UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION
JANUARY 2016 SEMESTER

COURSE CODE	:	IKB 31103
COURSE NAME	:	BUSINESS CONTINUITY PLANNING
PROGRAMME NAME	:	BIT (HONS) IN COMPUTER SYSTEM SECURITY
DATE	:	28 MAY 2016
TIME	:	9.00 am – 11.30 am
DURATION	:	2 HOURS 30 MINUTES

INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of TWO (2) sections; Section A and Section B.
4. Answer ALL questions in Section A. For Section B answer ONE (1) question ONLY from question 4 or question 5.
5. Please write your answers on answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 8 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

SECTION A (Total: 75 marks)

INSTRUCTION: Answer ALL questions.
Please use the answer booklet given.

Question 1

(a) You have been assigned by your manager to give presentation to your colleagues in your department regarding the importance of having Business Continuity Plan (BCP) in your organization. The presentation should include the definition of BCP and elaborate **THREE (3)** reasons why the organization should have BCP.

(8 Marks)

(b) In completing the business continuity plan, one of the process is conducting risk management, there are three main components of process in risk management; risk identification, risk assessment and risk control. Briefly explain the process of each component in risk management.

(6 marks)

(c) Give **FIVE (5)** components of IT systems that one should consider when identifying risk for IT system.

(5 marks)

(d) An organization most likely will have several risk categories to analyze and identify risks that are specific to the organization. Briefly explain **THREE (3)** categories of risk.

(6 marks)

Question 2

(a) Conducting risk management process involves issues on budget, time and resources. Suggest **THREE (3)** alternate approaches if the company faced issues such as lack of budgets, time and have similar infrastructure.

(6 marks)

(b) To ensure the effectiveness of any plan put in place for contingency operation, it must be tested. Identify **FIVE (5)** types of testing that a BCP team can carry out to test their BCP.

(5 marks)

(c) Indicate **SIX (6)** minimum audit plans when you have completed with your BCP to review the plan to assess whether it meets the company's overall needs.

(6 marks)

(d) Maintaining the BCP is the biggest challenge in the whole processes because there are constant changes in the organization. Explain **TWO (2)** methods to maintain the changes.

(8 marks)

Question 3

(a) Once you have decided to test your BCP plan, there are steps to implement the testing. Elaborate the **FOUR (4)** steps.

(8 marks)

(b) Why getting involvement of top management is vital in BCP?

(4 marks)

(c) In implementing the business continuity plan, there are phases of implementation of the plan after the disaster happen. Describe the following phases below.

(6 marks)

i. Activation Phase
ii. Recovery Phase
iii. Business Continuity Phase

(d) As an IT Manager and also part of BCP team, you are required to keep all company's data in a secured and safe environment and condition. One of the tasks you should consider is to back up the data. You are required to analyze the characteristics of **TWO (2)** types of data backup commonly use in risk mitigation strategies; full backup and incremental backup.

(4 marks)

(e) Commercial recovery sites permit an organization to continue computer and network operations in the event of a computer or equipment disaster. Indicate **THREE (3)** types of commercial recovery sites available.

(3 marks)

SECTION B (Total: 25 marks)

INSTRUCTION: Answer ONE (1) question.
Please use the answer booklet given.

Question 4

(a) There was a fire at a factory and 80% of the building was destroyed. The damage to the building was $800. Fire statistics reveal that the SaNa-ONE factory has had a similar fire an average of once every five years. Senior management decides to spend RM1200 installing a fire prevention system in the newly repaired factory. This system requires a RM 100 per year maintenance contract that extends the warranty of the fire prevention system to 15 years assuming the maintenance is performed annually. The warranty covers the cost of all repairs including parts and labor.

i. Given that the cost of the damages to the building was RM 800, what is the total asset value of the SaNa-ONE Factory?

(4 marks)

ii. Would you advise the management for or against buying the fire prevention system? Give your evaluation using calculations to prove your answer.

(7 marks)

iii. What is the Annual Rate of Occurrence (ARO) of fires at the SaNa-ONE factory? Show the calculation.

(3 marks)

iv. What is the Annual Loss Expectancy (ALE) due to the fires at the SaNa-ONE factory? Show the calculation. (3 marks)

(b) Your company sells Lenovo PC online and has suffered many DOS attacks. Your company makes an average RM 20000 profit per week, and a typical DOS attacks lowers your sales by 40%. You suffer seven DOS attacks on average per year. A DOS-mitigation service is available for a subscription fee of RM 10000 per month. The service has been tested and it is convinced that it will mitigate the attacks.

i. Calculate the Annual Rate of Occurrence

(2 Marks)

ii. What is the Annualized Loss Expectancy of lost iPod sales due to the DOS attacks?

(3 Marks)

iii. Is the DOS mitigation service a good investment?

(3 Marks)

Question 5

A widget manufacturer has installed new network servers, changing its network from a peer-to-peer network to a client/server-based network. The network consists of 200 users who make an average of $20 an hour, working on 100 workstations. Previously, none of the workstations involved in the network had anti-virus software installed on the machines. This was because there was no connection to the Internet, and the workstations didn't have floppy disk drives or Internet connectivity, so the risk of viruses was deemed minimal. One of the new servers provides a broadband connection to the Internet, which employees can now use to send and receive email, and surf the Internet. One of the managers read in a trade magazine that other widget companies have reported an 80 percent chance of viruses infecting their network after installing T1 lines and other methods of Internet connectivity, and that it may take upwards of three hours to restore data that's been damaged or destroyed. A vendor will sell licensed copies of anti-virus software for all servers and the 100 workstations at a cost of $4,700 per year. The company has asked you to determine the annual loss that can be expected from viruses, and determine if it is beneficial in terms of cost to purchase licensed copies of anti-virus software.

The question below is referring to above case scenario;

(a) What is the Annualized Rate of Occurrence (ARO)?

(2 marks)

(b) What is the value of ARO for above risk?

(3 marks)

(c) Define Single Loss Expectancy and calculate the Single Loss Expectancy (SLE) for this risk.

(10 marks)

(d) Using the formula ARO x SLE = ALE, calculate the Annual Loss Expectancy.

(6 marks)

(e) Determine whether it is beneficial in terms of monetary value to purchase the anti-virus software by calculating how much money would be saved or lost by purchasing the software.

(4 marks)

END OF EXAMINATION PAPER