UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: IT28X80/IT8X299
INFORMATION SECURITY GOVERANCE

CAMPUS: APK

EXAM SSA: JANUARY 2021

DATE	2021-01	**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 5 pages

QUESTION 1 (Risk Management) **[30]**

The Utopian National and International Switching Alliance (UNISA) is an organisation that ensures transactions between different banks are transferred correctly. Example: If an account holder in Bank A pays an account holder in Bank B, Bank A will send the transaction to UNISA and they will ensure that Bank B gets the transaction. UNISA ensures that these financial transactions do not only occur between banks in Utopia, but also between banks in other countries.

The financial switching infrastructure makes use of private connections between UNISA and the various banks. The banks pay UNISA a fixed monthly fee for using the switching infrastructure (At this stage the fee structure is not dependent on volume, but rather on availability). UNISA also has a service level agreement between themselves and the banks, that has a penalty clause in. This clause states that penalties are payable by UNISA when the switching system is not available. UNISA currently has 10 active banking customers that this SLA and penalty clause applies to.

The penalty clause states that UNISA must pay UD 250 (UD: Utopian Dollars) for every minute the switching system is not available. Over the past year UNISA experienced 10 full days of downtime because of distributed denial of service attacks.

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 UNISA. (18)
- Style of report (5)

~ Assessment Continue on the Next Page ~

QUESTION 2 (Security Education, Training and Awareness) **[30]**

The Utopian National and International Switching Alliance (UNISA) implemented several controls and mechanisms that address the risks associated with the scenario described in Question 1. Apart from these controls UNISA also created a new Incident Management and Tracking system.

During a few denial-of-service attacks it was seen that employees sometimes contribute to the downtime that is experienced on the switching system. There have been a few instances where an employee downloaded malicious software from the Internet. In all the cases the employee was either fooled into downloading the software through a phishing attack or thought the software would assist them in their day-to-day work.

The Compliance Manager of UNISA contacted you and raised their concern. It does not seem as if the IT department understands how to fully use the new controls that were implemented in Question 1 and it does not seem as employees in general understand their responsibility to Information Security or know how to handle cyber incidents.

The Compliance Manager would like you to **write** a **high-level proposal** to implement a SETA programme for UNISA. The high-level proposal should clearly **explain** the various principles of SETA. The proposal should also explain **how** the various principles of SETA will be implemented, together with **examples** showing the Compliance Manager what they can expect from such a programme.

Make sure to address the fact that the SETA program must accommodate employees with different levels of information security knowledge and their different roles in the organisation.

Marks are awarded as follow:

- Factual recall of Information SETA. (8)
- Application of SETA program related to the Compliance Manager's concerns. (16)
- Style of proposal. (4)

~ Assessment Continue on the Next Page ~

QUESTION 3 (Cyber security threat agents) **[20]**

Things have been going well since the initial risk management approach as well as implementing the SETA programme. Utopia, as a country, is going through a bit of political turmoil. The current Utopian president has been accused of mismanagement and fraud. Several smaller political parties and activists have all vowed to not stand for the current situation. The president's son is a shareholder in UNISA.

Apart from the political turmoil a cyber incident also occurred at UNISA. A rogue program was detected on the switching system. The rogue program caused some of the transactions to be modified. Transactions greater than UD 100 000 were targeted. For each of these transactions the transaction amount was reduced by UD 10. New transactions were then created for each ten Utopian Dollars where the targeted account was several separate bank accounts. It is estimated that more than UD 10 Million have already been stolen using this method.

Further investigation showed that there was an unpatched vulnerability on the switching system and an unknown user account with the permissions to install new software was found in the system.

A full forensics investigation has been launched. You have been included in the forensics team and are responsible in identifying potential threat agents that might have been involved in the incident.

Write a memo to the CEO of UNISA that identifies at most four of the most common cyber threat agents relevant to this investigation and clearly explain **why** these agents are relevant and what their capabilities are.

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)

~ Assessment Continue on the Next Page ~

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

Since the cyber incident, where UD 10 Million, was stolen, UNISA wants to ensure that their cyber security programme is focussed on this type of incident in the future. The forensics investigation that you were involved in, showed that an employee that had permissions on the system created the unknown user account, that was used to install the rogue program.

The Chief Information Security Officer of UNISA asked you to advise UNISA on how to be better prepared in the future. They want you to focus specifically on this type of incident.

You have decided to use Mitre Att&ck as the framework and knowledge base to implement a cyber incident programme for UNISA.

Write a proposal to the CISO that briefly describes what Mitre Att&ck is and provide a broad overview of how Mitre Att&ck will be used to implement a cyber incident programme for UNISA. Since the CISO is a person that understands through examples, provide as many realistics Mitre Att&ck examples where possible, but still relevant to UNISA's requirements.

Marks are awarded as follow:

- Describing the use of Mitre Att&ck. (4)
- Identifying and motivating why one framework is more applicable than the other. (12)
- Style of proposal: (4)

TOTAL PAPER **[100]**