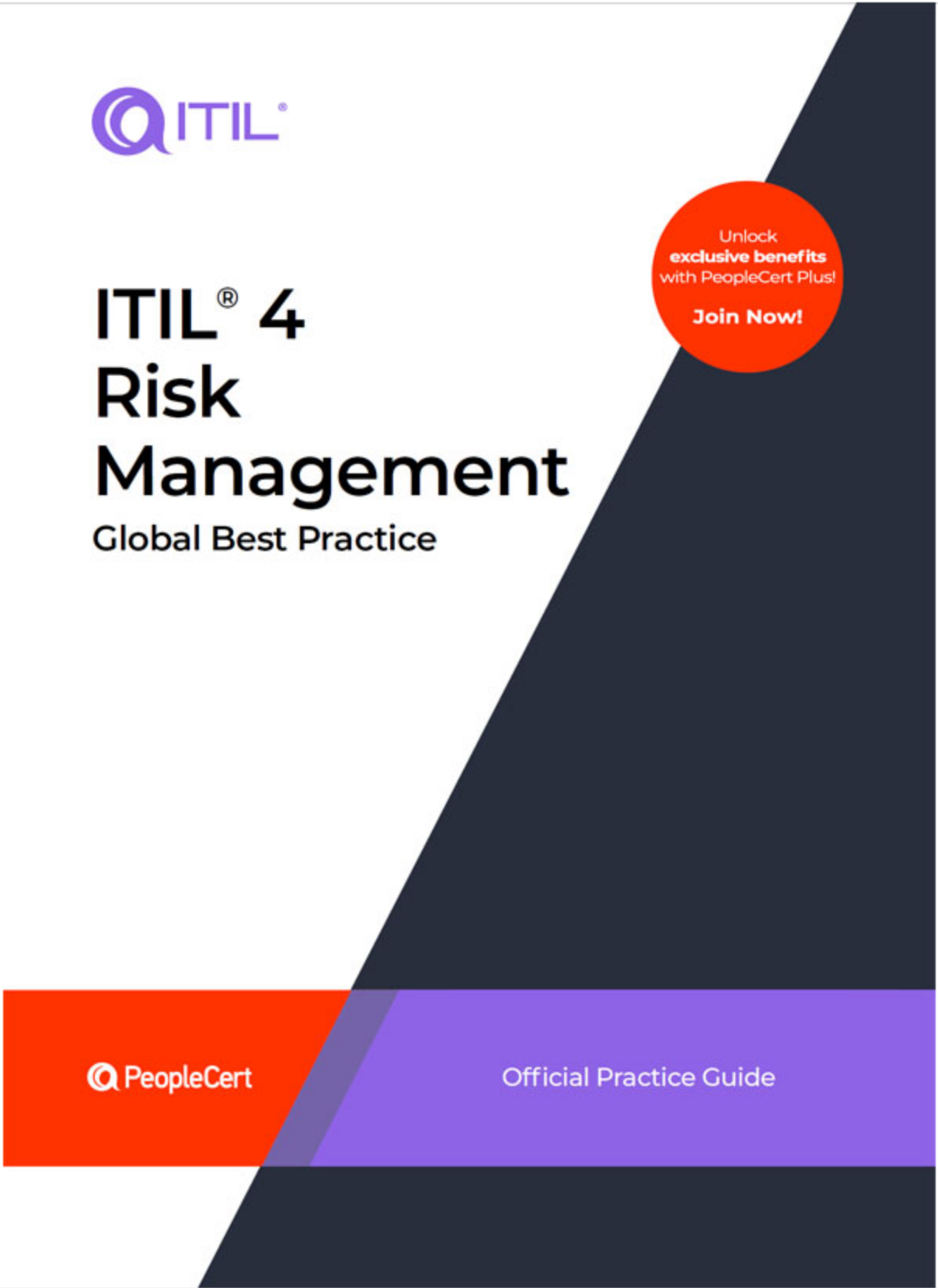


ITIL® 4 Risk management | Official Practice Guide

PeopleCert

expand all | collapse all

Cover	Cover
Title Page	iii
Copyright Page	iv
Contents	v
List of figures	vi
List of tables	vii
Welcome	viii
1. About this guide	1
2. General information	4
3. Value streams and processes	14
4. Organizations and people	25
5. Information and technology	31
6. Partners and suppliers	37
7. Capability assessment and development	41
8. Recommendations for practice success	48
Glossary	50
Index	53





ITIL[®] 4 Risk Management

Global Best Practice





Unlocking your potential to achieve more

Welcome to the ITIL® 4 Risk 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: 978-9925-34-560-1 (Digital)
 ISBN: 978-9925-34-559-5 (Print)
 ISBN: 978-9925-34-561-8 (ePub)
 Published in Cyprus
 Publication printed in Greece or reproduced electronically in Greece

Copyright® 2024 PeopleCert International Ltd.

All rights reserved. No part of this publication may be reproduced or transmitted in any form and by any means (electronic, photocopying, recording or otherwise) except as permitted in writing by PeopleCert International Ltd. Enquiries for permission to reproduce, transmit or use for any purpose this material should be directed to the publisher.

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® 2024





Contents

› [List of figures](#)

› [List of tables](#)

› [Welcome](#)

› [Chapters](#)

1. About this guide

ITIL[®] 4 qualification scheme

2. General information

2.1 Purpose and description

2.2 Terms and concepts

2.3 Scope

2.4 Practice success factors

2.5 Key metrics

3. Value streams and processes

3.1 Processes

3.2 Value stream contribution

4. Organizations and people

4.1 Roles, competencies, and responsibilities

4.2 Organizational structures and teams

5. Information and technology

5.1 Information exchange: inputs and outputs

5.2 Automation and tooling

6. Partners and suppliers

6.1 Dependencies on third parties

6.2 Support from third parties

7. Capability assessment and development

7.1 The practice capability levels

7.2 Capability self-assessment

7.3 Risk management capability development

8. Recommendations for practice success

› [Glossary](#)

› [Index](#)



Next



v

/ 55





List of figures

- Figure 2.1 Example matrix for qualitative risk analysis
- Figure 3.1 Workflow of the 'governance of risk management' process
- Figure 3.2 Workflow of the 'risk identification, analysis, and treatment' process
- Figure 3.3 Workflow of the 'risk monitoring and review' process
- Figure 7.1 Design of the capability criteria
- Figure 7.2 The capability development steps and levels



List of tables

Table 2.1	Risk treatment options
Table 2.2	Example controls
Table 2.3	Activities related to the risk management practice described in other Official Practice Guides
Table 2.4	Key metrics for the practice success factors
Table 3.1	Inputs, activities, and outputs of the ‘governance of risk management’ process
Table 3.2	Activities of the ‘governance of risk management’ process
Table 3.3	Inputs, activities, and outputs of the ‘risk identification, analysis, and treatment’ process
Table 3.4	Activities of the ‘risk identification, analysis, and treatment’ process
Table 3.5	Inputs, activities, and outputs of the ‘risk monitoring and review’ process
Table 3.6	Activities of the ‘risk monitoring and review’ process
Table 3.7	Risk management in key service value streams
Table 4.1	Competency codes and profile
Table 4.2	Roles involved in the risk management activities
Table 5.1	Automation solutions for the risk management practice
Table 5.2	Automation solutions for risk management activities
Table 7.1	Risk management capability criteria
Table 7.2	The risk management capability development steps
Table 8.1	Recommendations for the success of risk management



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

Stuart Rance, Konstantin Naryzhny

Reviewers

Roman Zhuravlev

2024 Revision

Antonina Douannes, Adam Griffith, Dmitry Isaychenko, Kaimar Karu, Stuart Rance, Roman Zhuravlev





Information icons

-  Key message
-  Definition
-  Tip



Chapter 1

About this guide

This Official Practice Guide provides practical guidance for the risk 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 from this guide is examinable as a part of the following syllabi:


- **ITIL® 4 Leader:** Digital and IT strategy
- **ITIL® 4 Specialist:** High-Velocity IT

Please refer to the respective syllabus documents for details.

Chapter 2

General information

2.1 Purpose and description

**Key message**

The purpose of the risk management practice is to ensure that the organization understands and effectively handles risks.

Managing risk is essential to ensuring the ongoing sustainability of an organization and co-creating value with its customers. Risk management is an integral part of all organizational activities and therefore central to the organization's service value system (SVS).

Risk management is performed at all levels of the organization. Strategic risk management considers long-term risks that may impact the ability of the organization to perform its mission. Programme and project risk management considers risks that may affect medium-term goals and objectives. Operational risk management is focused on short-term goals and objectives. Risk management at each of these levels must be based on direction from the governors of the organization.

The ITIL definition of a service specifically identifies that managing risks on behalf of service consumers is an essential part of every service: 'a means of enabling value co-creation by facilitating outcomes that customers want to achieve, without the customer having to manage specific costs and risks'.

Every service removes some risks, but also imposes additional risks on the service consumer. The service provider must understand and manage these risks in a controlled manner. The balance between the risks removed and the risks imposed is part of the value proposition of the service.

The risk management practice provides an organization with the resources required to identify and manage risks efficiently and effectively across all four dimensions of service management.

This practice is beneficial for both IT service providers and their service consumers. Benefits for service providers include:

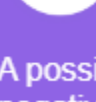
- reduced business risks
- protection for the reputation and credibility of the organization
- improved input to organization's strategy
- increased ability to demonstrate compliance with legal and regulatory requirements
- improved ability to control investments needed to manage risks
- improved reliability and consistency of all practices, value streams, and services.

Benefits for service consumers include:

- reduced business risks
- increased ability to demonstrate compliance to legal and regulatory requirements
- improved reliability of third party services.

2.2 Terms and concepts

2.2.1 Risk

**Risk**

A possible event that could cause harm or loss, or make it more difficult to achieve objectives. It can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.

Risk is normally avoided because of its association with threats. Although this association is generally true, risk is also associated with opportunity. Any uncertain outcome is a risk. When the risk is negative, the uncertain outcome would result in harm or loss. However, when the risk is positive, the uncertain outcome would result in benefits to one or more stakeholders. For example, an organization may invest in a new service with the expectation that it will attract customers and generate revenue. However, a positive outcome is not guaranteed; instead the outcome is uncertain or a risk. Positive risks are sometimes called opportunities.

2.2.2 Risk capacity

Risk capacity is defined by the governance of the organization. Risk management activities must ensure that risks remain below the risk capacity.

If the level of risk in an organization is too high, then this could have a major impact on the organization's ability to continue operating. The risk capacity of an organization is the maximum amount of risk that the organization can tolerate, and is often based on factors such as damage to reputation, assets, and so on.

2.2.3 Risk appetite

Risk appetite is defined by the governance of the organization and is used to facilitate decision-making and risk management activities.

Some organizations choose to take significant risks to make significant gains. Other organizations prefer to take few risks, but this also reduces their opportunities. The risk appetite of an organization is the amount of risk that the organization is willing to accept. This should always be less than the risk capacity of the organization.

2.2.4 Risk register

It is important to keep a record of identified risks, which records the risk's current status and history. This record is known as a risk register. Each entry in the risk register shows the history and status of a single risk.

Typically, this will include the following information (but this can vary depending on the needs of the organization):

- unique ID
- category (to group similar types of risk)
- description
- probability
- impact
- overall rating or score
- owner
- treatment
- updated rating or score after treatment (residual risk)
- action date(s).

An organization may have more than one risk register depending on the size and structure of the organization, and the number and types of risks that are being managed.

2.2.5 Risk treatment

Sometimes it is possible to eliminate a risk, but this is unusual. After the probability and the impact of the risk has been understood, the risk owner must agree on a suitable way to treat the risk. Actions that can be taken to treat a risk are shown in Table 2.1.

Table 2.1 Risk treatment options

Treatment	Description	Example
Risk avoidance	Prevent the risk by not performing the risky activity	Avoid the risk of an investment failing to deliver the expected value by rejecting the business case proposing the investment
Risk modification (or risk reduction)	Implement controls to reduce the likelihood or impact of the risk	Encrypt sensitive information when it is transmitted on the network to reduce the likelihood of it being intercepted
Risk sharing	Reduce the impact by passing some of the risk to a third party	Take out insurance against fire or against a cyber attack
Risk retention (or risk acceptance)	Intentionally decide to accept the risk because it is below an acceptable threshold (and within the risk appetite of the organization)	Accept the risk of an investment failing to deliver the expected value by accepting the business case proposing the investment

When dealing with positive risks (opportunities), the terms are usually expressed slightly differently. Risk retention becomes risk exploitation and risk reduction becomes risk enhancement. However, the term risk modification covers both positive and negative risks.

2.2.6 Control

**Control**

The means of managing a risk, ensuring that a business objective is achieved, or that a process is followed.

Risk modification requires implementation of controls to reduce the likelihood or impact of a risk.

A control can be based on technology, for example a firewall or a resilient network configuration, but it can also be related to any of the other dimensions of service management. Some examples of controls for each dimension are shown in Table 2.2.

Table 2.2 Example controls

Domain	Example controls
Organizations and people	Clear desk policy Security awareness training
Information and technology	Network firewall Audit records
Suppliers and partners	Contractual requirements for the supplier to be certified to a quality management system standard Regular audit of supplier activities
Value streams and processes	Evaluation of changes before deployment Reference checks during employee recruitment

2.2.7 Residual risk

Risk treatment does not usually eliminate a risk completely. Therefore, after the application of controls, it is necessary to perform a new risk assessment. This is to understand the new likelihood and impact, and to then calculate the residual risk. The organization could then choose to apply more controls to further reduce the risk. Alternatively, the organization could accept the residual risk which should be documented in the risk register and communicated to the interested stakeholders in the same way as any other retained risk.

2.3 Scope

The scope of risk management is very broad. Most activities and all people within an organization have some role to play in risk management. The service provider must understand and manage the many risks that are relevant to each service and to each customer. This risk management is not a separate activity performed by a separate team, it is an essential part of doing the work. Many of the management practices described in ITIL 4 require risk management as part of their activities. These include:

- **Project management:** every project should have a project risk register, which is maintained throughout the project's lifecycle and used to ensure that project risks are appropriately managed. Some project risks may need to be managed outside the project and for this purpose may be included on other risk registers.
- **Information security management:** this practice includes understanding and managing risks that relate to the confidentiality, integrity, and availability of information. An organization may choose to keep a risk register for information security management, but significant information security risks should also appear on an organizational risk register.
- **Portfolio management:** strategy implementation often requires changing the product and service portfolio and managing the associated risks.
- **Problem management:** every problem is a risk, and problem management activities aim to identify, assess, and control these risks in any of the four dimensions of service management. It is useful to adopt risk management tools and techniques for problem management.
- **Incident management:** diagnosing and resolving incidents can lead to risks. Everyone involved needs to use risk management practices to ensure that they understand what risks are involved, so that these can be managed appropriately.
- **Service continuity management:** this practice is used to manage a wide range of risks that might impact the availability or performance of services.
- **Continual improvement:** many organizations consider management of positive risks to be continual improvement, and only use the term risk management for negative risks.
- **Service level management:** this practice includes identifying and managing any risks that might impact service levels, and reporting these risks to customers and other stakeholders. Service level reporting should include explanations of how these risks will be managed.

There are several activities and areas of responsibility not included in the risk management practice, although they are still closely related to the management of risk. These are listed in Table 2.3, along with references to the Official Practice Guides in which they can be found. It is important to remember that the ITIL practices are merely collections of tools to use in the context of value streams; they should be combined as necessary, depending on the situation.

Table 2.3 Activities related to the risk management practice described in other Official Practice Guides

Activity	Official Practice Guide
Management of specific risks	All practices, especially those listed above
Implementation of changes to mitigate risks	Organizational change management Change enablement Project management
Costs control, financial evaluation of risks and risk mitigation options	Service financial management
Definition of vision and strategic objectives for risk management	Strategy management

2.4 Practice success factors

**Practice success factor (PSF)**

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

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

The risk management practice includes the following PSFs:

- establishing governance of risk management
- nurturing a risk management culture and identifying risks
- analysing and evaluating risks
- treating, monitoring, and reviewing risks.

2.4.1 Establishing governance of risk management

All risk management activities require a clear understanding of the organization's risk capacity and risk appetite. These cannot be defined by practitioners; they are critical aspects of organizational governance. This means that risk management is dependent on the overall governance of the organization.

If this governance is not provided, then practitioners need to respond and ensure that accountability for this is taken by the board of management (or equivalent). If risk management is performed without governance, then it will be difficult to make decisions based on the long-term needs of the organization.

Some risks pose an existential threat to the organization. These risks should be owned by the governing body of the organization. Ideally, the governance of risk management should be regularly discussed in board meetings. Moreover, risk capacity, risk appetite, and strategic risks should also be discussed, agreed, and regularly reviewed in board meetings.

2.4.2 Nurturing a risk management culture and identifying risks

After a risk has been identified, the organization can record it in a risk register and manage it. However, identifying risks can be extremely difficult, as there is no simple process or procedure for identifying risks and most organizations have a large number of unknown risks.

The methods that can help to identify risks are discussed in section 3.1.2, but the most important management activity to support this is nurturing a risk management culture. Everyone in the organization should take responsibility for identifying and reporting any risks that they discover. This requires a culture where people feel safe to identify mistakes made by themselves and others without fear of reprisal. Therefore, managers and leaders need to nurture an open and honest culture.

Employees will anticipate potential problems when risk management is embedded within the culture of the organization. The employees can then consider how to mitigate the risk, whether they are working on strategic initiatives or routine operational tasks.

2.4.3 Analysing and evaluating risks

The analysis of risks involves understanding the likelihood and potential impact of each risk. The analysis can be qualitative or quantitative.

2.4.3.1 Qualitative risk analysis

Qualitative risk analysis uses a simple scale, such as high, medium, or low, to distinguish between different levels of likelihood and impact. Qualitative risk analysis will often utilize a table, which is used to derive an overall risk level from the levels of impact and likelihood, as shown in Figure 2.1.

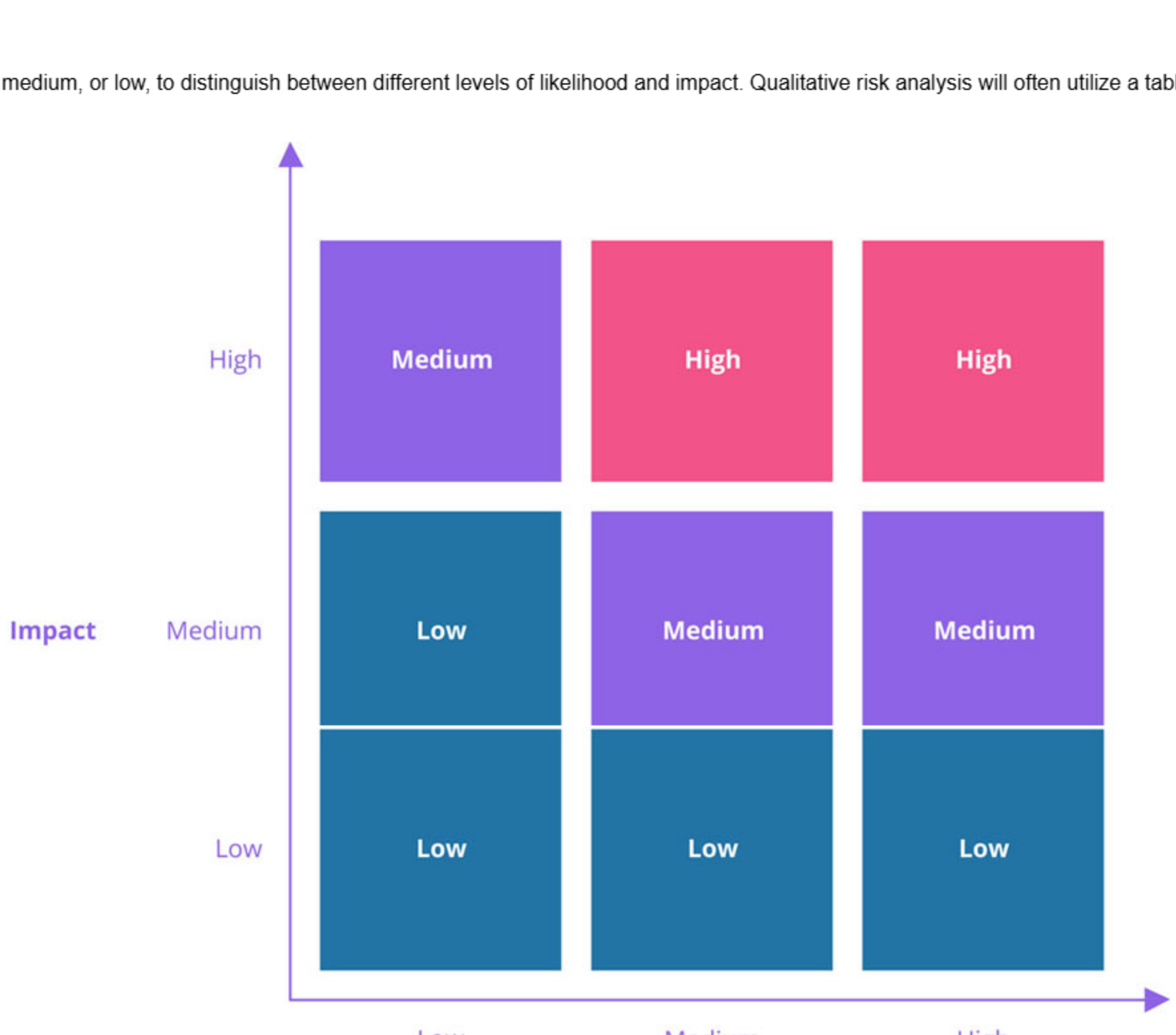


Figure 2.1 Example matrix for qualitative risk analysis

The output of this risk analysis determines the level of risk which is documented in a risk register and used to decide the required risk treatment. In the example in figure 2.1, a risk that has a medium likelihood and a high impact would be rated as a high risk. This result is specific to the organization and cannot be compared with risk analysis from a different organization.

Some organizations use a five-point scale, rather than the simple three-point scale (high, medium or low) illustrated in Figure 2.1, but the approach is still the same.

2.4.3.2 Quantitative risk analysis

Quantitative risk analysis considers the risk impact on a financial basis, as well as on other numerical bases. The likelihood is considered a probability. This risk analysis supports calculations that can be used in a business case to justify investments that may be needed to manage the risk.

- **Annual rate of occurrence (ARO):** the probability that a specific risk will occur in a single year. The annual rate of occurrence is calculated based on the expectations of how frequently the risk is likely to occur. For example, an event that is expected to occur once every fifty years has an ARO of 2%.
- **Single loss expectancy (SLE):** the expected financial loss due to a risk each time that a risk occurs. The SLE is calculated based on the average cost incurred if the risk happened. This is usually expressed in financial terms, but in some organizations, it may be expressed in other measurable ways, such as sales lost.
- **Annualized loss expectancy (ALE):** the expected financial loss due to a risk, averaged over a one-year period. ALE is calculated by multiplying the single loss expectancy (SLE) by the annual rate of occurrence (ARO). The result can then be compared to the cost of controls, so that a decision can be made on how much to invest in managing the specific risk.

2.4.3.3 Combining qualitative and quantitative risk analysis

Quantitative risk analysis is considerably more time-consuming than qualitative risk analysis, so the two are often combined to optimize the time spent analysing data. This involves performing a qualitative risk analysis of every identified risk. Then, a quantitative risk analysis is performed for those risks that exceed a certain threshold for the level of risk and the cost of mitigation. For example, the organization's risk management policy may state that low-rated risks will be managed using controls if the cost of the controls is below £5,000. Quantitative risk analysis will be performed if the cost of the controls is higher than £5,000.

2.4.4 Treating, monitoring, and reviewing risks

Every risk must be treated in the same way. Even if a decision is made to accept a risk, this does not mean that no action will be taken. An accepted risk should be documented, communicated to relevant stakeholders, and reviewed regularly to ensure that changes to the probability, impact, or cost of controls are considered.

When a decision is made to modify a risk, suitable controls need to be designed and implemented. These controls must be maintained to ensure that they remain relevant, and that they are properly implemented to provide the agreed level of protection. For example, if the organization has a clear desk policy, then it is important to communicate this to all staff that may be in a position to leave papers on desks, with regular reinforcement and audits. Similarly, a control that requires all computers to run up-to-date antivirus software must have the technology in place to identify any computers that are not up to date.

Some aspects of defining controls will be described in section 3.2.1, but treating, monitoring, and reviewing risks requires the right balance across all four dimensions of service management. It is not only a process issue.

2.5 Key metrics

Key metrics for the risk management practice are mapped to its PSFs. They can be used as KPIs in the context of value streams to assess the contribution of the practice to the effectiveness and efficiency of those value streams. The key metrics are listed in Table 2.4.

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 Official Practice Guide cannot recommend universal key performance indicators for risk management: the target values for each metric can only be defined in the organization's context.

Table 2.4 Key metrics for the practice success factors

Practice success factors	Key metrics
Establishing governance of risk management	Time since risk appetite and risk capacity were last reviewed and updated Percentage of strategic risks with clearly documented likelihood, impact, owner, treatment plan, and next action date
Nurturing a risk management culture and identifying risks	Percentage of employees who say they feel free to identify risks and mistakes in anonymous surveys Number of risks identified by people who do not work in specific risk management roles
Analysing risks	Percentage of risks on the risk register with clearly documented likelihood, impact, and owner
Treating, monitoring, and reviewing risks	Percentage of risks on the risk register with clearly documented treatment plan and next action date Percentage of risks on the risk register that have been reviewed in the last six months Percentage of controls that have been subject to a control review and audit within the last six months

Chapter 3

Value streams and processes

3.1 Processes

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

Process

Risk management activities form three processes:

- governance of risk management
- risk identification, analysis, and treatment
- risk monitoring and review.

3.1.1 Governance of risk management

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

Table 3.1 Inputs, activities, and outputs of the 'governance of risk management' process

Key inputs	Activities	Key outputs
Environmental factors (PESTLE) Competitive environment Threat environment Regulatory requirements Organization strategy Changes in the organization's context	Monitor the organization and the environment Evaluate the organization and the environment Document risk capacity and risk appetite Document risk management policy and framework Provide direction to management	Risk management framework Risk capacity Risk appetite Risk management policy Budget for risk management Risk management guidelines

Figure 3.1 shows a workflow diagram of the process.

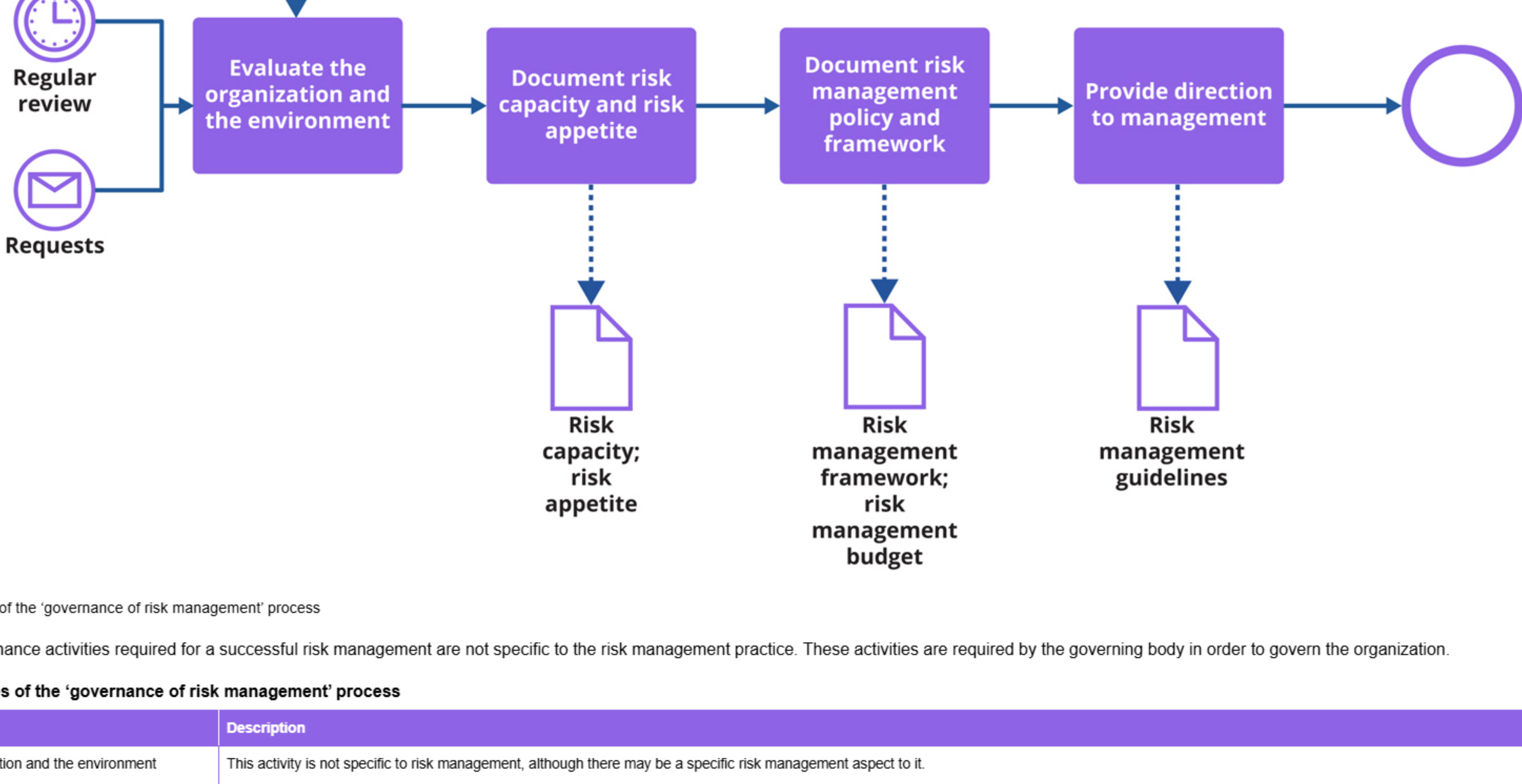


Figure 3.1 Workflow of the 'governance of risk management' process

Many of the governance activities required for a successful risk management are not specific to the risk management practice. These activities are required by the governing body in order to govern the organization.

Table 3.2 Activities of the 'governance of risk management' process

Activity	Description
Monitor the organization and the environment	This activity is not specific to risk management, although there may be a specific risk management aspect to it. The governing body reviews audit and management reports, and monitors the organization and its environment, to ensure that risk management is proceeding according to their intentions and direction. If there are any significant deviations, this may trigger a requirement to re-evaluate the environment and review risk capacity, appetite, and policy.
Evaluate the organization and the environment	This activity is not specific to risk management. The governing body evaluates the organization and its environment, including: <ul style="list-style-type: none">• the PESTLE factors that constrain and influence the organization (political, economic, social, technical, legal, and environmental)• regulatory requirements• the competitive environment• the threat environment. Based on these and other factors, the governing body sets the overall organization strategy, which includes the strategy for risk management. This activity is usually scheduled, typically once a year, but may also be triggered by any event which could impact the organization's strategy, or a stakeholder's request.
Document risk capacity and risk appetite	Based on the evaluation of the organization and the environment, the governing body establishes and documents the risk capacity and risk appetite of the organization.
Document risk management policy and framework	The risk management policy specifies the approach to be taken to identify, analyse, and manage risks. This may include the adoption of specific standards and guidelines, such as ISO 31000. Creation of this policy requires specialist knowledge of risk management, but the decisions and authorization remain with the governing body. The risk management framework specifies the risk analysis method, scope, and objects. It can also include role descriptions for activities such as identification and monitoring. The governing body allocates a budget for risk management, which must be sufficient to support the requirements of the policy.
Provide direction to management	This activity is not specific to risk management (but the specific direction to be provided is about risk management). The governing body shares the risk capacity, risk appetite and risk management policy and framework as appropriate, and provides relevant guidance to ensure that managers and employees throughout the organization are aware of their responsibilities in relation to risk management.

3.1.2 Risk identification, analysis, and treatment

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 'risk identification, analysis, and treatment' process

Key inputs	Activities	Key outputs
Risk management policy Risk management framework Risk appetite Budget for risk management Existing risk register(s) Service portfolio Service models Risks identified as part of other activities Standards and frameworks Threat assessment and vulnerability assessment services from third parties	Risk identification Risk analysis and evaluation Risk treatment	Updated risk register(s) New and updated controls

Figure 3.2 shows a workflow diagram of the process.

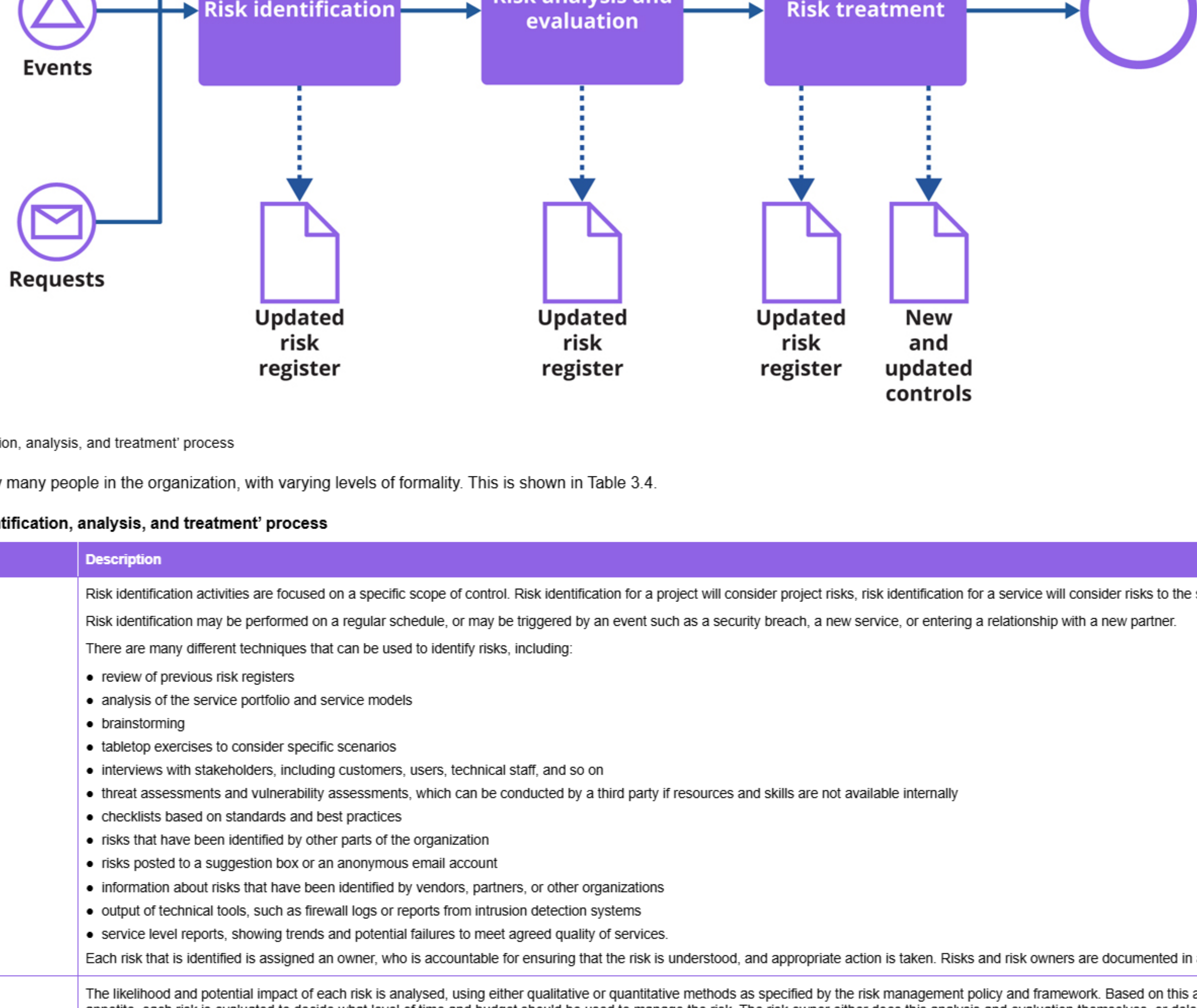


Figure 3.2 Workflow of the 'risk identification, analysis, and treatment' process

These activities may be performed by many people in the organization, with varying levels of formality. This is shown in Table 3.4.

Table 3.4 Activities of the 'risk identification, analysis, and treatment' process

Activity	Description
Risk identification	Risk identification activities are focused on a specific scope of control. Risk identification for a project will consider project risks, risk identification for a service will consider risks to the service, and so on. Risk identification may be performed on a regular schedule, or may be triggered by an event such as a security breach, a new service, or entering a relationship with a new partner. There are many different techniques that can be used to identify risks, including: <ul style="list-style-type: none">• review of previous risk registers• analysis of the service portfolio and service models• brainstorming• tabletop exercises to consider specific scenarios• interviews with stakeholders, including customers, users, technical staff, and so on• threat assessments and vulnerability assessments, which can be conducted by a third party if resources and skills are not available internally• checklists based on standards and best practices• risks that have been identified by other parts of the organization• risks posted to a suggestion box or an anonymous email account• information about risks that have been identified by vendors, partners, or other organizations• output of technical tools, such as firewall logs or reports from intrusion detection systems• service level reports, showing trends and potential failures to meet agreed quality of services. Each risk that is identified is assigned an owner, who is accountable for ensuring that the risk is understood, and appropriate action is taken. Risks and risk owners are documented in a risk register.
Risk analysis and evaluation	The likelihood and potential impact of each risk is analysed, using either qualitative or quantitative methods as specified by the risk management policy and framework. Based on this analysis, and the organization's risk appetite, each risk is evaluated to decide what level of time and budget should be used to manage the risk. The risk owner either does this analysis and evaluation themselves, or delegates it and reviews the findings. The risk register is updated with the output of the risk analysis and evaluation.
Risk treatment	A risk treatment option is chosen for each risk. <ul style="list-style-type: none">• If the risk is accepted, then this decision must be documented and communicated to appropriate stakeholders.• Selection of controls for managing each risk may be based on the risk management policy or framework, on standards and best practices, or may be designed specifically for the situation.• Risk treatment may require design, investment, development, testing, deployment, and other activities. These should all be managed to ensure that the risk treatment is fully implemented as agreed by the risk owner. The risk register is updated to show the risk treatment, including dates of implementation where relevant.

3.1.3 Risk monitoring and review

This process includes the activities listed in Table 3.5 and transforms the following inputs into outputs.

Table 3.5 Inputs, activities, and outputs of the 'risk monitoring and review' process

Key inputs	Activities	Key outputs
Risk management policy Risk register(s) Threat and vulnerability assessment services	Control assessments and evaluation Risk audits	Updated risk register(s) Audit reports Requirements for new and updated controls

Figure 3.3 shows a workflow diagram of the process.

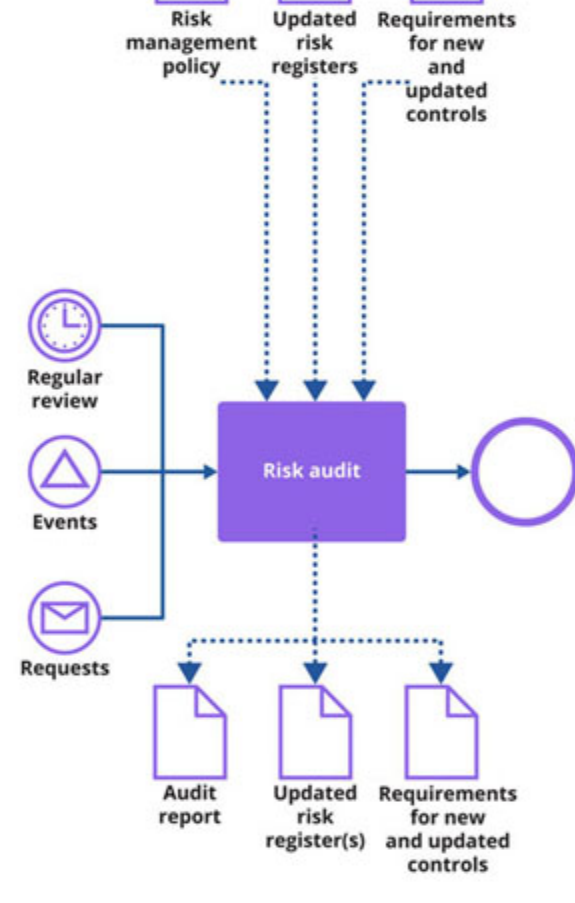


Figure 3.3 Workflow of the 'risk monitoring and review' process

The process activities are described in Table 3.6.

Table 3.6 Activities of the 'risk monitoring and review' process

Activity	Description
Control assessment and evaluation	Control assessment and evaluation ensures that controls have been fully and correctly implemented, and that they are still fit for purpose, and able to provide the level of risk management that is required. This activity should be performed on a regular basis, which in a high-risk environment may be weekly or even daily. It may also be triggered by an event such as a security incident, a new or changed service, or entering a relationship with a new partner. Control assessment analyses the extent to which one or more controls have been implemented. For example, by auditing computers to establish that they have the correct version of anti-virus software installed, or by inspecting offices to see that the clear desk policy is being adhered to. Control evaluation analyses the continuing relevance of the control to determine whether it is still fit for purpose. For example, by determining that the risk the control is intended to modify still exists. Control assessment and evaluation is often performed for a specific subset of controls. Some controls may need to be reviewed every day, but others may need to be reviewed much less frequently. The risk register is updated in updates to risk registers, identification of a need for new or updated controls, or a need for a risk audit.
Risk audit	Audits ensure that risk management remains appropriate and relevant as the environment changes. Audits are usually performed on a scheduled basis, but may be triggered by an event such as a security incident, or entering a relationship with a new partner. Audits may be performed internally, or by third parties. The output of the audit may identify a need to implement new or updated controls, and will provide an input to the 'monitor the organization' activity of the 'governance of risk management' process.

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 identify 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 and the true flows of work, then analyse them in order to identify and eliminate the non-value-adding activities and other forms of waste.

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

Many organizations follow best practice recommendations for various service management practices, such as incident management, change enablement, software development, and many others. However, the practices are often adopted and organized in a siloed, isolated manner, just as they are presented in 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 Risk management in service value streams

Risk management is an important practice for all service value streams as it provides the ability to identify and manage risks that could impact the ability to carry out value stream activities or achieve the intended outcomes. Also, risk management directly contributes to value streams where risks are identified and managed.

Table 3.7 describes how the key service value streams involve risk management.

Table 3.7 Risk management in key service value streams

Value stream	The role of risk management
Creation of a new or changed product or service	Identification and management of risk at all stages of the value stream, including market risks, portfolio risks, technical risks, organizational risks, process risks and others. Management of positive risk (how likely it is that the new or changed service will create the intended value) as well as negative risk (what could go wrong).
Service delivery	Identification and management of risks related to both manual and automated delivery of services, helping to ensure that services are delivered to meet the expectations of service consumers.
Product and service support	Identification and management of risks related to support, including aspects of problem management, incident management, and communication with service users.
Product and service operations	Identification and management of operational risks. Many operational activities are themselves risk controls, for example creating backups, or testing recovery plans.
Continual improvement of products and services	Managing positive risks that can result in improvements to services, practices, or any other aspect of product and service management. Identification and management of risks related to the design or implementation of improvements.

3.2.3 Analysing a service value stream

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

1. **Identify the scope of the value stream analysis:** this 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 consumers, B2B and B2C products, or services based on products developed in-house or sourced externally. Interactions with users and customers during incident handling and resolution may follow different models in each of these scenarios.

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. The definitions of service quality should be aligned with the organization's strategy and support value creation for the organization and other stakeholders.

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? Does it support the relationship approach?)
- effectiveness or performance (is the step performed well?)
- availability (are required resources available to execute the step?)
- capacity (are the 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. Some commonly performed interactions between stakeholders and team members can be undocumented or even contradict the agreed procedures.

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 ITIL® 4 Continual Improvement Official Practice Guide for a practical improvement model. Include relationship models in the continual improvement plan for the value streams.

3.2.3.2 Risk management considerations in a service value stream analysis

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

• At the scoping step (1), identify all external and internal stakeholders related to the value stream. What risks should they be identifying? What risk management activities should they be performing? Do they contribute to or use risk registers?

• During the service value stream walk (3a), identify the practices involved at every step and how risks are managed. What specific actions are taken to identify risks? What is done when risks are identified? Are there situations where risks are not identified and managed? Are people aware of their risk management responsibilities? Do they understand the organization's risk appetite and risk management policy?

• During the workflow steps evaluation (3c), evaluate the impact of risk management on the value stream's effectiveness and efficiency. Does risk management stimulate the right behaviour? Does risk management create any delays in the value stream? Are risks reliably identified? Are risk registers available and used when appropriate? Are people suitably trained and is a risk management culture nurtured appropriately?

• At the reflection and planning steps (4.5), ensure that risk registers are available to the relevant stakeholders throughout the value stream and their provision and use are optimized for business value. Ensure that risks are communicated appropriately, and that risks are actively managed rather than just identified and logged. Consider whether training and encouragement of staff is sufficient.

• Include the creation or update of risk registers, improvements to how risks are managed and communicated, and improvements to risk management training and culture in the value stream improvement plans (6).

Chapter 4

Organizations and people

4.1 Roles, competencies, and responsibilities

4.1.1 Risk manager

Every organization requires a risk manager, but this role is often combined with other roles depending on the size and nature of the organization. In some organizations there may be a risk management committee that takes on this role, led by a dedicated risk manager.

This role is typically responsible for:

- working with the board (or other governance entity) to establish and communicate the organization's risk capacity and risk appetite
- documenting and managing the organization's risk management policy and framework
- nurturing a risk management culture across the organization
- managing the organization's risk management budget
- establishing a hierarchy, structure, and format of risk registers to be used throughout the organization
- managing the highest level risk register that includes strategic risks that might impact the whole organization
- ensuring that the performance of risk management is monitored, reviewed and improved.

4.1.2 Risk owner

Every risk must have an assigned owner who is accountable for ensuring that the risk has been understood and appropriately managed. The risk owner should be assigned as soon as the risk has been identified and should be documented in the risk register.

The risk owner may not be responsible for the actions needed to manage the risk, but they must ensure that these actions are appropriate and that they are actually taken.

4.1.3 Risk management roles in an organization

The ITIL practices 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 profile

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

The roles which are typically involved in the risk management activities are listed in Table 4.2, together with the associated competency profiles.

Table 4.2 Roles involved in the risk management activities

Activity	Responsible roles	Competency profile	Specific skills
Governance of risk management			
Monitor the organization and the environment	Risk manager	TA	Visibility over organization performance metrics
Evaluate the organization and the environment	Risk manager (on behalf of the board of directors)	TCMA	Visibility across PESTLE factors influencing the organization
Document risk capacity and risk appetite	Risk manager	MCTA	Ability to define concise, holistic and objective systems of risk indicators
Document risk management policy and framework	Risk manager	MCTA	Awareness of the organization's specific documentation requirements
Provide direction to management	Risk manager Finance manager or budgeting committee	CLT	Enabling communication channels; ensuring ongoing engagement of managers to ensure clarity, and ongoing realization of risk management policies
Risk identification, analysis, and treatment			
Risk identification	Subject matter expert Service or Product owner	TA	Professional competencies and visibility over PESTLE factors that influence the object in scope of risk assessment
Risk analysis and evaluation	Subject matter expert Risk owner	TAC	Ability to systematically apply qualitative and quantitative risk analysis tools and draw conclusions
Risk treatment	Risk owner, cyber security, project managers, service continuity manager	TMCA	Project management skills
Risk analysis and evaluation	Subject matter expert Risk owner	TAC	Ability to systematically apply qualitative and quantitative risk analysis tools and draw conclusions
Risk treatment	Risk owner, cyber security, project managers, service continuity manager	TMCA	Project management skills
Risk monitoring and review			
Control assessment and evaluation	Risk owners Risk manager	MTCA	Awareness of existing controls and control maintenance requirements as set out in the risk management policies
Risk audit	Internal and external auditors	MTAC	Audit management techniques Command of common audit practices Assured auditor integrity, objectivity and independence

4.2 Organizational structures and teams

The risk management practice underpins everything that the service provider does to enable value co-creation. Therefore, the practice is everyone's responsibility, within their scope of control. This scope of control may be quite narrow for junior staff, but everyone must identify and manage risks that could impact their ability to perform their role or deliver expected results.

In a large commercial organization, the board of directors (or other governing body) is accountable to the organization's stakeholders, for implementing a risk management framework. The ongoing development of the risk management framework is usually delegated to a risk manager or one or more risk management committees and is under the board's oversight.

The risk management framework defines the risk analysis method, scope, and objects. Role descriptions, such as identification and monitoring, can be contained within the framework even for operational line staff, depending on the organizational design for risk management activities. The key goal of the governing body is to ensure that all tiers of management in the service provider organization implement the risk management framework within their scopes of control.

Different aspects of risk management will be delegated to specific groups within the organization; for example, the information security team may be responsible for cyber risks, while the finance team is responsible for financial risks, and the facilities team is responsible for risks related to buildings and infrastructure. This delegation of risks must be clearly defined to ensure that significant risks do not get missed because everyone thinks they are someone else's responsibility.

In a small organization, the role of risk manager may be combined with other roles, such as information security manager or operations manager, but these need to be senior roles that work with the organization's governing body. It is essential that the scope of risk management remains wide enough to cover all risks, and not just those related to information security, operations, or other areas of responsibility. It is also important that everyone in the small organization understands their risk management responsibilities and supports the risk manager when needed.

In a product focused organization, each product team takes responsibility for risks related to their product, but there also needs to be an overall risk manager, or risk management committee, that considers organization-wide risk, helps to define the risk management framework, and ensures that risk management is effective. It is also essential that risk registers are coordinated so that risks that start out on a product specific risk register can be moved (or reflected) in a higher level risk register when necessary, and that risks that might impact multiple products can be identified and a consistent risk management approach adopted.

Chapter 5

Information and technology

5.1 Information exchange: inputs and outputs

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

- the risks that the risk owners own
- raising a new risk record
- an easily identifiable and objective risk importance
- forecasted and appropriately assigned tasks.

This information may take various forms. For example, a risk register may be as simple as a spreadsheet used to log and manage risks in a small team, or as complex as a dedicated risk management tool that coordinates multiple risk registers across a large and complex organization.

The key inputs and outputs of the practice are listed in chapter 3.

5.2 Automation and tooling

The risk management practice can significantly benefit from automation. Where this is possible and effective, it may involve the solutions outlined in Tables 5.1 and 5.2.

Table 5.1 Automation solutions for the risk management practice

Automation tools	Application in risk management
Analysis and reporting tools	Analysis of risks Creation of risk audit reports
Automated testing tools	Control assessment and evaluation
Business process modelling tools	Identification of risks Evaluation of risk impact
Collaboration and communication tools	Working across practices to integrate risk management into value streams for designing, creating, maintaining, monitoring, and continually improving services Communicating about risks to stakeholders
Enterprise architecture management tools	Identifying risks Evaluating risk impact
Knowledge and document management tools	Sharing knowledge and information about risk policy and framework, risk appetite, risk management tools, controls, and priorities Communicating about risks to stakeholders Creating and maintaining risk registers
Learning management systems	Educating stakeholders in risk management to help nurture a risk management culture Assessing effectiveness of risk management training and communications
Monitoring and event management tools	Identifying when a potential risk has been realized and triggering corrective action
Risk management tools	Identifying risks Assessing and lifecycle management of risks Creating and maintaining risk registers
Service catalogue tools	Identifying risks Evaluating risk impact
Service configuration management tools	Identifying risks Evaluating risk impact
Web portals and social media	Communicating about risks and helping to nurture a risk management culture
Workflow and task management tools	Managing the lifecycle of identified risks

Table 5.2 Automation solutions for risk management activities

Process activity	Means of automation	Key functionality	Impact on the effectiveness of the practice
Governance of risk management			
Monitor the organization and the environment	Collaboration and communication tools Learning management systems Knowledge and document management tools Enterprise architecture management tools, business process modelling tools, service catalogue tools, service configuration management tools	Capturing and analysing information about the environment in which services are delivered and consumed	High
Evaluate the organization and the environment	Collaboration and communication tools Learning management systems Knowledge and document management tools Enterprise architecture management tools, business process modelling tools, service catalogue tools, service configuration management tools	Capturing and analysing information about the environment in which services are delivered and consumed	High
Document risk capacity and risk appetite	Risk management tools, knowledge and document management tools	Documentation and communication of risk capacity and appetite	Medium
Document risk management policy and framework	Risk management tools, knowledge and document management tools	Risk management framework, including the policy, guidelines, existing and prospective controls, as well as the risk register, needs to be easily accessible by the service provider staff; external stakeholders, such as customer representatives and regulators, should also have adequate visibility over the framework	High
Provide direction to management	Risk management tools, collaboration and communication tools, knowledge and document management tools		High
Risk identification, analysis, and treatment			
Risk identification	Automated testing tools, business process modelling tools, enterprise architecture management tools, risk management tools, service catalogue tools, service configuration management tools, web portals, and social media	Many different tools can help to identify risks, each within its own context. Some tools help to identify strategic and business risks, others can identify technical or people risks	High
Risk analysis and evaluation	Risk management tools, business process modelling tools, enterprise architecture management tools, service catalogue tools and service configuration management tools, analysis and reporting tools	Depending on the nature of the identified or updated risk, analysis can be underpinned by a variety of management systems data. Risk owner ensures that analysis and evaluation decisions are informed	High
Risk treatment	Workflow and task management tools	Risk countermeasures, whether one-off or ongoing, technical, organizational, or otherwise, should be implemented in a controlled manner, ensured by existing change management and project management tools	Medium
Risk monitoring and review			
Control assessment and evaluation	Risk management tools, analysis and reporting tools, automated testing tools, learning management systems, knowledge and document management tools	The assessors should have access to the risk management framework including the risk register, although risk management culture within the organization must be observed through non-automated interactions	Medium
Risk audit	Risk management tools, analysis and reporting tools, business process modelling tools, knowledge and document management tools	The auditors should have access to the risk management framework including the risk register, although risk management culture within the organization must be observed through non-automated interactions They also need access to enterprise architecture and business process modelling tools to evaluate the relevance of controls to the current business needs	Medium

5.2.1 Recommendations for automation of risk management

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

- **Integrate risk controls in the automated workflows:** make sure that, where possible, risk controls are integrated in the organization's workflows and workflow management tools. This can be achieved in many ways, from simple reminders for employees to consider relevant risks, to AI-enabled assessment of risks and optimization or interruption of the workflows.
- **Collect and analyse risk data from multiple sources:** integrate risk-focused monitoring at multiple levels, from digital infrastructure to the organization's status and environment. Automate data gathering, processing, and presentation as much as possible.
- **Ensure high quality of risk records:** risk registers should provide high-quality input to analysis of risks and effectiveness of risk treatments, assessment and planning of risk appetite and capacity, and automation of risk management activities.
- **Use AI to enhance risk monitoring and assessment:** especially when risks originate from complex combinations of threats and vulnerabilities (rather than a simple causation scenario).
- **Consider specialized risk management tools:** specialized risk assessment and management tools are available for many industries and business profiles. If applicable to the organization, consider use of these tools; however, make sure that the tools are tailored to the strategy, risk capacity, and risk appetite of the organization. At the same time, do not leave areas and aspects of the organization and environment not currently covered by the specialized tools without attention.
- **Integrate risk management processes with tools:** ensure that risk management processes are effectively integrated by relevant automation tools, preventing gaps between governance, execution, and review of risk management.

Chapter 6

Partners and suppliers

6.1 Dependencies on third parties

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 ITIL practices for supplier management and service level management.

Partners and suppliers to the service provider can generate and mitigate risks to the service provision and change profiles of the existing ones. The service provider needs to be aware of the latter, when onboarding new partners and suppliers.

It is also crucial that the risk management frameworks for the parties are mutually aligned, and appropriate communication channels are established between respective risk owners. For example, a failure within a supplier managed infrastructure segment needs to trigger the response for the service provider risk mitigation. Risk identification and proper signalling must be built into the service model, with a supplier, and regularly tested.

Although the actual risk mitigation activities are likely to be covered by other practices, it is the risk management practice that covers the risk management framework alignment among the parties. The practice also ensures that the parties invest the appropriate amount of effort into risk identification and analysis.

Where organizations aim to ensure fast and effective risk management practice, they usually try to agree to close cooperation with their partners and suppliers, removing formal bureaucratic barriers in communication, collaboration, and decision-making. All parties in such relationships should aim for mutual transparency and visibility of the changes that may affect the other parties (see the ITIL® 4 Supplier Management Official Practice Guide for more information). Even if these informal processes are effective, it is still important that risk management is specified in contractual documents to ensure that the requirements are clearly understood.

6.2 Support from third parties

Partners and suppliers may also provide services and solutions to support the risk management practice. The organization should ensure the methods used and reports provided by the supplier are relevant and meet the requirements of the organization. It is also important to ensure that the supplier's access to the organization's data is approved by the organization and meets its information security policies.

Third party support for risk management may include:

- **Provision of software tools:** most software tools used for risk management are shared with other practices. However, some tools may be acquired and used exclusively to manage risks. The organization should define the automation requirements from all related practices to ensure that the right tools are procured, implemented, and used in an optimal way.
- **Performing threat assessments:** a third party may have specialist knowledge of the threat environment, based on their experience with a specific industry, location, technology, or a wider skill in the area of threat assessments. This can help to ensure that threats are correctly identified and analysed and make significant contributions to risk identification.
- **Performing vulnerability assessments:** a third party with specialist tools or knowledge of the technology platform may be able to carry out vulnerability assessments more effectively, more frequently, or at a lower cost than trying to do this using the service provider's own resources. Many organizations use third party vulnerability assessment services to help identify technology risks, and assess the effectiveness of controls.
- **Performing risk audits:** a third party can provide an independent view of risk management effectiveness. This may be required to demonstrate compliance with a standard or other external framework, or for legal, regulatory, or contractual reasons.
- **Consulting and advisory:** specialist suppliers who have developed expertise in risk management can help establish and develop the practice, adopt specific methods and techniques, and initially develop the risk management policy and framework. However, risk management cannot be completely delegated to an external consultant.

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. The ITIL maturity model defines the following capability levels applicable to any management practice:

- Level 1** The practice is not well organized; it is 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 2 to level 5. 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 practice automation are typically defined at level 3 or higher because effective automation is only possible if the practice is well-defined and organized.

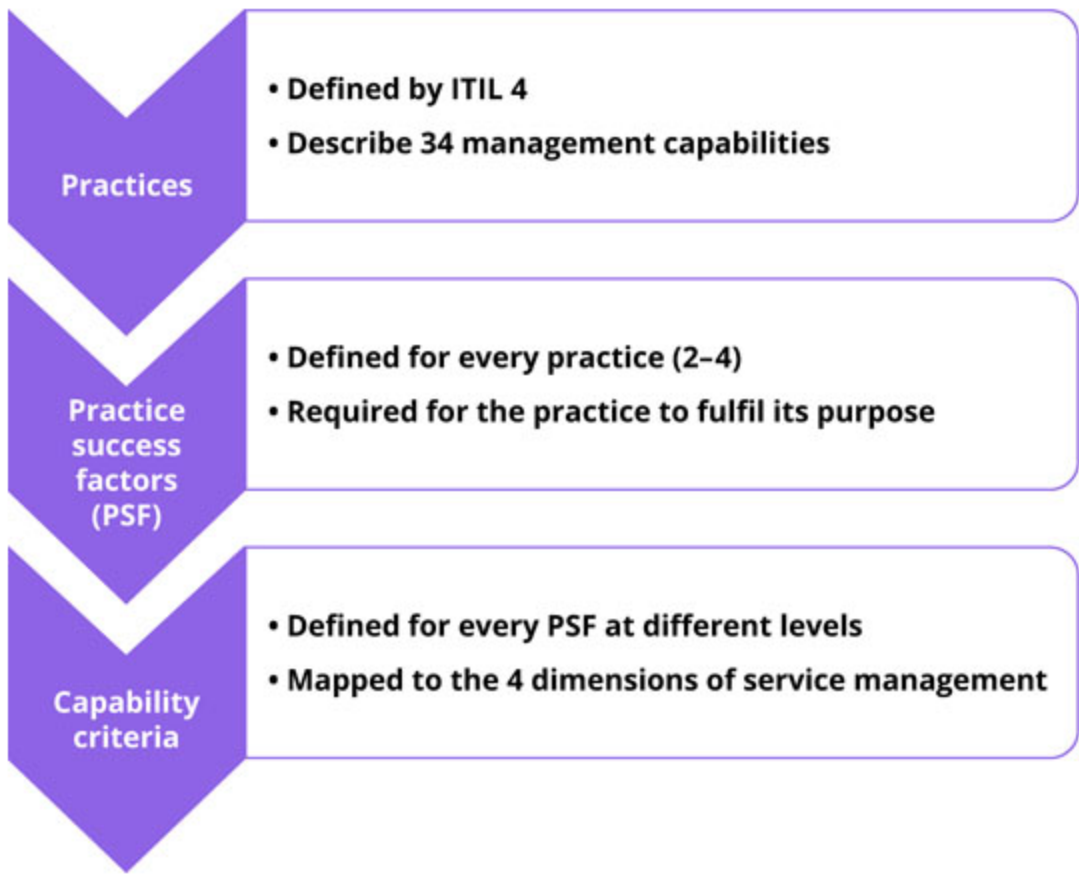


Figure 7.1 Design of the capability criteria

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 risk management practice.

Table 7.1 Risk management capability criteria

PSF	Criterion	Dimension	Capability level
Establishing governance of risk management	Risk management activities are governed at the organizational governance level	Value streams and processes	4
	The risk management framework is regularly reviewed and continually improved	Value streams and processes	5
Nurturing a risk management culture and identifying risks	Risks are identified and registered	Value streams and processes	2
	Members of the organization know how to identify and manage risks	Organizations and people	2
	Risk identification is consistent across various value streams	Value streams and processes	3
	Responsibility for risk identification and registration is clearly assigned	Value streams and processes	3
	Common principles of risk identification and management are defined and shared by the members of the organization	Organizations and people	3
	The organization's principles of risk identification and management are shared with and accepted by the key members of the organization's supply chain	Partners and suppliers	3
	Information about risks is tracked and kept up to date in an integrated information system	Information and technology	4
Analysing and evaluating risks	Identified risks are analysed and evaluated	Value streams and processes	2
	Responsibilities for risk analysis and evaluation are clearly assigned	Value streams and processes	3
	The competencies required for risk analysis and evaluation are identified and sourced in an agreed way	Organizations and people	3
	Partners and suppliers are involved in risk analysis and evaluation when necessary	Partners and suppliers	3
	The performance of risk analysis and evaluation is tracked and assessed	Value streams and processes	4
	Risk analysis and evaluation is tracked in an integrated information system	Information and technology	4
	Risk analysis and evaluation is regularly reviewed and continually improved	Value streams and processes	5
Treating, monitoring, and reviewing risks	Risks are treated, monitored, and reviewed	Value streams and processes	2
	The responsibilities for treating, monitoring, and reviewing risks are clearly assigned	Value streams and processes	3
	The competencies required for treating, monitoring, and reviewing risks are identified and sourced in an agreed way	Organizations and people	3
	Partners and suppliers are involved in treating, monitoring, and reviewing risks when necessary	Partners and suppliers	3
	The performance of treating, monitoring, and reviewing risks is tracked and assessed	Value streams and processes	4
	The treating, monitoring, and reviewing of risks is tracked in an integrated information system	Information and technology	4
	The treating, monitoring, and reviewing of risks is regularly reviewed and continually improved	Value streams and processes	5

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

7.2 Capability self-assessment

A 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 the 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 Risk management capability development

Management practices should support the achievement of the organization's objectives and enable the creation of value for 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. No organization requires all management practices to be at capability level 5. A higher capability level provides higher assurance of the fulfillment of the practice's purpose, but it comes with a cost: the cost of management, automation, and training, for example. To achieve optimal performance with a 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 Official Practice Guide is aligned with the development steps.

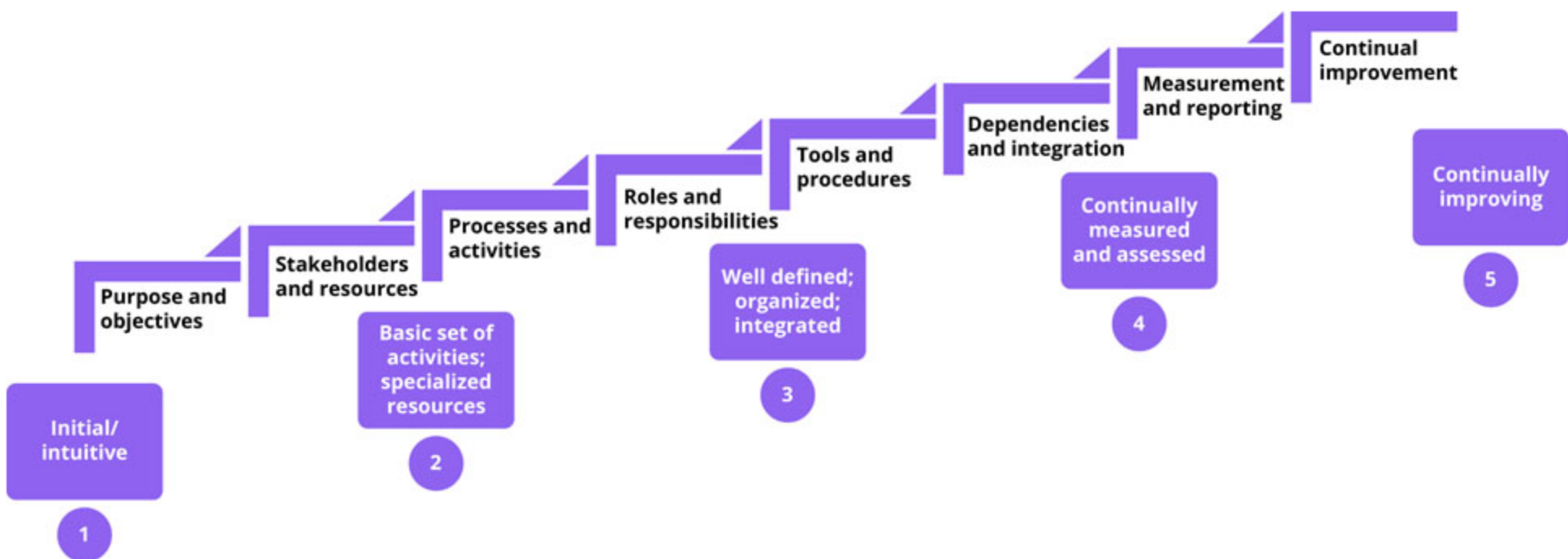


Figure 7.2 The capability development steps and levels

Table 7.2 The risk management capability development steps

Capability level	Define, agree, and implement	Comment for risk management	Chapter (for recommendations)
2	Purpose and objectives	Strategy and services	2.1
	Scope	Relationships with other practices	2.3
	Processes and activities	Risk lifecycle management, assessment, and audit	3.1
	Roles and responsibilities	Roles and responsibilities, automation, and information exchange	4
	Tools and procedures		5
3	Dependencies and integration	Risk governance	3.2
		Integration in the organization's service value streams	
		Use of integrated information system	5
		Suppliers and other parties involved in risk management	6
4	Measurement and reporting	Metrics	2.5
5	Continual improvement	Regular review of practice and the risk management capability development	2.4, 2.5, 7

Chapter 8

Recommendations for practice success

Most of the content of the Official 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 Official 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.

In Table 8.1, recommendations for the success of the risk management practice are linked to the relevant guiding principles.

Table 8.1 Recommendations for the success of risk management

Recommendation	Comments	ITIL guiding principles
Understand and communicate the risk appetite	It is not possible to eliminate all risks, so everyone in the organization needs to understand what level of risk is acceptable and what needs to be addressed.	Focus on value Collaborate and promote visibility Keep it simple and practical
Encourage and reward people who identify risks	It is essential to create a culture where people feel safe to identify and report risks. This can be facilitated by recognizing and rewarding this behaviour, rather than the very common approach of blaming people for not preventing risks.	Collaborate and promote visibility Progress iteratively with feedback
Consider risks from all four dimensions of service management	Many organizations focus exclusively on risks from technology or from people. It is equally important to consider suppliers and partners, and value streams and processes.	Think and work holistically Focus on value
Identify and manage strategic, tactical, and operational risks	Some organizations only consider strategic risks, others tend to focus on project risks or operational risks. It is important to have multiple risk registers, each of which is focused on a particular area or domain, so that all risks can be given appropriate consideration, with appropriate levels of management involvement.	Focus on value Keep it simple and practical
Automate risk treatment where practical	A risk treatment plan that is not used when needed has no value. The plan is only effective if people recognize when the risk has been realized and take the appropriate action. This can best be achieved by automation.	Optimize and automate Keep it simple and practical
Integrate risk management into the organization's value streams	Risk management needs to be integrated with many other practices to ensure that risks are identified, logged, treated, and managed throughout their lifecycle.	Think and work holistically Collaborate and promote visibility



Glossary

control

The means of managing a risk, ensuring that a business objective is achieved, or that a process is followed.

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.

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.

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

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

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.

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.

risk

A possible event that could cause harm or loss, or make it more difficult to achieve objectives. It can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.

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.

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.

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.



Index

C

control, 5, 7-9, 11-13, 17-19, 21-22, 29, 33, 35-36, 40, 51-52

F

four dimensions of service management, 5, 9, 12, 43-44, 49, 51-52

I

information and technology, 3, 8, 44-45, 51

ITIL continual improvement model, 51

ITIL guiding principles, 49, 51

ITIL maturity model, 43-44, 51

ITIL service value chain, 51

M

metric, 12-13, 28, 47, 51

O

organization, 3, 5-12, 15-18, 21-24, 26-30, 33-36, 39-40, 43-47, 49, 51-52

organizations and people, 3, 8, 26, 44-45, 51

output, 11, 15, 17-19, 21, 33, 51

P

partners and suppliers, 3, 38-39, 44-45, 51

practice, 3, 5, 8-9, 12-13, 15-16, 18-19, 21-24, 27, 29, 33-34, 39-40, 43-49, 51-52

practice success factor, 9, 12-13, 43, 51

process, 3, 8, 10, 12, 14-23, 27-28, 33-36, 39, 44-46, 49, 51-52

R

risk, 3, 5-13, 15-22, 24, 27-30, 33-36, 39-40, 44-47, 49, 51

S

service provider, 5, 8, 29, 35, 39-40, 45-46, 51-52

service provision, 39, 52

service relationship, 39, 51-52

service value system, 5, 43, 51-52

stakeholder, 6, 8-9, 12, 16, 18-19, 22-24, 28-29, 33, 35, 45-46, 51-52

supplier, 3, 8, 38-40, 44-45, 47, 49, 51-52

U

user, 18, 22-23, 52

V

value, 3, 5, 7-9, 12, 14, 21-24, 29, 33, 43-47, 49, 51-52

value stream, 5, 8-9, 12, 14, 21-24, 33, 44-45, 47, 49, 52

value streams and processes, 8, 14, 44-45, 49, 52