Student:	Email:
Kaleb Alstott	alstottk1@mymail.nku.edu

Time on Task:	Progress:
	100%

Report Generated: Friday, December 3, 2021 at 4:40 PM

Guided Exercises

Part 1: Research the Business Impact Analysis Process

3. **Explain** Figure 3-2: Business Impact Analysis Process for the Information System on Page 16.

Looking into the figure of 3-2, business impact analysis process for the information system, we can first start with the stockholders input which then defines what possible critical business functions/processes that. Once identified we then move onto the possible potential impacts of these CBF and potential downtime which gives us an idea of how and when we should schedule such process and who it will be affecting. After this step we keep moving down the chart to possible components or equipment that would be involved with said process, which then implies a specific recovery time in order to start the system back up. Notice how the downtime should always be higher than you're revery time. Finally, we have an FIPS 199 chart which identifies the possible impact levels into 3 security objectives which are confidentiality, integrity, and availability.

4. **Explain** Figure 3-3: Cost Balancing on Page 18.

To start we can identify that in a cost balancing chart there is an optimal point between the cost to recover and the cost of disruption, and that optimal point is called the cost balance point. When looking at the chart we can see when the longer disruption occurs the higher the cost will be. Vise versa, when there is a shorter RTO the more expensive the recovery costs will comet to be. To find the optimal approach for a company you need to plot the cost balance points which will show an optimal point between disruption and recovery costs.

5. **Summarize** the BIA process in your own words.

To summarize a BIA we would always start off with the role of the ISCP coordinator and stakeholders. The next goal that we would look at in a BIA is the CBF and process of the business. Once identified we would then start to identify the systems and technology that supports the CBF. This step helps us move on to identifying such things as MTD, RTO, RPO, etc values. Which lastly comes to our conclusions of what availability, confidentiality, and integrity does the BIA hold in each of the processes taking place.

Part 2: Explore the BIA Template

3. **Review** the template and **describe** the three main sections.

In this template we can see that this is an introduction used to describe the purpose of the BIA system and what it is. This section is all about the information systems such as the physical and logical standpoint of the business process along with the system descriptions. Lastly there is a big data collection that describes how the data will be gathered and retrieved.

5. **Map** the subsections under Section 3 with the subsections under Section 3.2 of NIST SP 800-34.

3.1-Determine Process and System Criticality NIST SP 800-34 3.2-Identify Resource Requirements NIST SP 800-34 3.2.1-Determine Business Processes and Recovery Criticality 3.2.2-Identify Resource Requirements Template 3.2.3-Identify System Resource Recovery Priorities 3.3-Identify Recovery Priorities for System Resources NIST SP 800-34

6. **Describe** the Maximum Tolerable Downtime (MTD) value.

MTD is the total amount of time the system owner is willing to allow for a business process outage that also includes the possible impacts that may happen.

7. **Describe** the Recovery Time Objective (RTO) value.

Recovery Time Objective (RTO) value is the maximum amount of time that a system resource can remain unavailable before there may be an unacceptable impact on other systems or system resources.

8. **Describe** the Recovery Point Objective (RPO) value.

The recovery point objective (RPO) value is the point in time prior to a system outage in which a businesses data can be recovered after the outage.

9. **Explain** the relationship between MTD and RTO.

The relationship between MTD and RTO is that the RTO is used to select and identify the appropriate technologies for the MTD. Once again the RTO needs to always be less than the MTD.

10. **Explain** the difference between RTO and RPO.

The difference between an RTO and RPO is that RPO is not considered part of the MTD. Instead the RPO is like a factor or contribution about how much data loss and cost the business process can tolerate during the recovery process

Challenge Exercise

Identify the impact to Cost for the eCommerce business process and explain why you chose that impact level.

High, this was because it directly affects the revenue of the company

Identify the impact to Prestige for the eCommerce business process and explain why you chose that impact level.

High, do to Acme being an e-commerce company the possible impact prestige could be ruined

Identify the impact to Cost for the Payroll business process and explain why you chose that impact level.

High, do to the cost of payroll and how its used to pay your employees and deals with the company revenue.

Identify the impact to Prestige for the Payroll business process and explain why you chose that impact level.

Low, internal process has nothing to do with companies impact to prestige.

Identify MTD, RTO, and RPO values for the eCommerce business process, then describe the drivers for these values (for example, customer satisfaction, regulations, performance measures, or compliance with a standard).

MTD: 4-6 hours RTO: 2-3 hours RPO: 24 hours The driver: Customer satisfaction the goal and chance to prestige

Identify MTD, RTO, and RPO values for the Payroll business process, then describe the drivers for these values (for example, customer satisfaction, regulations, performance measures, or compliance with a standard).

MTD: 6-7 days RTO: 4 days RPO: 1 week The driver, payroll should be bi weekly or monthly.

Identify the information systems (servers, security devices, etc.) that play a role in the eCommerce business process.

front-end server, database server, router, firewall, switch, DMZ, PCI DSS, possible multi-factor identification ,

Identify the information systems (servers, security devices, etc.) that play a role in the Payroll business process.

server, domain controller, switch, firewall

Identify the RTO values for each information system you identified in the previous steps and provide justifications.

RTO Values front end server- 2-3 hours database server - 2-3 hours router- 2 hours firewall- 2 hours switch- 2 hours DMZ - 3 hours PCI DSS - 3 hours Multi-factor - 1-2 days