Sri Lanka Institute of Information Technology

# B.Sc. Special Honours Degree in Information Technology

Field of Specialization: Cyber Security

Final Examination
Year 3, Semester 2 (2018)

# IT 351 – Enterprise Standards for Information Security

Duration: 2 Hours

Instructions to candidates:

- This paper is preceded by a 10- minute reading period. The supervisor will indicate when answering may commence.
- Answer all questions.
- Total Mark 100.
- This paper contains 4 (Four) Questions on 3 (three) pages with a cover page.

## Question 1 (ISO – 27001) (25 marks)

**Read following popular security breaches of 2008 and answer all the questions.**

**Bank of New York Mellon**

An unencrypted backup tape with 4.5 million customers of the Bank of New York Mellon went missing on Feb. 27, after it was sent to a storage facility. The missing tape contains social security numbers and bank account information on 4.5 million customers - including several hundred thousand depositors and investors of People's United Bank of Connecticut, which had given Bank of New York Mellon the information so it could offer those consumers an investment opportunity.

**Hannaford Data Breach**

In March, the Maine-based Hannaford Brothers grocery store chain announced that 4.2 million customer card transactions had been compromised by the hackers. More than 1800 credit card numbers were immediately used for fraudulent transactions.

The affected banks and credit unions were forced to reissue the credit and debit cards. Within two days of the breach announcement, two class action suits had been filed on behalf of customers against the retailer. The retailer claims its systems were PCI-compliant and had passed a PCI assessment shortly before the hack was discovered.

**Countrywide Insider Theft**

In August, a former Countrywide Financial Corp. senior financial analyst, Rene Rebollo, was arrested and charged by the FBI for stealing and selling sensitive personal information of an estimated 2 million mortgage loan applicants. How he did it over a two-year period was to download about 20,000 customer profiles each week onto flash drives, working on Sunday nights, when no one else was in the office. Rebollo then took the excel spreadsheets of business center stores and email it to buyers.

Countrywide, now owned by Bank of America, was already facing money and reputation issues because of the subprime loan meltdown before it faced the insider threat of Rebollo.

a. What is the main focus of ISO 27001 standard?
b. What is the importance of developing risk assessment for an organization?
c. Briefly describe PDCA model in ISO 27001 implementation
d. 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 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

(25 marks)

## Question 2 – (ITIL) (25 marks)

"Steering committee of ABC Company has decided to move five (5) critical servers to cloud environment"

You have been asked to provide a consulting report by considering the following:

What are the advantages, disadvantages, and service desk requirements for the ABC organization, in your answer consider

- Is the above a good strategic decision?
- How to design the migration?
- How to do a service transition?
- How to do service operations?
- How to do continuous service improvement?
- Required to cover IT service management Concepts.

(25 marks)

## Question 3 – (ISO 20000) (25 marks)

a. What major benefit would be added to an organization by following the standard ISO 20000?

(4 marks)

b. Compare similarities between ITIL and ISO 20000.

(4 marks)

c. Define Specification and Code of practice with reference to ISO 20000.

(4 marks)

d. Write a consultancy report on how to implement a quality by accreditation with ISO 20000.

(13 marks)

## Question 4 – (ISO 31000) (25 marks)

a. What are risk, risk management and effective risk management?

(6 marks)

b. Using a diagram explain an overview over view of ISO 31000?

(6 marks)

c. Write a report on "Why an organization would certify with ISO 31000? "

(13 marks)