Business Continuity & Risk Management

Final Project

E-commerce Organization

Team member 1: John Ehab

ID: 100-2096

Team member 2: Kerelose Malak

ID: 100-1125

Team member 3: Shahenda Magdy

ID: 100-0739

Team member 4: Karim Salem

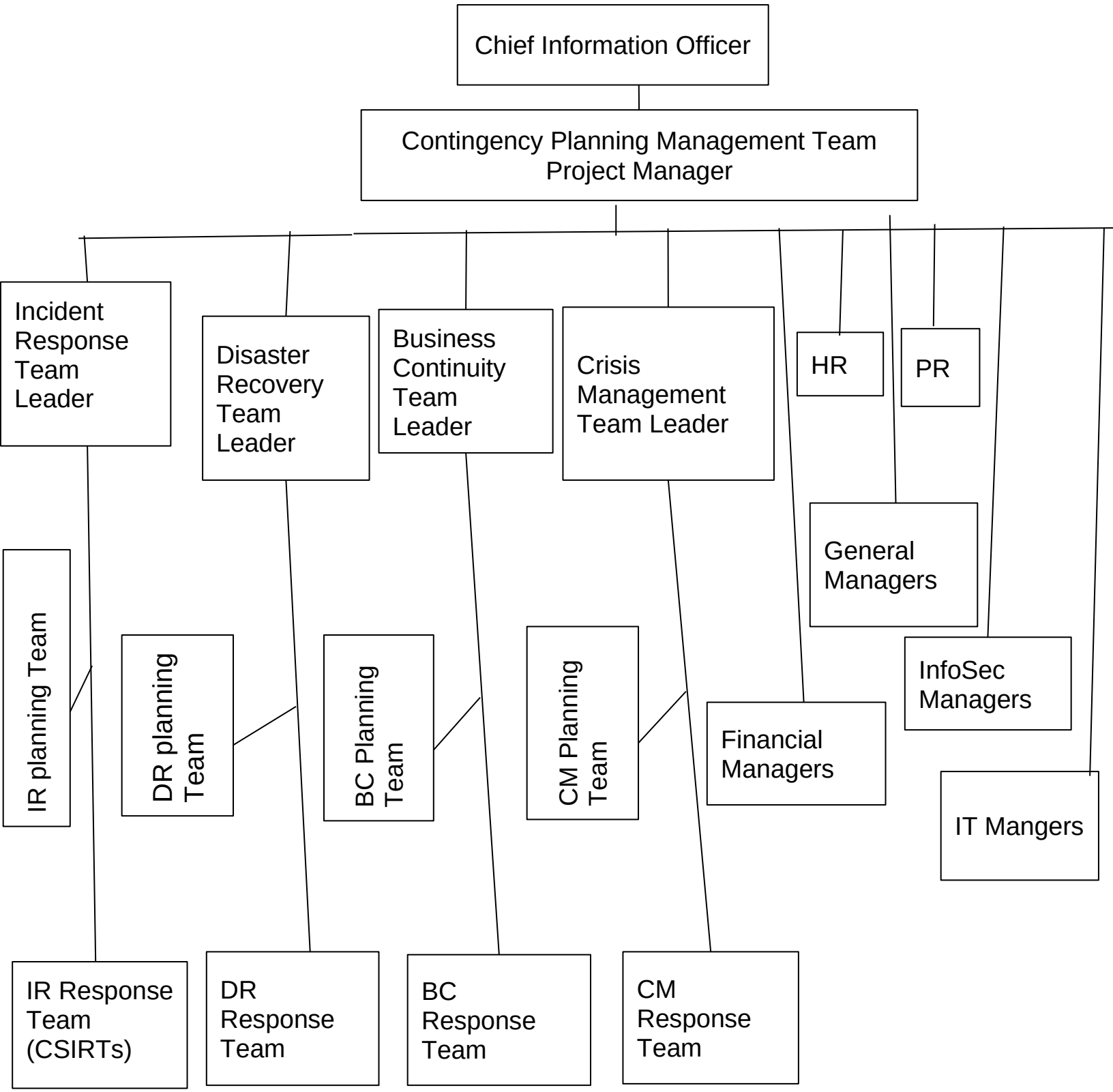
ID: 100-1619

Risk Management

Asset	Threat	Vulnerabilities	Likelihood	Impact
Central Database	Ransomware	Weakness in Anti viruses	Moderate	Major
Web servers	SQL Injection	Insufficient input validation	Almost Certain	Moderate
Personnel's accounts	Identity Theft	Non trained Personnel	Rare	Major
Accounting Ledgers	Data leakage	Excessive or unnecessary privileges	Moderate	Major
Network Routers	DDos	Weakness of firewalls	Almost Certain	Moderate

Contingency Planning Process

1. **Draw the hierarchy of the CP**



2. **Conduct of BIA**

Business Process	Threats/Incidents	Resources needed	Recovery Criticality (High, Low)
Online Ordering	DDOS	Redundant Web Servers or CDNs	High
Customers' Accounts and new customer's registration	Ransomware / SQL Injection	Backup database / Packets Filtering, Defenders, and Anti viruses' systems	High
Accounting & Finance	Data Leakage	Alert Systems	High

3. **Dealing with incidents**

a) After conducting the BIA, choose the most 2 critical incidents and classify them (What are the types of incidents).

- DDOS (Type: Denial of Service):
  This attack affects the main and most important service of the organization, our business is all about selling goods online to customers across the world. It also affects organization's public image, it's an issue which can't be hidden from our customers.

- Ransomware (Type: Malicious Code):
  This incident can cause damage to the organization's whole data and a huge financial loss. If it is executed, it can destroy our information assets by deleting/encrypting it. A huge financial loss will happen because we will have to pay for the attacker to decrypt the data and be able to use it again and continue our business.

b) Which detection strategy would be used to detect the incidents? (Explain the whole process)

Our strategy for detection is done by implementing NIDSs and HIDSs to analyze the incoming and upcoming packets. They detect incidents and produce alerts, it can be signature-based (searching for patterns that match known signatures) or statistical anomaly-based detections (by periodically sampling network activity and using statistical methods to compare the sampled network activity to the pre-defined baseline, and check for any packet entering that seems to be abnormal, or doesn't follow the expected behavior).These alerts are either prevented by the systems if it's 100% sure that it's an incident, or can be sent to the IT specialists to check if it's a false positive and ignore it or a real incident and start taking the appropriate action responding to it.

c) What is the response that should be taken to contain, eradicate (if needed) and recover from this incident? (Explain each one briefly)

1- DDos:

- Containment Phase:
  - Shut off the network connection that the incident is using as a conduit.
  - Temporarily blocking incoming packets.
  - Implement filtering based on the characteristics of the attack.
  - Contact the ISP / upstream partners for assistance in filtering the attack.
  - Relocate the target.
  - Notify upper management.

- Eradication Phase:
  - Identify and mitigate all vulnerabilities that were used.

- Recovery Phase:
  - Return affected systems to an operationally ready state.
  - Confirm that the affected systems are functioning normally.
  - Implement additional monitoring to look for future related activity.

2- Ransomware:

- Containment Phase:
  - Identify infected systems.
  - Disconnect infected systems from the network.
  - Block the transmission mechanisms for the malicious code.

- Eradication Phase:
  - Disinfect, quarantine, delete, and replace infected files.

- Search for any rootkits or back doors that may have been installed by the attacker to allow future returns.
- Mitigate the exploited vulnerabilities for other hosts within the organization.

- Recovery Phase:
  - Recover the lost data from the backup database.
  - Return affected systems to an operationally ready state.
  - Confirm that the affected systems are functioning normally.
  - Implement additional monitoring to look for future related activity.