UNIVERSITY OF JOHANNESBURG
FACULTY OF SCIENCE

MEMO

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 8 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 between banks. 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 make 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)

MEMO

Why IS Risk Management is part of ISM	The student should mention some aspect of Risk Management discussed in ISM best practices such as ISO27002 and Cobit. (2) It is the responsibility of the Board and Executive Management (2)	4
Components of risk	A discussion on the following three factors Asset Vulnerability Threat	3
Risk Man Approach	Student should describe at least the following aspects: Asset Identification Value each asset Threat identification Risk Analysis \ Risk Evaluation. Estimation (Mention qualitative and quantitative) Treatment	6
Applying the approach	Here the student should apply the scenario for each step in the approach example:	12

	Asset Identification: Switching system **(1)** **Value**: UD 250 per minute. **(1)** **Threat Identification**: Availability **(2)** **Risk Evaluation**: **Impact**: UD 250 per minute **(1)** per client **Probability**: 10 Days **(1)** **Risk Value**: 10 * 24 * 60 * 250 = UD 3.6 Million x 10 = UD 36 Million. **(2)** **Prioritise risks**: Only the one **(1)** **Risk Treatment**: **(3)** Potential backup links need to be implemented with redundant systems running from various geographical locations. An automated switch over mechanism can be implemented to ensure the system switches between different routes when one is not available. The switching servers are also duplicated with multiple switching servers running at the same time.	
Style	See description in the question	5

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

The Utopian National and International Switching Alliance (UNISA) implemented several controls and mechanisms that addresses 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 contributes 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 IT department understand how to fully use the new controls that was 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)

MEMO

(One mark per fact, maximum 8 marks) **Factual recall for the following aspects:** Differences between Education, Training and Awareness. **Education** focusses on Why. Levels of Insight. **Training** focusses on How. How to use the system. **Awareness** focusses on What. What is important. Must also include aspects of: **Unconscious Incompetent**. They don't know what they are doing wrong. **Conscious Incompetent**. We have made them aware of what they are doing wrong, but they are still doing it wrong. **Conscious Competent**. Employees know how to do it right but must actively concentrate to do it right. **Unconscious Competent**. Our employees are automatically doing the right thing.	(Two marks per specific, although marks must be based on the completeness of the discussion) **Application of the given scenario into a realistic SETA program.** The proposal should highlight that a one size does NOT fit all. **Measure** the existing IS knowledge or skills specific for their skills. This can be done using some basic online tests and questionnaires. **Who?** **A general awareness** program can be created that target all users. This awareness program can highlight the dangers of phishing emails and malicious attachments and downloads. The **awareness** activities can address many of the *unconscious incompetent* staff and move them into the *Conscious Competent* category. **Example**: Poster programme that introduces cyber threats such as Phishing, Denial of Service and Malicious Software. **Who?** **Training** sessions to help network administrators know what must be done to switch over to backup links and equipment. **Training** sessions can also assist employees move from *Conscious Incompetent* to *Conscious Competent*. Example: Train employees to help identify phishing email. Train employees to use the incident management system to report malicious software attacks. **Measure Training:** The effectiveness of the training programmes can be measured using different techniques. Internal phishing campaigns can measure employee's phishing resistance. Red team exercises can highlight the ability of the IT team to address specific denial of service attacks. **Who?**

	Education. Since the focus on education is to understand why, line managers targeted to complete formalised cyber security courses. **Education**. Critical employees in the IS Compliance and Operations areas will be encouraged to get a formal certificate or degree in cyber security.

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 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.

You have been included in the forensics team and are responsible in identifying potential threat agents that might be 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.

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)

MEMO

Friendly: Are agents that assists the organisation though their activities. Hostile: Are agents that can cause harm through their actions and activities.
The following are a few threat agents that may be identified with some valid motivations. Each agent may get (4) marks. Two (2) marks identifying and describing and two (2) marks motivating.

Only four agents may be identified.
Employee: Internal to the organisation. Part of the Low Capability group of threat actors because cyber-attacks are not normally part of their job responsibilities, but since they already have access to systems, their impact may be quite severe. A inside employee may have been coerced or blackmailed into doing something specific. An inside employee having existing permissions on the server, may have either created the account or installed the software.
Cyber Criminal: Is profit oriented. They use existing tools but may also deploy their own set of tools and because of previous profits may have access to high levels of infrastructure and can employee high levels of skills. Cyber Criminal may make use of internal employees to conduct their operations. Since UNISA works with potential money, they literally transfer money. Cyber criminals would like to get access to the money controlled by UNISA's systems. The unpatched vulnerability may point to a single external agent, but they may be working with an internal agent as well.
Hacktivists: They are socially motivated. They may either develop or use a number of tools. They normally have access to highly skilled individuals, but also have access to necessary infrastructure. Because of the link between UNISA and the president, the hacktivists might have targeted the organisation, but since money was stolen and no message was created, it may be that they are just acting as a modern "robin hood"
Cyber Fighters \ Cyber Warriors: They are nationally motivated citizens. Access to tools and infrastructure is great. This may be one or more motivated political parties that either need the funds. Or just want to cause the president some distress through his son.
Many other roles may be mentioned, the role's motivation must first be measured before marks may be awarded to the role.

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 was 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.

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)

MEMO

Mitre Att&ck:

- Knowledge base of adversarial techniques.
- Technique: offensively oriented actions that can be used against platforms.
- Adversarial Techniques are mapped against tactics.
- Tactics describes why a technique is used. It provides context.

The proposal should mention the process described below:

Identify techniques. **A valid local account was used**.

Once identified confirm if the technique is not related to other techniques. **The Local account technique may also be related to OS Credential Dumping. This would have been relevant if the local account did not have the correct permissions.**

Train the Information Security Operations Team and Compliance Team, how the technique works by looking at various processes where it was used.

Implement the mitigation steps. This may be a few quick wins or can result in a number of major projects. In this example. **Password Policies can help enforce strong passwords for these privilege accounts, and special privilege account management can be used.**

Implement the detection steps. Some detection steps require manual auditing, while other steps can be implemented by using logging with relevant alerts. **In this example, local accounts need to be audited by the Compliance Department every week or month. Special audit events can also be enabled to alert privilege account logins at strange hours, such as after hours.**

Train the team members how to use the mitigation steps.

Train the team members how to use the detection methods and identify potential threats.

Train the team members how to respond.

Conduct a red team exercise. **The red team can try and attack one of the switching servers and install a benign program on the server trying to utilise one of the local accounts on the servers.**

TOTAL PAPER **[100]**