INCIDENT MANAGEMENT: A BEGINNER'S GUIDE

The increasingly ubiquitous nature of technology has resulted in our near dependence on it. Whether it be home, work, school, health, or civic needs, technology is involved. That's why we get so frustrated with any disruption from normal operation. Social media is awash with stories of systems not performing as they should: banking systems, healthcare portals, airline booking, online shopping, or even the social media platforms themselves.

For this reason, most relationships between any service provider and its customers are weighed heavily on whether the service provider can ensure minimal disruption. When the inevitable disruption does occur, you must manage the incident in a way that the consumer has agreed to tolerate.

Incident management is the formal name of this necessary business practice, and it's not one for companies to take lightly, no matter your industry. This article will get you started with the basics of incident management, then point you to more in-depth resources on the topic.

What is incident management?

When it comes to ensuring that operational services provide value to customers, incident management is among the most important disciplines. ITIL 4 defines an **incident** as an unplanned interruption to a service or reduction in the quality of a service.

Here are some examples of an incident in an online system:

- Users not being able to log in
- The system's lack of responsiveness to commands
- Perceived slowness compared to normal
- Corrupted or hacked data

Your company's ability to quickly address incidents is a key factor in user and customer satisfaction, your credibility, and the value you create in your relationships—which all make incident management a critical activity. Of course, not all incidents are visible to the end user but still require the attention of the service provider.

The purpose of the **incident management** practice is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible. Detecting, responding to, communicating, handling, and resolving incidents as quickly as possible is at the heart of good incident management. And that means having a clear understanding of what the customer agreed to or is willing to tolerate regarding the duration and handling of any particular incident. This is usually defined in service level agreements (SLAs) or contracts, which include timelines for responding and resolving incidents based on some criteria, usually priority as a function of impact and urgency.

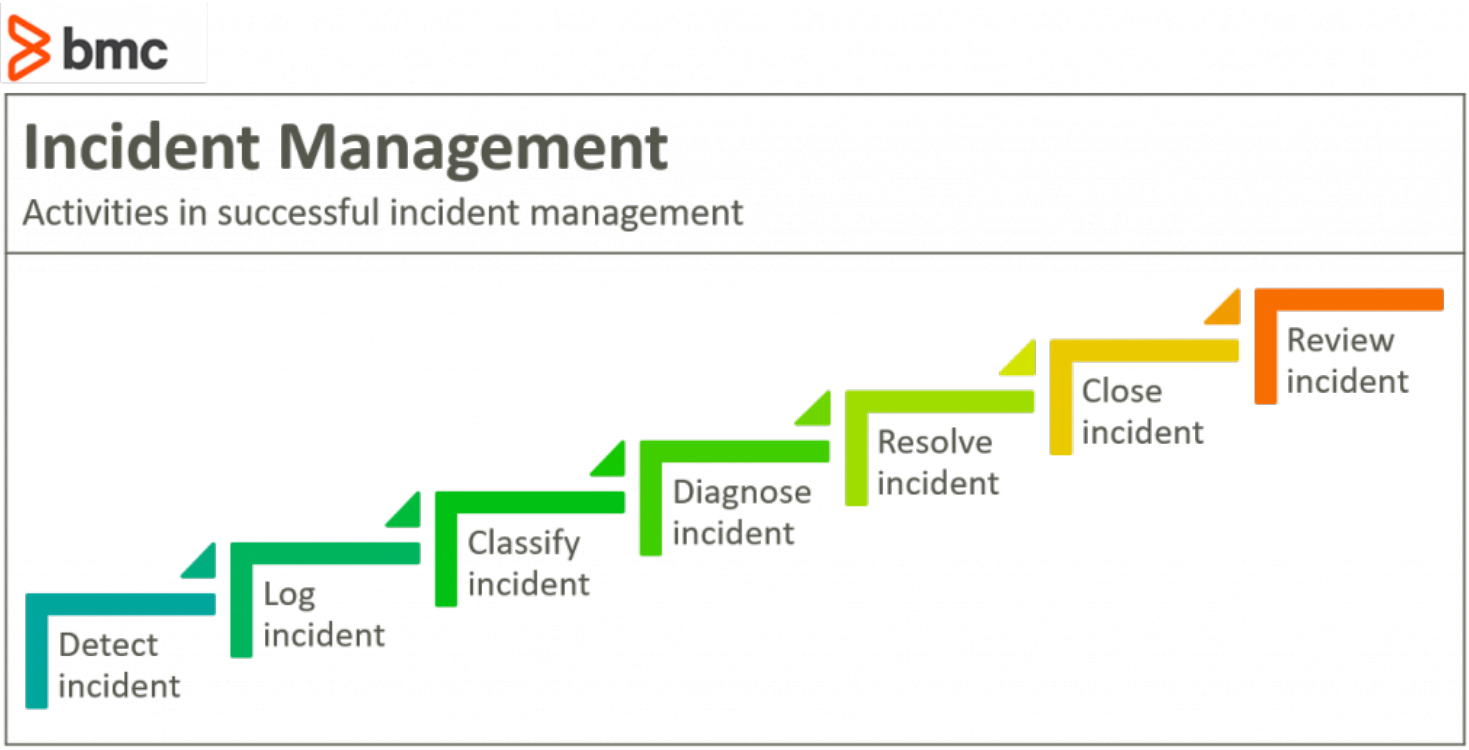
(Note that incident management focuses on how you handle an unplanned service interruption. It's different from problem management, which focuses on how you handle the problem in the future.)

How the service provider organizes themselves to handle different types of incidents is a major driver in your incident management execution. Some incidents may be repeatable, with their causes known. In these cases, you can define and use incident models for handling and resolution. An **incident model** is defined as a repeatable approach to managing a particular type of incident. Models help reduce resolution time as well as the learning curve for new service provider employees.

Where a solution to an incident is not easily found, a workaround may be applied to try and lessen the impact and/or probability of recurrence. Workarounds, such as restarts or reconfigurations, can quickly restore services back to an acceptable level of quality.

Incident management activities

In order to handle incidents in a way that meets the needs of customers and relevant stakeholders, your IT team will perform a variety of activities, generally in this order:



1.Detect the incident

Incident detection usually happens in one of two ways:

- A user reports a service issue and the service provider validates it as an incident.
- The service provider identifies an incident from alerts or trends from the components used to provide the service.

2.Log the incident

The service provider logs the incident. This should register it in a system for purposes of proper management, including assigning the right handler to the incident, and tracking the handling progress, particularly the timelines.

3.Classify the incident

In the incident classification phase, the service provider categorizes the incident in terms of:

- Type
- Impact, as in who and what is affected
- Urgency, or the speed required for resolution
- Priority, with regard to business and customer perspectives

Classification is useful for accelerating the process of identifying who should handle the incident, what model, if any, is best suited, and whether existing workarounds can be used.

4.Diagnose the incident

During incident diagnosis, the service provider investigates in order to (a) identify what has gone wrong and (b) determine the fastest way to recover normal service.

Diagnosis can be done by one person (handler) where the symptoms relate to a previously known and documented incident. But, for more complex and/or relatively new incidents, a team of cross-functional representatives, known as a swarm, may conduct a joint investigation. Diagnosis may result in an update to the classification of the incident.

5.Resolve the incident

Incident resolution refers to when the solution is applied—be it a workaround or a permanent fix. Resolution can take one or several forms:

- Implemented automatically
- Documented for the end user to apply it by themselves
- Handled by the support team
- Forwarded to a more skilled unit or even the vendor

Depending on the length of time the incident is taking and its classification, communication with affected users and stakeholders must be carried out in parallel, informing them of status and timelines. Fallback to diagnosis or triggering of disaster recovery plans may be required if resolution efforts are not bearing fruit at the required speed.

6.Close the incident

Once the incident is resolved, formal incident closure of the record takes place. Closure might require communication and confirmation from users that service experience is normalized, billing of handling activities, and configuration information updating where required.

7.Review the incident

During the incident review, sometimes known as an incident postmortem, the process owners or management may review how the incident was handles to determine what was done right and what went wrong. Both can be useful in future incidents and illustrating what activities might need to be changed or reinforced.

Review can usher in process activities from other ITM practices such as problem management, service level management, information security management, release and deployment management, service design, and change management, among others.

Successful incident management: factors and tips

Speed is the name of the game when it comes to incident management. Customers, users, and stakeholders all want normal services to resume as quickly as possible, with the impact of the incident and its repeat probability minimized as much as possible.

For the most successful incident management, consider how your organization is set up for these factors:

- Detecting incidents early—and *before* customer impact
- Responding to and resolving incidents as quickly as possible
- Central managing of incident information in order to communicate, collaborate, and measure the incident response

- Ownership and coordination of incident handling activities
- Continual improving on all elements of incident management

There are many moving parts involved in incident management. Therefore, it is imperative that you apply a rigorous approach across all process activities, ensuring that service value and customer perception is not eroded by mishandling or poor coordination. At the same time, continual review and analysis of incident management activities will ensure that a cost-effective approach, which maximizes on the service provider's capabilities, is maintained progressively.

Additional resources

To dive deeper on incident management, check out these additional BMC Blogs:

- How To Map the Incident Management Process
- Five Ways to Improve Incident Management with Decision Support
- Introduction to Critical Incident Response Time (CIRT): A Better Way to Measure Performance
- Digital Forensics and Incident Response (DFIR): An Introduction