ICTSAS530

Use network tools

Assessment 1 of 6

Short Answer Questions

Assessor Guide

SWINBURNE OPEN ED

Version 1

Assessment Instructions

Task Overview

This assessment task consists of 10 short answer questions. Read each question carefully before typing your response in the space provided.

Important: Before commencing your work, you must update your *Student name* and *Student number* in the footer from **page 2** onwards.

Additional Resources and Supporting Documents

To complete this assessment, you will need:

- Essential Eight Maturity Model (November 2022).pdf
- Network and security threat incident response process.pdf
- Security and software update management process.pdf

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the Learning Platform. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Read the following scenario and access the resources provided to answer Question 1.

Scenario: An organisation's IT infrastructure is located in NSW, Australia.

As part of maintaining the security of the organisation's network, the Network Administrator is required to conduct several physical tests on the network equipment. The equipment is located in the organisation's server room environment, which consists of live electrical equipment.

Resources: Refer to the relevant Work Health and Safety standards and work tasks by accessing the following:

- Safe Work Australia
- Information media and telecommunications | SafeWork NSW

Question 1

Outline the work health and safety (WHS) standards and legislative requirements that apply when conducting work tasks to maintain high-security networks according to the given scenario.

To support your answer provide references to specific sections in the relevant Act(s) and Regulation(s).

(Word count: 100-150 words)

Assessor instructions: Students must outline WHS standards and legislative requirements relating to work tasks.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Following are some of the essential WHS standards and legislative requirements that are governed by the **Work Health and Safety Act 2011** and the **Work Health and Safety Regulation 2017** that apply in NSW Australia.

- **Duty of Care (WHS Act section 19)** - Employers have a duty to ensure, so far as is reasonably practicable, the health and safety of their workers. This includes providing and maintaining a safe working environment when tasks involve maintaining high-security networks.
- **Ergonomics and Safe Work Practices (WHS Regulation Part 4):**

  Employers must consider ergonomic principles to minimise the risk of work-related injuries, especially when employees engage in tasks involving extended periods of using network tools for maintenance.
- **Electrical Safety (WHS Regulation Part 4.7):**

  Specific regulations address electrical safety, which is relevant when dealing with network hardware and equipment. Compliance with these regulations ensures the safe operation of electrical devices within the network infrastructure.

  Other answers may include:
- **Risk Management (WHS Act Section 32):**

  Employers must identify, assess, and control risks associated with network maintenance tasks. A risk management approach is crucial to address potential hazards related to cybersecurity threats and network vulnerabilities.

- **Consultation and Participation (WHS Act Section 47):**

  Employers must consult with workers and their representatives on matters related to health and safety, including the implementation of security measures. This involves seeking input from employees involved in maintaining high-security networks.

- **Training and Instruction (WHS Act Section 19):**

  Employers must provide information, training, and instruction to workers to ensure they can perform their work safely. Training programs should cover secure network maintenance practices, proper use of tools, and awareness of cybersecurity risks.

- **Control of Risks (WHS Regulation Part 3):**

  Employers are required to implement control measures to eliminate or minimise risks, which may include using secure configurations, encryption, and regularly updating security software in network tools.

- **Incident Notification (WHS Regulation Part 3.2):**

  Employers are obligated to report certain types of workplace incidents, including those resulting in serious harm, to the relevant authorities. This ensures that any workplace incidents related to network security are appropriately addressed.

Question 2

Outline three (3) examples of organisational policies that apply when conducting work tasks to maintain high-security networks and outline their relevance.

(Word count: 75-100 words)

Assessor instructions: Students must outline organisational policies and procedures relating to work tasks.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Information Security Policy:

- Clearly outlines the organisation's commitment to information security.
- Defines roles and responsibilities related to maintaining high-security networks.
- Establishes the framework for risk management and compliance.

Backup and Recovery Policy:

- Defines procedures for regular data backups and testing of recovery processes.
- Specifies storage locations, retention periods, and encryption practices for backups.
- Ensures the organisation's ability to restore operations in the event of a security incident.

Acceptable Use Policy:

- Defines acceptable and unacceptable behaviours related to the use of network resources.
- Outlines consequences for policy violations.
- Ensures employees are aware of their responsibilities in maintaining network security.

Other answers may include:

Access Control Policy:

- Defines procedures for granting, modifying, and revoking access to network resources.
- Enforces the principle of least privilege to limit access based on job responsibilities.
- Requires strong authentication mechanisms, such as multi-factor authentication.

Incident Response and Management Policy:

- Establishes procedures for identifying, reporting, and responding to security incidents.
- Defines roles and responsibilities during incident response activities.
- Outlines the process for post-incident analysis and improvement.

Security Awareness and Training Policy:

- Requires ongoing education for employees regarding security best practices.
- Outlines procedures for conducting security awareness programs.
- Encourages reporting of security concerns or incidents by employees.

Read the following scenario and access the resources provided to answer Questions 3 to 5.

Scenario: An organisation wants to implement 'Maturity Level 3' for their network according to the 'Essential Eight Maturity Model'.

Refer to the *Australian Signals Directorate* by accessing:

- the cyber.gov.au official website at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- the 'Essential Eight Maturity Model' PDF document (Long URL: https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202022%29.pdf)

Note: A copy of this PDF version is provided to you as an additional resource.

Question 3

Outline the key organisational processes and requirements for conducting back up and restore operations according to the given scenario.

(Word count: 95-120 words)

Assessor instructions: Students must outline organisational processes and requirements for backing up and restoring operations.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Backups of data, applications and settings are:

- performed and retained in accordance with business criticality and business continuity requirements

- synchronised to enable restoration to a common point in time
- retained in a secure and resilient manner

Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.

Unprivileged accounts:

- cannot access backups belonging to other accounts
- cannot access their own backups
- are prevented from modifying and deleting backups

Privileged accounts (excluding backup administrator accounts):

- cannot access backups belonging to other accounts
- cannot access their own backups
- are prevented from modifying and deleting backups

Backup administrator accounts are prevented from modifying and deleting backups during their retention period.

Question 4

Outline the key organisational processes and requirements for updating settings of online services, applications and operating systems according to the given scenario.

(Word count: 95-120 words)

Assessor instructions: Students must outline organisational processes and requirements for updating settings

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

To identify missing patches or updates for vulnerabilities, a vulnerability scanner is used at least:

- daily - in operating systems of internet-facing servers and internet-facing network devices.
- fortnightly - in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.

Patches, updates or other vendor mitigations for vulnerabilities in online services, applications (e.g. office productivity suites, web browsers and their extensions, email clients, PDF software and security products) and operating systems (e.g. internet-facing servers and network devices) are applied:

- within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
- within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Other answers may include:

- Using an automated method of asset discovery at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

- A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
- PowerShell settings should be configured to use 'Constrained Language Mode'.
- The security settings of the following cannot be changed by users:
    - Office productivity suite
    - Web browser
    - Microsoft Office macro
    - PDF software

Question 5

Outline the key organisational requirements for raising cybersecurity threats and incidents to supervisory personnel according to the given scenario.

(Word count: 50-85 words)

Assessor instructions: Students must outline organisational processes and requirements raising threats and alerts to supervisory personnel

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

According to the requirements for implementing maturity level 3 of the Essential Eight Maturity Model:

Cyber security incidents should be reported to:

- the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
- the Australian Signals Directorate (ASD) as soon as possible after they occur or are discovered.

Following the identification of a cyber security incident, the cyber security incident response plan is enacted.

Read the following scenario and access the resources provided to answer Question 6.

Scenario:

Late in the evening, the network monitoring tools of a medium-sized financial institution detect unusual activity indicating a potential security threat. Anomalies include multiple failed login attempts on critical servers and an unexpected surge in data transfer. The network security tools promptly generate alerts. As the IT administrator on duty, you are responsible for handling this situation.

Resources: Refer to the organisation's incident reporting process as outlined in the 'Network and security threat incident response process.pdf' document.

Question 6

Assessor instructions: When answering the following sub-questions, students must demonstrate their understanding of the organisational processes and requirements involved when raising threats and alerts to supervisory personnel.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

a. What immediate steps would you take to address the potential security threat?
(Word count: 75-100 words)

A sample answer is provided below.

Step 1 - Isolate and investigate:

- Isolate the affected servers of systems to contain the potential threat
- Investigate the nature of the anomalies, analysing logs and network traffic to determine the source and intent of the suspicious activity.

Step 2 – Notify the IT security team and other relevant technical staff to assist in the investigation and response.

Step 3 – Escalate the situation to the supervisory personnel

Step 4 – Communicate: Maintain clear and timely communication with supervisory personnel. Update them on the progress of the investigation and on any actions taken.

b. Identify two (2) supervisory personnel to whom you would escalate this situation and the type of information you would provide/request.

(Word count: 45-65 words)

A sample answer is provided below.

IT Security Manager/Director: Inform them of the incident, providing initial findings and the current status. Request their guidance on the appropriate course of action.

Network Security Manager: Specifically inform this individual about the unusual network activity. Collaborate on measures to mitigate and prevent the further spread of the threat.

Read the following scenario and access the resources provided to answer Question 7.

Scenario: In a large financial institution, the IT Security Manager receives a notification about a critical security vulnerability affecting the organisation's financial management software. Additionally, the software vendor releases an important update with security patches. As the IT administrator, you are responsible for handling this situation.

Resources: Refer to the organisation's incident reporting process as outlined in the 'Security and software update management process.pdf' document.

Question 7

Outline five (5) key organisational processes and requirements for reporting security and software updates according to the incident in the scenario.

(Word count: 85-120 words)

Assessor instructions: Students must outline organisational processes and requirements for reporting security and software updates.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

1. Conduct a thorough vulnerability assessment to understand the nature and severity of the security vulnerability affecting the financial management software.
2. Engage the organisation's patch management process to prioritise and deploy the security patches released by the software vendor.
3. Utilise established communication channels to notify relevant stakeholders, including IT teams and affected business units, about the security vulnerability and the impending software update.
4. Integrate the software update into the organisation's change management process, ensuring proper testing procedures are followed to minimise disruptions.
5. Implement a targeted user awareness campaign to inform employees about the importance of promptly updating their financial management software for enhanced security.

Other answers may include:

- Ensure strict adherence to regulatory requirements and industry standards governing security updates, documenting each step of the process for compliance purposes.
- Implement continuous monitoring and auditing mechanisms to track the status of the security update, ensuring that all systems are brought up to date.

Read the following scenario and access the resources provided to answer Question 8 and 9.

Scenario: As the network administrator of a financial institution, you are tasked with enhancing the documentation and recommending the use of network tools to maintain a high-security network. You are also considering the need for clear policies, procedural guides, diagrams, and incident response plans.

Question 8

Outline the organisational formats for documentation related to utilising network tools according to the scenario.

(Word count: 50-85 words)

Assessor instructions: Students must outline organisational formats for documentation and recommendations.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

- Policy Documentation:

  Develop a comprehensive security policy outlining acceptable network practices, access controls, and incident response procedures. Clearly communicate these policies to all staff members.

- Procedural Guides:

  Create detailed procedural guides for configuring and maintaining network security tools. Include step-by-step instructions for implementing updates, conducting audits, and addressing common security concerns.

- Network Architecture Diagrams:

  Develop clear and updated network architecture diagrams. Highlight the placement and functionality of key security tools, aiding both IT personnel and other stakeholders in understanding the network's security posture.

Other answers may include:

- Tool Configuration Manuals:

  Document specific configurations and best practices for each security tool in use. Include information on setting up alerts, thresholds, and integration with other security measures.

- Incident Response Plans:

  Establish and document incident response plans. Clearly outline roles, responsibilities, and escalation procedures in the event of a security incident. Regularly review and update these plans to align with emerging threats.

Question 9

Outline specific recommendations related to utilising network tools according to the scenario.

(Word count: 50- 85 words)

Assessor instructions: Students must outline organisational formats for documentation and recommendations.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

- Regular Audits:

  Implement regular network audits using tools like Nessus or Qualys. Schedule automated scans to identify vulnerabilities and ensure the continuous resilience of the network.

- Employee Training:

  Conduct thorough training sessions for IT staff on the proper use of security tools. Emphasise the importance of staying updated with tool functionalities and industry best practices.

- Documentation Review:

  Establish a periodic review process for all documentation related to network security. Ensure that policies, procedural guides, and tool configurations are up-to-date with the latest security standards and organisational requirements.

Other answers may include:

- Collaborative Communication:

Facilitate open communication channels between IT teams. Document channels for reporting and responding to security incidents promptly and collaboratively.

- Continuous Monitoring:

  Emphasise the need for continuous monitoring using tools like Snort or Wireshark. Detect and respond promptly to emerging threats, ensuring the network's security posture remains robust.

Question 10

Outline the functions and features of security guidelines for using network tools when maintaining high-security networks.

[Approximate word count: 45 - 75 words]

Assessor instructions: Students must demonstrate their understanding of the functions and features of security guidelines.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Functions of security guidelines include prescribing best practices for tool selection, configuration, and operation to safeguard against threats.

They define access controls, encryption standards, and authentication methods, ensuring confidentiality, integrity, and availability.

Comprehensive guidelines aid in threat detection, incident response, and vulnerability management.

Features encompass clear instructions on firewall rule sets, intrusion detection parameters, and secure VPN configurations. Regular updates and testing protocols validate the tools' efficacy, promoting a proactive approach to mitigating evolving cyber threats and fostering a secure network environment.

Security guidelines also feature clear access controls, encryption protocols, incident response plans, and compliance frameworks, providing a structured approach to maintaining robust cybersecurity measures.

Assessment submission checklist

Students must have completed all questions within this assessment before submitting. This includes:

1	10 short answer questions completed in the spaces provided.	☐

Assessment feedback

Assessors are to indicate the assessment outcome as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S	☐ NYS

Congratulations, you have reached the end of Assessment 1!