

31)

Compliance

This term covers the practices, guidelines and procedures required to fit security regulation, security standards of the industry, laws and guidelines to protect sensitive data.

Its essential for organisations because the lack of its implementation can lead to punitive actions as result of no accomplishment of legal obligation, loss of reputation, as result of loss of trust in the organisation and also implies the implementation of good practices regarding risk management.

32) Cryptography:

The cryptography in data security covers the practices that allow the encryption and decryption of sensitive data in storage or communication. It implements the use of private and public keys to apply the encryption and decryption processes either in synchronous or asynchronous approach.

It allows the feasibility, integrity, and security in communication as well as authentication and non-repudiation, which allows to attach a piece of data to a particular origin or source.

33) Information Security Policy:

An Information Security Policy is a set of rules, guidelines and procedures that apply within an organisation in order to maintain a protect data storage, communications, and prevent information security threats.

An ISP should include:

- Behaviour rules, to ensure that end users apply best security practices.
- Access controls, defining who, how, what and when data can be accessed.
- Contingency plans for risk mitigation and Business Continuity.

34) Intrusion Detection System:

An IDS is implemented in order to monitor analyse and evaluate security breaches and threats in the network. It allows organisation to prevent intrusions and external threats by detecting in advance any attempt of non desired access or cyber attack to the systems used by an organisation, including data storage and communication systems.

35) Physical security

The term physical security covers the implementation and application of physical security measures that rely on physical structures and approaches to control access to sensitive ~~data~~ and assets.

An example of Physical Security measure is the use of ID cards or biometric controls to access specific resources.

Section B:

1. Security Mechanisms.

In data protection multiple security mechanism ~~can~~ be implemented.

The term security mechanism ~~cover~~ all the measures applied within an organisation to ensure data protection and the alignment with compliance and best security practices and behaviours.

This can be achieved through the implementation of multiple practices:

- Access Controls, allow to define who can access different levels of security data protection by defining when, how and why a particular set of data can be accessed in particular circumstances.
- The use of firewalls allow to set the rules and constraints to data transmission and traffic either within an organisation or to external networks. These rules are defined in sets of inbound and outbound rules that allow to implement permissions to access defined ports by defined IPs using different protocols.
- IDS are used to monitor, watch and evaluate non desired access to the organisations network and preventing it from cyberattacks. It is applied through different detection systems, as can be the monitoring of traffic and request, the attempts of log in or failed attempts of data decryption.

2). Risk Management:

The Risk Management is applied in order to evaluate and analyse security risks and threats, and to ensure the implementation of the best security practices to fit Data Compliance rules and laws as well as to allow the correct implementation of data protection.

Different strategies can be used to identify and assess risks as can be the performing of periodic penetration tests, the continuous monitoring of the network resources and communications and the implementation of Intrusion Detection systems through threat alerts.

The evaluation of security policies implemented by other organisations in the past, also called benchmarking, it is also a valuable method for Risk analyse and management implementation.

An essential part of Risk Management procedure is the implementation of Contingency Plans to ensure disaster recovery, and Business Continuity and effective timely response periods when addressing security breaches.

This can be achieved by the application of various elements as employee training and awareness (SETA) to ensure that the members of an organisation are ready to deal with security threats and to implement good practices to prevent from security failures.

Another important element of Risk Management is the state and implementation of Recovery and Contingency Plans to allow organisations to maintain business continuity.

4) Security Management Models:

A Security Management Model is a security framework provided by an institution to set a standard of information security practices and procedures in the industry.

One of the most recognised SM is the ISO 27001 ISMS (Information Security Management System) model which provides a widely accepted internationally security framework that allows organisations all across the world to share common security rules and standards. This model is widely used and accepted and covers different Information Security elements allowing to fit different security and data protection laws and approaches.

Another widely used ~~IS~~ ISM is the NIST (National Institute of Standards and Technology) model which is a well accepted standard of information security in the U.S. This framework covers a wide range of information security practices and procedures that fit US regulations.

An advantage of the ~~ISM~~ ISMS over the NIST model is its scalability, making it more suitable ~~of~~ for organisations willing to spread internationally as it allows to fit different law frameworks and regulations.

In the other hand, the NIST is less complex, therefore more easy to apply and implement, being more accessible for small organisations that need to fit the US standards and regulations.

Hammade Ballale Ebbi 2308208

Level 7 January 2024 Module Code: ACCA 7028
Data Security, Governance and Compliance.

Section A:

- 1/ D. Authentication
- 2/ C. Intellectual property
- 3/ B. Penetration Tester
- 4/ C. Polymorphic Threat
- 5/ B. Leading
- 6/ A. End-user license agreement
- 7/ False
- 8/ D. Watchstanders.
- 9/ D. Global Information security Officers
- 10/ A. Framework Design
- 11/ B. Risk Analysis
- 12/ D. People, Process and Technology
- 13/ D. Risk Control Plan (RC)
- 14/ A. Termination
- 15/ A. Confidential Data
- 16/ False
- 17/ C. Polygraph Test
- 18/ B. Two-Person Control
- 19/ C. Alert Roster
- 20/ B. Disaster Relief Plan
- 21/ D. Remote Journaling
- 22/ A. Difference Analysis
- 23/ D. Remote Journaling
- 24/ False
- 25/ C. DMZ
- 26/ A. Public Control of NI
- 27/ B. VM PM
- 28/ D. Expunge
- 29/ B. ACL
- 30/ D. Critical Path