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 paper

Base mark: 80

1	
State **two** internal threats to an organisation's network.	
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.

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

3

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

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

4

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

- Clients.
- Business.
- Suppliers.

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.

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

6

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

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

7

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

- Confidentiality.
- Integrity.
- Availability.

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.

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

9

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

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.

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

11

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

- Digital signatures.
- Hashing.

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

12

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

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

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

13

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

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

14

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

- Least Privilege.
- Defence in Depth.

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

15

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

- Organisational Culture.
- Disgruntled employees.

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

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.

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.

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