



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 will either 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	2219819
2	Title of Examination Paper	Data security governance and compliance
3	Module Code	ACCA7028
4	Date and Time of Examination	11/01/22
5	Examination Venue	IG Building, Swan Sea. 310
6	Seat Number	50.

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

List the numbers of the questions you have attempted	Office Use
A1-30	22
31	4
32	5
33	0
34	3
35	4
B1	10
B2	10
B4	11
Total	69

Section - A

22

1. D ✓
2. C ✓
3. B ✓
4. C ✓
5. C ✓
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. D ✓
21. A ✓
22. A ✓
23. D ✓
24. D ✓
25. False ✓
26. C ✓
27. A ✓
28. B ✓
29. D ✓
30. B ✓

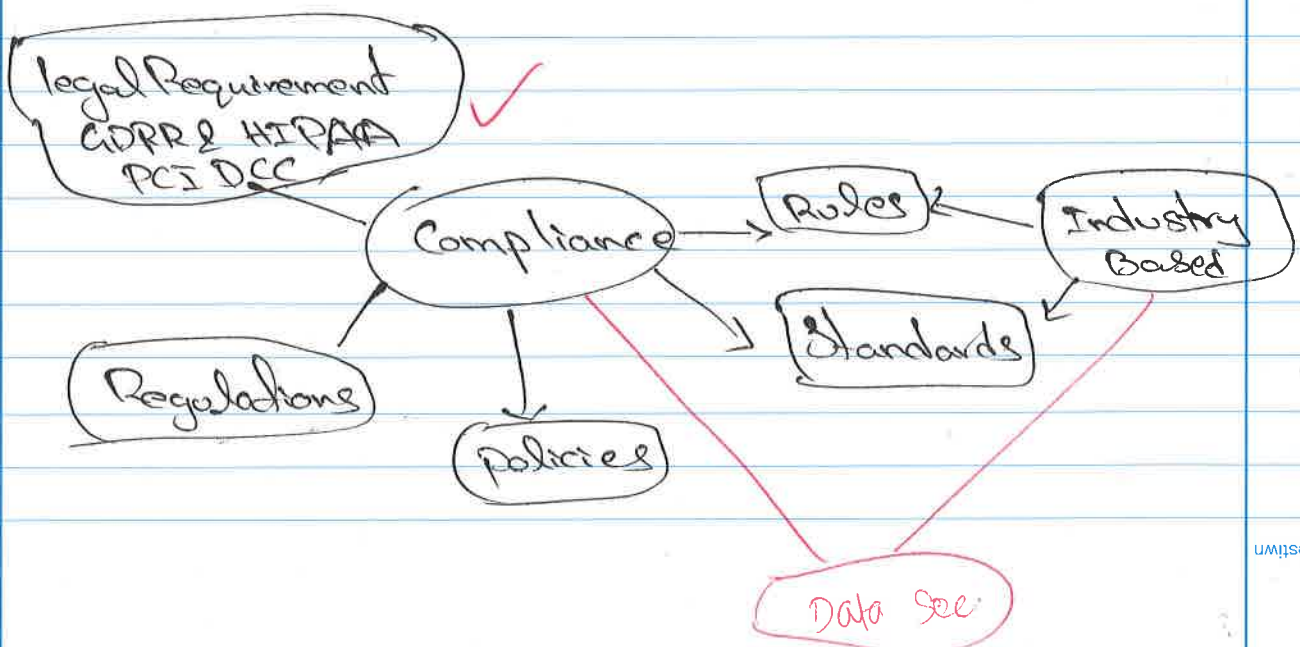
3A) Compliance.

Compliance is a data security to ensure the attach to establish the policies, law, regulations for an organisation. It also ensure the critical to mitigate risks from the cyber attacks, and threats. Compliance concerning the role that can legal requirement like GDPR and HIPAA.. It also the create guidelines to understanding unauthorized access. to for an organisation and also gains the customer trust. In compliance there are many role sectors to follow.

1) Health sector: It prevent to secure the. indend, from attack to the. patient information, and, sensitive data.

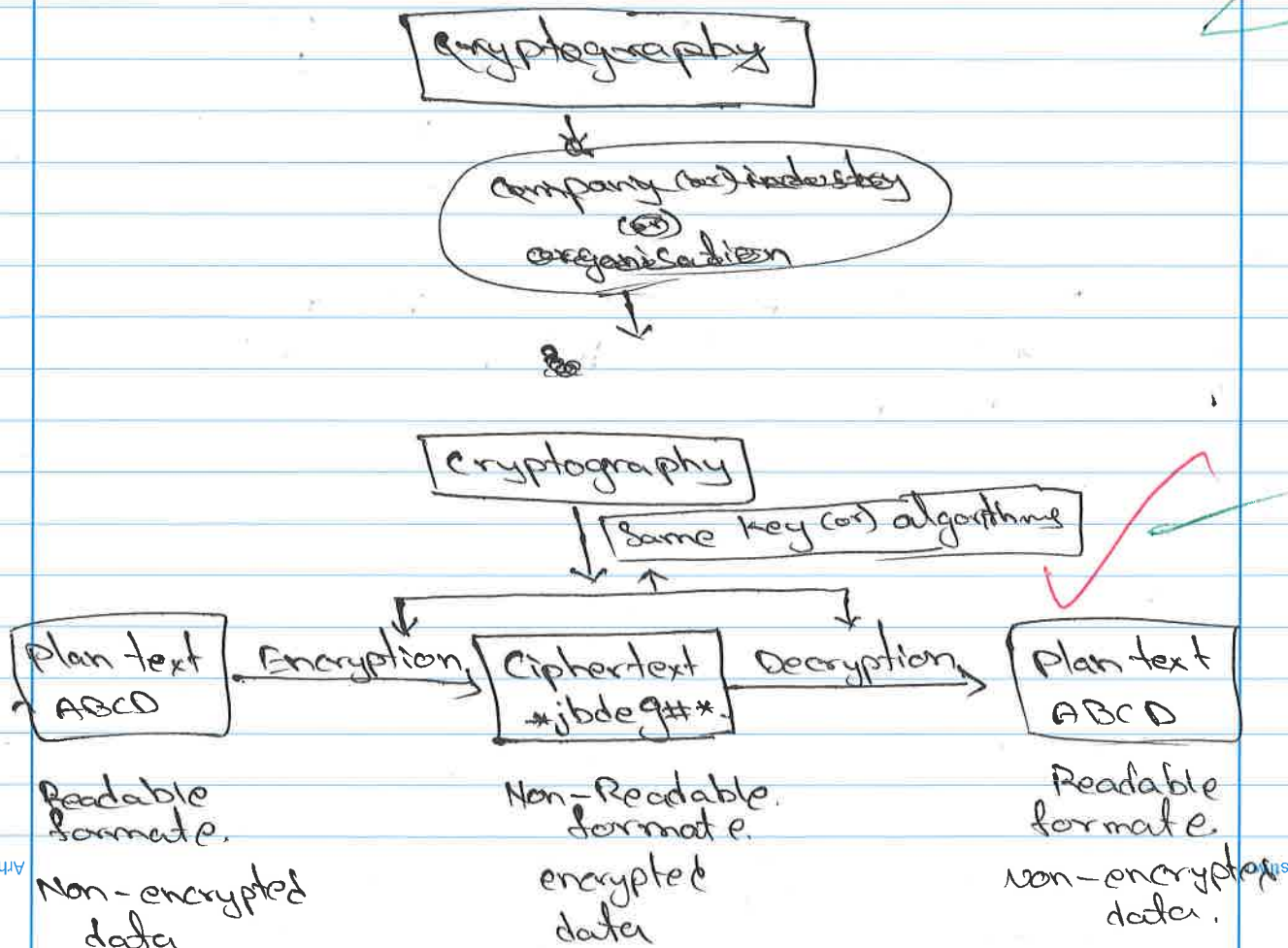
2) Financial sector: In Financial Sector major check the invest, trade, and stakeholder which can be prevent from attack.

3) Information sector: In IT Sector data is always an issue to casus to prevent mitigate. take legal and on requirements. Non-compliance is risks affect the, cyberattack, loss trust from customer.



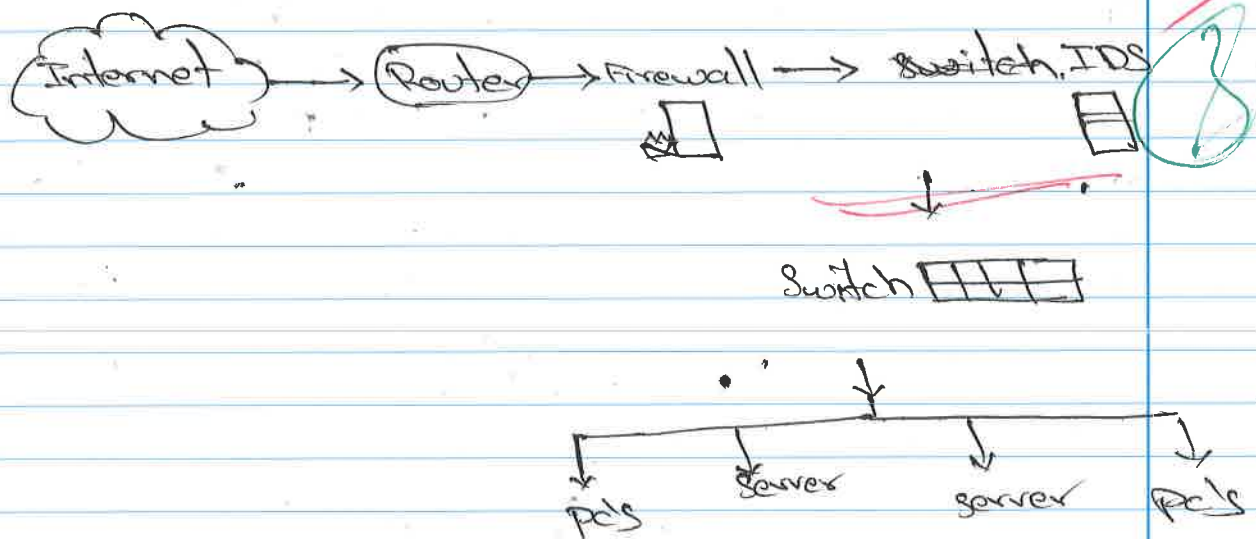
32) Cryptography

In cryptography play a pivotal role to secure the sensitive data from attacks, so it decodes the data in other formate. and encrypted. once data is transfer from proper user and organisation then give right proper key (or) algorithm then the data can be access. In this process there are several technology like ~~RES~~, and ~~ARS~~ ^{AES}. These ~~technical~~ techniques is helpfull to decrypt the data. and ~~data~~ data is always prevent the ~~into~~ cyber attacks, and to ~~unauthorize~~ access. In cryptography is an user is access into a industry (or) organisation. is requires the main Identity like, Host-Based, Signature-Based, Access-Based, and also secure the integrity, confidentiality, Accountability.



3a) Intrusion Detection Systems (IDS) is a tool to design the for sensitive data to ^{detect} ~~monitor~~ and assessing the data from cyber attacks, and threats. And not only that is also detection traffic in network to find the risks.

In Intrusion Detection ^{System} Systems help to detect the ~~malware~~ ^{malware} attack in system and find unauthorized access, & various threats it help organizations maintain data security and also secure information the ~~firewalls~~ ^{firewalls} etc.



Intrusion Detection System is detecting attack & to secure the information, data security, for an organization. ✓

35A) Physical Security

Physical security involves major role in industry (or) organization to protect information data, ~~from~~ from a unauthorized access, users, and attacks.

physical security measure ~~to~~ to create password and access card to secure the data for an organization. not only that, it also checks ~~the~~ the surveillance (CCTV)

For example: physical security like Biometrics, Face Ids, ~~eye~~ retina (eye), ~~pa~~ Access cards. those are ~~the~~ security to protect information and data which also not allows unauthorized user in the organization and building.

Physical security creates a barrier to check the end-to-end entries in an organization.

(Physical security)



company (or) Industry
(or)
organization



Security



~~the~~ Biometrics



Access cards



check points



Barriers.

Section - B

1A) Security Mechanisms

Security mechanism is used to protect the sensitive data. from attacks. It plays main role to safeguard the integrity, ~~and~~ of an organization and create guidelines from the data to protect. Security mechanisms indicate the access controls, detecting attack through system, and to measure to protect the information. In security mechanisms ~~to~~ indicates different strategies to secure the data. Such as:

Access controls

→ It the access the list of data to assess from guidelines and control the ~~system~~ in same time.

→ It also stops the ~~user~~ user from an organization.

→ Role-Based Access controls (RBAC) is major one to detecting threat Firewalls:

→ Normally firewall are stops traffic from network, and create barrier, ~~and~~ gates to stop the attacks.

→ It also detecting threat to protect the data ~~for~~ from an attackers

→ It finds the proxy-firewalls to prevent the unauthorized access.

Intrusion detection system:

It detection insecure data and network to stop attacks ~~to~~ from an industry. not only also allocated, gate to prevent measure solve problem.

→ "Intrusion detection system (IDS) and Intrusion prevention system (IPS) these are ~~may~~ the security

Strategy to assessing risks controlling and mitigating threats and try to manage data to keep it secure.

To mitigate the attacks from unauthorized access and also it conducts from an organization to test its information systems and network defense. to establish user identity is legitimate, and also mitigate the traffic on the network and find data signature, to Access control the data through an organisation.

Additionally Security Mechanism is ~~used~~ assess a ~~positive~~ ~~information~~ ~~system~~ security information and Events mechanism (SIEM) system to prevent the data, and create the tools to help to data should be secure.

Overall, Security mechanisms is create update, on the system and player to protect it data for an organisations.

Security
Risk Mechanism

- Encipherment
- Data integrity
- Data Signature.
- Traffic padding.
- Normalization
- Fire walls
- Access control

2A) Risk Management:

Risk Management assesses a system and detecting risk from various directions and to prevent threats, it implements strategies for controlling and mitigating the risks of cyber attack and threat, unusual activity. Risk Management can identify threats, Evaluation, Control strategies.

Risk Identification

→ It identifies the ID's of attack to prevent risk and also find where attacks happen.

→ Identify to inform the organisation about threats and attacks on the data.

Risk evaluation

→ It values the quantities and qualities of attacks and also finds the attacks through data security.

Risk Control strategies:

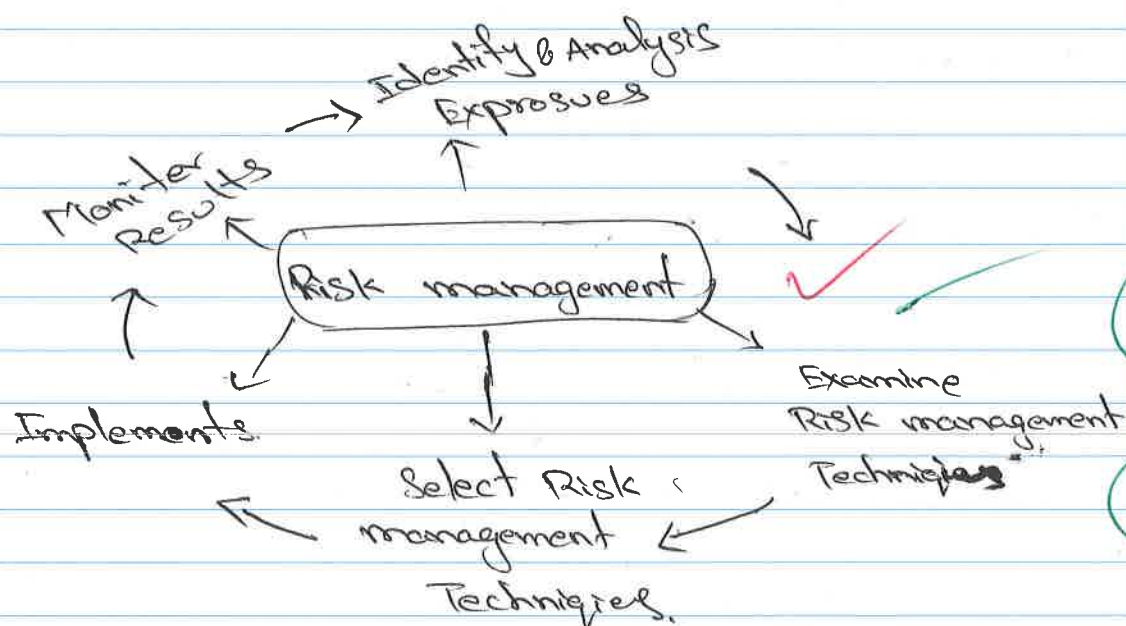
→ It creates strategies to control the data and information from an organisation not only that, it also risks Risk to an organisation.

→ It also focuses to work on every part of organisation data and proper.

Additionally → Normally organisation often transfer their data through cyber security insurance and (or) deals the third party vendors to access their data. in this case sometime data should be misplaced and go to unsecure people.

hands. so that every organisation always every potential threats to secure there information attacks.

Overall - Risk management design the guidelines to protect data and information, sensitive data to and also mitigate in different strategies for controlling the attack from, so these are major in data security and identify and assessing to secure the data from risks



4a) Security Management Models and Practices:

Security management model and practices are try understand, threats, attacks, to prevent weakness and strengths. In security management model and practices are main uses to safeguard the organization from threats.

In organization there are many of models are to prevent to give security. But some point view these are major model follow in present organization.

1) ISO 27001

Advantage: create guidelines framework, high standards informations, to assign the information from organization.

Disadvantage: lack of framework, detecting threats to late secure.

2) NIST cyber framework

Advantage: ~~Too~~ It framework focus on business protect data, facing high level risk and assigned to organization.

Disadvantage: Complex for smaller organization, effectively to industries.

3) COBIT (Control objective and information and Related Technologies)

Advantage: Control the wide range data, protect information from any kind attacks.

Disadvantage: Require documentation for every work.

1) Zero trust model

Advantage: It is traditional secure ~~the~~ level data to security and management the trust from the user and devices.

Disadvantage: Complex to organisation, cultural way change infrastructure in other industry

2

②

Several model and practices require to secure to manage every data from organisation and also manage data. ~~like, on a~~ In security management there main focus like, risk, tolerance, growth and depth of organization addressing threat to an organisation.

2

①

2) Assessment of measure

- * Scalability and Feasibility
- * Resources
- * Risk management
- * growth and depth

✓

✓