



Examination Answer Books

12 Pages

Instructions to Candidates

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.

1	Student Number	1708241
2	Title of Examination Paper	Data Security Governance and Compliance
3	Module Code	ACCA7028
4	Date and Time of Examination	11/1/24 9:00
5	Examination Venue	305
6	Seat Number	
7	Number of Answer Books handed in	

List the numbers of the questions you have attempted	Office Use
Section A	
Section B	
1, 2, 4	
A1-30	22
31	3
32	2
33	2
34	3
35	2
B1	11
B2	9
B4	6
Total	60%

- 1 D ✓ ✓
- 2 C ✓ ✓
- 3 B ✓ ✓
- 4 C ✓ ✓
- 5 A ✗ ✓
- 6 A ✓ ✓
- 7 False ✓ ✓
- 8 A ✗ ✓
- 9 D ✓ ✓
- 10 A ✗ ✓
- 11 A ✗ ✓
- 12 D ✓ ✓
- 13 D ✓ ✓
- 14 A ✓ ✓
- 15 C ✗ ✓
- 16 False ✓ ✓
- 17 C ✓ ✓
- 18 D ✗ ✓
- 19 C ✓ ✓
- 20 B ✓ ✓
- 21 C ✓ ✓
- 22 A ✓ ✓
- 23 D ✗ ✓
- 24 False ✓ ✓
- 25 C ✓ ✓
- 26 A ✓ ✓
- 27 B ✓ ✓
- 28 D ✓ ✓
- 29 C ✗ ✓
- 30 D ✓ ✓

22

22

31. Compliance is adhering to the requirements of an organisation in terms of legal, regulatory, contractual and regional requirements.

This is essential for maintaining privacy/data laws in certain regions, avoiding legal consequences and fines, loss of business or disruption of operations.

3
③

32. Cryptography involves the use of algorithms to convert readable data into unreadable code/data that can only be converted back to readable form with the use of the decryption key.

Encryption & Decryption

It is particularly useful in protecting data in storage or transit by making it private to anyone without a means of decryption. Another form of encryption known as hashing can maintain the integrity of data by matching the hash values to confirm the data is unaltered. DES, AES, etc. ...

2
②

33. An Information Security Policy is a set of defined rules for an organisation to adhere to in order to protect its assets. This policy should be well documented and accessible.

Key elements of the policy should define the scope of the policy, identify specific rules such as BYOD (Bring your own device) and adhere to responsible use of resources. These elements should align with the needs of the organisation.

2
②

34. Intrusion Detection System (IDS) is an automated tool for defending an organisations network. ✓
It works by monitoring a network and identifying unusual ~~or~~ ~~un~~ activity such as, increased network traffic, unauthorised access, multiple access attempts or any other activity that may be suspicious. ✓
IDS helps maintain data security by alerting an organisation to potential intrusion in real-time, thereby reducing risk from such threats. ✓

3
8

35. Physical Security involves the protection of physical assets such as people, premises, infrastructure and any other physical property. ✓
An example of a physical security measure is CCTV surveillance. ✓ This works by the use of cameras to cover important areas such as entrances/exits, valuable property or persons safety. ✓
Footage from CCTV can be monitored in real-time by surveillance operatives as well as recorded and stored for referencing incidents. ✓

2
7

Bio-metric
face detection
etc.

Section B

Question No.

Examiner Only

1 ~~36~~. Security Mechanisms are imperative for adequate data protection. They should be chosen to align with the requirements of an organisation and combine to defend against specific threats/risks, often complementing each other. Firewalls are a commonly used security mechanism for information systems and act by filtering traffic to a network. They can be set to block specific packets to specific network areas and devices, thereby protecting infrastructure from external threats.

Access control may come in several forms. One type involves filtering traffic, similarly to firewalls, but more specifically using Access Control Lists (ACL) to allow or deny access to or from certain devices or subnets.

Access control can also be role-based, allowing access to certain personnel that may need to access certain areas or data.

Access control may protect physical assets as well as digital assets. Electronic locking mechanisms and key-cards can control whether persons may enter certain zones or premises.

Intrusion detection systems can alert security personnel to attempted intrusions by monitoring network activity to identify suspicious patterns. Multiple access attempts might indicate an attempted network intrusion. Or increased volume of traffic might indicate a Denial of Service (DoS) attack.

~~NIDS + HIDS~~

Wi-Fi security standards are another security mechanism to protect wireless networks and infrastructure. They can involve password protection, or AES encryption to protect data from interception.

Security Mechanisms should be integrated into Information Systems depending on an organisations need. It is highly unlikely that a single Security Mechanism will offer adequate protection and therefore multiple Security Mechanisms are typically combined to complement each other to strengthen the overall security posture.

Section B

2. Risk Management is an important aspect of Information Security that involves a comprehensive process for mitigation.

A risk management policy should begin with risk-identification to establish what type of risks an organisation might be faced with. This process is very specific to an organisation's needs. Some risks may be identified by infrastructure. An example of this may be staff using their own devices or working from home. The use of cloud-based technologies may bring data storage risks. Wireless network usage may identify interception risks.

With each potential risk identified, they should then go through risk assessment. Likelihood of risk being realised should be considered, with a likelihood score being assigned to each risk. Threat-level should also be established. In considering the severity/impact each risk may have.

A risk strategy should consider methods for mitigating the risks an organisation are faced with. For the previously mentioned risks such as personal device usage, a Bring Your Own Device (BYOD) policy should be established to control the use of devices. Staff working from home could be mitigated by VPN protection, and wireless networks should use Wi-Fi encryption standards.

Each risk should not only be considered for mitigation methods, but also monitored for continual improvement to address evolving landscape.



Further to the different kinds of risk, disaster strategies should be considered, as well as potential acts of terrorism

Section B

4. Organisations can establish Information Security Systems through the use of Security Management Models and Practices. Various models exist, such as the NIST Framework for Information Security Management, or the ITIL Library for best business practices. An organisation should choose a model that aligns with their business needs and principles.

One of the most widely recognised models is the ISO/IEC 27000 Standards. This family of standards can be chosen individually, ~~or~~ tailored to an organisation's needs. ISO/IEC 27001 defines a set of recommended practices for the implementation of an Information Security Management System (ISMS), a comprehensive security system that is suitable for organisations of all types and sizes. It also offers scalability for changing business needs/sizes.

The ISO/IEC 27001 model involves various factors, such as an ISMS scope, staff structure, risk management, operations security, auditing and evaluation, compliance, and progression.

The benefits of an ISMS using ISO/IEC 27001 offer a comprehensive security plan that can also provide recognised certification to boost an organisation's profile/reputation. One of the disadvantages is cost. For an ISMS to work, it does not need all of the recommendations in the standard, nor does it require certification. It should therefore be balanced by the individual requirements of the organisation's needs and budget/resources that it can spend.

What about NIST, COBIT, etc.