

# Event Management: A CA Service Management Process Map

Nancy Hinich-Gualda

PRINCIPAL CONSULTANT

CA SERVICES



---

## Table of Contents

<b>Executive Summary</b>	<b>1</b>	SECTION 4: CONCLUSIONS	<b>10</b>
SECTION 1: CHALLENGE	<b>2</b>	SECTION 5: REFERENCES	<b>10</b>
<b>Simplifying ITIL</b>		ABOUT CA	<b>Back Cover</b>
How to Use the CA Service Management Process Maps			
SECTION 2: OPPORTUNITY	<b>4</b>		
<b>Event Management</b>			
Detect (Includes Fault Detection)			
Filtering and Correlation			
Select Response			
Review and Action			
SECTION 3: BENEFITS	<b>9</b>		
<b>Realizing the Benefits of Event Management</b>			

# Executive Summary

## Challenge

To achieve effectiveness and efficiency in the delivery of services (a struggle for many organizations), a formalized Event Management process helps contribute to controlled and repeatable operations. The goal of the Service Operation lifecycle is to effectively manage the technology used to deliver and support services which ensure value for the customer and for the provider of services. Strategic objectives can be realized thru service operations, therefore the proactive capabilities of Event Management are critical.

Organizations struggle with providing and managing well designed processes for the daily operation of IT services such as monitoring service performance, assessing metrics and gathering data to support service improvement initiatives and activities. Most organizations today are drowning in data, with little to no information relevant to managing operations, let alone proactive delivery of this information.

## Opportunity

Even though it wasn't until ITIL v3 that Event Management was specifically called out as a "process", most organizations have been monitoring service components and managing events for many years. As the world of IT has changed and become more complex, managing the enormous volume of events without understanding the critical business services can leave an organization vulnerable and at risk.

A sound and repeatable Event Management process provides an organization with the ability to quickly detect events, understand them, and then decide on an appropriate control activity or action to prevent an incident and/or service interruption from occurring. A key opportunity that Event Management provides is the ability for an organization to act in a proactive manner which increases operational efficiency and can reduce unnecessary cost due to preventable service disruptions.

CA has developed a unique approach to representing the ITIL framework and its interdependent IT Service Management processes across the service lifecycle at in the form of an easy-to-navigate process subway map. This map is an ideal starting point for understanding and communicating about ITIL and helps you to successfully plan and implement Service Operations processes, including Event Management.

## Benefits

When formally integrated with other Service Management processes such as Incident Management, Problem Management, Availability Management, Capacity Management and Service Level Management, Event Management can proactively signal expected or unexpected status changes allowing an organization to conduct early responses to improve overall performance.

Formally adopted good Event Management practices as outlined with CA's process map helps an organization realize the following benefits:

- Increased ability to conduct "proactive" incident and problem management with early detection of incidents and potential service interruptions
- Increased operational efficiencies
- Improved risk management capabilities
- Increased speed of impact analysis
- Better allocation of resources ready to respond to expected or unexpected state changes

SECTION 1: CHALLENGE

## 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.

*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.*

### How to Use the CA Service Management Process Maps

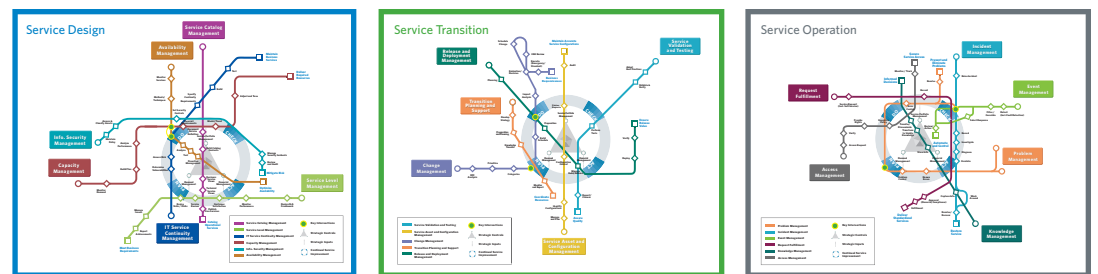
CA's Service Management process maps illustrate every process (or track), each activity (or station) and the key relationships that are relevant to navigating continuous IT service improvement. The ITIL quality cycle takes the form of a "circle" with each Plan-Do-Check-Act (P-D-C-A) step as a process integration point (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.

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

CA has developed three maps: Service Design, Service Transition and Service Operation since most ITSM discussions focus on these critical ITIL disciplines.

### SERVICE DESIGN, SERVICE TRANSITION, SERVICE OPERATIONS MAPS





## Event Management

A good repeatable Event Management process provides an organization with the ability to detect Events, understand them, and then decide on an appropriate control activity or action to prevent an incident and/or service interruption. Appropriate activities or actions can include an action to dismiss an event or to record an incident. Efficient service operations rely on the timely handling of the many activities required to prevent incidents and service outages.

An “event” as defined with the ITIL, can be considered an expected or unexpected change of state that could negatively impact service availability, service reliability and security. An event can also be triggered by an alert or notification created by an IT service, Configuration Item (CI), or monitoring tool based on business rules and referential data. Events typically require IT personnel to take action and often will lead to an incident record being created either manually or automatically. An “alert” is a warning that can be set up for notification that action may be required; basically it is a systematic message that demands attention for some reason. The alert could be an indication that a threshold has been reached or is about to be reached, something has changed either expectedly or unexpectedly or a failure has occurred. Alerts should be managed by an Event Management process because events sometimes lead to incidents which would then be managed by a controlled incident management process. There is a strong link between Event Management and incident management (as we saw in ITIL v2 where it was ‘assumed’ that events were part and parcel with incident management). As we can see in Figure C below, Event Management intersects almost immediately with Incident Management.

FIGURE C

Track illustrates where Incident and Event Management processes integrate.

PROCESS INTEGRATION WITH INCIDENT MANAGEMENT





This snapshot illustrates how Event Management activities are a critical input to the Incident Management process. Event Management outputs to Incident Management providing Incident Management with the timely detection of events. This in turn allows Incident Management to act proactively and optimize the Problem Management process (for more information on Incident Management, please refer to the Incident Management Technology Brief).

Because Event Management provides the ability to detect incidents early, an organization can configure technology to support an Event Management process to trigger an incident after it has been automatically detected and be automatically assigned to the appropriate resolver group for action before any actual service interruption or outage occurs. Using technology to support an Event Management process makes it possible for some activities to be monitored by exception which can help eliminate the need for expensive and resource intensive “real time monitoring”, while at the same time, reducing unavailability or down time.

Within Event Management there are several different types of events to manage which include:

**NORMAL OPERATION EVENTS** – these types of events can include an automatic notification that a scheduled workload job has completed as expected or a user has logged into an application that they had the right level of access to, or an email has reached an intended recipient. Normal operation events are important to monitor because they could represent a breach of policy or non compliance to a process.

**EXCEPTION EVENTS** – these types of events could include user attempts to access an application with an incorrect password too many times or, a device’s CPU is above an acceptable utilization rate or a PC scan reveals the installation of unauthorized software.

**UNUSUAL EVENTS** – these types of events usually represent something unexpected and require immediate attention such as a server memory utilization within 5% of the highest expected performance level, or the completion time of a transaction 10% longer than normal.

The key point with any of these event types is that immediate action should occur in order to either raise an incident record or a “dismiss and log” of the event for further monitoring and trending.


Before we move on to the key activities of an Event Management process as outlined by CA’s process map, there are several important inputs to the Event Management process and key outputs of the process. These are key activities for optimal efficiency and have the highest potential for automated support eliminating the need for intensive resources and manual support (meaning more room for human error and slowed response times).

Inputs to Event Management include:

- Event monitoring systems
- CMS (Configuration Management System)
- Identity and Access Management systems

When we look at a generic process model, we see that data enters a process (an input), that data is processed, and then that data becomes an output. Inputs to the Event Management process can include data gathered from an Event monitoring system where we configure technology to continually look at critical components that make up a service and tell us (or alert us) when something is expected or something is not expected and requires action.

*Many IT organizations spend too much time defining the service bottom-up i.e. concentrating on the technical and operational aspects of the service. SLM can enhance IT’s value to the business by gathering first the SLRs from the customer/ consumer and then working their way down to the technology. By mapping SLRs to SLAs and further down to existing/known technical and operational metrics (part of Operation Level Agreements – OLAs) the gap between the “is” and “to be” state becomes transparent and can be closed (top down design bottom up construction).*



Inputs to Event Management can also come from a Configuration Management System (CMS). Configuration Management delivers an organization a logical model of services, assets and the infrastructure by recording the relationships between Configuration Items (for more information on Configuration Management, please reference the Configuration Management technology brief). The CMS holds all of the information for CIs within a designated scope. The CMS maintains the relationships between all service components and any related service management records and documentation. A CMDB is a Configuration Management database that is used to manage configuration records throughout their lifecycle and keeps a record of the attributes and relationships of CIs. Thru verification and audit activities, a CI may be discovered missing or incorrect which is an event type and would follow the Event Management process.

We also see inputs to Event Management from security management or specifically identity and access management systems. This involves monitoring of user access to systems to ensure the right people are accessing only those systems or applications that they are entitled to. An organization would want to monitor user access and be alerted to any unexpected access attempts to the network or business critical systems to take immediate action to protect critical information.

Outputs of Event Management:

- Notified resources
- Incident records
- Updated log files

The main outputs from a process should be driven by the objectives of the process (in this case, to detect events, make sense of them, and determine the appropriate control action) and should always include process measurements, reports and process improvement. The outputs produced by a process should conform to operational norms that are derived from the business objectives.

The main outputs of the Event Management process include the right resources notified in a timely manner to take controlled action. Automatic notification ensures quick reaction times in response to events that require attention in the form of a page out or in the form of automatic incident record creation, classification and assignment to the appropriate resolver group.

In the case of an incident record not automatically created, and an alert dismissal is the only required action based on business rules, the output is an updated log file. Updated log files are necessary to build an accurate record of activity. Proactive problem management for example would look at the log files during trend analysis activities and reactive problem management would examine log files during root cause analysis activities (for more information on Problem Management, refer to the Problem Management Technology Brief).

Now let's review the Event Management process journey, assessing each critical process activity (or station), and examining how technology can be applied to optimize each stage of the journey, ensuring arrival at the last stop on the track.



### **Detect (Includes Fault Detection):**

Most organizations today have invested in monitoring tools configured with business rules and referential data to monitor critical business services and components for potential activity that requires immediate attention. Most often these are event monitoring systems, a Configuration Management System (CMS) and identity and access management systems. Event monitoring systems are configured with rules to monitor thresholds, i.e. security thresholds, capacity thresholds and availability thresholds. A CMS is also used to detect events by monitoring unexpected (or expected) CI changes of state. Identity and access management systems are used to monitor unauthorized access to the environment or password attempts (denial of service or unauthorized access detection).


In all of these areas the goal is to configure the systems to monitor and raise alerts according to the rules set in place and set remediation activity in motion. It is through automation of event monitoring that IT organizations can quickly detect events and potentially raise an incident record before the incident has negatively impacted services. Detecting events early (including faults) allows for increased speed of incident resolution before service levels are impacted. Early alerting of detected events helps ensure that those events can be correlated quickly and remediated quickly before a service failure occurs and service availability is compromised.

Monitoring tools can be configured with business rules to continuously examine critical business services and their underlying IT components to detect faults in the network or specific systems and applications. The benefit to using monitoring tools to monitor critical services is the reduction of resources required to watch for alerts, reduction of human error monitoring service components and the ability to integrate with other service management systems (like an incident management system and CMDB) for quicker response times and timely data processing. However, organizations are often challenged with the generation of large amounts of trivial events sent to multiple consoles, requiring multiple staff resources to monitor those consoles and manually assess critical events from non critical events. For this reason, it is crucial to understand the business and the business impacts in order to effectively manage (and prioritize) events. Once we understand the business requirements, a benefit of automated monitoring is the ability to quickly correlate the data the system is monitoring to take appropriate action. That brings us to the next station on CA's Event Management process track: Filter and Correlate events.

### **Filtering and Correlation:**

Once alerts are raised within an event monitoring system, there is an event correlation based on business rules. Many organizations struggle today with data correlation due to their complex IT environments and lack of formalized process and understanding of the critical needs of the business. The sheer volume of data produced from event monitoring systems can become unmanageable if the proper process controls are not formalized and well understood. Once critical services are defined and mapped to the component level, it then becomes more manageable to make well informed decisions on correlating event information based on those service components.

Rules are configured within monitoring systems that require a certain amount of activity to occur before an alert is generated or is based upon criticality of the service or components being monitored. The pre-defined system logic reaches a decision point to raise an incident



record (or not) in an incident management system. For optimal efficiencies this decision point should be automatic to reduce the amount of manual intervention to filter and correlate the data to take immediate action.

Effective event filtering and correlation will help identify the originating point of events and a subsequent incident and disregard of non-critical events or expected events. Once a correlation of the data occurs, a response is required.

### **Select Response:**

Once the business services are well understood and the children components are mapped, it is possible to select the most appropriate response to events in a more efficient and quick manner because prioritization of events is possible.

The decision to respond to an event can involve a decision to create an incident record based on the event type and the event rules. This activity is at the “CHECK” junction of the PDCA cycle with Incident Management. An event type may require a page out to an on-call resolver group and/or an incident record created depending on SLAs in place. If an incident record is not required, the system log file is updated with the course of activity which enables traceability and the ability to examine activity at a later time (for Root Cause Analysis activities as an example).


When an incident record is required, the action is automated; an incident record is automatically raised in the Service Desk application (incident management system). Automatic incident creation includes automatic classification and prioritization of the incident (again, based on predefined business rules) based on the CI/affected Service Asset. Once the incident record is classified/categorized, the incident is also automatically assigned to the appropriate resolver group. This automatic assignment requires a mapping of services to subject matter experts and/or technical resolver groups. In order to maintain service levels and adhere to SLAs, upon assignment to resolver groups, the SLA clock would be started to capture the most accurate mean time to restore services. This brings us to the last stop on the Event Management track; review and action.

### **Review and Action:**

The process terminus on the Event Management track involves aggregating all of the collected data; reviewing that data and then appropriately acting upon the data.

Depending on the nature of the event and the criticality of the service being monitored, a resulting automatic incident record may also require a review and set of actions by a SME and/or technical resolver group. As an example, if a business critical application experienced an unexpected utilization rate causing slow performance that was in breach of an SLA, an event threshold could trigger multiple actions that could include an alert generation and creation of an automatic incident record.

Event monitoring systems integrated with incident management systems may also automatically page IT personnel upon incident record creation. If an alert and subsequent incident raised was security based, the Security Management process may be triggered. At this point, the technician/SME reviews the incident record and determines the next course of action.



These actions then result in the initial support and diagnosis of the incident (see Incident Management process activities) and progression of the course of actions to restore services. Revisiting our critical business application example with the unexpected utilization rate causing slow performance, this demonstrates how an input into the capacity management activity to assess demand of IT resources can proactively plan for future adequate capacity (for more information on capacity management refer to the Capacity Management technology brief).

The review and action activity also includes a review of the string of activities: was the course of activity still appropriate? Do the business rules need to be changed? Is the Event Management process as efficient as possible? Am I monitoring the right business service components? This ensures continual improvement of the process and ensures the goals of the process are being achieved.

---

## SECTION 3: BENEFITS

### Realizing the Benefits of Event Management

By formally implementing these key activities of an Event Management process, organizations are able to increase operational efficiencies by becoming more proactive at managing operations that experience faults and service outages. In today's complex IT environments, the volume of data being produced on a daily basis can be overwhelming and unmanageable without controlled and repeatable processes and the technology to support those processes. Millions of business transactions that rely on IT support are conducted every day. Without an understanding of critical business processes, managing events becomes an inefficient best-guess effort.

Effectively managing events can speed data correlation and the time it takes to raise an incident record, allowing an IT organization to take immediate action to restore services before an end user or SLA is affected.

Effective Event Management also helps risk reduction; by proactively monitoring critical services and deploying business rules to take immediate action, an organization is better poised to respond to potential threats and vulnerabilities.

Other efficiencies include:

- Increased customer satisfaction levels with more consistent availability of services
- Elimination of process silos (Event Management directly integrated with incident and problem management)
- More efficient use of resources (with use of automated systems) aligned to the business objectives

---

## SECTION 4: CONCLUSIONS

### Conclusions

With the complexities of IT organizations today, the need for good Event Management practice is important and the need for technology enabled processes is critical for optimal operational efficiencies. The objective of an Event Management process is to detect events of critical service components and take immediate action to manage those events. Today we need data collected, correlated, processed and analyzed as quickly and accurately as possible. Efficiencies begin with prior planning to determine which services are critical and require monitoring along with regular review sessions to keep these rules defined, accurate and relevant.

Technology plays a critical role in optimizing the Event Management process by automating the actual process activities themselves (such as event detection, event notification and automatic incident creation), and by accessing the outputs from other related processes (like Configuration Management). Integration with other processes (especially Incident Management, Problem Management, Availability Management, Configuration Management and Service Level Management) is vitally important to ensure that events are managed effectively and that the highest levels of availability and service are maintained.

By utilizing CA's process map for Event Management, you are well on your way to understanding the key process steps and the automation opportunities to help you achieve your goals.

---

## SECTION 5: ABOUT THE AUTHOR

**Nancy Hinich-Gualda**

Principal Consultant, CA Services

### About the Author

Nancy Hinich-Gualda is a Principal Consultant for CA Services where she advises senior management of customer organizations to identify opportunities for ITIL best practices and implementation programs for business service improvements. She has 10 years of IT experience and holds a Manager's Certificate in IT Service Management (ITIL v2) and ITIL v3 Foundations. She was a contributing author to CA's Service Management Process Maps: Your route to service excellence book (2007) and a contributing editor of ITIL® and the Software Lifecycle: Practical Strategy and Design Principles (2008).

---

To learn more about the CA ITIL solutions, [visit ca.com/itil](http://ca.com/itil).



CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies the management of enterprise-wide IT for greater business results. Our vision, tools and expertise help customers manage risk, improve service, manage costs and align their IT investments with their business needs.