ITIL

Service Operation & Continual Service Improvement

Phases of Lifecycle in ITIL

1. **Service Strategy** : Describes business goals and customer requirements and how to align objectives of both entities.
2. **Service Design** : Outlines practices for the production of IT policies, architectures and documentation.
3. **Service Transition :** Advises on change management and release practices, and also guides admins through environmental interruptions and changes.
4. **Service Operation :** Offers ways to manage IT services on a daily, monthly and yearly basis.
5. **Continual Service Improvement :** Covers how to introduce improvements and policy updates within the ITIL process framework

Service Operation

- Service operation ensures that services are being provided efficiently and effectively as per SLAs.
- It includes monitoring services, resolving incidents, fulfilling requests and carrying out operational tasks.
- Service operation encompasses the day-to-day activities, processes, and infrastructure responsible for delivering value to the business through technology

What is service operation? 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.

Service operation encompasses the day-to-day activities, processes, and infrastructure that are responsible for delivering value to the business through technology. Just as most people expect the lights to turn on at every flick of a switch, business users have become completely dependent on the capabilities that IT services enable.

Think of service operation as a managed service provider or a utility company responsible for providing the power that customers need to do their jobs. Without electricity, many activities would come to a halt. Further, without the processes to ensure the delivery of that electricity, the service would be unreliable. Utility companies must also be proactive, for example, trimming trees to prevent outages from falling branches that may sever electric lines. Customers don't care about all the required resources (e.g., people, process, and technology) involved in delivering electricity to their homes. They just want reliable service when they need it and at a fair cost.

IT users have similar expectations about consuming technology services. As a result, IT organizations must work to ensure that the underlying service delivery and support infrastructure is optimized to provide continuous value and service to their customers. Effective operations teams must first work to prevent problems. If an issue occurs, they must understand the impact from a user's perspective and then follow up with swift, corrective action to restore service.

Just as a utility company provides various service packages to its customers— such as energy conservation programs along with the delivery of gas and electricity— IT offers a catalog of services to its customers. ITIL Service Operation focuses on the well-planned capabilities, functions, processes, and controls that need to be in place to provide continuous utility to the business based on the promised warranties and service level agreements (SLAs).

ITIL Service Operation stresses the importance of measuring the experience from a user perspective, instead of merely monitoring all of the discrete infrastructure components.

User consumption of IT resources for software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) is totally dependent on IT asset availability. Operations must be agile and high performing; otherwise, users will seek alternate solutions to enable business outcomes, introducing new risks and complexities.

IT must be able to create a “consumerized” experience for users who interact with the services they provide. This experience should expand on the concept of user self-service and work effectively with mobile computing platforms.

With the growth in Bring Your Own Device (BYOD) initiatives, you need to manage personal devices with the same rigor as any other corporate-owned device. Finally, as more people turn to social media for IT support, you need to incorporate and integrate social media channels with your IT Service Management (ITSM) solutions to enable the service desk to easily and seamlessly engage with the user.

Each stage of the lifecycle influences the other stages and relies on them for input and feedback. This interaction and interdependence between stages creates a lifecycle that is highly dynamic in nature.

For example, service operation should include a strategy for improvement initiatives. Service operation is directly supported by service strategy and continual service improvement, and the results should be designed and transitioned into operations effectively and efficiently.

IT needs to be integrated with the business. By following the principles of service operation, IT can increase its standing as a strategic business asset. IT must demonstrate specialized skills, capabilities, and resources to support business outcomes.

With closer collaboration, IT can help the business become more effective, efficient, and economical. Through innovations, such as cloud computing, social, and mobile technologies, IT can help the business unlock new opportunities and explore different ways of working.

IT operations can help deliver the power its customers need to be successful. Ultimately, IT should aim to provide users with the same excellent experience at work that they enjoy with their personal devices. In a very real sense, the expectations that users bring into the workplace are helping to increase the performance of the IT organization.

Event Management

- The objective of this process is to make sure all CIs are monitored constantly. It also filters and categorizes the events in order to decide on appropriate actions.
- objective of event management is to detect events, analyze them, and determine the right control action (if any).

- Provide a strong foundation to automate key components of your IT operation
- Improve detection and response times to incidents, changes, exceptions, etc.
- Reduce downtime as a result of the above

Thousands (or millions) of events happen across your IT infrastructure every day. In large enterprises, the number could be billions. Why? Because an event is simply a change to the state of an IT service or configuration item (CI) that is significant to its management.

A server moving from online to idle could be an event, or the completion of a regular server maintenance script: they’re worth knowing about, and there may even be an action you wish to take as a result. By doing so, the event management process also provides a strong foundation for service assurance, reporting, and service improvement.

It’s important to know, though, that monitoring and event management are not the same thing. Monitoring is certainly a component of event management, in that it is a useful way to detect events as they occur. Event management, on the other hand, is focused on extracting meaning out of events, to help IT take appropriate actions (when required).

The scope and benefits of event management Event management can be applied to any aspect of service management that needs to be controlled and which can be automated — from networks, servers, and applications all the way to environmental conditions like fire and smoke detection and security and intrusion detection.

Since event management can be applied to just about every aspect of service management in your IT organization, the benefits are widespread.

So what does success look like? In event management, success is being able to detect, communicate, and take the appropriate action for every event (or change in state) that is significant to managing your IT services and the CIs that support them.

Event management process flow

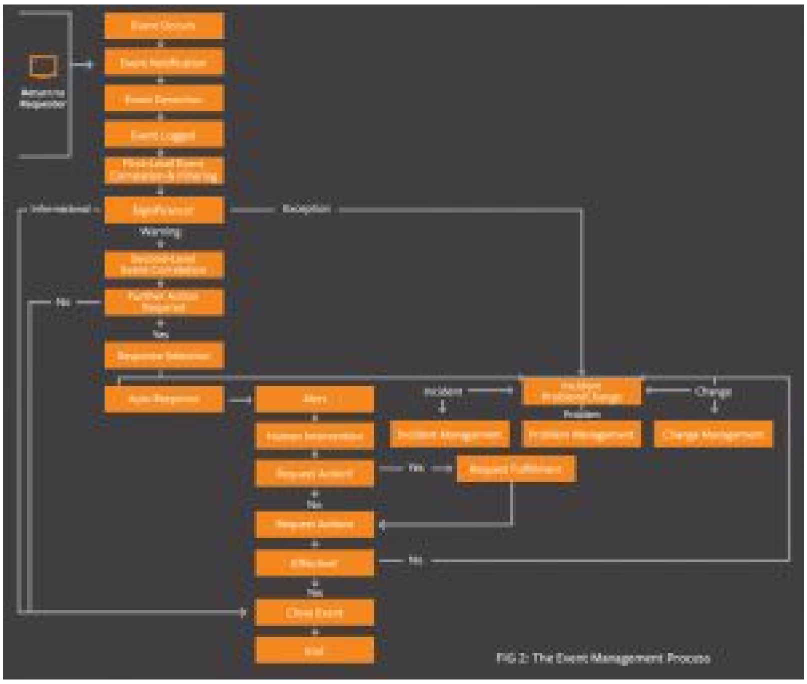


FIG 2: The Event Management Process

What's the difference between events and incidents? It's a great question, and the answer is simple. Incidents are unplanned interruptions or significant reductions in the quality of an IT service. When an incident occurs, something is wrong. Events, on the other hand, are simply changes in the state of your services, CI's, or pretty much anything of significance across your IT infrastructure.

So can an incident be an event? Absolutely. All incidents are events, since an outage or service quality reduction is a change in the state of that service. But not all events are incidents, since an increase in utilization, a user logging in, or an automated backup service completing represents a status change, but not a disruption or degradation in service quality.

In fact, there are three types of events defined by ITIL:

1. **Information.** These events typically don't require a response of any type, since they are basic status updates, or data generated to aid with reporting, etc. Logs and reports are great examples.
2. **Warning.** Warnings are indicators of activity that outside the norm — like a threshold being approached. Like a hurricane or tornado warning, a warning means that you should monitor conditions to make sure they do not worsen — or take action to prevent them from worsening when appropriate. An example of this type of event would be server capacity reaching 75 percentage, or a standard transaction taking 15 percentage longer to complete than normal.
3. **Exception.** Exception events are indicators that something is wrong. The services (and business they support) may be negatively impacted. A network or server being down (as opposed to just approaching capacity) is an example of an exception.

What other activities could be considered events and trigger the event management process? Quite a few — from exceptions to automated processes to simple status changes in a server or database. The sky is the limit.

It is ultimately the job of IT to designate what types of activities they will consider information events, warning events, and exception events. As a general rule, though, you will want to categorize an event as "information" when it will purely be used to gain insight and inform better decision-making. "Warning" events are typically those that may require closer monitoring or even intervention to help you prevent exceptions from occurring. "Exception" means something is really wrong that typically requires immediate action.

The key activities of event management During the design phase of your IT services, you should define which types of events need to be generated, and how they will be generated, for each type of configuration item (CI) involved in delivering the service. The typical event lifecycle is:

1. **Event occurrence** Events occur 24 x 7 x 365. In ITIL Event Management, the key is defining the types of events that are significant to your operation and ensuring you have a system in place to detect them.

2. **Event notification** Notifications are typically sent by monitoring tools or CIs (configuration items). At this stage, these are simply notifications that an event has happened — and have typically not yet been interpreted or correlated to understand the meaning or impact.

3. **Event detection** In this step, a monitoring system, automated agent, or systems management solution receives the notification and determines the meaning of the event.
4. **Event logged** A record of the event is made, along with any subsequent actions taken. This may be done by your systems management solution, or by the individual applications / services / hardware that triggered the event.
5. **Event filtering and correlation** Can the event be ignored, or does it need to be passed on to the events management system? Often, information events are ignored. Warnings and exceptions often require additional action, though. So the first step of this process — called first-level correlation and filtering — is simply filtering which events should be ignored versus passed on to the event management system.In the second level of correlation, a correlation engine uses predefined business rules to determine the significance of warning and exception events, and decide the appropriate next steps.
6. **Event response / further action** Remember, all events (and responses) should be logged. In addition, based on the event type and severity, the correlation engine may determine it is appropriate to escalate the event to a team or individual, or in the case of more severe warnings and exceptions, even automatically create an incident, problem, or change.
7. Closing the event

   If an event results in an incident, problem, or change being created, event closure should be handled through those respective processes. They can be "closed" in the event management system by ensuring the event is properly logged as well as the subsequent action taken, and including a link to the corresponding incident, problem, or change request.Like most other ITIL process, event management doesn't live in a bubble. While event management primarily interfaces with incident, problem, and change management (for dealing with exceptions), it also interfaces with:

   - Capacity and availability management for understanding the significance of events, thresholds, etc.
   - Asset Management for managing the status of assets
   - Configuration Management, for managing the status of CIs.

Measuring Your effectiveness To help you gauge the efficiency and effectiveness of your Event Management process, these are just a few of the KPIs you can track.

- The number or percentage of events that become incidents.
- The CIs that generate the most events
- How many events are reported by your monitoring tools, and the breakdown by event category
- The total percentage of events that become incidents (or alternately result in changes), and more specifically, how many of these incidents are reported by your automated systems.

Key recommendations First, be sure to perform a thorough study of the types of events that occur in your IT environment. Know which systems log events, and where, and what the events mean.

That makes it much easier to understand and define which types of events require additional care — whether it's human intervention or automated workflows for handling changes or raising incidents.

Since it's not humanly possible for a live person (or even team of people) to monitor and manage every event triggered by all of your systems, your goal is to create a simple, streamlined set of workflows to automate the easy stuff — and alert your team when more significant events that threaten services (or that require human assistance of any type) occur.

Finally, make sure your event logs are capturing the appropriate level of details — what happened, when it happened, how it was handled, who it was escalated to, and any details of communication with other people or systems to support any actions taken. You'll also want to capture whether events are breaching any of your SLAs or OLAs, to help you remain compliant and provide accurate reporting.

Incident Management

- The purpose of Incident Management is to restore the service to the previous stage as early as possible.
- 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
- Incident as an unplanned interruption to or quality reduction of an IT service. T

Stages in Incident

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization

Incident response

- Initial diagnosis
- Incident escalation
- Investigation and diagnosis
- Resolution and recovery
- Incident closure

ITIL incident management 101 itil service operation

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.

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.

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.

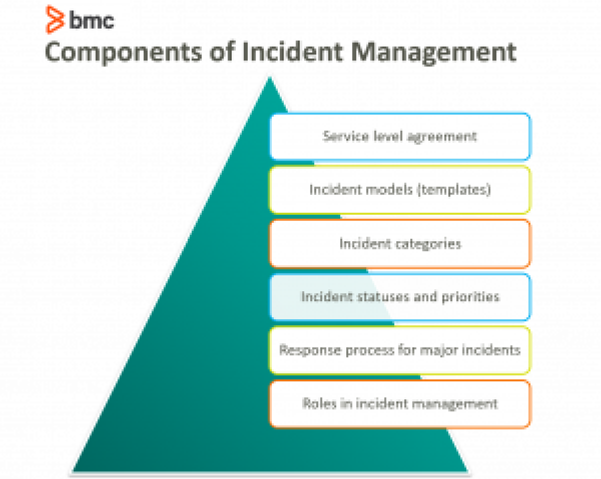
Incidents differ from both problems and requests. An incident interrupts normal service; a problem is a condition identified through a series of multiple incidents with the same symptoms. Problem management resolves the root cause of the problem; incident management restores IT services to normal working 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:


bmc
Components of Incident Management
Service level agreement
Incident models (templates)
Incident categories
Incident statuses and priorities
Response process for major incidents
Roles in incident management

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.

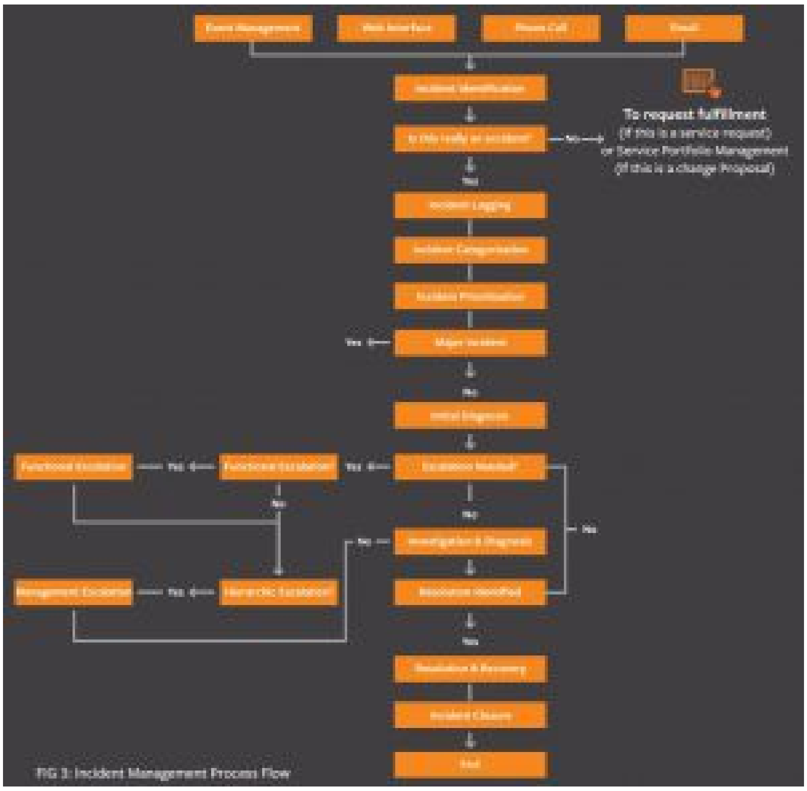


FIG 3: Incident Management Process Flow

Incident statuses Incident statuses mirror the incident process and include:

1. New
2. Assigned
3. In progress
4. On hold or pending
5. Resolved
6. 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).

Request Fulfillment

- This process deals with handling requests such as change password, create new user and create email id etc.
- The types of service you offer, and the requests you receive, will vary dramatically from company to company.

When a user submits a formal request for something — a password change, new hardware or software they would like, or pretty much anything they want or need, it's called a **service request**.

ITIL's formal definition of service request is *"a request from a user for information, advice, a standard change, or access to a service."*

So what's a standard change? A **standard change** is simply a pre-approved change that is low risk and that follows a standard procedure.

It's important right out of the gate to point out the difference between service requests and incidents, though, since they're easily confused but follow much different ITIL processes.

Incidents are unplanned interruptions to your IT services, or reductions in the quality of your IT services. So when a user reports an incident, they are notifying you of the unavailability or decreased performed of an IT service they normally have access to.

Service requests, on the other hand, deal with requests for something new to be provided to the user that they don't already have, whether that's a new version of a software program, or access to an online portal.

In general, service requests are often lower risk, requiring less approval protocol. In fact, many service requests may be things that are already preapproved — like being granted access to a printer in a common area, or upgrading a laptop to the latest version of a company's preapproved productivity software suite.

Since these types of requests are frequent (but also less risky than incidents), ITIL draws a distinction between them, and suggests handling them with their own set of processes.

To that end, request fulfillment is exactly that: the process to handle service requests.

The objectives of request fulfillment

Simply put, request fulfillment is all about making sure customers have easy access to the IT services they need to get their jobs done. Top objectives are:

- To help users clearly understand what services are available, how to request them, and how long it will take for them to be fulfilled
- To create a distinct process for handling service requests that is different from your change management and incident processes
- To properly deliver all of the components of the standard services requested (like software AND licenses, for example, in the instance of a software request)
- To assist with general information, comments, and complaints

Scope Unlike incidents, which are unplanned, service requests can be planned for. That means the process for how you handle each type of service request can be broken down into a thoughtful, methodical set of steps or actions and documented in a process flow.

These request models should be built for each type of request you will receive, and address each step or phase of request fulfillment. Be sure to consider:

- **Who will handle the request?** What individuals or teams are needed?
- **How is the service delivered?** What's the process?
- **How quickly will you fulfill the service request?** Is there an SLA or time window?
- **If the service can't be completely fulfilled, what happens?** Plan for how you will escalate.

Ultimately, it's up to each organization that provides standard services to properly document their offerings.

Why do it, anyway?

Simple. Request fulfillment is all about efficiency and cost reduction. By making it super easy for users to get what they need, you can cut down on the confusion and bureaucracy often associated with asking for what you need. Simple, repeatable processes cost the business far less to fulfill, and in general, result in far happier users.

The service request process

The process begins when a user places a service request. This is often handled through the service desk, using self-help tools where they can easily choose the service they require from a standard menu of selections you have pre-defined.

Not every service request has to come through a web-based self-help interface, however. It's not uncommon for a requestor to call the service desk directly, for instance.

Once a service is requested, it may be automatically approved or alternately routed for approval, since occasionally services are offered that still require management or financial approval, or even approval from a compliance perspective.

In those cases, your request model should include all appropriate approval steps, along with plans for how the request will be handled once approved and declined.

After a requested service is approved, or when no approval is required, the request must be assigned to the appropriate individual or team for review, and ultimately, fulfillment. Simple requests are often handled by the service desk team, whereas requests that require third party products or services may be forwarded on to vendors or other internal / external resources.

At each step of the way, it's important that the service desk keep track of the status of the request. Typical request statuses are:

1. Open
2. Assigned
3. In Progress
4. Pending (approval, additional information, availability, etc.)
5. Complete
6. Closed

Once the service has been delivered (and completion is verified), it should be referred back to the service desk for closure, prior to which the service desk should confirm that the requestor is satisfied with the services delivered.

The 5 sub-processes of ITIL request fulfillment ITIL 2011 completely revised the request fulfillment process, breaking it down into 5 sub-processes:

Request Fulfillment Support

Objective: To provide and maintain the tools, processes, skills and rules for an effective and efficient handling of Service requests.

Request Logging and Categorization

Objective: To record and categorize the Service Request with appropriate diligence and check the requester's authorization to submit the request, in order to facilitate a swift and effective processing.

Request Model Execution

Objective: To process a Service Request within the agreed time schedule.

Request Monitoring and Escalation

Objective: To continuously monitor the processing status of outstanding Service Requests, so that counter-measures may be introduced as soon as possible if service levels are likely to be breached.

Request Closure and Evaluation

Objective: To submit the Request Record to a final quality control before closed. The aim is to make sure that the Service Request is actually processed and that all information required to describe the request's lifecycle is supplied in sufficient detail. In addition to this, findings from the processing of the request are to be recorded for future use.

Relationships to other ITIL processes It's worth noting the linkages between Request Fulfillment and other ITIL processes. While request fulfillment is pretty simple, it still connects to your Financial Management process (to understand the cost of services, and ensure that the resources and workload involved in fulfillment them is accounted for) and your Change Management process (whenever a request relates to a Standard Change).

Measuring your effectiveness ITIL also defines a few key metrics you can use to judge both the efficiency and effectiveness of your request fulfillment process, including:

1. How satisfied your users are with how their service requests are handled
2. The amount of outstanding service requests currently in your backlog
3. How long it takes you to handle each type of service request
4. Cost (per type of service request, on average)
5. The percentage of service requests that are handled within agreed SLAs
6. A breakdown of service requests by stage (i.e., in progress, closed, etc.)

Key recommendations

- **Make it easy to request your services.** Start with the most popular, easy-to-fulfill services, and create a web-based request catalog (using a shopping basket approach) to make it easy for users to place their requests. Ask for the information you need to fulfill the request, but be careful not to bog users down with too many form fields or unnecessary information.
- **Be sure to clearly communicate your SLA's.** It's important that both your service desk, any other parties involved in fulfillment, and your users / customers are all in agreement around how long fulfillment will take.

- **Document the details.** For each service you offer, make sure you think through and document who is allowed to request them, what approvals are required, who pays for them, etc.
- **Stay on top of user satisfaction.** Clear communication at every stage about what to expect and when can keep your customer satisfaction ratings high and reinforce the value of your service desk operation.

Access Management

- This process deals with granting rights to authorized user to use the service.
- Access Management deals with granting access to authorized access while preventing access to non-authorized users.
- Access Manager is the process owner of this process.

Key Points

- Access Management is also known as rights management or identity management.
- Access Management process is executed by technical and application management functions.
- Access Management can be initiated by Service Request through Service Desk

Value to Business

Access Management adds value to business in following ways:

- Employees have right level of access to execute their jobs effectively
- The ability to audit use of services and to trace the abuse of services.
- Controlled access to services ensures that organization is able to maintain more effectively the confidentiality of its information.

Problem Management

- This process deals with finding root cause of the problem and prevent incident to occur again.
- **Problem Management** ensures the identification of problems and performs Root Cause Analysis.
- It also ensures that recurring incidents are minimized and problems can be prevented.

Key Points

- Problem Management comprises of activities required to diagnose the root cause of the incident and to determine the resolution to those problems.
- When a problem is resolved after root cause analysis, it becomes known error.
- Problem Management also records information regarding problems in a system called **Known Error Database (KED)**.

Continuous Service Improvement (CSI)

- **Continuous Service Improvement (CSI)** deals with measures to be taken to improve the quality of services by learning from past successes and failures.
- Its purpose is to align and realign IT Services to the changing needs by identifying and implementing improvements to the changing business needs.
- Increasing the cost-effectiveness and process efficiency of the IT service.

What is ITIL Continual Service Improvement (CSI)? Continual Service Improvement is a type of process which utilizes techniques from quality management so as to learn from prior success and failures and aims constantly to increase efficiency and effectiveness of IT services and processes.

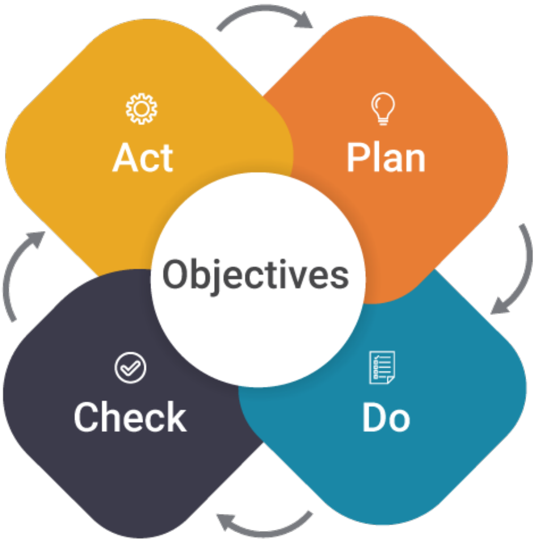
Objectives of ITIL Continual Service Improvement (CSI) ITIL Continual Service Improvement should predominantly focus on maximizing the effectiveness and also increasing the efficiency of the IT Service Management Process. Listed below are a few objectives of ITIL Continual Service Improvement:

- To evaluate, analyze, and make necessary recommendations to improve the existing opportunities in each phase of the ITIL Service Lifecycle such as Service Strategy, Service Design, Service Transition, and Service Operation
- To ascertain and implement activities to increase the quality of the IT service and improve the effectiveness and efficiency of the IT service management process.

- To increase the cost-effectiveness of IT service delivery while maintaining the same level of customer satisfaction.
- To ensure that a standard and relevant method is used for quality management.

The Deming cycle-The PDCA cycle The Deming Cycle (also known as the PDCA cycle) is used as the foundation for quality improvement activities across various types of enterprises. It is used in various industries for controlling and measuring results and taking appropriate steps based on the results to come up with a better output in the later steps.

The PDCA cycle is a four-part lifecycle and thus constitutes the acronym PDCA cycle: Plan, do, check, and act.



- **Plan:** The first step of the process involves planning the improvements. A gap analysis is undertaken and a plan is made to overcome the gap through a series of improvement steps.
- **Do:** The second phase refers to the Implementation of improvements. A project is instigated to close the gaps identified in the previous phase. This phase includes a series of changes to improve the process.
- **Check:** This phase is more accurately defined as monitoring, measuring, and reviewing. The end result of the implemented improvements is associated with the measures for success identified and approved in the planning phase.
- **Act:** The identified improvements are entirely implemented in this step.

The PDCA cycle can be utilized to improve any of the ITIL Service Management processes.

7 Step Improvement Process

The focus of Continual Service Improvement is on service improvement to support business processes. To accomplish this, Continual Service Improvement uses a seven-step process plan for improvement which is crucial for CSI and other stages in the ITIL lifecycle.

The main purpose of this process is to define and manage the steps required to identify, define, gather, process, analyze, present and implement the improvements which have been made over a period of time.

The 7 step improvement process is essential in supporting CSI and operates across the entire service lifecycle. It focuses on identifying the improvement opportunities, not merely for processes and services, but for all the disciplines implemented as a part of the IT Service Lifecycle.

Scope of the Seven-Step Improvement Process

The scope of the CSI seven-step improvement process contains the following areas:

- It includes continuously aligning the portfolio of IT services of the organization to the present and future business requirements.
- The seven-step improvement process includes analysis of the performance and actual capabilities of the services and processes throughout the lifecycle, partners, and technology.

- It makes the best use of whatever the technology that the organization possesses and tries to acquire and utilize new technology when a business case demands it.
- To determine the capabilities of the personnel in the enterprise and to inquire if the right people with the relevant skills are working in appropriate positions.

Value of the Seven-Step Improvement Process

With the help of aforementioned seven-step Improvement processes in ITIL Continuous Service improvement, current and future business requirements are met by constant monitoring and analyzing service delivery. Indeed, it also enables repetitive assessment of the present situation against business requirements and identifies the opportunities available for improving the provision of service to the customers.

Principles and Basic Concepts of the Seven-Step Improvement Process

Continual Service Improvements should center on increasing efficiency, maximizing the effectiveness, reducing the cost of service, and underlying IT service management. And the only way to accomplish the task is to ensure that the improvement opportunities are identified throughout the service lifecycle.

- The service providers operate in a very competitive market and they need to assess their services against the expectations in the market persistently.

- New delivery mechanisms such as cloud computing can increase the efficiency of the service and need to be considered for implementation.

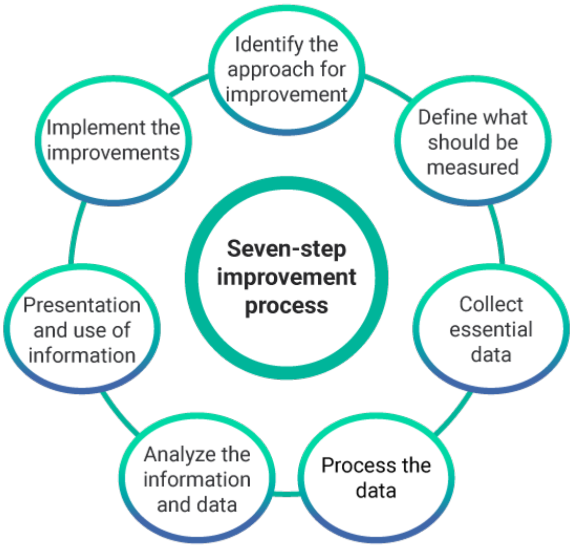
- The service provided must be compared to the present market offerings to ensure that the service adds actual business value to the clients, so that the service provider remains competitive.

- The services must be regularly reviewed to keep up with the latest technological advances to ensure that the services they are delivering are the most efficient.

Stages in the Seven-Step Improvement Process

The below mentioned seven steps constitute what is known as a knowledge spiral. The knowledge gathered from one level becomes the input to the other level. It moves from operational management to tactical management and finally strategic management.

Feedback from any stage of the service lifecycle can be used to identify improvement opportunities for any other stage of the lifecycle.


Identify the approach for improvement
Define what should be measured
Collect essential data
Process the data
Analyze the information and data
Presentation and use of information
Implement the improvements
Seven-step improvement process

{}

The stages in the 7 step improvement process are listed below:

1. **Identify the approach for improvement:** Prior to implementing an improvement strategy, it's necessary to understand the necessity for continuous improvement. We must take into account the final goals we have set for the business and see how the IT organization can assist in achieving those targets through continuous improvements. Whilst accomplishing this, consider future and present plans as well.

2. **Define what should be measured:** A comparison should be made amid what we can ideally measure and what we can actually measure. Gaps should be identified and a realistic measurement plan should be incorporated to support the strategy for improvement.
3. **Collect the essential data:** Data is gathered through persistent monitoring. The process of monitoring can be done either through manually or technology can be utilized to the fullest to automate the entire process and simplify it.
4. **Process the data:** Once the data is collected through continuous monitoring, it is then converted into the form required by the audience. This can be considered as a conversion of metrics into Key Performance Indicator (KPI) results and change the available data into information.
5. **Analyze the information and data:** The multiple sources of data are combined to transform the information into knowledge, which is further analyzed to find the gaps and their impact on the overall business. The information is further evaluated considering all the relevant internal and external factors. It also helps to answer questions regarding something that is good or bad and is it expected and in line with the targets.
6. **Proper presentation and utilization of information:** The information which is gathered and analyzed needs to be presented in a proper manner with the right amount of detail so that the information is comprehensible and provides the required amount of detail to support informed decision making.
7. **Implement the improvements:** A change implemented with continuous improvement sets a new baseline for the entire process. The knowledge obtained should be combined with the previous experience and are used to make informed decisions and necessary improvements. The improvements which are made must focus on optimizing and correcting the services, processes, and tools.

To conclude

The 7 step improvement process is a vital process of CSI and thus identifies the opportunities available for improving services, tools, processes, etc. The process initiates service measurement, service reporting, and improvement. This helps to define the service baseline and processes, metrics, KPIs, critical success factors, and corrective measures are taken to identify and improve the gaps in the IT service management.

ITIL CSI desires a commitment from the people working throughout the service lifecycle. It requires enduring attention to monitoring, analyzing, a well thought plan, and reporting results aiming towards improvement.