THE OPEN UNIVERSITY OF SRI LANKA
DEPARTMENT OF COMPUTER SCIENCE
BSC IT DEGREE PROGRAMME – 2024/2025
FINAL EXAMINATION
ISU6300 – IT Risk Management
DURATION: TWO HOURS (2 HOURS)

Date: 17.06.2025 **Time:1.30 pm – 3.30 pm**

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of 06 questions on 04 pages.
3. Answer any 04 questions only. All questions carry equal marks.
4. First Question (Q1) is compulsory. Select three (03) more questions from the rest.
5. The answer for each question should commence on a new page.
6. Draw fully labeled diagrams where necessary.
7. Involvement in any activity that is considered an exam offense will lead to punishment.
8. Use blue or black ink to answer the questions.
9. Clearly state your index number in your answer script.

Q1

A national retail company outsources its customer relationship management (CRM) to a third-party cloud service provider. This provider stores sensitive customer information, including purchase history, payment preferences, and loyalty program data. Recent events suggest that similar vendors have been targeted by hackers, resulting in breaches exposing personal data.

Industry reports suggest a **50%–90% chance** that a third-party CRM provider may face a breach within a year. If it occurs, **tens of thousands of customer records** may be exposed, leading to public backlash, fines, and brand damage. Based on the tables provided:

i. Determine the **qualitative likelihood rating**.

ii. Determine the **consequence rating**.

iii. Use the risk matrix to identify the **overall risk level**.

The company's risk appetite statement includes:

"We accept moderate operational risks to optimize customer engagement, but we will not tolerate risks that compromise customer trust or result in large-scale data loss."

iv. Does this third-party breach risk align with the company's risk appetite?

A potential data breach at the CRM vendor could cost the retail company **$500,000 per incident** (including legal, notification, and reputational costs). Based on similar organizations, there's a **60% annual chance** of such a breach.

Calculate:

v. **Single Loss Expectancy (SLE)**

vi. **Annual Rate of Occurrence (ARO)**

vii. **Annualized Loss Expectancy (ALE)**

To mitigate this risk, the company considers implementing a **third-party risk management (TPRM) platform** and conducting regular audits of the CRM provider. The total cost is **$50,000/year**. This effort is projected to reduce breach risk by **70%**.

viii. **New ALE after mitigation**

ix. **Risk savings**

x. **Net benefit** of implementing the TPRM solution

Q2

i. Define the key concepts of risk, threat, vulnerability, and impact in the context of information security. Illustrate your answer with real-world examples.
ii. Discuss the potential impacts of a data breach on an organization. How should organizations prepare to minimize such impacts?
iii. Why is risk identification in the risk management lifecycle considered a critical first step, and what are the consequences of failing to identify risks properly?
iv. Define threat modeling and describe its purpose in the context of cybersecurity. How does it contribute to proactive risk management?

Q3

i. What measures can organizations take to mitigate risks associated with the human attack surface?
ii. What tools and methods are commonly used to implement Continuous Monitoring ?
iii. Discuss how Key Risk Indicators (KRIs) contribute to proactive decision-making and risk mitigation.
iv. How does internal compliance in organizational governance support ethical practices?

Q4

i. Discuss the risks and consequences of non-compliance with regulatory standards.
ii. Why is Vendor Risk Management (VRM) crucial for organizations to assess and monitor their vendors' security practices?
iii. How does Business Continuity Planning (BCP) contribute to an organization's overall resilience against cyber threats and other disruptions?
iv. Compare proactive vs. reactive security approaches.

Q5

i. Discuss the three (03) core principles of Zero Trust Security and their role in enhancing an organization's cybersecurity posture.

ii. Discuss the differences and collaboration between Red, Blue, and Purple teams in a cybersecurity environment.

iii. Identify and explain five (05) key metrics used in cybersecurity dashboards that support effective risk management.

iv. Illustrate how key principles of effective security reporting can improve understanding and response to cyber threats.

Q6

i. Evaluate the effectiveness of hypothesis-driven threat hunting compared to IOC-based and TTP-based hunting methodologies.

ii. Discuss the differences between internal and external risk audits.

iii. Analyze the cybersecurity implications of IoT adoption in industrial environments.

iv. Why is it important to view cyber insurance as complementary rather than primary defense?

All Rights Reserved