

Incident Management: A CA IT Service Management Process Map

Peter Doherty

CA TECHNICAL SALES



Table of Contents

Executive Summary

SECTION 1: CHALLENGE **2**

Simplifying ITIL

How to Use the CA Service Management
Process Maps

SECTION 2: OPPORTUNITY **4**

Incident Management

Raise Incident — Event

Detect Event

Record

The Check Junction

Investigate and Diagnose

Escalate

The Act Junction

Resolve

Optimizing the Incident Management Journey

Avoiding Potential Incident Management Issues

SECTION 3: BENEFITS **10**

Benefits of Incident Management Best Practices

SECTION 4: CONCLUSIONS **11**

SECTION 5: ABOUT THE AUTHOR **11**

Executive Summary

Challenge

The Information Technology Infrastructure Library version 3 (ITIL® V3) process framework approaches IT Service Management (ITSM) from the lifecycle of a service. ITIL V3 best-practice guidelines across the five phases of the service lifecycle are complex and challenging to interpret. Moreover, they are not designed to provide definitive advice about implementing ITSM processes. Many IT organizations consequently undertake an ITIL journey without a firm idea of their goals and the path to achieve those goals.

Incident Management presents its own challenges as it is often the most visible customer facing process and it is generally enacted when things go wrong. This is why it is so important to be able to identify the business impact and apply resources appropriately.

Opportunity

ITIL places great emphasis on the timely recording, classification, diagnosis, escalation and resolution of incidents. The objective of the Incident Management process is to return IT services to a normal service level, as defined in a Service Level agreement, as quickly as possible and with minimum disruption to your business. Incident Management should also keep a record of incidents for reporting purposes and integrate with other processes to drive continuous improvement.

The Service Desk plays a key function within Incident Management, acting as the first line of support and actively routing incidents to specialists and subject matter experts. Incident Management is strongly linked to Problem Management, which is charged with determining the root cause of an incident.

CA has developed a unique approach to charting the ITIL journey through a visual representation of the ITIL framework and its interdependent ITSM processes in the form of a subway map. This map is an ideal starting point for understanding and communicating about ITIL and helps you to successfully plan and implement Incident Management programs.

Benefits

The CA ITSM process map for Incident Management enables your IT organization to support services and better align IT to the needs of your business. Following the Incident Management map provides:

- Timely resolution of incidents resulting in reduced business impact
- More efficient resource utilization of Service Desk and other staff
- Enhanced ability to measure and monitor IT performance relative to SLAs
- Better data to support executive decisions regarding service quality
- Proactive identification of process enhancements

CA ITSM Process Maps illustrate at a high level how best to navigate a journey of continual service improvement guided by strategic controls throughout the service lifecycle. Each map describes the relevant ITIL processes and activities you'll need to work with to reach your goals.

Simplifying ITIL

The ITIL V3 process framework focuses on the service lifecycle and the way that service management components are structured and linked. It embodies critical guidance for IT organizations that are seeking to improve service quality and align more closely with business goals to create value for their business and its customers.

But, the ITIL V3 best-practice guidelines across the five stages of the service lifecycle are complex and challenging to interpret. Moreover, they are not designed to provide definitive advice about implementing ITSM processes. Many IT organizations consequently undertake an ITIL journey without a firm idea of their goals and the path to achieve those goals.

CA has developed a unique approach to charting the ITIL journey through a visual representation of the ITIL framework and its interdependent ITSM processes in the form of a subway map. These maps present an easy-to-navigate, high-level view of the ITIL terrain. IT executives, strategists and implementers can use these ITSM process maps along with the family of CA ITSM Process Map Technology Briefs that expands on them. The maps and technology briefs provide a common reference point for understanding and communicating about ITIL and help you with program planning and implementation.

How to Use the CA IT Service Management Process Maps

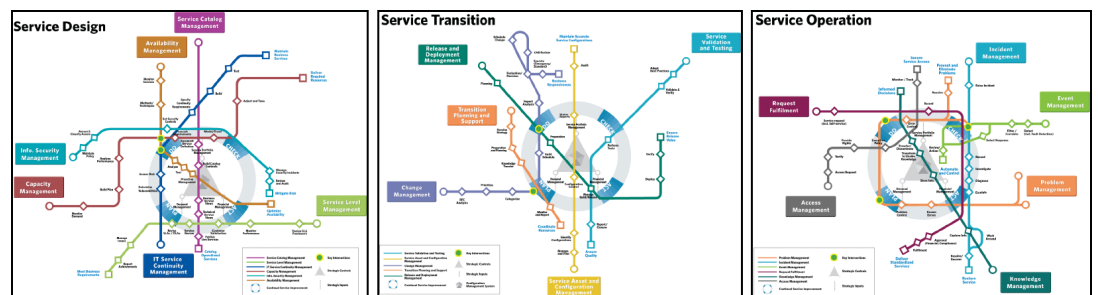
CA's ITSM Process Maps apply the analogy of subway system maps to illustrate how best to navigate a continual service improvement journey guided by strategic controls throughout the service lifecycle. Each map describes the relevant ITIL processes (tracks), the ITIL process activities (stations) that you'll need to navigate to achieve ITIL process goals (your destination), and the integration points (junctions) that you need to consider for process optimization.

CA has developed three maps (see Figure A) that portray the critical ITIL disciplines that most ITSM discussions focus on. They are: Service Design, Service Transition and Service Operation.

FIGURE A

The five critical ITIL phases of the service lifecycle: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement.

CA ITSM PROCESS MAPS

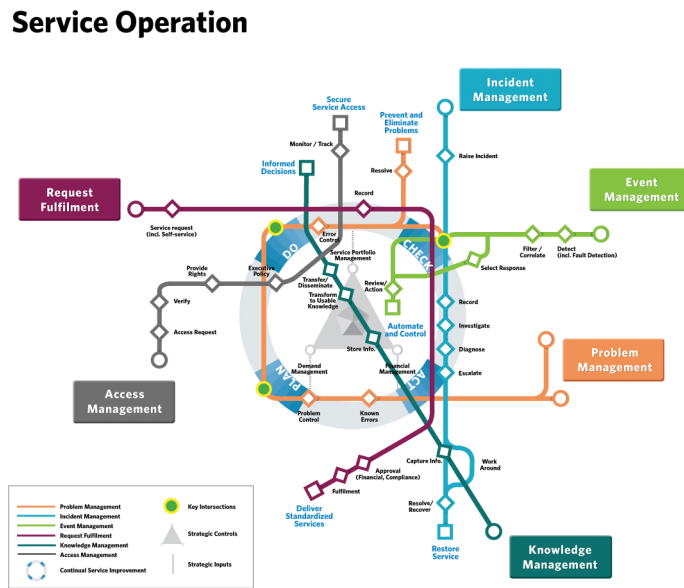


The Service Operations phase of the lifecycle, as shown by the CA ITSM Process map for Service Operation (Figure B), is typically where organizations have begun the ITIL journey — to simply address the complexities of “keeping the lights on.” Its role in the service lifecycle has far reaching impact, as its “tracks” are responsible for executing processes that optimize the cost and quality of services.

FIGURE B

The CA ITSM Process map for Service Operation visualizes the journey to improve day-to-day IT processes by providing essential service support to ensure continuous business operations.

SERVICE OPERATIONS MAP



This map depicts the major ITIL processes as the stations en route to an organizational process (destination) or goal. The ITIL process stations are served by tracks, which are positioned relative to one another to illustrate how they support the goal of continuous improvement. The ITIL continuous improvement cycle takes the form of a circle or central line, with each Plan-Do-Check-Act (P-D-C-A) step as a process integration point or junction on the line. Junctions serve both as reference points when assessing process maturity and as a means to consider the implications of implementing a process in isolation.

This paper is part of a series of ITSM Process Map Technology Briefs. Each technology brief explains how to navigate a particular ITIL process journey, reviewing each process activity that must be addressed to achieve process goals. Along each journey, careful attention is paid to how technology plays a critical role in both integrating ITIL processes and automating ITIL process activities.

Incident Management

ITIL places great emphasis on the timely handling of the processes required to prevent and resolve incidents. These processes include: logging, categorization, prioritization, investigation and diagnosis, escalation, resolution and recovery, and closure. The objective of the Incident Management process is to return IT services to a normal service level, as defined in a Service Level Agreement (SLA), as quickly as possible and with minimum disruption to your business. Incident Management should also keep a record of incidents for reporting purposes and integrate with other processes to drive continuous improvement.

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 categorize and 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 most IT organizations nevertheless lack the ability to correlate incidents and associate them with business service levels.

Let's review the Incident Management process line (see Figure B), assessing each critical process activity (or station), and examining how technology can be applied to optimize each station along the journey, ensuring arrival at the last stop on the track — the efficient restoration of IT services.

Raise Incident

The first station on the Incident Management journey is 'raise incident', which ITIL defines as an unplanned interruption or reduction in service quality to an IT service. Incidents can include hardware and software errors. Incidents can be created manually through methods such as email, a phone call to the Service Desk, an employee self-service web interface, and so on.

Incidents can also be created based on an event that is detected within the IT infrastructure. Users of IT services are often the first to detect service failures. However, with appropriate automation, IT can rapidly detect incidents before they adversely affect IT services, which is how users experience them (that is, from the viewpoint of the business). The goal is to detect events and solve the underlying incident quickly, before they affect your IT service levels or impact your business.

ITIL V3 has a separate Event Management process to help ensure that events can be correlated and remediated prior to a service failure occurring.

Record

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

While many tools are available to automatically record incidents, most IT organizations nevertheless lack the ability to correlate incidents and associate them with business service levels.

Many Service Desk solutions provide self-help and knowledge-based capabilities, but even if user's resolve the issue themselves, they should record the incident. It is important for the Service Desk function to proactively leverage an accurate base of recorded incidents to facilitate improvements in other ITIL processes. By giving users the ability to log incidents that are not time-critical through a web-enabled interface, combined with a knowledge management tool to provide self-service answers to questions will greatly reduce the number of calls made to the Service Desk.

Categorization

Categorizing the incident is part of the Incident Management record function. Effective categorization of incidents has two aspects:

- Classification to determine incident type (for example, IT Service=degraded)
- The Configuration Item (CI) that is affected

During this phase, Service Desk analysts need the means to correctly categorize the incident using appropriate, standardized coding criteria. Many organizations mistakenly combine the IT Service/CI into the incident type (hence we say that there are two aspects). As a result, the incident categorization methodology becomes far too complicated and a high percentage of incidents are incorrectly classified.

Prioritization

After classification, it is important to properly prioritize the incident. Service Desk solutions can help by automatically determining the priority based on the type of the incident (for example, IT Service=Outage), and the business services that are affected. You can also use current SLAs to help determine priority. 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 Service Desk function can bypass the investigation and diagnosis stages, and initiate resolution and recovery procedures.

If the incident has a high priority and cannot be resolved immediately, the incident manager should create a linked problem record and initiate the Problem Management process. It is interesting to note that Problem Management has a different focus from Incident Management, which can potentially result in conflicts. Incident Management is charged with restoring the IT service, while Problem Management is charged with determining a root cause and updating the status of the incident to a known error. In the majority of cases where there is a conflict, Incident Management should take priority since it is often more critical to restore normal service levels, even with workarounds, than to ferret out root causes.

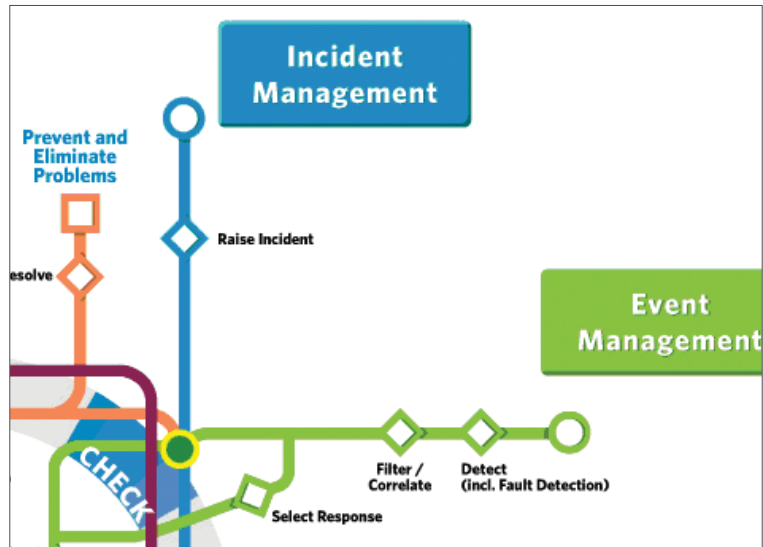
The Check Junction

Before continuing on our Incident Management track, 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. Figure C shows that, after the detection and recording stations we arrives at a critical point — the Check junction.

FIGURE C

The Check function looks at leveraging Problem Management and Known Error Information as well as proactively contributing to Problem Management from a trend perspective.

THE CHECK JUNCTION



The Check junction illustrates how 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, technology can play a key role, integrating both Incident and Problem Management within a single solution.

Investigate and Diagnose

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

While at this station, analysts must have access to comprehensive historical incident, problem and knowledge data that is centralized and maintained within the Service Desk. Also critical is the capability to augment incident management records with diagnostic data supplied by SMEs or using integrated management technologies. 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, and so on
- Automatic linkage and extraction of CMDB data for the examination of service failures
- 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

Escalate

Having conducted investigation and diagnosis, you arrive at the Escalate station. Critical here is the ability to rapidly escalate incidents according to agreed service levels and to allocate more support resources if necessary.

Escalation can follow two paths: horizontal (functional) or vertical. Horizontal escalation is required when the incident needs to be escalated to different SME groups that are 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, which in turn, increases the likelihood of breaching SLAs. 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 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, which lengthens overall resolution times. Here, technology can play yet another key role by automating the escalation process itself and pinpointing the exact source of errors. The former capability is important because it ensures the correct incident hand-off to appropriate SME groups early in the support cycle.

The Act Junction

At the Act junction (see Figure D), iterative investigation and diagnosis has determined the nature of the incident and the actions that need to be initiated to resolve the error. Service failures must be restored as quickly as possible (through workarounds if necessary), and incidents need to be escalated to Problem Management to detect the underlying cause of the problem, provide resolutions and prevent incidents from reoccurring.

FIGURE D

Performing the functions to improve service by interacting with Problem management.

THE ACT JUNCTION



Work Around

In some cases it will be possible to determine a workaround to the service failure and assist with temporarily resolving incidents associated to the error. In these cases where Problem Management has become involved, the Problem Record must remain open to firstly determine if the risk / impact justifies moving to root cause analysis and then continue on to find a permanent solution to the Problem. The Workaround needs to be documented in the Problem Record, a Known Error Record needs to be created, preferably in a Knowledge Base. During the analysis and Root Cause determination, an organization may find an actual resolution to a problem, but management may deem too costly to put a permanent fix in place. In these cases, the Workaround is the permanent fix the Problem Record denotes this status. In these cases you can continue to review these types of permanent fixes over time, in case the organization determines that more outages are occurring and downtime with the workaround is ineffective and more costly than the actual resolution to the problem.

Resolve and Recover

The final station is Resolve and Recover. 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 automation supports the timely and accurate transfer of incident details to the Change Management process. Once SMEs resolve the service failure, the incident is routed back to the Service Desk function, which confirms with the initiator of the incident that the error has been rectified and that the incident can be closed. While at this station, integrated processes 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.

Restore Service

The goal of the Incident Management process is to restore service. You must ensure that all information on the incident is properly captured, such as proper categorization and documentation, and record all details around the resolution of the incident. You will also want to periodically perform customer satisfaction surveys to ensure you are delivering high-quality services that meet or exceed customer expectations .

Optimizing the Incident Management Journey

Since the primary goal of the Incident Management process is to ensure that user's can get back to work as quickly as possible, activities should incorporate technologies that support the functions: logging, categorization, prioritization, investigation and diagnosis, escalation, resolution and recovery, and closure of incidents. Tools that help enhance the Incident Management process should provide:

- Features to automate the detection, recording, tracking and monitoring of incidents.
- Integrated CMDB information to ensure that the support analyst has access to accurate information during critical diagnosis and investigation to help estimate the impact of incidents according to business priority.
- A comprehensive and integrated Knowledge Base (available to both users and analysts) detailing how to recognize incidents, together with what solutions and workarounds are available, as well as access to Known Errors.
- 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.
- The ability to accumulate incident data for decision-making purposes, such as:
 - 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 to the Knowledge Base (with escalation and routing to subject matter experts)
 - Breakdown of incidents by classification, department, business service, and so on
 - Number of incidents resolved by analyst group, Individual analyst and SME group

Avoiding Potential Incident Management Issues

The following paragraphs describe some common issues for you to be conscious of in order to avoid problems in the Incident Management process.

BYPASSING INCIDENT MANAGEMENT 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 clearinghouse for all incidents — and integrating Incident Management within a broader Incident, Problem, Change and Configuration Management process. Incident Management bypass can also happen when users informally approach the SME groups for help. From a process perspective, however, the SME group should not take on the work until the Service Desk function has logged the incident.

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 detail and make the analyst navigate through many sublevels to select the incident type. This increases the time it takes to create the incident and often leads to the incorrect classification because 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 and the configuration components that support the service, together with agreed service levels.

SECTION 3: BENEFITS

Benefits of Incident Management Best Practices

The benefits of implementing an Incident Management process in line with ITIL best practices include:

- Timely resolution of incidents resulting in reduced business impact
- Improved user satisfaction
- More efficient utilization of Service Desk and other staff
- Enhanced ability to measure and monitor IT performance relative to SLAs
- Better data to support executive decisions regarding service quality
- Improved ability to track incidents and service requests efficiently
- Proactive identification of process enhancements

SECTION 4: CONCLUSIONS

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

Technology can play a critical role in optimizing the Incident Management 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 Management, Change Management, Configuration Management and Service Level Management) is vitally important to ensure that incidents are kept to a minimum and that the highest levels of availability and service are maintained.

SECTION 5

About the Author

Peter Doherty has nearly 25 years experience in the IT industry, predominately working in the Service Management arena as well as Enterprise Network and Systems Management.

During his early years, Peter was involved with the implementation of some of the largest System and Service Management systems in Australia. For the last 15 years, Peter has worked in consulting and project management roles with a heavy emphasis on Service Management Programs.

Peter is a regular presenter at international itSMF and Service Management conferences from both a plenary and SME perspective. He presented the Keynote at the inaugural itSMF Korea conference in 2005 and won the President's Award for best paper at the 2004 itSMF Australian conference..

Peter holds the Manager's Certificate in IT Service Management (with Distinction). He was a contributing author to the Service Operations book for the ITIL V3 refresh

To learn more about the CA ITIL solutions, visit ca.com/itil.

CA (NASDAQ: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP331991008

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

