|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification details** |  | | |
| **Training Package code and title** | **ICT - Information and Communications Technology** | | |
| Qualification National Code & Title | **ICT40120 Certificate IV in Information Technology** | **State code:** |  |
| Unit National Code & Title | **BSBXCS404 Contribute to cyber security risk management** | **State code:** |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Student’s name:** | | | Richard Pountney | **Student ID:** | 30007736 | |
| **Assessor’s name:** | | |  | **Assessment Date:** |  | |
| **Time allocated:** | | | 2 weeks | | | |
| **Resources allowed:** | | | Internet, Blackboard, PowerPoint Presentations | | | |
| **Assessment Task Instructions:** | | | **Scenario**: *You are a member of the CITE MS security team. The management team of one of your clients wants to expand their understanding of risk management in relation to cyber security. As such, they have sent a series of questions, the answers of which are aimed to help guide their decision-making for training material in the future.*  Fully answer all questions in detail and submit to the lecturer via Blackboard as an electronic copy. Any and all external sources used (images, websites, articles, or otherwise) need to be referenced. | | | |
| **Questions to be answered by the student:** | | | | | **Satisfactory**  **Response** | |
| **Yes**  | **No**  |
| Q1 | Name and describe the Australian legislation that pertains to data protection and privacy. In your answer, specifically include how this legislation relates to cyber security. | | | |  | |
| **Response:**  [Privacy Act 1988](https://www.legislation.gov.au/Details/C2014C00076)  This legislation sets out rules for businesses to follow.  It outlines the requirements on how to collect, use, store & disclose personal information.  This is meant to protect your personal information privacy & not your physical privacy.  This contains the 13 Australian Privacy Principles (APP). These principles provide guidance on how personal information should be handled. | | | | |  |  |
| Q2 | | Explain how the Notifiable Data Breach legislation affects organisations and how it links to other Australian legislation. | | |  | |
| **Response:**  All organisations or agencies the Privacy Act 1988 covers must notify affected individuals & the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved this is required for the Notifiable Data Breaches (NDB) scheme. | | | | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Q3 | Describe the General Data Protection Regulations (GDPR), its major provisions, and how it relates to Australian entities. In your response, describe at least two differences it has to Australian privacy legislation. |  | |
| **Response:**  Even though GDPR was made & passed by the European Union (EU), it imposes obligations onto organisations anywhere, while they target or collect data related to people in the EU.  The General Data Protection Regulation (GDPR) is the toughest privacy & security law in the world.  The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy & security standards, with penalties reaching into the tens of millions of euros. Ten million euros ≈ 14805452.20 AUD  The Provisions are a right to:   * Access their personal data. * Rectify inaccuracies in their personal data. * Have personal data erased in certain cases. * Restrict the processing of their personal data. * Portability (Data Portability Right) * Object to data processing. * Not be subjected to automated processing including profiling (Right to No Profiling)   The Provision information is from here:  <https://www.lexology.com/library/detail.aspx?g=5ae76660-9770-4718-9010-6657a9351496#:~:text=Under%20the%20GDPR%2C%20individuals%20have,right%20to%20object%20to%20data> | |  |  |
| Q4 | Describe the objective and purpose of regular organizational training in relation to risk management. |  | |
| **Response:**  Education, Training, & Awareness (ETA) is a means to help address one of the most major issues within organisation security, users.  People are ultimately the weakest link in security. They are often gullible, fallible, & have access to the systems.  Roughly 85% of all ‘attacks’ are initiated from a user-triggered action. These aren’t necessarily malicious & are often accidental.  Have you ever accidentally deleted your work?  Because of this, it would be best to have some training to help minimise the ‘attacks’ by informing the user what causes the ‘attacks’ & telling them the correct way to do something. | |  |  |
| Q5 | Describe the objective and purpose of regular threat assessment in relation to risk management. |  | |
| **Response:**  The objective of threat assessment is to check if there are any gaps in risk management & the purpose is to improve the area where a gap is found.  Threat assessment provides a way to update & review risks as new developments occur & then take steps to protect the organisation, people, & assets using risk management.  Threat assessment is the process to review any threats/risks & risk management is the process to maintain power or minimise the threats/risks. | |  |  |
| Q6 | Describe the objective and purpose of a cyber security incident response plan in relation to risk management. |  | |
| **Response:**  The aim is to minimize the negative impact on the business.  Risk management helps to prepare businesses for unexpected disruptions.  Cyber security incident response plan help resumes an ICT service to normal as quickly as possible after a disruption.  Cyber security incident response plan helps to demonstrate IT’s value to the business by aligning IT activities to business priorities.  The purpose is to reduce the impact on the business & user with improved monitoring.  The objective is to meet legal & regulatory compliance. | |  |  |
| Q7 | Describe the objective and purpose of clear escalation routes in relation to risk management. |  | |
| **Response:**  Incident escalation is what happens when an employee can’t resolve an incident themselves & needs to hand off the task to a more experienced or specialized employee. This usually happens when the existing knowledge base does not consist information for the reported incident.  By having a well-planned incident escalation process, organisations can ensure that all incidents are managed at an appropriate level by the appropriate personnel. | |  |  |
| Q8 | Describe the procedures involved in analysing and reviewing risk management methodologies. |  | |
| **Response:**  Risk management is best understood as a cyclical process in which new & ongoing risks are continually identified, assessed, managed, & monitored.  This is a structured approach to addressing risks & can be used in companies of all sizes & across any industry.  The Process steps are:   * Risk & Hazard identification * Determining the likelihood & size of potential losses * Creation of controls & mitigation measures * Record, review, & monitor.   Some info was got from here: <https://reciprocity.com/blog/types-of-risk-assessment-methodologies/> | |  |  |
| Q9 | Describe the procedures involved in developing communication plans. |  | |
| **Response:**   1. Perform a situation analysis 2. Define objective 3. Define the target audience 4. Identify communication media/channels 5. Establish communication expectations 6. Evaluate results   A communication plan can be done verbally, non-verbally, written, visually, or in formal communication. | |  |  |
| Q10 | Describe the procedures involved in evaluating effectiveness of risk management strategies. |  | |
| **Response:**  You match the outcomes of a risk management plan with its objectives.   * Check if the risks are avoided, transferred, mitigated, or accepted according to the plan.   Evaluate if all the activities that are in the plan would be effective.   * The strategy is only as strong as the weakest link.   Evaluate the business environment.   * Check if the strategies have affected the business environment.   Identify areas of improvement.   * After all, evaluations try to make possible changes in the action plan to get the desired results. | |  |  |
| Q11 | Describe the procedures involved in monitoring cyber risk. |  | |
| **Response:**  The procedures are:   * Monitoring changes in the internal & external environment. * Identifying new &or emerging risks. * Ensuring the effectiveness & relevance of controls & implementation of treatment programs. * Get further information to improve the understanding & management of already identified risks. * Analyse & learn lessons from past events, including near-misses, successes, & failures. * Record the results and observations from the monitoring & reviews. | |  |  |
| Q12 | Describe the procedures involved in reviewing currency of risk register. |  | |
| **Response:**  Monitor & review changes periodically to ensure that the controls in place are still suitable for the current landscape.  New IT asset addition to the infrastructure.   * The introduction of new assets into the infrastructure will create new risks. The organisation must identify the additional assets to be able to manage the threats & risks associated with the assets. * Assets can be hardware, software, or intangible assets like knowledge.   Technology advancement.   * As technology advances, new systems will be created &or changes will be made to existing systems. This will inevitably introduce new threats & risks. * Some technology advancements are:   + New tech products   + Software/firmware updates   + Additional features for current or older technology   Changes in the work procedures.   * When there are changes in work procedures, the organisation should review its risk landscape. Changes in the work procedures may increase or decrease existing risks or cyber threats. * This can include a role change or new employees. * The cyber security strategy may need to be changed in relation to the work procedure changes.   New threats in the wild.   * Sometimes even if the risk management strategies are current & valid, new threats may still arise. These threats are often referred to as zero-day exploits. * Zero-day exploits are threats where no existing resolutions are available.   Interim solutions may be applied to avoid or mitigate these exploits. | |  |  |
| Q13 | You have been tasked to review the risk management strategies for a client in the **healthcare industry**. What kind of industry-specific considerations should you keep in mind when implementing the risk management procedures? |  | |
| **Response:**  I should be considering:   * Confidentiality of information * External threats   + Data Breach   + Ransomware   + Spear Phishing & Business Email Compromise (BEC)   + Distributed Denial-of-Service (DDoS) Attacks * Internal threats   + Malicious Insiders   + A Lack of Security Awareness   Some info was got from here: <https://contentsecurity.com.au/cyber-security-concerns-in-healthcare/> | |  |  |
| Q14 | List and describe the steps involved in updating technology based on an industry-accepted guideline. |  | |
| **Response:**  Make sure that the industry guideline accepts the technology that is being updated or added by using a SWOT analysis.  SWOT analysis: it helps identify Strengths, Weaknesses, Threats & Opportunities associated with risks that may occur.  Fishbone Diagram: the cause & effect diagram is used to break down a problem to identify the root causes behind it. This diagram can also work backward because it can help identify the causes of an effect. This can be useful for presenting multiple options. | |  |  |
| Q15 | Describe 2 business process design principles in relation to risk management. |  | |
| **Response:**  Manual methods are effective when strategies are implemented physically & compliance is dependent on user behaviours.  Examples of Manual methods are:   * Audits * Periodic spot checks * Logs review * Whistleblowing * Physical observation   Automation methods are effective when strategies are implemented logically & when user activities are consistent. It is highly recommended that a baseline/pattern can be established so that anomalies can be flagged out.  Examples of Automated methods are:   * Security alerts * Rule-based monitoring * SIEM dashboards * Sensors & triggers | |  |  |
| Q16 | Explain what and how reporting mechanisms are used for tracking organisational cyber security maturity. |  | |
| **Response:**  Well established feedback process enables any new risks to be reported & managed effectively. This can also encourage users to report any new risks proactively. The end users are more likely to encounter anomalies with the system than the security team.  To track reporting you can use a timeline of information to see if the risk is still present &or has it escalated. | |  |  |

|  |  |  |
| --- | --- | --- |
| **Assessor Feedback** | | |
| **Assessment Decision** | ☐ Satisfactory | ☐ Not Yet Satisfactory |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Is student eligible for reassessment (Re-sit)?** | No | Yes | **Reassessment Date:** |  |

|  |
| --- |
| **Feedback to student** |
|  |
| **Feedback from student** |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student’s signature:**  *(Once feedback has**been**provided)* |  | **Date:** |  |
| **Assessor’s signature:**  *(Once feedback has**been**provided)* |  | **Date:** |  |