Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

Time on Task:	Progress:
Unknown	100%

Report Generated: Monday, July 7, 2025 at 9:41 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.

This is how a BIA would look like. The first step is to determine mission/business processes and recovery critically. This step would also include the outage impacts and the estimated downtime. The second step would be to identify resource requirements. Here a evaluation of whats needed to return to normal is done. Lastly you need to identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Here there is also Maximum Tolerable Downtime (MTD) which represents the total amount of time the systemowner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. There is also Recovery Time Objective (RTO), which defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Lastly there is Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.

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

This is a cost balancing graph. The longer a disruption is allowed to continue, the more costly it can become to the organization and its operations. Conversely, the shorter the RTO, the more expensive the recovery solutions cost to implement. For example, if the system must be recovered immediately, zero downtime solutions and alternate processing site costs will be much higher, whereas a low-impact system with a longer RTO would be able to implement a less costly simple tape backup system. Plotting the cost balance points will show an optimal point between disruption and recovery costs. The intersecting point (Cost Balance Point) will be different for every organization and system based on the financial constraints and operating requirements.

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

A BIA finds out which systems and services are most important to a company. It looks at what would happen if they stopped working and how long it would take. The results help the company plan how to recover and what to fix first.

Part 2: Explore the BIA Template

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

The three main sections are the overview, system description, and BIA Data collection. The overview introduces the purpose for the BIA. It has the objectives and summarizes the 3 steps that compose the BIA. The system description just wants to get a understanding of the environment and its functionality, knowing everything about things such as physical location, general location of users and more. Lastly the BIA data collection goes through the steps of the BIA. It says "Identify Outage Impacts and Estimated Downtime, Identify Resource Requirements, Identify Recovery Priorities for System Resources"

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

Determine mission/business processes and recovery criticality, identify resource requirements, identify recovery priorities for system resources.

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

The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations

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

RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD

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

The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

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

RTO defines the maximum amount of time a system resource can be unavailable before it seriously impacts operations. MTD is the longest amount of downtime the organization can endure before facing major consequences. The RTO must always be less than or equal to the MTD to ensure recovery happens in time to avoid unacceptable damage. Determining the RTO helps guide the selection of technologies and strategies that meet the MTD requirements.

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

RTO defines the maximum amount of time a system resource can be unavailable before it seriously impacts operations. RPO defines the maximum amount of data loss that is acceptable during a disruption. So RTO deals on how quick recovery needs to happen, and RPO is about how much data can be lost without impacting operations.

Challenge Exercise

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

High: The total cost of the outage to Acme will be over 0K. I chose this impact level because it handles customers and their payments, which is how they get their revenue. If this were to halt, profits would be cut and could hurt their reputation.

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

High: Company image will be ruined, most customers will be lost. eCommerce deals with sensitive information, and if there info would be leaked, their reputation would be dragged in the mud. Customers won't trust the company again, which would hurt financially.

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

Moderate: The total cost of the outage to Acme will be between K and 0K. The payroll business process is crucial to employees. If they don't get paid it could cause dissatisfaction and cause productivity to go down and complaints to fly around. It wouldn't be high, but it would still have a noticeable impact

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

Moderate: Company image will be affected badly, some customer loss. If employees don't get paid and word gets out, customers may stop buying from the company. Not getting paid would affect employee moral, and the companies public image and trust.

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: 3 hours. A downtime that is too long will lose faith from customers. If the downtime is too long sales will be lost, people will complain and buy from other companies RTO: 1 hour. People expect a quick fix for these issues. If its not fixed they'll buy from other place. If there is a quick fix they will also think more highly of your company. RPO: 10 minutes. Having a short RPO is necessary as it minimizes the risk of losing sensitive data

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: 12 hours. If the payment of someone is delayed by 12 hours, they won't complain that much. It would be more of an inconvenience that them complaining. RTO: 4 hours. It impacts employees directly so it should be dealt with quickly to ensure loyalty to employees. Affects employees directly so should be dealt with.RPO: 1 hour. Contains sensitive info, so a short RPO ensures that not that much data is lost

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

Database server, eCommerce Platform, Payment Server, Firewall and Security devices, Network Access Control

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

Payroll server, Database server, Email Server, Backup server, authentication server, SIEM system, Intrustion detection

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

Payroll Server: 2 hoursDatabase Server: 2 hoursEmail Server: 4 hoursAuthentication Server: 30 minutesBackup server: 8 hoursSIEM system: 4 hoursIntrusion Detection System: 4 hours