CLO1:

Refer to the below analysis weighted factor worksheet and answer the questions.

Asset Impact on Revenue (40) Impact on Profitability (20) Impact on Public Image (40) Result

Mail Server 0.10 | 0.5 | 0.6

Web Server 0.20 | 0.30 |0.4

Application Server 0.20 | 0.70 | 0.8

1- Calculate the weight value of each asset and show your work. (6 marks)

Mail Server: 38

Web Server: 30

Application Server: 54

2- Which asset is the most important asset based on your results in step 1 above? (3 marks)

1. Application Server

2. Mail Server

3.Web Server

Question 2

CLO1:

Shaikhah is going to conduct the risk management process in her company. Define what is risk management and explain its subprocesses. What is the relationship between risk management and BIA?

Risk management is the process of identifying vulnerabilities in an organization’s information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the systems’ components.

Sub Processes of Risk Management are:

1. Risk management process

Identifying and controlling information asset risks, Security managers play the largest roles, Including contingency planning

2. Risk identification process

Examining, documenting, and assessing the security posture of an organization’s IT and the risks it faces

3. Risk control process

Applying controls to reduce the risks

BIA is Business Impact analysis. In Risk Management we calculate the BIA

Question 3

CLO2:

An organization decides to have a warm site in case of disaster. However, the organization are not aware of the preparation and the needed equipment at the warm site. Brief the organization with the required preparation at the warm site.

Warm sites partially site with hardware and no software installed or configured. Has connections to recover data quickly.

Question 4

CLO2:

Apply your knowledge to build the Computer Security Incident Response Team (CSIRT) at your organization, describe how do you select members for the team, what kind of structure you will use and what staffing model, and describe nontechnical skills needed for the team.

Making CSIRT:

Step 1: Obtain management support and buy-in

Step 2: Determine the CSIRT strategic plan

Step 3: Gather relevant information

Step 4: Design the CSIRT vision

Step 5: Communicate the CSIRT vision and operational plan

Step 6: Begin CSIRT implementation

Step 7: Announce the operational CSIRT

Step 8: Evaluate CSIRT effectiveness

CSIRT staffing models

Employees: organization performs all IR work- Limited contractor technical and administrative support, Partially outsourced: portions of IR work outsourced, 24-hour-a-day; 7-day-a-week (24/7) monitoring, Basic IR work performed in-house; contractors assist

Question 5

CLO2:

a) An organization needs to replicate a database in remote locations, across a public or private carrier. Illustrate three different replication types that can be used for the backup.

The three types of Replications are:

1. Snapshot replication

2. Merger replication

3. Transaction replication

b) Choose a suitable data replication solution for your organization and justify your selection.

I would choose transaction replication as it can perform what company requires. It can even replicate in off-site.

Question 6

CLO3:

As part of an interview for an Incident Responder role, you were asked to identify four (4) probable indicators of an Incident. Be specific in your answer.

- Activities at unexpected times; Network traffic levels.

- Presence of unexpected new accounts

- Reported attacks

- Notification from IDPS: if it real or a false positive.

Question 7

CLO3:

a) Khalid is deciding to implement security in the network, he is confused to select one of them between Intrusion detection system and intrusion prevention system? Explain the two technologies and which one is better then other in terms of application? ( 6 marks )

Intrusion detection systems (IDSs):

Detects a violation and activates an alarm and have Custom configuration levels available

Intrusion prevention system (IPS):

Detects intrusion and prevents successful attack using an active response

I think Intrusion detection systems (IDSs) is way better as it allows custom configuration and has more alarm types

b) what are the possible alarm types? (3 marks)

The three Alarm types are:

1. Audible

2. Visual

3. Silent

Question 8

During a DoS incident, one possible containment strategy is to block the address the attacks are coming from. In addition, the organization may want to change its filtering strategy. What are the advantages and disadvantages of this approach?

Altering the filtering rules, either temporarily or permanently, may resolve the issue. The attacker may not only shift spoofed addresses, but may also shift source protocols. Also be aware that the more rules present in a device, the slower it will run. Thus, changing the organization's filtering strategy should only be done on a temporary, emergency basis if it causes issues. For long-term solutions, the organization may want to consider upgrades to critical network technologies to make such responses insignificant.

Question 9

CLO4

As a contingency planner at your organization, you have been asked to form a business continuity team, explain the structure of such team.

Business Continuity plan created by a team of specialists with CPMT overall direction

Begin with Business Continuity team leader assembling the Business Continuity team

The BC team includes:

Information Technology Department and Information Security Department representatives

Breadth and depth of the nontechnical members drawn from business units in the organization

Question 10

CLO4:

Develop three different mechanisms to test your Disaster Recovery Plan at your organization.

- Desk check

- Structured walk-through - Simulation

- Parallel testing - Full-interruption

- War gaming

Question 11

CLO4

A ransomware attack was a worldwide cyberattack that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The attack begun on May 12, 2017 and within a day more than 230,000 computers were infected. Classify this event, i.e., routine incident or disaster, man-made or natural etc.? Show a justification for your selection.

This is a Man-made attack as the hackers were hacking the windows system and were demanding ransom for fixing the hack. It is obviously man-made as in natural or routine disaster no one asks for a ransom to fix it. So it is a man-made

Question 12

CLO4

The principal objective of the disaster recovery policy is to develop, test and document a well-structured and easily understood plan which will help the organization recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Explain in detail 4 elements that should appear in the Disaster Recovery Policy statement.

The 4 main and key elements that should appear in the DR policy statement should include:

1. Purpose

2. Roles and Responsibility

3. Exercise and testing schedules

4. Plan maintenance schedule