UNIVERSITY OF JOHANNESBURG
FACULTY OF SCIENCE

MEMO

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: IT28X80/IT8X299
INFORMATION SECURITY GOVERNANCE

CAMPUS: APK

EXAM SSA: NOVEMBER 2021

DATE	2021-11-30	**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 6 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 (Risk Management) **[30]**

UtopiaHost is a national Internet Service Provider for most government and commercial organisations in Utopia. Part of the services UtopiaHost offers are cloud services. One of the most popular cloud services used by many organisations is their hosted customer relationship management (CRM) system. The CRM system allows organisations to handle all their sales and marketing processes.

UtopiaHost has a service level agreement with a penalty clause. The penalty clause states that a customer can claim 100 Utopian Dollars for every hour the CRM system is unavailable. UtopiaHost currently has 50 customers, that this penalty clause applies. In the last year, UtopiaHost experienced several denial-of-service attacks on the cloud infrastructure that caused the CRM system to be unavailable for ten (10) days.

The CEO of UtopiaHost contacted you because they are unsure what their options are. For some reason, the IT department cannot fix the problems, and the normal risk management committee says they do not know how to manage the risk.

Answer the following questions related to this scenario

1.1 Briefly explain why Risk Management is part of Information Security Governance. (4)

1.2 Clearly identify the components of risk. (3)

1.3 Using the information supplied, explain to the CEO the process UtopiaHost can follow to manage the risk. The process must use this scenario as the basis and include risk analysis, estimation, and treatment. (18)
Five marks may be awarded if the answers are properly numbered and written in a clear and concise format. (5)

MEMO

1.1	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
1.2	A discussion on the following three factors Asset Vulnerability Threat	3
1.3	Student should describe at least the following aspects: Asset Identification (1) Value each asset (1) Threat identification (1) Risk Analysis \ Risk Evaluation. (1) Estimation (Mention qualitative and quantitative) (1) Treatment (1)	6
	Here the student should apply the scenario for each step in the approach example: **Asset Identification**: Cloud infrastructure **(1)** **Value**: UD 100 per hour. **(1)** **Threat Identification**: Availability **(2)**	12

	Risk Evaluation: **Impact**: UD 100 per hour **(1)** per client **Probability**: 10 Days **(1)** **Risk Value**: 100 * 24 * 10 * 50 = UD 1.2 Mil **(2)** **Prioritise risks**: Only the one **(1)** **Risk Treatment**: **(3)** The student can define many aspects here. Put in redundant hardware. Ensure the hardware is running from different data centres. Improve the backup and recovery systems.	
Style	See description in the question	5

QUESTION 2 (Organisation) **[30]**

After several discussions with yourself, the CEO of UtopiaHost realise that they drastically need to improve the organisation of their Information Security function. UtopiaHost currently only has an IT Manager whose tasks include those of basic Information Security operations. The CEO of UtopiaHost realised that the IT department is overworked and understaffed and needs a new structure to manage the Information Security function fully.

The CEO asked you the following: "If you have a clean slate, how will you organise the Information Security function in UtopiaHost?".

Write an email to the CEO that clearly explains how the Information Security function may function for UtopiaHost. Make sure to include recommendations that you see fit around departments, positions and working groups that must be formed. Make sure to motivate the recommendations.

Marks are awarded as follow:

- Applying the IS function to UtopiaHost (25)
- Readability and style of the email. (5)

MEMO

	The student should highlight the two major IS structures	
IS Operational Management	Describe: (3) The IT Manager job can stay as is, but it can be augmented with potentially a separate department or area in the department with an IS Manager. New department or a specific function in the IT department for this function: 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)	12

	Brings together technical IS requirements and interests of: User departments, Audit department and IT department	
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. 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.	13
Style		5

QUESTION 3 (Information Security Governance - Arguments) **[20]**

Critically discuss each of the following statements. Critical discussions require that you either agree or not with the statement and comprehensively motivate your answer.

3.1	'Information Security is a technical issue and belongs in the IT department.'	(4)
3.2	'An organisation is at a severe disadvantage without a Corporate or Enterprise Information Security Policy.'	(4)
3.3	'Information Security Policy statements that cannot be measured is not worth the paper it is written on.'	(4)
3.4	'An organisation will always be reactive in its Information Security approach if there is no proper Information Security Awareness programme.'	(4)
3.5	'The CIS Controls framework is extremely difficult to use for Information Security planning purposes'	(4)

MEMO

3.1	There are many arguments that can be made here. First approach is the Governance argument that flows from Corporate Governance to IT Governance to IS Governance. Another argument is the compliance aspects of IS Governance. Measuring of IS operations must be established outside the control of the teams that implements them to ensure oversight.	(4)
3.2	Without a EISP there is not clear guideline on what the organisations strategy is wrt IS. IS personnel has no idea what needs to be implemented. It opens the door for employees to abuse IT assets. There is no clear IS organisation without the policy.	(4)

3.3	IS Policy must be measured to ensure that policy statements are not just made to sound great. Without having the ability to measure or confirm policy statements no one can be held accountable when something goes wrong.	(4)
3.4	People are part of the IS architecture. People can both maliciously or accidentally cause cyber security incidents. Awareness addresses the vulnerabilities that may be exposed by employees.	(4)
3.5	The CIS Controls are well constructed. It contains Implementation Groups that assists organisations of different sizes to focus on the correct set of controls. Each control category contains several safeguards that can be adopted by the different implementation groups. Each safeguard describes what is required, the asset type it focuses on and which security function it addresses.	(4)

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

After an extensive Risk Management exercise, the following risks have been identified and listed on the risk register.

Risk Number	Description	Risk Level
R16	At this stage, the recovery time of various IT systems is unknown. No formal disaster recovery tests have been performed on individual systems.	High
R18	There is no single repository that stores information about all the software systems in the organisation.	High
R21	Ad-hoc vulnerability scans show that there is no managed vulnerability scanning occurring in the environment.	High
R22	There is no central authority that can be contacted in case of an information security incident.	High
R33	There seem to be several unauthorised remote access points for people working from home. A fair number of remote-control software has been loaded on office computers without any centralised authentication mechanisms.	High

The NIST Framework for Improving Critical Infrastructure Cybersecurity explains five core functions that are adopted by many other frameworks.

4.1 Briefly describe each of the five functions that make up the core of the framework (10)

4.2 For each function, describe at least one activity that will improve the risk register for UtopiaHost, based on the five functions described in the framework. When describing the activity, highlight the risk item addressed by the activity and explain in which core function the activity resides. (10)

MEMO

4.1	Two marks for each aspect. **Identify**. Improve the understanding of the organisation around various aspects of their IS architecture, such as system, people, assets, data and capabilities. **Protect**. Limits the impact of a potential cyber security event, by implementing safeguards. **Detect**. Activities that improve the ability to identify the occurrence of cyber events. **Respond**. Improve the capabilities to take action when a cyber security event occurs.

	Recover. Develop plans to improve the recoverability of the organisations during and after an event.
4.2	Depending on the activity the student's answer may differ. One mark for grouping the activity and one mark for describing the activity to address the risk. Recover. **R16**. Recovery plan is executed during or after a cybersecurity incident Identify. **R18**. Software platforms and applications within the organisation are inventoried Identify\Protect\Detect\Respond. **R21**. The management of vulnerabilities occur in identify, where vulnerabilities are identified. Under protect a plan needs to be established. Under detect the vulnerability scans are performed. Under respond processes are in place to receive vulnerability notifications from internal or external sources. Respond. **R22**. Personnel know their roles and order of operations when a response is needed Protect. **R33**. Remote access is managed.

TOTAL PAPER **[100]**