



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 ignore illegible 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: Sunil

FORENAME(S): Ajay

1	Student Number	2406774
2	Title of Examination Paper	Data Security Governance and Compliance
3	Module Code	ACCA7028
4	Date and Time of Examination	JANUARY 2025 9:00 am
5	Examination Venue	SWANSEA
6	Seat Number	011
7	Number of Answer Books handed in	

List the numbers of the questions you have attempted	Office Use
Sec 1-Q2	30
Sec 2	27
Total	57

SECTION A

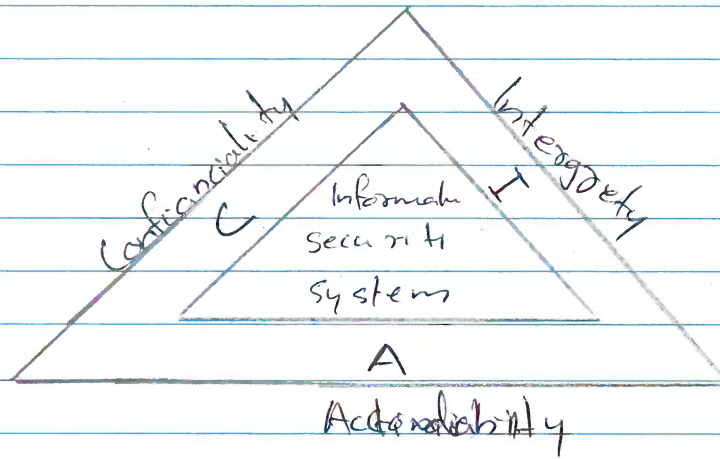
1,

- a) The Information Security system which is used to protect from unauthorised access from the system. Moreover it is reduce the risk from the third party application and misfiles from the internet.

There are four type of Info Sec process

- i Identification : Identification is the process which identify the User, for instance the User and login id is checking is it correct or not.
For example, Login id in a User and the password when its correct. Then the login access is granted.
- ii Authentication : The security process is called authentication. There are different types of authentication such as password, two-factor Authentication and Security Code. which are used to tight the privacy and security.
- iii Authorization : The authorization means the organization is to test the information system to check wheather its correct or not from the verified Authorization. For example numerous sites are available on the internet also application is it to check authorized or unauthorized from the site.

- iv Accountability means the information security process which is used for prevent the unfraud activity with the system. For example the money management like transferring money to the secure application process.

b₂

The CIA triad is a security system which is used for stronger the security for an Authorization, like Bank and hospital etc. The Confidentiality is used for make sure the privacy and security of the company. For example, HR manager, Employers etc.

The Integrity is the Company policy information is manager very fast and easy with the Company employers without any mistakes.

m

23

2, Nature Garden is one of the biggest brand in the world. The Company is very famous and high presence around the globe. Now the Company facing some security problems and threats. Using the high security features and analyzing the problems is to be increase the security of the Company.

The CIA is one of the main element of the Company to protect the information and policies moreover to secure the information tightly.

The 27001 Security Framework is a great thing to protecting the factors from the Company and CISCO and CIO is important factors in the Information Security.

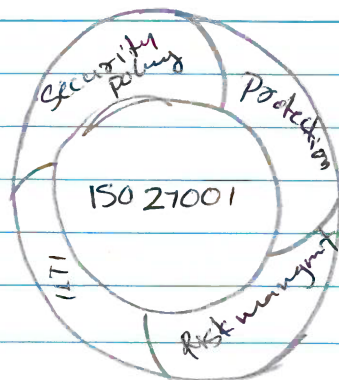
The Security policies is one of the important factor to be consider as a Company such as CIA and the Identification, Authentication, Authorization and Accountability.

The Security policies is very important for a Company. Because so many data and information are going and managing the Company so the security policies is highly confidentiality which is only authorized by the Company managers and high level employees.

Risk management have important role. Because Natural disaster and Human kind disaster, Non kind disasters are happen anytime. So the risk management is ~~to~~ ~~recollect~~ the always prepared to ~~to~~ protect the data and recollect the data from a disaster when it is happened.

The Natural disaster like Earth quick, Swenami and other things. So it is important to be manage the risk at anytime.

Security Management Model and practices. The security management process is used to secure the Information Security from the management. The CIA and 2000 and 27001 is one of the main security models. Moreover that the security is highly recommend the company to get the information which is always keep in the authorization.



The protection Mechanisms is highly practicable in the Company and the Security Features. which is highly Consider the protection ways of the Company which lead the Company policy to get a good protection.

Protection from ~~virus~~ Malivirus

~~virus~~
 worm
 dogenhorse
 antivirus
 advirus

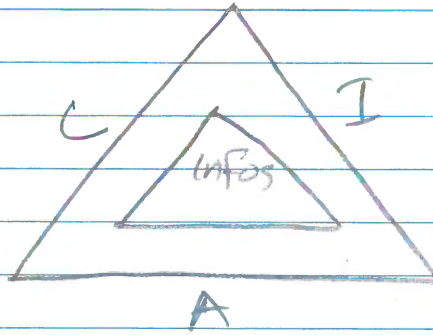
Virus which is come from a file ~~with~~ which is spread all over when the file is installed

worm - is a virus which is installed through the online which is dangerous

antivirus is one which is spread the system

Advirus is highly danger to follow the ad to the Customer and following their data.

(30)



SECTION B

- 1, True ✓
- 2, Accountability +
- 3, Competitive intelligence +
- 4, Penetration tester ✓
- 5, Polymorphic treat ✓
- 6, Controlling +
- 7, Objective ✓
- 8, Leading X
- 9, Technological Feasibility +
- 10, Enterprise Information Security Policy X
- 11, Descriptive Ethics ✓
- 12, ~~Electronic Communication~~ Privacy Act (ECPA) ✓
- 13, False X
- 14, Public Control of medical Information ✓
- 15, Hospitals ✓

- 16, Network monitoring and testing +
- 17, True ✓
- 18, Jurisdiction ✓
- 19, ~~Computer Fraud~~ PATRIOT Act ✓
- 20, Analyse the data. ✓
- 21, Values statement +
- 22, False ✓
- 23, Infosec planning +
- 24, An individual or group who has a vested interest ✓
- 25, Mission statement +
- 26, ~~Mid-Level manager~~ initiating +
- 27, True ✓
- 28, Mid-Level Managers ✓
- 29, Monitor ✓
- 30, Lack of stakeholder support X

- 31 System-specific security policy X
- 32 True ✓
- 33 Delete X
- 34 It contains an issue statement X
- 35 Enterprise Information Security policy
EISP X
- 36 Rule-based policies X
- 37 True X
- 38 Investigation phase X
- 39 End-user terms of use agreement X
- 40 Performing a risk assessment ✓
- 41 Security analyst ✓
- 42 True X
- 43 Security technicians X
- 44 CISSP ✓
- 45 More than 100, less than 1000 ✓

46

True ✓

47. Certified Information Systems Security Professional ✗

48. They enable the organization to hold employees accountable ✗

49. Critical Path ✓

50. Security Education ✗

51. True ✗

52. Enterprise Risk Management ERM ✓

53. ~~Framework~~ Executive governance and Support. ✓

54. Risk management policy developers ✗

55. Pilot test ✗

56. CIA ✓

57. CISO ✗

58. CIA ✗