Incident Management:
A CA IT Service Management Process Map

Peter Doherty — Senior Consultant, Technical Service, CA, Inc.
Peter Waterhouse — Director, Product Marketing, Business Service Optimization, CA Inc.
June 2006
Table of Contents

Introduction ..........................................................................................................................................................................................................3
Incident Management ..................................................................................................................................................................................4
  Event ..............................................................................................................................................................................................................4
  Detect ............................................................................................................................................................................................................4
  Record ............................................................................................................................................................................................................4
  Investigate and Diagnose ..........................................................................................................................................................................6
  Escalate..........................................................................................................................................................................................................6
  Resolve ..........................................................................................................................................................................................................7
Optimizing the Incident Management Journey .......................................................... .............................................................................7
Potential Issues with Incident Management............................................................... .............................................................................7
Summary................................................................................................................................................................................................................8
About the Authors .............................................................................................................................................................................................8
Introduction

CA's IT Service Management (ITSM) Process Maps provide a clear representation of the ITIL best practice framework. We use the analogy of subway or underground system transport maps to illustrate how best to navigate a journey of continuous IT service improvement. Each map details each ITIL process (track), the ITIL process activities (stations) that must be navigated to achieve ITIL process goals (your destination), and the integration points (junctions) that must be considered for process optimization.

CA has developed two maps (Service Support — Figure A; and Service Delivery — Figure B), since most ITSM discussions are focused around these two critical areas. The Service Support journey represents a journey of improving day-to-day IT service support processes that lay the operational foundation needed upon which to build business value. The Service Delivery journey is more transformational in nature and shows the processes that are needed to deliver quality IT services.

Close examination of the maps shows how a continuous improvement cycle has become a ‘circle’ or ‘central’ line, with each Plan-Do-Check-Act (P-D-C-A) improvement step becoming a process integration point or ‘junction’. These junctions serve as reference points when assessing process maturity, and as a means to consider the implications of implementing a process in isolation. Each of the ITIL processes are shown as ‘tracks’, and are located in a position most appropriate to how they support the goal of continuous improvement. Notice too, how major ITIL process activities become the ‘stations’ en-route towards a process destination or goal.

This paper is part of a series of 10 ITSM Process Map white papers. Each paper discusses how to navigate a particular ITIL process journey, reviewing each process activity that must be addressed in order to achieve process objectives. Along each journey careful attention is given to how technology plays a critical role in both integrating ITIL processes and automating ITIL process activities.
Incident Management

The objective of the Incident Management process is to return to a normal service level, as defined in a Service Level Agreement, as quickly as possible with minimum disruption to the business. Incident Management should also keep a record of incidents for reporting, and integrate with other processes to drive continuous improvement. ITIL® places great emphasis on the timely recording, classification, diagnosis, escalation and resolution of incidents. Within Incident Management the Service Desk plays a key function, acting as the first line of support and actively routing incidents to specialists and subject matter experts (SMEs). To be fully effective, the Service Desk has to work in unison with other supporting processes. For example, if a number of incidents are recorded at the same time, the Service Desk analyst needs sufficient information to prioritize each incident. Technology can be a key contributing factor by ranking incidents according to business impact and urgency. Today many tools enable the automatic recording of incidents within the Service Desk function, but lack the capabilities to correlate incidents and associate them with business service levels.

Let’s review the Incident Management process journey (see Figure 1), assessing each critical process activity (or station), and examine how technology can be applied to optimize the every stage of the journey, ensuring arrival at the process terminus — the efficient restoration of IT services.

**EVENT**

Incident Management starts with an event that, according to ITIL, isn’t not part of the standard operation of a service and which causes, or may cause an interruption or reduction in service quality. Incidents can include hardware and software errors, and user service requests which are typically not associated with IT infrastructure failures. Examples of service requests include functional questions or requests for information, or a request to have a user password reset.

**DETECT**

The first activity along the Incident Management process journey is the mechanism to detect incidents as they occur within the operational infrastructure and result in deviations from normal service. Users of IT services are the first to detect service deviations, yet with automated management, IT can rapidly detect incidents before they adversely affect end-users and IT services. In some cases IT can use process automation tools to detect errors before they affect IT service levels and to solve problems quickly before they impact the business.

**RECORD**

In most cases incidents will be recorded by a Service Desk function, which should record all incidents to ensure that compliance with service level agreements can be reported correctly. The location of an incident will determine who or what reports it. Naturally, users should have a facility to rapidly report incidents, supplying all information to the front line analyst, but a truly effective reporting function also should enable the system itself to automatically record incidents as they occur.

*Figure 1. Incident Management Process Line.*
Many Service Desk solutions provide self-help and knowledge-based capability, but even if users resolve the issue themselves, they should record the incident. This is important, since the IT function can proactively use an accurate base of recorded incidents to facilitate effective process improvements along other IT Service Management process lines. Also, giving end users the ability to log non-time critical incidents through a web-enabled interface combined with a knowledge management tool greatly reduces the number of calls made to the Service Desk.

Part of the Incident Management recording function should involve the effective classification (to determine incident category) and matching (to determine if a similar incident has occurred previously). Technology can help by providing front-line support with information pertaining to the configuration items (CI’s) supporting the end user who recorded the incident. During this phase Service Desk analysts review previous incident activity to understand the reason for the incident. The analyst should also have the means to correctly classify the incident using agreed coding criteria, identifying type of incident (e.g. IT Service=degraded), and the Service or CI affected (e.g. Order Entry Service). Many organizations mistakenly combine the IT Service / CI into the incident type. By doing so, they find that their incident classification methodology becomes far too complicated and people resort to incorrectly classifying incidents.

After classification, it is important to properly prioritize the incident. Service Desk solutions can help by automatically determining the priority based on the types of incident (e.g. IT Service=Outage), and the business services that are affected. The priority may also be determined by existing Service Level Agreements. After classification, the analyst should use incident matching to see whether a similar incident has occurred previously, and whether there is a solution, workaround or known error. If there is, then the investigation and diagnosis stages may be bypassed, and resolution and recovery procedures initiated.

If the incident has high priority and can’t be resolved immediately, the incident manager should create a linked problem record and initiate Problem Management process activities. Interestingly enough, Problem Management will have a different focus to Incident Management and could be in conflict. Incident Management should restore the IT service while Problem Management should determine a root cause and update the status to a known error. In the majority of cases where there is a conflict, Incident Management should take priority, since it is more critical to restore normal service levels, even with workarounds.

Before continuing along our Incident Management process journey, it is worth considering how the effective detection, recording and classification of incidents (achieved thus far) can facilitate an “optimum” journey along other ITIL process lines. In Figure 2 we can see that after the detection and recording activities, the Incident Management process arrives at a critical point — The Check junction. Incident Management outputs derived from the timely detection and accurate reporting of incidents provide the means to be more proactive and optimize the Problem Management process. For example, the accurate recording of all incidents will assist Problem Management with the rapid identification of underlying errors. Where justified, Problem Management will strive to permanently correct these errors, and reduce the amount of repeat incidents. Alternatively, the Check junction enables Incident Management to take inputs from Problem Management to further streamline the overall process. For example, by delivering information about known errors (from an integrated known error database) the “journey time” to the ultimate destination — service restoration — will be reduced dramatically. Naturally, technologies can play a key role, integrating both Incident and Problem Management within a single solution.
monitored, horizontal escalation can lead to incidents bouncing around the system without anyone taking ownership and the increased likelihood of breaching service level agreements. This is why it is so important to have a proactive approach and use process automation to correctly route incidents to the appropriate SME groups. Vertical escalation is where the incident needs to gain higher levels of priority. As part of the activity, it is essential that rules are clearly in place to ensure timely escalation, and avoid the need for support analysts to work out when to escalate — a recipe for disaster!

For every resolution attempt, accurate data must be attached to the incident detail to save repeating recovery procedures and lengthening overall resolution times. Technology can play another key role, automating the escalation process itself, and pinpointing the exact source of errors. This latter capability is important since it ensures the correct incident hand-off to appropriate SME groups early in the support cycle.

If no immediate solutions are available, then the Service Desk function needs to be able to route incidents to subject matter experts (SMEs). During the investigation and diagnosis phase, support analysts will collect updated incident details and analyze all related information (especially configuration details from a CMDB linked to the Service Desk).

During this phase, the support staff must access to comprehensive historical incident, problem and knowledge data, centralized and maintained within the Service Desk. Also critical is the capability to augment incident management records with diagnostic data supplied by SMEs or via integrated management technologies. The role of management technologies can play a key role here in correctly identifying and routing incidents to the appropriate SMEs. By its very nature, investigation and diagnosis of incidents is an iterative process, and may involve multiple Level 1, 2 and 3 SME groups as well as external vendors. This demands discipline and a rigorous approach to maintaining records, actions, workarounds and corresponding results. Integrated Service Desk technology can help in this process by providing:

- Flexible routing of Incident Management data according to geographic region, time etc.
- Automatic linkage and extraction of CMDB data for the examination of failed items.
- A strong knowledge base and tools to expedite the diagnostic function.
- Management dashboards and reports to provide an overall status of Incident Management.
- Controls to ensure process conformance and provide comprehensive audit logs.

Having conducted investigation and diagnosis, the Incident Management journey arrives at another station — Escalation. Critical here is the ability to rapidly escalate incidents according to agreed service levels and allocate more support services if necessary. Escalation can follow two paths; horizontal (functional) or vertical. Horizontal escalation is needed when the incident needs to be escalated to different SME groups better able to perform the Incident Management function. If not closely monitored, horizontal escalation can lead to incidents bouncing around the system without anyone taking ownership and the increased likelihood of breaching service level agreements. This is why it is so important to have a proactive approach and use process automation to correctly route incidents to the appropriate SME groups. Vertical escalation is where the incident needs to gain higher levels of priority. As part of the activity, it is essential that rules are clearly in place to ensure timely escalation, and avoid the need for support analysts to work out when to escalate — a recipe for disaster!

For every resolution attempt, accurate data must be attached to the incident detail to save repeating recovery procedures and lengthening overall resolution times. Technology can play another key role, automating the escalation process itself, and pinpointing the exact source of errors. This latter capability is important since it ensures the correct incident hand-off to appropriate SME groups early in the support cycle.

At this stage of the journey, the Incident Management process line has arrived at the ACT junction (see Figure 3). Here, iterative investigation and diagnosis will have determined the nature of the incident, and what actions need to be initiated to resolve the problem. Customer service must be restored as quickly as possible (through workarounds if necessary), and incidents should be escalated to Problem Management to detect the underlying cause of the problem, provide resolutions and prevent incidents from reoccurring.
The final stage along the Incident Management journey is Resolution and Recovery. Here the main activities include resolving the incident with solutions or workarounds obtained from previous activities. For some solutions, a Request for Change (RFC) will need to be submitted, so it is vital that technologies support the timely and accurate transference of incident details to a Change Management process. Once the solution is resolved by the SME groups, the incident is routed back to the Service Desk function, which confirms with initiator of the incident that the error has been rectified and that the incident can be closed. During this phase, integrated technologies must support a number of service improvement functions, such as providing restricted access to the incident closing function, and ensuring that incidents are matched to known errors or problem records.

Optimizing the Incident Management Journey

Since a primary role of Incident Management process is to ensure that users can get back to work as quickly as possible, activities should incorporate technologies that support the functions of recording, classification, routing to specialists, monitoring and resolution. Tools that help enhance the Incident Management process should at a minimum provide:

- Facilities to automate the detection, recording, tracking and monitoring of incidents.
- Capabilities to ensure the integration of an accurate CMDB that will help estimate the impact of incidents according to business priority. Integrated CMDB information also ensures the support analyst has access to accurate information during critical diagnosis and investigation phases of the Incident Management process.
- A comprehensive Knowledge Base (available to both users and support analysts) detailing how to recognize incidents, together with what solutions and workarounds are available.
- Strong workflow capability to streamline escalation procedures and ensure timely incident hand-offs between various support groups.
- Tight integration and proactive controls between supporting processes. For example, automatic logging of incidents during unapproved changes to configuration records.
- Mechanisms to report Key Performance Indicators on the Incident Management process. At a minimum, reports and service dashboards should be capable of providing the following information:
  - Total number of incidents.
  - Average incident resolution time (by Customer and Priority).
  - Incidents resolved with agreed Service Levels (by Customer and Priority).
  - Incidents resolved by front-line support or through access the knowledge base (with escalation and routing to subject matter experts).
  - Breakdown of incidents by classification, department, business service, etc.
  - Number of incidents resolved by analyst group / individual analyst / SME group, etc.

Potential Issues with Incident Management

The following is a list of issues to look out for to avoid problems in the Incident Management process:

- **Incident Management Bypass.** If users attempt to resolve incidents themselves, IT cannot gauge service levels and the number of errors. Technology can help by centralizing the Service Desk function — essentially acting as the clearing house for all incidents, and integrating Incident Management within a broader Incident, Problem, and Change and Configuration Management process. Incident Management bypass can also happen by informally approaching the SME groups for help. From a process perspective, however, the SME group should not take on the work until the incident has been logged in the Service Desk function.

- **Holding on to Incidents.** Some organizations mistakenly fuse Information Management and Problem Management into a hybrid Incident Management process. This is detrimental from the perspective of metrics and the ability to prioritize the problems properly. There should be a clear separation between the two processes, and incidents should be closed once the customer confirms that the error condition has gone away. Based on business rules the analyst can make the decision as to whether a related problem record should be created to look for a permanent solution.

- **Traffic Overload.** This occurs when there are an unexpected number of incidents. This may result in the incorrect recording of incidents leading to lengthier resolution times and degradation of overall service. Technology can help, by automating procedures to deploy spare capacity and resources.
• **Too many choices.** There is the temptation to classify incidents in finite detail and make the analyst navigate through many sub-levels to select the incident type. This increases the time it takes to create the incident and will often lead to the incorrect classification, as the analyst gives up searching for the most correct match.

• **Lack of a Service Catalog.** If IT services are not clearly defined, it becomes difficult to refuse to provide help. A Service Catalog can help by clearly defining IT services, the configuration components that support the service, together with agreed service levels.

**Summary**

The objective of Incident Management is to rapidly restore services in support of service level agreements. Unlike Problem Management, whose focus is on finding the root-cause of problems, Incident Management is essentially about getting things back up quickly, even if this means performing workarounds and quick fixes.

Technologies can play a critical role in optimizing this process, by automating the actual process activities themselves (such as incident recording and classification), and by accessing the outputs from other related processes. Integration with other processes (especially Problem, Change, Configuration and Service Level Management) is especially important to ensure that incidents are kept to a minimum and that the highest levels of availability and service are maintained.

**About the Authors**

Peter Doherty is a Senior Consultant with CA. He is a 15 year Service Management practitioner and holds a Manager’s Certificate in IT Service Management. A highly sought speaker for IT Service Management seminars and conferences, he won the President’s Award for best content and presented paper at the 2004 Australian itSMF National conference. Peter has published on the subject of IT Asset Management as an extension of ITIL and is a regular contributor to industry publications.

Peter Waterhouse is Director of Product Marketing in CA’s Business Service Optimization business unit. Peter has 15 years experience in Enterprise Systems Management, with specialization in IT Service Management, IT Governance and best practices.