UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: **IT28X80/IT8X299**
INFORMATION SECURITY GOVERNANCE

CAMPUS: **APK**

EXAM SSA: **NOVEMBER 2021**

QR Access Code: 2f2783fd

DATE	2021-11-30	**SESSION**	Normal
INTERNAL EXAMINER		Dr J du Toit	
EXTERNAL EXAMINER		Dr H Abdullah	
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
4. Start the invigilator app before taking the exam.
5. **Not using the invigilator app during the exam is seen as an assessment transgression and the exam submission will not be marked**. Exams are only eligible for marking if the uploaded assessment images in Invigilator matches the uploaded submissions on eve.
6. You are not allowed to assist or gain assistance from anyone. You are only allowed to communicate with the lecturer during the assessment.
7. You are not allowed to copy text from any source and use that as your answer. All answers must be written by yourself during the assessment.

QUESTION 1 (Risk Management) [30]

UtopiaHost is a national Internet Service Provider for most government and commercial organisations in Utopia. Part of the services UtopiaHost offers are cloud services. One of the most popular cloud services used by many organisations is their hosted customer relationship management (CRM) system. The CRM system allows organisations to handle all their sales and marketing processes.

UtopiaHost has a service level agreement with a penalty clause. The penalty clause states that a customer can claim 100 Utopian Dollars for every hour the CRM system is unavailable. UtopiaHost currently has 50 customers, that this penalty clause applies. In the last year, UtopiaHost experienced several denial-of-service attacks on the cloud infrastructure that caused the CRM system to be unavailable for ten (10) days.

The CEO of UtopiaHost contacted you because they are unsure what their options are. For some reason, the IT department cannot fix the problems, and the normal risk management committee says they do not know how to manage the risk.

Answer the following questions related to this scenario

1.1 Briefly explain why Risk Management is part of Information Security Governance. (4)

1.2 Clearly identify the components of risk. (3)

1.3 Using the information supplied, explain to the CEO the process UtopiaHost can follow to manage the risk. The process must use this scenario as the basis and include risk analysis, estimation, and treatment. (18)

Five marks may be awarded if the answers are properly numbered and written in a clear and concise format. (5)

QUESTION 2 (Organisation) [30]

After several discussions with yourself, the CEO of UtopiaHost realise that they drastically need to improve the organisation of their Information Security function. UtopiaHost currently only has an IT Manager whose tasks include those of basic Information Security operations. The CEO of UtopiaHost realised that the IT department is overworked and understaffed and needs a new structure to manage the Information Security function fully.

The CEO asked you the following: “If you have a clean slate, how will you organise the Information Security function in UtopiaHost?”.

Write an email to the CEO that clearly explains how the Information Security function may function for UtopiaHost. Make sure to include recommendations that you see fit around departments, positions and working groups that must be formed. Make sure to motivate the recommendations.

Marks are awarded as follow:

- Applying the IS function to UtopiaHost (25)
- Readability and style of the email. (5)

QUESTION 3 (Information Security Governance - Arguments) **[20]**

Critically discuss each of the following statements. Critical discussions require that you either agree or not with the statement and comprehensively motivate your answer.

3.1 'Information Security is a technical issue and belongs in the IT department.' (4)

3.2 'An organisation is at a severe disadvantage without a Corporate or Enterprise Information Security Policy.' (4)

3.3 'Information Security Policy statements that cannot be measured is not worth the paper it is written on.' (4)

3.4 'An organisation will always be reactive in its Information Security approach if there is no proper Information Security Awareness programme.' (4)

3.5 'The CIS Controls framework is extremely difficult to use for Information Security planning purposes' (4)

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

After an extensive Risk Management exercise, the following risks have been identified and listed on the risk register.

Risk Number	Description	Risk Level
R16	At this stage, the recovery time of various IT systems is unknown. No formal disaster recovery tests have been performed on individual systems.	High
R18	There is no single repository that stores information about all the software systems in the organisation.	High
R21	Ad-hoc vulnerability scans show that there is no managed vulnerability scanning occurring in the environment.	High
R22	There is no central authority that can be contacted in case of an information security incident.	High
R33	There seem to be several unauthorised remote access points for people working from home. A fair number of remote-control software has been loaded on office computers without any centralised authentication mechanisms.	High

The NIST Framework for Improving Critical Infrastructure Cybersecurity explains five core functions that are adopted by many other frameworks.

4.1 Briefly describe each of the five functions that make up the core of the framework (10)

4.2 For each function, describe at least one activity that will improve the risk register for UtopiaHost, based on the five functions described in the framework. When describing the activity, highlight the risk item addressed by the activity and explain in which core function the activity resides. (10)

TOTAL PAPER **[100]**