JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN IT AND SECURITY AUDIT

2ND YEAR 1ST SEMESTER 2016/2017 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE   : IIT 5216

COURSE TITLE   : DISASTER RECOVERY PLANNING AND BUSINESS CONTINUITY

EXAM VENUE   :   STREAM   :

DATE   : Dec 2016   EXAM SESSION   :

TIME: 2.00 HOURS

INSTRUCTIONS:

1. Answer Question 1 (Compulsory) and ANY other two questions
2. Candidates are advised not to write on the question paper
3. Candidates must hand in their answer booklets to the invigilator while in the examination room

QUESTION ONE 20 MARKS

a) Describe the following terms as used in database backup as a form of disaster recovery planning techniques.
   - i. Logical Backups **(2 Marks)**
   - ii. Cold backups **(2 Marks)**
   - iii. Hot backups **(2 Marks)**

b) Backup encryption should be one of many activities that formulate a comprehensive security strategy. In many environments, storage has operated outside of the realm of security officers for some time, as their main focus has been primarily on areas such as perimeter security, intrusion detection/prevention and protection of host systems. As a result, the storage infrastructure – both primary storage and especially copies of primary storage – is likely to be an Achilles' heel when it comes to security. Policies for data security are a corporate concern and should be a fundamental element of an enterprise security strategy. Strategic security policies can then spawn tactical and operational policies through the joint efforts of the security and storage organisations. To that end, storage must become an integral part of the corporate security strategy.

Task
You are required to describe at least five best practices for protecting backup data **(10 Marks)**

c) A successful Business Continuity Management (BCM) programme, established to respond to any potential disruption, is essential for all organisations. Ensuring a holistic Business Continuity Management System (BCMS) is in place will not only help your organisation recover from disasters, it will also prevent the reputational damage that can arise from any operational outages, missed deadlines, upset customers, or direct financial loss. Certification against the requirements of ISO 22301, the International standard for Business Continuity Management, enables you to demonstrate your commitment to having a most robust BCMS in place. ISO 22301 provides a comprehensive set of controls based on BCM best practice, covering the whole BCM lifecycle. It defines the strategic and tactical capability of an organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level. You are required to explain atleast four benefits of ISO 22301 certification to an organization. **(4 Marks)**

QUESTION TWO 20 MARKS

a) Business Continuity Plans (BCP) are the detailed, documented recovery plans that give management and staff the blueprint to adjust to and continue to operate despite the impacts of a disruption. Describe the content of BCP of any organization of your choice.
(4 Marks)

b) Business Continuity Plans (BCP) are the detailed, documented recovery plans that give management and staff the blueprint to adjust to and continue to operate despite the impacts of a disruption. As an expert in Disaster Recovery Planning and Business Continuity, you are tasked with the responsibility of differentiating the following terms;
   - i. Disaster Recovery **(2 Marks)**
   - ii. Resumption Planning **(2 Marks)**
   - iii. Contingency Planning **(2 Marks)**
   - iv. Emergency response **(2 Marks)**
   - v. Recovery Time Objectives (RTO) **(2 Marks)**
   - vi. Recovery Point Objectives (RPO) **(2 Marks)**

c) In the process of establishing continuity culture in an organization, documenting the Disaster Recovery Plan is one element of developing a strategy. The plan's success, however, depends upon some factors. You are required to highlight those factors. **(4 Marks)**

QUESTION THREE 20 MARKS

d) Majority of business organizations tests their business continuity processes ones or twice a year, however, this can be increased due to some factors in a given organization. As an expert of Disaster Recovery Planning and Business Continuity explain at least FIVE of those factors. **(10 Marks)**

e) Conducting same test twice a year would quickly lead to stagnant outcomes and boredom among the participants. Describe atleast FIVE types of test available for organizations and their implications. **(10 Marks)**

QUESTION FOUR 20 MARKS

a) Should social media be a component of organization's business continuity program? Discuss. **(6 Marks)**

b) What are some best practices of monitoring social media during a crisis event? **(8 Marks)**

c) Communicating through a social media channel present a range of potential risks that companies needs to monitor in general. What are the risks of using social media to support business continuity program? **(6 Marks)**

QUESTION FIVE 20 MARKS

a) What is a Business Continuity Plan? **(1 Mark)**

b) Describe FOUR situations in which a business continuity plan would be helpful. **(8 Marks)**

c) The key to coping with Information System disasters is advance planning and preparation, identifying activities that will keep a business viable when the computing technology is disabled. Outline three steps in business continuity planning. **(6 Marks)**

d) Investigate your university's or employer's security plan to determine whether its security requirements meet all the conditions we studied during this course. Outline atleast FIVE Network security threats **(5 Marks)**