

Complete, fold and seal
(see note 2 below)

FORENAME(S): NIKHITHA.

12 Pages

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, for the invigilator to see, and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners cannot 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	2406304
2	Title of Examination Paper	DATA SECURITY, GOVERNANCE AND COMPLIANCE.
3	Module Code	ACCA7028.
4	Date and Time of Examination	07-01-2025. 9:00 AM.
5	Examination Venue	310
6	Seat Number	017
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
Sec 1-Q1	10
Sec 2	50
Total	60

SECTION-B.

1. True. ✓
2. Authentication. (d) ✓
3. Intellectual property. (c) ✓
4. Penetration tester. (c) ✗
5. Polymorphic threat. (c) ✓
6. Leading. (b) ✓
7. Directive. (d) ✗
8. Organizing. (a) ✓
9. Behavioural feasibility. (c) ✓
10. Issue-specific Security policies. (b) ✓
11. Descriptive ethics. (d) ✓
12. Electronic communications privacy Act (ECPA) (d). ✓
13. True. ✓
14. Public control of medical information. (a) ✓
15. Hospitals. (c) ✓
16. Vulnerability Management program maintenance. (b) ✓

17. True. ✓
18. Jurisdiction. (b) ✓
19. computer fraud and Abuse Act. (c) ✗
20. Analyse the data. (d) ✓
21. Mission Statement. (d) ✓
22. True. ✗
23. Organizational profiling. (c) ✗
24. An individual or group who has a vested interest. (d) ✓
25. values statement. (a) ✓
26. Diagnosing. (b) ✓
27. True. ✓
28. Mid-level Manager. (c) ✓
29. Monitor. (a) ✓
30. Lack of management Support. (b) ✓
31. Enterprise information Security policy. (c) ✓

32. True.

33. Expunge. (d)

34. It addresses hardware implementation issues. (c)

35. Task-specific security policies. (d)

36. Access control lists. (b)

37. False.

38. Analysis phase. (d)

39. End-user license agreement. (a)

40. Performing a risk assessment. (c)

41. Security analyst. (c)

42. False.

43. See

43. Security technicians. (a)

44. CISSP. (b)

45. More than 100, less than 1000. (c)

46. True.

47. Global information security officer. (d)

48. They can improve configuration rule Security. (d) ✓

49. critical path. (d) ✓

50. Security Awareness. (d) ✓

51. False. ✓

52. Enterprise Risk Management (ERM). (c). ✓

53. Executive governance and Support. (d). ✓

54. RM framework team. (b). +

55. Direct takeover. (d). ✓

56. The triad protection characteristics for information security are:

1) Confidentiality. ✓

2) Integrity. ✓

3) Availability. ✓

1) Confidentiality: Only authorised users can access the data.

2) Integrity: The data should be accurate while transmission of data.

3) Availability: Authorised users can have access when data is required.

57.

58.

SECTION A.

QUESTION ONE.

b) Importance of CIA triad..

In general information security is being free from danger.

In another words information security securing the data.

In the process of securing the data 3 protection characteristics are important. It is called CIA triad.

CIA triad plays an important role in protecting the data.

CIA stands for

1) confidentiality.

2) Integrity.

3) Availability.

1) confidentiality : when only authorised users can access the data, it is called confidentiality.

⇒ Because when securing confidential data it should be access to only authorised users.

⇒ confidentiality is applied in government operations, business information, etc....

2) Integrity : When data is accurate while transmission, it is called integrity.

⇒ Because, when data is transferring, many changes can happen to that data.

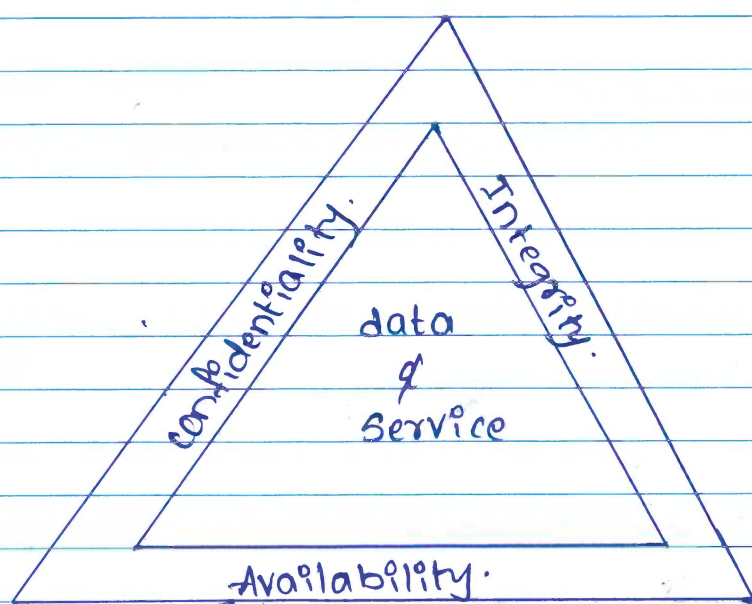
⇒ It can be modified or it can be deleted.

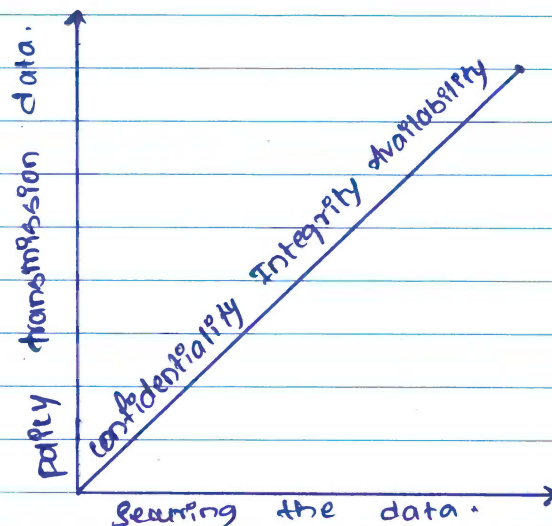
⇒ So, while transferring the data, it should be accurate.

3) Availability : When authorised users can have access when data is required, it is called availability.

⇒ Here, data is available for only authorised users because it is confidential data.

⇒ Data ~~is~~ cannot be accessed by unauthorised users.





⇒ From the first diagram we can say that Confidentiality, Integrity and Availability is a triad.

⇒ Confidentiality, Integrity and Availability is used to secure data and service.

⇒ To secure data confidentiality, Integrity and Availability are most important characteristics.

⇒ Securing the confidential data is most important for an organization.

⇒ And keeping accurate is also the important part in an organization.

⇒ And data is available for only authorised users to access it.

⇒ Finally, to secure the data confidentiality, Integrity and Availability are most important.

⇒ They play vital role in securing confidential data.

X

a) i) Identification : When data is accessed it should be identified.
⇒ It should be aware of who is accessing the data.

ii) Authentication : When data is accessed authentication is important.

⇒ Authentication is done by only user agreement or permission.

3

10