INCIDENT MANAGEMENT IN ITIL 4

Whenever the warranty aspects of a service (availability, capacity, security and/or continuity) are negatively impacted, we require actions to bring them back to agreed service levels in a timely manner that meets stakeholder expectations. These actions are encapsulate in the ITIL 4 practice of incident management. **The purpose of incident management is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible.** Incident management can have an enormous impact on customer and user satisfaction, and the perception of those stakeholders of the service provider.

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 ›

In ITIL, **we define an incident as unplanned interruption to a service or reduction in the quality of**

a service. Each incident should be logged and managed to ensure that it is resolved in a time that meets the expectations of the customer and user. Target resolution times should be agreed, documented, and communicated in advance to ensure that expectations are realistic when an incident occurs. Information about incidents should be stored in incident records in a suitable tool that allows correlation with other relevant service management information such as configuration items (CIs), problems, known errors and changes. This is vital to facilitate quick and efficient diagnosis and recovery. Tool capability may extend to incident matching and intelligent analysis which can generate recommendations for helping with future incidents.

After incidents are logged, they should be prioritized based on an agreed classification to ensure that incidents with the highest business impact are resolved first. Prioritization is an important consideration for the design of an organization's incident management practice, enabling it to align the appropriate levels of resource and management and resource to different types of incident. Low impact incidents must be managed efficiently to ensure that they do not consume too many resources, while high impact ones may require more resources and more complex management, particularly if they involve information security.

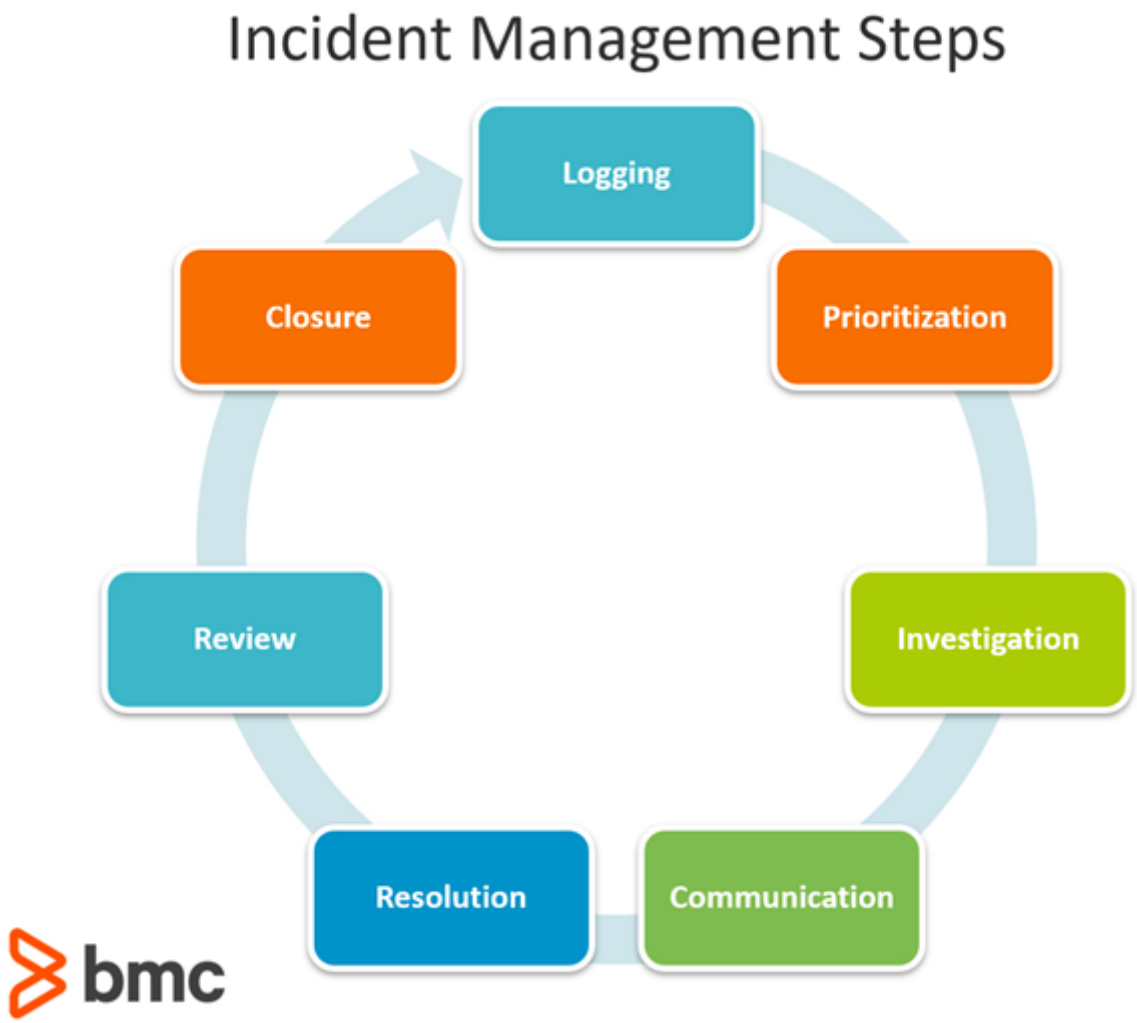

Figure 1: Incident Management Steps

The management of simple incidents should be optimized, through the use of knowledge, self-help, automation, and/or standard scripts for first-line agents. Investigation of more complicated incidents often requires knowledge and expertise, rather than procedural steps. Incidents may be diagnosed and resolved by people in many different groups, depending on the complexity of the issue or the incident type, so all of these groups need to understand the process, and how their contribution to

this helps to manage the value, outcomes, costs, and risks of the services provided. Hence, in a typical organization:

- Some incidents will be resolved by the users themselves, using self-help.
- Some incidents will be resolved by the service desk.
- More complex incidents will usually be escalated to a support team for resolution, or even suppliers and partners who offer support for products and services they provide.
- The most complex incidents, and all major incidents, often require a temporary team (including suppliers and users) to work together to identify the resolution.
- In some extreme cases, disaster recovery plans may be invoked to resolve an incident.

Effective incident management often requires a high level of collaboration within and between teams as this can facilitate information-sharing and learning, as well as helping to solve the incident more efficiently and effectively. There may also be a need for good collaboration tools so that people working on an incident can work together effectively. One technique that takes advantage of collaboration is termed **swarming**. This brings many different stakeholders together to work on the issue. Management of incidents may require frequent interaction with third party suppliers, and routine management of this aspect of supplier contracts is often part of the incident management practice.

It is important that people working on an incident provide good-quality updates in a timely fashion. These updates should include information about symptoms, business impact, CIs affected, actions completed, and actions planned. Each of these should have a timestamp and information about the people involved, so that the people involved or interested can be kept informed. Without adequate communication, users and other stakeholders may become frustrated, leading to overwhelmed service desk agents and dissatisfaction with overall service delivery.

(This article is part of our ITIL 4 Guide. Use the right-hand menu to navigate.)

Contribution of Incident Management to the Service Value Chain

Incident management is involved mainly in the ***engage***, and ***deliver and support*** value chain activities of the service value chain (but not ***plan***) as shown below:

Engage	Requires regular communication to understand the issues, set expectations, provide status updates, and agree that the issue has been resolved so the incident can be closed.
Design and Transition	Ensure incidents occurring in test environments, as well as during service release and deployment are resolved in a timely and controlled manner.
Obtain/Build	Ensure incidents occurring in development environments are resolved in a timely and controlled manner.
Deliver and Support	This value chain activity includes resolving incidents and problems.
Improve	Incident records are a key input to improvement activities, and are prioritized both in terms of incident frequency and severity.

ITIL® is a registered trade mark of AXELOS Limited. IT Infrastructure Library® is a registered trade mark of AXELOS Limited.