UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

CAMPUS: **APK**

EXAM: **OCTOBER 2021**

QR Access Code: aa134d3c

DATE 2021-10-25 **SESSION** Morning

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 4 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 test 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 (Multi-dimension discipline) **[23]**

Yellow Cab-Taxis (YCT) is a taxi company operating in Utopia. The company employs many drivers and owns its own fleet of taxis. Historically people would have to phone YCT to arrange a taxi to drive them from one point to another. The management of YCT has decided to embrace the digitalisation of the system.

The digital product allows customers to register their details using a mobile app, including a valid credit card number. The customer can then use the app to book a ride, track the assigned taxi, and make the necessary payment. The whole system is run without any staff operating the phones. Payments are also handled by the system, minimising the risk of riding around with cash.

The CEO is very happy about the success of the new system. At a recent business conference, the CEO heard that the IT department might not have the capacity to take responsibility for all of the Information Security aspects. The CEO contacted you, hoping that you can clarify the message from the conference.

Write a memo to the CEO of YCT explaining why Information Security isn't just the responsibility of the IT department. Describe at least five (5) Information Security dimensions that are affected because of the new system. Clearly demonstrate how each of the Information Security dimensions is changed by the new system.

Marks are awarded according to the following aspects:

1.1	Describe each of the five dimensions	(10)
1.2	Describe how each of the dimensions is affected by the new system	(10)
	Style of the memo.	(3)

QUESTION 2 (Information Security Education, Training and Awareness) **[23]**

Yellow Cab-Taxis (YCT) employed a new Information Security Officer. The IS Officer is fully aware that they need a proper Information Security Education, Training and Awareness (ISETA) programme that must include the new taxi management system.

The IS Officer has approached you about how to implement an ISETA, based on the IS controls and risks surrounding the new taxi management system.

2.1	It is important to consider the Conscious Competency Learning Model (CCLM) when planning an ISETA. **Name** and **briefly describe** each of the four stages of this model	(8)
2.2	Clearly explain how the CCLM can be used to plan and implement a SETA programme that addresses the new taxi system. Clearly explain what will be done in each of the four CCLM phases. The explanation must be relevant to the new taxi management system	(12)
	Answering questions 2.1 and 2.2 in a structured and readable manner.	(3)

QUESTION 3 (Generalised attack process) **[24]**

On Friday, you received an urgent message from the IS Officer of Yellow Cab-Taxis (YCT). It seems as if they have been a victim of a coordinated cyber-attack. Without any warning, the IS Officer received an email from an anonymous person. The email claims that all the customer information, including credit card information, has been stolen and is now in the hands of cyber attackers. The email provided proof of the attack by including 100 customer records with the credit card details of the 100 customers. The attackers claim that they have all the customer records that YCT stored.

A forensic investigation showed that the attackers got access to the taxi system six months ago already. It seems as if an employee accidentally accessed a fake email site while working from home and accidentally logged in using their login credentials. The attackers used the login credentials to access the VPN system and plant a password cracking program inside the taxi management system server. The original user account did not have the necessary permission to access the customer database. The password cracking program eventually returned the login credentials of a database admin, which was used to access the customer information.

The IS Officer would like to know what process the attackers might have followed to exfiltrate the results.

Explain to the IS Officer the eight (8) phases a general attack goes through and explain what the attackers did in each phase to access customer information eventually.

Marks are awarded as follow:

- Naming each of the phases. (8)
- Describing the activities of the attackers in each of the phases. (16)

QUESTION 4 (Cyber security frameworks) **[30]**

A few months after your last engagement with YCT you receive the following email from the IS Officer

To: *isconsultant@security.co.ut*

From: *iso@yct.co.ut*

Subject: *Cyber security frameworks*

Dear consultant,

We have made great strides in enabling Information Security in YCT. One of my problems is that I do not always know whether we are doing the right things. We have limited Information Security Risk Management processes, but I would like to be more proactive.

I can remember you telling me about a "deep" approach and a "wide" approach, but I cannot remember what you told me about them.

Can you please remind me again of the difference between a "deep" approach and a "wide" approach? What are the advantages and disadvantages of these two approaches? Can you remind me again of a framework that makes use of a "wide" approach and which one makes use of a "deep" approach?

Is there a way both approaches can be combined to ensure we can get the best of both worlds? How would we implement such an approach that considers both "wide" and "deep"?

Information Security Officer

Write a reply to the IS Officer, where you address all the questions in the email. Remember that you are replying to the IS Officer. Ensure that the IS Officer can understand your response, but also so that they know you are answering each of their questions.

4.1	Critically evaluating a "deep" approach and a "wide" approach against each other. (Listing and evaluating the various advantages and disadvantages of both and weighing them up against each other)	(10)
4.2	For both a "deep" and "wide" approach, briefly describing a real-world framework and why that framework is seen as either "deep" or "wide."	(6)
4.3	Discuss how both approaches can be used to implement an Information Security programme.	(12)
	Style of email:	(2)

TOTAL PAPER **[100]**