BSBXCS404

Contribute to cyber security risk management

Assessment 1 of 5

Short Answer Questions

ASSESSOR GUIDE

Version 1

Assessment Instructions

Task overview

This assessment task is divided into sixteen (16) questions. Read each question carefully before typing your response in the space provided.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Question 1

Briefly outline the aim of the following Australian legislative acts relevant to cybersecurity and data protection:

- Privacy Act 1988 (Cth)
- Security of Critical Infrastructure Act 2018 (Cth)
- Telecommunications (Interception and Access) Act 1979 (Cth).

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must briefly outline the aim of the Australian legislative acts relevant to cybersecurity and data protection in the table below.

The response must include the following:

<<Insert your response here>>

- Privacy Act 1988 (Cth) aims to protect people’s personal information by regulating what data can be collected, how it can be used and who can access it.
- Security of Critical Infrastructure Act 2018 (Cth) aims to manage Australia-wide security risks from sabotage, coercion and espionage by foreign entities, including those posed by cyber connectivity.
- Telecommunications (Interception and Access) Act 1979 (Cth) aims to provide a legal framework for the privacy of private communication between two parties except in investigating serious crimes.

Question 2

Summarise the Australian Privacy Principles of the Privacy Act 1988 (Cth).

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must summarise the Australian Privacy Principles of the Privacy Act 1988 (Cth) in the table below.

The response must include the following:

<<Insert your response here>>

The Australian Privacy Principles (APPs) provide guidelines to organisations on how to meet the requirements of the Privacy Act 1988. The thirteen APPs provide guidelines on the rights, obligations, and standards for:

- the collection, use and disclosure of personal information
- an organisation or agency’s governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

Question 3

Explain what an organisation that must comply with the Privacy Act 1988 must do in the event of a notifiable data breach under the Notifiable Data Breaches scheme.

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must explain what an organisation that must comply with the Privacy Act 1988 must do in the event of a notifiable data breach under the Notifiable Data Breaches scheme in the table below.

The response must include the following:

<<Insert your response here>> The organisation must notify the Office of the Australian Information Commissioner (OAIC) as well as any individuals affected if the data breach is likely to cause them serious harm. The organisation must also put the data breach notification on their website if they are unable to contact all affected individuals and promote the data breach via other channels such as social media, advertisements, or newspapers.

Question 4

Outline what a notifiable data breach notification must include under the Notifiable Data Breaches scheme.

[Approximate word count: 40 – 80 words]

Assessor instructions: Students must outline what a notifiable data breach notification must include under the Notifiable Data Breaches scheme.

The response must include the following:

<<Insert your response here>> The organisation must include the following information in the notifications: • the organisation or agency's name and contact details • the kinds of personal information involved in the breach • a description of the data breach • recommendations for the steps you can take in response.

Question 5

Briefly outline the following international legislation relevant to cybersecurity and data protection:

- European Union General Data Protection Regulation (GDPR)
- The United Kingdom Data Protection Act 2018.

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must briefly outline the international legislation relevant to cybersecurity and data protection.

The response must include the following:

<<Insert your response here>> • The European Union General Data Protection Regulation (GDPR): imposes obligations on any organisation that collects data related to people in the European Union for the protection and use of this data. • The United Kingdom Data Protection Act 2018: is the United Kingdom's implementation of the GDPR and imposes controls on how personal information is used by organisations, businesses or the government entities that collect this information in the UK.

Question 6

Briefly summarise why each of the following are key risk management strategies for dealing with cybersecurity risks:

a) Regular organisational training (20 – 40 words)
b) Regular threat assessment (50 – 60 words)
c) Cyber security incident response plan (20 – 40 words)
d) Clear escalation routes. (30 – 50 words)

Assessor instructions: Students must briefly summarise why each of the following are key risk management strategies for dealing with cybersecurity risks.

The response must include the following:

<<Insert your response here>>

- Regular organisational training: keeps employees up to date on the latest cybersecurity risks, raising cybersecurity awareness on how to identify them and how they are to be dealt with.
- Regular threat assessment: ensures that evolving cybersecurity threats are regularly monitored to ensure that business continuity for the business network is maintained and that responses can be developed to deal with them if they occur. It also ensures that cybersecurity awareness training can be better informed to help minimise emerging evolving cybersecurity risks.
- Cyber security incident response plan: sets out the steps that information technology staff must follow in a cybersecurity event, including responsibilities and techniques that must be adhered to when dealing with them.
- Clear escalation routes: sets out the rules of escalation processes if a cybersecurity event cannot be dealt with by the person designated to respond to the event, including who they need to contact and how they do this.

Question 7

Briefly explain what a risk management methodology is and why it's important to analyse and review this methodology regularly. Write your answers in the template provided.

[Approximate table word count: 60 – 70 words]

Assessor instructions: Students must briefly explain what a risk management methodology is and why it's important to analyse and review this methodology regularly.

The response must include the following:

What is a risk management methodology?	<<Insert your response here>> A risk management methodology outlines the organisational processes for identifying hazards, assessing the risks of those hazards, how the risks are to be controlled, and monitoring these controls for effectiveness.
Why is it important to regularly analyse and review this methodology?	<<Insert your response here>> Regularly analysing and reviewing how risks are managed in the workplace is important to ensure that risk management processes are continually evolving and improving to minimise the impact of risks on business operations.

Question 8

Briefly outline how an organisation's Communication Policy impacts on the development of communication plans.

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must briefly outline how an organisation's Communication Policy impacts on the development of communication plans.

The response must include the following:

<<Insert your response here>> The Communication Policy is to set out organisational practices and processes for different reasons of communication in the workplace, both internally and externally, including how this communication is to take place to ensure the message is adequately conveyed and received and the required privacy and confidentiality provided for.

Question 9

Outline three (3) components that a policy and procedure must contain so that the effectiveness of the risk management strategies can be evaluated successfully.

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must outline three components that a policy and procedure must contain so that the effectiveness of the risk management strategies can be evaluated successfully.

The response must include three (3) of the following:

<<Insert your response here>> ▪ how the review data from monitoring over time will be measured to determine effectiveness (for example, benchmarks, KPIs, etc.) ▪ how a cyber security maturity model will be used to evaluate the cyber security maturity of the business ▪ how and when cybersecurity tests will be undertaken (for example, penetration testing) to help determine effectiveness ▪ how the network, application, and system activity will be monitored to validate effectiveness. ▪ how monitoring information will be documented.

Question 10

Briefly outline the following procedures that organisations implement to monitor cybersecurity risks:

- Cybersecurity Audit
- Cybersecurity Risk Threat Assessment.

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must briefly outline the listed procedures that organisations implement to monitor cybersecurity risks.

The response must include the following:

<<Insert your response here>>

- Cybersecurity Audit: a systematic assessment of an organisation's cybersecurity protection measures to help identify possible cybersecurity issues or organisational security risks.
- Cybersecurity Risk Threat Assessment: an assessment of the possible cybersecurity risks the organisation might face and the threat they pose to business continuity.

Question 11

Briefly outline what a risk management policy and procedure must contain so that reviewing the currency of cybersecurity risks in a risk register is effective.

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must Briefly outline what a risk management policy and procedure must contain so that reviewing the currency of cybersecurity risks in a risk register is effective.

The response must include the following:

<<Insert your response here>>

It must outline the schedule for when each risk is to be reviewed, who has the responsibility of reviewing each risk, what the outcome of the review is, the action to be taken, and who the incident should be reported to.

Question 12

Briefly outline three (3) industry-proven cybersecurity protection measures/procedures organisations can implement when applying cybersecurity risk management strategies.

[Approximate word count: 60 – 80 words]

Assessor instructions: Students must briefly outline three industry-proven cybersecurity protection measures/procedures organisations can implement when applying cybersecurity risk management strategies.

The response must include three (3) of the following:

<<Insert your response here>>

- Access management: an organisational process that sets up individual roles and groups within a business network to control who can access business data and what they can do with it.
- Administrative protection procedures: designed to that guide employees on what they must do to minimise cybersecurity risks.
- Anti-malware software: installed software on the business network designed to identify cybersecurity threats and quarantine these threats from the system.
- Backup and recovery procedures: designed to ensure that business data is regularly backed up and that this data can be recovered swiftly in case of any issues affecting the business data used on a business network.
- Cybersecurity awareness program: a program designed to teach employees about emerging cybersecurity threats and what to do if these occur.

Question 13

Using the template below:

a) Briefly outline why an organisation must implement a Change Management Policy as a guideline when updating the technologies used in its business network.

b) Research and list the 7 R's of a Change Management guidelines that could be implemented when updating an organisation's technology.

[Approximate table word count: 80 – 100 words]

Assessor instructions: Students must complete the table below following the instructions provided in the question.

The response must include the following:

a) Why organisations must use a change management policy when implementing changes.	Organisations use a Change Management Policy to outline processes that must be followed for implementing any organisational change, including technology changes or work processes affecting technology, to ensure that any cybersecurity risks are identified and controlled as part of the changes being implemented by the organisation.
b) 7 R's of Change Management.	▪ The REASON behind the change? ▪ RISKS involved in the requested change? ▪ RESOURCES required to deliver the change? ▪ Who RAISED the change request? ▪ RETURN required from the change? ▪ Who is RESPONSIBLE for creating, testing, and implementing the change? ▪ RELATIONSHIP between suggested change and other changes?

Question 14

Specify three (3) business process design principles employees should be mindful of when designing a new business process so that risks in this process are minimised and accounted for.

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must specify three (3) business process design principles employees should be mindful of when designing a new business process so that risks in this process are minimised and accounted for.

The response must include three (3) of the following:

<<Insert your response here>>

- ensuring that the roles and responsibilities of parties involved in the business process are clearly defined
- ensuring that the process design has continuous improvement processes built into the design
- organisational goals and objectives are factored into the process design

- risks are identified early in the design so the process design can account for them
- stakeholders are informed about and involved in the process design so that potential risks can be more readily identified.

Question 15

Briefly outline the four (4) maturity levels that organisations need to measure and report their cyber security maturity upon using the Essential Eight Maturity Model developed by the Australian Cyber Security Centre (ACSC).

[Approximate word count: 40 – 50 words]

Assessor instructions: Students must briefly outline the four maturity levels that organisations need to measure and report their cyber security maturity upon using the Essential Eight Maturity Model developed by the Australian Cyber Security Centre (ACSC).

The response must include the following:

<<Insert your response here>>

- Maturity Level Zero: signifies weaknesses in an organisation's overall cybersecurity processes.
- Maturity Level One: signifies that the organisation's cybersecurity processes are partially effective.
- Maturity Level Two: signifies that the organisation's cybersecurity processes are mostly effective
- Maturity Level Three: signifies that the organisation's cybersecurity processes are fully effective.

Question 16

If your company is dealing with a company in the United States, what is the primary federal cybersecurity regulation you need to comply with?

Assessor instructions: Students must explain what the primary federal cybersecurity regulation in the USA is.

The response needs to reference the Act below:

<<Insert your response here>>

The primary law governing cybersecurity in the United States is the Federal Trade Commission Act (FTCA).

Assessment checklist:

Students must have completed all questions within this assessment before submitting. This includes:

1	Sixteen (16) short answer questions to be completed in the spaces provided.	□

✓

Congratulations you have reached the end of Assessment 1!