Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Sunday, November 17, 2024 at 7:10 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.

According the NIST SP 800-34, Figure 3-2 is a "sample BIA process and data collection activities consisting of a representative information system with multiple components (servers), are designed to help the ISCP Coordinator streamline and focus contingency plan development activities to achieve a more effective plan." This helps the ISCP Coordinator determine the criticality of components and how each components works with the others. The figure streamlines the work to create a targeted contingency plan. This helps to minimize disruptions and recover more quickly during outages.

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

Figure 3-3 represents the "optimum point to recover" on a given information system concerning costs, disruption time, and "overall support for critical mission/business processes." The longer a disruption lasts, the more it costs the organization. Reducing downtime with faster recovery can be more expensive to set up.

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

The BIA process defines how to identify and prioritize critical business functions and systems to minimize the impact of disruptions. It focuses on understanding how outages affect operations, determining recovery priorities, and establishing recovery time objectives. By analyzing the importance of each system and its components, organizations can plan effectively to reduce downtime, protect critical operations, and position resources where needed during an incident.

Part 2: Explore the BIA Template

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

The overview section explains the purpose of the BIA, which is to identify critical system components and assess how system outages could affect the organization's mission or business processes. It gives three key steps: determining critical processes and downtime tolerances, identifying necessary resources for recovery, and setting recovery priorities.

The system description section presents an overview of the analyzed system, including its architecture, functionality, and details like physical location, users, and backup procedures. It includes information necessary for recovery planning, such as diagrams and system dependencies.

The BIA data collection section outlines how to gather and analyze data for the BIA. It focuses on identifying critical processes, estimating tolerable down times, determining recovery objectives such as Recovery Time Objective and Recovery Point Objective, and documenting the resources required for recovery. It has prioritized system resources for recovery and detailed alternative strategies.

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 (BIA template) maps to 3.2.1 Determine Business Processes and Recovery Criticality (NIST SP 800-34)

3.2 Identify Resource Requirements (BIA template) maps to 3.2.2 Identify Resource Requirements (NIST SP 800-34)

3.3 Identify Recovery Priorities for System Resources (BIA template) maps to 3.2.3 Identify System Resource Recovery Priorities (NIST SP 800-34)

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

The longest time managers and leaders are willing to let a business process or system be down or disrupted without causing a severe impact. It includes possible implications of the disruption, like financial losses, customer dissatisfaction, or harm to the organization's mission. Knowing the MTD helps planners decide on the right recovery methods and how much detail is needed in the recovery plan to ensure a process is restored within that time frame.

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

The maximum amount of time a system or resource can be unavailable before it starts causing severe problems for other systems or important business processes. It helps organizations determine the right strategies to quickly recover a resource to avoid exceeding the Maximum Tolerable Downtime.

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

The RPO represents how much data your organization can lose during a system outage. It tells you how far back in time you need to recover data from backups after a disruption.

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

MTD is the longest time an organization can tolerate a process or system being down before it causes significant problems. It sets the overall deadline for recovery. RTO is the specific target for quickly recovering a system or resource to stay within the MTD. The RTO must always be less than or equal to the MTD to ensure recovery happens before something becomes unacceptable. MTD is the limit, and RTO is the goal.

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

RTO is how quickly you must restore a system or process after an outage to avoid severe problems. RPO is how much data you can afford to lose, measured by how far back in time your backups go. Both work together to guide recovery planning. RTO focuses on how fast it can recover, while RPO focuses on how much data can be lost. They work together to ensure systems are restored quickly with minimal data loss.

Challenge Exercise

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

The impact to cost for the eCommerce business process is high. The eCommerce business process is a critical revenue-generating process that would result in revenue loss, operational disruption, service-level agreement failures, and added recovery costs.

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

The impact to prestige for the eCommerce business process is high. The eCommerce business process is a critical customer-centered operation. Downtime would seriously impact the reputation due to customer expectations, pressure from competition, customer loyalty, public perception, and customer trust in data security.

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

The impact to cost for the payroll business process is moderate. The payroll business process mainly affects internal operations and employees. A few considerations justify a moderate impact such as delayed payment penalties, recovery costs, employee morale, and backup frequency.

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

The impact to prestige for the payroll business process is moderate. The employee payroll process directly impacts internal operations, such as employee trust and morale. Even though it does not directly impact external customer prestige, there are significant internal and organizational consequences, such as risk to employee retention and indirect external reputation.

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 is 24 hours
The drivers are customer satisfaction, revenue loss, and market competition.
RTO is 4 hours
The drivers are operational continuity, performance on SLAs, and reputation protection.
RPO is 1 hour
The drivers are data accuracy on transactions, regulations and compliance requirements, and customer trust.

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 is 72 hours
The drivers are employee satisfaction and timely compensation, regulations such as labor laws, and employee morale.
RTO is 24 hours
The drivers are regulatory compliance, employee morale and trust, and preventing additional costs.
RPO is 1 day
The drivers are data backup frequency, payroll accuracy, and backup restoration.

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

Front-End Server (DMZ)
Database Server (Internal Network)
Firewall
Router
Network Switch
Internet Service Provider (ISP)
Backup Systems

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

Payroll Server
Domain Controller
Internal Network Switch
Backup System

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

eCommerce Business Process
Front-End Server (DMZ)
RTO: 2 hours
Justification: Critical for customer transactions; downtime leads to revenue and reputational loss.

Database Server
RTO: 2 hours
Justification: Assures transaction data integrity and availability.

Firewall
RTO: 1 hour
Justification: Protects network traffic and prevents security risks.

Router
RTO: 1 hour
Justification: Provides critical connectivity for customer access.

Network Switch
RTO: 2 hours
Justification: Maintains communication between critical eCommerce systems.

Backup System (eCommerce)
RTO: 24 hours
Justification: Supports recovery only after primary system recovery fails.

Payroll Business Process
Payroll Server
RTO: 24 hours
Justification: Required to ensure timely employee payments.

Domain Controller
RTO: 24 hours
Justification: Critical for authentication and access to the payroll server.

Network Switch
RTO: 24 hours
Justification: Connects payroll systems and ensures timely employee payments.

Backup System (Payroll)
RTO: 48 hours
Justification: Supports recovery of payroll data only after primary system recovery fails.