

Section A.

- |          |          |                        |
|----------|----------|------------------------|
| 1. D     | 12. D    | 23. <del>10/10</del> A |
| 2. C     | 13. D    | 24. False              |
| 3. B     | 14. A    | 25. C                  |
| 4. C     | 15. D    | 26. A                  |
| 5. C     | 16. True | 27. B                  |
| 6. A     | 17. C    | 28. D                  |
| 7. False | 18. D    | 29. B                  |
| 8. C     | 19. C    | 30. D                  |
| 9. D     | 20. B    | <del>21m</del>         |
| 10. A    | 21. D    |                        |
| 11. B    | 22. A    |                        |

31. Within the context of data security compliance refers to adherence with laws, legislation, and guidelines around the storage, transmission, and processing of data. Compliance ensures not only legal and ethical practice but also prevents data breaches, instills confidence in stakeholders and clients, and prevents legal trouble and damage to reputation.

32. Cryptography is fundamental to preventing access to sensitive information by unauthorised parties. It utilises algorithms and keys to encrypt data and make it un-readable. Authorised parties are then able to use keys to unencrypt the data and utilise it properly. Cryptography is essential in maintaining data confidentiality and security during storage and transmission.

33. 'Information security policy' is a set of expected rules or behaviours to be followed by employees as set out by governance. Policies ensure that employees are able to understand how organisation wishes them to act. A comprehensive Information security policy should include the outlining of clear roles and responsibilities, clear lines of command, and integrate principles that work to meet overall organisational goals.

34. 'Intrusion Detection Systems (IDS)' are a security component that monitor network and system activities for unusual activities or specific attack signatures. Once <sup>such</sup> activity is detected, they notify administrators who can then act swiftly and appropriately to prevent or mitigate damage.

35. 'Physical Security' refers to the protection of physical assets such as buildings, personnel, or paper documents ~~that~~ from damage. One example of a physical security measure is the use of security cameras in an area in which sensitive documents are held. This could aid in detecting unauthorised access and in providing evidence in the case of a security breach.

# Aaron David ACCA7028 exam.

## Section B.

1. ~~Secure~~ Once the risks to organisational <sup>data</sup> security have been established, the implementation of security ~~measures~~ <sup>mechanisms</sup> is essential for their detection, prevention, and overall management. A diverse range of mechanisms are needed, each dealing with specific security issues. In this essay I will outline the use of some of the most fundamental.

Likely the most common security mechanism in data security is the use of Access Controls. This involves the use of authorisation, the allocation of certain access and privileges to personnel in specific roles to certain data systems, and the use of authentication, the process of checking ~~that~~ <sup>if</sup> the person attempting to access data ~~has~~ <sup>and what they have</sup> permission to do so, through the use of methods such as biometrics or passwords. Access controls ensure confidentiality and integrity of data by ensuring only those authorised to do so can access data.

Another widely used security measure is the use of firewalls. Firewalls are generally the first line of defence against external threats. They monitor and filter network traffic, using a predetermined set of rules, and prevent network access to unauthorised parties who violate the rule set. This ensures that malicious actors are unable to violate the organisations network and access sensitive information or cause damage.

Intrusion Detection systems <sup>(IDS)</sup> are a mechanism that work alongside firewalls. IDS monitor network and system activities for unusual behavior or specific attack signatures. Notifying administrators if any are detected, Personnel can then act swiftly to prevent or mitigate damage caused by the potential threat.

A final mechanism that I would like to discuss is the use of antivirus software. Antivirus software is used ubiquitously across the field of data security to prevent virus access to systems, or detect their presence. Regular antivirus scans can ensure that malicious actors are prevented in infecting systems and damaging data confidentiality, integrity and security.

continued)

In conclusion, the use of these measures across organisational networks, and their regular monitoring and updating is instrumental in organisational data security.

2. Risk management is a pivotal part of creating and maintaining an effective and comprehensive security strategy.

The first step in risk management is the identification of the risks that an organisation faces. This can be divided into threat detection and vulnerability detection. Threats refer to things such as attacks by malicious hackers, or negligence by internal personnel. Vulnerabilities are the things that facilitate the potential for threats, such as out of date software which lacks security, or weak passwords.

Once risks have been identified, they must be assessed. The assessment of risks involves evaluating the likelihood that a risk will take place, and the potential damage that it could then cause. This process is essential in order to prioritise risks, and the resources that are allocated to manage them. This is a complex process but if done correctly can protect the organisation while also dealing with resources efficiently.

The next step is to implement measures to combat risks. These measures can be preventive, detective, or corrective. Preventive measures aim to stop the risks from ever taking place, an example being the use of firewalls to prevent access to an organisation's network. Detective measures monitor networks, systems, and assets in order to detect potential security events and then notify personnel who can then act to stop or mitigate damage. Finally corrective measures involve taking steps to enable recovery in case of a security event such as data backups, or the use of redundant systems to ensure business continuity.

A final but crucial part of risk management is its continuous and comprehensive monitoring and maintenance. Risks are always evolving and organisational context

## 2. Continued...

...is always changing. therefore risk management is an ongoing process.

In conclusion, ongoing and thorough risk management is pivotal in establishing an effective and comprehensive security strategy.

4. The use of information security models is core to the development of an effective and comprehensive security strategy. They offer specific ~~frameworks~~ and guidelines and frameworks that allow an organisation to build on a foundation of verified and actionable knowledge compiled by experts in the field of security. In this essay I will discuss three of the most widely used in modern data security; ISO 27001 standard, NIST cyber security framework <sup>(NIST CSF)</sup> and COBIT.

ISO 27001 is a security standard that forms a core part of the ISO/IEC 27000 series. It is an internationally recognised guide for the design and implementation of an Information Security Management System (ISMS). Widely seen as a gold standard for security, the standard is comprehensive and highly structured, covering specific actions that organisations must take to reach ~~ISO~~ the series' high standard. A primary advantage and attraction of the standard is the fact that it offers certification, meaning that an organisation that meets all of its requirements can be verified as ISO/IEC 27000 compliant. This instils great confidence in stakeholders and potential clients, due to its reputation. While its thorough nature is a benefit, it also comes with disadvantages. Implementation of the standard is a long and arduous process ~~that~~ and certification must be reassessed regularly. This requires a great deal of resources and commitment from an organisation.

NIST CSF on the other hand is a highly flexible framework for cybersecurity that provides guidance on risk assessment, organisational profiling, ~~the~~ the implementation of controls, and compliance, and much more. It is highly tailorable to an organisation's...

#### 4. Continued)

... Specific context. Mandated originally by the US government for use by organisations critical to federal infrastructure, NIST is most commonly used in the US and offers a route to ensuring compliance with many standards set by US Federal bodies. ~~Like~~ Unlike ISO 27001 NIST does not offer certification, therefore while being easier and less resource intensive to implement, does not ensure standards are met. / COBIT is a model that focuses mainly on organisational governance, and the creation of a holistic approach to organisational processes that integrates core organisational goals into all aspects of the organisation. ~~The~~ <sup>the</sup> Security strategy should always work towards reaching, or at a minimum not hinder an organisation, in reaching ~~an~~ <sup>its</sup> organisations main goals. ~~Therefore implementation~~ COBIT takes a organisation wide approach to data security that can be vital to an effective security strategy. However due to its lack of specificity and very high level approach to security, it must be used alongside other models.

In order to select security management models and practices an organisation must thoroughly assess its context. For large international organisations, implementation of ISO 27001 and certification ~~may be worth~~ <sup>and</sup> the security assurance ~~and~~ <sup>and</sup> recognition ~~and~~ <sup>and</sup> may outweigh the high resource cost that comes with it. An international organisation may also be drawn to ISO as certification would mean that you are likely compliant to many international laws and regulations. For smaller organisations, particularly those in the US, NIST CSF may be adequate and potentially preferable due to its flexibility and ease of implementation compared to ISO 27001. The major disadvantage being that a lack of certification does little to instill confidence in stakeholders and potential clients. COBIT should be useful to all organisations in establishing a holistic approach to security that ensures synchronicity between governance, management, and security.

To conclude, there are a myriad of costs and benefits to consider when choosing models. They must be assessed based on the organisations specific needs and context.