

ITIL® 4 Create, Deliver & Support




Module 3 Study Guide



Welcome to your Study Guide

This document is supplementary to the information available to you online. You can use it to study offline, to print out and to annotate key points as part of your studies.

Study Guide Icons

	Tip	This will remind you of something you need to take note of or give you some exam guidance.
	Definition	Key concept or term that you need to understand and remember.
	Role	Job title or responsibility.
	Purpose or Objective	For a process, practice or activity.

IP and Copyright Information

© IT Training Zone Ltd. and AXELOS Limited 2020. All rights reserved

ITIL® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited.

All rights reserved. The Swirl logo™ is a trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.

Text in "*italics and quotation marks*" source: ITIL 4 Foundation Manual, Create, Deliver and Support, Drive Stakeholder Value, High Velocity IT, Direct, Plan and Improve & Practice Guides. Copyright AXELOS Limited 2020. Material is reproduced under license from AXELOS Limited. All rights reserved.

Contents

Welcome to your Study Guide.....	1
Study Guide Icons	1
1 Module 3 – Value Streams for User Support	4
2 Lesson 1: Value Streams for User Support Overview.....	5
3 Lesson 2: Practices that Contribute to a Value Stream for User Support	8
3.1 Scenario for User Support	8
4 Lesson 3 - Service Desk	11
4.1 Purpose and Description	11
4.2 Service Empathy.....	12
4.3 Practice Success Factors (PSFs)	13
4.3.1 Communication Channels.....	13
4.3.2 Integration to Value Streams	15
5 Lesson 4: Incident Management.....	16
5.1 Purpose and Description	16
5.2 Terms and Concepts.....	17
5.3 Practice Success Factors (PSFs)	19
5.3.1 Detect Incidents Early	19
5.3.2 Resolve Quickly	20
5.4 Continually Improve.....	22
5.5 Incident Handling and Resolution	23
6 Lesson 5 – Problem Management.....	26
6.1 Purpose and Description	26
6.2 Terms and Concepts.....	26
6.3 Practice Success Factors (PSFs)	27
6.4 Proactive Problem Management.....	28
6.5 Reactive Problem Identification	30
7 Lesson 6: Knowledge Management	32
7.1 Purpose and Description	32
7.2 SECI Model of Knowledge Dimensions.....	33
7.3 Practice Success Factors (PSFs)	34

ITIL® 4 CDS

7.3.1	PSF: Creation and Maintenance.....	35
7.3.2	PSF: Effective Information for Decision-Making.....	35
8	Lesson 7: Service Level Management	36
8.1	Practice Success Factors (PSFs)	38
8.1.1	PSF: Establishing a Shared View.....	39
8.1.2	PSF: Meeting Service Levels	40
8.1.3	PSF: Improvements.....	41
9	Lesson 8: Monitoring and Event Management.....	42
9.1	Purpose and Description	42
9.2	Practice Success Factors (PSFs)	44
9.2.1	PSF: Approaches and Models	44
9.2.2	PSF: Timely, Relevant Data.....	44
9.2.3	PSF: Detecting and Acting on Events	45

1 Module 3 – Value Streams for User Support



The objectives for this module are for you to study:

- How to use a value stream to provide user support
- How specified ITIL practices contribute to a value stream for user support

In this module, the ITIL practices are applied to the creation of a user support value stream. The practices are:


- Service desk
- Incident management
- Problem management
- Knowledge management
- Service level management
- Monitoring and event management

We studied these six practices and how they can be combined to create and use a value stream specifically to provide user support.

2 Lesson 1: Value Streams for User Support Overview

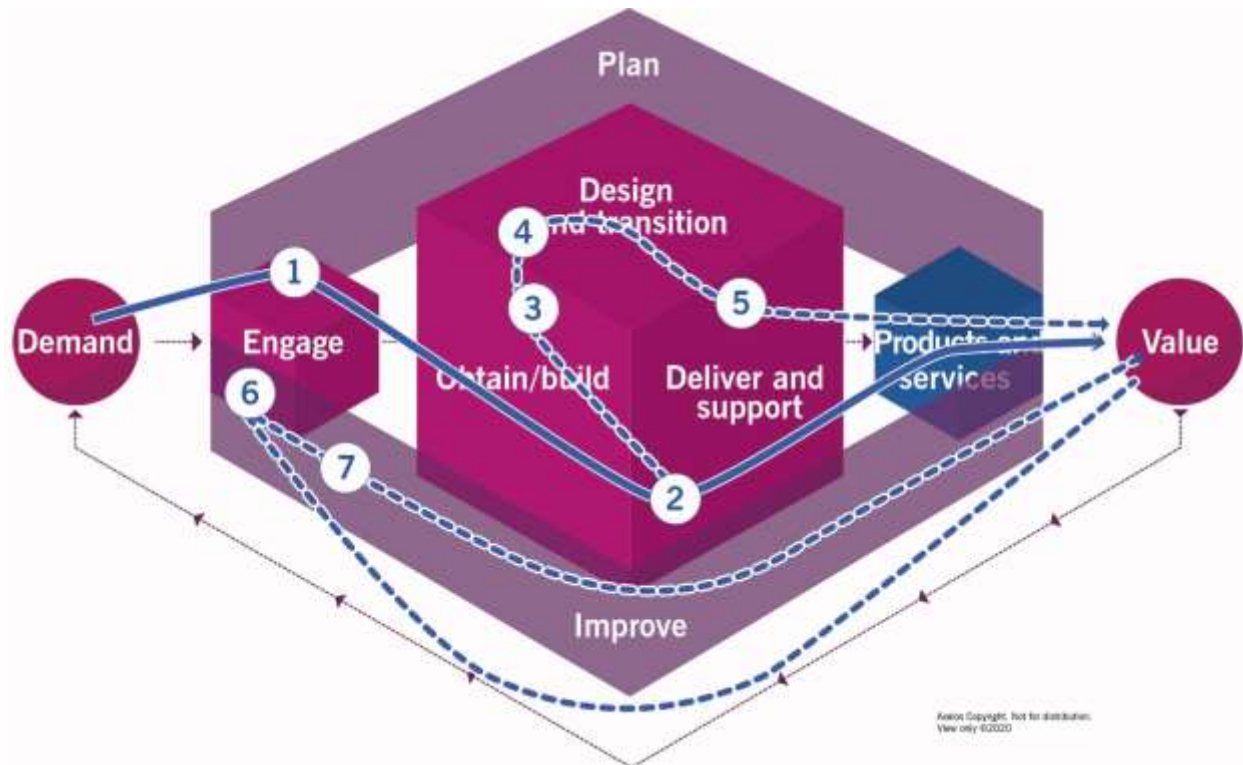
Value stream mapping can be used to improve existing value chains. In this lesson, the focus is on user support. Most organizations will have a standard incident value stream with some adaptations for specific circumstances such as VIP users or major incidents. Existing value streams need to be assessed when there is a new or changed service to ensure they are appropriate. Touchpoints with other practices need to be mapped. To create a value stream for user support, you will need to consider areas such as:

- Stakeholders
- Internal or external resources
- Escalation paths and work methods: dedicated, standby, swarming, self-support, shift left
- Hours and levels of support

	Shift-left	<p>Shift left in a support context means moving knowledge closer to the customer to improve resolution times and CX.</p> <p>This could be via FAQs and self-service portals, via better trained front line teams, or using approaches like swarming.</p>
---	-------------------	--

ITIL® 4 CDS

The diagram below illustrates how ITIL's service value system is used in each step of the user support value stream.



ITIL 4 CDS fig. 4.12 Restoration of a live service

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

1. Acknowledge and record the user contact (engage)
2. Investigate the event, classify it as an incident, attempt to fix it (deliver and support)
3. Get a fix from the specialist team (obtain/build)
4. Apply the fix (design and transition)
5. Verify the fix resolved the situation (delivery and support)
6. Ask for user feedback (engage)
7. Identify improvement opportunities (improve)


Note there is a split in the activity line at step 2. If the issue is resolved, then value is restored. If not, then the activities follow the dashed line. Realize that the value stream could also end at step 5. Regardless, it is common to collect feedback after the situation has been resolved.

ITIL® 4 CDS

There are several practices that might help to improve a user support value stream. Not all practices are examinable (examinable practices are in **bold**). The practices to improve a user support value stream include:

- **Incident management**
- **Service desk**
- Risk management
- **Knowledge management**
- Supplier management
- Service configuration management
- **Monitoring and event management**
- **Problem management**
- Software development and management
- Infrastructure and platform management
- Financial management
- Service validation and testing
- Deployment management
- Continual improvement
- **Service level management**

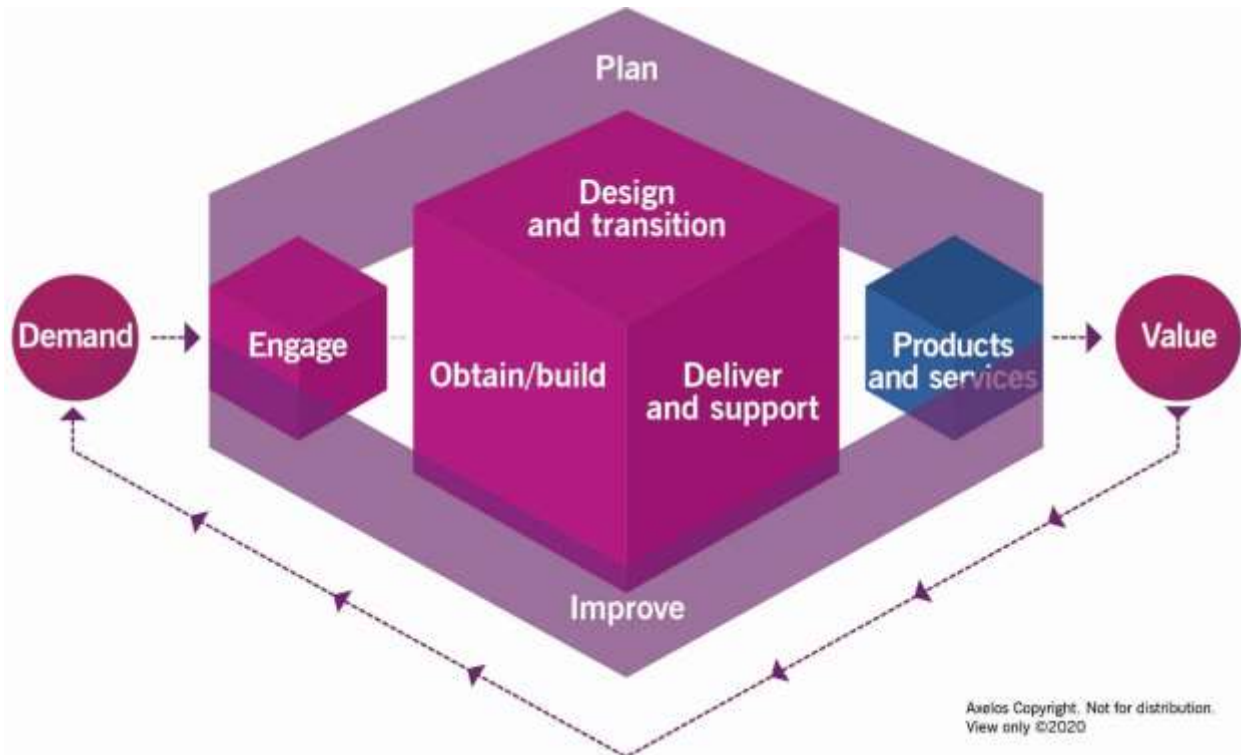
3 Lesson 2: Practices that Contribute to a Value Stream for User Support

	<h3>Purpose</h3>	<p>This lesson addressed the development of a value stream for user support. The focus is on the ITIL practices that support the user support value stream. The practices are:</p> <ul style="list-style-type: none">▪ Service desk▪ Incident management▪ Problem management▪ Knowledge management▪ Service level management▪ Monitoring and event management <p>These practices are presented at a high level before detail is added later in the module and study guide.</p>
---	------------------	---

3.1 Scenario for User Support

As most organizations have a fairly robust incident management process, let's check our understanding. Using the activities of the service value chain, the following activities occur:

- **Plan:** not engaged in this activity
- **Engage:** acknowledge and register the user event; request feedback after a fix has been deployed
- **Design and transition:** deploy the fix from the specialist team
- **Obtain/build:** from specialist teams, create a fix – either permanent or a workaround
- **Deliver & support:** confirm the event is an incident, attempt first-call resolution using past history; verify the incident has been resolved
- **Improve:** identify opportunities to improve practice, process, service, component



ITIL 4 CDS fig. 0.2 The Service Value Chain

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

Using your case study, Seylon Ordnax, we studied how the six practices would work together and provide user support. Here is the scenario:

Tom, a customer of Seylon Ordnax has called the service desk several times over the past week complaining that he has not been able to log on to his account, or when he has been able to get to his account, there is information missing. He is getting more and more frustrated as he is trying to book a surprise holiday for his family.

Let's see how this situation is resolved using ITIL's practices.

- Tom contacts the Seylon Ordnax service desk to report his issue...again.
- Carol, a service desk agent at Seylon Ordnax, listens carefully to Tom as he describes his issue.
- Carol has opened a new ticket, prioritizes it as urgent, and quickly looks at the history and activities that have been occurring. She sees that the Holssec technical specialists for the user accounts has been working on the issue. They have discovered that Tom is not the only one who has the same issue. They have discovered that many users have multiple accounts. They have been working to consolidate these accounts for all

affected users. They just haven't gotten to Tom yet. She also sees a problem management ticket has been opened and it's being worked on.

The problem management team also found that there were user multiple accounts – not only for Tom but for many other users. They are now investigating how that could happen and working on a solution to ensure it can't happen in the future. This team has been using the data and information resources from knowledge management to review service designs and technical specifications for the Holsec service.

In this encounter, the service desk practice engaged in the issue with empathy and provided good communication. Additionally, Carol provided a solution to Tom by booking his surprise holiday and Tom left the call with an excellent customer experience (CX). Carol had been empowered by the organization to go beyond typical activities to ensure a positive CX.


The incident management practice was being followed but, in this case, escalation and delivering a solution within the defined timeframe (the service level management practice, specifically the Holsec SLA), didn't occur. Once this issue has been technically resolved, the incident management practice will look to improve their handling of multiple issues.

Problem management engaged once the service desk alerted them to the multiple occurrence of the same issue. This team then followed reactive problem management activities. In their investigation, data and information from the monitoring and event management practice (log files for Holsec) and knowledge management practice (service design documentation) assisted in their understanding and solution development.

Based on the outcomes from the problem management investigation as well as the number of issues that were continuing to accumulate, the service level management practice initiated a review of the Holsec and began the process to update this service.


While Tom is only aware of his interaction with Carol, many practices work the issue simultaneously. An integrated service management toolset allows the sharing of information and supports the collaborative nature of the work.


4 Lesson 3 - Service Desk

	Objective	In this lesson, we explored key elements of the service desk practice. Those elements include: <ul style="list-style-type: none">▪ Purpose and description▪ Service empathy▪ Practice success factors
---	------------------	---

4.1 Purpose and Description

Most of us have experienced an interaction with a service desk and we come away from that engagement with a positive or negative impression of the organization. The service desk is often the first and only encounter we have with a service providing organization. The service desk needs to deliver a great user experience and work to achieve high levels of customer satisfaction.

	Purpose or Objective	The purpose of the service desk is “to capture demand for <i>incident</i> resolution and service requests. It should also be the entry point and single point of contact for the service provider for all users.”
---	-----------------------------	---

	Incident	“An unplanned interruption to a service or reduction in the quality of a service.”
---	-----------------	--


The service desk team typically supports multiple service management practices including:

- Incident management
- Service request management
- Problem management
- Service configuration management
- Relationship management practices.

These relationships are based on the direct contact and communication the service desk has with users. Any value stream activity that requires user communication will utilize the service desk.

4.2 Service Empathy

A critical characteristic of a service desk role is the ability to empathize.


	Service Empathy	Service empathy is <i>“the ability to recognize, understand, predict, and project the interests, needs, intentions, and experiences of another party in order to establish, maintain, and improve the service relationship.”</i>
---	------------------------	--

Service empathy is a critical element of user satisfaction and the success of the service provider.

4.3 Practice Success Factors (PSFs)

The service desk practice includes two practice success factors:

- “Enabling and continually improving effective, efficient, and convenient communications between the service provider and its users.”
- “Enabling the effective integration of user communications into value streams.”

	<p>Practice Success Factor (PSF)</p>	<p>“A complex functional component of a practice that is required for the practice to fulfil its purpose.”</p>
---	---	--



4.3.1 Communication Channels

Support channels for users should be easy to locate, easy to use, and provide the necessary support efficiently. The design of the user interface is determined by numerous factors such as:

- Service relationship model and type – is the relationship public or private, internal or external; is the type of relationship basic, cooperative, or a partnership?
- User profile – what are their capabilities based on location, age, culture, diversity, etc.?
- Service provider profile – what are their technical capabilities, user satisfaction strategy, etc.
- External factors – consider PESTLE impacts

	<p>Basic</p>	<p>“A basic relationship is usually appropriate for standard products and services, when the efficiency of service operation is a cornerstone.” From DSV</p>
	<p>Cooperative</p>	<p>“In a cooperative service relationship, the service provider usually tailors the products and services to the service consumer needs. The customer expects that the service provider will think about service outcome and experience, not only service levels.” From DSV</p>

ITIL® 4 CDS

	<p>Partnership</p>	<p><i>Partnership “In a partnership, the service provider and the service consumer may act as one organization coordinating activities across a great range of functions and processes. As the level of interdependency and integration grows, both parties may align on a strategic level by setting goals and priorities together.” From DSV</i></p>
	<p>PESTLE</p>	<p>PESTLE analysis looks at these factors as part of an analysis:</p> <ul style="list-style-type: none"> ▪ Political ▪ Economical ▪ Social ▪ Technological ▪ Environmental ▪ Legal

Due to the advances in technology, communication channels for user support can be provided by a human or through technology. Some examples of communication channels include:

Human	Technology
Voice	Web portals
Live Chat	Interactive voice menus
Email	Mobile Applications
Walk-in	Chat-bots

Typically, service providers will use multiple channels to provide user support. These channels should be connected and integrated or omnichannel.

Omnichannel communication allows the user to start a support call using a mobile application creating an appointment, follow up with a call to a service desk, and then eventually have a solution applied by a technician without ever providing the same information at each progressive check.

Multichannel communication that is not integrated could require information to be entered at each step with a risk of creating gaps in the support actions or losing or corrupting Information.


	Omnichannel Communication	<i>“Unified communications across multiple channels based on sharing information across the channels and providing a seamless communication experience.”</i>
---	----------------------------------	--

4.3.2 Integration to Value Streams


The service desk provides bi-directional communication between the service provider and the user. The service desk practice focuses on the accuracy of capturing, recording, and integrating communication into relevant value streams.

One example of a communication by the service provider to the user would be a notification around planned changes. The content, format, and timing of the message is determined by change enablement and release management practices, but the service desk establishes and maintains the communication channel.

User initiated communication (queries) must be triaged by the service desk, so it is forwarded to the appropriate value stream. Once forwarded, that specific value stream processes and acts upon the query following their specific processes and procedures.


	Triage	<p>The concept of triage comes from a military medical context. It focuses on identifying the most urgent work so it can be dealt with first. Low priority work has to wait until high and medium priority work has been completed.</p> <p>Triage can be used to manage workloads such as development backlogs and incident queues. It's important to make sure the low priority work doesn't get left forever though.</p>
---	---------------	--

5 Lesson 4: Incident Management


	<h3>Objective</h3>	<p>In this lesson, we explored key elements of the incident management practice. Those elements include:</p> <ul style="list-style-type: none">▪ Purpose and description▪ Terms and concepts▪ Practice success factors▪ Incident handling and resolution
---	--------------------	---

5.1 Purpose and Description

Incident management is probably the most well-known service management process – everyone has experienced some sort of technical failure that has needed resolution. That is exactly what the incident management practice does.

	<h3>Purpose</h3>	<p>The purpose of incident management is: <i>“to minimize the negative impact of incidents by restoring normal service operation as quickly as possible.”</i></p>
---	------------------	---

Notice the purpose is very clear – restore service as quickly as possible; minimize the impact of an incident. These are important statements – incident management is about service **restoration** and not finding the cause or developing a permanent fix. That is the problem management practice.

	<h3>Incident</h3>	<p><i>“An unplanned interruption to a service or reduction in the quality of a service.”</i></p>
---	-------------------	--

Another key word in the purpose is the word ‘normal.’ What does normal mean? Normal operation is defined in the technical specification for the service or within the configuration item (CI). The takeaway here is the service should operate as expected and as agreed. When it doesn't, then the incident management practice follows their processes for a quick restoration of service to:

- Achieve user and customer satisfaction
- Maintain or improve the credibility of the service provider
- Maintain or improve value co-creation

	<p>Configuration Item</p>	<p><i>“Any component that needs to be managed in order to deliver an IT service.”</i></p>
---	----------------------------------	---

5.2 Terms and Concepts



Two factors enable the achievement of the incident management purpose:

- Early incident detection
- Quick restoration of normal operations

Both factors are made possible with well-defined processes and procedures, automation (think about the monitoring and event management practice), good supplier relationships (not all service components are solely owned by the service provider), and properly trained and skilled specialist teams.

Incidents are rarely unique – there are definite patterns and trends within some services. These incidents are known errors, and these will have a workaround associated with them.


Additionally, organizations will develop incident models to optimize the handling and resolution of repeating incidents. Models help with efficiency (quick restoration of service) by applying a proven and tested solution (workaround).

	<p>Known Error</p>	<p><i>“A problem that has been analyzed but has not been resolved.”</i></p>
	<p>Workaround</p>	<p><i>“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.”</i></p>

	Incident Model	<i>“A repeatable approach to the management of a particular type of incident.”</i>
---	-----------------------	--

Some incidents will dramatically effect service operation, causing severe performance issues, unavailability, and potentially negatively impact user and customer satisfaction. These are known as major incidents.

Major incidents have significant business impact – the key deliverable of an organization is not available. For example, at the Minute Maid plant, the question at the service desk when a call comes in is, “Is juice still flowing?” If it is, it is not considered a major incident.

	Major Incident	<i>“An incident with significant business impact requiring an immediate coordinated resolution.”</i>
--	-----------------------	--

A major incident model is typically created to clearly define what is a major incident and what isn't. Other characteristics of this model include:

- Named coordinator and a dedicated team (in place only when the major incident is active)
- Other dedicated resources (such as budget!)
- Communication model
- Agreed procedure for review and follow-up activities

The use of workarounds is common practice within the incident management process. The workaround allows for the quick restoration at an acceptable level of quality. But...continued application of workarounds can increase technical debt and may lead to new future incidents. The problem management practice has a purpose of looking for the root cause of an incident (or group of incidents) and then developing a solution to overcome it. These actions will reduce the technical debt caused by incident management workarounds.



Technical Debt

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

5.3 Practice Success Factors (PSFs)

There are three practice success factors for incident management. They are:

- Detect incidents early
- Resolve incidents quickly and efficiently
- Continually improve the practice.



Practice Success Factor (PSF)



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

5.3.1 Detect Incidents Early

Historically, the most common method of detecting incidents was collecting information from users or technical specialists. Now, automation can detect and register incidents (see the monitoring and event management practice). Why is automation useful? The benefits include:

- Earlier detection (decreased service downtime)
- Higher quality initial data leads to faster resolution time (including the trigger for self-healing)
- Some incidents may not be seen by users – they will be 'seen' by automated methods
- Some incidents are resolved before they impact agreed service quality
- Incident cost decreases

Automation may be improved with the advances in machine learning – learning from past incidents, events, known errors and other sources can improve incident detection and categorization.



	Self-healing	Automated resolution
	Categorization	The act of assigning a category to something. For example, an incident will be categorized as low, medium or high priority depending on its impact and urgency.

The key to success for the incident management practice is early detection. What if there are no automated technologies? In this situation, aim to develop and promote a culture of responsible service consumption and encourage the reporting of suspicious events. Remember value is co-created – users should be encouraged to report the unusual as quickly as possible.

5.3.2 Resolve Quickly

If incidents are detected early and then the resolution is delayed, where's the value? Consider the following situations:

- Recurring and simple incidents have pre-defined resolutions that may be automated or standardized via a proven model
- Complex situations where the system is well known, escalate to the specialist group for diagnosis and resolution.
- Very complex situations where it's impossible to define which specialist group should handle the incident, deploy a collective approach called swarming.

	Escalation	<i>"An activity that obtains additional resources in order to meet service targets or customer expectations."</i>
	Swarming	<i>"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."</i>

The purpose of swarming is to decrease the level of complexity of the (major) incident by having numerous specialists involved in the individual investigation and resolution activities. This way, specialists with the correct expertise are working on elements of the incident rather than having a generic group trying to solve the incident as a whole. Physical meetings are typically avoided with swarming allowing the specialists to experiment, and design scripts and other tools for discovery activities. No matter what technique is used to resolve incidents quickly, ensure the data being analyzed is correct and accurate. While incidents should be resolved as soon as possible, the resources to perform that work may not be available. Prioritization is necessary. Note the difference between the following definitions.



- Task priority – *"the importance of a task relative to other tasks. Tasks with higher priority are worked on first. Priority is defined based on all the tasks in the backlog."*
- Prioritization – *"selecting tasks to work on first when it's impossible to assign resources to all tasks in the backlog."*

Some rules for prioritization include:

- Impact and urgency of an incident is not prioritization, but their estimation is useful for prioritization.
- Prioritization is only needed when there is a resource conflict
- Incidents should be processed with other tasks in a single backlog
- Prioritization is used to assign people to tasks; those teams will estimate processing time and resource availability (even with target resolution times defined in an SLA, teams can override those targets if in their estimation, the current incident has a greater impact than what was expected when the SLA was agreed.)




ITIL® 4 CDS

Visualization tools (such as Kanban and Lean principles) can be used to help limit work in progress and support prioritization.

	Impact	Direct effect of an incident (or problem) on the business (e.g., Who was impacted?, Where impacted?, When?...)
	Urgency	How much time is available to resolve the incident (or problem) before the business is negatively affected.

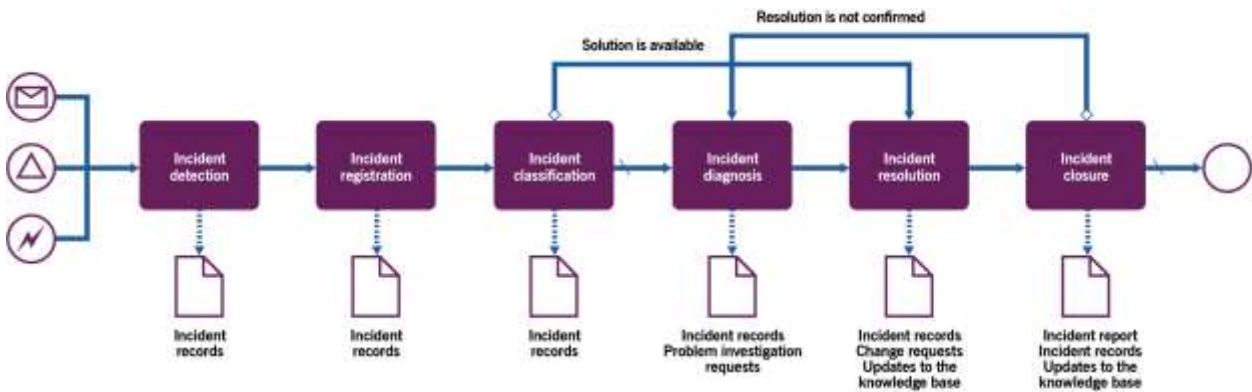
5.4 Continually Improve

Reviewing incident management records at regular intervals helps to identify areas for improvement as well as areas that are working well. Additionally, knowledge sharing between specialist teams creates efficiencies that may improve or introduce incident models. Reviews also allow the analysis of stakeholders' satisfaction with the incident management practice. Know the importance of data to the reviews of incidents. Data should be concurrent, complete, and comprehensive.

	Concurrent	Data that describes exactly what was done, when, to assist in continual improvement. Requires stakeholders to update incident records during the event and not after. An accurate timeline is useful for investigation.
	Complete	Ensure data accurately describes what activities have been done
	Comprehensive	Describe why activities were done (as important as the initial description)

5.5 Incident Handling and Resolution

Review the diagram below and the following table.



AXELOS Copyright Not for distribution View only ©2019

ITIL 4 Practice Guide: Incident Management Fig. 3.2 Workflow of the incident handling and resolution process

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

"Activity	Manually processed user-detected incidents	Automatically detected and processed incidents
Incident detection	The user detects a malfunction in service operation and contacts the service provider's service desk via the agreed channel(s). The 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,	Based on pre-defined rules, the following is automatically discovered:


	<p>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.</p> <p>In some cases, classification helps to reveal a previously defined solution for this type of incident.</p>	<ul style="list-style-type: none"> ▪ the incident's impact on services and users ▪ the solutions available <p>the technical team(s) responsible for the incident resolution, if automated solutions are ineffective or unavailable.</p>
Incident diagnosis	<p>If classification does not provide an understanding of a solution, technical specialist teams perform incident diagnosis. This may involve escalation of the incident between the teams, or joint techniques, such as swarming.</p> <p>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).</p>	<p>If the automated solution is ineffective or unavailable, the incident is escalated to the responsible technical team for manual diagnosis. It may involve escalation of the incident between the teams, or joint techniques, such as swarming.</p> <p>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 practice guide).</p>
Incident resolution	<p>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.</p>	<p>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.</p>
Incident closure	<p>After the incident is successfully resolved, a number of formal closure procedures may be needed:</p> <ul style="list-style-type: none"> ▪ user confirmation of service restoration 	<p>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</p>

<ul style="list-style-type: none">▪ resolution costs calculation and reporting▪ resolution price calculation and invoicing▪ problem investigation initiation▪ incident review. <p>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.</p>	<p>incident has been communicated to other stakeholders at any of the previous steps, the closure of the incident should also be communicated."</p>
---	---

ITIL® 4 Practice Guide: Incident Management, Table 3.2


© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

6 Lesson 5 – Problem Management

	<h3>Objective</h3>	<p>In this lesson, we'll explore key elements of the problem management practice. Those elements include:</p> <ul style="list-style-type: none">▪ Purpose and description▪ Problem identification▪ Practice success factors▪ Proactive problem identification▪ Reactive problem identification
---	--------------------	--

6.1 Purpose and Description

In the previous lesson, we studied the incident management practice. The problem management practice closely follows and relates to incident management.

	<h3>Purpose</h3>	<p>The purpose of problem management is:</p> <p><i>"To reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents and managing workarounds and known errors."</i></p>
---	------------------	--

With any service, perfection is rare, and incidents will occur. While the incident management practice will manage incidents, the problem management practice will manage the **cause** of the incident. A problem is "a cause, or potential cause, of one or more incidents."

6.2 Terms and Concepts

There are three phases to the problem management practice:

- Problem identification
- Problem control (non-examinable)
- Error control (non-examinable)

Note the evolution of a problem to an error.

Problem identification has two approaches:

- **Reactive problem management** – investigates the causes of incidents that have already occurred with an aim of prevent incidents from recurring.
- **Proactive problem management** – identifies problems **before** an incident is caused, assesses the related risks, and creates a response that minimizes the possibility of an incident or reduces its impact

Information sources for proactive problem management include vendor communication (vulnerabilities in their products); developer, designers, or testers discovering errors in live versions, user communities, monitoring data, technical audits.

6.3 Practice Success Factors (PSFs)

There are two practice success factors for the problem management practice which are to:

- *“Identify and understand the problems and their impact on services”*
 - When organizations understand the errors in their products and services, incidents can be mitigated or even prevented. Problem management ensures problem identification, contributing to continual improvement of products and services.
- *“Optimize problem resolution and mitigation.”*
 - Once problems are identified, manage them appropriately. Not all problems can be removed (or need to be removed) – problems should be permanently resolved balancing costs, risks, and impact on service quality.



Practice Success Factor (PSF)

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

6.4 Proactive Problem Management

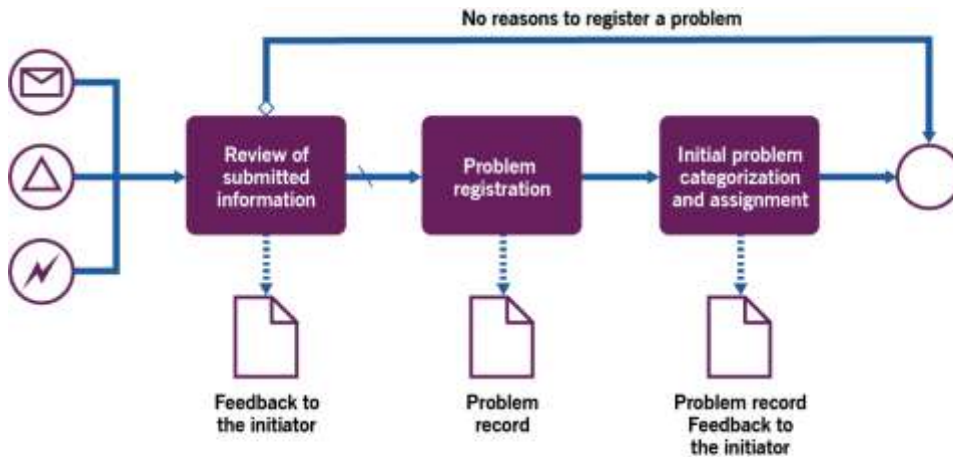
Proactive problem management identifies problems before an incident occurs. The table below defines the key inputs, activities and key outputs.

"Key Inputs	Activities	Key Outputs
<ul style="list-style-type: none"> ▪ Error information from vendors and suppliers ▪ Information about potential errors submitted by specialist teams ▪ Information about potential errors submitted by external user and professional communities ▪ Information about potential errors submitted by users ▪ Monitoring data ▪ Service configuration data 	<ul style="list-style-type: none"> ▪ Review of the submitted information ▪ Problem registration ▪ Initial problem categorization and assignment 	<ul style="list-style-type: none"> ▪ Problem records ▪ Feedback to the problem initiator"

Problem Management ITIL® 4 Practice Guide, Table 3.1

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

The workflow for the proactive problem identification process is shown below.



AXELOS Copyright Not for distribution View only ©2019

ITIL 4 Practice Guide: Problem Management Fig. 3.2 Workflow of the proactive problem identification process

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

The review of the submitted information is completed by a specialist. They will ensure:

- The submitted information isn't duplicating a current problem record
- It's applicable to the organization

If it is related to ongoing incidents, the problem would be registered at this point or rejected (with a notification to the submitter). To register the problem, a problem record is created. During the creation, the problem is initially categorized. Initial categorization is based on the submitted information and the outputs of the initial review. The problem is then assigned to a specialist group which is responsible for the presumed CI, service or product at fault. Problem categorization can change as the technical specialist investigates.

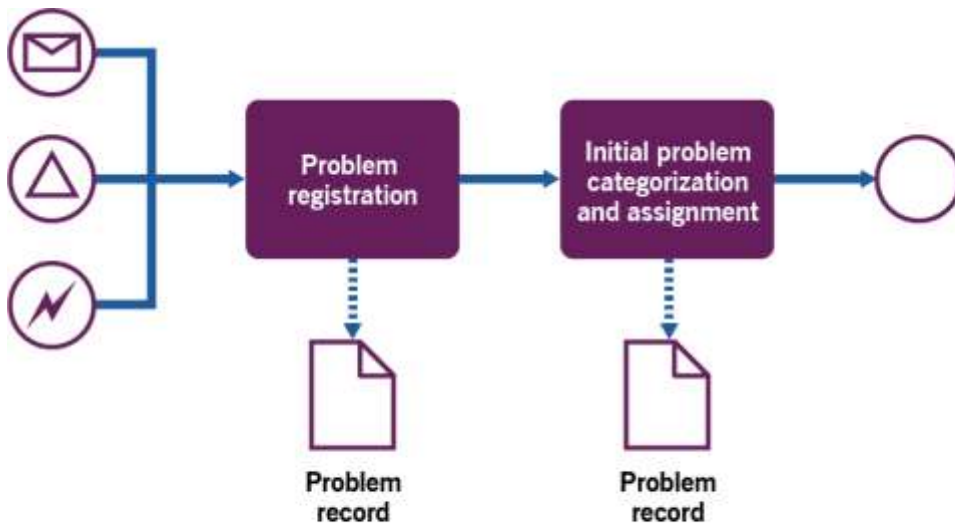
Proactive problem identification activities identify potential errors in products and services. Information used in this discovery includes sources other than incident records.

	Sources of Information	Additional information sources include vendor communication (vulnerabilities in their products); developers, designers, or testers discovering errors in live versions, user communities, monitoring data, technical audits.
---	-------------------------------	--

Proactive problem identification is a form of risk management. The activities include identification, assessment, and analysis of the vulnerabilities and associated risks. The focus of proactive problem management should be key systems and components that could cause the highest impact to the organization if they failed. In the assessment of the possible problems, consider the probability and impact of the identified vulnerabilities.

6.5 Reactive Problem Identification

The workflow for the reactive problem identification process is below.



AXELOS Copyright Not for
distribution View only
©2019

ITIL 4 Practice Guide: Problem Management Fig. 3.2 Workflow of the proactive problem identification process

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

Problem registration in reactive problem identification is triggered by an ongoing incident. It could be a single incident that has significant impact or multiple incidents across the enterprise. A problem could also be registered after the resolution of the incident. Initial problem categorization and assignment of the problem record based would be completed by the person registering the problem. Information included is:

- Description
- Associated CIs
- Estimated impact and probability of incidents
- Associated and potentially affected services
- Impact to the organization and customers

The problem is then assigned to the appropriate specialist group.

Problems could also be registered by an analysis of incident records. Based on those incidents, the specialist team reviewing them may decide to register a problem record. The justification could be a high number of similar incidents, major incidents, poor availability, among others. When registering a problem

ITIL® 4 CDS

based on incident analysis, the analyst performs categorization and includes similar information to the ongoing incident activity. The record is assigned to an appropriate specialist group based on associated CI, service, or product.

Reactive problem identification uses information from past and ongoing incidents, as well as monitoring data, configuration data, and service level agreements. The key inputs, activities and key outputs of reactive problem identification are shown in the table below.

Key Inputs	Activities	Key Outputs
<ul style="list-style-type: none">Information about ongoing incidentsIncident records and reportsMonitoring dataService configuration dataService level agreements (SLAs)	<ul style="list-style-type: none">Problem registrationInitial problem categorization and assignment	<ul style="list-style-type: none">Problem records

Problem Management ITIL®4 Practice Guide, Table 3.2

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

The incident management and problem management practices are used within a single value stream and will share the same resources (including teams, tools, procedures). Methods used in problem identification include statistical analysis, impact analysis, and trend analysis. These techniques allow for the identification of common causes.



Tip

After you complete your course, why not do a bit of research to learn more about the techniques used in root cause analysis?

You might start your investigation [here](#).

7 Lesson 6: Knowledge Management



In this lesson, we explored key elements of the knowledge management practice. Those elements include:

- Purpose and description
- SECI model of knowledge dimensions
- Practice success factors

7.1 Purpose and Description

The knowledge management practice provides a method, structure, and culture for the development, collection, processing, and analysis of data, information, and knowledge across all value streams and practices.



Purpose

Every value stream and practice benefits from the knowledge management practice. Its purpose is:

"To maintain and improve the effective, efficient, and convenient use of information and knowledge across the organization."

Simply put, knowledge management aims to provide the right information, to the right person, at the right time.


The activities within the knowledge management practice transform information and organizational intellectual capital into value for employees and service customers. To accomplish this, there must be an established and integrated process for managing knowledge assets. Additionally, people must be empowered to develop and share knowledge.

Two premises exist for the knowledge management practice:

- Knowledge is processed and used in every value stream and as such, information must be available and on time.
- The focus of this practice is on the discovery and provision of high-quality information, meaning information is available, accurate, reliable, relevant, complete, timely and compliant.



7.2 SECI Model of Knowledge Dimensions

The ability to learn is critical to people and organizations, especially when innovation and the ability to change dominate today's environment. The organization's absorptive capacity must be continuously developed through the creation and use of new knowledge.

	Absorptive Capacity	<i>"The organization's ability to recognize the value of new information, to embed it into an existing knowledge system, and to apply it to the achievement of business outcomes."</i>
---	----------------------------	--

The SECI (socialization, externalization, combination, internalization) model of knowledge dimension describes knowledge sharing and the transformation process across any organization.

Two types of knowledge form the basis of this model:

	Explicit Knowledge	<i>"Knowledge transferred to others, codified, assessed, verbalized, and stored. It includes information from books, databases, descriptions, and so on."</i>
	Tacit Knowledge	<i>"Knowledge that is difficult to transfer to others, difficult to express, codify, and assess. It is based on experience, values, capabilities, and skills."</i>

According to the SECI model, knowledge has two dimensions for knowledge creation:

- Converting tacit knowledge to explicit knowledge and vice versa
- Transferring knowledge from an individual to a group(s) or organization

Knowledge is used through socialization, externalization, internalization, or through a combination approach.


	<p>Socialization</p>	<p>Tacit to tacit sharing; knowledge is shared face-to-face or through experiences (coaching, mentoring).</p>
	<p>Externalization</p>	<p>Tacit to explicit sharing; experiences are described or formulated in documentation.</p>
	<p>Internalization</p>	<p>Explicit to tacit; an individual develops their knowledge independently or through formal training.</p>
	<p>Combination</p>	<p>Explicit to explicit; data from internal and external sources is combined, analysed, and presented to form new knowledge.</p>

Using and exchanging knowledge happens continually – note the spiral in the diagram. It represents the continuity and evolution of knowledge. Remember, the purpose of knowledge is to support data-driven decisions (“I know” vs. “I think” decisions).

7.3 Practice Success Factors (PSFs)

The knowledge management practice has two practice success factors which are:

- Creation and maintenance of knowledge and its transfer and use across an organization
- Effective use of information for decision-making across an organization

	<p>Practice Success Factor (PSF)</p>	<p><i>“A complex functional component of a practice that is required for the practice to fulfil its purpose.”</i></p>
---	---	---

7.3.1 PSF: Creation and Maintenance

There must be an effective culture around knowledge sharing that is developed, maintained, and supported.

The knowledge management practice describes tools and techniques that will only be effective in a nurturing culture – one where the organization embraces the need to identify, understand, use, analyse, learn, unlearn, transfer, present and discuss data and information in a way that supports the organizational mission, vision, and strategy.

Knowledge can be a competitive advantage and as such, knowledge transfer can run into many barriers. Stakeholders must stress the value and importance of sharing knowledge and create the appropriate atmosphere to support knowledge transfer.

7.3.2 PSF: Effective Information for Decision-Making

A successful knowledge management practice develops not only the tools and techniques to collect and maintain knowledge but also the people. The development of a knowledge culture is crucial to the practice.

Successful organizations work to develop the competencies to use, collect, and share information throughout the organization. Information quality is paramount to their operations – not only for good decision making, but also as a performance measure of the practice.

When designing a knowledge management system, consider the following errors and design to overcome them.

- Errors in the information collection (poor data entry)
- No alignment or integration between internal and external sources (no consistency in format or entry standards)
- Lost information due to unstructured data storage
- Loss of data during migrations
- Difficult to use interfaces (poor tool to support data search)

Remember, the purpose of data is to support effective decision-making. Data describes the past. Decisions are typically predicting the future. As data is being collated and analyzed, intuition and creative thinking skills of an individual combined with the power of forecasting tools, creates possible alternatives and then the best solution. But, the quality of the decision is directly related to the quality of the data!

8 Lesson 7: Service Level Management



In this lesson, we explored key elements of the service level management practice. Those elements include:

- Purpose and description
- Scope
- Practice success factors

The service level management practice creates and manages a shared view of quality services between the service provider and consumer.



Purpose

The purpose of service level management is:

"To set clear business-based targets for service levels, and to ensure that delivery of services is properly assessed, monitored, and managed against these targets."

The shared view is documented (normally in a service level agreement - SLA) and the focus is on service quality and value. Service agreements are in place throughout the entire service relationship.

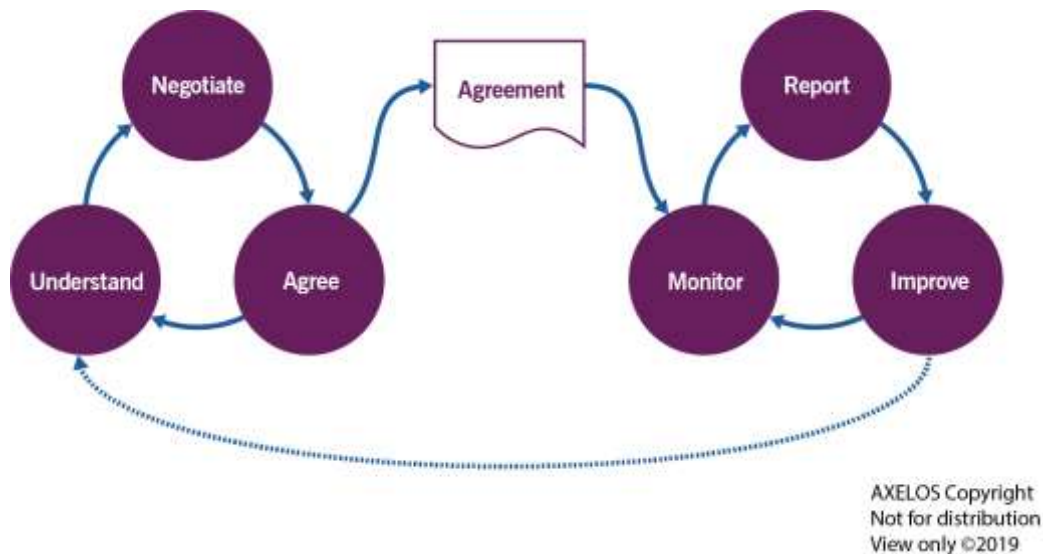


Service Level Agreement (SLA)

"A documented agreement between a service provider and a customer that identifies both services required and the expected level of service."

ITIL® 4 CDS

The key activities of the service level management practice are shown in this diagram.



ITIL 4 Practice Guide: Service Level Management Fig. 2.1 Key activities of the service level management practice

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

The service level management practice scope includes:

- Tactical and operational communication with customers about expected, agreed, and actual service quality
- Negotiating, agreeing and maintaining SLAs with customers
- Understanding the design and architecture of services and their dependencies
- Continual review of achieved service levels versus agreed and expected
- Initiation of service improvements (applied to agreements, monitoring, reporting, service performance)

	<p>Service Levels</p>	<p><i>"One or more metrics that define expected or achieved service quality."</i></p>
--	------------------------------	---

There are several activities in other service management practices that support the service level management practice. The practices and their associated activities are shown in the table below.

“Activity	Practice Guide
<i>Strategic communications with customers and sponsors</i>	<i>Relationship management</i>
<i>Operational communications with users</i>	<i>Service desk</i>
<i>Establishing and managing of contracts with suppliers and partners</i>	<i>Supplier management</i>
<i>Identification and documentation of services</i>	<i>Service catalogue management</i>
<i>Design of products and services</i>	<i>Service design</i>
<i>Analysis of innovation opportunities and new requirements for services outside of existing utility and warranty options</i>	<i>Business analysis</i>
<i>Design and control of financial models for commercial service delivery</i>	<i>Service financial management</i>
<i>Ongoing management and implementation of improvements</i>	<i>Continual improvement</i>
<i>Implementation of changes to products and services</i>	<i>Change enablement Project management Other practices</i>
<i>Monitoring technology, team and supplier performance</i>	<i>Monitoring and event management”</i>

Table 2.1, Service Level Management ITIL® 4 Practice Guide

© Copyright AXELOS Ltd 2020. All rights reserved. Material is reproduced under license from AXELOS Ltd

8.1 Practice Success Factors (PSFs)

There are several practice success factors (PSFs) for service level management. The PSFs are:

- *“Establishing a shared view of target service levels with customers”*
- *“Overseeing how the organization meets the defined service levels through the collection, analysis, storage, and reporting of the relevant metrics for the identified services”*
- *“Performing service reviews to ensure that the current set of services continues to meet the needs of the organization and its customers”*
- *“Capturing and reporting on improvement opportunities, including performance against defined service levels and stakeholder satisfaction.”*



Practice Success Factor (PSF)

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

8.1.1 PSF: Establishing a Shared View

Customer interactions will differ depending on the service relationship model – consider a tailored or ‘out of the box’ relationship. The ‘out of the box’ customer will need to accept the available services (or have minimal negotiation) while a tailored service offers great flexibility. In a tailored service, there is great flexibility in defining the service level targets. Know that these targets do need agreement before the service is delivered and consumed.

To establish a tailored service, customer needs and expectations are the main discussion. Ensure both the customer, including users and sponsors, and service provider, represented by service delivery teams, service provision sponsors, service architects, service designers, business analyst, and service development teams, can agree to the service specifications. As these discussions progress, the scope of service quality is refined and narrowed until it represents a service level that can be delivered at the necessary levels of assurance and liability.

In ‘out of the box’ services, service levels are typically predefined. These definitions come from analyzing the market to create a generic profile need for that specific service. There might be a tiered service delivery (gold, silver, bronze) for those who wish to use (and pay for) additional functionality.

Regardless of the relationship, all agreed service levels should have a clear method to measure and report. If possible, define the metrics early and ensure measurement and reporting tools are integrated into the service. Metrics that measure overall service quality include functionality, availability, performance, timeliness, user support, accuracy, and user experience (UX) measures.

What happens when the agreed service level quality differs from the expected quality levels? This is where good relationship management skills are needed. The ITIL guiding principles can also help develop a mutually shared view of service quality.

8.1.2 PSF: Meeting Service Levels

Once the service level targets are established, services are being delivered and consumed. The service provider should control the quality of the service keeping in mind these three views:

- Achieved service level – compare to what was agreed
- User satisfaction – feedback from the service desk, surveys...
- Customer satisfaction – feedback from reviews, surveys, social media comments...

Collect, store, analyze, and report on this data to relevant stakeholders for provider and consumer. Understand that service level management does **not** design or execute data collection. Other practices, specifically service design, monitoring and event management, and measuring and reporting, will perform this work. The service level management practice will make sense of the data and then communicate and review with stakeholders.

The service review purpose is to share the achieved service quality and value enabled by the service. As a result, service improvements may be initiated.

Service reviews can be one of two types.

- **Event based**
 - This type of review is triggered by events (major incidents, request for a significant change to a service, change in business need...).
- **Interval based**
 - This type of review is scheduled at regular and agreed time periods. The interval between meetings is usually based on previous satisfaction with the service, number of changes to the service, likelihood of changes to the service expectations or requirements. The typical timeframe is monthly but should be no longer than every three months.


No matter the form of the review and when it takes place, service reviews are critical in the service relationship. There is a distinct relationship between the quality of a service review and the quality of the services and stakeholder satisfaction. Additionally, service reviews are the main source for service improvements, which is the next PSF.

8.1.3 PSF: Improvements


Service reviews provide the opportunity to improve services – based on underperformance of the service or to improve the level of satisfaction from users and customers. Of course, improvements can also be made to practice processes, tools or other resources. Transparency is critical with improvements – ensure that any improvement suggestion is visible so that those who have the suggestions know that they have been considered. This promotes the ITIL guiding principle of 'collaborate and promote visibility'.

All improvements to the product or service are owned by the role that is accountable (product owner or service owner). For effective implementation of practice, product, and service improvements, follow the guidance in the continual improvement practice.

9 Lesson 8: Monitoring and Event Management



	<p>In this lesson, we explored key elements of the monitoring and event management practice. Those elements include:</p> <ul style="list-style-type: none"> ▪ Purpose and description ▪ Practice success factors
---	--

9.1 Purpose and Description

	<p>Purpose</p>	<p>The purpose of monitoring and event management is <i>“to systematically observe services and service components, and record and report selected changes of state identified as events.”</i></p>
---	-----------------------	--






Activities of this practice include the identification and categorization (analysis) of events throughout the infrastructure and between a service and its customers. This practice has two parts:

- Monitoring focuses on services and their components to detect changes of state that have significance. This information is communicated to relevant parties.
- Event management manages the identified events from monitoring activities and initiates the correct response to the event.

	<p>Event</p>	<p><i>“Any change of state that has significance for the management of a service or other configuration item (CI).”</i></p>
	<p>Configuration Item</p>	<p><i>“Any component that needs to be managed in order to deliver an IT service.”</i></p>

	<p>Monitoring</p>	<p><i>“Repeated observation of a system, practice, process, service, or other entity to detect events and to ensure that the current status is known.”</i></p>
---	--------------------------	--


Monitoring proactively observes designated services and service components and reports any changes of state (alert) as an event. These alerts are defined by predetermining thresholds for the monitored components that when breached, will trigger a response. The action taken will depend on the classification of the event. Typical categories, in order of increasing significance, are informational, warning, and exception.

	<p>Alert</p>	<p><i>“A notification that a threshold has been reached, something has changed, or a failure has occurred.”</i></p>
	<p>Threshold</p>	<p><i>“The value of a metric that triggers a pre-defined response.”</i></p>
	<p>Informational</p>	<p><i>“Informational events provide the status of a device or service or confirm the state of a task and do not require action at the time they were identified.”</i></p>
	<p>Warning</p>	<p><i>“A warning allows action to be taken before any negative impact is experienced. Warning events signify that an unusual, but not exceptional, operation is occurring.”</i></p>
	<p>Exception</p>	<p><i>“Indicates that a critical threshold for a service or component metric has been reached, indicating failure, significant performance degradation, or loss of functionality.”</i></p>

9.2 Practice Success Factors (PSFs)

There are three practice success factors for monitoring and event management. They are to:

- *“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.”*

	Practice Success Factor (PSF)	<i>“A complex functional component of a practice that is required for the practice to fulfil its purpose.”</i>
---	--	--

9.2.1 PSF: Approaches and Models

Monitoring and event management has a significant challenge within its activities: data collection. This practice must be clear in its approach and the models it develops to collect data as there is a risk of collecting too much data. The intent is to collect just enough meaningful information that will support the service management activities across the organization. To accomplish this PSF:

- Identify and prioritize services and the components that are monitored. This decision is based on the business objectives and the dependency of the components to achieve them.
- Balance the need for information, the granularity of the data, and the frequency it is collected. The more data that is collected, the less information will be produced if only due to the amount of data collected and the effort required to filter and analyze the data. Automation and machine learning are useful tools to deploy for data analysis.
- Maintain an appropriate level of technology to collect, analyze, report and store monitored data. Define policies to address different types of events and their associated responses.

9.2.2 PSF: Timely, Relevant Data

Data that is relevant and timely allows fact-based decisions and actions. This is critical for the delivery of high-quality services (meeting service performance requirements) and continual improvement activities (identification of underperforming areas). Ensure this data is available to relevant stakeholders.

For example, data from monitoring and event management can answer these questions:

- **Service provider** – is the service performing as designed? Benchmark the service against the design specifications
- **Customer** – am I getting what I paid for? Data showing performance has met (or not met) agreed service levels
- **Customer and service provider** – who's at fault? Data can show where, for example, the customer is causing service faults and there is a need for training

9.2.3 PSF: Detecting and Acting on Events

The last PSFs focuses on the efficiency of detecting events and then acting on them. The practices within monitoring and event management can be clearly defined but if the architecture design and/or age of the components are overly complex or not compatible to modern monitoring tools, then this practice will not provide the benefit it should. Monitoring and event management is heavily dependent on technology. Exploit the capabilities of the technological advances – utilize automation, artificial intelligence, machine learning to reduce the need for manual collection, analysis, and reporting.