AP CYBERSECURITY • EXERCISE SHEET

2.1 Cyber Foundations

Name: ____________ Class: ________ Date: __________ **Total: 13 marks**

Objective

Build the skills to answer exam questions on the **CIA triad** 中央情报三要素, **risk** 风险, and types of security control.

You must be able to:

- state the CIA triad and say which goal a control protects
- define risk and the four risk responses (avoid, transfer, mitigate, accept)
- classify controls by type (physical/technical/managerial) and function (preventative/detective/correc

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ The CIA triad

Confidentiality = only authorised people read the data. Integrity = the data is accurate and unaltered. Availability = it is there when needed. Encryption serves confidentiality, a hash checks integrity, a backup serves availability.

■ Classifying controls

By type: physical (locks, fences), technical (firewalls, encryption), managerial (policies). By function: preventative (a lock), detective (a camera), corrective (patching). A camera is physical by type and detective by function.

2 Practice

2.1 State the three goals of the **CIA triad**. [3]

2.2 Define **risk** in terms of a threat, a vulnerability, and an asset. [2]

2.3 Classify each control below.

(a) A door lock - by function (preventative/detective/corrective)? [1]

(b) A CCTV camera - by function? [1]

(c) Patching a vulnerability - by function? [1]

3 Exam-style questions

3.1 Encrypting a stored file mainly protects which CIA goal? [1]

- **A** availability
- **B** confidentiality
- **C** integrity
- **D** authority

3.2 An organisation buys insurance against a cyber loss. Which risk response is this? [1]

- **A** avoid
- **B** transfer
- **C** mitigate
- **D** accept

3.3 A company adds a firewall, a camera, and a written access-review policy.

(a) Classify each by type (physical/technical/managerial). [3]

4 Go further

- work through the **2.1 Cyber Foundations** lesson on the **Learn** page;
- read the **Securing Spaces** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 confidentiality; integrity; availability.

2.2 risk occurs when a threat can exploit a vulnerability to compromise an asset.

2.3 (a) preventative. (b) detective. (c) corrective.

3.1 B. encryption hides data, protecting confidentiality.

3.2 B. shifting the burden to an insurer is transference.

3.3 (a) firewall = technical; camera = physical; access-review policy = managerial.