

INTRODUCTION TO IT EVENT MANAGEMENT



In ITIL, it's a piece of the IT infrastructure management strategy. It includes monitoring, investigating, escalating and responding to events that occur on the IT platform. Event management includes incident management, which is important to enterprise operation and information [security](#) puzzle.

At its most basic unit, an event is a piece of data that offers important insight about state changes that occur on the IT infrastructure to a manager.

This data has a few critical objectives:

- Allows IT managers to detect, interpret and respond to events with required actions
- Provides centralization of event management duties via event hub
- Provides a notification system that supports automating critical tasks

In this article, we'll introduce IT event management to give you a better idea of why your organization needs it.

Incidents or Events?

When it comes to incident management, a critical duty of event managers, it's important to understand the differences between an event and an incident.

An event is any state change that occurs in the IT infrastructure. A new user log-in? That's a state change. A transaction? That's a change of state, too. Any number of things can trigger an event to be

logged.

However, when an event is logged because of a potential problem in the system, that's an incident. If there's a network outage? That's an incident. A decline in service quality? That's an incident, too. Because of the serious nature of incidents, they often require immediate action, whereas some events may not require a response at all.

In a [previous post](#), we outlined that ITIL events are generally characterized by a few common traits:

- **Informative:** Informative events are often basic system updates telling of mundane state changes. They don't often require any real follow up.
- **Warnings:** Warnings provide information that lets the system manager know that something is amiss. This could be something like server capacity is almost full, or network bandwidth is lagging. These are important to respond to as they can impact service quality and information security.
- **Exceptions:** Exceptions tell the system manager that an event has occurred that's caused a problem. This is what you get when an entire server goes down, or another piece of the infrastructure isn't functioning as it should. These require immediate action.

IT system managers will need to designate what state changes trigger "informative events," as well as which ones trigger "warnings" and "exceptions."

IT Event Management Lifecycle

After defining what types of events exist within your enterprise IT infrastructure, it's good to understand what a typical lifecycle looks like for event management. In many cases, the lifecycle includes these key activities:

1. **An event has occurred:** Something in the infrastructure has shifted its state.
2. **A notification is generated:** Monitoring tools and configuration items play a large part in generating the event notification.
3. **An event is detected:** Usually an automated process, the event is detected by monitoring system, automated agent or systems management solution.
4. **An event has been logged:** In this step, the event is annotated in a system log.
5. **An event is filtered or correlated:** An automated event filtration system helps to determine if the event should be ignored or escalated. If it's escalated, it's through a process of correlating it with some kind of response required.
6. **An event is responded to:** Event response is logged, and it's determined if further action is required.
7. **An event is closed:** Once the lifecycle process is completed and all actions are logged, the event is closed.

You should expect to invest in tools and resources that help automate this process along the way.

Role of Configuration Management Database

Some organizations buy into the idea that a configuration management database (CMDB) is static and can't compete with today's IT demands. But that's a myth.

With the advent of automation, CMDBs have become more useful than ever in helping to control the

flow of information and data. They are so handy that savvy IT departments can use them within the ITIL framework to assist with event management. Here's how:

CMDBs help reduce the noise of automated alerts

In the event that an incident does occur and system failure is the result, your enterprise IT infrastructure sends a number of alerts that flood your event management notifications. A CMDB can offer certain visibility in areas that help managers reduce the IT noise created by notification, like hierarchies and parent relationships within data sets.

They offer prioritization assistance

With greater visibility, managers can prioritize events. Even after noise reduction occurs, there will still often be a ton of events and choosing where to start can be overwhelming without a CMDB or other system to inform the process. Visibility into key insights, like what services are most affected by an outage, can offer prioritization assistance.

Predict service issues before they occur

CMDB's offer data that can help managers predict a problem before it happens and prevent it from occurring. Through internal mechanics, CMDBs can learn what sort of things trigger a problem and alert you to those areas of the infrastructure before it occurs.

There are many benefits to using a CMDB in conjunction with automation as part of your overall strategy for ITIL event management.

IT Event Management Challenges

There are a number of challenges that are typical for service managers to experience when implementing IT event management. A few common challenges are:

Event flood

Today's enterprise IT infrastructure requires businesses to have multiple connected systems to remain competitive. Also, it's not uncommon that a single data record will have multiple records associated with it and different relationships exist between records.

For this reason, when a system experiences a hiccup, it will usually trigger multiple notifications which create a lot of noise for IT systems managers to wade through. However, in a critical situation, the kind that's likely to trigger a bunch of alerts, there's no time to spend picking through the noise to find what you need to fix.

This is a challenge that IT service managers need to be able to overcome, whether using a CMDB, as described above or partnering with a company like BMC for their technology needs.

Data fidelity

The attrition of data fidelity can cause major issues for a company that relies on data points to trigger notifications. In any enterprise business, it's important for data to be clean, to have velocity, volume, and variety.

In a previous article, we [outlined a lifecycle process](#) for data to help IT systems managers perform their data duties accurately. It looks like this:

- Acquisition and capture: Data is recorded.
- Backup and recovery: Data is backed up.
- Management and maintenance: Data is monitored for quality and maintained.
- Retention or destruction: After a given period, data is re-evaluated for necessity.

Ensuring data quality is important to any event management process.

Recommended: Automate Event Management

There are a number of benefits to implementing ITIL IT event management with automation to your organization's enterprise infrastructure. Below we're going to cover a couple of the most relevant to your business:

Predictive decision making

With machine learning and automation, companies can begin to make decisions about their infrastructure based on predicted sequences of events and automate outcomes. This allows for fewer resources and an overall more seamless infrastructure.

Faster time to decision

By automatically filtering the noise, stakeholders and CIOs can make faster and better decisions about their enterprise infrastructure, the lifeline of any digital business.

Additionally, here are a few more reasons CIOs care about automated event management:

- **Downtime is expensive:** Costly downtime can be avoided through advances in machine learning and automation in IT event management.
- **Talent is scarce:** There's an IT talent shortage and event management helps keep resources focused on the most important tasks.
- **Business innovation is competitive:** In the world of digital businesses, it's important to stay ahead of the competition in service quality, and proper event management helps enterprises do that.

To avoid expensive downtime and make sure your business is running as seamlessly as the competition, it's important to make investments in event management ASAP. [Contact BMC today](#) as your partner in ITIL event management, or download this eBook: **ITIL Event Management Best Practices**.