What is Incident Management?

Incident Management is an IT service management process intended to restore “normal” service operation as quickly as possible, minimizing any adverse impact on business operations or the user. Success is achieved by promptly and effectively dealing with all Incidents reported by users, discovered by technical staff or automatically detected by a monitoring solution. The IT Infrastructure Library (ITIL) defines an Incident as “an unplanned interruption that causes, may cause or reduces the quality of an IT Service.”

Common Incident Examples

Although there are endless reasons users contact the Service Desk for assistance, certain Incidents are common across every organization:

* Active Directory password reset
* Delete Active Directory account
* Error message when trying to launch or access an application
* Printer not printing
* Hardware – printer, fax, scanner, tablet not working
* Monitor flickering

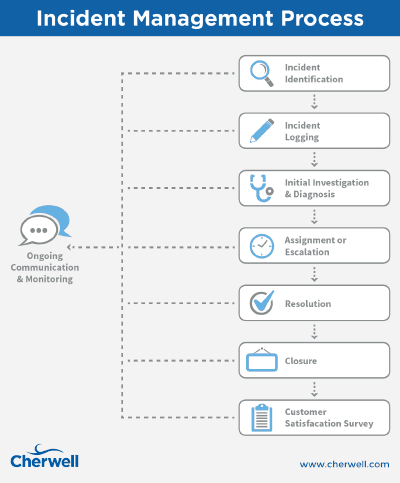
The Purpose and Importance of Incident Management

Each stage of the entire ITIL Service Lifecycle provides value to the business in one way or another. Service Operation delivers both long term incremental and short term ongoing improvements. The primary goal of the Incident Management process is to restore normal service operation as quickly as possible. When successfully implemented, Incident Management offers the following types of benefits:

* Reducing unplanned IT service staff costs by reducing the number of Incident tickets
* Decreasing business and user downtime with faster Incident detection and resolution
* Increasing productivity across the organization by restoring normal operation quickly
* Identifying training opportunities and potential service improvements
* Improving user satisfaction
* Demonstrating IT’s value to the business by aligning IT activities to business priorities
* Reducing the impact on the business and user with improved monitoring
* Reducing lost Incidents



[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)



The Incident Management Process  
(Also Known as the Incident Management Lifecycle)

How does Incident Management work? ITIL provides a framework, not a rigid set of instructions, for effective IT service delivery, adaptable by organizations to meet their IT service delivery needs. The Incident Management process can be structured to manage Incidents reported automatically by an event management tool, by users or service desk technicians via a self-service portal, over the telephone, email or in person. The Incident Management lifecycle includes:

1) Incident identification

Ideally Incidents are identified at a very early stage through automated event monitoring, even before it impacts a user. However, this isn’t always the case. Sometimes Incidents are identified by the impacted user reporting it to the service desk.

2) Incident logging

In order to maintain a complete historical record, all Incidents, regardless of the method used to identify and report them to the service desk, must be logged with all relevant details, including date/time, user information, description, related Configuration Item from the CMDB, associated Problem, resolution details and closure information.

* Incident classification – Once logged, all appropriate categories must be selected in order to properly assign, escalate and monitor frequencies and Incident trends.
* Incident prioritization – Assigning priority is critical in determining how, when and by whom the incident will be handled. Priority is based on the level of urgency – for example, the number of affected users or its impact on the business – and determines how quickly resolution is required.

3) Incident investigation and diagnosis

This step takes place immediately in order to determine the best course for correction. The technician may rely on the knowledge base, FAQs or known errors for diagnosis and/or resolution.

4) Incident assignment or escalation

Initially, the service desk technician attempts to resolve the Incident. However, if the service desk is unable to provide resolution, the Incident is escalated to the appropriate level of support, possibly involving either second- or third-level technical support staff who possess the skills to resolve the Incident.

5) Incident resolution

Once resolved, the solution can be implemented and tested to confirm service recovery.

6) Incident closure

Following confirmation that the Incident has been resolved, and the end-user is satisfied and in agreement, the Incident can be closed. The service desk technician should ensure that the initial classification details are accurate for future reference and reporting.

7) User satisfaction survey

A user satisfaction survey may be utilized to determine overall satisfaction with their service delivery. This is one of the most effective ways to build and maintain a positive relationship with your customers and users, especially if you pay close attention and implement improvements based on their feedback. There are several methods for gathering feedback, including after-call surveys, personal telephone surveys and, most commonly, the online survey.

There are a number of best practices one ideally follows when developing a user satisfaction survey:

* Explain the purpose of the survey
* Distribute the survey randomly for the most accurate results
* Keep it short, yet thorough
* Clearly state your questions
* Keep open-ended questions to a minimum
* Share survey results and the improvements you have made

\*\*\*Major Incidents – Occasionally, a major Incident will occur, causing serious interruption to important business services. These high impact and high urgency Incidents typically affect a large number of users and deprive the business of one or more critical services. In the case of a major Incident, a team will come together, placing the highest priority on restoring normal operation.

Each organization will develop their own criteria for identifying a major Incident, but characteristics include:

* Impacts a large number of customers
* Cost of downtime is substantial to customers and/or the business
* The time and effort involved in restoring normal operation is longer than agreed service levels

[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)

Inter-Related ITIL Processes

ITIL processes interface with one another throughout the service lifecycle. As mentioned earlier, an Incident is an unplanned disruption or reduction in quality of an IT service. Closely related are Problems, which are the unknown cause of one or more Incidents. Problem Management is designed to prevent or minimize the impact of Incidents by performing root cause analysis.

Occasionally, both terms are used interchangeably. A third term, Issue, may also be substituted, further adding to confusion surrounding the ITIL methodology.

Information to remember:

* An Incident can raise a Problem – If an Incident is reported and is likely to happen again, a Problem may be raised to identify and resolve the underlying root cause using the Change Management process.
* A Problem can cause an Incident – If a problem arises and is not resolved, an Incident, or multiple related Incidents, may be reported as a result.

The Role of Knowledge Management

Although the Knowledge Management process is associated with the Service Transition lifecycle stage, it is one that is executed across the entire lifecycle, especially during Service Operation. Knowledge Management can have a very strong impact during the Incident Management process. The Knowledge Management function is typically a feature within a larger IT service management technology solution. Its goal is to collect and share knowledge across the organization. This is especially important when service desk staff seek to quickly solve reported Incidents. Solutions within the knowledge base leverage existing knowledge to save time and lower the cost of service delivery.

Other Key ITIL Process Relationships

* Configuration Management
* Change Management
* Service Level Management
* Availability Management
* Capacity Management
* Event Management



[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)

Incident Management Roles and Responsibilities

Well defined roles and responsibilities are critical to the effective execution of the Incident Management process. The Incident Management team is comprised of the following:

Incident Manager

The Incident Manager has primary responsibility for driving and continually improving the Incident Management Process. In small- to mid-size organizations, this role is commonly assigned to the Service Desk Manager; in larger organizations, this may be a separately defined role. Key responsibilities include: team leadership, reporting key performance indicators (KPIs) back to management, direct management of first and second line support, managing the Incident Management system and enforcing the Incident Management process work flow.

First Line Support

First Line Service Desk Technicians are the single point of contact for end users seeking information and reporting service disruptions. They are primarily responsible for the initial support and classification of Incidents and the immediate attempt to restore a failed service as quickly as possible. If they are unable to resolve the Incident, the First Line Service Desk Technician will route the Incident to appropriate support personnel, monitor activity and keep users up to date on the status of their Incident.

Level Two Support

Second Line Support Technicians typically have more advanced knowledge than First Line Service Desk Technicians. They may become responsible for Incidents that First Line Support is unable to resolve. These technicians may interact with third party experts from software or hardware vendors to help restore normal service as quickly as possible.

[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)

Incident Management Key Performance Indicators (KPIs)

Measurements are important across all stages of the ITIL lifecycle. Each process has metrics that should be monitored and reported to effectively evaluate the overall performance. Continuous Service Improvement necessitates that the performance of each process be measured to identify areas needing improvement.

Typical Incident Management metrics include:

* Total Incidents reported (per category, priority, person, organizational unit, etc.)
* Status of Incidents
* Time between Incident creation and resolution
* Incidents and SLA (reached, breached)
* Average cost per Incident
* Reopen rate
* Incidents handled without escalation
* First call resolution
* Configuration Items experiencing recurring Incidents
* Incidents by time of day

KPIs should be related to Critical Success Factors (CSF) and CSFs should be related to objectives. This relationship helps with decision support for maintaining current state and improving to desired state. Although each organization is different, relevant reports for users, staff and management will help support important decisions that can be used to improve both the processes and the business as a whole.



[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)

Best Practices for Implementing Incident Management

Adopting the ITIL framework within a business can be a daunting task. As with any ITIL process, Incident Management implementation requires support from the business. Of particular importance is gaining buy-in from executives and upper management. Before beginning the adoption process, it’s important to have at least one person dedicated to the overall project management and orchestration of adherence to best practices for Incident Management. It is also extremely helpful to have an IT service management (ITSM) tool in place that will support your current state processes and desired future state processes, as well as a Service Desk acting as the primary interface with the IT department.

1) Understand the current Incident Management process

Occasionally an organization does not have a consistent process for handling incidents, or they have a less sophisticated one in place. Either way, it is important to map the existing process as well as possible in an effort to understand what the existing Service Desk process offers.

2) Identify long-term Incident Management process vision

It is also important to understand what the organization expects from the Incident Management process. The expectation may be based on generic Incident Management templates included with the ITSM tool or a more custom process based on the organization’s specific needs.

3) Conduct a gap analysis

Next, identify what must be adjusted between the organization’s current Incident Management process and its long-term vision for Incident Management. This will arm you with valuable information about the effort, time, money and resources necessary to achieve your Incident Management objectives and you overall service goals.

4) Create an implementation road map

Adopting any ITIL process will take time to develop, and you will need a road map to help set expectations for management. Use that road map to describe the activities, timeframe and efforts necessary to deliver. This roadmap should include quick wins, tool implementation, process changes, people and organization enablement, communication plans and overall governance changes.

5) Begin project implementation

It’s time for implementation to begin. Create a project plan that defines the actions or tasks, responsibilities and time line for completion of all tasks. Communicate the successes along the way as you achieve each milestone, demonstrating your progress towards your ultimate implementation goal.



[Back to Top](https://www.cherwell.com/products/it-service-management/itil-processes/essential-guide-to-itil-incident-management#Back-to-Top)

Conclusion

ITIL is a perfect way to help regulate the chaos that often exists within IT organizations, especially with rapidly changing technology needs and consumerized service expectations. Better service coordination and collaboration for effective and efficient use of organizational capabilities and resources are benefits of ITIL. ITIL does not provide organizations with an exact method for integrating processes into the business. It simply provides a structured framework, a guideline. Each organization is different and will adjust processes to fit their individual needs. ITIL provides templates to guide in the creation of categories, roles and metrics. These are not one-size-fits-all solutions, but rather a starting point that each business will customize and continually improve upon as they learn what works best, supporting the need to be more agile, demonstrate business value and maintain competitive advantage.