UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

IT28X17/IT00217

Information Security Risk Analysis

EXAM MEMO

3 November 2021

INTERNAL EXAMINER: Ms. M Fourie

EXTERNAL MODERATOR: Prof. A van der Merwe

TIME: 2 hours (30 minutes upload time) **MARKS:** 100

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 5 pages including this cover page
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.
7. Your final submission should be uploaded to eve.uj.ac.za using the following naming convention: Surname_Initials_StudentNumber_IT28X17.
8. You may type or write the test. If you submit a handwritten document, please number the pages clearly and use CamScanner to take clear photographs.
9. You may ask questions or raise concerns to your lecturer through the Discord channel or by sending an e-mail.

QUESTION 1 **[5]**

a) According to ISO 31000, risk is the "effect of uncertainty on objectives". Within the context of risk management, **explain what this statement means.** To support your answer, **provide two examples** of Information Security risks that modern businesses might face. (5)

- This statement refers to the fact that we live in a world filled with **uncertainties. In the context of risk management, uncertainty exists when there is incomplete knowledge or understanding of an event, consequence or likelihood.**
- When trying to achieve an objective – there is always the chance that things could go wrong – and **one does not always get the expected results**.
- In order to manage risk effectively, there is a **need to reduce uncertainty** as much as possible.
- Students may provide any two(2) valid examples to demonstrate risks that may affect business objectives (e.g. uncertainty of employee cyber-awareness levels, risks pertaining to the organisation's network security etc.)

QUESTION 2 **[10]**

*MZD-WebDesign is a new company that **develops, designs, and maintains** web applications for various small businesses all over the world. The company owner, Mzi, is concerned about the Information Security (IS) risks that such a business in the tech-space might face. Mzi is unsure, at this stage, whether the company is following appropriate IS best practices. The company is, therefore, looking for an Information Security Risk Model that will help them implement best practices in the business, analyse risks and manage them effectively.* (10)

a) **Discuss** the **ISF** risk model and provide reasons why you would recommend this risk model to the business described in the above scenario.

Students must refer to the scenario when providing the information on ISF:

- Information Security Forum (ISF) is an international association of over 260 leading companies and public sector organisations. It is, therefore,

internationally recognised which is good since XYZ-WebDesign develops apps for businesses world-wide.

- ISF products concerning Risk Analysis/Risk Management refer often to each other and can be used **complementarily.** Therefore, **XYZ WebDesign have access to well-rounded, interconnected Risk Analysis/Management approaches when using ISF.**
- The Standard of Good Practice provides a set of high-level principles and objectives for information security together with associated statements of good practice. XYZWebDesign would like to follow **recommended best practices for IS**.
- FIRM is a detailed methodology for the monitoring and control of information risk at the enterprise level. It has been developed as a practical approach to monitoring the effectiveness of information security. Since XYZ is **involved in maintaining client applications**, they will require **continued guidance on how best to monitor IS risk for their business**.
- The ISF's Information Security Status Survey (the Survey) is a comprehensive Risk Management tool that evaluates a wide range of security controls used by organizations to control the business risks associated with their IT-based information systems. **Evaluating controls is effective to keep and update the necessary safeguards to minimize IS risk**.

(Any valid fact about ISF along with reference to the scenario)

QUESTION 3 [20]

A consulting firm has approached you to assist them with implementing the **FRAAP** (Facilitated Risk Analysis and Assessment Process) methodology as their new risk management model. Compile a report for the managing committee of the firm to **explain** to them how FRAAP works and what it would **require from various stakeholders** in the business. (Hint: Your answer should refer to all three of the phases that form a part of FRAAP).

Answers should follow a framework that discusses each of the phases in enough detail to form a clear view of what each step involves:

1. The pre-FRAAP
2. The FRAAP session
3. Post-FRAAP

Answers should also mention the stakeholders and their roles in the FRAAP process, e.g. Owners, Custodians, Users, FRAAP facilitator etc.

Max 20 marks.

QUESTION 4 [10]

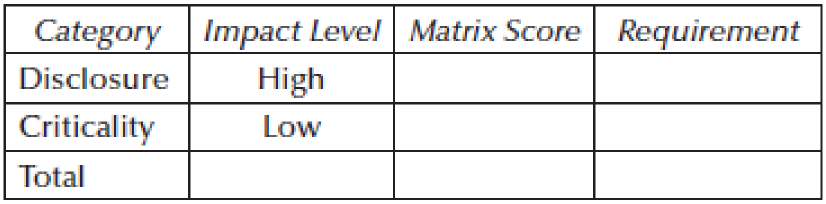
a) **Fully discuss** what the process of **performing a risk analysis** entails. Your answer should refer to the ways in which this process assists managers to fulfill their roles in modern organizations. (10)

- Risk analysis is used to document and demonstrate the business reasons why a new project should be approved.
- Answer must explain that risk analysis helps managers meet their due diligence requirement:
- Risk analysis is the process that allows management to demonstrate that it has met its obligation of due diligence when deciding about moving forward with a new project, capital expenditure, investment strategy, or other such business process.
- Due diligence has several variant definitions based on the industry that is being discussed. Typically, the consensus these definitions address is the measure of prudent activity, or assessment, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the circumstances.
- Due diligence is not measured by any absolute standard but depends on the relative facts of each case.
- The risk analysis or PIA examines the factors that come into play when trying to determine if a project should be approved.
- The PIA examines the tangible impacts (e.g., capital outlay, development costs, and long-term costs such as continued operations and maintenance).
- The risk analysis also addresses intangible impacts, such as customer connivance or regulatory compliance.
- When the risk analysis is complete, the results are presented to a management oversight committee that is charged with reviewing new project requests and deciding whether or not to move forward.

QUESTION 5 [15]

a) **Explain** the process an owner would follow to categorise an asset's mission criticality level as "low". **Draw** a pre-screening matrix that represents the end result of such an entry. (5)

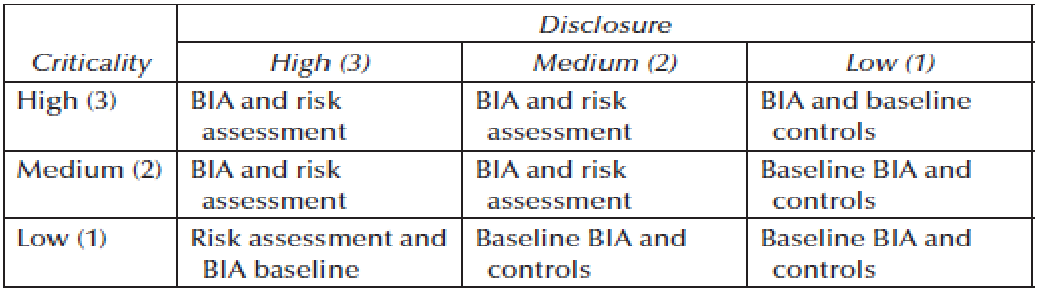
- The owner selects the most-appropriate category that describes the mission criticality of the asset that is scheduled to undergo the risk assessment.
- The impact level is entered on the pre-screening worksheet.
- We will select the category "Information is of such a nature that its unauthorized modification or destruction would have little or no impact to the organization" or low.
- The owner then looks to the pre-screening matrix and finds the intersection of the two levels and enters the number in the matrix score box of the worksheet.



Category	*Impact Level*	*Matrix Score*	*Requirement*
Disclosure	High		
Criticality	Low		
Total			

b) Draw a table that contains recommended actions for each of the **criticality** and **disclosure** values presented in the above tables. (5)

Table 3.12 Pre-Screening Example 3 Recommended Action



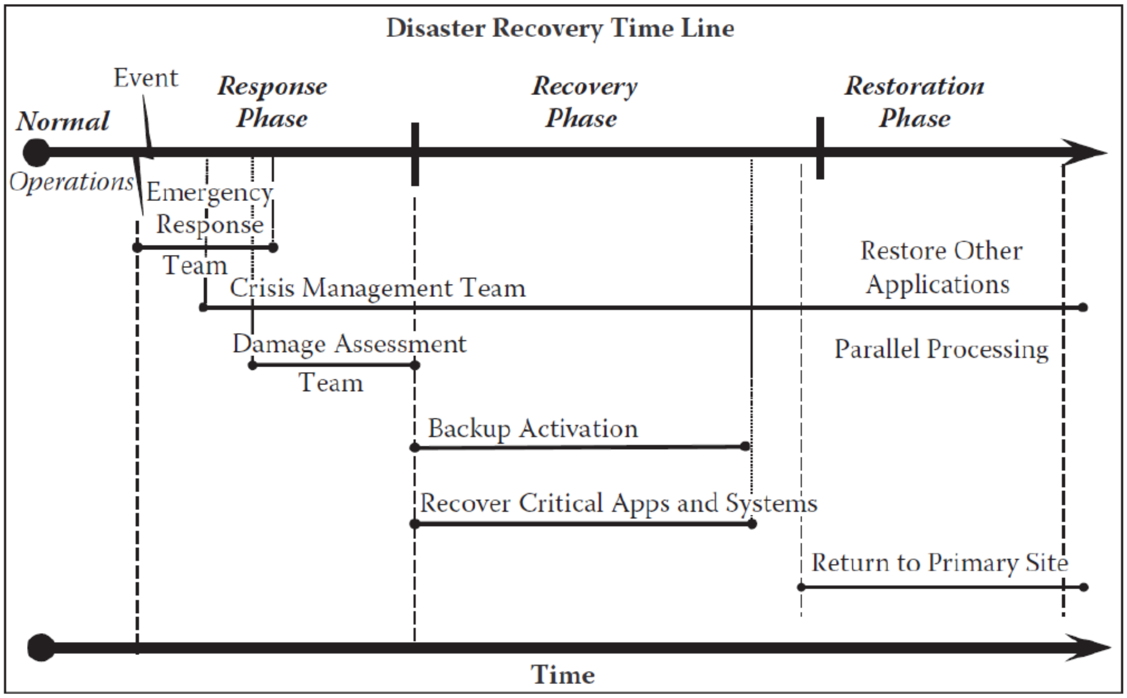
	Disclosure		
Criticality	*High (3)*	*Medium (2)*	*Low (1)*
High (3)	BIA and risk assessment	BIA and risk assessment	BIA and baseline controls
Medium (2)	BIA and risk assessment	BIA and risk assessment	Baseline BIA and controls
Low (1)	Risk assessment and BIA baseline	Baseline BIA and controls	Baseline BIA and controls

QUESTION 6 [5]

a) Business Impact Analysis and Risk Assessment are two complementing processes that might include a business continuity and disaster recovery plan. **Name and describe** the second and third phases in the Disaster Recovery Timeline. You may draw a diagram to support your answer. (5)

- During the **recovery phase** the organization will concentrate on bringing **mission-critical** services back online.
- The sequence of recovery order has been predetermined by the results of the BIA process.

- In addition to establishing recovery time objectives (**RTO**) the BIA has identified lines of dependency.
- The third phase is called restoration. This is the process where the organization **moves** into its **restored primary site** or has moved to a **new primary site.**
- Here the organization initially **recovers the remaining processes**, restores the **high-priority processes**, and deactivates the recovery site.



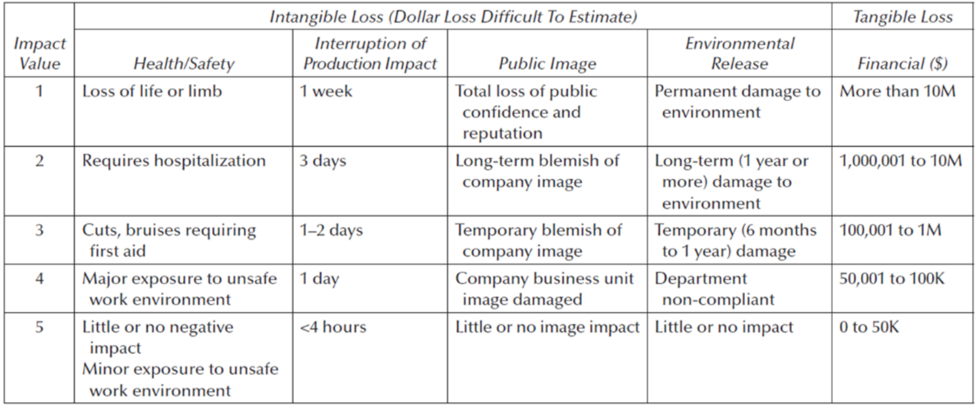
QUESTION 7 [13]

a) **Discuss** the Business Impact Analysis (BIA) process. **Draw** an example of a **single** BIA **impact table** to demonstrate what the process entails. (10)

- The results of the BIA process will be used by an organization to determine how critical a specific application, system, business process, or other asset is relative to all of the other assets in the organization.
- The BIA results are submitted to the senior management oversight committee, typically the information security steering committee, for review and approval.
- The BIA process begins with the creation of a set of definitions of possible impacts to the business or mission of the organization.

- From these definitions a set of impact tables should be created to identify the impact thresholds for the various categories. The BIA team will work with the specific departments to establish the criticality thresholds.
- A set of impact tables is established to be used by the organization to establish the RTO for each application, system, or business process.
- Table 4.2 – (actually 5 tables in one): 5 marks for any one of the columns drawn.

Table 4.2 BIA Impact Table



Impact Value	*Intangible Loss (Dollar Loss Difficult To Estimate)*				*Tangible Loss*
	Health/Safety	*Interruption of Production Impact*	*Public Image*	*Environmental Release*	*Financial ($)*
1	Loss of life or limb	1 week	Total loss of public confidence and reputation	Permanent damage to environment	More than 10M
2	Requires hospitalization	3 days	Long-term blemish of company image	Long-term (1 year or more) damage to environment	1,000,001 to 10M
3	Cuts, bruises requiring first aid	1–2 days	Temporary blemish of company image	Temporary (6 months to 1 year) damage	100,001 to 1M
4	Major exposure to unsafe work environment	1 day	Company business unit image damaged	Department non-compliant	50,001 to 100K
5	Little or no negative impact Minor exposure to unsafe work environment	<4 hours	Little or no image impact	Little or no impact	0 to 50K

b) **Name three** international standards you would recommend to an executive before considering a **GAP** analysis. (3)

Answer (Any 3):

- CobiT – Control Objectives for Information and related Technology
- ISO27002 – Code of Practice for Information Security Management
- ITIL – Information Technology Infrastructure Library
- NIST – Recommended Security Controls for Federal Information Systems.

QUESTION 8 [22]

Scenario: *A large logistics company has recently approached you to assist them in the process of selecting appropriate countermeasures and managing information security (IS) risks in a cost-effective way within the business. Upon investigation of the company's information security practices and business operations, you found the following: The company has appointed multiple new employees and a new IT Senior Manager. This manager has been pro-active in implementing information security risk control measures and creating awareness of the various threats the organization may face. When you spoke to employees in the various departments, they had a good understanding of the cyber threats within their department. They are also acquainted with the information security policies. This is because new candidates that are placed in critical departments must* *complete a Cyber-smart course during their probation period. The course also informs employees of the many complexities and IT security risks that are specific to the logistics industry One complaint you received from various employees was that the risk mitigation process of backing-up data is often disrupted. Back-up storage space often fills up quickly and weeks pass by before the person in charge of the back-ups, make enough storage space available.*

a) **Identify** which level in the **COBIT domain maturity model** corresponds to the scenario described above? **Justify** your answer by providing a **description** of the selected level and **refer** to the scenario. (12)

2 marks per point (max 12)

- Level 2: Repeatable
- There is an emerging leader for IT risk response. The new IT manager is taking initiative to implement control measures and create awareness of threats.
- There is individual awareness of threats and points of contact for direction when they materialise. The employees have a good understanding of the cyber and IS threats within their department.
- Control deficiencies may be identified but are not remediated in a timely manner. Back-up storage space often fills up quickly and takes weeks to be addressed.
- Risk mitigation processes are starting to be implemented where IT risk issues are identified. The back-up storage process aims to mitigate the risk of data loss.
- Minimum skill requirements are identified for critical areas of risk articulation, monitoring, and project and crisis management. The employees are required to complete an IS awareness course.
- Common approaches to the use of risk monitoring and response tools exist but are based on solutions developed by key individuals. The backup storage space is managed by one person.
- Students should sufficiently justify their choice.

b) Suppose you oversee the company described above. It is clear to you that properly implemented Information Security Policies are essential reference documents for modern organisations. **Discuss** how you **would ensure that the Information Security policies are effective?** Your answer must refer to the scenario. (10)

- Answers must refer to the scenario and discuss the following points:
- For policies to be effective, they must be properly:
- Developed using industry accepted practices
- Distributed or disseminated using all appropriate method
- Reviewed or read by all employees

- Understood by all employees
- Formally agreed to by act or affirmation
- Uniformly applied and enforced

THE END