



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, and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either reject 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	2220382
2	Title of Examination Paper	Data Security, Governance and Compliance
3	Module Code	ACCA7028
4	Date and Time of Examination	11/01/23 9:00AM - 11:00AM
5	Examination Venue	310
6	Seat Number	064
7	Number of Answer Books handed in	

List the numbers of the questions you have attempted	Office Use
A1-30	12
31	4
32	4
33	3
34	3
35	3
B2	12
B3	8
B4	14
Total	639

SECTION - A

1. D. Authentication ✓ ✓
2. C Intellectual Property ✓ ✓
3. B Penetration Tester ✓ ✓
4. C Polymorphic Threat ✓ ✓
5. A ~~Staffing~~ ✓ ✗
6. C End-user terms of use agreement ✗
7. False ✓ ✓
8. C Analysts' ✗ ✓
9. C Certified Information Security Managers ✗
10. A Framework design ✗
11. B Risk analysis ✗
12. D People, Process and technology ✓ ✓
13. C Business Continuity Plan (BCP) ✗
14. A Termination ✓ ✓
15. A Confidential data ✗
16. True ✗
17. C Polygraph test ✓ ✓

- 10.C separation of duties ✓ ✓
- 14.A Incident response policy ✓ ✗
- 20.C Disaster recovery plan ✓ ✗
- 21.B Traditional Data Backups ✓ ✗
- 22.D intrusion detection ✓ ✗
- 23.D ~~Database shadowing~~ Remote Journaling ✓ ✗ 4
24. True ✓ 4
- 25.D Internal-External zone (IEZ) ✓ ✗
- 26.B Boundaries on the use of medical information ✓ ✗
- 27.B Vulnerability Management Program Maintenance ✓ ✓
- 28.D Expunge ✓ ✓
- 29.D Security Policies ✓ ✓
- 30.C Slack time ✓
31. Compliance in the data security can be considered as the rules, regulations and policies which are required by an organisation or body to maintain its security and to keep an organisation in check with the laws both local and international. It is a set of rules that allows an organisation to keep in check its security protocols, regulations and policies. ✓ ✓ [12]

Compliance is essential for an organisation in many ways

- i) It helps define an organisation's policies, protocols and regulations which gives a proper channel and framework in identifying and assessing risks.
- ii) Having a streamlined compliance and regulations help an organisation or business to avoid any legal or unethical challenges as it keeps the organisation in check.
- iii) Compliance also helps in maintaining the reputation and trust of client and stakeholders as it abides by the international law which makes an organisation trustworthy and transparent.

32. Cryptography in data security refers to encryption of the data into unique cipher text or string to help protect it from theft, attacks and risks. This data can only be decrypted by a unique key which helps it to be secure from attackers and ransomware. This means that even if data gets stolen, it would make no sense as it was encrypted and converted into another format/string. It can only be retrieved by a unique deciphering key which allows a person to have more control over it.

Cryptography can secure data in following ways:

- i) By ciphering the raw data into a character of string so that only the user with the decryption key can have access to it.
- ii) By having end to end multi layer encryption and decryption from both user end and the machine or system where data is stored.
- iii) Cryptography also helps in protecting sensitive data by preventing the data to be stolen by an outside attack. It helps in securing the network and doesn't allow data being compromised either due to internal malicious attack or from outside the network.

33. Information Security Policy is the rules and regulations laid out for an organisation in order to maintain its security and secure its data. The security Policy acts as a guiding light for business and organisation to maintain ~~this~~ ~~its~~ integrity and to avoid any risks or legal issues. Every organisation must have their security Policy abide by the local and International Policies and regulations. In order to do that they must assess ~~add~~ ~~was~~ ~~was~~, prioritize risks which they can face and also to educate their employees, clients and stakeholders that each one has a unique role to play in order to maintain a safe and secure environment.

The three key elements that should be included in a comprehensive policy:

- i) The security policy of an organisation should be made by keeping the compliance and regulations of the local and international laws in check. Repeat
- ii) The Security Comprehensive Policy must be ~~made~~ aligned with the business goals of an organisation. Also, it should assess the level of threats an organisation can face and should not cost over the budget and investment of the clients and stakeholders.
- iii) The Comprehensive Policy should also have proper channel so that everyone working for the business can have knowledge and access to it so that each individual can understand their role in maintaining the organisation's security.

34. Intrusion Detection Systems (IDS) are a set of ~~frameworks~~ that identifies and protect ~~against~~ data breach, attacks, risks and ~~vulnerable~~ vulnerability. They can help organisation to detect a threat early so that proper action can be taken against them before it gets more severe. It also helps in monitoring and assessing logs so that the security team can have proper knowledge of the cause of the threat and be prepared for the next time.

— Intrusion Detection Systems can help maintain data security in two ways.

- i) Network Intrusion Detection System (NIDS)

NIDS monitors data threat in real time through the network traffic. If there is any unauthorised activity throughout the network channel, it will immediately alert the security and compliance team.

ii) Host-based Intrusion Detection System.

In these IDS, the host or machines are pinged with the secure channel so that if there is an attack or threat, the host machine will immediately identify the risk and the appropriate measures can be taken before it's too late.

35. "Physical Security" as by the term is described as the security of physical assets of an organisation. Though digital security is a big concern in today's world, it is also important to secure the physical data and devices from theft and steal.

A simple example of physical security is that an organisation has sensitive data in their server rooms. In order to protect it from unauthorised access, the organisation provides special Biometric ID's to the people who are concerned with that data. This allows only a handful of people to enter that facility. Also the ID's are regularly assessed and monitored by security so that they can keep a log of the entry and exit checkpoints. This ensures the safeguarding of that secure data.

Physical security can be taken into consideration through access control systems which means providing special tools to access the data like biometrics, ID's, signatures, etc. Also it comprises of monitoring of the data to keep in check on who has access to it.

SECTION - B

2. The role of "Risk Management" in data security is so huge that without it we cannot have an authentic and secure infrastructure. Risk Management includes the early identification of risks and how they can be detected before they can cause a serious damage. It also includes establishing proper channel and protocols in place so that the business can evaluate the nature of its threat and prevent it from happening again.

One of the major role of Risk Management is to identifying and assessing risks. It can be done by following ways

i) An organisation must have a baseline protocols to evaluate and assess the data risks. The identification of risk and threats can then be done by comparing them against the pre-defined security protocols in an organisation.

ii) The organisation should analyse and predict the severity of threats it can face. This can be done by Risk Prioritization which identifies as the level of security breach an organisation can have.

Not just data
but also
devices.

iii) An organisation can identify risks by assessing the data it has. If the level of investments and data is sensitive it should spend more in its security policy that complies with the international regulations and whose frameworks are compatible across various security channels.

iv) Identifying the threat landscape. By identifying the threat severity and its level of impact the organisation can start assessing their risk policies and security measures. If the threat of a breach is severe, it can result in heavy data loss therefore the business should comply with its goals and security policies.

Strategies for controlling these and mitigating risks can include installing comprehensive security policies. Also, to adapt a security framework and model which abides by the rules, policies and regulations.

To identify and eliminate risk by having dynamic intrusion systems which can identify and alert a risk or a threat.

The clients and stakeholders with their employees should be well aware of the organisation's security protocols in order to identify and immediately report a risk or threat if necessary.

3. The importance of Governance in security is vastly dependent on the policies and regulations the organisation has. The Governance policy should follow the compliance and protocols established.

by the local and international bodies. When an organisation has a sense of "oversight" they have a responsibility to abide by the laws and rules to avoid any unethical behaviors and to maintain trust and transparency. It also helps to maintain the brand value and gives a satisfaction to the clients and stakeholders who have invested themselves.

The Governance and its planning for security involves adopting a proper channel and model of ~~secure~~ information security so that ethically they can resolve any challenges or threats faced by them.

If an organisation's security is properly governed there will be less chance of data breach ~~data~~, threats and loss of company's assets and data. It also avoids any financial crisis which can bankrupt a company.

The governance policy established by an international body helps determine how the organisation should operate ethically. The data security is influenced ~~on~~ by the organisation's history of following ethics, ~~and~~ rules and regulations.

Very generic
not much technical

4. Security Management Models and Practices are frameworks which help organisation to maintain its security. These are different models which have different approaches to maintain the security and integrity of an organisation. Some of them are:

i) ISO - 27001 (Information Security Management System - ISMS)

This is the most renowned and well known security model. Its advantage is that it is internationally accepted and provides a very secure risk assessment framework which is communicable throughout various security layers.

The disadvantage of this model is that it is quite expensive to implement and sometimes can be tough to regulate with the local bodies.

ii) COBAA

This security framework is again internationally recognisable and has a simplified framework which most organisations use so it is easy to implement.

Its disadvantage is that it doesn't allow multiple security frameworks to be layered for a single organisation. Also it can be difficult to get due to its cost.

iii) Lockbox Model

This model of security is based on security protocols of identifying risks by the use of detect, recover, analyse, identify and recover.

But it is not widely used and accepted and therefore an organisation which has its body in other countries cannot consider this.

iv) NISP

This is again a very popular security framework model which identifies risk and assessing them on an immediate basis. It is also an internationally accepted security model. But its disadvantage is that it can have a few vulnerabilities and is less secure comparing with other model.

Selecting the most suitable model for an organisation should depend upon

- i) The level of threat it can face.
- ii) By analysing the risk priority, vulnerability and the threat landscape.
- iii) By analysing the budget of the organisation which they have for their security policy.
- iv) By complying with the security protocols and frameworks that the organisation has established.