UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

MEMO

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

CAMPUS: **APK**

EXAM: **OCTOBER 2020**

DATE	2020-10	**SESSION**	Morning
INTERNAL EXAMINER		Dr J du Toit	
EXTERNAL EXAMINER		Prof 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 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)

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 (Impact) 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: **Risk Analysis – Asset Identification** : Central banking system (**1**) **Risk Analysis – Impact**: Given is High. **(1)** **Threat – Identification**: Many options here. Exfiltration or Unauthorised modification. **(2)** **Threat – Assessment**: Medium threat. **(1)** **Vulnerabilities – Vulnerability Assessment**: High (Impact of the vulnerability) **(1)** **Risk Evaluation**: **(2)** Windows vulnerability. Medium (2) x High (3) = 6 Banner vulnerability. Low (1) x Medium (2) = 2 **Prioritise Risks:** Windows (6), Banner (2). **(1)** **Risk Treatment: (3)** The student can mention many things here that should address the Windows threat. The most likely course of action is to review and implement a full patch management program. The program is the control that needs to be implemented. The patches themselves is not a very good control, since it is a once-off solution.	12
Style	See description in the question	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)

MEMO

	The student should highlight the two major IS structures	
IS Operational Management	Describe: (3) IT Manager reports to Top Management IT Manager may be employed, or function can stay with financial manager. New department: IS Operational Department (7) IS Operational Department reports to IT Manager A new IS working group may be created. IS working group (IS Committee) is chaired by IT Manager. The IS Committee reports via IT Manager to Top Management IS Operational Management Dep: Responsible for day-to-day IS operational functions, such as, Logical access control, Firewall Management, Anti-Virus Management etc. IS Committee \ Working group: (2) Brings together technical IS requirements and interests of: User departments, Audit department and IT department	12
IS Compliance Management	IT Risk Manager reports directly into board. (6) IT Risk Manager chairs the Audit committee and IT Risk Management Committee. User deps, IT dep, IS Compliance Dep and Audit dep is part of IT Risk Committee.	13

	IS Compliance Management dep reports to IT Risk Manager. IS Compliance Management Department: (7) Requires data from different sources: Operational IT environment. Questionnaires etc. Consolidate and interpret the data. Calculate the current IT risk situation. Primarily to monitor and report on level of IT risk. Must have SLA with IT operational department for the data required.	
Style		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. (2)

MEMO

Diffs:	Friendly: Are agents that assists the organisation though their activities. Hostile: Are agents that can cause harm through their actions and activities.	(2)
Threat Agents:	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.	(16)

	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. Since there were known incidents originating from within the network, the chances that an employee is involved is quite high.	
	State: A state may have a national mission to conduct espionage on critical organisations in foreign countries. The foreign state may have access to high levels of skills and infrastructure and may use existing tools, or even deploy tools to conduct their espionage. FUB is a critical organisation for the citizens of Utopia. A foreign state may target FUB because of economic and political reasons.	
	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 FUB is a bank, they literally safekeep money. Cyber criminals would like to get access to the money controlled by FUB's systems. Since there has been both internal incidents and external attacks, this may point to a criminal organisation wanting to gain access to FUB	
	Cyber Terrorist: They are ideologically motivated. They may either develop a number of tools, or use a number of tools to launch their attacks. They normally have access to highly skilled individuals, but also have access to necessary infrastructure. Because of the tax laws in Utopia, these groups may target FUB to "get back" at the Utopian government for making the individual's lives more difficult in the neighbouring country.	
	Many other roles may be mentioned, the role's motivation must first be measured before marks may be awarded to the role.	
Style	Logical flow of ideas. Easy to differentiate between different agents and reasons why threat agents were selected.	(2)

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 considering 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)

MEMO

Comparing CIS with Mitre Att&ck:	CIS Controls are ordered from one (1) to 20. With the order being grouped into basic, foundational and advanced. This is the one dimension. First focus on basic, then foundational and then advanced. The CIS Controls are further grouped according to Implementation Groups. This can be seen as a second dimension that assists organisations in planning the IS programme. The three groups are typically grouped for small, regional and large organisations. Mitre Att&ck:	(6)

	Acts as a knowledge base for adversary activities. These activities are grouped into Tactics (Why the attacker does a specific action) and Techniques (How the attacker accomplishes the activity). Since this is a knowledge base it gives very detailed information on how an action is performed, but also provides information on how to mitigate such an attack and how to detect it	
Recommendation	Implementing an IS programme based on the content of the Mitre Att&ck will be very difficult. Mitre Att&ck is more useful after certain risks or threats have been identified but can also assist in threat modelling. Mitre Att&ck does not provide easy to use guidelines on how to implement a general IS programme. The focus on Mitre is when threats have already been identified. CIS Controls, provides easy to use guidelines that can be used to identify controls and incorporate these controls as part of an IS programme. Since the goal of FUB is to start an IS programme, CIS can be used to measure their existing IS controls and highlight which controls are lacking. This is more applicable in situations where not all the threats are immediate understood.	(4)
Implementation	Implementation plans should use: • Measuring existing exposure. • Identifying relevant controls given their risk. • Planning and organising the project according to risk and implementation time. • Re evaluation Use CIS to measure (audit) the organisation's existing IS implementation. The audit should highlight what has been achieved and what is lacking. Using the audit report as input, FUB can do a basic risk assessment on the outstanding controls to see if they are applicable. The outcome of the risk assessment should highlight the importance of the various controls. The controls can now be organised. Guiding principles such as: Risk level and Quick wins can act as guideline to help with the planning. Highest risk mitigating controls must be identified and put on the list of potential projects. Those that can be implemented the quickest can be given the highest priority for implementation. This will ensure a high impact quick win for FUB. The rest of the longer projects must be well planned and implemented. If the existing project plans show more time is available then more controls can be added according to their risk level and implementation time.	(6)
Style	It must look like a letter. Easy to read.	(4)

TOTAL PAPER **[100]**