Monitoring and event management
ITIL®4 Practice Guide

AXELOS.com

22 November 2019

Contents

AXELOS Copyright
View Only – Not for Redistribution
© 2019

1 About this document

This document provides practical guidance for the monitoring and event management practice. It is split into five main sections, covering:

- general information about the practice
- the processes and activities of monitoring and event management and their roles in the service value chain
- the organizations and people involved in monitoring and event management
- the information and technology supporting monitoring and event management
- considerations for partners and suppliers for monitoring and event management

1.1 ITIL® 4 QUALIFICATION SCHEME

Selected content from this document is examinable as a part of the following syllabuses:

- ITIL Specialist: Create, deliver and support
- ITIL Specialist: Drive stakeholder value

Please refer to the respective syllabus documents for details.

2 General information

2.1 PURPOSE AND DESCRIPTION

The purpose of the monitoring and event management practice is to systematically observe services and service components, and record and report selected changes of state identified as events. This practice identifies and prioritizes infrastructure, services, business processes, and information security events, and establishes the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents.

Event: Any change of state that has significance for the management of a service or other configuration item (CI).

Monitoring and event management is used to manage events throughout their lifecycle to understand and optimize their impact on the organization and its services. Monitoring and event management includes identification and categorization, or analysis, of events related to all levels of infrastructure and to service interactions between the organization and its service consumers. Monitoring and event management ensures appropriate and timely response to those events.

The monitoring part of the practice focuses on services and configuration items (CIs) to detect conditions of potential significance, track and record the state of servicers and CIs and provide this information to relevant parties.

The event management part of the practice focuses on those monitored changes of state defined by the organization as an event, determining their significance, and identifying and initiating the correct response to them. Information about events is also recorded, stored and provided to relevant parties.

Monitoring and event management data and information are an important input to many practices, including:

- Incident management
- Problem management
- Information security management
- Availability management
- Performance and capacity management
- Change enablement
- Risk management
- Infrastructure and platform management
- Software development and management
- ...and others.

A key point is that monitoring is necessary for event management to take place, but not all monitoring results in the detection of an event. Thresholds and other criteria determine which changes of state will be treated as events. Similarly, it is important to note that not all events have the same significance or require the same response. Criteria will define what category of event has occurred. Typical categories, in order of increasing significance, are informational, warning, and exception events.

2.2 TERMS AND CONCEPTS

Monitoring: Repeated observation of a system, practice, process, service, or other entity to detect events and to ensure that the current status is known.

Knowing the current status of services and service components is essential for managing them. Information about service health and performance enables the organization to respond appropriately to service-impacting events that have already occurred (reactive monitoring), or to take proactive actions, based on pattern analysis of past events, to prevent future adverse events from occurring (proactive monitoring).

Monitoring is accomplished by a variety of different means. CIs may share information about themselves through polling, that is, in response to request from a monitoring tool to collect specific targeted data, or through automatic notification to a monitoring tool when certain conditions are met. Interrogation of service components by monitoring tools represents active monitoring, whereas collection of notifications sent by CIs to monitoring tools represents passive monitoring.

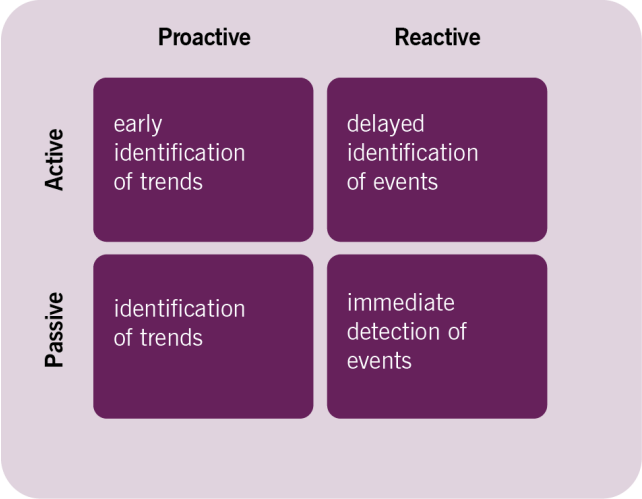

Figure 2.1 Types of monitoring

Note: When active monitoring is used to identify trends, it may help to identify trends earlier than passive monitoring (a monitoring tool requests information before it is sent by the CIs themselves). However, when active monitoring is used to detect events, it may do so later than passive monitoring: in active monitoring information is collected according to a schedule, however with passive monitoring it is shared by the CI immediately after the event. The significance of this note depends on whether active monitoring is continuous or interval-based. It is important to highlight that the longer the intervals are between requests from monitoring tools to services and CIs, the longer the potential delay will be between events and their registration.

Monitoring leverages the native monitoring features of the service components that are being observed. For example, data about operating systems (OS) such as disk space, CPU load, swap usage, etc. is already exposed by OS's and indicates the usage of underlying physical resources. Similarly, many web servers, database servers, and other software have built-in monitoring capabilities and will generate measurement data. All this data is easily sent to a monitoring tool.

In addition to native monitoring features, monitoring also employs designed-for-purpose monitoring systems. These are custom-built software features for observing web and cloud applications, infrastructures, networks, platforms, applications, and microservices. For certain service components, especially applications developed in-house, it may be necessary to add custom-built instrumentation to the services, i.e. code or interfaces which collect and expose the measurement data that is important for the organization.

Although monitoring and event management is traditionally focused on technology components of services, it can also be useful to understand the state of other service management resources and activities, including processes, people, and suppliers.

Metric: A measurement or calculation that is monitored or reported for management and improvement.

Metrics are sources of the raw data for the monitoring and event management practice. Metrics data is collected, aggregated, and analyzed by the monitoring systems. Metrics range across multiple layers, including:

- Low-level infrastructure metrics (host-, server-, network- and others)
- Application metrics (response time, error rate, resource usage…)
- Service level metrics, including infrastructure-, connectivity-, application-based and service action-based, where applicable
- Third party service performance metrics (based on agreed service levels)
- Operations, process and value stream performance metrics.

Threshold: The value of a metric that triggers a pre-defined response.

Responses to a threshold vary and may include:

- Creating an alert or other notification
- Creating an incident
- Change of a status of a previously recorded alert or notification
- Initiating a reactive action towards the respective component or service.

Thresholds are a way of initially filtering the vast amount of monitoring data which can be collected through the monitoring tools. Threshold values should be defined with a degree of care to prevent too many responses being generated and overwhelming the resources, human and machine, ability to respond to them. Other rules for processing the measurement data are usually

combined with thresholds, such as event correlation rules and engines. These can be prescribed by component vendors, defined by the organization, or supported by machine learning.

Some examples of thresholds in monitoring and event management examples could be: "More than X disk errors in an hour", or "CPU utilization reaches or exceeds N% three times with less than Z seconds between any two consecutive events".

Alert: A notification that a threshold has been reached, something has changed, or a failure has occurred.

Alerts are created and controlled by monitoring tools and are managed by the monitoring and event management practice. Alerting is a very important aspect of a monitoring system. The alerting system must have several characteristics, including:

- highly reliable
- flexible, so that it can notify operators through multiple media
- capable of generating detailed and actionable notification messages.

"Over-alerting" is a potential danger for monitoring and event management. A situation arises where more alerts are generated than the enterprise can deal with and where truly significant alerts become lost in the "alert noise". Aggregation, correlation, and filtering of alerts, nowadays enabled by Artificial Intelligence Operations (AIOps) and Machine Learning (ML), provide the remedy for this potential danger.

Changes of state for services and service components occur continuously in the IT environment. As mentioned in this practice, they are typically recognized through notifications created by an IT service, CI, or monitoring tool. To properly handle and respond to the stream of data, it is necessary to filter and categorize the incoming information.

Typical processing of change-of-state data places events into one of three event groups based on their impact and defines three respective responses: informational, warning, or exception.

- *Informational* events do not require action at the time they are identified. Informational events provide the status of a device or service or confirm the state of a task. Examples of informational events include: a user login, an operation completed, and so forth. Informational events signify that regular operation is occurring and are stored in log files for a set period. The organization may choose to analyse the informational events at a later date and may uncover proactive steps that can be beneficial to the service. Informational events can also be published on status dashboards for service provider's or service consumer's audience.
- *Warning* events allow action to be taken before any negative impact is experienced. Warning events signify that an unusual, but not exceptional, operation is occurring. A warning event notifies the appropriate team or tool to take necessary actions to prevent an exception from occurring. Examples of warnings include: scheduled backups are not running, or resource utilization is within 10% of the agreed exception threshold.
- *Exception* events indicate that a critical threshold for a service or component metric has been reached. This identified breach of an established norm for the service or component performance may not yet be having an impact on business operations. However, the exception event may also indicate that a service or component is experiencing a failure, performance

degradations, or loss of functionality. All of which impact business operations. In either case, exception events require action, as they signify that an exception to regular operation is occurring. Examples of exception events are: a PC scan reveals the installation of unauthorized software, a server is down, a backup has failed, etc. This is how detection of incidents is enabled by the monitoring and event management practice.

Event categorization focuses attention on the events that are truly significant for the management and delivery of services. It ensures that operational events are tracked, assessed, and managed appropriately.

Monitoring and event management enables the detection of incidents, distinguishing them from information events and warnings. Detected incidents are handled by the incident management practice. Monitoring and event management also enables problem identification by providing information about trends and events affecting services and service components. In addition, monitoring and event management enables error control for known errors by monitoring and reporting on services and service components. Identified problems and error control for known errors are handled by the problem management practice.

2.3 SCOPE

The scope of the monitoring and event management practice covers all aspect of organization's service management that needs to be controlled and can be automated. This includes:

- identifying and optimizing the scope of monitoring
- implementing and maintaining continuous monitoring
- establishing and maintaining event identification, categorization and processing rules
- implementing processes and automation tools to operationalize the defined event management rules
- ongoing processing of events according to the agreed and implemented rules and processes
- providing information about the current and historical state of the monitored services and resources to relevant stakeholders in an agreed form.

There are several activities and areas of responsibility that are not included in the monitoring and event management practice, although they are still closely related to monitoring and event management. They are listed in Table 2.1, along with references to the practices in which they can be found. It is important to remember that ITIL practices are merely collections of tools to use in the context of value streams and should be combined as necessary depending on the situation.

Table 2.1 Monitoring and event management-related activities described in other practice guides

Activity	Practice Guide
Management of incidents	Incident management
Investigation of causes of events and trends	Problem management
Management of changes in response to events	Change enablement
Communications with users	Service desk
Support decision-making based on monitoring data	Measurement and reporting
Setting targets and thresholds for service quality and performance	Service level management Availability management Performance and capacity management Information security management Continuity management
Setting thresholds for infrastructure and application components	Infrastructure and platform management Software development and management
Setting targets and thresholds for third parties' services	Supplier management

2.4 PRACTICE SUCCESS FACTORS

A Practice Success Factor (PSF) is a complex functional component of a practice that is required for the practice to fulfil its purpose.

A PSF is more than a task or activity; it includes components from all four dimensions of service management. The nature of the activities and resources of PSFs within a practice may differ, but together they ensure that the practice is effective.

The Monitoring and Event Management practice includes the following PSFs:

- Establish and maintain approaches/models that describe the various types of events and monitoring capabilities needed to detect them
- Ensure that timely, relevant, and sufficient monitoring data is available to relevant stakeholders
- Ensure that events are detected, interpreted, and if needed acted upon as quickly as possible.

2.4.1 Establish and maintain approaches/models that describe the various types of events and monitoring capabilities needed to detect them

Modern technologies provide opportunities to measure and monitor every aspect of the services and service components operation, but a practitioner should carefully manage the scope of the monitoring, as well as frequency and number of metrics.

The main challenge of the modern monitoring and event management practice is not lack of data but the *volume* of data. The focus of the monitoring and event management practice should be finding meaningful information to support service operations and improvement, decision-making and value creation. When establishing or improving the monitoring and event management practice, the following aspects should be considered:

2.5 IDENTIFYING AND PRIORITIZING SERVICES AND SERVICE COMPONENTS MONITORED

Identifying and prioritizing which entities should be monitored is a key activity of the practice, helping to detect changes of state (or lack of desired changes in state) that are most significant for the management of a service of CI. Deciding which services, systems, CIs, and other service components to monitor will be based on the organization's business objectives. It will also require a thorough understanding of the organization's service design architecture. Practitioners of monitoring and event management will need to know service dependency mapping: what top-level business capabilities map to which products and services support those capabilities, and in turn which products and services map to the underlying IT infrastructure that enables the products and services. By having a full end-to-end picture of what entities are involved in delivering a service, the monitoring and event management practitioners will be able to correctly identify and prioritize the critical entities that need to be monitored.

Here, 'monitorability' of a service component should also be assessed and effective set of criteria defined. Criteria chosen should be revealing enough and provide a basis for diagnostics and decision making.

2.6 FINDING BALANCE BETWEEN INFORMATIVITY, GRANULARITY AND FREQUENCY OF THE MONITORING

Establishing and maintaining monitoring of a service component could be considered as an investment of resources (monitoring tools, data storage, manhours, etc.), and the more data is captured, the less return is expected. This is because the greater the number of criteria monitored and frequency of probing, the more time and effort needs to be spent filtering, classifying and analysing data. Automation and machine learning-based solutions could help to free people and improve results of data analysis, but a practitioner should always aim at making the monitoring the most efficient.

2.7 MAINTAINING CAPABILITIES FOR DATA GATHERING, STORAGE, FILTERING AND DATA CORRELATION

The monitoring and event management practice relies heavily on the Information and Technology dimension of service management. Without the native monitoring features of the services and service components being observed, and without the IT monitoring tools (generic widely available commercial tools as well as custom-built tools) it would be virtually impossible to detect changes of state that have significance for the management of a CI or a service.

Communicating information about themselves is something that service elements do through polling, that is, in response to interrogation by a monitoring tool to collect specific targeted data, or through automatic notification to a monitoring tool when certain conditions are met. This communication depends on the availability of the monitoring tools and on the networks to transmit the event data.

Additional attention should be paid to the tools that do classification, filtering and correlation of data, as well as automation tools for event response.

Deciding which services, systems, CIs, and other service components to monitor will be based on the organization's business and mission objectives. It also requires a thorough understanding of the organization's service architecture. Practitioners of monitoring and event management will need to know service dependency mapping: how products and services map to the underlying IT infrastructure that enables them. By having a full end-to-end picture of what entities are involved in delivering a service, the monitoring and event management practitioners will be able to correctly identify and prioritize the critical entities that need to be monitored.

A great deal of the service architecture of individual services often consists of third-party products and services which the organization has integrated to deliver an end-to-end service to customers and users. The built-in monitoring capabilities of these third-party products and services are a key part of the monitoring and event management practice. Monitoring and event management practitioners along with their counterparts in the Service Design practice need to be able to cooperate frequently and well with their equipment and service vendors. In doing so, monitoring and event management and Service Design secure the necessary goods and services that constitute the organization's services and ensure that these services are monitorable and manageable.

Determining the appropriate control action for events relies on the filtering and categorization of the detected changes of state. Filtering and categorization, occurring in the Information and Technology service dimension, are largely done automatically by the organization's event management system (EMS) into which the IT monitoring tools feed the detected, collected, and transmitted information. The business rules, however, by which the EMS filters and categorizes the data and makes determinations of significance about them (deciding whether the data represent an Informational, Warning, or Exception event) are established in the Organization and People dimension of service management. The thresholds, the alerting parameters, the criteria which the monitoring tools and the EMS are configured to address are all the product of organizational priorities and the skilled leadership and staff working to ensure the operational health of the service ecosystem.

Policies need to be in place to handle different types of events. A "one size fits all" approach to events is inappropriate and a waste of resources. Different types of events require a response that is tailored and specific to the type of event it is. A common set of control actions should be established for each class of event. Policies will address when an auto response is appropriate, when an alert and escalation to human intervention is appropriate, when an Incident, Problem, or Change should be initiated, or when special handling is required. For example, in the case of a security breach that potentially could have operational impact but has not yet affected service availability. Policies are defined in the Organization and People dimension and are operationalized in the Information and Technology dimension.

Having in place a standard classification scheme for events, such as Informational, Warning, and Exception, enables common handling and escalation processes. It also enables event notifications to be sent only to those responsible for the handling of further actions or decisions related to the events. Often, in the incident, problem, or change management practices. Avoiding notifications to individuals not directly involved in processing events is an efficient use of resources. To do this, event notifications will identify which departments, groups or individuals need to respond to events. Maintaining event routing information is a constant task as new events are added or personnel responsibilities change.

A standard classification scheme for events will enable a common set of actions to be established for each class of event. In the value streams, when action is being taken on recognized events, operational and service level objectives for the service are taken into consideration. Actions for events that trigger the notification of incidents and problems can be tied into existing categorization and prioritization policies that have been established by incident and problem management.

Many of the IT monitoring tools and the EMS itself will likely be supplied by third party suppliers with whom the monitoring and event management practice in conjunction with the supplier management practice will maintain solid working relationships.

2.7.1 Ensure that timely, relevant and sufficient monitoring data is available to relevant stakeholders

The reporting aspect of monitoring and event management enables ground truth with respect to a service provider's actual operating performance and behaviour when benchmarked against the standards in the original service design and in the Service Level Agreements (SLAs) agreed with the customers. Monitoring and event management provides direct observation results, real-world empirical evidence as opposed to intended or aspirational results.

Gathering data that has accuracy and integrity in the monitoring and event management practice is critical to the work of delivering a high-quality service and a high-quality customer experience when using the service. Service measurement (the gathering of data about the service) depends on monitoring and event management monitoring and reporting. Monitoring and event management is critical for Continual Improvement efforts due to its focus on the effectiveness and efficiency of services and service components.

Monitoring and event management identifies weak areas, so that remedial action can be taken (if there is a justifiable business case), therefore improving future service quality. Monitoring and event management can also show where customer actions are causing the fault and identify where working efficiency and/or training can be improved. Monitoring and event management can also address both internal and external suppliers since their performance must be evaluated and managed as well.

2.7.2 Ensure that events are detected, interpreted, and if needed acted upon as quickly as possible

Defining rules for monitoring and event management is not enough; actual detection and processing of events is required to make these rules valuable. Efficiency and scope of event management heavily depends on the service architecture and level of service management automation. In digital infrastructure and modern application, many tools for monitoring and event management are built-in, and the focus of the practice is on the integration and tuning of the event processing rules.

Contrary to that, organizations with many legacy systems which were not designed for monitoring must focus on implementation of specialized monitoring and event management tools and add-ons, or even on manual monitoring and event management.

Technology opportunities and constraints should inform monitoring and event management scope, policy making, and daily activities.

Regardless of how limited organization's monitoring and event management capabilities, they should be subject to continual improvement, to ensure that the practice meets the needs of the organization.

2.8 KEY METRICS

The ITIL practices are means or tools for the management of products and services. Like the performance of any tool, practice performance can be assessed only in the context of that tool's application. However, tools can differ in quality. This difference defines the tool's potential or capability to be effective when used according to their purpose.

The same applies to practices: their performance should be assessed in the context of value streams, but their potential is defined by their design and the quality of the resources. Further guidance on metrics, KPIs, and other techniques that can help with this can be found in the measurement and reporting practice guide.

Key metrics for the Monitoring and Event Management Practice are mapped to its PSFs. They can be used as KPIs in the context of value streams to assess the contribution of the Monitoring and Event Management Practice to the effectiveness and efficiency of those value streams. Some examples of key metrics are given in table 2.2.

Table 2.2 Example metrics for the practice success factors

Practice Success Factors	Example Metrics
Establish and maintain approaches/models that describe the various types of events and monitoring capabilities needed to detect them	• Satisfaction of the stakeholders with monitoring and event management approach • Adherence of the organization to the approach • Percentage of the recommendations / requirements of the approach that are not followed or found unrealistic
Ensure that timely, relevant and sufficient monitoring data is available to relevant stakeholders	• Satisfaction of the stakeholders with monitoring data and its presentation • Quality of the monitoring data (as per agreed data quality criteria)
Ensure that events are detected, interpreted, and if needed acted upon as quickly as possible	• Impact of event management errors • Number and impact of event communications 'noise' • Impact of incidents and problems that could not be prevented or resolved due to poor event management

The correct aggregation of metrics into complex indicators will make them easier to use for the ongoing management of value streams and for the periodic assessment and continual improvement of the Monitoring and Event Management Practice. There is no single best solution. Metrics will be based on the overall service strategy and priorities of an organization, as well as on the goals of the value streams to which the practice contributes.

3 Value streams and processes

3.1 VALUE STREAM CONTRIBUTION

Like any other ITIL management practice, the monitoring and event management practice contributes to multiple value streams. Remember, no value stream is made up of a single practice. The monitoring and event management practice combines with other practices to provide high-quality services to consumers.

3.2 PROCESSES

Each practice may include one or more processes and activities that may be necessary to fulfil the purpose of that practice.

> Process
>
> A set of interrelated or interacting activities that transform inputs into outputs. Processes define the sequence of actions and their dependencies.

The monitoring and event management practice activities form 3 processes:

- **Monitoring planning process.** This is a process of adding an element into monitoring, defining the priority of the element, choosing features to monitor, establishing metrics and thresholds for event classification, mapping events with the action plans and teams responsible.
- Event handling process.
- **Monitoring and event management review.** This process is scheduled or triggered review process for major event post-mortems, updates on filtering and correlation analysis, services 'health models', improvements to automate and operationalize monitoring.

Table 3.1 Inputs, activities, and outputs of the monitoring planning process

Key inputs	Activities	Key outputs
• Service health criteria from service design • SLAs • Service performance thresholds from availability, capacity and performance management practices • Knowledge articles • Service catalogue • CI data	• Defining the objective of monitoring • Assessing measurements available and criteria to be monitored • Defining types of events for the object of monitoring • Defining the thresholds for different type of events • Defining a service 'health model' (end-to-end events) • Defining events correlations and rule sets • Mapping events with action plans and functions responsible and notified	• Monitoring plan for the object • Service health model • Defined types of events, criteria for event detection, priority and response to the events • Responsibility matrix for events

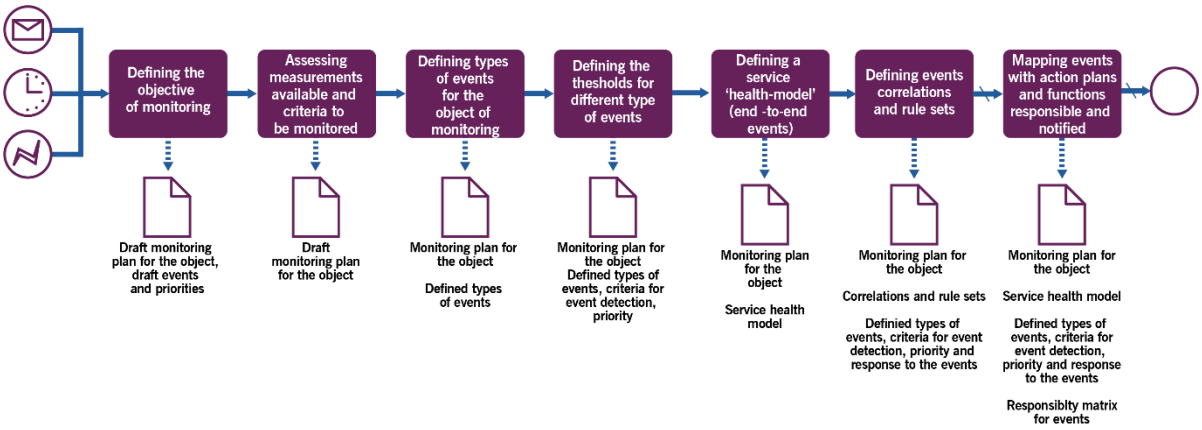

Figure 3.1 Workflow of the monitoring planning process

Table 3.2 Activities of the monitoring planning process

Activity	Description
Defining the objective of monitoring	With information received from the service design stage and service validation and testing practice and practices involved in the development of the service (availability, capacity and performance management practices) and service level management practice, the team defines key objectives of monitoring. This discussion should move from warranty to utility requirements (first covering the most obvious functionality requirements, that were, for example, in the user stories for the application). Also, it should increase in granularity, starting with the key service performance and moving to more details and components. Team should make a list with descending monitoring priority.
Assessing measurements available and criteria to be monitored	Monitoring priority list items are then mapped or translated into available measurements or synthetic measurements based on available measurements. Adding measurements should be explored.
Defining types of events for the object of monitoring	Team defines and classifies different types of events. Types could be general, like informational, warning, exception, or may depend on the functionality, user groups and their priorities, divided by components or types of key monitoring objectives.
Defining the thresholds for different type of events	Team, together with service or component development team, defines the thresholds for types of events. The same component

	metric could be treated differently based on the service it contributes into, depending on the existing SLAs and availability, capacity and performance requirements defined for the service or component. Also, event handling throughput should be taken into consideration, as, although modern IT systems can detect almost any event, not any event should be acted upon. So generally monitoring and event management should be developed iteratively, from preventing disasters in the very beginning, to refinement of components later.
Defining a service 'health model' (end-to-end events)	Based on input from teams involved in the service design, a 'health model' is built, that reflects the key events in the service and connections between them. There could be several models for one service. Such models let monitoring team assess user experience of the service. For example, a model can be built for a single bank customer transaction, and measure how much time it takes from a request in mobile app, with all the bank database systems in-between, to the notification of completed transaction in the mobile app. Service 'health models' could also be implemented as reports or dashboards on service health and performance and used at ad-hoc basis by service owners, teams involved in other practices, and other stakeholders. This way the information about the service is 'pulled' by a stakeholder.
Defining event correlations and rule sets	Together with teams involved in the service design, event correlations and corresponding sets of rules are defined. Some correlations might use second event as a check of the first event, or to further filter the scope of the event. Also, defined correlations can help preventing some negative synergic effects events might have when occurring simultaneously. A rule set consists of several rules that define how the event messages for a particular event will be processed and evaluated. For example, a warning event may be generated each time a disk log file reaches its capacity, but an exception event will be generated if more than four warning events have been generated. Rules themselves are typically embedded into monitoring and event handling technologies. They consist of Boolean kinds of

	algorithms to correlate events that have been generated in order to create additional events that need to be communicated. These algorithms can be codified into event management software typically referred to as correlation engines. Artificial Intelligence (AI) systems could be used to define typical and atypical behaviors of users, admins, systems, etc. This may form an additional check to filter the events.
Mapping events with action plans and functions responsible and notified	For each event or group of events, an action plan to minimize the negative impact of event is defined. Based on the action plan, the team or function responsible for actions following the event, can be defined. Action plans can also be executed automatically or be semi-automated, including human intervention for some important actions. Action plans created at this stage become a basis for event procedures and automation.

Table 3.3 Inputs, activities, and outputs of the event handling process

Key inputs	Activities	Key outputs
• Notifications from objects of monitoring, monitoring tools • Monitoring plan	• Event detection • Event logging • Event filtering and correlation check (might be iterative) • Event classification • Event response selected • Notifications sent, response procedure carries out	• Event record • Events statistics updated • Event response errors • Major event post-mortem initiated • Stakeholder notifications • Knowledge articles update • Incidents logged • Updated reports and dashboards

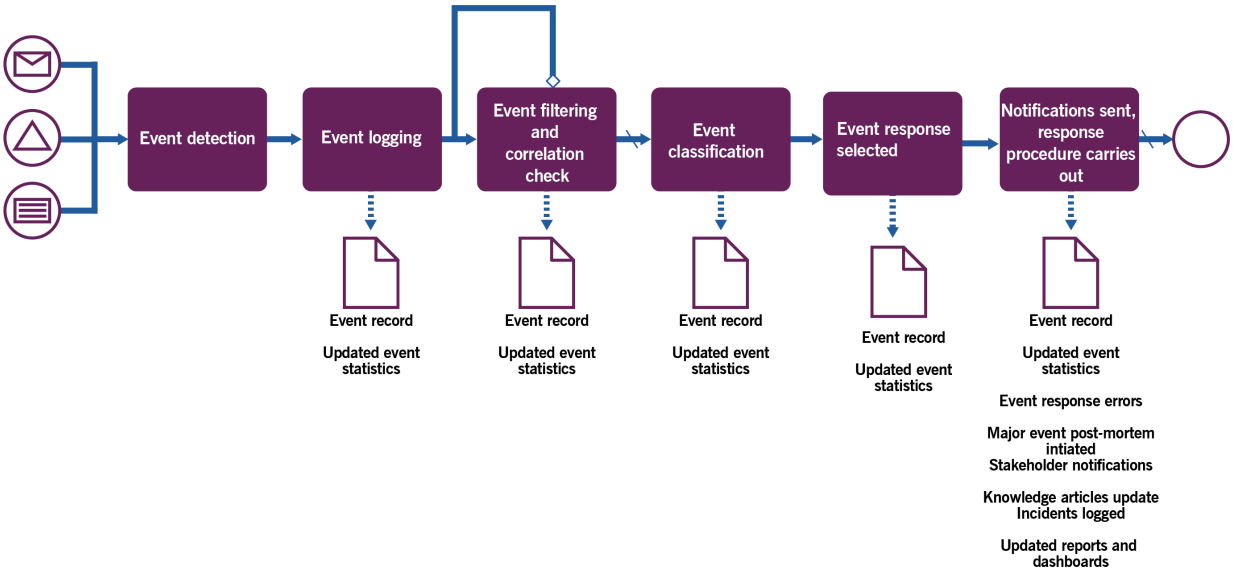

Figure 3.2 Workflow of the event handling process

Table 3.4 Activities of the event handling process

Activity	Description
Event detection	Event detected by monitoring systems, or as a result of manual monitoring. Not all events should be detected and monitoring systems bandwidth should be taken into consideration. Only critical events and events that can be acted upon should be detected within existing resource constraints.
Event logging	Event should be logged in the monitoring system, preferably automatically.
Event filtering and correlation check (might be iterative)	Event should be treated according to rule sets, to filter and find correlations, to enable better classification. This activity might be iterative.
Event classification	Event classified into a group or type, and specific event is filtered further within a group if needed to select a proper response.
Event response selected	Action plan or response procedure should be planned for each event in the monitoring planning process. Based on the rules

	defined in planning, event response and teams notified are is selected.
Notifications sent, response procedure carries out	Response procedure carries out, teams responsible for actions or supervision (if response procedure is fully automated) are notified.

Table 3.5 Inputs, activities, and outputs of the Monitoring and event management review process

Key inputs	Activities	Key outputs
• Updated knowledge articles • Major event records • Major incident records • Improvement proposals • Event records and statistics • Information requests from service owners and stakeholders	• Post-mortem review for major events and incidents • Review of filtering and correlation analysis • Review of services 'health models' • Review of event response procedures and automation • Review of tools available for data analysis, correlation analysis, AI and ML • Review of statistical information gathered by monitoring tools	• Updated event response procedures • Improvement proposals for filtering and correlation analysis • Changes proposed to automation • Updated monitoring criteria and thresholds • Updated filtering methods • Updated list of tools and technology used • Updated list of reports and statistical information provided

Table 3.6 Activities of the monitoring and event management review process

Activity	Description
Post-mortem review for major events and incidents	The fact that a major incident occurred may often mean that some abnormal service or component behavior was not detected and acted upon. Therefore, major events and incidents provide a good basis for monitoring knowledge discovery and improvements. The nature of the major event should be reviewed, analyzed for event correlations, decomposed to component or even CI level, and corresponding metrics should be explored that may have helped to detect the major event or failure that led to the major incident. Additional or similar risks of the component should be explored, and events identified should be added into monitoring.

	Changes to monitoring should be proposed to detect the similar incidents in future.
Review of filtering and correlation analysis Review of services 'health models'	Filtering and correlation should be addressed when monitoring detects a huge number of events or does not detect events when it should. Sometimes temporary measures could be considered, like loosening the thresholds or grouping of events. Otherwise, detailed analysis and thorough rules definition should be undertaken, and changes to monitoring proposed as a result.
Review of event response procedures and automation	Incidents and failures occurred in result of event response should be reviewed and changes proposed. Also, this review should aim at increasing automation in both detecting events and responding to them. Additional automation should be proposed.
Review of tools available for data analysis, correlation analysis, AI and ML	Tools available internally and in the market that may increase efficiency of monitoring should be reviewed. Trials, pilot implementations should be proposed within monitoring budget. Also, this review should discuss any new techniques or best practices used in monitoring, market benchmarking should be carried out, and improvements to monitoring proposed.
Review of statistical information gathered by monitoring tools	Statistical information should be reviewed, to propose improvements to monitoring, services monitored. Trends detected for services should be reviewed by all teams involved in service lifecycle.

4 Organizations and people

4.1 ROLES, COMPETENCIES, AND RESPONSIBILITIES

The practice guides do not describe the practice management roles such as practice owner, practice lead, or practice coach. The practice guides focus on specialist roles specific to each practice. The structure and naming of each role may differ from organization to organization, so any roles defined in ITIL should not be treated as mandatory, or even recommended. Remember, roles are not job titles. One person can take on multiple roles and one role can be assigned to multiple people.

Roles are described in the context of processes and activities. Each role is characterized with a competence profile based on the following model:

Competence code	Description
L	Leader. Activities and skills associated with this competence include decision making, delegation, overseeing other activities, incentives and motivation, and evaluating outcomes.
A	Administrator. Activities and skills associated with this competence include the assignment and prioritization of tasks, record keeping, ongoing reporting, and basic improvement initiatives.
C	Coordinator/communicator. Activities and skills associated with this competence include the coordination of multiple parties, communication between stakeholders, and the running of awareness campaigns.
M	Methods and techniques expert. Activities and skills associated with this competence include the design and implementation of work techniques, the documentation of procedures, consulting on processes, work analysis, and continual improvement.
T	Technical expert. This competence focuses on technical (IT) expertise and expertise-based assignments.

Table 4.1 The roles involved in the Monitoring and Event Management Practice activities

Activity	Responsible roles (examples)	Competence profile	Specific skills
Monitoring planning process			

Defining the objective of monitoring	Service owner Designer Developer User Delivery manager Account manager Tester Service validation specialist Operations manager	CA	Understanding of service value for stakeholders and service proposition Knowledge of service levels and user experience
Assessing measurements available and criteria to be monitored Defining types of events for the object of monitoring Defining the thresholds for different type of events	Tester Service validation specialist Monitoring specialist Developer Designer Architect Operations manager	TM	Knowledge of service architecture and design Expertise in monitoring tools, probe detectors and sensors
Defining a service 'health model' (end-to-end events) Defining events correlations and rule sets	Service owner User Delivery manager Account manager Operations manager Tester Service validation specialist Monitoring specialist Developer	TMA	Knowledge of user experience Knowledge of warranty and utility requirements Knowledge of service subject matter and business processes Knowledge of service architecture and design

	Designer Architect		Expertise in monitoring tools and probe detectors and sensors
Mapping events with action plans and functions responsible and notified	Service owner User Delivery manager Account manager Tester Service validation specialist Monitoring specialist Developer Designer Architect	ATM	Knowledge of operations and support infrastructure and organization Knowledge of service architecture and design Expertise in monitoring tools and probe detectors and sensors

Event handling process.

All efforts should be made to make this process as automated as possible, so no roles are discussed for this process.

Monitoring and event management review			
Post-mortem review for major events and incidents Review of filtering and correlation analysis Review of services 'health models'	Service owner User Delivery manager Account manager Monitoring specialist Developer Designer Architect	TMA	Knowledge of service architecture and design Expertise in monitoring tools Knowledge of service subject matter and business processes Continual improvement skills
Review of event response procedures and automation	Service owner Delivery manager Account manager	ATMC	Knowledge of operations and support infrastructure and organization

	Monitoring specialist Developer Designer Architect Service desk manager Operations manager		Expertise in monitoring tools Expertise in automation Knowledge of service subject matter and business processes Continual improvement skills
Review of tools available for data analysis, correlation analysis, AI and ML	Monitoring specialist Architect Business analyst Technology consultant	MTA	Expertise in monitoring tools, AI, ML Expertise in automation Continual improvement skills
Review of statistical information gathered by monitoring tools	Monitoring specialist Architect Business analyst	MTA	Knowledge of service architecture and design Expertise in monitoring tools Knowledge of service subject matter and business processes Continual improvement skills

4.2 ORGANIZATIONAL STRUCTURES AND TEAMS

It is rare that a dedicated monitoring and event management team exists in the organization. Usually, people responsible for the service delivery and operations are those involved in the monitoring.

It is important to ensure that monitoring is planned at the design stage of the service lifecycle. Therefore people responsible for monitoring should be involved in the design phase, and teams that developed the service or component are available for service hand-over to operations and setting up the monitoring. This includes architects, software development teams, infrastructure teams, designers, teams responsible for service validation, availability, continuity, capacity and performance, etc.

5 Information and technology

5.1 INFORMATION EXCHANGE

The effectiveness of the Monitoring and event management practice is based on the quality of the information used. This information includes, but is not limited to, information about:

- customers and users
- services, their architecture, and design, acceptance criteria and SLAs
- partners and suppliers, including SLA information on the services they provide
- policies and requirements which regulate service provision
- ongoing service delivery, including:
  - information about the current operational status of services
  - service warranty and utility requirements
  - service metrics available
  - CIs the service is dependent on
  - interdependencies of service components and their performance
  - information about major incidents
  - information about planned and ongoing changes and expected impact on service performance
  - availability, capacity and performance targets
  - teams responsible for service and components
  - knowledge articles about the service
- information about the status of service improvements.

This information may take various forms. The key inputs and outputs of the practice are listed in the 'value streams and processes' section of this guide.

5.2 AUTOMATION AND TOOLING

In some cases, the work of the Monitoring and event management practice can significantly benefit from automation (see the 'value streams and processes' section of this guide for details on when this is applicable). Where this is the case, and automation is possible and effective, it may involve the solutions outlined in table 5.1.

Table 5.1 Table title

Process activity	Means of automation	Key functionality	Impact on the effectiveness of the practice
Monitoring planning process			
Defining the objective of monitoring Assessing measurements available and criteria to be monitored	Visualization tools (e.g. mind maps, service diagrams, architecture visualization) Service catalogue tools	Visualization of service structure, dependencies, CIs, etc. Providing information on service structure and	Medium

Defining types of events for the object of monitoring	CMDB	component/service interdependencies Providing information on service SLAs and requirements	
Defining the thresholds for different type of events Defining a service 'health model' (end-to-end events) Defining events correlations and rule sets	Monitoring and event management tools ITSM tool Software-defined infrastructure tools Infrastructure and platform built-in monitoring tools Service visualization tools	Active and reactive monitoring, event setup, data gathering, data analysis, alerting, rules setting	High
Mapping events with action plans and functions responsible and notified	Monitoring and event management tools ITSM tools Software-defined infrastructure tools Collaboration and communication tools Integration bus Automation systems AI and ML tools for event correlation, behavior monitoring and analysis	ITSM tools integration (e.g. incidents logging based on events) Notifications and communications, task creation. Automated scripts running AI and ML event correlation, normal/abnormal behavior analysis	High
Event handling process.			
Event detection Event logging Event filtering and correlation check (might be iterative)	Monitoring and event management tools ITSM tools Software-defined infrastructure tools	ITSM tools integration (e.g. incidents logging based on events) Notifications and communications, task creation.	High

Event classification Event response selected Notifications sent, response procedure carries out	Collaboration and communication tools Integration bus Automation systems Reports and dashboard tools and portals	Automated scripts running AI and ML event correlation, normal/abnormal behavior analysis Reports and dashboard publishing	
Monitoring and event management review			
Post-mortem review for major events and incidents Review of filtering and correlation analysis Review of services 'health models' Review of event response procedures and automation Review of tools available for data analysis, correlation analysis, AI and ML Review of statistical information gathered by monitoring tools	Visualization tools (e.g. mind maps, service diagrams, architecture visualization) Statistics and analysis tools, databases Service catalogue tools CMDB Monitoring and event management tools ITSM tools Collaboration and communication tools Reports and dashboard tools and portals Business analysis tools Benchmarking tools and knowledge management tools	Visualization of service structure, dependencies, Cis, etc. Providing information on service structure and component/service interdependencies Providing information on service SLAs and requirements, compliance and breaches Providing information on major incidents Reports and dashboard publishing Notifications, chats Analysis and assessment Knowledge sharing	Medium

6 Partners and suppliers

Very few services are delivered using only an organization's own resources. Most, if not all, depend on other services, often provided by third parties outside the organization (see section 2.4 of the ITIL® Foundation: ITIL 4 Edition publication for a model of a service relationship). Relationships and dependencies introduced by supporting services are described in the practice guides for supplier management.

Development of communications and cloud services made external monitoring services very popular. CIs like servers, database instances can have monitoring agents installed and feeding information into cloud repository. Such solutions make additional AI and machine learning (ML)-enabled analysis easier and cheaper. ML in such solutions is improved by merging data from thousands of monitoring objects and fine-tuned understanding of normal and abnormal behaviour of systems and users.

Another important consideration is the agreement concerning the access to monitoring for outsourced services and components, so that an organization has control over measurements and metrics agreed with the service provider.

Also, all services that are developed by external suppliers must be designed as monitoring-enabled, which means that a designed service must be able to provide information on its performance and health.

Where organizations aim to ensure fast and effective the monitoring and event management, they usually try to agree to close cooperation with their partners and suppliers, removing formal bureaucratic barriers in communication, collaboration, and decision making. Refer to the supplier management practice guide for more information on this.

7 Important reminder

Most of the content of the practice guides should be taken as a suggestion of areas that an organization might consider when establishing and nurturing their own practices. The practice guides are catalogues of things that organizations might think about, not a list of answers. When using the content of the ITIL practice guides, organizations should always follow the ITIL guiding principles:

- focus on value
- start where you are
- progress iteratively with feedback
- collaborate and promote visibility
- think and work holistically
- keep it simple and practical
- optimize and automate.

More information on the guiding principles and their application can be found in section 4.3 of the *ITIL® Foundation: ITIL 4 Edition publication*.

8 Acknowledgments

AXELOS Ltd is grateful to everyone who has contributed to the development of this guidance. These practice guides incorporate an unprecedented level of enthusiasm and feedback from across the ITIL community. In particular, AXELOS would like to thank the following:

8.1 AUTHORS

Dennis Cotter

8.2 REVIEWERS

Roman Jouravlev

8.3 CONTRIBUTORS

Dinara Adyrbai