Incident Management vs Problem Management: What’s The Difference?

ITIL (Information Technology Infrastructure Library) is a detailed set of IT service management practices that focuses on providing a framework of best practices for organizations. While ITIL has been around since the 1980s, there is still a lot of confusion about the difference between incident management and problem management, as well as where one stops and the other begins. (Find out more about ITIL here.)

Confusion between two terms and definitions wouldn’t normally be such a big deal, but not being familiar with the differences between these two processes can end up having a huge negative impact on both your infrastructure and, your business as a whole.
BMC Helix - The Future of Service and Operations Management

**BMC Helix** is the first and only end-to-end service and operations platform that’s integrated with 360-degree intelligence. Built for the cloud, this reimagined service and operations experience is unrivaled, giving you:

- **BMC Helix ITSM** optimized for ITIL® 4
- Enterprise-wide service including IT, HR, Facilities, and Procurement
- An omni-channel experience across Slack, Chatbot, Skype, and more
- Automation with conversational bots and RPA bots
- More than 7,500 IT organizations trust BMC ITSM solutions. [See why and learn more about BMC Helix >](#)

What is an Incident?

According to ITIL, “an incident is an unplanned interruption to a service, or the failure of a component of a service that hasn’t yet impacted service”. In order to be considered an incident, it must cause a disruption in service – and it has to be unplanned. Scheduled maintenance and servers that are only used during the day crashing after-hours, then, are not categorized as incidents, as they do not directly interrupt
the business process. Incidents need to be resolved immediately, whether it is by a permanent fix, a workaround, or a temporary fix.

**What is a Problem?**

Also according to ITIL, “a problem is a cause of one or more incidents”. This problem is initially unknown and results from a number of incidents that are related and have common issues. While problems are not classified as incidents, incidents can raise problems, especially if they may or do happen repeatedly. To refer to our above example, the situation of the server that is only used during the day crashing after office hours is a problem because although it isn’t currently causing a disruption in service, it could happen again and become an incident.

**What is Incident Management?**

The main goal of incident management is to resolve the disruption as soon as possible in order to restore service operations. Due to the fact that even minor disruptions in service can have a huge impact on the organization, it is necessary to fix incidents immediately. The process of incident management usually includes recording the details of the incident and resolving it.

Incident management often involves level one supports, which include:

- 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

What is Problem Management?

The goal of problem management is to identify the root cause of the incidents and try to prevent them from happening again. It might take multiple incidents before problem management can have enough data to analyze what is going wrong, but if undertaken correctly, it will help the problem become a “known error” and steps can be put in place to correct it. While incidents like a malfunctioning mouse may not result in a problem, those like repeated network outages need to be investigated.

Sometimes problem management is referred to as a reactive process that begins only after incidents have occurred. In actuality, problem management should be thought of as a proactive process because its end goal is to identify the problem, fix it, and prevent it from ever happening again. So, you could say the main goal of problem management is to identify the problem, troubleshoot it, document the issue (as well as the causes of it), and then ultimately resolve it.

Problem management has a very limited scope and includes the following activities:

- Problem detection
- Problem logging
- Problem categorization
- Problem prioritization
- Problem investigation and diagnosis
- Creating a known error record
- Problem resolution and closure
- Major problem review

To bring it all together, let’s look at an analogy comparing
The Firefighter and the Detective

Incident management is like a firefighter at a house fire: it swoops in, immediately fixes the problem, and saves the day. Firefighters come to the scene and notice the issue, and work fast to put out the fire as quickly as possible without stopping to question how it started. This is a similar situation to incident management. While it is necessary for incident management to provide fast results and repair issues within the infrastructure, it doesn’t help us find out what ultimately went wrong and why there was an issue in the first place. That’s where problem management comes in.

Problem management is like the detective that comes into the picture after the fact. They weren’t there to put out the flames themselves, but they can still investigate what went wrong, figure out how the fire started, and help educate people to take preventative steps so something similar doesn’t happen again. Problem management is a vital piece of the puzzle, addressing the root cause of the incidents and proactively preventing them from repeating and potentially causing major issues in the future. Without taking time to review incidents and problem solve, they will just continue to happen and potentially increase in seriousness.

Each Process Deserves a Dedicated Manager

Understanding the difference between incident management and problem management, and having dedicated managers for each separate scenario, ensures that you are not just putting out fires all day. While immediately fixing problems in the infrastructure with incident management provides temporary relief, it will soon exhaust your resources and employees
without finding the root of the problem. Bringing in problem management helps to investigate the cause of the incident and puts steps in place so it doesn’t continue to occur. By having a specific manager or team for this process, you will be one step closer to decreasing the rate of incidents in your organization and preventing major outages and service disruptions.

Additional Resources