Incident Management: The Response Process

Most IT executives know that ITIL is the best practice standard for service desk performance. Few, however, understand how it impacts every service request that comes in and the infrastructure efficiency and end user productivity it provides.

TICKET CREATION

The issue is brought to the service desk by the end user via phone call, email, or web submission. The service desk agent opens a ticket to begin collecting incident information.

INITIAL TRIAGE

The agent collects basic information about the end user reporting the incident, then asks questions to identify the exact symptoms of the issue and the impact it is having on the user's work productivity.

ASSIGN SEVERITY

The incident ticket is assigned a severity level according to an ITIL-based prioritization matrix, including factors such as urgency and impact. This determines the length of time in which the incident will likely be resolved in accordance with service level agreement (SLA) guidelines.
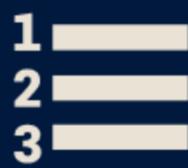
DIAGNOSTIC

The agent analyzes the incident symptoms and troubleshoots the issue until the most likely cause is determined, and whether or not that cause can be fixed at first contact. The diagnostic also helps determine if the issue is indicative of a larger problem (see below).

RESOLUTION

Using industry expertise and knowledge base documents, the agent resolves the incident and records the details of resolution. If the diagnostic has indicated the incident cannot be fixed at first contact, the issue is escalated to higher-level teams until resolved. Data is analyzed to determine how similar incidents can be resolved efficiently in the future.

BONUS: PROBLEM MANAGEMENT

The appearance of several similar incidents in a short amount of time indicates a possible *problem*. In that case, a *root cause analysis* is performed to find the direct cause for these incidents and address it, both solving current issues and preventing future incidents that would be due to that cause.