



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

1.	Student Number / Rhif Myfyriwr	0151968
2.	Title of Exam Paper / Teitl y Papur Arholiad	Data security, governance and compliance
3.	Module Code / Cod y Modwl	ACCA7028
4.	Date and Time of Examination / Dyddiad ac Amser yr Arholiad	07/01/25 9.00 am
5.	Examination Venue / Lleoliad yr Arholiad	T&L2

Section 1, Question 2 - 40

Section 2, All questions - 59

99

Please Complete and Fold this section after your paper has been printed by a member of the Registry Staff
A wnewch chi lenwi' r rhan hon a' i selio wedi l aelod o Staff y Gofrestrfa brintio eich papur

Surname / Cyfenw REES (BLOCK CAPITALS / LLYTHRENNAU BREISION)

FOLD / PLYGWCH

Forename (s) / Enw(au) Cyntaf SIMON TUDOR 5/2/25

Section A

Question 2

Issues identified at Nature Garden(NG)

Security Policies:

The three security policies for an organisation to implement as advised by the National Institute of Standards and Technology are:

- Enterprise Information Security Policy (EISSP)
- Issue Specific Security Policy (ISSP)
- System-Specific Security Policy (SysSP)

- Enterprise Information Security Policy (EISSP)

This sets out the information security philosophy the organisation will undertake and sets out the direction, scop and tone for an organisation's security efforts.

- Issue Specific Security Policy (ISSP)

This policy sets out how staff should utilise equipment at the organisation. For NG, it is key that they implement policies to provide guidance to staff on the usage of:

Social media, Email usage, Internet Usage, usage of mobile devices.

- System-Specific Security Policy (SysSP)

This policy provides guidance on the configuration of systems, this ensures that they are configured in a standard manner and meet the security requirements of the organisation.

Risk Management

This is key to an organisation's security efforts.

The definition of Risk is the intersection of Threat and Vulnerability.

A threat could be a cyber attacker, or a member of staff that has inadvertently cause an issue such as damaging a key system or deleting important information.

Vulnerabilities, these could be due to the use of older equipment, misconfigured equipment, or software/operating system that have not been updated.

Analysis of these threats can be used to determine the Likelihood of the threat against its impact.

See Fig.1 on the Exam paper.

A Threat Vulnerability Assessment (TVA) can also be conducted that will provide analysis of every threat in relation to the vulnerability. Providing the Information security (InfoSec) team with a information on which systems and Vulnerabilities that need to be resolved first.

It is then possible to score each of these assessments to provide a prioritised list of systems that need to be remediated first.

Risk Management strategies:

Conducting regular vulnerability assessments is key to identify these weaknesses so that they can be remediated, mitigated or removed entirely. Implementing preventative controls measures such as

Deter

Security Management models and practices

International Standards Organisation (ISO) 27000 is a suite of over 50 Security management models and standards that an organisation can implement. These standards are designed to work together.

ISO 27001 Provides guidance on Security for systems: This

ISO 27002 Providing guidance on how Implement Security Controls

ISO 27005 Risk Management

Cloud Security Alliance (CSA) Cloud Matrix Model (CMM)

This provides guidance to an organisation on how to configure their cloud infrastructure to secure it from cyber-attack.

NIST Cyber Security Framework (CSF)

The NIST CSF is designed to provide guidance on dealing with incidents. The CSF process followed is below:

Identify, Protect, Detect, Respond, Recover.

Information Technology Information Library (ITIL)

This provides organisation with guidance on service delivery (SD), setting guidance on Service Level Agreements (SLAs), providing targets for incident resolution and response times.

Following ITIL principles an organisation should become more efficient, reducing costs, and improve customer satisfaction.

COBIT 2019

This provides an overall single approach to data governance and is designed to work with other frameworks.

Contingency planning

Contingency Planning consists of the following:

Business Impact Analysis (BIA)

Incident Response (IR) Plan

Disaster Recovery (DR) Plan

Business Continuity (BC) Plan

Crisis Management (Plan)

Contingency Planning Management Team (CPMT) conducts the BIA, and forms the following teams:

IR Planning Team (IRPT)

DR Planning Team (DRPT)

BC Planning Team (BCPT)

BIA is the first process of the CP. According to NIST guidance the three steps procedure to implement is:

- Determine the Business/Mission process and system criticality
- Identify the resource requirements
- Identify the recovery priority of system processes.

The seven step process of conducting CP is.

- Develop the CP policy statement
- Conduct the BIA
- Identify preventative controls
- Create the contingency strategies
- Develop the contingency plans
- Ensure plan testing, training, exercises.
- Ensure plan maintenance.

The Teams involved in the CP are:

Contingency Planning Management Team (CPMT) are a group of senior managers and project leaders that lead on all security efforts at an organisation.

The CPMT Roles:

Conducts the BIA

Develops the CP policy statement

Develops the policy environment

Forms the IRPT, DRPT, BCPT.

Incident Response Team

An incident is an adverse event that impacts systems, with possible loss of data, but the organisation can still function.

The incident Response team resolves issues such as:

Viruses, system failure issues such as power supply failure, user error issues or deliberate attacks, such as a Denial of Service Attack.

An Incident is a adverse event that still allows an organisation to function. A process known as Incident Classification is used to determine if the incident is an actual incident see Fig.2

Incident indicators include

Possible Incident: e.g. Unexpected System crashes

Probable Incident: e.g. Reports from User

Definite Incident: e.g. Presence of Hacker tools, Notification from Hacker, Used Domain Account.

Incident Results:

Loss of Confidentiality, Integrity, Availability or Violation of Law or Policy.

IRPT Roles

Prepares for an incident

Develops and maintains the IR Plan

Forms the Computer Security Incident Response Team (CSIRT)

CSIRT Roles:

Executes the IR Plan

Detects and responds to and recovers from an incident

Conducts After Action Review (AAR)

Disaster Recovery (DR) Team:

The DR team respond to disasters that are adverse events that impact the whole organisation. Examples could be flood or fire. The DR Teams main aim is to reestablish business functions at the primary site following a disaster.

DRPT Roles:

Prepares for disaster

Develops and maintains DR Plan

DR Plan provides guidance on reestablishing business function the primary site or a new primary site

Forms the DR Response Team (DRRT)

It is crucial for DR Plans to be tested and rehearsed as this improves reaction times.

Identifies any gaps in the Plans, provides response teams with time to become familiar with plans, provide feedback to plans so that they can be updated and improved.

DRRT Roles:

Detects, Responds to a disaster

Reestablishes business functions at the primary site

Business Continuity (BC) Team

This is closely related to DR; the main difference is that the BC team recovers the system functions at an alternate site. This ensures the mitigation of the disaster to the organisation as they can still conduct business at the alternate site.

BR Planning team BRPT):

Prepares for disaster

Develops and maintains BC Plan

BC Plan provides guidance on reestablishing business function alternate site

Forms the DR Response Team (BCRT)

BC Response Team (BCRT):

Reestablishes the business function at an alternate site:

Hot Site: A location with all systems and data in place with connectivity. A replica of the primary site.

Warm site: A location with some systems but the most recent data will not be available.

Cold Site: A location with no systems or data in place.

Crisis Management (CM)

This is the process where a disaster has occurred, the CMs main responsibility is to personnel, the public and ensuring people are safe and kept informed of developments.

The CM Planning Team (CMPT):

Develop and maintain CM Plan

Verify Personnel Status

Cooperate with Emergency services

CM Response Team (CMRT)

Supporting Personnel and loved ones

Contacting major customers, partners, suppliers, media

Informing public

Responding to an incident.

The NIST Special Publication (SP) 800-61 outlines the process to use when responding to an incident. It outlines the Incident Response Lifecycle, See Fig.3

Once an incident has been detected, for example a virus, it is crucial for that virus to be contained. The containment strategies that can be used are:

- Disable compromised user account
- Modify firewall rules to stop malicious traffic
- Disable system processes or services
- Disable network or network segment
- Power off equipment

Examples of containment

- Disable compromised user account

This is crucial as the attacker would have the access to the systems or services that the account holder would have. Compromising Confidentiality, Integrity and possibly availability if they delete data.

- Modify firewall rules to stop malicious traffic

If a particular vulnerability were present on a system, such as with the Simple Network Management Protocol, an attacker could exploit this vulnerability. Therefore, it would be possible to disable the traffic to that server from the attacker, providing time to the CSIRT to resolve the vulnerability.

- Disable system processes or services

Using the SNMP example above, another method would be to disable the service on the device itself. This would allow the CSIRT team to resolve the issue, but the attacker would still be able to access the server.

- Disable network or network segment

If a virus had been discovered on a PC, then disabling a network or network segment would be an option to ensure that the virus does not spread to other PCs. Mitigating the risk to other devices on the network.

- Power off equipment

This is the most drastic containment strategy but could be the only option if a crypto malware were detected. This would stop the malware from encrypting data. But would also mean a severe impact to the organisation until services are resumed.

Protection Mechanisms

The three states of data are:

1. Data in Transit
2. Data in at rest – in storage (saved)
3. Data in Use.

Next Generation Firewall, this system can

Data Classification, using Confidential, Top Security on data will highlight their sensitive nature.

Data Loss Prevention (DLP) this is used in conjunction with Data Classification and can detect and stop documents being transmitted with "Classified" to entities outside the organisation.

Intrusion Detection Prevention System (IDPS). This system is able to detect, alerting the InfoSec team or prevent intrusions automatically.

Wireless Infrastructure:

As Wireless is a shared medium, it is not secure in itself. It is necessary that additional measures are implemented to provide security.

Authentication:

Ensure the Institute of Electrical and Electronic and Engineers (IEEE) 802.1X authentication is implemented on both wireless and wired networks.

This can be used to authenticate a user, and place that user on the correct Virtual Local Area Network (VLAN).

In relation to NG, this would allow staff to be placed on a VLAN that will grant them access to systems and services required for them to carry out their role.

Wireless Access Points (WAPs) can also utilise the 802.1X authentication, ensuring that only authorised WAPs are connected to the network.

If a guest were to attempt to authenticate, they can either be blocked entirely, or if NG wishes they can be placed on a Guest VLAN providing them with basic Internet access.

Confidentiality:

Implementing a Virtual Private Network Infrastructure such as Internet Protocol Security (IP Sec) would provide confidentiality as the data will be encrypted. Therefore, anyone attempting to intercept wireless traffic will not be able read or amend data in transit.

This will mitigate against a hacker connecting to the wireless network and attempting to access NG systems.

Full Disk Encryption (FDE) – This will ensure the data is secure while at rest. So that if a laptop is stolen the data itself will remain confidential.

Wired Infrastructure.

NG utilise 95% of its infrastructure is wireless. As stated above this is not a secure medium. It would be advisable to implement a wired infrastructure with Wired PCs so that sensitive data such as Intellectual Property is contained within the organisation's infrastructure.

Service Level Agreements (SLA)

SLAs are an agreement between a customer and supplier, to set out the level of support and services.

Section B

1 T ✓

2 D ✓

3 C ✓

4 B ✓

5 C ✓

6 B ✓

7 C ✓

8 A ✓

9 C ✓

10 B ✓

11 D ✓

12 D ✓

13 T ✓

14 A ✓

15 C ✓

16 B ✓

17 T ✓

18 B ✓

19 A ✓

20 D ✓

21 D ✓

22 F ✓

23 A ✓

24 D ✓

25 A ✓

26 B ✓

27 T ✓

28 C ✓

29 A ✓

30 B ✓

31 C ✓

32 T ✓

33 D ✓

34 C ✓

35 D ✓

36 B ✓

37 F ✓

38 D ✓

39 A ✓

40 C ✓

41 C ✓

42 F ✓

43 D ✓

44 B ✓

45 C ✓

46 T ✓

47 B ✓

48 D ✓

49 D ✓

50 D ✓

51 F ✓

52 C ✓

53 D ✓

54 A ✓

55 D ✓

56 Confidentiality, Integrity, Availability ✓

57 Policy ✓

58 Benchmarking X