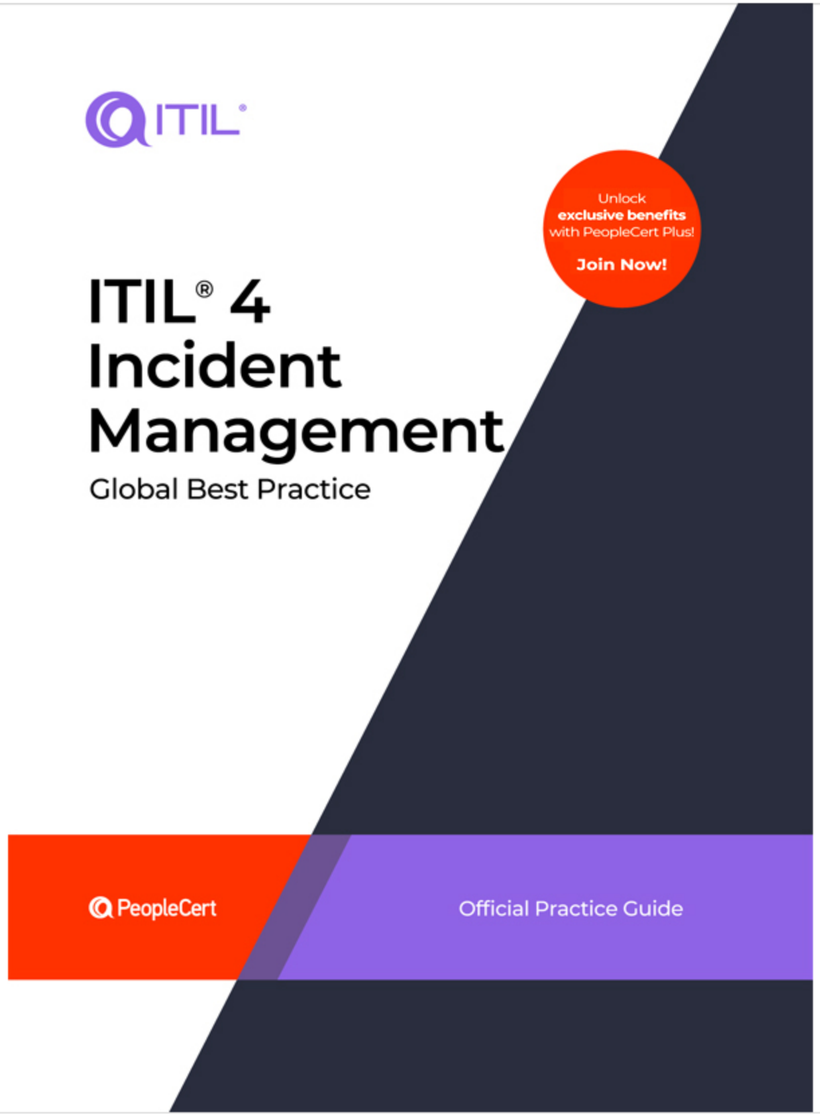


ITIL® 4 Incident Management

Global Best Practice

Unlocking your potential to achieve more

Welcome to the ITIL® 4 Incident Management Official Practice Guide.
Established in 2000, **PeopleCert** is the global leader in the certification industry. **PeopleCert** develops global best practice frameworks and certifications, manages exams, and delivers certifications. Its product portfolio in IT & Digital Transformation, Project Management, Business, and Languages includes two of the most globally recognized IP-protected frameworks, developed and evolved by the UK Government over 30 years: ITIL® and PRINCE2®.

PeopleCert certifications are delivered across 200 countries and territories, 50.000 Corporates (82% of Fortune 500), and 800 government organizations through a global network of 2.500 Accredited Training Organizations and 30.000 venues worldwide, as well as through **PeopleCert's** award-winning Online Proctoring solution. **PeopleCert** consists of over 1.000 employees from 40 nationalities and has received over 50 awards in Entrepreneurship, Business, Technology, and Sustainability.

Powering
Best
Practice

Published by PeopleCert International Ltd.
ISBN: 978-9925-34-291-4 (Digital)
ISBN: 978-9925-34-290-7 (Print)
ISBN: 978-9925-34-292-1 (ePub)
Published in Cyprus
Publication printed in Greece or reproduced electronically in Greece

Disclaimer
This publication is designed to provide helpful information to the reader. Although every care has been taken by PeopleCert International Ltd in the preparation of this publication, no representation or warranty (express or implied) is given by PeopleCert International Ltd as publisher with respect as to the completeness, accuracy, reliability, suitability or availability of the information contained within it and neither shall PeopleCert International Ltd be responsible or liable for any loss or damage whatsoever (indicatively but not limited to, special, indirect, consequential) arising or resulting of virtue of information, instructions or advice contained within this publication.

First edition PeopleCert International copyright® 2023
Second edition PeopleCert International copyright® 2024

Contents

List of figures

List of tables

Welcome

Acknowledgements

PeopleCert is grateful to everyone who has contributed to the development of this Official Practice Guide. These Official Practice Guides incorporate an unprecedented level of enthusiasm and feedback from across the ITIL community. In particular, PeopleCert would like to thank the following people.

Authors

Barry Corless, Roman Zhuravlev, Andrew Vermes

Reviewers

Akshay Anand, Sofi Fahlberg, Michael G. Hall, Steve Harrop, Piia Karvonen, Anton Lykov, Paula Määttänen, Christian F. Nissen, Mark O'Loughlin, Tatiana Orlova, Elina Pirjanti, Stuart Rance

2023 Revision

David Cannon, Antonina Douannes, Peter Farenden, Adam Griffith, Roman Zhuravlev, Kaimar Karu, Barclay Rae, Stuart Rance, Nicola Reeves

Information icons

Chapter 1
About this guide

This guide provides practical guidance for the incident management practice. It is split into seven main sections, covering:

- general information about the practice
- the practice's processes and activities and their roles in the service value chain
- the organizations and people involved in the practice
- the information and technology supporting the practice
- considerations for partners and suppliers for the practice
- information on assessing and developing the capability of the practice
- recommendations for succeeding in the practice.

ITIL® 4 qualification scheme

Selected content of this guide is examinable as a part of the following syllabi:

- **ITIL® 4 Specialist:** Create, Deliver and Support
- **ITIL® 4 Specialist:** High-velocity IT
- **ITIL® 4 Specialist:** Monitor, Support, and Fulfil

Please refer to the respective syllabus documents for details.

Chapter 2
General information

2.1 Purpose and description

Key message

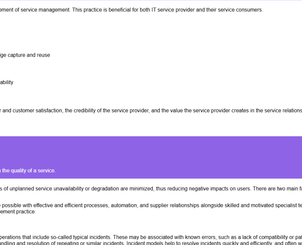
The purpose of the incident management practice is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible.

The definition refers to a 'normal service operation'. Conditions of normal service operation are typically defined within service level agreements (SLAs), or other forms of service quality specification, either agreed with the customer or defined by the service provider. In some cases, internal service provider's specification can include more quality criteria than were initially agreed with the customers (see more on this in the service level management practice guide).

The incident management practice is not limited to the service quality perceived by users. It includes restoration of the normal operation of services and resources, even when their failure or deviation is not visible to the service consumers. In this case, normal operation can be defined in the technical specifications of services or configuration items (CIs).

Finally, if there is no documented specification of a normal operation, an expert opinion may be used to assess the status of the resources and services.

A simple flow to decide if there is an incident:



If users perceive the situation as abnormal, it is recommended to register an incident and work on making users happy as quickly as possible, regardless of whether there is a breach of SLA

If users have not reported anything, but a service level agreement is breached, register an incident and work to restore the agreed level of service before it affects users.

If a service or configuration item are not working as defined in a technical specification, register an incident and work to restore normal performance before it affects the SLA and users.

If there is no formal specifications of service or component normal operation, or if the service works within the specifications, but a specialist thinks that it is not operating normally, register an incident and restore normal operation as quickly as reasonably possible.

The incident management practice is a fundamental element of service management. This practice is beneficial for both IT service provider and their service consumers.

Benefits for service providers include:
- Reduced losses caused by IT service unavailability
- Better image due to uninterrupted IT services
- Fulfilment of the SLAs with service consumers
- Reduced costs of service restoration due to knowledge capture and reuse
- Higher user satisfaction.

Benefits for service consumers include:
- Reduced losses caused by business service unavailability
- Better image due to uninterrupted business services
- Higher client and employee satisfaction.

The quick restoration of a service is a key factor in user and customer satisfaction, the credibility of the service provider, and the value the service provider creates in the service relationships.

2.2 Terms and concepts

Incident

An unplanned interruption to a service or reduction in the quality of a service.

The incident management practice ensures that periods of unplanned service unavailability or degradation are minimized, thus reducing negative impacts on users. There are two main factors enabling this: early incident detection and the quick restoration of normal operation.

The quick detection and resolution of incidents is made possible with effective and efficient processes, automation, and supplier relationships alongside skilled and motivated specialist teams. Resources from the four dimensions of service management are combined to form the incident management practice.

2.2.1 Incident models

Some systems and services demonstrate patterns of operations that include so-called typical incidents. These may be associated with known errors, such as a lack of compatibility or patterns of incorrect user behaviour. Service providers benefit from defining incident models to optimize the handling and resolution of repeating or similar incidents. Incident models help to resolve incidents quickly and efficiently, and often with better results, due to the application of proven and tested solutions.

Incident model

A repeatable approach to the management of a particular type of incident

The creation and use of incident models are important activities in the incident management practice. They are described further in chapter 3.

2.2.2 Major incidents

Although some incidents have a relatively low impact on service operation and on work of users, others may lead to dramatic consequences for service consumers and the service provider. These are called major incidents and require special attention

Major incident

An incident with significant business impact, requiring an immediate coordinated resolution.

A significant business impact is not the only characteristic of a major incident. Major incidents are often associated with a higher level of complexity. Many systems and services are designed for high availability, and single failures are unlikely to cause a significant business impact. Failures in these systems are quickly, and often automatically, detected and fixed. However, if multiple seemingly trivial events coincide, they may lead to a major disruption of multiple services and have a high impact on service consumers. Complex incidents such as this require a special approach to management and resolution.

It is recommended to implement a model to manage all major incidents, even though major incidents rarely recur and usually differ in nature. A model for major incidents typically includes:
- clear criteria to distinguish major incidents from disasters and other incidents
- a special accountable coordinator, sometimes referred to as the major incident manager (MIM)
- a dedicated temporary team created to investigate and resolve a major incident
- other dedicated resources (including budget), for example, for urgent consultations with third- party experts or procurement of components
- special methods of investigation (for example, swarming: see section 2.4.2)
- an agreed model of communications with users, customers, regulators, media, and other stakeholders
- an agreed procedure for review and follow-up activities.

2.2.3 Workarounds

Workaround

A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Some workarounds reduce the likelihood of incidents.

Sometimes, it may be impossible to find a systemic solution for an incident. In these situations, service providers may apply a workaround.

Workarounds promptly restore the service to an acceptable quality. However, workarounds can increase technical debt and may lead to new incidents in the future. The problem management practice can be used to reduce the technical debt created by incident workarounds. In many cases, understanding the cause or causes of an incident can help find an optimal solution.

Technical debt

The total rework backlog accumulated by choosing workarounds instead of systemic solutions that would take longer.

2.3 Scope

The scope of the incident management practice includes:
- detecting and registering incidents
- diagnosing and investigating incidents
- restoring the affected services and configuration items to an agreed quality
- managing incident records
- communicating with relevant stakeholders throughout the incident lifecycle
- reviewing incidents and initiating improvements to services and to the incident management practice after resolution.

There are a number of activities and areas of responsibility that are not included in the incident management practice, although they are closely related to it. These activities are listed in Table 2.1, along with references to the practice guides in which they can be found. Management practices should be combined to form service value streams, as described in section 3.2

Table 2.1 Activities related to the incident management practice described in other practice guides

Activity	Practice guide
Investigating causes of incidents	Problem management
Communicating with users	Service desk
Implementation of changes to products and services	Change enablement Deployment management Infrastructure and platform management Project management Release management Software development and management
Monitoring technology, teams, and supplier performance	Monitoring and event management
Management of improvement initiatives	Continual improvement
Management and fulfilment of service requests	Service request management
Restoring normal operations in case of a disaster	Service continuity management

2.4 Practice success factors

Practice success factor

A complex functional component of a practice that is required for the practice to fulfil its purpose.

A Practice Success Factor (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 PSF's within a practice may differ, but together they ensure that the practice is effective.

The incident management practice includes the following PSF's:
- detecting incidents early
- resolving incidents quickly and efficiently
- continually improving incident management.

2.4.1 Detecting incidents early

Previously, it was a common practice to register most incidents based on information from end users and IT specialists. This method of sourcing information is still widely used, but good practice currently suggests detecting and registering incidents automatically wherever possible. This can be done immediately after incidents occur and before they start affecting users. This approach has multiple benefits:
- Earlier incident detection decreases the time of the service unavailability or degradation, which in turn decreases the losses and other negative business impact caused by incidents.
- The higher quality of the initially collected data supports the correct response to and resolution of incidents, including automated resolution, also known as self-healing.
- Some incidents remain invisible to users, improving user satisfaction and customer satisfaction.
- Some incidents may be resolved before they affect the service quality agreed with customers, improving the perceived service and the reported service quality
- Costs associated with incident management may decrease.

Early detection of incidents is enabled by the monitoring and event management practice. This includes tools and processes for event categorization that distinguish incidents from other types of events.

Automatically detected incidents can be classified either automatically, manually, or with partial automation. A partially automated categorization is made manually but is based on suggestions made by the system. Automated incident detection and categorization may benefit from machine learning solutions, using the data available from past incidents, events, known errors, and other sources. See section 3.1.1 for more details on incident classification.

When automated incident detection is not possible, incidents are usually detected when they have already impacted users and their work. Even then, the earlier an incident is reported and registered, the better. This can be achieved by promoting a culture of responsible service consumption among users that includes encouraging reporting of suspicious events and behaviour, and tolerating false reports, within reason.

2.4.2 Resolving incidents quickly and efficiently

This PSF is vital for the success of the incident management practice and for general service quality. After incidents are detected, they should be handled effectively and efficiently, considering the complexity of the environment:
- In clear situations, such as recurring and well-known incidents, pre-defined resolution procedures are likely to be effective. These may include automated resolution or standardized routing and handling (according to an appropriate pre-agreed incident model).
- In complicated situations, where the exact nature of the incident is unknown but the systems and components are familiar to the support teams and the organization has access to expert knowledge, incidents are usually routed to a specialist group or groups for diagnosis and resolution. Sometimes this can assist in identifying patterns and lead to a model and/or a solution which can be applied to similar incidents in the future.
- In complex situations, where it is difficult or impossible to define an expert area and group, or where defined groups of experts fail to find a solution, a collective approach may be useful. This technique is known as swarming.

Swarming

A technique for solving various complex tasks. In swarming, multiple people with different areas of expertise work together on a task until it becomes clear which competencies are the most relevant and needed.

Usually, swarming assists in decreasing the level of complexity and makes it possible to switch to the techniques used in a complicated or clear situations. One example where swarming is particularly relevant are major incidents of an unknown nature. In these situations, pulling together numerous specialized resources is cost-effective compared to the losses resulting from the incident remaining unsolved.

Physical meetings are not required when swarming. When a plan is established, experts may work alone to run experiments, perform analysis, and use other tools to discover what is happening. To engage with the incident, swarming utilizes the correct people rather than a great amount of people. It is usual to involve people from different teams in swarming, this requires organizational solutions which allow involving team members on a very short notice.

Other techniques can be used in complex situations. For example, expert analysis may be replaced or combined with a series of safe-to-fail experiments which aim to improve the understanding of the nature of the incident. Adopting and utilizing a customarily based framework for decision-making[1] is useful for dealing with incidents in situations of high and changing complexity.

As mentioned in section 2.2.1, some incidents recur and can be handled in a well-known, repeatable way. Ideally, such recurrences should be analysed and further repetition prevented (this usually involves the problem management practice). However, problem management may take significant time, and some incident, even if well-understood, cannot be effectively prevented. Their occurrence and nature are clear, and their handling often can follow a well-defined incident model. To optimize the time and resources for resolution of such incidents, the shift left approach can be used.

Shift-left approach

An approach to managing work that focuses on moving activities closer to the source of the work, in order to avoid potentially expensive delays or escalations. In a software development context, a shift-left approach might be characterized by moving testing activities closer to (or integrated with) development activities. In a support context, a shift-left approach might be characterized by providing self-help tools to end-users.

In incident management, shift-left can be used to delegate more activities to users: not only reporting an incident, but also self-help using chat bots, FAQ pages and other resources. Another form of shift-left is training of the service desk agents to diagnose and solve more different types of incidents. Any opportunity to solve incidents without transferring them to other teams should be used, especially as the transfer is likely to take extra time and cost extra money. This should not, however, create unacceptable delays; the speed of incident resolution remains the most important requirement. The shift-left approach works best in clear, well-known situations, where less experienced people can successfully follow well-tested and safe instructions.

Regardless of the complexity, it is important to review and confirm the high quality of the incident data from the first steps of incident handling. This has a strong influence on the:
- correctness of the decisions made
- speed of service recovery
- effective use of resources
- ability to find and remedy the underlying cause(s)
- possibility and quality of machine learning.

2.4.1 Incident prioritization

Incidents should be resolved as soon as possible. However, the resources of the teams involved in incident resolution are limited and these teams are often simultaneously involved in other types of work. Some incidents should be prioritized over others to minimize negative impacts on users and optimize the use of resources.

Prioritization

An action of selecting tasks to work on first when it is impossible to assign resources to all tasks in the backlog.

Task priority

The importance of a task relative to other tasks. Tasks with a higher priority should be worked on first. Priority is defined in the context of all the tasks in a backlog.

There are a number of simple guidelines for prioritization which apply to all types of tasks, including incidents:
- Prioritization is a tool for assigning tasks to people in the context of a team. If an incident is handled by multiple teams, it will be prioritized within each team depending on resource availability, target resolution time, and estimated processing time. If resolution of an incident requires several tasks to be performed by different teams working in parallel, each team will be prioritizing their own task.
- Prioritization is needed only when there is a resource conflict. Where there are sufficient resources to process every task within the time constraints, prioritization is unnecessary.
- In each team, all types of tasks (including incidents) should await prioritization and assignment in a single backlog, together with other tasks (planned and unplanned).
- Visualization tools, such as Kanban, and Lean principles, such as the limiting of work in progress, are useful for effective prioritization.

These rules apply to all types of work, whether planned or unplanned, performed by the service provider's specialist teams. It is important that they are agreed and followed by everyone involved in the organization's service management activities, across all practices. Specific to incident management, the following additional recommendations should be considered.
- Evaluation of the impact and urgency of an incident is performed during the incident classification (see section 3.1.1). This evaluation and the related time constraints for its investigation and resolution (often guided by a service level agreement) is NOT prioritization. However, this evaluation provides important input for prioritization.
- Resource availability and estimated processing time are defined by each team. For well-known repeating operations, the processing time may be standardized. The target resolution time may be defined by SLAs and/or the internal service specifications of the service provider. The impact assessment and completion (resolution) time may change as support teams discover new information.

2.4.3 Continually improving incident management

Periodic reviews of incidents should be conducted to improve the effectiveness and efficiency of the incident management practice. Some incidents will require an individual review upon resolution. This usually applies to major incidents, new types of incidents, and incidents that were not resolved on time. Most incidents, however, do not require an individual review beyond confirming their successful resolution. Nonetheless, an overview of the incident management records at certain intervals will help to identify positive experiences and room for improvement, share knowledge between specialist teams, identify new types of incidents, and improve or introduce incident models.

Periodic reviews provide an opportunity to analyse the stakeholders' satisfaction with the incident management practice. Periodic incident review is also key for the continual improvement of the practice and the organization's products and services.

Key message

The importance of data

Effective reviews will always need data; therefore, it is important to agree the requirements for documenting it. Data should be:
- **Concurrent:** It is useful to know exactly what was done when, to assist in continual improvement. This requires stakeholders to update incident records during, not after, the event. Also, an accurate timeline may be useful for investigating the problem.
- **Complete:** A considerable amount of activity can be hidden behind a simple statement. For example, a statement such as 'We restarted the cluster and normal function was observed after 45 minutes' may hide useful detail. It could mean: 'We restarted Server 1, then 2, then 3 and found that Server 4, which was operating normally, stopped. We checked the manual and restarted Servers 2 and 4, then 1 and 3. All were processing data correctly after 10 minutes'.
- **Comprehensive:** Describing why an action was taken can be just as important as describing the action itself.

2.5 Key metrics

Key metrics for the incident management practice are mapped to its PSFs. The key metrics are listed in Table 2.2.

The practice metrics should be applied to a specific context such as type of incident, services, specialist groups, or periods of time.

The effectiveness and performance of the ITIL practices should be assessed within the context of the value streams to which the practices contribute. The context of the business and the value streams is important to define what is considered good or not so good performance of a practice. This is why this practice guide cannot recommend universal key performance indicators for incident management: the target values for each metric can only be defined in the organization's context.

Table 2.2 Key metrics for incident management

Practice success factors	Key metrics
Detecting incidents early	Time between incident occurrence and detection Percentage of incidents detected via monitoring and event management
Resolving incidents quickly and efficiently	Time between incident detection and acceptance for diagnosis Time of diagnosis Number of reassignments Percentage of waiting time in the overall incident handling time First-time resolution rate Meeting the agreed resolution time User satisfaction with incident handling and resolution Percentage of the incident resolved automatically Percentage of incidents resolved before being reported by users
Continually improving incident management	Percentage of incident resolutions using previously identified and recorded solutions Percentage of incidents resolved using incident models Improvement of the key practice indicators over time Balance between the speed and effectiveness metrics for incident resolution

[1] https://thecynefin.co/about-us/about-cynefin-framework/

Chapter 3
Value streams and processes

3.1 Processes

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

Process

A set of interrelated or interacting activities that transform inputs into outputs. A process takes one or more defined inputs and turns them into defined outputs. Processes define the sequence of actions and their dependencies.

Incident management activities form two processes:

- **Incident handling and resolution:** This process is focused on the handling and resolution of individual incidents, from detection to closure.
- **Periodic incident review:** This process ensures that the lessons from incident handling and resolution are learned and that approaches to incident management are continually improved.

3.1.1 Incident handling and resolution

This process includes the activities listed in Table 3.1, and transforms the inputs into outputs.

Table 3.1 Inputs, activities, and outputs of the incident handling and resolution process

Key inputs	Activities	Key outputs
Monitoring and event data User queries Configuration information IT asset information Service catalogue SLAs with consumers and suppliers/partners Capacity and performance information Continuity policies and plans Information security policies and plans Problem records Knowledge base	Incident detection Incident registration Incident classification Incident diagnosis Incident resolution Incident closure	Incident records Incident status communications Problem investigation requests Change requests Incident reports Updates to the knowledge base Restored CIs and services

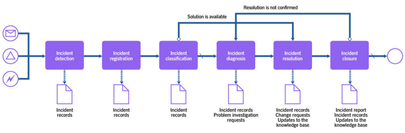


Figure 3.1 Workflow of the incident handling and resolution process

Throughout the process, ownership over each incident should be ensured. The ownership may be transferred via the handling and resolution process, but each incident should have a person responsible for it at any time. Also, stakeholder communications should be updated whenever there are changes in the status of the incident.

The process may vary significantly, depending on the incident model. Table 3.2 provides descriptions of the activities in two incident models (manual and automatic), which are just two of many options. They are meant to illustrate the difference between incident models.

Table 3.2 Activities of the incident handling and resolution process

Activity	Manually processed user-detected incidents	Automatically detected and processed incidents
Incident detection	A user detects a malfunction in service operation and contacts the service provider's service desk through the agreed channel(s). A service desk agent performs the initial triage of the user query, confirming that the query does indeed refer to an incident.	An event is detected by a monitoring system and identified as an incident based on a pre-defined classification.
Incident registration	The service desk agent performs incident registration, adding the available data to the incident record.	An incident record is registered and associated with the CI where the event has been detected. Pre-defined technical data is registered. If needed, a notification is sent to the relevant technical specialists.
Incident classification	The service desk agent performs initial classification of the incident: this helps to qualify incident impact, identify the team responsible for the failed CIs and/or services, and to link the incident to other past and ongoing events, incidents, and/or problems. In some cases, classification helps to reveal a previously defined solution for this type of incident.	Based on pre-defined rules, the following is automatically discovered: • the incident's impact on services and users • the solutions available • the technical team(s) responsible for the incident resolution, if automated solutions are ineffective or unavailable.
Incident diagnosis	If classification does not provide an understanding of a solution, technical specialist teams perform incident diagnosis. This may involve transfer of the incident between the teams (also known as functional escalation), or joint techniques, such as swarming. If classification is wrong because of an incorrect CI assignment, this information should be communicated to those responsible for configuration control (see the service configuration practice guide).	If the automated solution is ineffective or unavailable, the incident is escalated to the responsible technical team for manual diagnosis. It may involve transfer of the incident between the teams, or joint techniques, such as swarming. If an automated solution failed because of an incorrect CI association, this information should be communicated to those responsible for the configuration control (see the Service Configuration Official Practice Guide).
Incident resolution	When a solution is found, the relevant specialist teams attempt to apply it, working sequentially or in parallel. It may require the initiation of a change. If the solution does not work, additional diagnosis is performed.	If there is an automated solution available, it is applied, tested, and confirmed. If a manual intervention is required, a relevant specialist team attempts to apply it. It may require the initiation of a change. If the solution proves not to work, additional diagnosis is performed.
Incident closure	After the incident is successfully resolved, several formal closure procedures may be needed: • user confirmation of service restoration • resolution costs calculation and reporting • resolution price calculation and invoicing • problem investigation initiation • incident review. After all the required actions are completed and the incident records are updated accordingly, the incident is formally closed. This can be done by the product owner, service owner, incident manager, or service desk agent, depending on the agreed incident model.	If the automated solution proves effective, incident records are automatically updated and closed. A report is sent to the responsible technical team. If information about the incident has been communicated to other stakeholders at any of the previous steps, the closure of the incident should also be communicated.

3.1.2 Periodic incident review

This process is focused on the continual improvement of the incident management practice, incident models, and incident handling procedures. It is either performed regularly or triggered by incident reports highlighting inefficiencies and other improvement opportunities. Regular reviews may take place every two to three months or more frequently, depending on the effectiveness of the existing models and procedures.

This process includes the activities listed in Table 3.3 and transforms the inputs into outputs.

Table 3.3 Inputs, activities, and outputs of the periodic incident review process

Key inputs	Activities	Key outputs
Current incident models and procedures Incident records Incident reports Policies and regulatory requirements Configuration information IT asset information SLAs with consumers and suppliers/partners Capacity and performance information Continuity policies and plans Security policies and plans	Incident review and incident records analysis Incident model improvement initiation Incident model update communication	Updated incident models Updated incident handling procedures Incident records Communications about updated incident models and procedures Change requests improvement initiatives Incident review reports

Figure 3.2 shows a workflow diagram of the process.

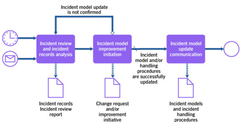


Figure 3.2 Workflow of the periodic incident review process.

Table 3.4 Activities of the periodic incident review process

Activity	Description
Incident review and incident records analysis	The incident manager, together with service owners and other relevant stakeholders, performs a review of selected incidents such as major incidents, those not resolved in time, or all incidents over a certain period. They identify opportunities for incident model and incident handling procedures optimization, including the automation of incident processing and resolution.
Incident model improvement initiation	The incident manager registers the improvement initiatives to be processed with the involvement of the continual improvement practice or initiates a change request (if incident models, procedures, and automation are included within the scope of the change enablement practice).
Incident model update communication	If the incident model is successfully updated, it is communicated to the relevant stakeholders. This is usually done by the incident manager and/or the service or resource owner.

3.2 Value stream contribution

3.2.1 Service value streams

To perform certain tasks or respond to particular situations, organizations create service value streams. These are specific combinations of activities and practices, and each one is designed for a particular scenario. Once designed, value streams should be subject to continual improvement.

Value stream

A series of steps an organization undertakes to create and deliver products and services to consumers.

In practice, however, many organizations come to use of the value stream concept after having worked for a while (sometimes for years) without the value streams being managed, mapped, or understood. This means that when the importance of the concept becomes clear, the first step is to understand and map the 'As Is' situation, the de-facto flows of work, and to analyse them in order to identify and eliminate the non-value-adding activities and other forms of waste.

Identifying and understanding the existing value streams is critical to improving organization's performance. Structuring the organization's activities in the form of value streams allows it to have a clear picture of what it delivers and how, and to make continual improvements to its services. Combined, organizations' value streams form an operating model which can be used to understand and improve how the organization creates value for the stakeholders.

Many organizations have been following best practice recommendations for various service management practices, such as incident management, change enablement, software development, and many others. Incident management is one of the most adopted and mature practices, organizations often start their ITSM journey with incident management.

However, the practices have often been adopted and organized in a siloed, isolated manner, just as they were presented in the service management bodies of knowledge. In reality, a flow of work required to create or restore value, for a customer or another stakeholder, is almost never limited to one practice.

3.2.2 Incident management in service value streams

3.2.2.1 The incident resolution value stream

The incident management practice is not enough to restore normal service after it has been interrupted. The real-life workflow may include the activities outlined in table 3.5, which are described as parts of different practices.

Table 3.5 Management practices in the incident resolution value stream

Activity	Practice
Incident detection	Service desk (for user-reported incidents) or Monitoring and event management
	Incident management
Incident registration	**Incident management**
Incident classification	
Incident diagnosis	**Incident management** Knowledge management Problem management
Incident resolution	**Incident management and one or more of:** Problem management Change enablement Software development and management Service validation and testing Deployment management Release management Service desk Infrastructure and platform management Supplier management
Incident closure	**Incident management** Service desk Monitoring and event management Problem management Knowledge management Relationship management

The incident management practice is core for this value stream, but it is not enough to complete the value stream and restore value co-creation.

ITIL 4 recommends organizations to examine how they perform work and map all the value streams they can identify. This will enable them to analyse their current state and identify any barriers to workflow and non-value-adding activities (waste). Wasteful activities should be eliminated to increase productivity.

Opportunities to increase value-adding activities can be found across the service value chain. These may be new activities or modifications to existing ones, which can make the organization more productive. Value stream optimization may include process automation or adoption of emerging technologies and ways of working to gain efficiencies or enhance user experience.

Value streams should be defined by organizations for all their products and services. Depending on the organization's strategy, value streams can be redefined to react to changing demand and other circumstances, or remain stable for a significant amount of time. In any case, they should be continually reviewed and improved to ensure that the organization achieves its objectives in an optimal way.

3.2.2.2 Incident management in other service value streams

The main and most obvious value stream involving incident management is described in section 3.2.2.1. Unlike most other practices, incident management is rarely involved in other value streams. Incidents occurring in other value streams trigger the value stream to restore normal operation, rather than involve the incident management practice in their own context. For example, if an incident occurs during a new product release, it triggers the value stream to restore normal operation, while the release-related value stream continues, most likely, rolling back the unsuccessful changes. Similarly, if an incident occurs during fulfilment of a service request, it does not involve incident management into the ongoing request fulfilment workflow; instead, it triggers the value stream to restore the normal operation, while the request-related value stream continues or restarts.

However, some organizations come up with operating models where incident management is involved in other value streams. The examples include:

Involving the incident management practice to deal with unplanned events in development, testing, and other pre-live environments. Although these events do not impact live services and don't have a direct business impact, they can be processed using the same or similar processes, competencies, tools and third parties. in other words, the same practice. In most cases, people involved in the related workflows are different from those involved in management of incidents in the live environment.

Separating the restoration value streams for incidents detected by users and incidents detected by monitoring. The former value stream would be initiated by users contacting service desk and focused on restoring the services to an agreed level and to the users' expectations. The latter value stream would be triggered by events captured by the monitoring systems and focused on restoring the components and services to an agreed technical specification, preventing any negative impact on the live services and their users.

There is no single operating model fitting all organizations. Different solutions work for different organizations, involving different value streams which in turn involve different management practices.

3.2.3 Analysing a service value stream

3.2.3.1 The key steps of a service value stream analysis

The following are some simple and practical recommendations for service value stream analysis and mapping.

1. **Identify the scope of the value stream analysis:** It can be mapped to a particular product or service or applied to most or all of them. Similarly, service value streams may differ for different consumers, for example, incidents can be solved and communicated differently for internal and external customers, or for B2B and B2C products, or for services based on products developed inhouse or sourced externally.
2. **Define the purpose of the value stream from the business standpoint:** Make sure the stakeholder's concerns are clearly understood, since they are the ones defining value. In case of incident management, it is usually user who needs to return to normal work as soon as possible; however, there are usually other interested parties. For example, internal users may be unable to provide normal service to a business customer because of the incident, and the value of the value stream should be considered from the business perspective, not solely from the user perspective.
3. **Do the service value stream walk:** Walk through or directly experience the steps and information flow as they go in practice (consider the Lean technique of Gemba walk).
   a. **Identify the workflow steps**
   b. **Collect data as you walk**
   c. **Evaluate the workflow steps:** Typically, the criteria for evaluation are:
      - value for the stakeholder (does the step add value for the business stakeholder?)
      - effectiveness or performance (is the step performed well?)
      - availability (are required resources available to execute the step?)
      - capacity (are required resources enough?)
      - flexibility (are the required resources interchangeable within the step?).
   d. **Map the activities and the information flows:** In an ideal situation, the flow goes smoothly without delays and pauses, there are no disconnections between the steps, and the workload is level with minimal (and agreed) variation.
   e. **Create and review the timeline and resource level:** Map out process times and lead times for resources and workload through the workflow steps.
4. **Reflect on the value stream map (VSM):** Identify factors that might not have been entirely apparent at first. The information collected is used at this step to find the waste.
5. **Create a 'to be' VSM:** This informs and drives improvement. The value stream should be considered holistically to ensure end-to-end efficiency and value creation, not just local improvements.
6. **Using the 'to be' VSM, plan improvements:** Refer to the continual improvement practice guide for a practical improvement model.

3.2.3.2 Incident management considerations in a service value stream analysis

To ensure that relevant incident management activities are included in service value streams, the following steps can be added to the above recommendations.

- At the scoping step (1), identify the IT and business services related to the value stream and the involved business stakeholders. For example, when an IT service provider delivers IT services consumed by business users who in turn provide services to the business clients, should the incident-related service value stream involve restoration of normal business services for the clients, or should it be limited to the restoration of normal IT services for the business users?
- Make sure the value stream is understood (step 2) from the standpoint of the business, not only of the service provider.
- During the service value stream walk (3a), identify other practices involved in dealing with incidents at every step. Which practices provide required information (configuration data, asset data, previously identified solutions, agreed timeline for the service restoration…)? What if the incident resolution requires changes? What if incident diagnosis and/or resolution involves third parties?
- During the workflow steps evaluation (3c), evaluate the step's impact on the value restoration. Special attention should be paid to steps with low business value, low performance, and availability or capacity issues. It is not unusual to find steps which serve some internal control or bureaucratic purposes but delay the incident resolution.
- At the reflection and planning steps (4-5), ensure that the incident management flow is optimized for business value throughout the stream, not only at the incident management practice activities.
- Include creation or update of incident models (see sections 2.2.1 and 3.1.2) in the value stream improvement plans (step 6).

Chapter 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. They focus instead on the specialist roles that are 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 competency profile based on the model shown in Table 4.1.

Table 4.1 Competency codes and profiles

Competency code	Competency profile (activities and skills)
L	**Leader:** Decision-making, delegating, overseeing other activities, providing incentives and motivation, and evaluating outcomes
A	**Administrator:** Assigning and prioritizing tasks, record-keeping, ongoing reporting, and initiating basic improvements
C	**Coordinator/communicator:** Coordinating multiple parties, maintaining communication between stakeholders, and running awareness campaigns
M	**Methods and techniques expert:** Designing and implementing work techniques, documenting procedures, consulting on processes, work analysis, and continual improvement
T	**Technical expert:** Providing technical (subject matter) expertise and conducting expertise-based assignments

4.1.1 Incident manager role

In many organizations, the incident manager role is performed by a dedicated person, sometimes under the incident manager job title. In other organizations, the responsibilities of an incident manager are taken by the person or team responsible for the CI, service, or product with which the incident is associated; this may be the resource owner, service owner, or product owner.

This role is typically responsible for:

- the coordination of incident handling in the organization or in a specific area, such as territory, product, or technology, depending on the organizational design
- coordinating manual work with incidents, especially those involving multiple teams
- monitoring and reviewing the work of teams that handle and resolve incidents
- ensuring sufficient awareness of the incidents and their status across the organization
- conducting regular incident reviews and initiating improvements of the incident management practice, the incident models, and the incident handling procedures
- developing the organization's expertise in the processes and methods of the incident management practice.

In some cases, organizations may introduce an additional role of the major incident manager (MIM). This role has similar responsibilities to the incident manager but focuses exclusively on major incidents. This role becomes the main point of contact and coordination during major incidents. The MIM usually has wider authority and may have dedicated resources for major incident management.

The competency profile for these roles is CMAT, though the importance of each of these competencies varies from activity to activity.

4.1.2 Other roles involved in incident management activities

Examples of other roles which can be involved in incident management activities are listed in Table 4.2, together with the associated competency profiles and specific skills.

Table 4.2 Examples of roles with responsibility for incident management activities

Activity	Responsible roles	Competency profile	Specific skills
Incident handling and resolution process			
Incident detection	Technical specialist User	TC	Understanding of the service design, resource configuration, and business impact of events and symptoms
Incident registration	Incident manager Service desk agent Technical specialist	AT	Good knowledge of IT service management (ITSM) tools and procedures
Incident classification	Incident manager Service desk agent Technical specialist	TC	Understanding of the service design, resource configuration, and business impact Good knowledge of requirements and commitments for incident resolution Good knowledge of incident models
Incident diagnosis	Supplier Technical specialist	TC	Understanding of the service design, resource configuration, and business impact Knowledge of incident models, diagnostic tools, methods Analytical skills
Incident resolution	Supplier Technical specialist User	T	Understanding of methods and procedures required for incident resolution
Incident closure	Incident manager Service desk agent Technical specialist	ACT	Understanding of the service design, resource configuration, and business impact Good knowledge of the requirements and commitments for incident resolution
Periodic incident review process			
Incident review and incident records analysis	Incident manager Product owner Service owner Supplier	TCL	Understanding of the service design, resource configuration, and business impact Good knowledge of the requirements and commitments for incident resolution Knowledge of incident models, diagnostic tools, methods, and analytical skills
Incident model improvement initiation	Incident manager Product owner Service owner	TMC	Understanding of the service design, resource configuration, and business impact Good knowledge of the requirements and commitments for incident resolution Knowledge of incident models, diagnostic tools, and methods Knowledge of the organization's continual improvement and change enablement practices
Incident model update communication	Incident manager Product owner Service desk agent Service owner	CA	Knowledge of communication procedures and tools

4.2 Organizational structures and teams

Organizational structure and the size of organization influences how the incident management practice is performed and how it is integrated in the organization's value streams. Incident management involves specialists with different areas and levels of expertise; these specialists may belong to different organizational teams. Typical methods of grouping specialists include, among others:

- technical domain
- product/service
- territory
- consumer types.

The method of organization will vary, depending on the organization's needs and resources. The incident management practice should take a flexible approach to its organization, involving resources from various internal and external teams as necessary. Either way, it is crucial to ensure effective cooperation between members of different teams involved in handling and resolution of incidents.

4.2.1 Tiered versus flat team structures

Historically, teams working on incidents had a tiered or levelled structure in which competency, expertise, and specialization increased with each level. It aimed to resolve most of the incidents at the lowest level possible to reduce costs. Incidents were transferred to the upper level, or escalated, if they could not be resolved in the current level. In such teams, there were clear boundaries between levels and clear procedures for the escalation of incidents. Unfortunately, such structures can restrain collaboration and information flow, resulting in prolonged resolution time. So, for high-priority incidents, teams collaborate to facilitate speedy resolution.

The expansion of Agile methods and evolution of IT systems (such as self-healing systems) call for the wider use of horizontal team structures, rather than hierarchical team structures. Flatter structures and respective collaboration methods, such as swarming, replace tiered ones to facilitate cooperation and the free flow of information. The main driver of such change is the rejection of rigid tiering and its replacement by a more dynamic, self-organized collaboration.

4.2.2 Team dynamics

The incident management practice is the foundation of team dynamics, because they affect the functioning of the support operation. The following issues regularly recur:

- incidents are bounced between teams
- team members experience a lack of autonomy and report being blocked by others
- a culture prevails where lone 'heroes' are rewarded when incidents are solved.

This leads to numerous negative effects, such as:

- the incident management practice being out of sync
- resolutions happening slowly or not at all
- a decrease in morale
- a lack of motivation
- an unhealthy degree of competitiveness entering the workplace.

Furthermore, trust between team members breaks down. Approaches such as DevOps and techniques such as swarming show some of the characteristics needed to encourage a positive culture, although it is not necessary to follow these approaches to achieve the correct team dynamic. The following three main areas need to be addressed.

4.2.2.1 Collective responsibility

If resolving incidents is the primary responsibility, that is what individuals within the teams will focus on. Team dynamics should come second to achieving the SLA or meeting a deadline. The first step in changing this is to build a culture where team members share successes and failures. Teams that share responsibility may have a single person who sees an incident through to resolution, but they should be encouraged to engage other experienced people in the process. When this occurs, the organization will benefit from a fast restoration of normal service as well as knowledge-sharing.

4.2.2.2 No-blame culture

There should be a no-blame culture within teams, otherwise this will lead to the deterioration of trust between individuals, teams, and suppliers. Incident investigations and reviews need to address incident resolution and service restoration. Incident teams must be encouraged to act without fear of retribution if their idea fails to work. This requires transparency and positive leadership. Mistakes should be treated as shared learning opportunities rather than personal failures.

4.2.2.3 Continual learning

Team members need to share the lessons that they have learned from experimenting so they can learn and improve. This can prove to be a significant cultural leap in many environments, particularly those with a large percentage of outsourcing.

Chapter 5
Information and technology

5.1 Information exchange

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

- customers and users
- architecture and design of services
- partners and suppliers, including contract and SLA information on the services they provide
- policies and requirements which regulate service provision
- stakeholder satisfaction with the practice.

This information may take various forms, depending on the incident models in use. The key inputs and outputs of the practice are listed in chapter 3.

Details of incidents are the most important pieces of information. These usually include:

- sources of information
- a reference to the product, service, or CI that is failing or performing below standard
- the impacted users or services
- the symptoms of the poor performance
- when the symptoms are observed
- the last known time of correct operation before the symptoms began
- whether an automatic fix was applied (and if not, the reason)
- the location, both geographic and virtual
- the nature and extent of the impact on normal operations
- similar systems which might be affected by the poor performance and are currently operating normally
- the sequence of events leading up to the observation of the symptom.

Additional information that will be exchanged and recorded during the incident management practice should include details of:

- the investigation
- every action taken, including the results.

Any actions taken should be documented to produce an accurate timeline. If it is not practical to document actions in real time, the documentation should specify when the action was started and completed to avoid the creation of a false history log. It is preferable, however, to capture real-time actions if the customer can see the information through a portal. Where possible, the registration of actions should be automated.

5.2 Automation and tooling

The incident management practice can significantly benefit from automation. The term automation is used in this and other ITIL publications to refer to the use of digital technology to enable, support, or enhance various activities. This includes, but is not limited to the full automation of activities where technology solutions remove the need for human intervention. Table 5.1 provides a list of the key automation supporting the practice and their most common application.

Table 5.1 Automation solutions for the incident management practice

Automation tools	Application in incident management
Monitoring and event management tools	Detection of incidents Analysis of trends and events during incident diagnosis Confirmation of incident resolution
Workflow management and collaboration tools (including user query ('ticket') management tools)	Management of incident lifecycle Support and automation of incident models Communications between specialists involved in incident handling and resolution Integration of the practices into service value streams
Knowledge management tools	Classification and assignment of incidents, identification of known incident solutions
Service configuration management tools	Incident classification and diagnosis
Classification and analysis tools, including ML-enhanced	Incident classification and analysis
Remote administration, diagnosis, deployment, and other infrastructure and software management tools	Incident diagnosis and resolution
Work planning and prioritization tools	Planning and tracking of improvement initiatives
Analysis and reporting tools	Practice measurement and reporting
Survey tools	Collection of feedback for practice improvement

Detailed descriptions of how these tools support the practice's activities are outlined in Table 5.2.

In some cases, all activities after a particular activity in the incident handling and resolution process can be fully automated using pre-defined scripts and scenarios for specific types of incidents.

Note that automation tools used in the incident management practice could include not only organization-wide tools, which are valid for all incidents, but also some local custom tools and scripts created as a result of a periodic incident review process for specific incident models. Both should be used to drive automation efforts.

Table 5.2 Details of automation of the incident management activities

Process activity	Means of automation	Key functionality	Impact on the effectiveness of the practice
Incident handling and resolution process			
Incident detection	Monitoring and event management tools	Early detection and correlation of incidents, initiating the incident management practice	High
Incident registration	Workflow management and collaboration tools, including user query ('ticket') management tools	Efficient registration of incidents	High
Incident classification	Workflow management and collaboration tools, including user query ('ticket') management tools Knowledge management tools Service configuration management tools Classification and analysis tools	Fast and correct classification and assignment of the incidents, identification of known solutions, identification of major incidents	Very high, especially when the number of incidents is high
Incident diagnosis	Workflow management and collaboration tools, including user query ('ticket') management tools Knowledge management tools Service configuration management tools	Fast and correct definition and testing of hypothesis, effective collaboration of multiple specialists/teams	High, especially when the number of complex incidents requiring manual collaborative efforts is high
Incident resolution	Remote administration, diagnosis, deployment, and other infrastructure and software management tools	Fast correction of the faulty CIs and restoration of the services	High, especially when services are provided in remote locations
Incident closure	Workflow management and collaboration tools, including user query ('ticket') management tools	Fast and comprehensive overview of the incident lifecycle	Medium
Periodic incident review process			
Incident review and incident records analysis	Analysis and reporting tools Workflow management and collaboration tools Survey tools	Remote collaboration, incident data analysis, and users survey data analysis and reports	Medium to high, especially for high volumes of incidents
Incident model improvement initiation	Workflow management and collaboration tools	Registration and tracking of the improvement initiatives	Low to medium
Incident model update communications	Workflow management and collaboration tools	Communicating updates to the relevant teams	Medium to high, especially when organization is large, and number of updates is high

5.2.1 Recommendations for automation of incident management

The following recommendations can help when applying automation to incident management:

- **Automate the value stream:** Although incident management is often one of the first practices to be developed by a service provider, the implementation of ITSM automation systems also often starts with the incident management processes. Even if other practices may not be mature at this stage, it is important to define requirements and design workflows that will support the full value stream, from detection, to resolution of incidents. For incident resolution that requires changes, the automation tool should allow for a simple change tracking workflow; for recuring incidents, it should be possible to capture and reuse of proven solutions. Think and work holistically.
- **Allow different workflows for user- and event- initiated incidents:** Detection, classification, communications, and conditions for closing a record are all handled differently for user-initiated and event-initiated incidents, even if the latter are handled manually. Attempts to fit both types of incidents in one workflow with the same forms and business logic are unlikely to be successful. The handling of event-generated incidents can and should be automated.
- **Do not overcomplicate the workflows and business rules:** Forms filled in manually should be user-friendly and should not take much time to fill in. When designing user journeys and interfaces, treat IT support teams as you would treat external users whose expectations are based on their experience with mobile apps and modern web sites.
- **Pay attention to measurement and reporting from the beginning:** Incident management is a high-load practice, and it is not possible to monitor the status of incidents and the performance of the practice without a convenient dashboard; it is impossible to understand the trends and to analyse the work of teams without a flexible reporting engine. The popular statement 'you cannot manage what you don't measure' is not always true, but it certainly applies to large amounts of data, and the incident management practice generates large amounts of data.
- **Allow for swarming and other forms of cross-team collaboration:** Some incident management tools are designed for a linear flow and transfer of incident records between the teams. When a joint action is required, it is often unsupported; specialists meet and work together, but the incident records do not reflect it. Design the tool for collaborative and non-linear workflows.
- **Communications are important:** Informing people about incidents, both on the service consumer side and within the service provider, is a crucial part of incident management. Relevant and proactive communications significantly reduce work duplication and optimize the resources of the incident management and service desk practices.
- **Leverage machine learning capabilities:** Incident detection, matching, classification and prioritization can be enhanced or fully automated using machine learning. Effective use of machine learning requires high-quality data and effective integration with various sources of information. If used properly, it can significantly improve the incident management practice.

Chapter 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 ITIL® Foundation: ITIL 4 Edition for a model of a service relationship). Relationships and dependencies introduced by supporting services are described in the practice guides for service design, architecture management, and supplier management.

Partners and suppliers may support the development, management, and execution of the incident management practice. The forms of support include the following:

- **Performing incident management activities:** Some incident management activities can be largely or completely performed by a specialized supplier. Third parties are often involved in incident diagnosis and resolution, and sometimes in other activities. It is important to ensure effective integration of the third parties in the incident-related workflows and information exchange, as well as their adherence to relevant policies. Incident models should define how third parties are involved in incident resolution and how the organization ensures effective collaboration. This will depend on the architecture and design solutions for products, services, and value streams. Nonetheless, the optimization of incident models supporting these solutions will involve the incident management practice. Generally, after the correct model is selected for an incident, further consideration of third-party dependencies is needed during incident diagnosis, resolution, and review. Defined standard interfaces may become an easy way to communicate the necessary conditions and requirements for a supplier to become a part of the organization's ecosystem. Such interface description may include rules of data exchange, tools, and processes that will create a common language in the multi-vendor environment. Where organizations aim to ensure fast and effective incident resolution, they usually try to agree close cooperation with their partners and suppliers, removing formal bureaucratic barriers in communication, collaboration, and decision-making (see the supplier management practice guide for more information).
- **Provision of software tools:** Most software tools used for incident management are shared with other practices. However, implementation and use of integrated service management information systems often starts with automating incident management (and service desk) activities. In this case, the owner of the incident management practice and the managers of the teams involved in incident management should define requirements and interact with other teams and practices of the service provider to ensure that the required tools are procured, implemented, and used in an optimal way.
- **Consulting and advisory:** Specialized suppliers who have developed expertise in incident management can help establish and develop practices, adopt methods and techniques (such as swarming), and initially develop incident models.

Chapter 7
Capability assessment and development

7.1 The practice capability levels

The practice success factors described in section 2.4 cannot be developed overnight. ITIL maturity model defines the following capability levels applicable to any management practice:

Level 1 The practice is not well organized; it's performed as initial or intuitive. It may occasionally or partially achieve its purpose through an incomplete set of activities.

Level 2 The practice systematically achieves its purpose through a basic set of activities supported by specialized resources.

Level 3 The practice is well defined and achieves its purpose in an organized way, using dedicated resources and relying on inputs from other practices that are integrated into a service management system.

Level 4 The practice achieves its purpose in a highly organized way, and its performance is continually measured and assessed in the context of the service management system.

Level 5 The practice is continually improving organizational capabilities associated with its purpose.

For each practice, the ITIL maturity model defines criteria for every capability level from level two to level five. These criteria can be used to assess the practice's ability to fulfil its purpose and to contribute to the organization's service value system.

Each criterion is mapped to one of the four dimensions of service management and to the supported capability level. The higher the capability level, the more comprehensive realization of the practice is expected. For example, criteria related to the practice automation are typically defined at levels 3 or higher because effective automation is only possible if the practice is well defined and organized.

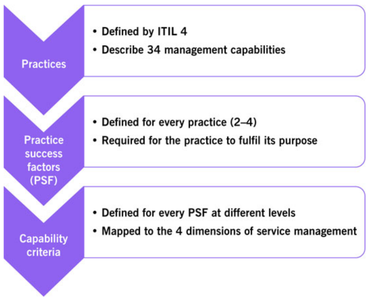


Figure 7.1 Design of the capability criteria

This approach results in every practice having up to 30 capability criteria based on the practice PSFs and mapped to the four dimensions of service management. The number of criteria at each level differs; the four dimensions are comprehensively covered starting from level 3, so this level typically has more criteria than others.

Table 7.1 outlines the capability criteria that are defined in the ITIL maturity model for the incident management practice.

Table 7.1 Incident management capability criteria

PSF	Criterion	Dimension	Capability level
Detecting incidents early	Incidents are usually detected immediately after they occur	Value streams and processes	2
	Incident detection is automated, where relevant	Information and technology	2
	The users and other relevant stakeholders know how to report incidents and report them as soon as possible	Organizations and people	2
	Incident detection is integrated into the relevant value streams	Value streams and processes	3
	Third-party incidents are detected and reported as soon as possible	Partners and suppliers	3
	Information about detected incidents is traced and managed in an integrated information system	Information and technology	3
	The effectiveness of incident detection is measured and reported	Value streams and processes	4
	The effectiveness of incident detection is regularly reviewed and continually improved	Value streams and processes	5
Resolving incidents quickly	Incidents are usually resolved in the quickest possible way	Value streams and processes	2
	Incidents are usually resolved within the agreed target resolution times	Value streams and processes	2
	The resolution of incidents is standardized, where relevant	Value streams and processes	3
	The resolution of incidents is automated, where relevant	Information and technology	3
	The competencies required to resolve incidents are identified and skilled human resources are available	Organizations and people	3
	The third-party dependencies affecting incident resolution are identified and third-party resources are available, where relevant	Partners and suppliers	3
	Information about incident resolution is tracked and managed in an integrated information system	Information and technology	3
	Incident resolution is optimized for the complexity of the environment	Value streams and processes	4
	Incident resolution is integrated into the relevant value streams	Value streams and processes	4
	The effectiveness of incident resolution is measured and reported	Value streams and processes	4
	The effectiveness of incident resolution is regularly reviewed and continually improved	Value streams and processes	5
Continually improving incident management	The approach to incident management is defined, discussed, and agreed at the relevant level of the organization	Value streams and processes	3
	The responsibility for the approach to incident management is clearly defined	Value streams and processes	3
	The competencies required for performing the incident management are identified and skilled human resources are available	Organizations and people	3
	The incident management approach is integrated with other standards and approaches adopted by the organization	Value streams and processes	4
	The effectiveness of the incident management approach is measured and reported	Value streams and processes	4
	The incident management approach is regularly reviewed and continually improved	Value streams and processes	5

These capability criteria can be used by organizations for self-assessment and improvement of the practice.

7.2 Capability self-assessment

The self-assessment can be conducted by the service provider's internal audit team, if the service provider has one, or by the respective team of the parent organization. If there is no specialized team in the organization, the assessment can be done by a team of practice owners and managers responsible for other management practices of the service provider, or a mixed team of the service provider's executive leaders and managers.

To perform a quick self-assessment using the capability criteria, the following rules should be followed.

1. Start with the level 2 criteria. Based on the knowledge of your organization, answer the question, 'Is this a valid description of our organization in MOST cases?'
2. If the answer to the question above is 'yes', make a list of at least three types of material evidence that could prove the answer. These can be records, documents, interviews with business stakeholders, or service provider's employees.
3. If the answer is 'yes' to all criteria of level 2, this level is considered achieved. Proceed to the criteria of level 3.
4. If not all criteria of level 2 are met, the practice is considered to be at level 1. Focus on the criteria that are not met; what is missing in the organization? Why? How can it affect the service consumer and the quality of the IT services? What can be done to meet the criteria that are currently missed?
5. The same approach is applied at every next level; the practice is considered to be at the level, where all criteria are met. It is important to focus on the missing capabilities and improvement opportunities, rather than on a formal achievement of a high capability level.

7.3 Incident management capability development

Management practices should support achievement of the organization's objectives and enable creation of value for the stakeholders. Depending on the service provider's strategy, positioning, and business and operating models, some practices may be more important and therefore require a higher level of capability. There is no organization that requires all management practices to be at the capability level 5. Higher capability level provides higher assurance of the fulfilment of the practice's purpose, but it comes with a cost; cost of management, automation, and training, for example. To achieve optimal performance with sufficient level of assurance, organizations should define a target capability level for each management practice.

Figure 7.2 and table 7.2 show the capability development model, which can be applied to every management practice. The structure of this publication is aligned with the development steps.

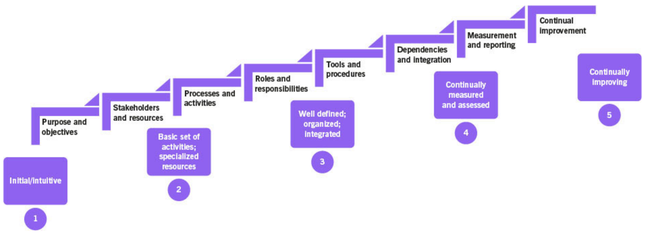


Figure 7.2 The capability development steps and levels

Table 7.2 The incident management capability development steps

Capability level	Define, agree, and implement	Comment for incident management	Chapter (for recommendations)
2	Purpose and objectives	Key stakeholder groups; types of incidents	2.1
	Scope		2.3
	Processes and activities	Workflows; incident prioritization; roles and responsibilities; automation and information exchange	3
	Roles and responsibilities		4
	Tools and procedures		5
3	Dependencies and integration	use of Integrated information system	5
		Suppliers and other parties involved in incident management	6
4	Measurement and reporting	Metrics	2.5
5	Continual improvement	Regular review of practice and the incident management capability development	2.4, 2.5, 7

Chapter 8
Recommendations for practice success

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. When using the content of the 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 ITIL® Foundation: ITIL 4 Edition.

Table 8.1 outlines recommendations for the success of the incident management practice, linked to the relevant guiding principles.

Table 8.1 Recommendations for the success of incident management

Recommendation	Comments	ITIL guiding principles
Look at the incidents from the service consumer perspective	For user-reported incidents, do not hide behind SLAs, aim to restore level of service which satisfies the users. For monitoring-based incidents, assess business impact even if there are no directly affected users yet. Prioritize incidents according to their business impact.	Focus on value Collaborate and promote visibility
Gather and reuse data	Many incidents recur. Significant time and resources can be saved by developing incident models and reusing known resolutions. Do not rely on individuals' experience, motivate team members to document and share their knowledge. Leverage automation tools to manage knowledge and to automate solutions, where possible.	Collaborate and promote visibility Optimize and automate
Understand, manage and improve the incident resolution value stream, not only the incident management practice	Incident lifecycle spans beyond one practice. Ensure effective integration with service desk, change enablement, problem management, and other relevant practices.	Think and work holistically Focus on value
Develop the practice continually but don't overcomplicate it	Start with the most critical products and services and with basic workflow from detection to resolution. Gradually increase both the scope and the capability level based on the business requirement and stakeholder feedback. Use the capability criteria and continual improvement model as a guidance.	Start where you are Progress iteratively with feedback Keep it simple and practical
Adjust for complexity	Shift left and automate handling and resolution of repeating clear incidents. Use swarming to optimize resolution of unusual, complex, and major incidents.	Optimize and automate Collaborate and promote visibility
Demonstrate business value	Measure the practice and produce regular reports and dashboards for internal (within the service provider) and external (service consumer) stakeholders. Use dashboards for the current status and regular reports for analysis and highlights.	Focus on value Collaborate and promote visibility

Glossary

four dimensions of service management

The four perspectives that are critical to the effective and efficient facilitation of value for customers and other stakeholders in the form of products and services.

incident

An unplanned interruption to a service or reduction in the quality of a service.

incident model

A repeatable approach to the management of a particular type of incident.

information and technology

One of the four dimensions of service management. It includes the information and knowledge used to deliver services, and the information and technologies used to manage all aspects of the service value system.

ITIL continual improvement model

A model which provides organizations with a structured approach to implementing improvements.

ITIL guiding principles

Recommendations that can guide an organization in all circumstances, regardless of changes in its goals, strategies, type of work, or management structure.

ITIL maturity model

A tool that organizations can use to objectively and comprehensively assess their service management capabilities and the maturity of their service value system.

ITIL service value chain

An operating model for service providers that covers all the key activities required to effectively manage products and services.

major incident

An incident with significant business impact, requiring an immediate coordinated resolution.

metric

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

organization

A person or a group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives.

organizations and people

One of the four dimensions of service management. It ensures that the way an organization is structured and managed, as well as its roles, responsibilities, and systems of authority and communication, is well defined and supports its overall strategy and operating model.

output

A tangible or intangible deliverable of an activity.

partners and suppliers

One of the four dimensions of service management. It encompasses the relationships an organization has with other organizations that are involved in the design, development, deployment, delivery, support, and/or continual improvement of services.

practice

A set of organizational resources designed for performing work or accomplishing an objective. These resources are grouped into the four dimensions of service management.

practice success factor

A complex functional component of a practice that is required for the practice to fulfil its purpose.

prioritization

An action of selecting tasks to work on first when it is impossible to assign resources to all tasks in the backlog.

process

A set of interrelated or interacting activities that transform inputs into outputs. A process takes one or more defined inputs and turns them into defined outputs. Processes define the sequence of actions and their dependencies.

service provider

A role performed by an organization in a service relationship to provide services to consumers.

service provision

Activities performed by an organization to provide services and/or supply goods. Service provision includes:

- management of the provider's resources, configured to deliver the service
- ensuring access to these resources for users
- fulfilment of the agreed service actions
- service level management and continual improvement.

service relationship

A cooperation between a service provider and service consumer. Service relationships include service provision, service consumption, and service relationship management. Relationships can be basic, cooperative or collaborative (also known as a partnership).

service value system

A model representing how all the components and activities of an organization work together to facilitate value creation.

shift-left approach

An approach to managing work that focuses on moving activities closer to the source of the work, in order to avoid potentially expensive delays or escalations. In a software development context, a shift-left approach might be characterized by moving testing activities closer to (or integrated with) development activities. In a support context, a shift-left approach might be characterized by providing self-help tools to end-users.

stakeholder

A person or organization that has an interest or involvement in an organization, product, service, practice, or other entity.

supplier

A stakeholder responsible for providing services that are used by an organization.

swarming

A technique for solving various complex tasks. In swarming, multiple people with different areas of expertise work together on a task until it becomes clear which competencies are the most relevant and needed.

task priority

The importance of a task relative to other tasks. Tasks with a higher priority should be worked on first. Priority is defined in the context of all the tasks in a backlog.

technical debt

The total rework backlog accumulated by choosing workarounds instead of systemic solutions that would take longer.

user

A person who uses services.

value

The perceived benefits, usefulness, and importance of something.

value stream

A series of steps an organization undertakes to create and deliver products and services to consumers.

value streams and processes

One of the four dimensions of service management. It defines the activities, workflows, controls, and procedures needed to achieve the agreed objectives.

workaround

A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Some workarounds reduce the likelihood of incidents.

Index