BSB 7.0

BSBXCS403

CONTRIBUTE TO CYBER SECURITY THREAT ASSESSMENTS

Aspire
Learning Resources

BSBXCS403

Contribute to cyber security threat assessments

Release 1

Learner Guide

Aspire Version 1.1

Aspire
Learning Resources

Aspire also has learning resources available in these areas:

- Foundation skills
- LLN and employability skills (non-competency)
- Community services
- Early Childhood Education and Care
- Allied health

Aspire is committed to developing quality resources that meet the needs of our customers. However, occasionally Aspire finds, or is notified of, errors. Please refer to our website at www.aspirelr.com.au to see if there are any updates that may be relevant to you.

Every effort has been made to ensure the information in this book is accurate; however, the author and publisher accept no responsibility for any loss, damage or injury arising from such information.

Except where an information source is acknowledged, the names and details of individuals and organisations used in examples are fictitious and have been devised for learning purposes only. Any similarity to actual people or organisations is unintentional.

All websites referred to in this unit were accessed and deemed appropriate at time of publication.

Aspire Training & Consulting apologises unreservedly for any copyright infringement that may have occurred and invites copyright owners to contact Aspire so any violation may be rectified.

Acknowledgement

Aspire Learning Resources wishes to acknowledge Hivint for providing an industry validation review of this Learner Guide. Hivint is a cybersecurity consultancy with offices in Melbourne, Sydney, Perth and Brisbane that provides leading edge security advisory and assurance services. We are grateful for their contribution.

BSBXCS403 Contribute to cyber security threat assessments, Release 1

Level 1, 464 St Kilda Road
MELBOURNE VIC 3004 AUSTRALIA
Phone: (03) 9820 1300

First published December 2020

Cover design: Anne-Marie Reeves Design
Printer: Doculink Australia Pty Ltd, 1d/28 Rogers Street, Port Melbourne VIC 3207

e-ISBN 978-1-76075-983-4 (PDF version)
ISBN 978-1-76075-982-7

Contact details

Participant
Name:
Start date:
Phone number:
Email:
Work location
Name:
Address:
Postal address:
Workplace supervisor name:
Phone number:
Fax:
Email:
Registered Training Organisation (RTO)
Name:
Address:
Postal address (if different):
Phone number:
Fax:
RTO contact name:
Mobile:
Email:

CONTENTS

Before you begin

This Learner Guide is based on the unit of competency *BSBXCS403 Contribute to cyber security threat assessments*, Release 1. Your trainer or training organisation must give you information about this unit of competency as part of your training program. You can access the unit of competency and assessment requirements at: www.training.gov.au.

How to work through this Learner Guide

This Learner Guide contains a number of features that will assist you in your learning. Your trainer will advise which parts of the Learner Guide you need to read, and which Practice Tasks and Learning Checkpoints you need to complete. The features of this Learner Guide are detailed in the following table.

Feature of the Learner Guide	How you can use each feature
Learning content	Read each topic in this Learner Guide. If you come across content that is confusing, make a note and discuss it with your trainer. Your trainer is in the best position to offer assistance. It is very important that you take on some of the responsibility for the learning you will undertake.
Examples	These highlight key learning points and provide realistic examples of workplace situations.
Practice Tasks	Practice Tasks give you the opportunity to put your skills and knowledge into action. Your trainer will tell you which practice tasks to complete.
Summaries	Key learning points are provided at the end of each topic.
Learning Checkpoints	There is a Learning Checkpoint at the end of each topic. Your trainer will tell you which Learning Checkpoints to complete. These checkpoints give you an opportunity to check your progress and apply the skills and knowledge you have learnt.

Foundation skills

As you complete learning using this guide, you will be developing the foundation skills relevant for this unit. Foundation skills are the language, literacy and numeracy (LLN) skills and the employability skills required for participation in modern workplaces and contemporary life.

The following table provides definitions for each foundation skill.

Foundation skill area	Foundation skill description
Learning	▪ Modifies behaviour following exposure to new information
Numeracy	▪ Interprets mathematical data ▪ Completes at times complex calculations and records mathematical data
Oral communication	▪ Asks open and closed probing questions and actively listens to clarify consultations ▪ Communicate findings of assessment of business impact to required personnel
Reading	▪ Recognises and interprets information from relevant sources to determine organisational expectations
Writing	▪ Uses clear, specific and industry-related terminology relating to cyber security ▪ Produces written reports on business impact of assessed threat
Teamwork	▪ Works collaboratively with interdisciplinary teams to ensure procedures are implemented
Technology	▪ Uses appropriate technology platforms to assist with cyber security threat assessments

What do you already know?

Use the following table to identify what you may already know. This may assist you to work out what to focus on in your learning.

Topic	Key outcome	Rate your confidence in each section
Topic 1: Contribute to cyber security audits	1A Identify policies, procedures and legislation	❑ Confident ❑ Basic understanding ❑ Not confident
	1B Contribute to cyber security audits	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 2: Conduct risk assessments	2A Assess cyber security risks	❑ Confident ❑ Basic understanding ❑ Not confident
	2B Assign risk levels	❑ Confident ❑ Basic understanding ❑ Not confident
	2C Identify security strategies	❑ Confident ❑ Basic understanding ❑ Not confident
Topic 3: Finalise threat assessment	3A Document threat assessment	❑ Confident ❑ Basic understanding ❑ Not confident
	3B Communicate threat assessment	❑ Confident ❑ Basic understanding ❑ Not confident
	3C Update threat assessment based on feedback	❑ Confident ❑ Basic understanding ❑ Not confident
	3D Distribute and store threat assessment	❑ Confident ❑ Basic understanding ❑ Not confident

Topic 1 | Contribute to cyber security audits

1A Identify policies, procedures and legislation

1B Contribute to cyber security audits

1A Identify policies, procedures and legislation

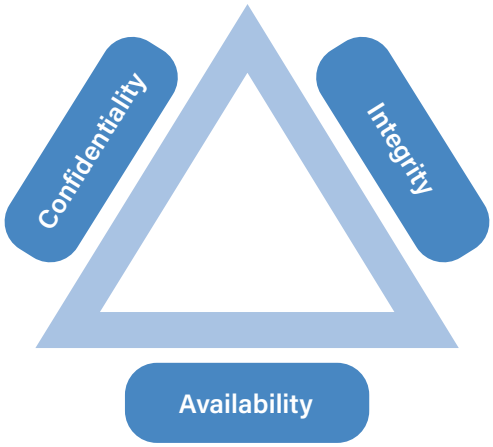
Check the paperwork before the audit begins.

Cyber security threat assessments and audits are valuable tools. They help ensure that an organisation's data and information is secure. They also determine if the information is managed according to information and communications technology (ICT) policies and procedures, as well as local and international legislation.

Workplace policies and procedures

Policies and procedures should be in place in order to protect data confidentiality, integrity and availability.

There are three principles that underpin an organisation's data security: confidentiality, integrity and availability. This is referred to as the CIA Triad.



Every potential data security issue and control can be related back to one or more of these three principles. Each principle is briefly explained in the following table.

Data confidentiality	This principle relates to protecting sensitive data and information from unauthorised access and use. Confidential data breaches may be intentional such as when hackers steal passwords and exploit security weaknesses. The breaches may also be unintentional such as when a staff member accidentally sends sensitive information to the wrong person, or accidentally publishes private information to a public website.

Data integrity

This principle relates to ensuring sensitive data is not manipulated, rendering it inaccurate or incomplete. As with confidentiality, the integrity of data can be threatened by malicious actions to corrupt it, for example by using malware or hacking into databases to change records. It is also subject to unintentional damage, either via user error or a system malfunction causing data loss.

Data availability

This principle relates to ensuring authorised users have efficient and uninterrupted access to sensitive data when required. Attacks such as a Denial of Service (DoS) attack, are designed to slow down systems and compromise data availability. Physical malfunctions can also result in downtime of critical systems, thereby restricting access to data.

All organisations should have policies and procedures in place relating to one or more of the CIA principles. The cyber security audit process should confirm that these policies and procedures are:

- being followed
- enabling the organisation to meet the CIA principles.

A selection of key workplace policies and procedures relevant to data confidentiality, integrity and availability are outlined in the following table.

Acceptable use policy	This policy specifies the ways staff are permitted to access and use information stored on an organisation's system. Typically, this policy specifies that organisational information: ▪ may only be used for the purpose of completing legitimate work tasks ▪ must not be used for any purpose other than in the context of performing work tasks. The policy may also specify activities which are classified as 'Unacceptable Use', such as: ▪ introducing malware to an organisation's network ▪ sharing personal passwords ▪ using an organisation's devices and network to harass others. This policy helps organisations to maintain data confidentiality.

Access control policy	Data held by the organisation should not be accessible to all employees. An access control policy outlines management of sensitive information. The policy may contain details about: ▪ the different types of account used in the organisation ▪ the conditions and access levels for each account type ▪ the process for authorising new accounts, and for changing the level of access for existing accounts ▪ the process for deactivating redundant accounts ▪ the way system usage is monitored. This policy helps to ensure that information can only be accessed by authorised users and helps organisations to maintain data confidentiality.
Information security policy	An information security policy is a wide-reaching policy that outlines a number of information security related controls. It might include details such as: ▪ types of infrastructure and information that need protecting ▪ classification of an organisation's information (from publicly accessible to highly confidential) ▪ typical threats to the organisation's security ▪ staff responsibilities (this section may include similar information to the acceptable use policy) ▪ access controls (this section may include similar information to the access control policy) ▪ rules for connecting external devices to the organisation's network, or for using remote access ▪ penalties for security violations ▪ procedures to be followed in the event of a security incident. This policy helps organisations to meet CIA requirements.
Data integrity policy	The aim of a data integrity policy is to ensure an organisation's information is both correct and complete. This may include identifying control measures such as: ▪ reconciliation routines that check data has not been modified ▪ verification programs that check the consistency of data held on the organisation's networks ▪ processes to monitor system performance and identify attempts to corrupt data integrity ▪ processes to report suspected damage to data integrity. The policy helps organisations to maintain data integrity.

Disaster recovery policy	This policy describes the processes in place to recover an organisation's ICT systems, applications and data in the event of a disaster (defined as any event which causes a major outage or service delay). ▪ This policy may include details of: ▪ immediate actions to take in the event of a disaster ▪ the order in which systems should be brought back online (in order of importance) ▪ the location of data back-ups and how to recover them ▪ the equipment essential to getting the organisation back online ▪ how frequently the disaster recovery plan should be updated. The disaster recovery policy may form part of an overall business continuity plan. This policy helps organisations to maintain data availability.

Policies and procedures such as those outlined above must be regularly reviewed and maintained in order to adapt to new technologies and emerging threats. While responsibility for this usually rests with an information systems security officer, you need to be aware of how to access these documents and their content. You should be able to locate relevant policies and procedures in a central location such as your organisation's quality management system or document management system.

Legislative requirements

Australian and international law requires organisations to protect sensitive information.

In addition to workplace policies and procedures, organisations that handle sensitive data, such as customers' personal information, are required to comply with Australian and international legislation. Cyber security audits help organisations to examine whether they are complying with local and international data handling legislation.

Commonwealth Privacy Act

Organisations handling personal information, such as customer details, need to ensure their ICT systems and processes comply with the requirements of the *Privacy Act 1988* (Cth). The Privacy Act is the most important federal legislation that relates to the management and protection of personal information. It includes requirements around the:

- collection of personal information
- use of personal information
- storage of personal information
- disclosure of personal information.

The Privacy Act applies to:

- Australian government agencies
- private organisations and businesses with an annual turnover more than $3 million.

Notifiable Data Breach (NDB) scheme

The Notifiable Data Breach (NDB) scheme commenced in 2018 and applies to organisations who have responsibilities under the Privacy Act. Under the NDB, organisations must report data breaches to both parties whose data is affected by the breach, as well as the Office of the Australian Information Commissioner (OAIC).

A data breach occurs when personal information is:

- accessed or disclosed without authorisation
- lost.

Examples of data breaches include:

- a device with an individual's personal information is lost or stolen
- a database with personal information is accessed without authorisation
- personal information is mistakenly given to an unauthorised party.

Personal information may include an individual's name, address, contact information, credit card details etc.

Failure to comply with NDB laws, can incur penalties for organisations.

Non-compliance could incur serious fines, for example:

- companies may be fined up to $1.8 million
- individuals may be fined up to $360,000.

The NDB scheme requires organisations and individuals to be proactive when dealing with personal information. This also relates to ensuring the confidentiality of data held in an organisation's ICT system.

There is more information about the NDB scheme on the OAIC website: aspirelr.link/oaic-data-breaches

International legislation

The ICT systems and processes used by Australian organisations may also need to comply with international data protection laws.

In 2018, The General Data Protection Regulation (GDPR) was enacted by the European Union. It is designed to protect personal data of European (EU) citizens and residents by increasing the regulatory requirements of organisations that collect and process data.

The GDPR offers EU citizens more rights over:

- who has access to their data
- where and how their data is stored and used
- having their personal information removed or deleted from databases.

There are large fines associated for organisations that breach the GDPR, even if they are not residing or registered in the EU.

Australian organisations need to comply with the GDPR if they;

- have a presence in the EU
- offer goods or services in the EU
- process data, or monitor the behaviour, of EU citizens and residents within the EU.

This GDPR is far reaching and overlaps with the Australian Notifiable Data Breaches (NDB) Scheme. Both protect the confidentiality of identifiable personal data; unauthorised sharing of personal data would be breaches under both GDPR and NDB regulations .

Example

Identify policies, procedures and legislation

Sara works in the ICT department of an online textbook retailer. She is aware of an upcoming cyber security audit and locates several policies and procedures used by the organisation to maintain the confidentiality, integrity and availability of systems and data such as the organisation's online store and customer information. Using the organisation's policy hub, she finds documents including the:

- Information security policy, containing information about acceptable use and access controls.
- Data integrity policy.
- Disaster recovery policy.

In addition to these workplace documents, Sara familiarises herself with the Australian Privacy Act including the NDB scheme, and the GDPR. As the organisation has more than $3 million in annual revenue, and stores data regarding its European customers, Sara knows it must comply with both local and international legal data handling requirements.

Practice Task 1

Question 1

Which of the following are workplace policies that help an organisation meet the principles of the CIA Triad? Tick all that apply.

- ◯ Information security policy
- ◯ Data integrity policy
- ◯ GDPR policy
- ◯ Notifiable data breach scheme
- ◯ Acceptable use policy

Question 2

Which of the following statements are correct? Select yes or no for each one.

a) The main piece of Australian legislation relating to security of sensitive data is the Privacy Act (1988). » Yes » No

b) Australian companies may need to comply with international legislation relating to cyber security. » Yes » No

c) Under the Notifiable Data Breach scheme, companies must be issued a formal warning before they can be fined. » Yes » No

d) The Privacy Act (1988) applies to companies with turnover less than $3 million. » Yes » No

1B Contribute to cyber security audits

The aim of audits is to find and repair security vulnerabilities.

Cyber security audits help organisations identify and understand their current weaknesses, and how to address them. The audit process can be conducted by an external auditor, or internally by an organisation's staff. Regardless of whether the process is external or internal, it is important to understand the audit process, including potential threats that may be identified, so you can contribute effectively when required.

The audit process

Follow a defined process to achieve quality outcomes.

Effective cyber security audits follow the five step process outlined in the following table.

Step 1: Define the scope of the audit

Due to time and budgetary constraints, it is unlikely that every aspect of an organisation's ICT system can be analysed in a single audit. Therefore, the first step involves identifying exactly what will be examined within the audit in question.

This involves first creating a list of all the organisation's ICT assets. These may include:

- physical devices and infrastructure, such as computers and servers
- digital infrastructure, such as networks and cloud services
- data held by the organisation
- internal documentation, such as policies and procedures.

Once all the assets have been identified, they need to be organised into two groups:

- assets that will be included in the audit
- assets that will be excluded from the audit.

For example, it might be decided during this step that:

- physical devices that store sensitive information, such as a server housing a customer database, will be included in the audit
- physical devices that do not store sensitive information, such as a hard drive dedicated to promotional graphics, will be excluded from the audit
- data deemed sensitive , such as customer credit card information, will be included in the audit
- data not deemed sensitive, such as publicly available annual reports, will be excluded from the audit.

Step 2: Identify the threats

For each asset that is included in the audit scope, potential threats need to be identified. A potential threat is anything that could compromise the confidentiality, integrity or availability of the asset.

Common threats include:

- careless or untrained employees
- phishing attempts
- viruses and malware.

These threats, and others, are explained in more detail shortly.

Each asset may have a number of different threats. The process of identifying threats may involve:

- interviewing staff about how they use ICT
- reviewing system logs for attempted and actual breaches
- physically inspecting equipment such as servers and computers contained in the audit scope
- conducting penetration tests in which you attempt to 'hack' into your organisation's network.

Step 3: Evaluate current security controls

Having identified the potential threat/s to each asset, you need to evaluate your organisation's existing security controls against each threat. Security controls used in your organisation may include:

- hardware and software controls, such as latest anti-malware software to protect against viruses
- policy and procedure controls, such as access control policy or back-up procedures)
- human controls, such as ability of staff to identify phishing attempts, or capability of staff to use systems correctly and not accidentally share sensitive information.

It is important that you avoid any personal bias when conducting this evaluation, especially when it comes to considering the protection provided by fellow employees. The weaknesses and strengths of staff must be accurately recorded in order to accurately identify potential risks, and additional security measures required.

Step 4: Prioritise the risks

This is possibly the most important step in the auditing process. It involves considering each threat identified in Step 2 and asking:

- What is the likelihood of this threat occurring?
- What is the potential consequence/impact if the threat occurs?

Answering these two questions will help you measure each threat. In turn, this will enable you to prioritise the threats/risks in order from most to least urgent. This process will be examined in greater detail in the next topic.

Step 5: Identify security strategies

Appropriate cyber security strategies need to be identified for each threat. Effective strategies should:

- reduce the likelihood of the threat occurring
- reduce the potential impact if the threat does occur
- a combination of the above.

Common security strategies for addressing cyber threats include:

- effective password management practices
- effective data back-up processes
- regular software updates.

These strategies, and others, will be explored in more detail in the next topic.

Identifying cyber security threats

Understanding common workplace threats will help you to identify them.

There are a number of cyber threats that may be identified during step two of the audit process. A selection of threats you might encounter during the audit are described in the following table.

Careless or untrained employees	Poor performance by employees may result in sensitive data being compromised. Without proper training, employees may be more likely to: ▪ overlook suspicious activity, such as phishing attempts ▪ use poor password practices, such as recycling or sharing passwords ▪ accidentally share sensitive data to unauthorised people or platforms.
Phishing attempts	'Phishing' is a term used to describe any attempt by unauthorised parties to trick someone into providing sensitive information, such as login usernames and passwords. Phishing attempts can be made via email, phone or text message, and can be very convincing. The majority of phishing attempts are financially motivated.
Weak password practices	Weak password practices include: ▪ using easily guessable passwords such as'123456', 'password' etc. ▪ using short passwords, such as four digits ▪ sharing passwords between employees ▪ using the same password for multiple accounts or systems. Practices such as these make it much easier for hackers to gain access to password-protected systems.

Criminal employees	While many hackers come from outside an organisation, the possible threat of employees with malicious and criminal intentions cannot be overlooked. Staff may take advantage of access to sensitive information and use this to harm their organisation or gain personal advantage.
Distributed denial of service (DDoS) attacks	A DDoS attack involves intentionally overloading a system, such as a web server, to slow or halt its service. With an online store, for example, attacks such as these can stop the business from making sales and income.
Employee devices	Employees using their own devices on organisation networks, also referred to as Bring Your Own Device (BYOD) can compromise the security of the entire network. If one employee's personal device has been hacked, it may open the gateway for hackers to enter the entire network.
Malware	Malware is any form of malicious software that is designed to damage devices and networks. Common forms of malware include: ▪ ransomware ▪ viruses ▪ worms ▪ spyware ▪ trojan horses. Some malware is designed to spread across devices and networks at great speed so as to cripple performance.
Physical theft	Physical devices which store sensitive data, such as servers, hard drives, computers and mobile devices, face the threat of being stolen.
Physical damage	In addition to theft, devices which house sensitive information also face the threat of physical damage due to factors such as: ▪ fire ▪ flood ▪ overheating. Any of these threats may totally destroy devices and the contained data.

Example

Contribute to cyber security audits

Felix works in the ICT department of an online video streaming service and has been asked to contribute to an internal cyber security audit.

Felix works first with his colleagues to develop a complete list of the organisation's assets. This list is then split into two groups; assets to be included in the audit, and assets to be excluded. Assets within the scope of the audit include all devices that store sensitive information such as financial records and client data. One of these devices is a server housed in the organisation's Brisbane office.

Felix and his team then identify potential threats to each asset. For the server, they identify several threats including:

- worms: a type of malware that spreads copies of itself from computer to computer
- DDoS attacks
- damage due to overheating.

Felix checks the current security measures in place for each threat and finds:

- Risk of worms: the server is running anti-malware software but it has not been updated in 18 months.
- Risk of DDoS attacks: no strategies in place to prevent DDoS attacks.
- Risk of damage due to overheating: server housed in a temperature controlled room.

Based on their potential likelihood and impact, Felix and his colleagues then prioritise these risks in the following order:

- 1st priority: risk of DDoS attacks
- 2nd highest priority: risk of worms
- 3rd highest priority: risk of damage due to overheating.

For each risk, Felix and the team identify several appropriate security strategies. For example, to address the risk of DDoS attacks, the following strategies are identified:

- develop a denial of service response plan
- create redundant network resources to cope with load should the main server be attacked
- procure a cloud-based DDoS prevention service.

Practice Task 2

Question 1

Number each step from 1 to 5 in the order you would follow when conducting a cyber security audit.

- ◯ Identify the threats.
- ◯ Evaluate current security controls.
- ◯ Identify security strategies.
- ◯ Prioritise the risks.
- ◯ Define the scope of the audit.

Question 2

Which of the following are common cyber security threats? Tick all that apply.

- ◯ Redundant servers
- ◯ Physical damage
- ◯ Phishing attempts
- ◯ AES encryption
- ◯ Careless employees

Summary

- Workplaces should have policies and procedures to help them meet the principles of data confidentiality, integrity and availability.
- Common workplace polices relating to ICT security include the acceptable use policy, access control policy, information security policy, data integrity policy and disaster recovery policy.
- Under the Notifiable Data Breach scheme, organisations must report data breaches to both the parties whose data is affected by the breach, as well as to the Office of the Australian Information Commissioner (OAIC).
- Australian organisations must comply with local legislation such as the Commonwealth Privacy Act, as well as international legislation such as GDPR.
- Cyber security audits should help companies to find ICT security weaknesses, as well as identify methods to address these weaknesses.
- Audits may be conducted by external auditors or internally by the organisation's employees.
- Audits commonly involve five steps: defining the audit scope, identifying threats, evaluating current controls, prioritising risks and identifying security strategies.
- There are a number of common cyber security threats that may be identified during an audit. These include untrained employees, phishing attempts and weak password practices, among others.

Learning Checkpoint 1

Contribute to cyber security audits

Part A

1. Identify three workplace policies or procedures that companies use to manage data confidentiality, integrity or availability.

2. What is the most important Commonwealth legislation relating to the handling of sensitive data?

3. In which of the following situations must an Australian organisation comply with GDPR requirements? Tick all that apply.

- ◯ The Australian organisation has a presence, such as an office, in the European Union (EU).
- ◯ The Australian organisation has an annual turnover higher than $3 million.
- ◯ The Australian organisation processes the data of EU citizens and residents.
- ◯ The Australian organisation offers shipping to customers in the United States of America.
- ◯ The Australian organisation offers goods and services to customers in the EU.

4. What are the maximum penalties relating to non-compliance with the Notifiable Data Breach scheme for both:

Part B

Read the case study and answer the questions that follow.

Case study

Sruthi works in the ICT department of an online cosmetics retailer and has been asked to contribute to an organisation-wide cyber security audit.

1. What are the five main steps contained in the audit process?

2. What are three common cyber security threats Sruthi might encounter during the audit?

3. What are two methods Sruthi might use to help identify threats?

Topic 2 | Conduct risk assessments

2A Assess cyber security risks

2B Assign risk levels

2C Identify security strategies

2A Assess cyber security risks

Accurately assessing cyber security risks allows us to manage them effectively.

Risk assessment is a critical part of the cyber security audit process as it enables us to understand how dangerous each threat to an organisation is, and to prioritise them accordingly. The two main parts of risk assessment are identifying:

- the likelihood of the risk occurring
- the potential impact (or consequence) on the organisation if the risk occurs.

Defining the concepts

A 'risk' can be defined as an uncertain outcome. Risks can be positive or negative, but in cyber security we generally focus on negative risks as they create unwanted outcomes for an organisation.

Common cyber security risks include:

- sensitive data being accessed by unauthorised parties
- critical data and systems being corrupted
- organisational data being lost.

In cyber security, risks exist when the two following factors are present:

Threats	A threat is an action that may cause harm to an ICT system. Threats can be intentional, such as phishing, ransomware or DDoS attacks, or unintentional, such as bad weather or staff accidents.
Vulnerabilities	A vulnerability is a weakness or gap in an ICT system which leaves it open to being damaged by a threat. Generally, vulnerabilities exist when there is an absence of security controls to protect the system.

In other words: threat + vulnerability = risk

For example, the threat could be from a hacker targeting company employees with a phishing attempt. Add to this the vulnerability that company employees have not received cyber training. This leads to, or equals, the risk that company systems are accessed by hackers using a password phished from an employee.

Assess risk likelihood

You need to understand both threats and vulnerabilities in order to assess risk likelihood.

The first step in risk assessment is to estimate the 'likelihood', or probability, of the risk occurring.

Assessing risk likelihood requires you to consider two factors:

- probability of an identified cyber threat occurring
- current vulnerability or weakness of your ICT system to the threat.

The following examples illustrate this concept:

- Australian financial planning companies are currently being targeted by ransomware attacks. You work at a financial planning company which uses outdated anti-malware software. In this instance the possibility of the ransomware threat occurring is high, and your organisation's vulnerability to the threat is also high, due to the outdated anti-malware. This would mean the overall likelihood of your company's data being corrupted by malware may also be high.
- Physical break-ins in your area are rare. The server room in your company uses a sophisticated alarm system and has electronic locks to protect equipment from thieves and damage. In this instance, the possibility of a burglary occurring is low and the vulnerability of company devices to theft is also low, due to physical protection controls. This would mean the overall likelihood of data being lost as a result of theft is highly unlikely.
- Hackers are currently conducting phishing attempts on organisations similar to yours. Your organisation has recently conducted cyber security training, that included how to identify phishing attempts, for all staff. In this instance, the possibility of a phishing attempt is relatively high but your organisation's vulnerability to the threat is relatively low due to the training controls. This would mean the overall likelihood of data being lost as a result of phishing may be either possible or somewhat unlikely.

Ranking risk likelihood

Consider both the probability of the threat occurring and your organisation's current vulnerability to the threat. Rank the overall risk likelihood using the following scale.

1	Highly unlikely
2	Unlikely
3	Possible
4	Likely
5	Almost certain

Risk management involves dealing with the unknown, so ranking the likelihood of each risk involves making some educated guesses. The accuracy of this process may be improved by asking:

- how often has our organisation experienced the same threat in the past?
- what current industry level threats, such as major hacking attempts or data breaches, are we aware of? Methods for identifying industry level threats are described later in this topic.

Rather than basing all the rankings on one person's opinions, it is a good idea to estimate risk likelihood in collaboration with colleagues and business stakeholders to improve the quality and consistency of rankings assigned.

Assess risk impact

What damage would a cyber threat cause?

Having estimated the risk likelihood, you now need to estimate the risk impact. Impact relates to the negative impacts on the organisation if a risk event, such as loss of data or system availability, takes place. The following table identifies several different impacts on business an organisation may experience as a result of a cyber risk.

Revenue loss	▪ If an online store's website crashes due to a hacking attempt, significant revenue losses will occur immediately. ▪ Some cyber threats result in more subtle impacts, such as system slowdown and increased downtime. While less immediately devastating, revenue lost as a result of IT downtime can quickly add up. ▪ In addition, significant costs may be required to repair or replace equipment damaged by a threat. ▪ The average cost of a data breach has been estimated at around $8 million.

Damage to brand reputation	▪ An organisation's reputation is often built on consumer trust. If sensitive customer data is hacked, customers will be much less likely to return to that organisation. ▪ Previous hacks, such as the 2014 hack of film company Sony Pictures, have also resulted in embarrassing internal emails being shared publicly, further damaging organisations' reputations.
Loss of intellectual property	▪ In addition to customer data, intellectual property (IP) is the most valuable asset held by many organisations. The loss of IP, such as designs and strategies, may cost an organisation its competitive edge. ▪ As a result of the Sony Pictures hack mentioned above, a number of movies in production were leaked online prior to their official release announcement.
Legal damage	▪ Data breaches may involve significant legal consequences from both regulators and those whose data has been breached. This may include the issuance of fines and penalties. ▪ Following a major data breach from a hack in 2017, Equifax was required to pay nearly $700 million in fines.

A single cyber risk may result in one or more of the above impacts. You can estimate the potential overall impact for each risk using the following scale, remembering that not every risk has a critical business impact.

1	Insignificant
2	Minor
3	Moderate
4	Major
5	Critical

Breaches of highly sensitive data, such as customer information or trade secrets, are more likely to have critical impacts, such as legal, commercial and reputational issues, on the organisation than breaches of less sensitive data.

Using an asset-based approach can help identify the impact rating for each risk. Assets that contain or transmit more sensitive information should receive higher impact ratings. For example, the risk of a server being hacked that contains highly sensitive personal information would most likely have an impact rating of 'major' or 'critical'. The risk of a computer being damaged by a fire, which contains internal, non-confidential files, would most likely have an impact rating of 'minor' or 'insignificant'.

Similar to estimating the risk likelihood, it is best to estimate risk impacts with colleagues and relevant stakeholders. You are unlikely to know everything about your organisation, so it is prudent to get a few viewpoints and insights in order to estimate the impact accurately.

Example

Assess cyber security risks

Sue works in the ICT department of an online retailer. During the process of an internal audit a number of potential cyber risks were identified. These risks included:

- **Risk 1:** highly sensitive information being disclosed to unauthorised parties due to staff carelessness.
- **Risk 2:** non-critical business systems being brought offline due to DDoS attacks.
- **Risk 3:** corruption of sensitive customer information due to malware entering the company network.

In collaboration with colleagues, Sue evaluates the likelihood and potential impact of each risk. The team makes the following evaluations:

- **Risk 1:** Likelihood is almost certain (5) due to lack of staff training and system controls. Impact is critical (5) due to potential financial, reputational and legal damage if sensitive information is disclosed.
- **Risk 2:** Likelihood is possible (3) due to other companies in the same sector recently being targeted. Impact is moderate (3) due to the non-critical nature of the systems. Redundant servers can also be brought online if the risk event occurs.
- **Risk 3:** Likelihood is low/unlikely (2) due to recent major investments in anti-malware software and ensuring all software is patched. Impact is major (4). Back-ups of the data in question are made, but the back-up process only occurs on a weekly basis.

Practice Task 3

Question 1

Draw a line to match each term about risk assessment to its definition.

» Threat	» Any uncertain, and usually unwanted, outcome for an organisation.
» Impact	» An action that may cause harm to an ICT system.
» Risk	» A weakness or gap which leaves an ICT system open to damage.
» Vulnerability	» The probability of an unwanted event occurring.
» Likelihood	» The potential consequences if an unwanted event occurs.

Question 2

List two potential impacts or consequences of a cyber risk on a business.

2B Assign risk levels

Identify the most urgent threats by assigning risk levels.

If you identify a large number of threats and associated risks, it can be difficult to know what to address first. Assigning levels to each risk helps define the urgency of each threat and enables decision-makers to identify how to allocate resources to address them.

Using a risk matrix

A matrix helps to visualise each risk.

As discussed in the previous section, the likelihood and potential impact for each risk needs to be identified. A 5-point scale can be used for each.

This information can be presented in a risk matrix. Different organisations use different risk matrix templates, but a common format is shown below.

		Consequences				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Likelihood	Almost certain (5)	High	High	Very high	Very high	Very high
	Likely (4)	Moderate	Moderate	High	Very high	Very high
	Possible (3)	Low	Moderate	High	High	Very high
	Unlikely (2)	Low	Low	Moderate	Moderate	High
	Rare (1)	Low	Low	Low	Low	Moderate

Depending on the likelihood and risk ratings, each risk will be located within certain shades of the graph. For example:

- risks with a likelihood of 4 and an impact rating of 3 will be located in the darkest (very high) part of the matrix
- risks with a likelihood of 2 and an impact rating of 4 will be located in the middle range (high to moderate) of the matrix
- risks with a likelihood of 1 and an impact rating of 2 will be located in the lightest (low) part of the matrix.

The following table outlines how different levels of risk should be managed.

High level	High level risks that need to be addressed urgently. The next section will cover potential strategies for mitigating these risks.
Medium level	Medium level risks that, while needing to be addressed, are not as urgent as high level risks. Potential strategies for mitigating these risks will also be covered in the next section.
Low level	These are low level risks that can be accepted by the organisation with ongoing monitoring and routine management.

Calculating risk scores

Risk scores are another way of quantifying each risk.

A total risk score for each risk can be calculated by multiplying the risk likelihood by the risk impact. For example:

- risks with a likelihood of 4 and an impact rating of 3 have a risk score of 12
- risks with a likelihood of 2 and an impact rating of 4 have a risk score of 8
- risks with a likelihood of 1 and an impact rating of 2 have a risk score of 2.

Similar to the matrix approach, the calculated total risk score can be used to identify whether a risk is low, medium or high level.

Risk score 12-25 (high level)	These are high level risks that need to be addressed urgently. The next section will cover potential strategies for mitigating these risks.
Risk score 3-11 (medium level)	Medium level risks that, while needing to be addressed, are not as urgent as high level risks. Potential strategies for mitigating these risks will also be covered in the next section.
Risk score 1-2 (low level)	These are low level risks that can be accepted by the organisation with ongoing monitoring and routing management.

Prioritising risks

Ranking risks in order of urgency helps us to focus on high risks.

Based on the audit process, you may have identified a large number of potential threats and associated risks. Identifying the highest risks enables you to make recommendations about which threats need to be addressed as quickly as possible.

A risk register can be used to document the risks you have identified. Organisations may use a variety of risk register formats, but a standard template (including examples) is provided below.

Risk description	Likelihood	Impact	Risk score	Risk level
Disclosure of sensitive data to unauthorised parties due to phishing attempts.	High (4) Staff have not been trained in spotting phishing attempts. Weak password practices are used throughout the organisation.	Critical (5) Loss of sensitive information will have wide ranging revenue and legal impacts on the business.	20	High
Corruption of sensitive data due to malware infection.	Unlikely (2) Latest anti-malware software has been installed on all devices.	Major (4) Back-ups of sensitive data are currently only run every month, so significant amounts of data may be damaged if malware enters the network.	8	Medium
Loss of system availability due to weather, or other, damage such as from heat, rain or fire, to server equipment in Melbourne office.	Highly unlikely (1) Extreme weather conditions occur very rarely in Melbourne. Servers are housed in highly secure weather and theft protected space containing multiple physical barriers.	Minor (2) Redundant off-site servers are available and can be brought online within 2-4 hours if main server goes down.	2	Low

As shown in the example above, risks should be listed from highest to lowest. Once this part of the risk register is complete, mitigation strategies for each risk can be identified and added to the register.

Example

Assign risk levels

Sue works in the ICT department of an online retailer. During an internal audit a number of potential cyber risks were identified.

Using the risk likelihood and impact scores identified for each risk, identified in collaboration with her colleagues, Sue calculates the risk score and level for each risk. She priorities the risks into a risk register as follows:

Risk description	Likelihood	Impact	Risk score	Risk level
Highly sensitive information being disclosed to unauthorised parties due to staff carelessness.	**Almost certain (5)** No staff training or system controls currently exist.	**Critical (5)** Disclosure of sensitive information likely to result in substantial financial, reputational and legal damage.	25	High
Non-critical business systems being brought offline due to DDoS attacks.	**Possible (3)** Other companies in the same business sector have recently been targeted by similar attacks.	**Moderate (3)** Systems are non-critical in nature. Redundant servers can also be brought online if this risk occurs.	9	Medium
Corruption of sensitive customer information due to malware entering the company network.	**Unlikely (2)** Major investments recently made in anti-malware software, ensuring all software is patched.	**Major (4)** Back-ups are made of the data in question, but the back-up process only occurs on a weekly basis.	8	Medium

Practice Task 4

Question 1

If the likelihood of a risk is 4 and the potential impact is 3, what is the total risk score?
Tick all that apply.

- ◯ 1
- ◯ 3
- ◯ 4
- ◯ 7
- ◯ 12

Question 2

Referring to the following risk matrix, what is the risk level of a risk with a likelihood of 2 (unlikely) and an impact of 5(catastrophic)?

Likelihood	Consequences				
	Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Critical (5)**
Almost certain (5)	High	High	Very high	Very high	Very high
Likely (4)	Moderate	Moderate	High	Very high	Very high
Possible (3)	Low	Moderate	High	High	Very high
Unlikely (2)	Low	Low	Moderate	Moderate	High
Rare (1)	Low	Low	Low	Low	Moderate

2C Identify security strategies

The aim of security strategies is reduction of risk likelihood and/or risk impact.

Having assessed and prioritised different risks your organisation faces, the next step is to identify potential security strategies. Security strategies should reduce, or mitigate, the risk level of one or more risks. By identifying and evaluating a range of mitigation strategies relevant to each risk, you can make recommendations about how to address current threats.

Strategies to reduce risk likelihood and impact

Each cyber threat has a variety of potential mitigation strategies.

The focus of risk mitigation is lowering the overall risk level or risk score for each cyber risk facing your organisation.:

- reducing the likelihood of a risk occurring
- reducing the potential impact if the risk event occurs
- a combination of the above.

Reduce risk likelihood

The risk likelihood rating reflects the probability that your organisation will be affected by a potential threat. While it is unlikely you can stop the existence of threats such as human error, hackers or physical damage, it is possible to reduce the likelihood that they will negatively impact your organisation. This is achieved through using strategies designed to lower your organisation's vulnerability to the threat.

To reduce risk likelihood, identify the major threat/s and select appropriate security strategies to reduce vulnerability. The following table outlines common threats, and mitigation strategies for each, aimed at lowering vulnerability and risk likelihood.

Cyber threats	Suggested risk mitigation strategies
Physical damage to equipment	▪ Ensure devices are housed in appropriate facilities to protect them from heat and water.
Outdated operating system or software	▪ Ensure all operating systems and software are updated to the current version. ▪ Retire devices that cannot support the latest versions of operating systems and software.

Cyber threats	Suggested risk mitigation strategies
Human error	▪ Provide staff training to ensure devices are used correctly. ▪ Implement controls to prevent human error where possible, such as prevent emails from being sent outside the organisation's network. ▪ Audit the users who have access to sensitive information and reduce/remove access if it is not required to perform their work.
Malware and viruses	▪ Ensure latest anti-virus and anti-malware software is installed and functioning. ▪ Provide staff training to reduce the likelihood of staff downloading malware and viruses to devices.
Physical theft of devices	▪ Ensure access to devices is controlled by physical security such as locks or physical barriers. ▪ Provide staff training on taking care of work mobile devices, such as not leaving devices unattended.
Staff dishonesty and corruption	▪ Avoid using shared passwords to ensure transparency about who is accessing/downloading information. ▪ Implement processes to monitor user and file activities. ▪ Provide training to ensure staff are aware their accessing of sensitive information is monitored.
Hacking attempts	▪ Implement password policies to prevent hackers guessing passwords to sensitive data. ▪ Use multi-factor authentication methods to protect access even if a password is obtained by a hacker. ▪ Use encryption to protect data. ▪ Provide training to staff in how to identify phishing attempts and other suspicious emails. This may include the use of phishing simulations. ▪ Provide training to staff about avoiding connecting to unsecured public wi-fi networks.

As illustrated in the table, there is usually more than one potential strategy for reducing your organisation's vulnerability (and therefore risk likelihood) to each type of threat.

Reduce risk impact

The degree of impact of a risk is generally related to the sensitivity of the information that is affected by a threat, such as disclosure, loss or corruption. While organisations will always hold some information that is confidential or restricted, the consequences of a device containing personally identifiable customer information being hacked are much worse than a hack of a device containing non-sensitive information.

The following table includes strategies to reduce risk impact.

Ensure regular back-ups	If a cyber threat, such as hacking, physical damage or employee carelessness, occurs, it may result in the loss or corruption of important organisational data. Maintaining a back-up program helps reduce the impact if a threat occurs as data and systems can quickly be brought back online, and corrupted data can be corrected. Some best practices for data back-ups include: ▪ maintaining and following an organisational back-up plan or policy ▪ using a combination of back-up methods ▪ ensuring back-ups are conducted regularly to minimise data loss ▪ assigning responsibility for conducting back-ups ▪ manually checking that back-ups have been performed correctly such as by attempting to restore back-up files.
Consider location of sensitive data	Identify which parts of your organisation's infrastructure are being used to store and transmit sensitive data. Ask the following questions: ▪ Is it essential for sensitive data to be stored or transmitted using infrastructure that is prone to cyber threats? ▪ Could sensitive data be stored or transmitted more securely using infrastructure that is less prone to cyber risk? By removing highly sensitive data from infrastructure that is identified as high risk, such as offshore servers that are subject to foreign laws, the potential risk impact if the infrastructure faces a cyber threat is also reduced.
Consider whether data needs to be stored	Data can be an organisation's most valuable asset, but it also contributes to increased risk impacts if it is breached. Many organisations hold on to sensitive data long after it is useful or necessary. The Australian privacy principles specify that when data no longer serves an approved purpose, it should be destroyed or de-identified. By lawfully destroying or de-identifying sensitive data it no longer needs, organisations can reduce the impact rating if a threat occurs. Any proposed destruction or de-identification of organisational information must be discussed with, and approved by, senior management.

Reviewing and recommending mitigation strategies

You may identify a number of different mitigation strategies for each cyber threat, so you need to review and evaluate each potential strategy in order to make a clear recommendation about how to best mitigate the risk.

The following table identifies criteria for evaluating security strategies.

How much will the risk be reduced by?	For each potential strategy, consider to what extent the strategy will: ▪ reduce the likelihood of the risk event occurring; what would the new risk likelihood score be from 1-5? ▪ reduce the potential impact if the risk event occurs; what would the new risk impact score be from 1-5? ▪ reduce the risk rating level; would the risk rating lower from high to medium, or from medium to low? ▪ reduce the total risk score; what would the new total risk score be from 5-25? Generally, the greater the reduction in the overall risk rating, the more preferable is the mitigation strategy. However, other criteria also need to be considered.
How expensive is the mitigation strategy?	Mitigating a risk may involve numerous costs, such as: ▪ staff time spent implementing control measures ▪ purchase of new hardware and infrastructure ▪ purchase of new software and operating systems ▪ staff time spent undergoing or delivering cyber training. While lower cost options might be preferable, they may not be as effective in reducing the overall risk level. When assessing the costs of mitigation strategies, consider conducting a cost-benefit analysis. This involves comparing the costs of implementing the security measure against the cost of leaving the risk uncontrolled. You want the costs of controlling the risk to be lower than the total impact costs if the risk is left uncontrolled.
How quickly can the strategy be implemented?	Different mitigation strategies have different timelines for implementation. The timelines for creating and delivering a staff cyber training program may be shorter than the timelines for implementing a complex network change. Shorter timelines are generally preferable, so that system vulnerabilities can be addressed as quickly as possible. However, the speed of implementation needs to be balanced with the potential effectiveness of the security measure.
How risky is the strategy?	Mitigation strategies are rarely 100% effective so the riskiness of each strategy needs to be considered. As a simple example, using a well-known and trusted anti-malware product may be less risky than using an unproven anti-malware product from a new publisher. Generally, less risky mitigation strategies are preferable to riskier strategies.

The criteria used, and their weighting, may vary depending on the particular problem. For example, addressing an urgent and major security threat may place greater importance on timelines than cost factors.

Review each potential strategy using the evaluation criteria to determine the best option. In some situations, more than one option may be appropriate to address the risk effectively. For example, it may be determined that addressing the risk of data loss from phishing attempts should be addressed by:

- implementing a new password policy across all organisational devices and accounts
- conducting a staff training program about how to identify phishing attempts.

The recommendations you identify should be documented in a threat assessment report for communication to relevant stakeholders. The process for creating and distributing a threat assessment is covered in the next topic.

Improving the audit process

In addition to identifying best practice strategies to mitigate your organisation's cyber threats, it may be appropriate to identify strategies to improve the audit process. Upon completion of an audit, be sure to meet with your audit team to reflect on how effective the process was and what improvements can be made for the next audit. The following table identifies questions you could ask during this meeting.

Questions to ask when reflecting on an audit
▪ Did we have access to the staff required to conduct the audit? ▪ Did we have access to the technology and resources required to conduct the audit? ▪ Did we have sufficient time to conduct the audit? ▪ Was our audit scope appropriate? ▪ Were our threat identification methods accurate? ▪ Were our threat identification methods reliable? ▪ Are we confident we identified all threats on assets contained in the audit scope? ▪ Did we have appropriate templates to record the threat identification process? ▪ Were relevant stakeholders consulted throughout the audit process? ▪ Are we confident in the ratings assigned to the risks identified? ▪ Have we considered and evaluated a number of mitigation strategies for each risk?

If the answer to any of the above questions was 'no', the audit process probably has some room for improvement. Potential improvements to your organisation's audit process may include:

- ensuring audit team staff have sufficient time and resources to conduct the process without competing work priorities
- identifying additional threat identification methods and techniques
- developing standardised templates for documenting the audit process

- adding quality assurance and stakeholder feedback processes to 'sense check' the risk ratings assigned
- inviting a wider range of stakeholders to help identify risk mitigation strategies.

Reviewing industry level threats

You need to be aware of emerging and dangerous cyber threats.

Most of this topic has discussed how to assess and manage threats and risks identified through the audit process. You must also be aware of emerging industry level cyber threats that may not be picked up during the audit process. Such threats may pose dangers to your organisation and need to be proactively assessed and managed.

Identifying industry level threats

One of the best sources of information regarding emerging risks is the Australian Cyber Security Centre (ACSC). The centre publishes alerts about major risks and is maintained by the Australian government. Examples of threat alerts published by the ACSC include:

- cyber criminals contacting Australian organisations pretending to be from Australian government agencies in an attempt to delude individuals into providing access to their devices and accounts
- ransomware attacks targeting Australian aged care and healthcare businesses
- phishing attempts via email and SMS attempting to convince people to hand over their login details for government services agency myGov
- major security vulnerabilities in software and operating systems
- Denial of service (DoS) threats from cyber criminals targeting companies in the banking and finance sectors.

The alert register can be accessed here: aspirelr.link/cyber-alert-register and you can also sign up to receive alerts regarding the latest threats.

Other sources of information publishing industry level threats are outlined in the following table.

Australian ICT news sources

There are a number of Australian news sites that specialise in cybersecurity. These sites are regularly updated and publish information about emerging threats to Australian organisations.

Websites to check include:

IT News Australia: aspirelr.link/it-news

Australian Cyber Security Magazine: aspirelr.link/australian-cybersecurity-magazine

Security Brief Australia: aspirelr.link/security-brief-australia

International ICT news sources

Many global cyber threats target Australian individuals and organisations, so stay updated on international cybersecurity developments. The following international news sites are all focussed on cybersecurity and are regularly updated. Be aware that not all the developments discussed are relevant to Australian regulations and/or practices.

Websites to check include:

Threat Post: aspirelr.link/threat-post

CyWare: aspirelr.link/cyware

The Hacker News: aspirelr.link/the-hacker-news

Wired: aspirelr.link/wired-security

Cyber Security News: aspirelr.link/cyber-security-news

Dark Reading: aspirelr.link/dark-reading

Hardware and software developer sources

A number of major hardware and software developers, in particular anti-malware software publishers, publish news and developments regarding cybersecurity. These articles may not always be entirely objective and should be approached with caution. However, they may provide accurate updates and information regarding the hardware and software you use in your organisation.

Websites to check include:

IBM: aspirelr.link/ibm-security

Microsoft: aspirelr.link/microsoft-security

Norton: aspirelr.link/norton-internet-security

Kaspersky: aspirelr.link/kaspersky-news

Assessing industry level threats

Industry level threats should be assessed and managed using the same processes and strategies outlined earlier in this topic. When an industry level threat is identified, for example via an alert from the ACSC, you should:

- assess the risk likelihood based on the nature of the threat, and your organisation's vulnerability to the threat
- assess the potential risk impact
- assign a total risk score based on the risk likelihood and impact scores and/or identify the risk level: high, medium or low
- identify and evaluate appropriate security strategies to mitigate the risk
- make recommendations about the most appropriate security strategy or strategies
- document findings and recommendations in the threat assessment report.

Example

Identify security strategies

Sue works in the ICT department of an online retailer. During the process of an internal audit, a number of potential cyber risks are identified and assessed. One of the risks that scored 25, 'high risk', relates to extremely sensitive information being disclosed to unauthorised parties due to staff carelessness.

In collaboration with her team, Sue identifies several strategies to reduce the likelihood and impact of this risk, including:

- developing and conducting a staff training program to lower the occurrence of mistakes, such as files being sent to the wrong person
- implementing system controls to prevent human error where possible, such as restricting the email system for certain users so that emails can be sent to internal addresses only
- reviewing the current level of system access for all staff and reducing or removing privileges if access is not required in order to complete their work.

Each strategy is evaluated to identify which control should be recommended to the organisation's stakeholders. The team determines a combination of staff training and system controls will result in the greatest lowering of the total risk score.

Practice Task 5

Question 1

What should best security strategies aim to achieve? Tick all that apply.

- ◯ Reduce risk likelihood
- ◯ Reduce costs of risk mitigation
- ◯ Reduce risk impact
- ◯ Reduce risk monitoring requirements
- ◯ Reduce both the risk likelihood and risk impact

Question 2

Draw a line to match each of the following risks to the most appropriate mitigation strategy.

» Loss of data via theft of server equipment	» Implement a data back-up program.
» Loss of data due to staff error	» Increase the physical security of the business premises.
» Theft of data from database by criminal staff members	» Implement encryption on sensitive data.
» Unauthorised breach of data by a hacker	» Implement processes to monitor staff access.

Summary

- 'Risk' can be defined as any uncertain outcome.
- The two main parts of risk assessment are identifying risk likelihood and risk impact or consequence.
- In cyber security, risks exist when both threats and vulnerabilities exist.
- Risk likelihood and risk impact can be assessed using a 1-5 point scale.
- Potential risk impacts/consequences to a business include damage to brand reputation, intellectual property and legal status and loss of revenue.
- Based on the likelihood and impact scores, risk levels, that is high, medium or low, can be identified using a risk matrix or total risk score.
- Identifying risk levels enables risks to be prioritised. A risk register can be used to document different risks in order of priority.
- Security strategies should reduce, or mitigate, risk by reducing risk likelihood, risk impact, or both.
- Reducing risk likelihood generally involves addressing security vulnerabilities.
- Different mitigation strategies can be reviewed and evaluated using criteria such as how much the risk level will be reduced, and the cost of the mitigation strategy.
- At the end of an audit, recommendations for future audits may be identified.

Learning Checkpoint 2

Conduct risk assessments

Part A

1. Which of the following are potential impacts/consequences to an organisation as the result of a cyber risk? Tick all that apply.

- ◯ Loss of revenue
- ◯ Use of outdated anti-malware software
- ◯ Legal consequences
- ◯ Damage to brand reputation
- ◯ Lack of staff trainin.

2. Which of the following statements are correct? Select yes or no for each one.

a) The assessment of risk likelihood involves thinking about both threat probability and current vulnerabilities. » Yes » No

b) Risk impact relates to the negative consequences to an organisation if a risk event occurs. » Yes » No

c) Generally, low risk likelihood and high risk impact scores are preferred. » Yes » No

d) Risk mitigation strategies should be designed to reduce risk likelihood, risk impact, or both. » Yes » No

e) Risk assessments should be conducted by one person to ensure objectivity. » Yes » No

3. Refer to the following table. If a cyber risk has a likelihood of 4 and an impact of 3, what is the risk level?

Risk score	Risk level
1-2	Low
3-11	Medium
12-25	High

Part B

Read the case study and answer the questions that follow.

Case study

Zadie has been assisting the ICT team to assess a number of threats identified in a cyber audit. The team is meeting to make recommendations about security strategies and the audit process.

1. One of the highest risks identified during the assessment was that of sensitive data being accessed by hackers. What are three best practice mitigation strategies to address this risk? Tick all that apply.

   - ◯ Ensure data is housed in a temperature-controlled room.
   - ◯ Use a cloud storage solution for sensitive data.
   - ◯ Implement strong password policies.
   - ◯ Encrypt sensitive data.
   - ◯ Implement multi-factor authentication on all devices and accounts.

2. List two potential recommendations Zadie's team might make about how to improve the quality of the audit process.

3. What are two examples of industry level cyber threats?

Topic 3 | Finalise threat assessment

3A Document threat assessment

3B Communicate threat assessment

3C Update threat assessment based on feedback

3D Distribute and store threat assessment

3A Document threat assessment

All the work done up to this point needs to be documented in a Threat Assessment report.

At this point, you have conducted the cyber security threat assessment, assessed the risks and identified mitigation strategies to control these risks. It is now time to collate your findings and recommendations into a threat assessment report which can then be distributed to stakeholders.

Threat assessment report format

While the findings and recommendations of each threat assessment report will be unique, these reports typically follow a similar structure.

By now you should have most, if not all, of the information required to compile a user-friendly report.

Before drafting a threat assessment report, find out if there is a report template used in your organisation. Using a template both saves time and means the report is in a format familiar to your stakeholders.

If there is not a specific threat assessment report template, check if an organisation style guide exists. This provides guidance such as font selection, format, spacing and layout and usually includes rules on use of brand and corporate identity.

Whether using an organisational template or developing the threat assessment from scratch, the main items to be included will generally include:

Threat assessment
▪ Executive summary. ▪ Introduction, including the rationale for conducting the audit. ▪ Audit scope. ▪ Methodology used for conducting the audit, assessing the risks and identifying recommendations. ▪ Threats identified. ▪ Assessment of risk likelihood and risk impact for each threat, resulting in total risk scores. ▪ Prioritisation of threats based on risk assessment. ▪ Recommendations, such as risk mitigation strategies, to control the threats/risks. ▪ Appendices, this may include the raw data/information analysed during the audit. ▪ Definitions of technical terms.

Use version control

It is a good idea to include version control information when drafting your report, as it is likely future updates will be required after feedback is received from stakeholders.

Depending on your organisation's document version and sharing policies, version information can be tracked in two ways:

1. **Manually edit version information within the document.**

Version information provided as a simple table at the front of review documents is often sufficient. The important information to include here is:

- who changed the document: author
- when they changed it
- what changes were made.

Here is what a document version control table may look like:

Version	Date	Author/s	Rationale
0.1	1-Sep-20	Jane Smith	First draft
0.2	12-Sep-20	Jane Smith	Reviewed by stakeholders

2. **Automatically manage version information using collaboration tools.**

There are many available collaborative tools such as Dropbox, Google Drive, Microsoft One Drive. These tools usually track versioning information automatically, every time the document is changed. These tools also usually enable you to access previously saved versions of the document when required.

Ensuring the report is effective

A threat assessment report should be clear, concise and avoid jargon in order to be effective.

The threat assessment report is an important document that should recommend actions to improve the security of your organisation's ICT security. It may be read by a wide range of stakeholders, so it is vital to ensure the report is as effective as possible by writing clearly, concisely and avoiding jargon.

Write clearly

Clear writing is easy to understand so always use plain English. This means avoiding complex language, using short sentences and short paragraphs. Never use a long or technical word if a simple word will do.

Paragraphs should only contain one thought or idea and be no longer than five or six lines. It is better to write a short paragraph than confuse your audience by putting two or more ideas in one paragraph. Clear writing means the reader is less likely to get confused.

Write concisely

Concise writing uses the fewest words possible to convey information. You need to explain exactly what is meant, avoid repetition or unnecessary information. Include specific details, definite statements and think carefully about what needs to be communicated. Only include information relevant to the situation and the receiver.

Avoid jargon and define terminology

Your assessment may be distributed to stakeholders who are not ICT security experts. This means you should avoid using jargon where possible and use plain English wherever possible. In some situations you may need to use industry terminology such as 'malware', 'cloud storage' or 'two-factor authentication'. Provide a simple definition for any terminology which may not be understood by your audience. This should also include providing definitions for any acronyms such as: AES means advanced encryption standard. All definitions should be included in a 'definitions' or 'glossary' section at the end of the report.

Example

Document threat assessment

Tamsin works in the ICT department of a large sporting equipment company. She has been involved in a cyber security audit process and has been asked to document a threat assessment. Tamsin collates all the information gathered and created during the audit process and collates this into a report. Her organisation does not have a threat assessment template and she includes the following main sections in the document:

- executive summary
- introduction
- audit scope
- methodology used for conducting the audit
- threats identified
- assessment and prioritisation of threats/risks
- recommendations, for example risk mitigation strategies, to control the threats/risks
- appendices, including raw data analysed during the audit
- definitions of technical terms.

When writing the document, Tamsin ensures the language she uses is both clear and concise. While avoiding the use of jargon, she does need to use some technical terms when identifying mitigation strategies, such as the use of encryption and two-factor authentication. She provides definitions for technical terms such as these in the definitions section of the document.

Practice Task 6

Question 1

What are three strategies to make a threat assessment report as effective as possible? Tick all that apply.

- ◯ Use short sentences and short paragraphs.
- ◯ Include multiple ideas in one paragraph.
- ◯ Avoid using industry terminology.
- ◯ Include a glossary for technical terms and acronyms.
- ◯ Use plain English.

Question 2

What are four sections that are usually included in a Threat Assessment report?

3B Communicate threat assessment

The threat assessment needs to be communicated to stakeholders in order to gather feedback.

Now that the threat assessment report has been drafted, you need to make sure it is communicated to all relevant stakeholders in your organisation. This may include members of the ICT team, as well as department managers and other staff who need to be aware of the threats and recommendations you have identified. The two standard ways to communicate the threat assessment are either in person or by email.

Communicating assessments in person

In person communication requires planning and preparation.

In person communication may involve the presenter and audience being in the same physical space or by using webinar technology, such as Zoom, Teams or Skype when audience members are in different locations.

Any presentation must provide your audience with accurate, clear, current information. Having a good understanding of your organisation's ICT threats is important; you also need to be a good communicator.

An effective presentation will ensure your audience gets an in-depth understanding of the cyber threats facing the organisation, as well as of appropriate strategies to address these threats. Using the strategies outlined in the following table will help you deliver a successful presentation.

Identify audience needs	Identify your audience's needs in order to communicate your findings as effectively as possible. Consider the following questions: ▪ How much prior knowledge does your audience have? Were they, for example, involved in the audit process? Do they have an understanding of ICT risk management? Do they know what ICT security measures are currently being used in your organisation? ▪ What are the language skills of the audience? If your audience speaks a different language from you, do not speak too fast or use needlessly complex language. ▪ Does anyone in your audience have a disability? For example, it may be appropriate to print handouts with large text for people with visual disabilities.

Select and order content	If your information is relevant, clear and logically organised, then your presentation will be easier for your audience to follow. All good presentations include: ▪ **Introduction:** where you introduce yourself, and the aim of the presentation. It is the opportunity to grab your audience's attention. ▪ **Body:** where you should focus on talking about the major cyber threats, their risk levels and the security strategies you have identified. Do not spend too much time talking about background information. ▪ **Conclusion:** where you summarise your presentation. Reinforce the recommendations you want the audience to remember after the presentation. If your audience already knows something about the cyber threats which face the organisation, start there. Then introduce new concepts such as the risk ratings and recommended security controls for each threat. Starting with the known and moving onto to the unknown makes it easier for your audience to process and retain information.
Prepare slides	Presentations often combine both visual and verbal elements to engage the audience. For example, many presenters include a slide show using software such as Microsoft PowerPoint or Prezi. Complicated information, including numerical data, is best summarised visually. An image can often convey an idea more powerfully than text. Limit the number of slides you include in a presentation as moving swiftly between too many slides can be distracting. Use a large font size and limit the amount of information you include on each slide, including only key phrases and essential information. Empty space on a slide improves its readability.
Provide time for questions and feedback	You should always provide time for questions and feedback, either during or at the end of the presentation, to allow your audience the opportunity to interact. Your audience may comprise experts who will provide quality feedback and questions about the recommendations you have presented. Be prepared to document any feedback or questions received, in case they necessitate changes to the threat assessment report.
Set a time limit	Confirm the length of time you have to present your threat assessment findings and recommendations. Plan your presentation by allocating time to each section to ensure you do not go over the prescribed time. Avoid speaking for too long as your audience may become bored and restless.

Rehearse the presentation	It is always useful to rehearse your presentation to build confidence and check your timing. Allow for nervousness, the type of audience, the technology and for questions. Read your presentation out loud and check that you are using: ▪ a clear, easy-to-follow structure ▪ concise words with clear meanings ▪ no jargon or terms that may confuse the audience ▪ pauses to emphasise important points. You can rehearse your presentation with colleagues, friends or family to check the information is clear and interesting.
Deliver the presentation	You might be nervous on the day of the presentation. To ensure your delivery is effective consider the following strategies: ▪ Arrive early so you can set up equipment and check everything is working. Remember to have a glass of water close by in case your throat gets dry. ▪ Use gestures and body language effectively. ▪ Do not overdo hand gestures. Only use them effectively to emphasise key points. ▪ Make eye contact and smile at various audience members to reach out and engage them from the start. ▪ Only refer to your notes occasionally. ▪ Speak slowly and modify your voice so everyone can hear, especially if you are not using a microphone. ▪ Check that the audience understands what you are saying by observing their facial expressions; notice if they are becoming restless.

Communicating assessments by email

Before emailing the threat assessment follow a few simple practices.

In some situations, it may be appropriate to communicate the threat assessment findings and recommendations by email, either as an email attachment or as main body text. There are some simple practices you should follow before sending it out. These practices are outlined in the following table.

Use an appropriate subject line	Ensure the subject line of the email is relevant. For example, 'Cyber threat assessment findings and recommendations (draft)'. Avoid using all capitals in the subject line as this can be interpreted as shouting.
Use an appropriate greeting	Depending on the seniority of your audience, it may be appropriate to start your email with 'Dear'. Otherwise, it may be appropriate to use 'Hi'. Avoid using informal greetings such as 'Hey'.

Use font tools	Use the tools within your email software to bold important text and headings, and use dot points for lists. Avoid underlining text as it may confuse a reader into thinking it is a hyperlink.
Use humour and emojis carefully	While emojis are used more and more in business communication, it is generally safest to avoid them. This is especially true if you are communicating with senior stakeholders or people you have not met. Similarly, humour can backfire so it is best to avoid jokes.
Consider the recipient list	Think carefully about who actually needs to receive the threat assessment. Check with your manager if unsure about who needs to receive the report. In some situations, you will be provided with a distribution list. If many stakeholders need to receive the report, consider using the Bcc option, to avoid lengthy email chains.
Spell check your email	You should have run a spell check on your threat assessment document; be sure to spell check your email too. Poor spelling and grammar will appear unprofessional to your audience.
Consider where the email is being sent	Generally, you will be sending the report to staff inside your organisation. Avoid sending the report to personal/non-work email addresses. These may be less secure than work accounts.
Include a call to action	As the purpose of this email is to gather feedback on your report from stakeholders, clearly specify: ▪ what type of feedback you want ▪ when you need it by.

Example

Communicate threat assessment

Fuchsia works in the ICT department of a large online audio equipment retailer. Fuchsia has been involved in drafting a threat assessment report and has been asked to deliver a 15 minute presentation to a group of the organisation's stakeholders. This group includes the head of finance, who is not well informed about cyber security but will be responsible for making money available to pay for security controls.

Fuchsia prepares a presentation in PowerPoint. Knowing she only has 15 minutes, she focusses on the main cyber threats facing the company, and the best strategies to address these threats. Fuchsia rehearses the presentation to ensure she can cover the required material in the allocated time, while allowing time for questions.

On the day of the presentation, Fuchsia uses a variety of strategies to engage the audience, such as maintaining eye contact and using body language. Her preparation pays off and the presentation runs smoothly.

Practice Task 7

Question 1

Which of the following are appropriate strategies to use when communicating a threat assessment via email? Tick all that apply.

- ◯ Use emojis and humour to connect with the audience.
- ◯ Avoid using the Bcc option if there are a lot of recipients.
- ◯ Avoid using all caps in the email subject line.
- ◯ Let recipients know if you need feedback.
- ◯ Avoid sending the report to non-work email addresses.

Question 2

What are three communication strategies you would use when presenting a cyber threat assessment in person?

3C Update threat assessment based on feedback

Be prepared to receive and consider stakeholder feedback.

It is rare that stakeholders have nothing to say about a threat assessment, so be prepared to receive at least some feedback. Depending on the number of stakeholders the assessment was communicated to, and their level of interest, the amount of feedback may be substantial. Once the report has been updated based on the feedback, it can be finalised.

Seeking feedback

Provide opportunities for stakeholders to provide you with feedback.

Depending on the method by which you communicated the threat assessment findings to stakeholders, you should be prepared to receive feedback in several ways. Some good practices for gathering feedback are outlined in the following table.

Did you communicate the threat assessment in person?	▪ Provide enough time either during or at the end of your presentation to answer questions and gather feedback. ▪ Note down any feedback received, along with the name of the person providing the feedback. Do not try to memorise all the feedback provided. ▪ Use both open and closed questions to confirm you have understood the feedback correctly. ▪ You may not have answers to questions and feedback on the spot. If in doubt, tell the person you will investigate their feedback and get back to them as soon as possible. ▪ Let the audience know how they can send any additional feedback and questions they think of later. This can be as simple as providing your email address and/or phone number for people to contact you.
Did you communicate the threat assessment by email?	▪ When sending out a threat assessment by email, let the audience know how to provide feedback and when you need it by. ▪ Asking people to record any specific feedback on your draft using track changes and comments makes it easy to review. ▪ Your audience may also send overall feedback in an email. ▪ Be sure to thank people who provide feedback.
How else might feedback be received?	In addition to feedback received during a presentation or in response to an email, you may receive ad-hoc feedback: ▪ in person, such as from staff dropping by your desk at work ▪ over the phone. In these situations, be ready to note down the feedback provided and the name of the person providing the feedback.

While there is no limit to the types of feedback you might receive from stakeholders, some of the most likely areas are:

- requests for more detail about the threats and recommendations you identified
- questions about how the threats were identified
- requests for more information about the process used to arrive at your recommendations
- suggested solutions that you may not have considered or included in your recommendations
- feedback on spelling, grammar and formatting.

You may also receive feedback endorsing your findings or complimenting your work.

Evaluating feedback

Not every piece of feedback you receive will mean changing the report. When reviewing stakeholder feedback, you should ask the following questions:

Is the feedback relevant to the scope of the report?	Stakeholders reviewing your report may forget, or not be aware, that a threat assessment usually does not look at every aspect of an organisation's ICT network. This means they may provide feedback or requests relating to devices, data or processes that were not included in the scope of the report.
Does the feedback support or conflict with existing information in the report?	Stakeholders will sometimes send feedback or information that strengthens or endorses your findings and recommendations. On the other hand, some stakeholders may disagree with your findings and recommendations or may provide conflicting information.
Does the feedback require further clarification from the stakeholder?	Stakeholder feedback may not always be clear. It may relate to operational processes, or parts of your organisation's ICT infrastructure, with which you are not familiar. If this happens, you may need to go back to the stakeholder to seek further information about what is being requested. You may also wish to talk with your manager for more clarification or information about the feedback.
Should the report be adjusted based on the feedback?	Depending on your answers to the above questions, you may need to update your report to reflect the information and feedback received from stakeholders.
What needs to be communicated back to the stakeholder?	It is good practice to thank stakeholders for taking the time to review your work and provide input, and to say that you have incorporated the feedback. If you are not incorporating feedback, such as because it falls outside of the scope of the report, it is best to let the stakeholder know this, and the reason why. This will avoid the risk of them asking for the same changes when the final version of the report is distributed.

If you receive strongly conflicting feedback from multiple stakeholders, it may be appropriate to convene a meeting with the relevant parties to discuss and confirm the changes to be made, rather than going back and forth with multiple stakeholders via email. If you are not sure which feedback should be included, discuss this with your manager to decide how to proceed.

Integrating feedback

Making a change in one part of your report may lead to other changes being required.

If you provided stakeholders with a deadline for providing feedback, wait until this date before you start making substantial changes to your document as you may receive conflicting feedback from different stakeholders.

Once you have gone through the process of identifying which feedback to accept, the process of updating your threat assessment should be straightforward. The following pointers will help you.

- Ensure that if you make a change in one part of the document, any other relevant parts of the document are updated for consistency. For example, if a stakeholder corrected the name of a piece of server hardware listed in the 'audit scope' section of the report, you need to make sure that any other references to this hardware are also updated.
- Depending on your organisation's practices, you may either need to track any changes to the document, so that changes based on feedback are clearly visible, or simply make and accept all changes to the document.
- Follow the version control processes used in your organisation when making changes to the document.

Finalising the assessment

Following some simple steps will give your report a professional edge.

After integrating stakeholder feedback, you need to finalise the report. Proofreading is an important part of this process. Whilst this is a time-consuming process, it is highly important in adding a layer of professionalism to your work.

Here are some tips for proofreading your report before you send out the final version:

Use an automatic spelling and grammar check	Every word processor has an inbuilt spelling and grammar checker, and you should run this on your document before distribution. Surprisingly, many people fail to use this simple technology. Make sure the language of your spelling checker is set to English (Australian). Remember that although automatic checks are great, they do miss things and you must always doublecheck your work. Common errors that are not always identified by automatic checkers are provided after this table.
Print your work before proofreading	Many people find it easier to identify errors on the printed page rather than on a computer screen. Being mindful of the environment, this should be done only after digital proofing tools have been used.
Read your report out loud	While it may feel strange, reading your work out loud is a great way to identify and address any unnatural language and grammar. It also helps with correct punctuation.
Check the first word of every sentence	Using the same first word over and over can be exhausting for a reader. Go through your report, identify any repetition, and look for alternate wording where appropriate.
Use appropriate tone and terminology	Consider the stakeholders who will be reading the report and ensure the tone and terminology is appropriate for them. Although your report is on a digital strategy, the stakeholder audience may not be very digitally literate. Avoid technical jargon and keep the tone clear and professional.
Ask a colleague or mentor to doublecheck	A second pair of eyes is always recommended to pick up errors you may have missed.

After you have integrated stakeholder feedback and proofread the document, it is ready to be finalised. The following table identifies some standard steps for finalising a document. These may vary depending on your organisation.

Update the version control information	Ensure the document's version control information is updated to a new version and is noted as a 'final' version.

Update or remove watermarks

If your draft document contained a 'draft' watermark, you need to remove this. Depending on your organisation's practices and sensitivity of the information contained in the report, you will need to either:

- add a 'confidential' watermark
- simply remove all watermarks from the document.

Check page numbering, headers, footers and table of contents

During the process of drafting and updating the document, details like page numbers, headers, footers and table of contents may become incorrect. As part of the finalisation process, check:

- page numbering is sequential and accurate
- the table of contents has been refreshed to ensure all major sections, and the correct page numbers, are included
- headers and footers are correct and consistent throughout the document.

Convert the document to PDF

It is likely you have drafted your recommendations document in an editable format such as Microsoft Word. As part of the finalisation process, you should convert the document to Portable Document Format (PDF) format. Converting the document to PDF prior to finalisation ensures:

- content in the document cannot be changed
- the formatting you applied will not be lost or changed when viewed on another computer
- the document can be opened by users who do not have access to document editing programs such as Microsoft Word.

Protect the document

Depending on the practices in your organisation, you may need to protect the document to prevent unauthorised access, distribution or changes. This may include setting a password to prevent unauthorised users from:

- opening the file
- copying information contained in the file
- printing the file.

Example

Update threat assessment based on feedback

Fuchsia presents the findings and recommendations of a threat assessment in person to company staff. Several staff members provide feedback on the assessment, which Fuchsia notes down, together with the names of the people providing the feedback. Fuchsia also provides her email and phone details during the presentation so that audience members can send feedback after the event. She receives a couple of pieces of feedback via email in the week following the presentation.

Fuchsia goes through the feedback and evaluates it. A selection of the feedback includes:

- Positive feedback about the clarity and quality of the assessment. Fuchsia thanks the person who provided this feedback and decides it does not entail changes to the report.
- Feedback asking why a particular server was not included the threat assessment. Fuchsia responds to this staff member to let them know this server was not included in the scope of this audit and lets the person know about the scope information provided in the report. No changes are required to the document.
- Feedback suggesting that staff training should be included as a recommended strategy to reduce the risk of phishing attempts. Fuchsia had not considered training before and agrees this is a good idea. She thanks the person and adds the recommendation about staff training to the report.
- Feedback noting incorrect terminology used for some of the company's ICT processes and procedures. Fuchsia thanks the person and updates this terminology in the report.

Having integrated the stakeholders' feedback, Fuchsia finalises the document. She conducts a number of proofreading checks such as running a spellcheck and reading the document out loud. She then updates the version history, removes the 'draft' watermark, ensures all the formatting is correct, and converts the document to a PDF.

Practice Task 8

Question 1

Which of the following are good practices for seeking stakeholder feedback when presenting a threat assessment in person? Tick all that apply.

- ◯ Tell stakeholders they should provide feedback on the spot as they might forget otherwise.
- ◯ Be prepared to provide answers to any questions asked by stakeholders on the day.
- ◯ Ask both open and closed questions to clarify any feedback you receive.
- ◯ Provide your email and phone details so stakeholders can send you feedback at a later date.
- ◯ Be prepared to note down any feedback received, along with the name of the person providing the feedback.

Question 2

What are two questions you should ask when considering whether stakeholder feedback should be integrated into a threat assessment?

3D Distribute and store threat assessment

Threat assessments need to be distributed and stored so the right people can access them.

The recommendations of the threat assessment process should lead to the implementation of security controls to manage threats. This means it is important that the threat assessment can be accessed when required by the relevant people, such as members of the ICT team or other company staff. This involves distributing and storing the report according to your organisation's policies and procedures.

Distributing and storing the assessment

Make sure you include all the relevant people when sharing the final report.

The finalised threat assessment should be made available to relevant stakeholders. This may be the same group which reviewed the draft report, but may also include other staff members not involved in the review process. Work with your manager to identify the appropriate people to include in the final report distribution list. Generally, the report should not be shared with people from outside your organisation.

Distribution methods

The following table outlines the most common ways to distribute the final report.

Email	Email is generally the most common way for distributing the final document. When using email to distribute the final report, remember the tips provided in topic 3B, namely: ▪ use an appropriate subject line ▪ use an appropriate greeting ▪ use font tools ▪ use humour and emojis carefully ▪ consider the recipient list ▪ spell check your email ▪ consider where the email is being sent. Instead of emailing the report document, it may be more appropriate to advise where the final report is stored in your organisation's network. Storage locations will be covered shortly.

Face to face or virtual meeting	You may be required to present the final report in a meeting with the stakeholder group. This can be conducted in person or using an online meeting tool. Remember the presentation techniques provided in topic 3B: ▪ arrive early so you can set up equipment and check everything is working. Remember to have a glass of water close by in case your throat gets dry ▪ use gestures and body language effectively ▪ do not overdo hand gestures. Only use them effectively to emphasise key points ▪ make eye contact and smile at various audience members to reach out and engage them from the start ▪ only refer to your notes occasionally If presenting in person, you may choose to print copies of the final report for attendees to review as you present it.
Collaboration tools	Your organisation may use online collaboration tools such as MS Teams, Slack or Trello. In some situations, it may be appropriate to share the final report using these tools. However, you should be careful to ensure the report is not shared with any unauthorised users.

Storage methods

The methods and systems used to store the final threat assessment will vary depending on the practices used in your organisation. Check where previous threat assessments, or similar documents, have been stored, or check with your manager if you are unsure. Some common storage methods are identified in the following table.

Storage methods for threat assessments
▪ Organisation's shared folder structure, such as a folder location dedicated for ICT staff. ▪ Organisation sanctioned cloud storage services, such as Google Drive, Dropbox and OneDrive. ▪ Document Management Systems (DMS) such as SharePoint, Hightail, Ascensio or DocuWare Cloud. ▪ Other bespoke quality or policy management software used by your organisation.

Regardless of the storage method used, some good practices when storing the final report include:

- ensuring the file name is clear and concise, for example 'ThreatAssessment-FINAL.docx'
- ensuring any old versions of the report are archived to avoid confusion
- ensuring the file is stored in a location which is only available to relevant stakeholders, not on a public folder accessible by all staff

- setting password controls to the file location if required, according to your organisation's password policies
- checking to make sure you can download and open the file from the storage location.

Manage ongoing feedback

Regardless of the distribution or storage method used, you may continue to receive feedback from interested stakeholders. While this feedback should be documented according to organisational procedures, you should advise stakeholders that the report has been finalised and any feedback will be considered for future reviews or threat assessments.

Follow policies and procedures

Depending on the scope of your threat assessment, the final report may include sensitive information about data, systems, staff and other information which is not allowed to be sent in an unprotected email. You also need to consider the audience who will be receiving the report, and the organisational policies in place for distribution of such reports.

You need to check your organisation's policies and procedures relating to the online distribution and storage of your report. The following table identifies some of the key documents you may need to consult.

Privacy policy	States the level of privacy required in the documents, such as naming of staff members.
Email usage policy	May determine the level of encryption, or whether a password is required, depending on the document's sensitivity level.
Transmission of sensitive data policy	States what is considered sensitive, the personnel to share it with, distribution methods, if encryption and if passwords are required.
Password management policy	Determines what level of password protection is required for sensitive documents, for example not using a simple password like 'password123'.
Digital copyright policy	Identifies requirements around copyright materials that may be included in your report.
Social media and web usage policy	States what types of information should not be shared online.
Encryption policy	Specifies what types of information must be encrypted and rules for encryption such as adding password protection.

Example

Distribute and store threat assessment

Zoe works in the ICT department of a library. She has been involved in documenting a threat assessment, which has recently been updated and finalised based on stakeholder feedback. Zoe checks with her manager to confirm the distribution list for the final report, as well as the appropriate location to store the report.

Threat assessments are stored in the library's 'U Drive', which is restricted and is not available to all staff. Zoe uploads the report to this location and ensures the file can be accessed and downloaded correctly. She then sends an email to the relevant stakeholders, following good email etiquette, advising where the final report can be accessed.

Practice Task 9

Question 1

What are three workplace policies or procedures you may need to be aware of when storing and distributing a threat assessment?

Question 2

Which of the following are good practices when storing a finalised threat assessment? Tick all that apply.

- ◯ Store the final document alongside previous versions.
- ◯ Apply a password to the document location if required.
- ◯ Use a clear and concise file name.
- ◯ Save the final report in a public folder so that it is easily accessible.
- ◯ Conduct checks to ensure you can access and download the document.

Summary

- The findings and recommendations of the threat assessment process should be documented in a threat assessment report.
- The structure of a threat assessment report may include details such as the threats identified, their risk level and recommended strategies to control the risks.
- Writing clearly, concisely and avoiding jargon will help improve the effectiveness of the report.
- The threat assessment findings and recommendations can be communicated either in person or by email.
- Presenting findings in person requires preparation and the use of delivery techniques.
- Communicating threat assessments by email requires the use of good email etiquette such as appropriate greetings, language and careful use of humour.
- Feedback needs to be proactively sought from stakeholders, regardless of the method used to communicate the findings and recommendations.
- Feedback needs to be carefully evaluated before being integrating into the report.
- Finalising the report requires careful proofreading, and should also involve updating version information, watermarks, and converting the document to PDF.
- The finalised threat assessment should be shared with stakeholders according to organisational policies and procedures.

Learning Checkpoint 3
Finalise threat assessment

Part A

1. Which of the following statements are correct? Select yes or no for each one.

   a) The findings of an audit can be documented in a threat assessment report. » Yes » No

   b) A threat assessment report may include details about the risk likelihood and business impacts for different threats. » Yes » No

   c) A threat assessment should use technical language instead of plain English wherever possible. » Yes » No

   d) Recommended strategies for addressing threats should be excluded from the report. » Yes » No

   e) Version control should be used during the process of drafting the report. » Yes » No

2. Which of the following strategies should be used when presenting a threat assessment in person? Tick all that apply.

   ◯ Refer to your notes frequently.

   ◯ Check the audience's facial expressions.

   ◯ Make eye contact and smile at audience members.

   ◯ Arrive early to troubleshoot any technical issues.

   ◯ Speak quickly to allow enough time for questions.

Part B

Read the case study and answer the questions that follow.

Case study

Marika works in the ICT department of a graphic design company. She has presented the findings of a threat assessment to a group of stakeholders in person.

1. What are three strategies Marika might use to seek feedback from her stakeholders?

2. Which of the following statements are correct? Select yes or no for each one.

   a) All stakeholder feedback received will result in changes to the final report. » Yes » No

   b) Feedback from different stakeholders may be inconsistent. » Yes » No

   c) Reading the report out loud is a good way to make sure it reads well. » Yes » No

   d) Making a change to one part of the report may mean Marika has to make changes to other parts of the report. » Yes » No

3. What are three workplace policies Marika may need to check when distributing the final report? Tick all that apply.

   - ◯ Privacy policy
   - ◯ Grievance handling policy
   - ◯ Email usage policy
   - ◯ Employee code of conduct
   - ◯ Password management policy

4. What are two methods Marika might use to distribute the final report?