**STUDENT – KNOWLEDGE ASSESSMENT TASK**

|  |  |  |  |
| --- | --- | --- | --- |
| Task Number | 1 of 3 | Task Name | Short answer questions |
| National unit/s code | VU23219 | National unit/s title | Manage the security infrastructure for the organisation |
| **National qualification code** | 22603VIC | **National qualification title** | Certificate IV in Cyber Security |
| RMIT Program code | C4424 | RMIT Course code | INTE5064 |

Section A – **Assessment Information**

|  |  |
| --- | --- |
| **Assessment duration and/or due date** | Due by the end of week 11. |
| **Task instructions** | |
| **Summary and Purpose of Assessment**  The purpose of this assessment task is for you to demonstrate knowledge on cyber hygiene processes, maintenance requirements, security methods and tools.  **Assessment instructions**   * Read and complete all 10 questions. * Seek assistance from your teacher if you need clarification with any of the questions. * Complete all sections before handing in your assessment for marking. * Your assessment responses will be assessed as per the marking criteria outlined in Section B of this document.   **Where**  This assessment will take place in class and/or outside of class time, as per your teacher’s instructions.  **How**  Students will be assessed against the criteria listed in the marking guide in Section B of this task. To achieve a satisfactory result, students will need to address all criteria satisfactorily. | |
| **Conditions for assessment** | |
| * Make sure you confirm your understanding of this task with your Assessor before beginning. * All work must meet the criteria to the standard described in the marking guide in Section B to be deemed satisfactory in this assessment. * You must submit all assessment evidence as instructed. Your assessor will assess the documentation you provide. * Please make arrangements with your assessor at least one week prior to the assessment due date if you feel you require special allowance or allowable adjustment to this task * Student must be observed undertaking this assessment task by a qualified assessor. * As an assessor you can negotiate a suitable time and location for assessment at least one week prior to the assessment taking place * Student must complete the task within the maximum allowed duration as directed by the assessor. * This is an individual assessment task. Student will be assessed individually against all assessment criteria. * Student can decide with the assessor at least one week prior to the assessment due date if they require special allowance or allowable adjustment to this task. * Students found in breach of assessment conditions can be charged with academic misconduct, have their results cancelled, be excluded from the program and receive other penalties. Penalties can also apply if a student’s test material is copied by others. * Plagiarism is the presentation of the work, idea or creation of another person as though it is one’s own. It is a form of cheating and is a very serious academic offence that may lead to expulsion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited. * RMIT special consideration is to enable students to maintain students’ academic progress despite adverse circumstances. The process for special consideration can be found at <http://www.rmit.edu.au/students/specialconsideration> * Students with a disability or long-term medical or mental health condition can apply for adjustments to their study and assessment conditions (Reasonable Adjustments and Equitable Assessment Arrangements) by registering with the Equitable Learning Services (ELS) at <https://www.rmit.edu.au/students/support-and-facilities/student-support/equitable-learning-services>  If students already registered with ELS and students’ study plan is approved, please inform your teacher if this assessment task is not adjusted in line with approved study plan. * Please ensure students full and correct name is written on the student version of this assessment task (do not use nicknames or abbreviations). * Student can appeal the assessment decision according to the [RMIT Assessment Appeal Processes](https://www.rmit.edu.au/content/dam/rmit/documents/about/policy/assessment/assessment-processes.pdf) * You will have the opportunity to resubmit any tools that are deemed unsatisfactory (one resubmission allowed per unit, so that means you have two opportunities to submit) | |
| **Instructions on submitting students’ assessment** | |
| Students need to submit this assignment through CANVAS with the naming convention of: **<Student\_Number>\_<Student\_Full\_Name> \_SAQ.docx** | |
| **Equipment/resources students must supply (if applicable):** | **Equipment/resources to be provided by RMIT or the workplace (if applicable):** |
| * Computer or Laptop * Internet access * Learning Resources/Software * Pen and paper | * RMIT internet access * RMIT Computer Labs and Learning Resources/Software * Availability of Canvas to submit the knowledge assessment |

**Section B – Student Answer Sheet**

|  |
| --- |
| **Q1: The NIST cybersecurity framework is a practical approach to managing cyber security risks in the workplace.** |
| **Outline how you would apply each NIST framework category, as shown below:**   * **Identify:** Identify potential entry points for viruses/malware/trojans, prioritize security controls to reduce risk. For example, patch management controls to keep applications up-to-date and secure. * **Protect:** Implement security controls such as access controls, firewalls, antivirus software, and intrusion prevention systems to reduce the likelihood of infection. * **Detect:** Monitor systems and networks for potential threats using security monitoring, event management tools, and regular security audits/vulnerability assessments to detect viruses/malware/trojans early and minimize impact of infection. * **Respond:** Act in response to a cybersecurity incident by isolating infected systems, removing viruses/malware/trojans, and conducting forensic investigations to determine the cause of the infection. Implement incident response plans to ensure a rapid and coordinated response. * **Recover:** Restore systems and data after a cybersecurity incident by restoring from backups, rebuilding infected systems, and implementing additional security controls to prevent similar incidents in the future. Implement strong recovery measures to minimize the impact of viruses/malware/trojans and return to normal operations as quickly as possible. |

|  |
| --- |
| **Q2: List three (3) methods in which cyber security attacks can occur and explain the impact these attacks can have.** |
| 1. Phishing Attacks: is a social engineering attack where the attacker tricks the victim into clicking a link or opening an attachment in a seemingly legitimate email or message. It can result in malware installation or the victim revealing sensitive information, such as passwords. A successful phishing attack can have severe consequences, including identity theft, financial loss, and compromised business data. 2. Malware Attacks: Malware attacks occur when malicious software is installed on a victim's device without their knowledge or consent. Malware can include viruses, trojans, ransomware, or spyware, and it can be used to steal sensitive information or to take control of a victim's device. The consequences of a malware attack can be severe, potentially leading to data loss, financial damage, and reputation harm. 3. Denial of Service (DoS) Attacks: DoS attacks are a type of attack that flood a website (or server), with traffic, making it inaccessible to legitimate users. These attacks can be carried out by a single attacker or by a group of attackers, and they can be used to disrupt online services or to extort money from victims. A successful DoS attack can cause significant consequences including loss of revenue, low productivity, and damage to an organization's reputation. |
| **Q3: List three (3) methods that are used to protect an organization’s data.** |
| 1. Access controls: Access controls are used to limit access to sensitive data to authorized personnel only. This can include measures such as password-protected accounts, two-factor authentication, and role-based access control. By controlling who can access data and what they can do with it, an organization can significantly reduce the risk of data breaches and unauthorized access. 2. Encryption: Encryption is a process of converting data into a code that can only be deciphered by someone who has the appropriate key. This method can be used to protect sensitive data at rest or in transit, making it unreadable to anyone who does not have the encryption key. This can help prevent data theft and unauthorized access, even if data is stolen or intercepted. 3. Regular data backups: Regular data backups are an important method for protecting data in case of data loss or corruption. By regularly backing up data to a secure location, an organization can ensure that it can recover data in case of a security incident or disaster. Additionally, regular backups can help detect data breaches or unauthorized access, allowing an organization to take steps to prevent further damage. |

|  |
| --- |
| **Q4: List three (3) tools used to protect an organization’s data.** |
| 1. Antivirus software: Antivirus software is a tool that is designed to detect and remove malware from an organization's computer systems. Antivirus software scans files, email attachments, and downloads to identify potential threats and can help prevent malware infections that can lead to data breaches or other security incidents. 2. Firewalls: Firewalls are network security tools that can be used to monitor and control network traffic between an organization's computer systems and the internet. Firewalls can help prevent unauthorized access, malware infections, and other security incidents by blocking or filtering network traffic that does not meet certain criteria. 3. Data loss prevention (DLP) software: DLP software is a tool that can be used to prevent data loss or unauthorized data access. DLP software can monitor data usage patterns, detect unusual activity, and prevent unauthorized data access or transmission. DLP software can help prevent data breaches, ensure compliance with data privacy regulations, and protect sensitive data from being leaked or stolen. |
| **Q5: List two (2) cyber hygiene processes and outline the requirements for each.** |
| 1. Password management:  * Use strong and unique passwords for each account and change them regularly (every 90 days or less). * Do not use the same password for multiple accounts. * Use multi-factor authentication (MFA) wherever possible, especially for high-risk accounts. * Avoid sharing passwords with others or writing them down in easily accessible locations.  1. Software patching:  * Regularly update and patch software and operating systems to fix known vulnerabilities. * Prioritize critical security updates and patches, especially for high-risk systems and applications. * Establish a process for testing and deploying patches to ensure they do not disrupt normal operations. * Maintain an inventory of all hardware and software assets and keep track of patching status and requirements. |

|  |
| --- |
| **Q6: Outline three (3) maintenance procedures used to protect the security of an organization.** |
| 1. Regular software updates: One of the most important maintenance procedures for protecting an organization's security is to keep all software and systems up-to-date. This includes operating systems, applications, and security software. Regular updates can patch vulnerabilities and fix security flaws, reducing the risk of a security breach. 2. Backup and recovery procedures: Another important maintenance procedure is to regularly back up important data and systems to prevent data loss in the event of a security incident. This includes setting up automated backups, testing backup and recovery procedures, and keeping backup data in a secure location. 3. Security audits and assessments: Regular security audits and assessments can help identify potential vulnerabilities and areas for improvement in an organization's security posture. This includes reviewing access controls, network configurations, and security policies and procedures. By conducting regular assessments, organizations can proactively identify and address potential security risks before they are exploited. |
| **Q7: Provide two (2) examples of malware scanners and list two (2) features of each scanner.** |
| 1. Malwarebytes Anti-Malware: a popular malware scanner that detects and removes malware, spyware, and adware from your system. It is known for its ease of use, speed, and effectiveness in removing malware. 2. Norton Antivirus: is a well-known antivirus software that scans and removes viruses, spyware, and other malware. It provides real-time protection against new threats and is known for its fast-scanning speed and easy-to-use interface.  |  |  | | --- | --- | | Antivirus Software: | Features: | | Malwarebytes  Anti-Malware | Real-time protection that detects and blocks malware as it tries to enter your system. Customizable scanning options that allow you to choose specific files or folders to scan. | | Norton Antivirus | Automatic updates that keep your virus definitions up to date. Customizable scanning options that allow you to choose specific files or folders to scan. | |

|  |
| --- |
| **Q8: Provide two (2) examples of virus scanners and list two (2) features of each scanner.** |
| 1. McAfee VirusScan is a well-known antivirus software that detects and removes viruses, spyware, and other malware from your system. It provides real-time protection against new threats and is known for its fast-scanning speed and ease-of-use. 2. Avast Antivirus is a popular antivirus software that uses advanced threat detection technologies to protect against viruses, spyware, and other malware. It also provides real-time protection and customizable scanning options and is known for its user-friendly interface.  |  |  | | --- | --- | | Antivirus Software | Features | | McAfee VirusScan | Real-time protection that detects and blocks viruses and malware in real-time. Customizable scanning options that allow you to choose specific files or folders to scan. | | Avast Antivirus | Advanced threat detection that uses artificial intelligence to detect and block sophisticated threats. Customizable scanning options that allow you to choose specific files or folders to scan. | |
| **Q9: What are the benefits of using MS baseline security analyzer?** |
| 1. Identify security vulnerabilities: MBSA scans your systems and identifies potential security vulnerabilities, such as missing security updates, weak passwords, and open network ports. By identifying these vulnerabilities, you can take steps to mitigate the risks and improve your overall security posture. 2. Simplify security management: MBSA provides a centralized interface for managing security across multiple systems. This allows you to identify security issues and track remediation efforts quickly and easily. 3. Save time and resources: MBSA automates many of the security management tasks that would otherwise require manual effort, such as scanning for missing security updates and checking password policies. This can save time and resources, while ensuring that your systems remain secure. 4. Provide actionable recommendations: MBSA provides actionable recommendations for addressing security vulnerabilities, such as installing security updates or changing password policies. This makes it easier to prioritize remediation efforts and ensure that your systems remain secure. |

|  |
| --- |
| **Q10: What are the benefits of using MS security compliance manager?** |
| 1. Streamlined security management provides a centralized interface for managing security across multiple systems. This allows you to define and deploy security baselines, monitor compliance, and track remediation efforts quickly and easily. 2. Customizable security baselines provides a set of pre-defined security baselines that are based on industry best practices, such as the Center for Internet Security (CIS) benchmarks. These baselines can be customized to meet your specific security requirements and deployed across your organization. 3. Improved security posture: by defining and deploying security baselines, organizations can improve their security posture and reduce the risk of security breaches. 4. Compliance reporting: Built-in reporting capabilities that allow you to generate compliance reports, such as CIS benchmark scorecards, to track your organization's compliance with security baselines. 5. Simplified regulatory compliance: SCM can help organizations comply with regulatory requirements, such as HIPAA and PCI DSS, by providing pre-defined security baselines that address specific regulatory requirements.  Easy way to memorize:  |  |  | | --- | --- | | Feature | Description | | Security management | * Provides a centralized interface for managing security across multiple systems. * Allows you to define and deploy security baselines, monitor compliance, and track remediation efforts quickly and easily. | | Security baselines | * Provides a set of pre-defined security baselines based on industry standards that can be customized to fit your specific needs and applied across your organization. | | Security posture | * Organizations can improve their overall security and reduce the risk of security breaches. | | Compliance reporting | * Built-in reporting tools that help monitor compliance with security baselines, making it easier to identify areas for improvement. | | Regulatory compliance | * Can help organizations meet regulatory requirements like HIPAA and PCI DSS by providing pre-made security baselines that comply with those regulations. | |

Section C – **Marking Guide**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task 1: Knowledge assessment | Actions to be observed (performance) *Minimum requirements to be met: Tick each checkbox when action is observed* | | S | NYS |
| **Short answer questions** | Questions demonstrated sufficient knowledge (Questions 1 – 10) | | ☐ | ☐ |
| Give feedback as required to ensure the students’ understanding of the topics are consolidated and/or reviewed | | * For detailed explanation of each question, refer the Rubric. * The feedback is given through rubric as required to ensure students understanding of the topics are consolidated and/or reviewed.   You will get a score of **satisfactory** for the answers demonstrated sufficient knowledge (Questions 1 – 10) | | |

Section C **– Feedback to Student**

|  |  |  |  |
| --- | --- | --- | --- |
| **Has the student successfully completed the task?** | | Yes No | |
|  | |  |  |
| **Feedback to student:** | | | |
|  | | | |
| **Assessor Name:** | **Date:** | | |