Qualification title: Level 3 Advanced Technical Extended Diploma in Digital Technologies (5220-32)

Test title: Level 3 Digital Technologies (Cyber Security) – Theory exam (2) – Sample marking scheme

Base mark: 80

1

State **two** internal threats to an organisation’s network.

Answer

One mark each for any of the following, to a maximum of 2 marks:

- Organisational culture **(1)**
  - Complacency
  - lack of effective control
- Organisational climate **(1)**
- Disgruntled employees **(1)**
- Industrial espionage **(1)**
- Misplaced trust **(1)**
- Malpractice **(1)**
- Incompetence **(1)**
- Untrained staff **(1)**
- Fraud **(1)**
- Theft **(1)**
- Criminal Damage **(1)**

Test spec reference: 336 – 1.1	**Total marks:** 2

2

Explain **each** of the following Social Attack Vectors that can be used to gain access to sensitive information.

- Spear Phishing.
- Catfishing.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Spear Phishing: is where a malicious actor pretends to be someone trusted by the email recipient **(1)** in order to induce the recipient into revealing confidential information **(1)**.

- Catfishing: is where a malicious actor creates a fake identity on social media **(1)** to target a specific individual for some form of deception **(1)**.

Test spec reference: 336 – 2.4	**Total marks:** 4

3

State **two** threats to a business where Disaster Recovery can be used to reduce the impact.

Answer

One mark each for any of the following, to a maximum of 2 marks:

- Environmental **(1)**
  - fire
  - flood
  - earthquake
  - tornado
- Infrastructure **(1)**
  - power
  - transport
  - communications
- Political **(1)**
  - civil disturbance
  - general strike
- Criminal **(1)**
  - terrorism
  - theft
  - arson
- Software bugs **(1)**
- Hardware failure **(1)**
- Administrative error **(1)**

Test spec reference: 337 – 1.2	**Total marks:** 2

4

Explain one impact of an Information Systems (IS) outage on the Business Continuity for **each** of the following.

- Clients.
- Business.
- Suppliers.

Answer
Two marks each for any of the following, to a maximum of 6 marks:

- Clients: may feel a loss of confidence in the business **(1)** leading to a long term loss of trust in their ability to perform **(1)**.

- Business: may suffer a loss of revenue **(1)** which may affect the profitability of the organisation **(1)**.

- Suppliers: whilst they are unable to deliver the goods to the affected business **(1)** the goods being held, may spoil over time **(1)**.

Test spec reference: 337 – 1.1	**Total marks:** 6

5

Explain **each** of the following elements of a plan used to protect a mission critical Information System, from an unplanned outage.

- Identification of critical data.
- Administrative requirements.

Answer
Two marks each for any of the following, to a maximum of 4 marks:

- Identification of critical data:
  all data that is vital to the successful operation of the organisation **(1)** should be copied to the High Availability solution **(1)** in case of system failure.

- Administrative requirements:
  all user accounts should be synchronised to the HA solution **(1)** in order to maintain availability of service **(1)** if the primary system fails.

Test spec reference: 337 – 2.1	**Total marks:** 4

6

State **four** organisations that develop and maintain standards related to Information Systems (IS) Governance.

Answer

One mark each for any of the following, to a maximum of 4 marks:

- ISO **(1)**
- COBIT **(1)**
  - Common Objectives for Information and Related Technology
- NIST **(1)**
  - National Institute of Standards and Technology
- ITIL IT **(1)**
  - Infrastructure Library
- IISP **(1)**
  - Competency model for IS professionals

Test spec reference: 338 – 1.3	**Total marks:** 4

7

Explain **each** of the following concepts related to Information Security.

- Confidentiality.
- Integrity.
- Availability.

Answer

Two marks each for any of the following, to a maximum of 6 marks:

- Confidentiality: protecting information from being accessed **(1)** by anyone that doesn't have authorisation **(1)**.

- Integrity: ensuring that information remains unaltered **(1)** when being transmitted from one place to another **(1)**.

- Availability: ensuring that information is accessible **(1)** for authorised business use **(1)**.

Test spec reference: 338 – 1.4	**Total marks:** 6

8

Explain **each** of the following responses to risks that can be adopted by organisations.

- Avoidance.
- Transfer.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Avoidance: alter the direction of a project **(1)** to eliminate the possibility of the risk occurring **(1)**.
- Transfer: where the risk is contractually assigned to a 3rd party **(1)** to minimise the impact on the organisation **(1)**.

Test spec reference: 338 – 3.1	**Total marks:** 4

9

State **four** processes that can be carried out when vetting an Ethical Hacker.

Answer

One mark each for any of the following, to a maximum of 4 marks:

- Interviews **(1)**
- References **(1)**
- Background checks **(1)**
  - qualifications
  - employment
  - residence
- Professional memberships **(1)**
- Professional qualification **(1)**
  - Certified Ethical Hacker
  - CREST
  - SANS
  - CLAS
- Security Vetting **(1)**
- Government vetting **(1)**
  - Baseline Personnel Security Standard (BPSS)
  - Security Clearance
  - Counter Terrorism Check
  - Disbarring and Vetting Service

Test spec reference: 339 – 1.2	**Total marks:** 4

10

Explain the purpose of **each** of the following hacking techniques when used by an Ethical hacker.

- Binoculars.
- Bluetooth scanners.
- Dumpster Diving.

Answer

Two marks each for any of the following, to a maximum of 6 marks:

- Binoculars: are used to 'shoulder surf' from a distance **(1)** allowing the hacker to observe login details **(1)** entered via the keyboard.
- Bluetooth scanners: are used to identify all Bluetooth devices within range **(1)** along with the presence / absence of any security controls **(1)**.
- Dumpster Diving: is used to look for discarded password information **(1)** by searching through large waste receptacles (Skips) **(1)**.

Test spec reference: 339 – 2.1	**Total marks:** 6

11

Explain **each** of the following encryption concepts when used in a business environment.

- Digital signatures.
- Hashing.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Digital signatures: secure data by using a digital code generated using public key encryption **(1)** which is attached to an electronically transmitted document verifying the sender's identity **(1)**.
- Hashing: ensures data integrity **(1)** by using an algorithm to convert plain text into a numerical value **(1)** which can be used to identify changes to data.

Test spec reference: 340 – 1.1	**Total marks:** 4

12

Explain **each** of the following Attack Vectors.

- Boomerang.
- Man-in-the-middle.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Boomerang: is a highly complex mathematical attack **(1)** that uses differential analysis to break a cypher **(1)**.
- Man-in-the-middle: when communication between two systems is intercepted **(1)** allowing the alteration of the data **(1)** to benefit the interceptor.

Test spec reference: 340 – 3.1	**Total marks:** 4

13

Identify **four** types of Administrative Access Control that can be used on a network.

Answer

One mark each for any of the following, to a maximum of 4 marks:

- Policies **(1)**
- Procedures **(1)**
- Security clearances **(1)**
    - Counter Terrorism Check
- Identity validation **(1)**
    - passport
- Staff Training **(1)**
- Support **(1)**
- Helpdesk **(1)**

Test spec reference: 341 – 1.3	**Total marks:** 4

14

Explain **each** of the following principles of Access Control.

- Least Privilege.
- Defence in Depth.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Least Privilege: is the practice of limiting user access to a system **(1)** to the absolute minimum needed to perform their role **(1)**.
- Defence in Depth: is where multiple layers of security protect valuable information **(1)** and if one layer fails the next layer steps in to protect the information **(1)**.

Test spec reference: 341 – 1.1	**Total marks:** 4

15

Explain **each** of the following internal threats to Access Control in an organisation.

- Organisational Culture.
- Disgruntled employees.

Answer

Two marks each for any of the following, to a maximum of 4 marks:

- Organisational Culture: where the employees are complacent about accessing the system **(1)** and may not log off when leaving a workstation **(1)** for a short time.
- Disgruntled employees: where a malcontent employee tries to gain 'revenge' on the organisation **(1)** by deliberately breaking security protocols **(1)** and leaving the system open to attack.

Test spec reference: 341 – 3.2	**Total marks:** 4

16

You are an Infrastructure Technician specialising in network security that has been seconded to a multi-national charity.

You have been tasked with reporting on how the charity can improve the resilience of their local systems in parts of the world that are prone to earthquakes and other natural disasters.

Discuss the technologies and considerations involved in meeting this requirement.

Answer

Indicative content:

A candidate's discussion may include consideration of:

- Planning
    - Tools
        - Logical tools
        - Physical tools
    - Policies
    - Procedures
- Hardware
    - UPS
    - Firewalls
    - Software
    - Operating System
    - Applications
    - Protocols
    - ACLs
    - Anti-virus
    - Ports
- Skill requirements
    - Staff training
- Data requirements
- Backup
- HA Systems
- Security
    - Threats
    - Vulnerabilities
    - Risks
    - Data
    - Countermeasures
    - Cloud Services
- Maintenance
    - Security
    - Accounts
    - Fault log
    - Data backup
    - Data restoration

0 marks

No awardable material.

Band 1: 1 – 3 marks

The response demonstrates a limited understanding of the relevant threats and solutions involved and is mostly a statement of facts which are not developed or supported. The approach to the task is inconsistent. Statements may be inaccurate, and the use of precise technical language is sparse.

Band 2: 4 – 6 marks
The candidate has produced a discussion that expands on the factual knowledge but lacks detail in some areas.
They show an adequate understanding of the relevant threats and solutions involved including some reasons for their inclusion.
They have provided some valid reasons to support their choices which are structured and presented in a logical order.

Band 3: 7 – 9 marks
The candidate has shown a thorough understanding of the relevant threats and solutions involved.
They have covered these in a logical order, including reasons behind the processes and solutions, the factors that need to be considered and the impact these factors may have on the implementation.

Test spec reference: Unit 336 Unit 337, Unit 338, Unit 339, Unit 340, Unit 341	**Total marks:** 9

17

You have been employed as a Network Technician in a private hospital that has recently experienced a security breach.

This happened when a patient discovered a username and password combination on a post-it note; and used it to log into the system. There is a suspicion that they may have downloaded unauthorised software onto the system.

The hospital has requested that you conduct a security audit and advise on any necessary mitigation required.

Discuss how you would conduct the security audit and the mitigations you would advise.

Answer

Indicative content:

A candidate's discussion may include consideration of:

- Planning
  - Tools
    - Logical tools
    - Physical tools
  - Methodologies
  - Legislation
  - Regulations
  - Compliance
  - Skill requirements
    - Encryption
    - Decryption
    - Hashing
    - VPN
    - Digital Signatures
    - Cloud Services
    - Peer-to-peer networks
    - Client server networks
  - Security
    - Threats
    - Vulnerabilities
    - Risks
    - Data
    - Countermeasures
  - Hardware
  - Software
  - Testing
    - Test plan
- Maintenance
  - Security
  - User support
  - Accounts
  - Data backup
  - Data restoration

0 marks

No awardable material.

Band 1: 1 – 3 marks

The response demonstrates a limited understanding of the relevant processes and solutions involved and is mostly a statement of facts which are not developed or supported. The approach to the task is inconsistent. Statements may be inaccurate, and the use of precise technical language is sparse.

Band 2: 4 – 6 marks
The candidate has produced a discussion that expands on the factual knowledge but lacks detail in some areas. They show an adequate understanding of the relevant processes and solutions involved including some reasons for their inclusion.
They have provided some valid reasons to support their choices which are structured and presented in a logical order.

Band 3: 7 – 9 marks
The candidate has shown a thorough understanding of the relevant processes and solutions involved.
They have covered these in a logical order, including reasons behind the processes and solutions, the factors that need to be considered and the impact these factors may have on the implementation.
They have provided valid reasons for their choices with responses being clear, coherent and accurately presented.

Test spec reference: Unit 342, Unit 343, Unit 345, Unit 346, Unit 347	**Total marks:** 9