should be given to economic value of improvements, because all organizations have to recover cost for service delivered in order to exist. Financial management concepts and metrics pertaining to ROI, TCO, VOI, and ROA help here.