UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

IT28X17/IT00217

Information Security Risk Analysis

EXAM

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 4 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 examples** of Information Security risks that modern businesses might face. (5)

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.

QUESTION 3 [20]

a) 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). (20)

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)

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 result of such an entry. (5)

b) Draw a table that contains recommended actions for each of the **criticality** and **disclosure** values presented in the above tables. (10)

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)

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)

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

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)

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)

THE END