WHITE PAPER

EFFECTIVE INCIDENT AND PROBLEM MANAGEMENT IN THE DYNAMIC IT ENTERPRISE

By Venkatesh Pandian Rajagopalan

Abstract

This paper discusses effective IT services management (ITSM) processes, specifically the incident management processes, that were implemented by an energy utility client and a food processing client of Infosys. It aims to demonstrate how existing ITSM processes can be improved by relaying the best practices and tailored processes used by Infosys in such infrastructure projects. It also explains how we leveraged a proven problem management technique to prevent enterprise-wide outages and improve the mean time to resolve (MTTR) across the IT landscape. The practices outlined here can be applied to any ITSM framework used in IT operations like ITIL, DevOps, COBIT, etc.

Infosys®
Navigate your next

Introduction

One of our energy utility clients was experiencing at least two to four critical incidents (P1) and five to seven urgent incidents (P2) per week. They wanted to address the critical incidents quickly and effectively to ensure reliable infrastructure operations.

Infosys did an in-depth assessment and customization of the existing ITSM processes. Best practices were used across the project, yielding better outcomes. Incident management, problem management and change management were leveraged across the enterprise to improve day-to-day business operations. Enabling innovation across these processes can help clients avert major outages and minimize downtime of enterprise IT systems.

Effective ITSM incident management practices

Incident discovery and prioritization - Best practices

1. Ask the right questions

When any major incident is reported to the incident manager, it must be followed by robust and rapid decision making to determine if the incident is business-critical. At this initial outage stage, some key questions must be asked by the incident manager. These are:

- How severe is the Outage caused by the Incident?
- How many critical applications or business users are impacted?
- Are there any business-critical servers that are down?
- Is this a security incident that could have organization-wide impact?

These are some of the common questions to be asked during the initial phase. Although many incidents are often reported as 'critical', most do not qualify as critical incidents. It is up to the incident manager, the technical program manager or the application manager to validate that the incident in question is actually critical based on responses to the above questions. Once this is done, the incident will be treated as 'critical' and will follow the critical incident management process.

These questions are important to assure program owners that they are, in fact, dealing critical incidents and not provisioning resources for non-critical issues. Further, when critical issues do arise, response time is of paramount importance.

2. Plan ahead to save time

In preparation of critical incidents, it is recommended to have some key aspects integrated with the existing processes to improve critical incident MTTR. Enterprises can plan ahead through the following steps:

- Incident managers must have valuable enterprise operational data readily available. Pre-planning and documenting the Operations flow of the IT enterprise is an on-going exercise and needs to be done on a constant basis. This data can be very helpful to understand which direct and indirect elements are impacted by the incident.
- Any important data that is available at hand during the critical incident becomes valuable to solve the issue on time and quickly restore services
- The right decisions made during the discovery stage will help determine the correct resources, team and time that is needed to swiftly resolve the critical issue
- Business-critical applications, servers and business users that may disrupt services to the organization must be documented in Operations Handbook. The document should also map applications to their corresponding servers. In this way, if a specific server is down, users will know which applications may be impacted. Such documentation must be done on a weekly basis so that all new enterprise systems become part of the ITSM process

In some cases, the incident may appear to be a non-critical issue or outage. Here, the incident manager can downgrade the issue to a low priority incident that is either 'urgent' or 'expedited'. This prevents the enterprise IT team from diverting their focus.

Incident analysis and communication – Best practices

1. Communicate major incidents to stakeholders

When an incident is categorized as a business-critical one, all relevant stakeholders must be alerted within 15 to 30 minutes. By this time, incident managers may already be engaged in conference calls to commence the resolution phase of the Incident.

To achieve best results, we recommend using a standard and organization-approved incident communication template. The template should contain important information that explains the problem in brief. Such criteria should include:

- Date and time of the critical incident
- Events leading to the crisis
- The current status, which may change as relevant teams work on resolving the issue
- Steps taken until now by different teams in their attempt to contain the incident. This should be in reverse chronological order. The steps should be listed briefly, with minimal technical description, in a way that is understandable by all stakeholders
- List of all applications, servers, users, and groups affected
- Methodology of incident management communication
- A critical incident number, which in case of multiple critical tickets, is the first reported incident
- Contact section that contains the contacts of the primary incident manager, technical manager, application manager, and other senior managers

These eight sections should be presented in a table. The format should be saved for usage at any time.

Major Incident Communication		
Major incident summary		
Date and time of critical incident	Thursday, 01-JUN-2019 8:00 AM	
Events leading to the crisis		
Current status		
Steps taken (listed in descending order)		
Groups, locations and applications affected		
Methods used to communicate with clients/stakeholders	Email, pager Technical bridge/WEBEX details:	
Incident ticket number	**INC000000000**	
Emergency change order ticket number		
Contacts	**Incident manager**	**Phone number**
	Technical manager (from support team)	**Phone number**
	IT manager-in-charge	**Phone number**

Table 1: A major incident communication template

Once the initial communication of outage has been sent within 15-30 minutes of its occurrence, the person in charge should send periodic updates every hour until the problem is resolved. Depending on the criticality, these timelines can be revised according to the situation. One may have a leadership call for very critical outages, which would be outside of the Incident management call. The suggested methodology can be adapted by the Incident management or Operations management team.

It is always best to compose the communication email in a non-technical manner and explain the situation broadly. Stakeholders are from different units and they are interested only in the area of impact, high-level remediation steps, current status, and estimated time of arrival (ETA).

Incident remediation, resolution and closure – Best practices

While incident-related communication must be sent at intervals as the relevant technical teams work on solving the problem, it is also important to document all the steps or actions taken by various teams trying to resolve the problem. Each update must be appended in reverse chronological order to the 'steps taken' section. In this way, users will get a clear summary of the direction of problem resolution.

1. Resolving the Critical Incident -Enable vendors and external parties, as necessary. Provide New ETA.

The incident manager must play a proactive role in provisioning additional teams as required. In many cases, IT teams should reach out to product vendors. Incident managers along with the relevant technical team should facilitate the remediation discussion with any external parties or vendors. The faster this decision is made, the better equipped all teams are to address the issue.

At the outset of issue resolution, it is recommended to inform stakeholders that a solution has been identified and provide them with an updated ETA. If the root cause of the problem has been identified, it is better to inform users of the same so that they know what could have caused the issue. Sharing such information promptly will help improve adoption of the problem management practice. Further, the associated team will be careful in the future to avoid similar problems.

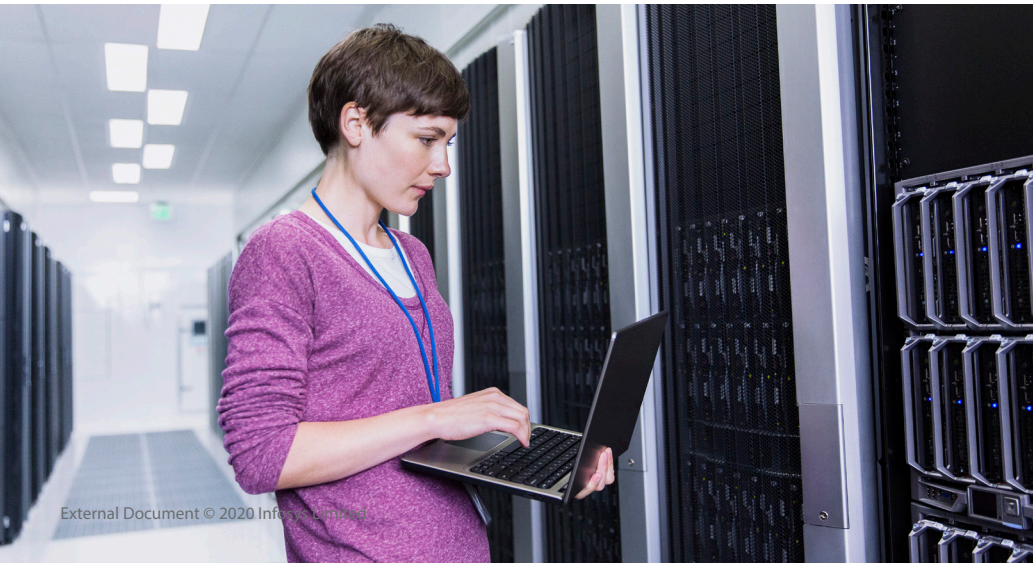
2. Closure of Critical Incident-Reaffirm the solution is working, Initiate problem management and "One last good Communication".

The incident manager or the technical manager must get validation results from different teams and impacted users. He should cross-check that all applications, systems and servers are responding properly. It is important to validate the solution across all the relevant areas. In many instances, the problem reappears after closing the ticket – a situation that must be avoided as much as possible.

The closing communication should summarize the issue and provide key information about the problem. This should include:

- Area where the problem was encountered and applications/systems impacted and restored
- Applications, systems, servers, and users that validated the solution
- The team(s) responsible for resolving the issue
- Remediation steps followed to resolve the issue now and what can be done in the future
- Problem ticket details. While this is optional, it is recommended to provide this detail along with the names of the owners of the problem ticket

Once the email on problem validation and closure summary is sent, all channels of communication related to the critical incident management process are closed. Following this, the problem management process begins.



Infosys recommends sending a daily report containing information about critical and urgent incidents to the IT enterprise team. All critical incidents resolved during the week as well as ongoing critical incidents should be included in the report.

Integrating incident and problem management as a part of ITSM strategy

The scope of proactiveness during incident management may be limited. However, there is always a wide scope of using problem management to achieve better results in the IT environment. For this reason, one of the most important aspects of the ITSM process is the problem management practice.

The more proactive the problem management, the more successful enterprises are in avoiding repeated critical outages to their IT systems.

Associating problem tickets with critical incidents (P1/P2)

Any critical incident in the IT landscape (all P1 and some P2 incidents) must have a problem ticket after the closure of the critical incident. In most ITSM tools, this functionality is integrated. In environments where it is not integrated, we strictly recommend integrating incident and problem tickets. Thus, for any P1 incident, a problem ticket is automatically generated by the system.

P2 incidents that may need problem tickets must be determined by the incident manager (or problem manager) along with the IT technical manager. A problem ticket is needed for a P2 incident in the following cases:

- When the P2 incident is repetitive
- When the P2 incident may escalate to a critical or P1 issue now or in the near future
- When the P2 incident is a result of a change ticket that was carried out in the recent past

Overview of the problem ticket process

The problem management process can be tailored to the unique needs of every enterprise.

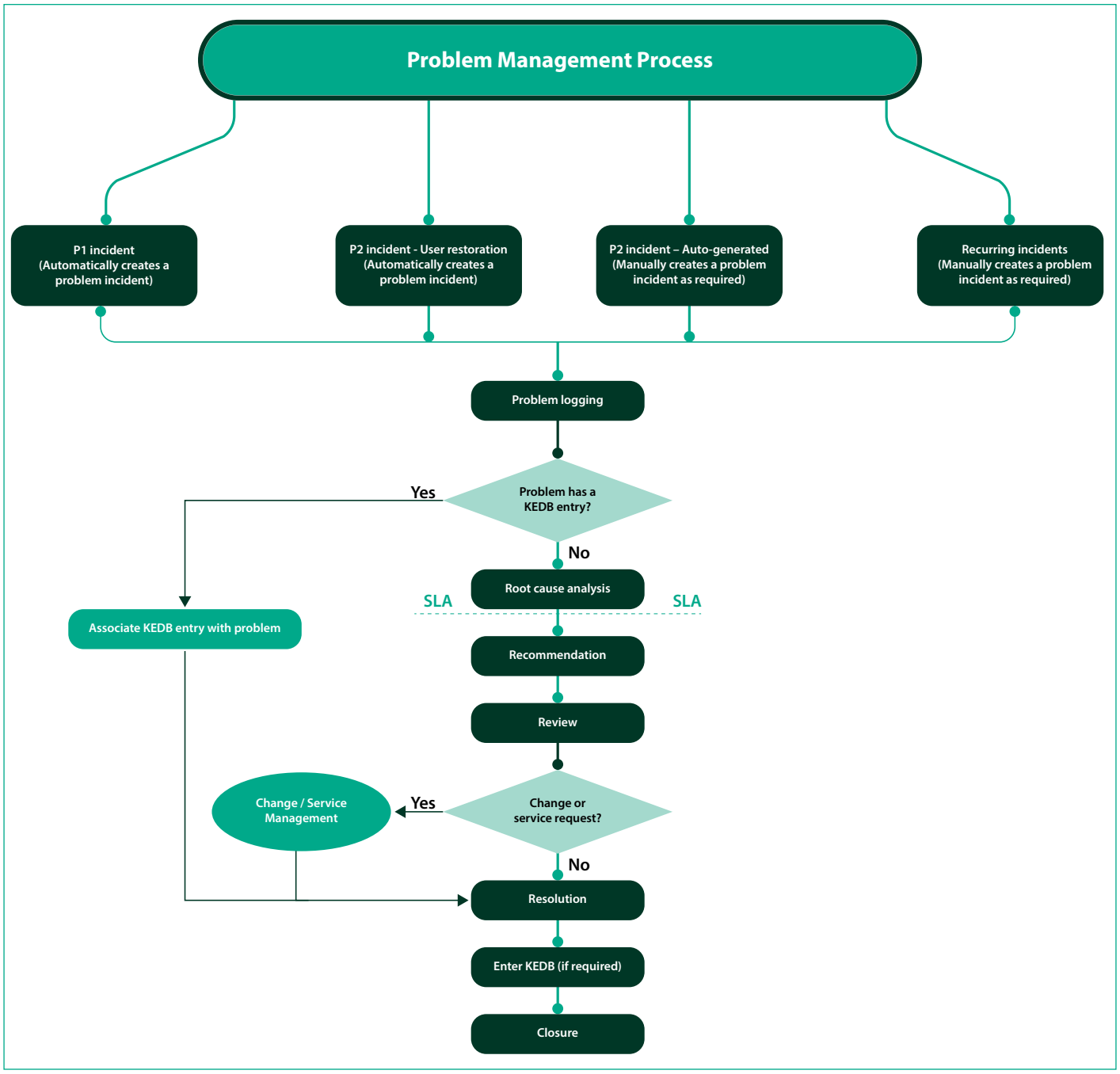
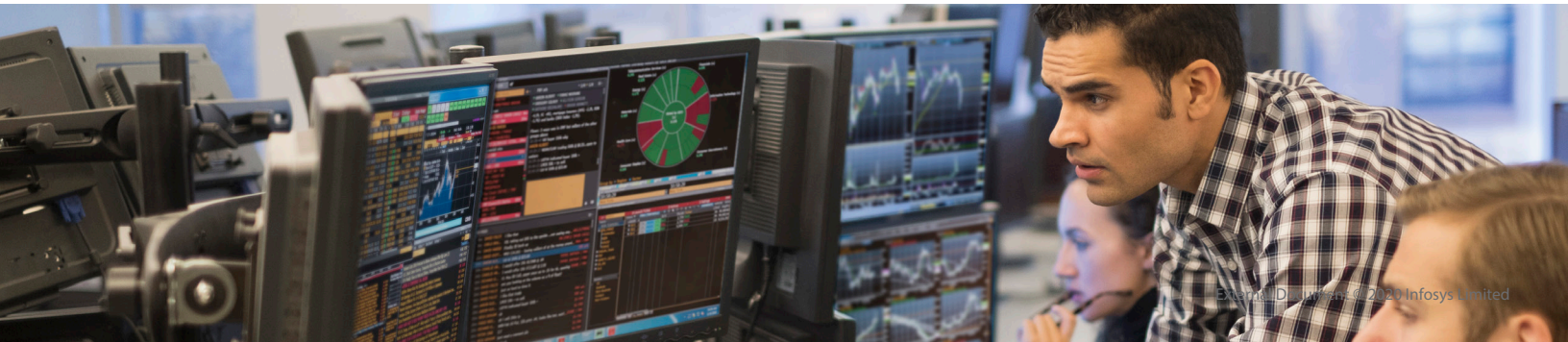


Fig 1: Overview of the problem management process

The problem manager or incident manager should consistently work with the service management team to enable new functions and automation in the ITSM tool. Depending on the organization's practices, the ITSM flow must be revised and integrated in the tool. Any automation or improvisation will increase the productivity of enterprise IT teams in a significant way.



Proactive problem management practices

The problem manager should step in after the closure of a critical incident. He should follow up with the problem ticket owner to actively drive the root cause analysis and close the problem ticket on time. Some of the most important responsibilities of the problem management practice are:

- Ascertain if every critical incident (P1 or P2) has a relevant problem ticket opened
- Identify the owner of the problem ticket. Sometimes, finding the owner of the root cause analysis process is challenging as there may have been multiple teams responsible for solving the critical incident. For example, application as well as infrastructure teams can collectively solve a critical incident
- Facilitate a meeting if the problem ticket has multiple owners and effectively assign the problem ticket to a single owner. Collaborate and follow-up with all the relevant teams until the problem ticket is closed
- If any IT change process is required as a part of root cause analysis (or problem ticket), coordinate with the change manager and the relevant technical team to deploy the change request in the next immediate change window. Try to associate the problem ticket/critical incident to the change request for a holistic view
- Follow up daily and weekly on the problem tickets and their owners until all the problem tickets are closed. Sometimes, a problem ticket will remain open days after the critical incident occurred. This may be due to a rift in the root cause analysis process, which can cause the critical incident to recur
- In case there is a delay in completing the root cause analysis and a temporary solution is found to resolve any similar critical incidents in the near future, these solutions must be included in the Known Error Database (KEDB)
- Publish weekly metrics of problem tickets to the enterprise operational team and relevant technical team. The healthier the metrics, the better equipped are the teams to ensure that the issue does not recur

Building the KEDB over a period will enable the IT enterprise to collect reusable solutions. Thus, many recurring problems can be resolved in a shorter turnaround time. This will also be useful for the helpdesk teams for IT operations.

There are many cases where the KEDB database is idle or obsolete even though the ITSM tool has a provision for such databases. It is up to the incident manager or the problem manager to drive this exercise along with the relevant IT teams. Gathering data about major incidents and root cause analyses and updating the KEDB can greatly benefit enterprises through more efficient and streamlined operations.

Conclusion

Incident management and problem management should be handled together in order to achieve best results in the ITSM model. In today's dynamic business environment, new features, functions and automation must be integrated with the ITSM workflows. While ITSM frameworks are designed to work efficiently, the processes must be periodically evaluated. Highly specific IT processes must be tailored to fit the existing ITSM model. This approach will alleviate process bottlenecks and improve the productivity of enterprise IT systems. Collaboration between different IT teams and stakeholders can significantly reduce the frequency of major incidents and amplify problem solving to minimize impact. Such process innovation can drive growth and enhance customer satisfaction.

About the Author

Venkatesh Pandian Rajagopalan
Lead Consultant, Infrastructure Management, Infosys

Venkatesh has 16+ years of experience in Application development & Maintenance, Infrastructure Systems and Operations, Database Administration and Project Management. He has also worked as a major Incident Manager and Problem Manager for various clients overseeing different technologies ranging from VMware servers, CITRIX, Linux, AIX, Databases, Network to Email servers etc. In addition to a bachelor's degree in Computer Science, Venkatesh is an IBM-certified IT specialist, IBM-certified Database Administrator and ITIL v3 foundation-certified.

For more information, contact askus@infosys.com

Infosys®
Navigate your next