UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

CAMPUS: **APK**

EXAM: **OCTOBER 2020**

DATE	2020-10	**SESSION**	08:30 – 10:30
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. This is an open book assessment. You may consult your notes and textbook during the assessment.
5. You are **NOT** allowed to copy from any notes.
6. You are **NOT** allowed to assist or gain assistance from anyone else.

QUESTION 1 (Risk Management) [30]

The First Utopian Bank (FUB) is one of the commercial banks in Utopia. FUB has approximately 2.5 Million customers. FUB makes use of a central banking system that keeps track of customer information and banking transactions. FUB relies absolutely on the banking system and the information it provides to conduct their business.

You have been contacted by the IT Manager of FUB to conduct an automated vulnerability scan on their network. The vulnerability scan highlighted the following vulnerabilities.

Microsoft Windows Patches Missing	
Multiple Windows patches were identified as missing from the Windows systems leaving them susceptible to vulnerabilities ranging from Privilege Escalation to Remote Code Execution. Exploitation of the most critical of these vulnerabilities could allow an attacker to gain unauthorised access to the device with administrative access. The Windows computers identified in this finding were all located inside the organisation's local area network and is not directly accessible from the Internet and runs some of the components of the central banking system.	
Impact: High	**Likelihood**: Medium
Banner information disclosure	
Information disclosure was identified within the network service banners that revealed technical configuration details. Such information could be used by an attacker to understand the software in use. Disclosed version details could allow the attacker to attempt to exploit any vulnerabilities that may be present within the installed software. At this stage, the version of the installed software did not have any known vulnerabilities. The banner information is only available from inside the corporate network and is not accessible from the Internet.	
Impact: Low	**Likelihood**: Medium

The IT Manager also informed you that the executive officers of FUB do not fully understand their responsibility towards Information Security Risk Management. The IT Manager needs you to describe how the identified vulnerabilities affect the organisation's risk and how the risk management process can work to manage their Information Security risks, given the vulnerability scan.

Write a report to FUB that will contain the following aspects around risk management. (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 the scenario of FUB. (18)
- Style of report. (5)

QUESTION 2 (Organising the Information Security Function) [30]

After your report to the board of FUB, FUB decided to increase their investment in Information Security, but the board are considering investing into more expensive firewalls. Because of the good job you did with the vulnerability scan the IT Manager asked for your help again.

You have been granted a meeting with the CEO of FUB. During the meeting, the CEO made the following statement: “I don’t understand why the IT guys cannot keep our IT infrastructure up to date with security patches. Surely all Information Security activities should fall under the IT department.”. The meeting unfortunately ended before you could respond to the CEO, but you were invited to respond to the CEO through a letter.

Prepare a letter to the CEO of FUB. In the letter propose **how** the Information Security (IS) function can be incorporated into the FUB **organisation** to improve the overall IS governance. Make sure to add recommendations on how IS should function inside FUB and if necessary which positions or departments should be created. Clearly indicate to the CEO where in the organisation the various IS functions exist and how the reporting lines would work.

Marks are awarded as follow:

- Applying the IS organisation to the FUB scenario. (25)
- Style of letter. (5)

QUESTION 3 (Cyber security threat agents) [20]

FUB implemented the organisational structures you recommended to them in your previous letter. Since then the IS compliance department have seen several IS incidents. Most of the incidents were picked up by the Internet Firewall’s intrusion detection and prevention system, but there were also a few incidents that seemed to have originated from inside the organisation’s network.

On the political stage, Utopia has had several political disagreements with one of their neighbouring countries. The political disagreements have caused the neighbouring country’s economy to suffer, because of trade taxes.

The CEO of FUB contacted you and requested your advice on understanding their exposure to cyber security threat agents.

Write a memo that identifies at most four of the most common cyber threat agents relevant to FUB and clearly explain **why** these agents are applicable to FUB.

Marks are awarded as follow:

- Describing the differences between Friendly and Hostile agents. (2)
- Identifying and describing the applicable threat agents. (8)
- Motivating why the threat agents are relevant. (8)
- Style of memo. (4)

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

A few months after your last engagement with FUB you received the following email

> ***To:*** *myfavouriteconsultant@isg.co.ut*
>
> ***From:*** *ciso@fub.co.ut*
>
> ***Subject:*** *Cyber security frameworks*
>
> *Dear consultant,*
>
> *We have made great strides in enabling Information Security in FUB. 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 a bit more proactive.*
>
> *We are currently consitering using either the Centre for Information Security (CIS) Controls or the Mitre Att&ck as a basis for a Cyber Security program that will run over the next two years.*
>
> *I am not certain which of the two frameworks are more applicable for what we want to achieve. Can you please explain the difference between the two frameworks to me, and can you explain why one framework may be more applicable than the other framework? I also need advice on how to start using the best framework for our organisation's Information Security Programme.*
>
> *Chief Information Security Officer*

Write a reply to the CISO that briefly compares CIS with the Mitre Att&ck and then highlight why you would recommend one over the other for their requirements.

Marks are awarded as follow:

- Comparing and contrasting CIS with Mitre Att&ck (6)
- Identifying and motivating why one framework is more applicable than the other. (4)
- How you recommend they use the framework to plan their IS programme. (6)
- Style of email: (4)

TOTAL PAPER **[100]**