

Fundamental Concepts of Data Security

ISEC2001/ISEC5006

Business Continuity II

Question 1

Explain the fundamental difference between business continuity planning (BCP) and disaster recovery planning (DRP).

Question 2

What is business impact analysis (BIA), and what is it used for?

Question 3

What is the fundamental difference between BIA and risk assessment?

Question 4

The comprehensive approach to emergency or disaster management typically consists of four phases: Prevention, Preparedness, Response, and Recovery (PPRR). Which phase does Business Impact Analysis (BIA) belong to? Describe two (2) examples of critical activities of a typical software firm that need to be established as part of business impact analysis.

Question 5

Explain why it is important for large organisations to have a proper BCP in place? What is the implication if a lack of BCP is found?

Question 6

Consider the statement “*Business continuity planning is only about recovery of computer systems.*” Is it true or false? Explain your reasoning.

Question 7

Does business continuity planning provide any additional benefits to an organisation apart from providing the ability to recover from major disruptive events.

Question 8

Describe the advantages and disadvantages of hot sites.

Question 9

Describe the advantages and disadvantages of cold and warm sites.

Question 10

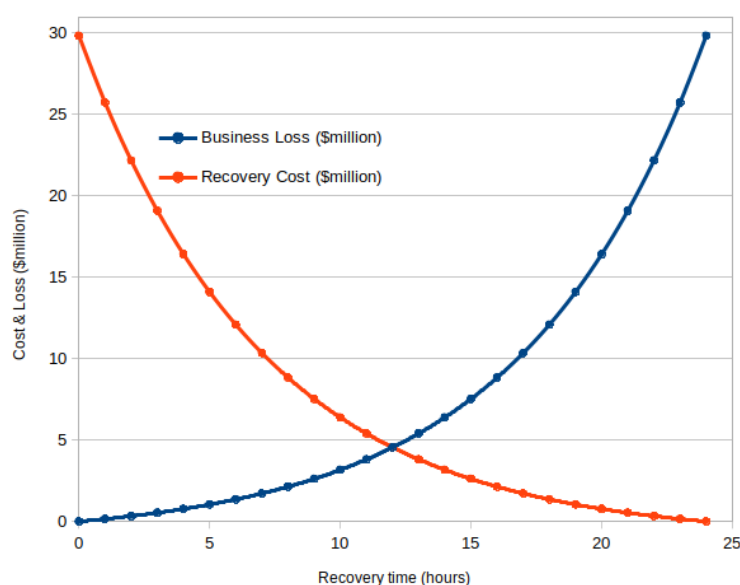
What is the fundamental difference between recovery time objective (RTO) and maximum tolerable downtime (MTD)? Suppose that RTO has been fixed, which aspects of data backup could be influenced by MTD? Discuss.

Question 11

What are the the MTD, RPO, RTO values of the following scenario: *Susan is the new BCM coordinator and needs to identify various preventive and recovery solutions her company should implement for BCP/DRP efforts. She and her team have carried out an impact analysis and found out that the companys order processing functionality cannot be out of operation for more than 15 hours. She has calculated that the order processing systems and applications must be brought back online within eight hours after a disruption. The analysis efforts have also indicated that the data that are restored cannot be older than five minutes of current real-time data.*

Question 12

The BIA team of an organisation is determining the recovery time of their core system due to a disaster. The team has been able to plot the relationships between the business loss (due to ceasing of critical business activities) and the recovery cost (due to offsite facility and other related expenses) against recovery time below. The core system definitely needs to be recovered within 24 hours and the BIA team believes that a much quicker recovery can be achieved. Suppose that this is the only information available, suggest the *optimal* recovery time that the BIA team should aim for and explain your suggestion. Your argument must be based on the plot given below.



Question 13

What are the three main phases in a contingency plan as per the NIST SP800 standard? Briefly describe the activity in each phase.