|  |  |  |  |
| --- | --- | --- | --- |
| **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:** | | | Poorav Sharma | **Student ID:** | 30045900 | |
| **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 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: Australian legislation that pertains to data protection and privacy is the Privacy Act 1988. It outlines requirements on how to collect, use, store and disclose personal information. This legislation relates to cyber security because it requires regulated entities to take reasonable steps in circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.** | | | | |  |  |
| Q2 | | Explain how the Notifiable Data Breach legislation affects organisations and how it links to other Australian legislation. | | |  | |
| **Response:** U**nder the Notifiable Data Breaches scheme, an organisation or agency the Privacy Act 1988 covers must notify affected individuals and 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 difference it has to Australian privacy legislation. |  | |
| **Response:** **The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. It was drafted and passed by the European Union (EU). It imposes obligation onto organizations anywhere, so long as they target or collect data related to people in the EU. This means any Australian entities that target or collect data related to people in the EU must follow the GPDR principles. The five GDPR principles are Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality (security); Accountability. The Privacy Act 1988 does not have accountability principles where as GDPR does. GDPR however does not have principles for rights that Privacy Act 1988 has, GDPR has it in a separate provision.** | |  |  |
| Q4 | Describe the objective and purpose of regular organizational training in relation to risk management. |  | |
| **Response: The objective and purpose of regular organizational training in relation to risk management is to help the origination recognise and understand their risks and how to manage them in order to lower the damage they may cause.** | |  |  |
| Q5 | Describe the objective and purpose of regular threat assessment in relation to risk management. |  | |
| **Response:** | |  |  |
| Q6 | Describe the objective and purpose of a cyber security incident response plan in relation to risk management. |  | |
| **Response:** | |  |  |
| Q7 | Describe the objective and purpose of clear escalation routes in relation to risk management. |  | |
| **Response:** | |  |  |
| Q8 | Describe the procedures involved in analysing and reviewing risk management methodologies. |  | |
| **Response:** | |  |  |
| Q9 | Describe the procedures involved in developing communication plans. |  | |
| **Response:** | |  |  |
| Q10 | Describe the procedures involved in evaluating effectiveness of risk management strategies. |  | |
| **Response:** | |  |  |
| 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:** |  |