**CLA #3 BIA & disruption scenario planning**

**Question 1: Crisis versus Disaster (3 marks)**

 (a) How does  HB 292-2006  distinguish a crisis from a disaster?   (1.5 marks)

HB292-2006 is a guide that provides a summary of both currently accepted and emerging practices in managing disruptions, used within Australasia, USA and UK. According to it, both crisis and disaster are considered to be unexpected events that result in disruption of daily operations of either a part of or full organization (as it requires diverting attention, energy and time from normal operations). The difference between them is that during crisis, management can still cope, whilst during disaster, the management has been overwhelmed.

(b) How would this type of distinction inform crisis management in your role at Nike. Consider the information presented in figure 2 in chapter in giving your response (1.5 marks)

My role in Nike is that of a Senior Crisis Management consultant who would need to perform several task, including:

* Translating business requirements into technical recovery plans and tools (to test, promote and implement them),
* Conducting risk and impact assessments,
* Defining and validating recovery requirements, capabilities, priorities, metrics and reports,
* Performing crisis management exercise, etc.

Thus knowing about the difference would help me properly prioritize, plan and prepare for all crisis, ensuring that I don’t miss any small events (like harassment, discrimination, etc.) which could escalate to disastrous levels.

**Question 2. BIA and disruption scenarios (5 marks)**

(a) What is a business impact assessment and why are disruption scenarios helpful in planning for a business impact assessment? (3 marks)

According to HB292-2006, it’s a process that analyses how certain disruption risk scenarios effect an organization’s operations and notes the resources and capabilities that are needed to manage them. This helps the organization identify areas of improvement and develop ways to protect it from those disruption’s consequences.

Thus, disruption scenarios are extremely helpful here as they help determine the source of disruption, resources that are directly affected by it and the key resources or areas that they are linked to. This in turn helps the organization understand the value these resources hold (in terms of organizational objectives), estimate the impact of their disruption and also find the ways to manage them. Basically, disruption scenarios lead the organization into developing BIA.

(b) Please provide your Nike interviewers with a relevant example of a Disruption Scenario. Your example should describe the benefits of disruption scenario planning in your answer (2 mark)

An example of a relevant disruption scenario would be a DDOS (distributed denial of service) attack occurring on nike.com (a digital platform of Nike). This would have a direct effect of overloading the resources (like servers) used to maintain the platform, which would prevent customers from accessing products and services. Thus, it would result in the company losing out on potential sales, crucial information for growth of business (like consumer analytics), business reputation, etc. Hence by planning for it, Nike would know which resources are connected to nike.com, the full level of impact it will have to Nike’s organizational objective and also realize the impacts of similar attacks on its other digital platforms.

**Question 3. Recovery Objectives (2 marks)**

 (a) What is a recovery objective / metric (1 mark)

It basically sets the maximum tolerable downtime by stating the minimum level of capability that the organization aims to recover in a certain time after a disaster occurs. It is divided into two parts, recovery point objective (point in time to which system and data must be recovered) and recovery time objective (time taken to recover it).

(b) how would it apply in the context of the disruption scenario and impact assessment you have just described at 2b above? (1 mark)

It can be used to set a limit to the time needed to bring system back to pre-disaster condition, like aiming to ensure at least 75% of the server and resources used for the nike.com are functional within 12hrs of the DDOS attack.