00243

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree/Diploma

in

Information Technology

(Specialized in Cyber Security)

Final Examination

Year 3, Semester II (2022)

IE3102 – Enterprise Standards for Information Security

Duration: 2 Hours

November 2022

Instructions to Candidates:

- This paper contains 4 questions
- Answer all questions in the booklet given.
- The entire exam is worth **100 marks** which contributes to **50%** of the final grade.
- This paper contains 5 pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed
- Exam paper is to be collected back with the answer booklet.

Question 1 **(25 Marks)**

a. List five current information security-related standards and briefly explain their targeted industries.

(5 marks)

b. Describe the aims of security compliance for a typical organization?

(6 marks)

c. Explain the purpose of security compliance for a typical organization.

(3 marks)

d. Explain the impacts of noncompliance on the organization and its customers

(5 marks)

e. Analyze the costs associated with compliance from an organizational perspective and describe strategies you would use to manage cost reduction in the workplace.

(6 marks)

Question 2 **(25 Marks)**

a. How the CIA triangle helps the business in information security.

(4 marks)

b. What is the main objective of ISO 9001:2015 and ISO 14001:2015?

(4 marks)

c. Compare certification and accreditation.

(4 marks)

d. Please use the following Case Study to answer the questions below:

Case Study

Biosen is a manufacturer of Internet of Medical Things devices in the healthcare industry. headquarters based in Singapore and factories located in Sri Lanka. An IS auditor within the enterprise has been asked to perform preliminary work that will assess the organization's readiness for a review to measure compliance with new US-based regulatory requirements. This new regulation demands that strict data privacy requirements are met and controls are implemented to mitigate the cybersecurity risks which emerge with the changing landscape of threats. These requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment and

will assess management's review and testing of the general IT controls. Areas to be assessed include:

- Data Privacy and Confidentiality
- Production control and network management
- IT governance
- Weak Access Controls
- Security by Design

The IS auditor has been given three months to perform this preliminary work. It was reported in previous audits that weak access controls and risks to data privacy and confidentiality were among the major findings. In anticipation of the work to be performed by the IS auditor, the chief information officer (CIO) requested direct reports to develop narratives and process flows describing the major activities for which IT is responsible.

i. What should be the initial task of the IS auditor?

(5 marks)

ii. When investigating risks against the confidentiality and privacy of protected health information list three areas in which the patient information is most vulnerable?

(3 marks)

iii. Referring above scenario write a report suggesting suitable controls to be implemented to minimize risks in Biosen.

(5 marks)

Question 3 **(25 Marks)**

a. Define what ISMS stands for?

(1 mark)

b. The main change to the 2022 edition of ISO/IEC 27001 is the update of Annex A to reflect ISO/IEC 27002:2022. Explain the new controls that are introduced in the ISO27001:2022 standard and justify the reasons why new controls are introduced.

(8 marks)

c. Describe the four dimensions of Service Management in ITIL.

(4 marks)

d. The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card account data security. Describe what changes are being made in the PCI-DSS 4.0 standard compared to the PCI-DSS-3.2.1

(8 marks)

e. Sri Lanka Personal Data Protection Act (PDPA) passed on 19 March 2022. It covers all the bases related to data subject rights (DSRs). Assess the impact of the data protection areas. under GDPR and Personal Data Protection Act No.9 of 2022 in Sri Lanka.

(4 marks)

Question 4 **(25 Marks)**

Case study of "Dinocom"

Dinocom A healthcare insurance provider in the US reported major data breaches affecting over 1 million accounts by the end of 2019. On further investigation, Dinocom confirmed that all 1 million accounts were affected in this cybersecurity incident. This is known to be the biggest data breach in the world of healthcare insurance providers. The cyber-attack targeted 1 million accounts and obtained account names, email addresses, Credit card information, telephone numbers, date of birth, hashed passwords, and some encrypted and unencrypted security questions. They reported this breach to the public in 2020 and believed this to be the work of an organized Cybercrime group. In a twist of events, Dinocom filed an SEC report early in April to inform that they were not aware of the data breach. But when another report was filed in May after disclosing the data breach to the public, Dinocom accepted the fact of knowing the intrusion into their system.

Later investigations revealed that the compromised data was sold in the Darkweb by Cybercriminals.

a) List two Assets, two vulnerabilities, and two threats based on the above scenario.

(3 marks)

b) "A comprehensive risk analysis would have flagged the above incident as critical based on the impact" justify this statement using your own words.

(5 marks)

c) According to the Information Security Triad what is/are the security principle violated according to the given scenario?

(3 Marks)

d) Critically evaluate the Business Impact, Financial Impact, and Public Reputation impact areas respectively.

(8 Marks)

e) You have been asked to suggest suitable countermeasures that the Dinocom can implement to prevent further attacks.

(6 Marks)

End of the Question Paper