



UNIVERSITY OF JOHANNESBURG
FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: IT28X80/IT8X299
INFORMATION SECURITY GOVERNANCE

CAMPUS: APK

EXAM: SSA JANUARY 2020

DATE 2020-01

SESSION 08:30 – 10:30

INTERNAL EXAMINER

Dr J du Toit

EXTERNAL EXAMINER

Prof M Loock (UNISA)

DURATION 2 Hours

MARKS 100

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 3 pages

QUESTION 1 (Information Security Governance Model)**[30]**

The Utopian Space Agency (USA) is a space tourist company that allow citizens to take space flights to the moon and back. The USA is dependent on the health records of the space tourists to ensure the tourists' continued health during the tourists training and preparation for the trip.

New legislation is forcing the USA to re-evaluate their Information Security Governance. The new legislation states that health records of space tourists should be kept **confidential** and tourists must **provide special permission** before health records can be used for any purpose at the USA.

Discuss the impact the above legislation has on the information security governance of the USA.

Marks are awarded according to the following rubric:

Explanation.	The various levels and activities are recalled.	Same as the previous and the interaction between the levels are described.	Same as the previous and the student is using realistic examples of the artefacts and interactions in the different levels.
Possible marks.	(0 - 9)	(10 - 15)	(16 - 25)
Structure of discussion.	Unstructured set of ideas.	Student is using well defined paragraphs.	The paragraphs are focused, and the flow of the text supports the process.
Possible marks.	(0 - 1)	(2 - 3)	(4 - 5)

QUESTION 2 (Risk Management)**[30]**

The CEO of USA recently came back from a business trip. During the trip he read an article in an Airline magazine highlighting court cases where companies were held accountable for data leaks. Yesterday the CEO phoned you and the conversation can be summarised in the following few sentences from the CEO: *"I know that business risk exists, but I never realised our Information Technology systems and the way we work with information also carries risk. The new health information legislation really has me worried. Are we doing enough?"*.

You promised the CEO that you would give the CEO a **report** on the Risk Management and specifically the **impact that the new legislation** has on **Information Security risk**.

Your report should include a discussion of the following aspects (The marks associated with each aspect is displayed in brackets):

- Why Information Security Risk Management is seen as part of Information Security Management. (4)
- The components of risk. (3)
- The risk management approach applied to USA. (18)
- Style of report (5)

Exam Continues on Next Page

QUESTION 3 (Security Education, Training and Awareness)**[20]**

After implementing the directives and managing the risk created by the legislation, the Information Security Compliance Manager for the USA contacted you. During the compliance monitoring, they found that employees still did not follow procedure to apply for access to the Health Records of the space tourists.

You suspect that the lack of compliance from the users are because of their level of security education, training and awareness (SETA). Write a **high-level proposal** to implement a SETA program for USA, that specifically focusses on the **concern** of the IS Compliance Manager. The proposal must specifically state **how** you recommend implementing SETA that addresses the IS Compliance Manager's concern.

Marks are awarded as follow:

- Factual recall of Information SETA. (8)
- Application of SETA program related to the CEO statement. (8)
- Style of proposal. (4)

QUESTION 4 (Cyber security)**[20]**

The USA has recently made an exciting announcement on the Utopian news media. Since the USA stores health records of space tourists, the insurance industry has become interested in these health records. The USA has decided to expand the business offering by allowing life insurance companies access to the health records for a fee over the Internet.

After you read the statement you realised that the CEO of USA, may not understand the various cybersecurity concepts and the relationships these concepts have on each other. **Draft a MEMO** to the CEO of USA that specifically highlights the **cybersecurity concepts** and how they all **relate** to each other.

Marks are awarded as follow:

- Factual recall of the various concepts. (7)
- Identifying realistic examples of the concepts and how they relate to each other. The examples must be applicable to the given scenario. (9)
- Style of memo. (4)

TOTAL PAPER**[100]**