Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized Cyber Security

Final Examination
Year 3, Semester 2 (2019)

IE3102 – Enterprise Standards for Information Security

Duration: 2 Hours

October 2019

Instructions to Candidates:

- This paper is preceded by a 10- minute reading period. The supervisor will indicate when answering may commence.
- This paper has 4 questions.
- Answer all questions in the booklet given.
- The total marks for the paper are 100.
- 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

Question 1 ISO 27001 (25 marks)

Read following popular security breaches of the decade and answer all the questions.

MoviePass

When: Aug. 20

Number of people affected: Tens of thousands of users and more than 160 million records

What happened: A report from cybersecurity company "SpiderSilk", obtained by TechCrunch, found that 160 million MoviePass records were left unencrypted. Because the company's database wasn't password protected, it left customers' credit card numbers and credit card details exposed. The database remained online until Tuesday. MoviePass didn't immediately respond to request for comment. This isn't the first time MoviePass has landed in hot water. Earlier this month, the service faced criticism for changing passwords to keep users from ordering tickets. The company has also been accused of spiking prices at peak times. Last year, the company was said to be reactivating accounts and asking former customers to opt out of being subscribed again.

Equifax

When: Approximately mid-May 2017

Number of people affected: About 143 million people

What happened: Hackers stole customer names, Social Security numbers, birthdates and addresses in a hack that stretched for three months. In addition, hackers nabbed 209,000 credit card numbers and 182,000 documents containing personal information. It's unclear what the hackers did with the data during that time. The company estimates that half of the US population was affected but didn't include international victims. It was the biggest known leak of 2017. You can still check to see if you were affected, worthwhile since you might get reimbursed for it. The credit reporting company agreed to pay between $575 million and up to $700 million on July 22 as part of a settlement with the Federal Trade Commission.

Yahoo

When: 2013- 2014

Number of people affected: 3 billion

What happened: Yahoo users were urged to change their passwords after hackers stole personal information associated with about half a billion email accounts. At the time, the numbers made it the biggest data breach in history. Initially, the casualties were reported at 500 million, still making the hack the biggest in history. Yahoo slowly raised the number but reported in 2017 that none of its 3 billion accounts had gone unscathed in the original breach. That's 3 billion names, email addresses, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions. The culprit? A 23-year-old Russian hacker-for-hire named Karim Baratov. Baratov was sentenced to five years in prison, paid the victims restitution and $2.25 million in fines. Yahoo didn't go without punishment either. The company had to pay $50 million in damages and provide credit monitoring for at least two years for about 200 million people who'd been hacked.

a. Briefly explain what is meant by information assets. (3 marks)

b. Describe the need of ISO 27001 implementation to an organization (3 marks)

c. Briefly explain main risk treatment methods (4 marks)

d. Identify the importance of developing risk assessment for an organization. (5 marks)

e. Identify security breaches in above mentioned scenarios and fill out the threat/vulnerability accordingly (At least for 3 assets)

Asset	Threat	Vulnerability	Probability	Impact	Raw risk	Non detectability	Control	Risk level

(10 marks)

Question 2 ITIL (25 marks)

a. List 4 P's of service management (4 marks)

b. Briefly explain what is meant by "service" in ITIL (2 marks)

c. "There's no doubt the various versions of the ITIL framework have transformed ITSM. They've helped countless IT departments to improve their performance, while saving a massive amount of work, by providing clear guidelines on how best to go about their most important tasks".

   i. Analyze how the ITIL framework has shaped IT support departments to go about their daily tasks. (6 marks)

   ii. Briefly describe what are the challenges of implementing ITIL in a traditional organization (6 marks)

d. "NewGenApps" is a startup company with one branch. They are planning to expand the organization by opening two branches in Kandy and Galle. Organization decided to transfer workload – applications, websites, database, storage, physical & virtual server, and entire data center to the cloud environment. As an ITIL consultant create a guideline on how to use service transition processes as a strategic road map for cloud migration.

(7 marks)

Question 3 ISO 20000 & ISO 31000 (25 marks)

a. Identify the impact of ISO 31000 standard on business continuity. (6 marks)

b. Using a diagram explain the process for managing risk focuses on individual or group of risks.

   (Hint: You may use "process" define in ISO 31000 overview diagram) (6 marks)

c. Define the main focus of ISO 20000 standard (5 marks)

d. Clients of ABC company always complaints about the quality of IT services provided by the company. As an ISO 20000 consultant you are recommend to implement ISO 20000 by giving the benefits of implementation to the ABC organization.

(8 marks)

Question 4 ISO 9001 (25 marks)

a. Identify what is customer focus principle in ISO 9001:2008 (5 marks)

b. Using a diagram explain the implementation and certification process of ISO 9001

(Hint: You may use a flow chart) (8 marks)

c. Justify "Why an organization would certify with ISO 9001?" (12 marks)

END OF THE QUESTION PAPER