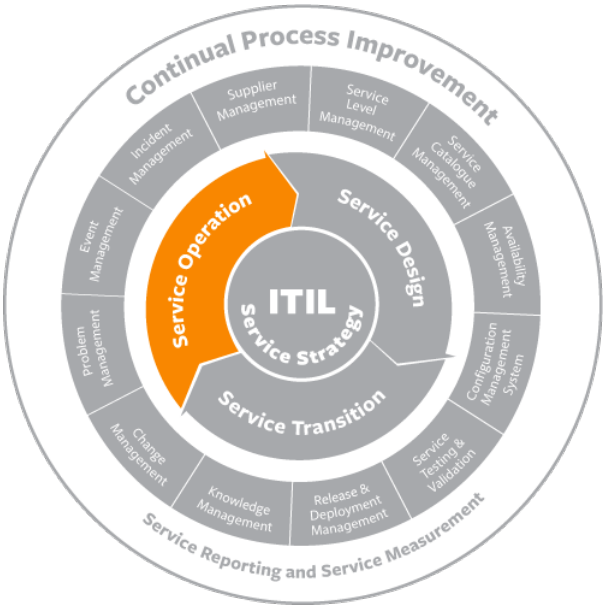
ITIL INCIDENT MANAGEMENT: AN INTRODUCTION

ITIL 4 Incident Management ›

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.

Download Now: ITIL 4 Best Practice e-Books

These all-new for 2020 ITIL e-books highlight important elements of ITIL 4 best practices. Quickly understand key changes and actionable concepts, written by ITIL 4 contributors.

Free Download ›

Free Download ›

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.

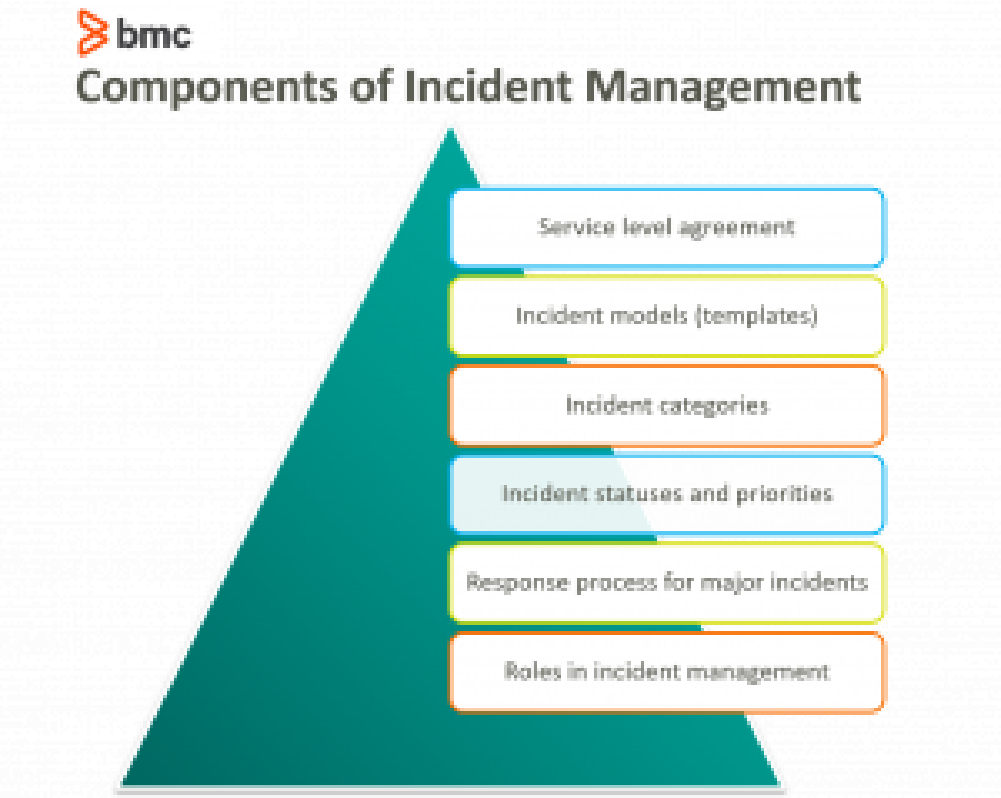
What is ITIL incident management?

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:



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.

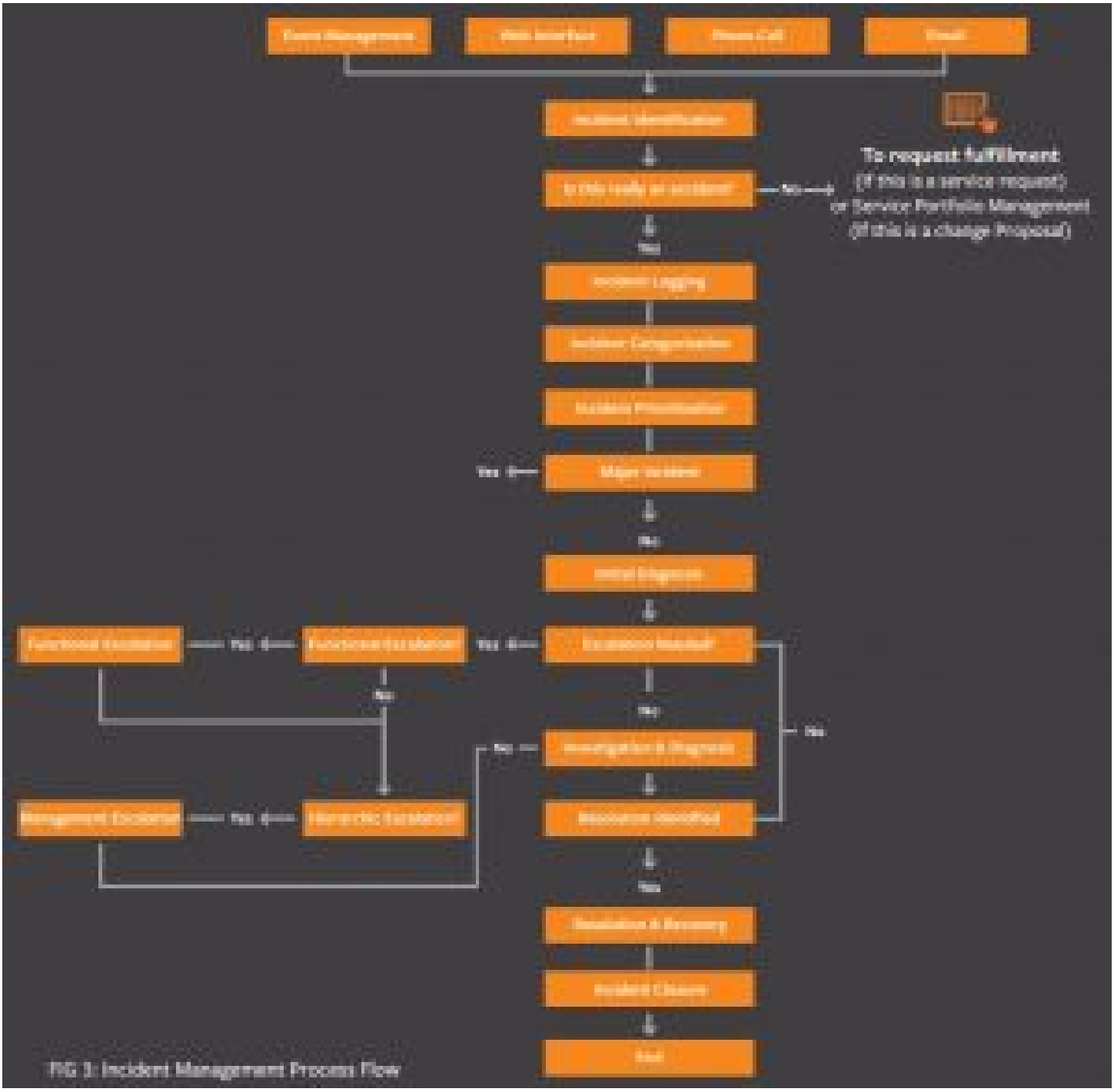


FIG 3: Incident Management Process Flow

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).