



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 be 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	230 4602
2	Title of Examination Paper	Data security, Governance and compliance.
3	Module Code	ACCA7028
4	Date and Time of Examination	11/1/2024
5	Examination Venue	I2 310
6	Seat Number	045

7	Number of Answer Books handed in	
---	----------------------------------	--

List the numbers of the questions you have attempted	Office Use
A1-30	18
31	1.5
32	1.5
33	3
34	0.5
35	1.5
B1	7
B2	1
B3	5
Total	39

18
1.5
1.5
3
0.5
1.5
7
2
5
39



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. A ✓ ✓
13. D ✓ ✓
14. A ✓ ✓
15. A ✓ ✓
16. FALSE ✓ ✓
17. C ✓ ✓
18. D ✓ ✓
19. C ✓ ✓
20. B ✓ ✓
21. D ✓ ✓
22. A ✓ ✓
23. D ✓ ✓
24. FALSE ✓ ✓
25. C ✓ ✓
26. A ✓ ✓
27. B ✓ ✓
28. C ✓ ✓
29. B ✓ ✓
30. A ✓ ✓

18

18

31. In the field of data security, "compliance" refers to compliance to regulations, industry standards and policies. It is essential for organizations to meet policy requirements and make strong ~~strategy~~ strategies. Compliance will ensure organizations rapidly ~~evolving~~ in threat ~~to~~ environments. 1/2 1.5
32. The role of cryptography in data security is to protect information and prevent them from being theft and leak in a network or a system. The core of cryptography is encryption and decryption. We can use a key to encrypt ~~a~~ original datas and then decrypt them with the same key to access the original datas. It is crucial for organizations to use this technique to protect information and manage risks. 1/2 1.5
33. "Information security Policy" is a policy that organizations make it to manage risks, protect datas and intellectual property. The first key element in this policy is compliance. any policies should be made under compliance. The second key element is risk management. before ~~we~~ organizations discuss how to protect information, the first thing they do is to know what risks they are facing. The last key element is protection, ~~protecting crucial information~~ how to protect crucial information plays an important role in information security Policy. 3 3

34. IDS is designed to detect risks and vulnerabilities in a network or a system. When IDS detected risks, it will alert administrators. So the administrators can find them and then establish some strategies to defense them.

0.5

35. Physical security is designed to protect physical assets, facilities and systems. A fingerprint is a physical security measure. Only using the correct fingerprint in the systems can access those physical assets.

1.5

1 1/2

Section B

1. Security Mechanisms used in data protection are crucial for organizations to protect information in big data era. There exists many mechanisms such as access controls, fire walls and IDS. Access Control is designed to control who can access ~~the~~ the network or systems which storing various crucial information. Only one who have authorized before this can access those crucial datas. Firewalls can preventing attack, ~~from~~ this mechanisms is common nowadays. No matter private networks or public networks, firewalls play a crucial role in data protection. IDS can detect risks and vulnerabilities in a network or system. It is helpful for organizations because they can quickly find where is it and then make strategies to defense it. The three mechanisms play different role in an organization's security strategy. so in various organizations put them intergrated to protect information more effectively.

NIDS
HIDS

2. Risk management is so crucial that ~~any~~ all organizations should do it before making strategies. Before organizations establish a policy ~~to protect~~ information, they should know what risks they are facing and will face in the future. Only when ~~if~~ organizations know this key point, they can do better in ~~into~~ data security.
3. Governance plays a crucial role in data security. The key point of strategic planning for security is to know what types of ~~sec~~ data organizations owned. The importance and amount of data is also ~~so~~ important. So, data classification and grading can be an effective way to governance. According to the difference ~~be~~ among data, organizations can classify them into different types, such as employee data, intellectual property and others. And then organizations can grade these data according to the importance of them. Confidential data ~~is~~ are most important data so they will be protected strictly, and just manager can access them. Organizations can manage data security effectively through data classification and grading. This is the way how effective governance can influence an organization's ability to manage data security.