



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

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 read your legible 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.

Complete, fold and seal
(see note 2 below)

SURNAME: KOCHAMPARAMPIL ANIL

FORENAME(S): AKHIL

1	Student Number	2409841
2	Title of Examination Paper	DATA SECURITY GOVERNANCE AND COMPLIANCE
3	Module Code	ALCA7028
4	Date and Time of Examination	07/01/2025 9:00 am
5	Examination Venue	IQ 310
6	Seat Number	014
7	Number of Answer Books handed in	

List the numbers of the questions you have attempted	Office Use
Sec 1 - Q1	30
Sec 2	34
Total	64

Section A

Question One

a, Information Security (Info Sec).

Information Security refers to secure the information from ~~unad~~ unauthorized access, threats and safeguard intensive information. There are ~~numerous~~ ~~neumours~~ steps to make our information the main step is CIA Confidentiality Integrity Availability. If we organize these steps correctly we can safe our information or data securely.

Confidentiality

Confidentiality refers to make our data only access to the authorized people. So that we can avoid a huge occurrence of data breaches. So it should be safe.

eg: If a data of a big organization access to all the members, it is accessible for data breaches and data threats, so confidentiality is a main step for secure our sensitive data or information.

Integrity

Integrity refers to known as the policy and guidance of the data and also it should be ensure that the data must be trustworthy and genuine.

Availability

Availability describes about the authorize members can access the data at any time we want to access. If the organizer or the member can't access the data at correct time it may occur huge issue like hacking, unauthorized access may occur.

i, Identification

Identification is a main process of info sec. The main function of identification is to identify the user or entity is it genuine. It may identify in similar way like username and password.

eg: If a user trying to login a site using username and password there occurs the system will verify or identify the user is correct or genuine.

By identification the system can ensure the organizer and the members so that we can safeguard our sensitive information or data. There are lot of issues now occurring the user details may be hacked by the hackers and they use that data to make criminal activities. Nowadays, the value of a data of a person is huge they can use that data in anywhere and they can use unused activities and the data owner will be occur the criminal because all the information is in his name.

ii, Authentication

Authentication is a guard of our data or a user. The use of authentication is high because of the user issues.

The Authenticator works by verifying the user is genuine or not by checking the biometric verification, face recognition or multifactor Authentication (MFA).

Authenticator plays a major role in the safeguarding of information or data.

By Authentication we can analyze the user details and the information like fingerprints or face recognition match with the registered user. If it is matched we can access to the data or system. 6

Nowadays, all the technical device and all device is unlocked by authenticator like fingerprints and face recognitions. It is very safe to protect our device and information from third parties.

iii, Authorization

Authz Authorization defines that the organization or a member or user can only access to the authorized department or permission. So that it can be helpful to reduce the occurrence data breaches. Mainly the sensitive data of a organization is only accessible for authorized people's no unauthorized user can access this data.

eg: If our smart phone have lot of data of our privacy and personal things we can't give it another one because our information and data are very important. So that authorization means the data is only ~~author~~ accessible for authorized user.

The organization have to organize or limit permission to the user that the department related to the user. User can't access ~~the~~ to the other department.

eg: If we install a editor app in our Smartphone, after installation the app ask for the permissions, allow the permission to access the gallery, file manager. If we don't want to like the app access our gallery or file manager we can't deny the permission.

Same like the example above, the user must have ~~to~~ access to permitted to only the department which the user is related.

iv, Accountability

Accountability defines that the organizer must be organize the employees, that what the employer doing what changes they making. There should be a continuous tracking and recording of the employees actions so that it should be a source. if any issues occur in that section.

eg: If a employer done an unauthorized activity in the data and the organization found that occurrence, but they have no source to express this employer done this activity.

So in this occurrence we have to keep tracking and records every action doing by the user or employer. By this accountability we can maintain or defend unauthorized activities from sensitive data or information.

Identification, Authentication, Authorization, Accountability these are the four processes of information security to safeguard our data from unauthorized activities.

b, CIA triad

Confidentiality Integrity Availability triad is a base step for guidance and policy of a data defense in CNSS (Committee of National System Security) it is also known as Mcumber Cube.

As we take the info sec the data is protected by the step by step condition and layers Included by CIA we want to make sure CIA even confirmed in the data. we can say CIA is the pillar of the data security system.

Confidentiality

Confidentiality refers that the data must only access to the authorized peoples otherwise there is a huge increase of data breach occurrence.

If we have to secure a data we have to confirm the confidentiality to ensure our data safe.

Integrity

Integrity define that the data we have to protect must be trustworthy and followed the guideline and policy of laws. Then only we can protect the data properly without any fail.

Availability

Availability defining that we have to access to the data when we need at any occurrence. we have to available the system and data at the time to if any issue occur. then only we can fix it otherwise the time is gone they may occur large loss of data.

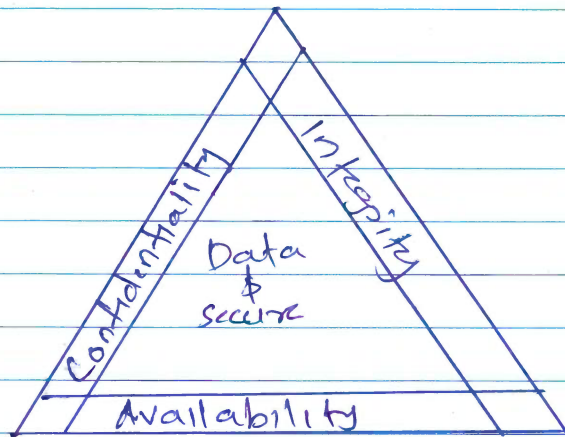


fig: CIA Triad

Section B

- 1, True. ✓
- 2, Authorization (c) ✗
- 3, ~~Intelligence~~ ~~properly~~ Competitive intelligence (d) ✗
- 4, Penetration tester (b) ✓
- 5, Polymorphic threat (c) ✓
- 6, Discreting (c) ✗
- 7, Objective (c) ✓
- 8, Controlling (b) ✗
- 9, ~~Th. Technological~~ ~~feasibility~~ operational feasibility (d) ✗
- 10, Issue-specific security policies (b) ✓
- 11, Normative ethics (a) ✗

12, ~~12~~ Electronic Communications Privacy Act (ECPA) (a) ✓

13, False ✗

14, Public Control of medical information (a) ✓

15, Hospitals (c) ✓

16, Vulnerability Management Program Maintenance (b) ✓

17, false ✗

18, Jurisdiction (b) ✓

19, Computer Fraud and Abuse Act. (c) ✗

20, Analyse the data (d) ✓

21, objectives statement (c) ✗

22, True ✗

23, Overall Strategic Planning (a) ✓

24, An individual or group who has a vested interest (d) ✓

25, vision statement (b) ✗

26, Diagnosing (b) ✓

27, True ✓

28, Mid Level Manager (c) ✓

29, Monitor (a) ✓

30, Lack of stake holder Support (c) ✗

31, Issue specific Security Policy (b) ✗

32, True ✓

33, Expunge (d) ✓

34, It addresses specific technology based resources (a) ✗

35, System Specific Security Policies (c) ✗

36, Access Control lists (b) ✓

37, True ✗

38, Analysis Phase (d) ✓

39, End user terms of use agreement (c) ✗

40, Performing a risk assessment (c) ✓

41, Security Analyst (c) ✓

42, False ✓

43, Watch Standers (d) ✓

44, CISSP (b) ✓

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

46, True ✓

47, Security+ (b) ✓

48, (b) +

49, Critical Order (a) +

50, Security Certification (b) +

51, False ✓

52, Enterprise Risk Management (c) ✓

53, Framework design (a) +

54, RM framework team (b) +

55, Pilot test (b) +

56, ~~CIA Grad CNSS (Committee of National System Security)~~

57, CNSS +

58 Frameworks. +

59, CIA Confidentiality Integrity Availability ✓

Confidentiality refers to access to only authorized users.

Integrity refers to define the data is trustworthy and obey the policies and guidance

Availability defines we can access at any time we ~~need~~ need.

~~CNN~~

CNSS - Committee of National Security System

It is also known as Mccumber cube.

34