



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 over 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	2225674
2	Title of Examination Paper	DATA SECURITY GOVERNANCE & COMPLIANCE
3	Module Code	ACCA7028
4	Date and Time of Examination	11/01/2024 09:00am
5	Examination Venue	10310
6	Seat Number	047
7	Number of Answer Books handed in	

List the numbers of the questions you have attempted	Office Use
1-30	2.2
31	2.5
32	3.5
33	3
34	2.5
35	3.5
36	
1	8
2	2.5
3	2.5
Total	50

22
2.5
3.5
3
2.5
3.5
8
2.5
2.5
50

SECTION A

- 1 D ✓ ✓
- 2 C ✓ ✓
- 3 B ✓ ✓
- 4 C ✓ ✓
- 5 B ✓ ✓
- 6 A ✓ ✓
- 7 False ✓ ✓
- 8 C ✓ ✓
- 9 D ✓ ✓
- 10 A ✓ ✓
- 11 B ✓ ✓
- 12 D ✓ ✓
- 13 D ✓ ✓
- 14 A ✓ ✓
- 15 A ✓ ✓
- 16 False ✓ ✓
- 17 C ✓ ✓
- 18 C ✓ ✓
- 19 C ✓ ✓
- 20 B ✓ ✓
- 21 D ✓ ✓
- 22 A ✓ ✓
- 23 Risk Assessment X
- 24 False ✓ ✓
- 25 C ✓ ✓
- 26 A ✓ ✓
- 27 B ✓ ✓
- 28 D ✓ ✓
- 29 B ✓ ✓
- 30 D ✓ ✓
- 31

(22)

31 ~~Compliance~~ in the context of data security refers the act of aligning business goals, policies,

31 Compliance in the context of data security is the ability of adopting security policies, standards, tools techniques which align with legal laws in ensuring the security of an organisation data. This is essential to ensure that the confidentiality, integrity and availability of data is followed or observed.

It is also essential to prevent loss of data either in transit or at rest.

Every organisation that operates in a certain environment must comply by abide by the local, or international legal law within that environment.

32. The role of Cryptography in data security
Cryptography is the utilisation of security tools in protecting the confidentiality, integrity and availability of data. Cryptography tool encrypt data with a unique key generated from the encryption, the availability of data will only be accessed by someone with that key.
Two types of encryption exist:

1. Symmetrical
2. Asymmetrical

Cryptography protects the sensitivity of information in a way that data or sensitive information can only be accessed by an authorised person. It ensures that sensitive information remains confidential, without losing its

Integrity, and is available when needed by an authorised person.

33. Information Security policy refers to a well planned and documented guidelines that regulates the use of information by organisations. These guidelines and procedures if well implemented will ensure the security of information.

Information security policy contains key elements like risk assessment plan, Contingency plan, and more.

The key elements that must be included in a Comprehensive policy are:

1. Incident Response Plan
2. Disaster recovery Plan
3. Business Continuity Plan

34. Intrusion Detection Systems (IDS) is a system designed to protect organisational data from incident, data breaches or loss. IDS contains mechanism that detects abnormal traffic in real time, and analyse the traffic for any threats and take action based on the analysis. If it detects any threats, it mitigates the threat before it affects the data.

IDS protects organisation internal network from any threat that come through an external network.

IDS has different features that it uses in ensuring that data security is maintained,

~~protect data from data breach~~

Some of these features are!

1. Packet analysis: ~~this~~ analyzes every incoming packets from the network, and tries to block them.
2. Firewall: It has a built firewall that blocks traffic that tries to breach into the network.
3. monitoring: It has the interface which helps Information Security experts of an organisation to monitor the current status of their network and make necessary decisions or steps towards ensuring data security.
4. logging: IDS provides logs of every activities that goes on within the system.

35. Physical Security is an implementation of a Physical Security measures towards ensuring the security of data. Physical Security includes measures like; ~~fences, etc~~

1. Key locks ~~by~~ Security systems that prompts users to access a data room by tapping on ID Card, or authenticating their identity by fingerprint or iris scan.
2. Surveillance Cameras is another physical security.
3. Having security personnel who monitors every activities from a control room through the screens or even standing the entrance detector is a physical security.

An example of a Physical Security is a student who has a student ID Card, he tries to use the ID to access the network room or server room, he will be denied entry, this is because his ID Card is only configured

to allow entrance to lecture classrooms.
Even a staff of the school has limited access to certain rooms within the school.

SECTION B

1. Security mechanism used in data protection is designed to ensure data maintains its confidentiality, integrity, and availability. These mechanisms help to prevent data breaches, authorised access or theft. Security mechanisms has features like:

a) Access Controls: access control limits the availability of data to only authorised users. It ensures that access is granted to users based on their rights and privileges of data access.

b) Firewalls: firewalls are security features that ensures the right traffic is entering the security system or network. It filters and blocks any ports like traffic. It is configured to block ports that is open to any malicious network. Firewalls are important component of a security mechanism.

c) Intrusion detection systems: IDS detect when there is a potential threat to the network or server. It alert security personnel about a potential risk that could damage data. It also block and signal that is not known to the network.

With the integration of Access Control, Firewalls and IDS into an organization's security strategy, data protection can be ensured.

2. Risk management plays a big role in data security. It is a plan put in place to manage risks that could ~~accident~~ lead to loss of data. Risk management has different phases:

Identify the risk: Identify the type of risk

Assess the risk: ~~check the~~ ^{to} see the value of risk

Evaluate the risk: Categorise the risks according to its potential of affecting the availability of data.

It is a high risk that must be attended to? or it can be ignored?

2.5

3. Governance is the procedure that governs how an organisation adopts strategies to ensure that ~~security~~ every stakeholder of the organisation implements all required steps towards ensuring the security of data. The approach adopted by an organisation in ensuring the security of data is governance. Each organisation is governed by different governance.

~~Govern~~ The impact of governance on Strategic Planning can help foster a more robust Incident response plan

The impact include:

Access Control: Controls who can access data.

Risk assessment: Effective governance can help setup and implement

2.5



a more effective assessment plan.

Incident response: an effective governance help organisation respond more effectively to incident that could be detrimental to life.

Ris