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 (2017)

IT 351 – Enterprise Standards for Information Security

Duration: 3 Hours

Instructions to candidates:

- Answer all questions.
- Total Mark 100.
- This paper contains 5 (Five) Questions on 9 (Nine) pages with a cover page.

Part 1 – Answer the following Multiple Choice questions [you may write the question number and the correct answer/s (a, b, c, or d only)]

Question 1 – MCQs (20 marks)

1. A customer-based Service Level Agreement structure includes:

A . an SLA covering all Customer groups and all the services they use

B . SLAs for each service that are Customer-focused and written in business language

C . an SLA for each service type, covering all those Customer groups that use that Service

D . an SLA with each individual Customer group, covering all of the services they use

2. Which of the following would normally be included in a Capacity Plan?

1 Options

2 Management summary

3 Business workload forecasts

4 Backout plans

A. 2, 3 and 4

B . All of them

C . 2 and 3 only

D . 1, 2 and 3

3. An IT department is seeking to set its prices to match those of external suppliers selling the same services. Which one of the following is the best description of this approach?

A. The going rate that is agreed with Customers

B. Market rate

C . Cost-plus

D. Profitable

4. Which of the following is not an element of Availability Management?

A. Verification

B. Security

C. Reliability

D. Maintainability

5. The extent of CI information held in the CMDB should:

A . be as detailed as possible so that frequent reports can be produced to avoid spending alot of money

B. be as high level as possible

C . match the organisation's requirement for information to be held

D . vary according to cost

6. ISO/IEC 20000-1 can be applicable to a service provider:

A. Even if its customers or suppliers have demonstrated conformity to ISO/IEC 20000 requirements

B. Only if its suppliers have demonstrated conformity to ISO/IEC 20000 requirements

C. Only if its suppliers haven't demonstrated conformity to ISO/IEC 20000 requirements

D. Only if its customers have demonstrated conformity to ISO/IEC 20000 requirements

7. In the Plan-Do-Check-Act (PDCA) methodology, which can be applied to all processes, what does the ACT phase cover?

A. Implement a process

B. Take an action to improve process performance

C. Establish objectives and processes to deliver results

D. All of the above

8. For a Service Provider, the first step for developing an information security policy is:

A. classifying information assets

B. setting an owner of its information asset

C. overviewing past experiences

D. aware staff

9. Which of the following could be excluded from configuration management?

A. The relationships between configuration items and service components

B. The requests for change of configuration items

C. The financial management of configuration items

D. None of the above

10. The number of personnel and the experience and qualifications of personnel assigned to conduct an audit should be dependent on:

A. The scope of the audit

B. The time available to perform the audit

C. The purpose of the audit

D. All of the above

Part Two – structured Questions

Question 2 – (ITIL) (20 marks)

a) What is IT Service Management? Briefly discuss the objectives of ITIL.

[4marks]

b) What is Configuration Management? Discuss the advantages of maintaining a Configuration Management Database (CMDB) within an organization.

[4 marks]

c) Briefly discuss the functions of the Service Desk and state 3 problems of not having a service desk within an organization.

[4 marks]

d) What are the objectives of Service Level Management? Illustrate the process of service level management using a diagram?

[4 marks]

e) Briefly discuss what is mean by Incident Management and the activities involved in incident management process.

[4 marks]

Question 3 – (ISO 27001) (20 marks)

Read the following case study and answer the questions given below.

Introduction

The Business is a very small business in it's tenth year of operation. It has one full-time employee, the owner, and occasional part-time help from the owner's husband and various employees hired on a short-term "Casual Labour" basis. Last year the Business had under $100,000 in gross sales. The Business is in the business of retail sales over a dedicated WWW site and via the mails. More specifically, it is in a niche market, one of only a handful of businesses in exactly this market on the entire Internet. Only over the Internet are there sufficient buyers for this business to be a full-time job. There are many companies like this in the United States.

Before

The first step in the audit was to get initial impressions and a general understanding of the Business, for context on what the owner told me. I (Refer to the Auditor) toured the physical office setup and stock storage areas, and then followed some customer orders through the process from the customer through order fulfilment to records storage and retention.

The Physical Setup

The office for the Business is a single dedicated room in the owner's house, an outwardly unremarkable dwelling in a middle-class neighbourhood. The office has the following physical security: there is a deadbolt lock on the (solid core wooden) door. This lock is not on the same master key as other doors in the house. There are two 1' x 4' openable windows, both of which are normally closed when the office is not in use. The house, which is 100' from its nearest neighbour and 50' from the road, has smoke alarms and external motion-sensor lights.

In the office are the following computers and equipment:

· A Macintosh G4 desktop computer ("the Big Mac") that stores the owner's and company's email, customer orders, and the Business's financial records.

· A gray-box PC used for personal use and for editing the website.

· An old desktop PC running Linux. This computer serves as a staging server for the website (the actual production site is offsite at a shared hosting facility).

· A Macintosh iBook laptop computer that stores the inventory database and the credit card authorization software (and hence a database of past credit card transactions).

· An HP LaserJet 4 network printer.

· A wireless/wired cable modem router/firewall appliance.

· Two Game Consoles used by the employees to play games in free time.

All but the iBook are connected together via normal category five network cabling; the iBook uses an Airport card to connect to the network and a modem to dial up the Business's credit-card authorization provider. All computers are using NAT and DHCP provided by the router and have IP addresses in a private IP range. There are no other computers connected to this network. Stock is stored in filing cabinets and in plastic bins in the (attached) garage. The other half of the two-car garage is used for general household storage.

The Ordering Process: Web Orders

Web orders, which comprise over 90% of the Business's orders, come to the Business in the following way. A customer browses the Business's website, which is hosted on a shared server at a commercial hosting facility. This site is running an open source shopping cart system written in Perl and heavily modified by the owner's husband. When the customer submits an order, the order is filed in an order log and two emails are sent. The customer gets an order summary (minus credit card information); the owner gets a terse note that says simply "You have an order, Boss."

The owner then FTP's to the server from the Big Mac and downloads the order log. After verifying that it looks correct and complete, she replaces the server's order log with a blank document. The orders in the order log are then split into separate documents, printed, and saved, named by customer name and order date, into an"Orders" directory on the hard drive of the Big Mac. The printed copy of the order, containing all customer information, is placed onto an "Orders" clipboard.

The Ordering Process: Phone Orders

Phone orders, which comprise approximately 3% of the Business's orders, come to the Business in the following way. A customer calls the Business (on the Business's own phone line: the home phone is separate) and states that she wishes to place an order.

The owner or her husband, grabs a scrap of paper (quarter sheets are kept near all Business phones) and writes down the order and all of the customer's information, including her credit

card number. The order is then scotch-taped to the owner's computer monitor until it is placed onto the "Orders" clipboard.

The Ordering Process: Mail orders

Mail orders, which comprise another approximately 3% of the Business's orders, come to the Business in the following way. A customer writes an order down and mails it to the Business with a money order. The Business hopes that customers use the written order form from the website for this purpose, but they do not more often than they do. The owner places the money order in a bank bag for deposit and places the order onto the "Orders" clipboard.

Order Fulfilment

The owner (or an employee) takes the "Orders" clipboard to the garage, pulls from stock the required items, and brings them back to the office. If an item is not in stock, the order is placed on the "Back Orders" clipboard, and the customer is notified. For each order she fills, she creates a customer record (if there is none) on the iBook, opens the sale in the POS (point of sale) software, and runs the customer's credit card (if not a mail order) in the credit card authorization module.

When the transaction is authorized, she closes the sale and prints two copies of the receipt. She then packages the order and uses the PC to create a mailing label. One copy of the receipt goes into the package; the other is retained for records. In the late

afternoon of each day, the owner drives to the Post Office and mails all the packages. Order fulfilment is complete.

Data Storage/Retention

The owner takes the remaining copy of the receipt from each order, staples it to the order itself, and places them in a pile. At the end of the day, these orders and receipts are gathered, attached to the credit card settlement report, and filed by day in a file folder. Each month gets one or more labelled file folders, depending on volume; each year gets one or more labelled file boxes in the garage.

At the end of the day, the owner also goes through the receipts from the packages being shipped that day and moves the order files on the Big Mac into an "Orders Shipped" directory. These are kept forever, sorted by year, then by month, then by order date and customer last name. The file boxes are kept on open wooden shelves in the garage for seven years, the record retention time specified by the Business's credit \card service provider. At the end of that time, the files are shredded.

Policies

The Business has very few policies, all related to customers' orders and promises regarding customers' privacy. There were no other written policies or procedures. Employees, who are always casual labour hired for the short term (when the Business gets a huge rush or the owner is otherwise getting behind), work under the owner's direct supervision, getting orders filled and

out. They do not get or require keys or logins to the computers: when an employee is working, the owner logs herself into all computers that require it.

a) If you are the CIO for this organization, write a memo to all the organizational employees explaining the benefits and costs of implementing ISO 27001 for this organization.

[6 marks]

b) How important to handle third party (vendors/consultants/suppliers) organizations in an ISO 27001 implementation.

[7 marks]

c) Write a small report to show the risks within the organization on the threat/vulnerability study

[7 marks]

Question 4 – (ISO 31000) (20 marks)

ISO 31000:2009 is:

- An international standard that provides principles and guidelines for effective risk management
- Not specific to any industry or sector
- Able to be applied to any kind of risk
- Able to be applied to any kind of organization
- Intended to be tailored to meet the needs of the organization

"The generic approach described in this Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context."

a. What major benefit would be added to an organization by following the standard ISO 31000?

[4marks]

b. Explain the reason behind organization's need to follow ERM (Enterprise Risk Management) programs.

[4marks]

c. Explain the process of internal auditing and its impact for compliance certificates

[4marks]

d. What are the specific measurable performance goals, measures and targets that will use to demonstrate the achievement of objectives and the improvement of organizational and individual performance?

[4marks]

e. Is risk management tailored and embedded in all the organization's culture, practices and processes (esp. policy development, business and strategic planning) in a way that it is adequate, relevant, effective and efficient?

[4marks]

Question 5 – (ISO 20000) (20 marks)

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

[4 marks]

b. Compare and contrast similarities between ITIL and ISO 20000.

[4 marks]

c. ISO 20000 Standard is divided into two distinct parts:
Part 1 - Specification
Part 2 - Code of Practice for Service Management

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

[4 marks]

d. What is Availability Management and discuss the advantages of maintaining a Availability Management within an organization.

[4 marks]

e. Write a report to MD/CEO, describing the importance of IT Service Continuity Management with an organization.

[4 marks]

End of Paper