

# BEST-PRACTICE RECOMMENDATIONS IT INCIDENT MANAGEMENT

Sun Services  
White Paper  
May 2007

## **Abstract**

When systems or processes fail, things can go wrong quickly. Portions of the world economy can stop, business processes can come to a grinding halt, and email and other communication can stop flowing. When these incidents happen, IT organizations need to manage each to a successful conclusion. Unfortunately, how well an IT organization manages incidents can become the metric for evaluating IT's overall performance. An effective incident management program allows the organization to efficiently collect incident information, prioritize incidents, and resolve them. Proactive incident management programs combine services, technology, processes, and information to minimize the impact of IT incidents on the organization. This paper outlines several best practices to help organizations become more effective and proactive in incident management.

## Contents

Why is incident management important? .....	1
What is incident management? .....	2
Challenges involved with incident management programs .....	2
The basics of incident management—reacting .....	3
Making incident management proactive .....	4
Conclusion .....	5

### Three simple rules for incident management

#### *Rule 1 – Incident management is critical to effective operations*

Incidents of all sizes have an impact on the business. Little incidents can add up and big incidents can stop your business.

#### *Rule 2 – Incident management is information management*

Incident management is all about information—information on the incident and information on how to restore service. Resources such as the SunSolve™ program can be your best tools in managing the chaos of incidents.

#### *Rule 3 – Incident management can be proactive*

While incident management may seem like constantly reacting to problems, it can be proactive. Automation and process integration are best practices in becoming proactive in incident management.

## Why is incident management important?

Incidents happen every day within IT systems and the challenge—besides the stress and anxiety they cause—is to deal with them effectively. While weak incident management can have negative business impacts, strong incident management can actually free valuable resources within an organization.

What would happen, for example, if the database for your company's billing system becomes corrupted, making it impossible to record revenue and send bills to customers? Weak response to this incident could mean losing millions of dollars of revenue, threatening the company's ability to keep its doors open.

While the benefits of a well-run incident management process are obvious in the situation above, there are many other areas where benefits are not so obvious—yet they are still important for your business. A more common incident might involve a line worker who is unable to access a key system required to perform his or her job. If the problem takes six hours to resolve, the company loses productivity. The loss of six hours for one person may not seem like much, but if this productivity loss is multiplied by thousands of incidents a year, the impact on the company can be staggering.

This is why a well-run incident management program can give valuable resources back to the organization. Forrester supports this assertion, noting that IT managers pointed to incident management as the most important element of the Information Technology Information Library (ITIL) process model for delivering IT services<sup>1</sup>.

## What is incident management?

For purposes of our discussion, an incident is *any event that is not part of the normal operation of an organization and causes a disruption of IT services*. Within this context, incident management is *the process to restore normal IT operations as quickly as possible to the organization while minimizing the impact within defined service levels*. It's important to note that incident management is about restoring service and not about resolving the underlying problem. So incident management's role is to react to incidents, but it becomes proactive when it integrates, aligns, and shares information closely with other areas of IT.

ITIL<sup>2</sup> and the International Standards Organization<sup>3</sup> (ISO) have defined best practices for incident management programs that generally span five core areas:

- Detection and recording
- Classification, prioritization, and tracking
- Investigation, escalation, and diagnosis
- Resolution and recovery
- Closure and communication

While every organization's incident management program is different, we believe it's important to consider these best practices when designing your processes and selecting the appropriate services and technology to support your operations.

## Challenges involved with incident management programs

On the surface, the elements of an incident management program may seem basic — and easy to implement. Unfortunately, all the tinkering, integration, and projects done in the name of “efficiency” can really complicate incident management. Some of the biggest culprits in today's incident management programs are:

- **Open networks** – As organizations collaborate more with customers and suppliers, IT systems and networks interconnect — creating more points of failure and external configuration dependencies.
- **Heterogeneous systems** – Organizations are buying and using every kind of server, operating system, and storage equipment they can find. In these heterogeneous environments, more opportunities arise for interoperability and configuration incidents.
- **Service-oriented architectures (SOAs)** – The foundations on which an SOA is built create a broad array of services that must interoperate for proper delivery of integrated services. An incident involving a key SOA component can create a tangled mess and be very difficult to resolve.

- **Changing source of incidents** – Over the past decade, hardware systems have become significantly more reliable while also becoming more integrated. As a result of both trends, incidents are more prone to be “soft” failures from configuration items or conflicts rather, than easily diagnosed hardware failures.

This new era of challenges requires IT organizations to pay special attention to the design and deployment of their incident management programs. These programs need to evolve and adapt as IT environments become more sophisticated. The rest of this paper will examine practical steps for enhancing the maturity of your incident management program.

## The basics of incident management—reacting

Because standards organizations such as ITIL, ISO, and COBIT<sup>4</sup> have written extensively on best practices for incident management, we will not go into those details here. Rather, we will highlight some rational steps you can take to improve your incident management program towards these best-practices goals.

- **React to the complaints** – In the most basic sense, incident management is about reacting to the complaints of users of IT service when things go wrong. To preserve order and ensure that IT can react to all of the incidents, some basic processes are needed. A common service desk should be the central point for receiving, recording, escalating, and managing all incidents based on a common process. While a common service desk and defined processes are a very rudimentary step, they lay the foundation for the way an organization deals with all incidents.
- **Organize the chaos with service-level agreements** – Once you can systematically collect incidents, IT will need a way to classify and prioritize user complaints. A prioritization and classification scheme defined by business requirements for IT service delivery is best. If your organization has formal service-level agreements between IT and the business, those can become the basis for prioritization and classification. If not, time spent with your business counterparts can greatly help to define how you prioritize incidents. Business alignment will help avoid conflicts and ensure that you are delivering IT services that support the organization.
- **Use standards** – Above, we referenced various control frameworks and standards bodies such as ITIL, ISO, and COBIT. All control frameworks pay particular attention to incident management and define a series of best practices. Adoption of these standards is a choice each organization will make, but their underlying tenets can benefit anyone. We highly recommend referencing these standards and understanding their best-practice recommendations. These best practices can help improve your processes and prepare your organization for implementation, in case you do decide to implement one of these frameworks.

## Making incident management proactive

While the job of an incident manager can be a thankless one, there is hope. An incident management program can become very proactive in its approach and play a key role in helping its organization minimize the overall business impact of IT incidents. The following points highlight some simple but powerful steps for becoming proactive in incident management:

- **Share information** – Giving the incident management process access to information greatly improves its capability to resolve incidents quickly and efficiently. Information stores such as change management databases and knowledge management systems play a key role. If you're reading this paper, you have access to a wealth of information in the SunSolve program that can dramatically increase your ability to manage incidents. SunSolve and other knowledge bases will identify known problems, recommend fixes and workarounds, and alert you to potential issues. Using these resources is a proactive step that you can take in managing incidents, and it is an ITIL-recommended best practice<sup>5</sup>.
- **Integrate with other IT processes** – Closely linking incident management processes with configuration and problem management<sup>6</sup> will improve your ability to share information and manage incidents proactively. Problem management processes allow your organization to eliminate the pesky root causes of incidents. Close ties to configuration management will allow potential configuration problems to be identified and resolved prior to the occurrence of incidents.
- **Automate** – Every IT organization should seek to automate processes whenever possible, and the incident management process is no exception. Automation is important because it minimizes processing errors, facilitates faster response times, and helps to ensure process compliance. There are countless options for automating the processes related to incident management, ranging from help-desk software for incident tracking to automated event alerts provided by hardware components. What is critical is selecting and using automation wisely. Buy and use the automation tools that make sense for your organization — those that help you manage incidents more efficiently and effectively.

## Conclusion

While incident management can be a thankless job, it's a core process that every IT staff needs to master. Incident management is the linchpin that connects the community of IT services users to the resources for resolving incidents that exist within IT shops. Incident management identifies, classifies, and manages the resolution of incidents while minimizing their impact to the business. This role is critical in ensuring that the impact of IT incidents on the business is managed effectively. And it offers the hope that future incidents can be mitigated as incident management programs become more proactive.

### Endnotes

- 1 Gledman, Chip, "Transitioning for Incident to Problem Management: Key Issues and Challenges," Forrester, 2006.
- 2 Best Practices for Service Support, ITIL - Office of Government Commerce, The Stationary Office, London, United Kingdom, 2000.
- 3 "Information Technology - Service Management Parts 1 & 2, ISO 20000," International Standards Organization, Geneva, Switzerland, 2005.
- 4 Control Objectives for Information and related Technology (COBIT) is a set of best practices for IT management created by the Information Systems Audit and Control Association and the IT Governance Institute.
- 5 Best Practices for Service Support, ITIL - Office of Government Commerce, The Stationary Office, London, United Kingdom, page 79, 2000.
- 6 ITIL indicates integration of incident management to configuration management and problem management as best practices for incident management programs. Per ITIL, problem management "seeks to get to the root cause of Incidents and then initiate action to improve or correct the situation." Configuration management "provides a logical model of the infrastructure or service by identifying, controlling, maintaining and verifying the versions of Configurations Items in existence."

