|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student Name |  | | Student Number | |  |
| Unit Code/s & Name/s | VU23223 Apply cyber security legislation, privacy and ethical practices | | | | |
| Cluster Name  *If applicable* | N/A | | | | |
| Assessment Type | Assignment  Project  Case Study  Portfolio  Third Party Report (Workplace)  Third Party Report (Peer)  Other | | | | |
| Assessment Name | Cyber security legislation, privacy and ethical practices Portfolio | | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | | Date Submitted | | / / |
| **Assessor Feedback:** | | | | | |
| **Attempt 1** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| **Student provided with feedback and reassessment arrangements**  *(check box when completed)* | | | Date scheduled for reassessment | | / / |
| **Attempt 2** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| Note to Assessor: Please record below any reasonable adjustment that has occurred during this assessment e.g. written assessment given orally. | | | | | |
|  | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assessment Criteria / Benchmarks  ***The evidence submitted demonstrates that the student has satisfactorily:*** | Attempt 1 | | Attempt 2 | |
| **Date**  \_\_/\_\_/\_\_ | | **Date**  \_\_/\_\_/\_\_ | |
| Y | N | Y | N |
| **PART 1 – Review of cyber security legislative and regulatory requirements for Australian organisations** |  |  |  |  |
| **ORGANISATION 1** |  |  |  |  |
| * 1. Evidence that the scenario has been read by completing the following:  1. Overview of the sector of the scenario presented provided 2. Current Federal, State/Territory and sector-specific cyber security and related legislation that applies to the organisation provided   Table provided has been utilised. | ☐  ☐ | ☐  ☐ | ☐  ☐ | ☐  ☐ |
| 1.2 Business operations analysis completed:  a) International cyber security legislation that has an impact on their data security has been identified  b) Areas of the business affected by the international legislation identified  c) The impact on the business operation and data security identified | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| * 1. At least one (1) interdependency between different legislative instruments related to cyber security have been identified and explained. |  |  |  |  |
| * 1. One (1) instance where a regulator can contribute to the security of business data operations has been identified. Impact of the contribution clarified. |  |  |  |  |
| * 1. This task covers both organisations.   For each of the regulators presented below, identify and explain their role and scope.   * Australian Prudential Regulation Authority (APRA) * Australian Securities and Investments Commission (ASIC) * Australian Competition and Consumer Commission (ACCC) * Australian Energy Sector Cyber Security Framework (AESCSF) * Protective Service Manual (Australian Government rules for cybersecurity) | ☐ ☐  ☐ ☐☐ | ☐ ☐  ☐ ☐☐ | ☐ ☐  ☐ ☐☐ | ☐ ☐  ☐ ☐☐ |
| * 1. Current and upcoming reforms in privacy legislation and how these could benefit each organisation have been investigated and explained. |  |  |  |  |
| * 1. Current and upcoming reforms in consumer and surveillance legislation and how these could benefit each organisation have been investigated and explained. |  |  |  |  |
| * 1. After completing the review of the two organisations in the preceding tasks, write the recommendations you would make as the Cyber Analyst/Consultant for each organisation, regarding:   2. Compliance with legislation and regulatory requirements   3. International cyber security legislation impacting their businesses   4. Potential impact of upcoming reforms in privacy and consumer and surveillance legislation | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| **ORGANISATION 2** |  |  |  |  |
| * 1. Evidence that the scenario has been read by completing the following:  1. Overview of the sector of the scenario presented provided 2. Current Federal, State/Territory and sector-specific cyber security legislation that applies to the organisation provided   Table provided has been utilised. | ☐  ☐ | ☐  ☐ | ☐  ☐ | ☐  ☐ |
| 1.2 Business operations analysis completed:  a) International cyber security legislation that has an impact on their data security has been identified  b) Areas of the business affected by the international legislation identified  c) The impact on the business operation and data security identified | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| 1.3 At least one (1) interdependency between different legislative instruments related to cyber security have been identified and explained. |  |  |  |  |
| 1.4 One (1) instance where a regulator can contribute to the security of business data operations has been identified. Impact of the contribution clarified. |  |  |  |  |
| 1.5 Already completed above. This task covers both organisations. |  |  |  |  |
| 1.6 Current and upcoming reforms in privacy legislation and how these could benefit each organisation have been investigated and explained. |  |  |  |  |
| * 1. Current and upcoming reforms in consumer and surveillance legislation and how these could benefit each organisation have been investigated and explained. |  |  |  |  |
| * 1. After completing the review of the two organisations in the preceding tasks, write the recommendations you would make as the Cyber Analyst/Consultant for each organisation, regarding:   2. Compliance with legislation and regulatory requirements   3. International cyber security legislation impacting their businesses   4. Potential impact of upcoming reforms in privacy and consumer and surveillance legislation | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| **PART 2 – Examine organisations’ policies and procedures compliance** |  |  |  |  |
| **ORGANISATION 1** |  |  |  |  |
| 2.1 Privacy policy has been examined, and the following has been addressed:   1. Policy 2. Standards 3. Review 4. Compliance | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ |
| 2.2 Access the Organisational Practices from the documentation provided and select two (2) practices that could be improved.  a) Evaluate each practice and identify their shortcomings  b) Propose improvements for each practice selected. | ☐ ☐ | ☐ ☐ | ☐ ☐ | ☐ ☐ |
| 2.3 After examining the organisation’s privacy policies and practices, write a report including your findings and a set of recommendations for the organisation, regarding:  a) The level of compliance with current privacy legislation and required improvements  b) Adequacy of current practices and required improvements | ☐  ☐ | ☐  ☐ | ☐  ☐ | ☐  ☐ |
| **ORGANISATION 2** |  |  |  |  |
| 2.1 Privacy policy has been examined, and the following has been addressed:   1. Policy 2. Standards 3. Review 4. Compliance | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ | ☐ ☐  ☐ ☐ |
| 2.2 Access the Organisational Practices from the documentation provided and select two (2) practices that could be improved.  a) Evaluate each practice and identify their shortcomings  b) Propose improvements for each practice selected. | ☐ ☐ | ☐ ☐ | ☐ ☐ | ☐ ☐ |
| 2.3 After examining the organisation’s privacy policies and practices, write a report including your findings and a set of recommendations for the organisation, regarding:  a) The level of compliance with current privacy legislation and required improvements  b) Adequacy of current practices and required improvements | ☐  ☐ | ☐  ☐ | ☐  ☐ | ☐  ☐ |
| **PART 3 – Review the organisations’ ethical practices and procedures** |  |  |  |  |
| **ORGANISATION 1** |  |  |  |  |
| 3.1 Four (4) red team tools the organisation that could use to exploit and compromise blue team defences have been identified and described. |  |  |  |  |
| 3.2 Four (4) blue team tools the organisation could use to protect the network from cyber-attacks have been identified and described. |  |  |  |  |
| 3.3 A set of ethical practices employees can apply when using red and blue team tools in public networks have been outlined. |  |  |  |  |
| 3.4 Consequences of unethical behaviour:   1. Outline the legal consequences of misusing skills gained using red and blue team tools and the potential data breaches that can occur when using these skills unauthorised. 2. The consequences of unauthorised access to network devices have been identified. 3. The consequences of bypassing copyright media and applications obtained via file sharing or downloading have been outlined. | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| 3.5 A minimum of four (4) examples of unethical behaviour that could happen in the organisations by the hand of cyber security technicians have been identified. For each example, explain the impact on the overall network and data security | ☐ | ☐ | ☐ | ☐ |
| **ORGANISATION 2** |  |  |  |  |
| 3.1 Four (4) red team tools the organisation that could use to exploit and compromise blue team defences have been identified and described. |  |  |  |  |
| 3.2 Four (4) blue team tools the organisation could use to protect the network from cyber-attacks have been identified and described. |  |  |  |  |
| 3.3 A set of ethical practices employees can apply when using red and blue team tools in public networks have been outlined. |  |  |  |  |
| 3.4 Consequences of unethical behaviour:   1. Outline the legal consequences of misusing skills gained using red and blue team tools and the potential data breaches that can occur when using these skills unauthorised. 2. The consequences of unauthorised access to network devices have been identified. 3. The consequences of bypassing copyright media and applications obtained via file sharing or downloading have been outlined. | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ | ☐  ☐ ☐ |
| 3.5 A minimum of four (4) examples of unethical behaviour that could happen in the organisations by the hand of cyber security technicians have been identified. For each example, explain the impact on the overall network and data security | ☐ | ☐ | ☐ | ☐ |
| **ONE ORGANISATION ONLY** |  |  |  |  |
| 3.6 Ethics Code Practice  An Ethics Code of Practice has been written for one of the two organisations presented. The policy applies to the organisation’s cyber security technicians. Distribution and implementation of the code have been outlined. |  |  |  |  |
| 3.7 Three (3) downloading file-sharing services have been identified. For each service, identified outline its suitability and the security risks associated with. |  |  |  |  |
| **PART 4 – Contingency task** |  |  |  |  |
| 4.1 Assume that due to staff shortages, two junior cyber security technicians have been assigned responsibilities above their expertise level. They are happy with the new job but concerned about their new responsibilities. Provide at least three (3) support measures that could be used to ease their role transition.  At least three appropriate support measures have been provided. |  |  |  |  |
| **End of Marking Criteria** | | | | |