|  |  |  |  |
| --- | --- | --- | --- |
| **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  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:**  Under the Notifiable Data Breaches (NDB) scheme any organisation or agency 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. | | | | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 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:**  The GDPR is the toughest privacy & security law in the world. Even though it was made & passed by the European Union (EU), it imposes obligations onto organisations anywhere, as long as they target or collect data related to people in the EU.  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 | |  |  |
| 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? | |  |  |
| Q5 | Describe the objective and purpose of regular threat assessment in relation to risk management. |  | |
| **Response:**  To check if there are any gaps in the risk management & to improve that area.  It provides a way to update & review assessments as new developments occur & then to take steps to protect the organisation, people, & assets. | |  |  |
| Q6 | Describe the objective and purpose of a cyber security incident response plan in relation to risk management. |  | |
| **Response:**  It aims to minimize the negative impact on the business.  To prepare businesses for unexpected disruptions.  Resumes an ICT service to normal as quickly as possible after a disruption.  It demonstrates IT’s value to the business by aligning IT activities to business priorities.  To reduce the impact on the business & user with improved monitoring.  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 | |  |  |
| Q9 | Describe the procedures involved in developing communication plans. |  | |
| **Response:** | |  |  |
| Q10 | Describe the procedures involved in evaluating effectiveness of risk management strategies. |  | |
| **Response:**  SWOT analysis | |  |  |
| Q11 | Describe the procedures involved in monitoring cyber risk. |  | |
| **Response:** | |  |  |
| Q12 | Describe the procedures involved in reviewing currency of risk register. |  | |
| **Response:** | |  |  |
| 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:** | |  |  |
| Q14 | List and describe the steps involved for updating technology based on an industry accepted guideline. |  | |
| **Response:** | |  |  |
| Q15 | Describe 2 business process design principles in relation to risk management. |  | |
| **Response:** | |  |  |
| Q16 | Explain what and how reporting mechanisms are used for tracking organisational cyber security maturity. |  | |
| **Response:** | |  |  |

|  |  |  |
| --- | --- | --- |
| **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:** |  |