Knowledge assessment: Workplace security knowledge

Criteria

Unit code, name and release number

BSBXCS404 - Contribute to cyber security risk management (1)

ICTICT451 - Comply with IP, ethics and privacy policies in ICT environments (1)

Qualification/Course code, name and release number

ICT40120 - Certificate IV in Information Technology (3)

Student details

Student number

880644379

Student name

Gavin Lampe

Assessment Declaration

Note: If you are an online student, you will be required to complete this declaration on the TAFE NSW online learning platform when you upload your assessment.

This assessment is my original work and has not been:

- plagiarised or copied from any source without providing due acknowledgement.
- written for me by any other person except where such collaboration has been authorised by the Teacher/Assessor concerned.

Student signature and Date

Version:	20210601
Date created:	1 June 2021
Date modified:	5 May 2022 – recontextualized for the gaming industry

For queries, please contact:

Contact Details: Technology and Business Services SkillsPoint

Location: Parramatta

Assessment instructions

Table 1 Assessment instructions

Assessment details	Instructions
Assessment overview	The aim of this assessment is to assess your knowledge of: • legislation and organisational policies and procedures related to: a. cyber security risk management, b. IP, ethics and privacy • risk management strategies • protocols for cyber security
Assessment Event number	2 of 2
Instructions for this assessment	This is a written assessment that assesses your knowledge of the unit. **This assessment is individual work.** This assessment is in one part: 1. Short answer questions. And is supported by: • Assessment feedback
Submission instructions	On completion of this assessment, you are required to submit it to your Teacher/Assessor for marking. If you are completing this as an online quiz, ensure you click the submit button when complete. You can save as you progress to avoid losing your work. Ensure you have included your name at the bottom of each document you submit. This is not required for an online quiz. It is important that you keep a copy of all electronic and hardcopy assessments submitted to TAFE and complete the assessment declaration when submitting the assessment.

Assessment details	Instructions
What do I need to do to achieve a satisfactory result?	To achieve a satisfactory result for this assessment all questions must be answered correctly. If a resit is required to achieve a satisfactory result it will be conducted at an agreed time after a suitable revision period.
What do I need to provide?	• TAFE NSW student account username and password. If you do not know your username and password, contact your campus or service centre on 131601. • Computer or other device with word processing software and internet access • Writing materials, if required.
What the Teacher/Assessor will provide	Access to this assessment and learning resources, including the student workbook and any supporting documents or links.
Due date **Time allowed**	Two hours (indicative only)
Supervision	This is an unsupervised, take-home assessment. Your Teacher/Assessor may ask for additional evidence to verify the authenticity of your submission and confirm that the assessment task was completed by you. You may access your referenced text, learning notes and other resources.

Assessment details	Instructions
Assessment feedback, review or appeals	In accordance with the TAFE NSW policy *Manage Assessment Appeals,* all students have the right to appeal an assessment decision in relation to how the assessment was conducted and the outcome of the assessment. Appeals must be lodged within **14 working days** of the formal notification of the result of the assessment. If you would like to request a review of your results or if you have any concerns about your results, contact your Teacher/Assessor or Head Teacher. If they are unavailable, contact the Student Administration Officer. Contact your Head Teacher for the assessment appeals procedures at your college/campus.

Part 1:

Read each question carefully and provide your answers.

1. Given on the left are Gelos/Game Environment cyber security protocols. On the right are the risks, if protocols are not followed. Match the protocols on the left with their respective risks on the right. Place the relevant letter in the column on the left

Cyber Security Protocols	Risks, if Protocols Are not Followed
BYOD policy **C**	**A** -Data theft
Email policy **B**	**B** - Spam attacks
Data storage policy **A**	**C** -Data leakage or loss

2. Given on the left are the examples of Game Enviroment's IT assets. On the right are the organisational policy or procedures. Match the IT assets on the left with their respective procedures on the right. Place the relevant letter in the column on the left

IT Asset	Organisational policy or procedure
Software Code **A**	**A** - Ensure any applicable copyright is shown on all documentation.
Unique and Innovative Game Mechanics **B**	**C** - The company logo or the logo of the company product can be trademarked so it is not used on product not authorised or produced by the company.
Company Logo **C**	**B** - Make sure everyone is aware of what Designs and Patents are registered and what they need to do to protect them.

3. List at least 3 each of the ACS Code of Ethics and the ITPA Code of Ethics.

ACS Code of Ethics:

- **Honesty**: You will be honest in your representation of skills, knowledge, services and products.
- **Competence**: You will work competently and diligently for your stakeholders
- **Professionalism**: You will enhance the integrity of the Society and the respect of its members for each other.

ITPA Code of Ethics:

- **Fair Treatment:** I will treat everyone fairly. I will not discriminate against anyone on grounds such age, disability, gender, sexual orientation, religion, race or national origin.
- **Privacy:** I will access private information on computer systems only when it is necessary in the course of my duties. I will maintain the confidentiality of any information to which I may have access. I acknowledge statutory laws governing data privacy such as the Commonwealth Information Privacy Principles.
- **Communication:** I will keep users informed about computing matters that may affect them -- such as conditions of acceptable use, sharing of common resources, maintenance of security, occurrence of system monitoring and any relevant legal obligations.

4. Given on the left are the APPs. On the right are the procedures by which the APP relates to the Games industry. Match the APPs on the left with their respective procedures on the right. Place the relevant letter in the column on the left

APP	Procedures by which the APP relates to the IT industry
Open and transparent management of personal information **A**	**A -** Ensures that companies in the Games Industry manages personal information that is held on servers/databases in an open and transparent way.

Collection of solicited personal information **C**	**B -** The Games Industry must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. The Industry must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
Quality of personal information **B**	**C -** Provides guidelines to how and when personal information can collect information that is solicited for storing in IT systems

5. Given on the left are the components of a cyber risk management strategy. On the right are factors under consideration. Match the components on the left with their respective factors on the right. Place the relevant letter in the column on the left

Component	Factors to consider
Regular organisational training **C**	**A-** Need to have a process in place that kicks off the plan immediately a risk becomes an incident and ensure that is understood and followed and reviewed
Regular threat assessment **B**	**B -** Need to have a policy in place to assess all threats – known and potential, and having the right process in place to ensure that it is understood, followed and reviewed
Incident Response Plan **A**	**C -** Training needs to be easy to access and easy to understand and cover all cyber risk aspects relevant to the people being trained
A process for escalating issues **D**	**D -** Need to provide clear steps in how to escalate cyber security risks and issues and who to escalate them to.

6. Given on the left are procedures you would use in implementing a risk management strategy. On the right are the pointers showing the importance of the steps to the risk strategy. Match the procedures on the left with their respective pointers on the right. Place the relevant letter in the column on the left

Procedures	Importance of this step to the risk strategy
Identify the risk **B**	**A -** This helps you understand the probability of whether the risk will occur
Estimate the likelihood of it happening **A**	**B -** You need to first work out all the things that could go wrong
Estimate the impact if it does happen **E**	**C -** Risks that are deemed a priority can then have an approach or strategy put in place, with appropriate actions to either mitigate or negate the risk.
Determine the severity of the risk **D**	**D -** Severity is a factor of impact x probability and assists in prioritisation of which risks to most focus on
Decide the mitigation approach **C**	**E -** This help you understand the consequence or how much an impact will be felt by the business if the risk occurs

7. What is meant by a company's **Cyber Security Maturity**? Describe each of the Maturity Levels

Cyber Security Maturity means how strong is a company's cyber security, or how *mature* (as in developed) is their cyber security. If they have very weak security then they have not developed proper policies or protocols and their system is *immature.*

Maturity Level 0 signifies that there are weaknesses in an organisation's overall cyber security posture – this means that they essentially do not have proper cyber security protocols or protections in place.

Maturity Level 1 is bad actors using easily and widely available tools to find exploits in any system rather than targeting a specific company.

Maturity Level 2 is adversaries that have significantly higher capabilities. They invest more time on a specific target and more time developing their tools.

Maturity Level 3 is adversaries who are much more adaptive in their techniques and don't use public tools as much. They can exploit more opportunities such as outdated software and poor security logging and monitoring.

8. An important part of tracking an organisation's **cyber security maturity levels** is to report on the current state and desired future maturity levels. Discuss two methods for reporting these maturity levels.

(use the following: https://www.protectivesecurity.gov.au/publications-library/policy-5-reporting-security)

There are two methods for reporting maturity levels depending on how classified the information that is being protected is. Both methods are for completing and annual report of a company's maturity level to be sent to the Attorney-General's Department.

For information that is classified up to the level of "Protected" companies can use an online reporting portal to complete their annual assessment.

For information that is classified higher than "Protected", the online portal cannot be used, so a reporting template is used instead.

Both reports must provide rationales for their assessment, details of strategies to mitigate risks, a summary of the risk environment, and key risks to people, information, and assets.

9. Given on the left are the legislative and regulatory requirements related to cyber security risk management. On the right are discussions. Match the requirements on the left with their respective discussions on the right. Place the relevant letter in the column on the left

Legislation	Discussion of requirements related to cyber security risk management

Data protection legislation **D**	**A -** Cyber security risk management must consider all 13 Australia Privacy Principals and ensure they have the appropriate management in place to ensure breaches don't occur.
Notifiable Data Breach legislation **C**	**B -** Organisations must meet any ISO standards (eg 31000) with regards to cyber risk management.
Australian privacy laws **A**	**C -** Organisations must ensure they meet the requirements of the Privacy Amendment (Notifiable Data Breaches) Act 2017 whenever there has been a cyber security risk/breach.
Established international legislation **B**	**D -** From a cyber risk point of view, organisations must ensure that they assess and mitigate against any breach of privacy legislation where personal information is stolen or misused

10. Given on the left are the types of IP in the ICT industry. On the right are the names of key legislation. Match the IPs on the left with their respective legislations on the right. Place the relevant letter in the column on the left

Type of IP	How the legislation applies to evaluating and implementing IP
Trademark **B**	**A -** This legislation defines the legally enforceable rights of creators of creative and artistic works under Australian law and applies to any copying or re-use performed in Australia, even if the owner of copyright in the work that is being copied is a citizen of another country.
Patent **C**	**B -** This legislation defines the law in regards to what things can be registered as a Trademark and what constitutes infringement of this type of intellectual property
Copyright **A**	**C -** This legislation governs the granting of a temporary monopoly on the use of an invention, in exchange for the publication and free use of the invention after a certain time.

Assessment Feedback

NOTE: This section must have the Teacher/Assessor and student signature to complete the feedback. If you are submitting through the TAFE NSW online learning platform, your Teacher/Assessor will give you feedback via the platform.

Assessment outcome

☐ Satisfactory

☐ Unsatisfactory

Assessor feedback

☐ Has the Assessment Declaration for this assessment event been signed and dated by the student?

☐ Are you assured that the evidence presented for assessment is the student's own work?

☐ Was reasonable adjustment in place for this assessment event?

If yes, ensure it is detailed on the assessment document.

Comments:

Assessor name, signature and date:

Student acknowledgement of assessment outcome

Would you like to make any comments about this assessment?

Student name, signature and date
