Week 9

Task 1. Select Security Objectives

For each of the selected sub-categories, give the function, category and sub-category, and then explain why it is important and explain an attack/vulnerability it may mitigate.

CSF : Cyber Security Framework

The CSF is organized around five core functions: Identify, Protect, Detect, Respond, and Recover.

Function: Protect; Category: Data Security; Sub-category: Information Protection Processes and Procedures (PR.DS-2)

Reason for importance: Information protection processes and procedures are important for ensuring that sensitive information is properly protected from unauthorized access, modification, or destruction. By implementing effective processes and procedures for protecting information, organizations can prevent data breaches, insider threats, and other types of cyber attacks.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as data breaches, insider threats, and social engineering attacks by ensuring that proper controls are in place for protecting sensitive information.

Function: Protect; Category: Risk Management; Sub-category: Risk Assessment (PR.RA-3)

Reason for importance: Risk assessments are important for identifying potential threats and vulnerabilities that could be exploited by cyber attackers. By conducting regular risk assessments, organizations can identify and prioritize potential threats, and develop effective strategies for mitigating those threats.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as malware infections, phishing attacks, and data breaches by identifying potential vulnerabilities and implementing effective controls to mitigate those vulnerabilities.

Function: Detect; Category: Anomalies and Events; Sub-category: Security Information and Event Management (SIEM) (DE.AE-3)

Reason for importance: Security information and event management (SIEM) is important for monitoring and analyzing security events and alerts, and for identifying potential cyber threats in real-time. By implementing effective SIEM controls, organizations can quickly detect and respond to potential cyber threats.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as advanced persistent threats (APTs), insider threats, and ransomware attacks by continuously monitoring and analyzing security events and alerts.

Function: Detect; Category: Response Planning; Sub-category: Communications (DE.CM-1)

Reason for importance: Communications planning is critical for ensuring that all stakeholders are informed and involved in the incident response process in the event of a cyber attack. By developing effective communication plans, organizations can ensure that everyone is on the same page and can work together to mitigate the attack.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as data breaches, network intrusions, and ransomware attacks by ensuring that all stakeholders are informed and involved in the incident response process.

Create Asset Inventory

Tables of assets for the six (6) asset types, ensuring the Data assets also are classified.

Data Assets:

Asset Name	Classification	CIA Protections
Customer database	Confidential	Confidentiality
Financial records	Sensitive	Confidentiality, Integrity
Intellectual property	Critical	Confidentiality, Integrity
Personnel records	Confidential	Confidentiality
Marketing plans	Sensitive	Confidentiality, Integrity
Product designs	Critical	Confidentiality, Integrity
Legal documents	Confidential	Confidentiality

Hardware Assets:

Asset Name	Identification Information	CIA Protections
Servers	IP addresses, serial numbers	Availability, Confidentiality, Integrity
Routers	MAC addresses, serial numbers	Availability, Confidentiality, Integrity
Firewalls	IP addresses, firmware versions	Availability, Confidentiality, Integrity
Switches	MAC addresses, port configurations	Availability, Confidentiality, Integrity
Workstations	Asset tags, user names	Availability, Confidentiality, Integrity
Laptops	Asset tags, serial numbers	Availability, Confidentiality, Integrity

Software Assets:

Asset Name	Vendor	CIA Protections
Operating system	Microsoft, Apple, Linux	Availability, Confidentiality, Integrity
Antivirus software	Symantec, McAfee,	Availability,

	Kaspersky	Confidentiality, Integrity
Office productivity suite	Microsoft Office, Google Workspace	Availability, Confidentiality, Integrity
Web browser	Google Chrome, Mozilla Firefox	Availability, Confidentiality, Integrity
Email client	Microsoft Outlook, Gmail	Availability, Confidentiality, Integrity
Database management system	Oracle, Microsoft SQL Server	Availability, Confidentiality, Integrity

Physical Assets:

Asset Name	Location	CIA Protections
Building	Street address, floor plan	Availability, Confidentiality
Data center	Street address, access control list	Availability, Confidentiality, Integrity
Backup tapes	Offsite storage facility	Confidentiality, Integrity
Locks	Manufacturer, key code	Availability, Confidentiality
Security cameras	Location, manufacturer	Availability, Confidentiality

Personnel Assets:

Asset Name	Position	CIA Protections
CEO	Chief executive officer	Confidentiality
IT manager	Information technology manager	Availability, Confidentiality, Integrity
Database administrator	Database administrator	Confidentiality, Integrity
Sales representative	Sales representative	Availability, Confidentiality
Human resources manager	Human resources manager	Confidentiality

Network Assets:

Asset Name	Description	CIA Protections
Wireless access point	Model, encryption method	Availability, Confidentiality
Virtual private network	VPN gateway IP address, encryption protocol	Confidentiality
Domain name system	DNS server IP addresses, domain names	Availability, Confidentiality, Integrity
Network	Storage capacity, access	Availability,

attached storage	control list	Confidentiality, Integrity
Intrusion detection system	IDS sensor IP addresses, alerting thresholds	Availability, Confidentiality, Integrity

Task 3. Information Flow Check

Diagrams of information flows for two (2) important assets

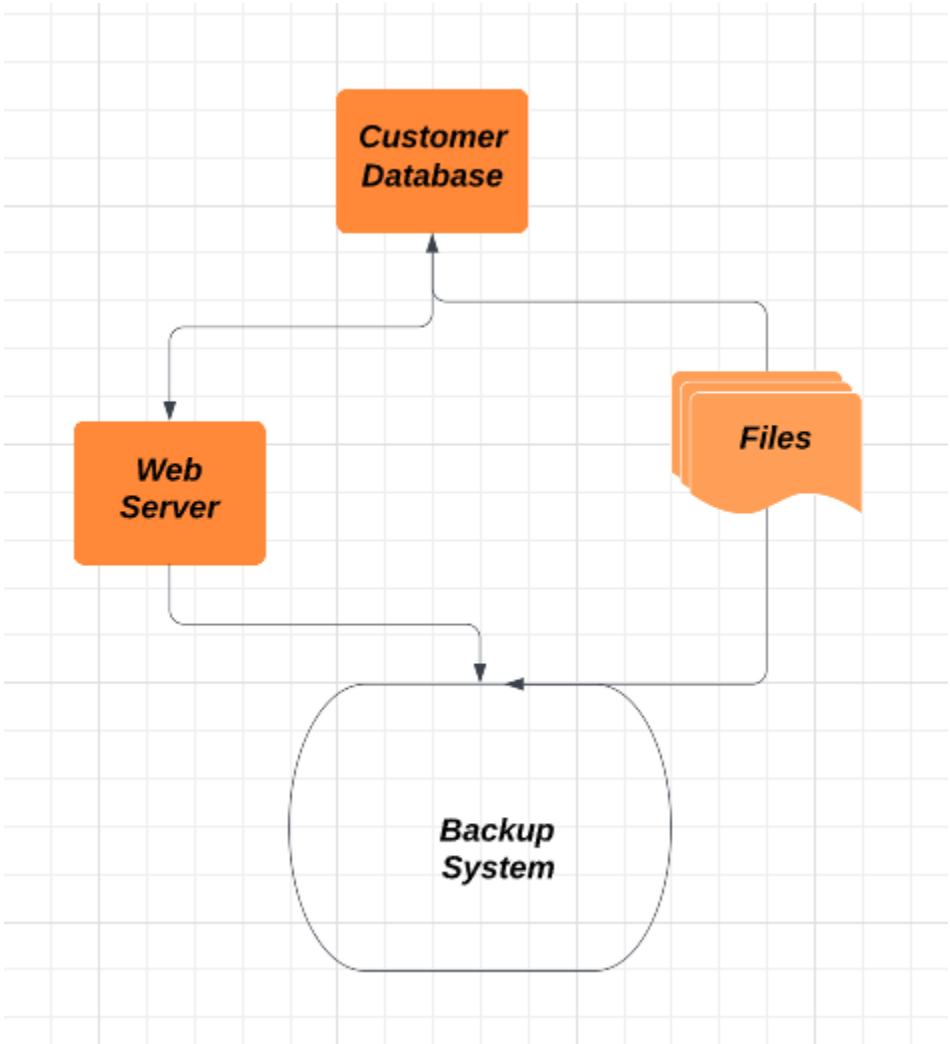
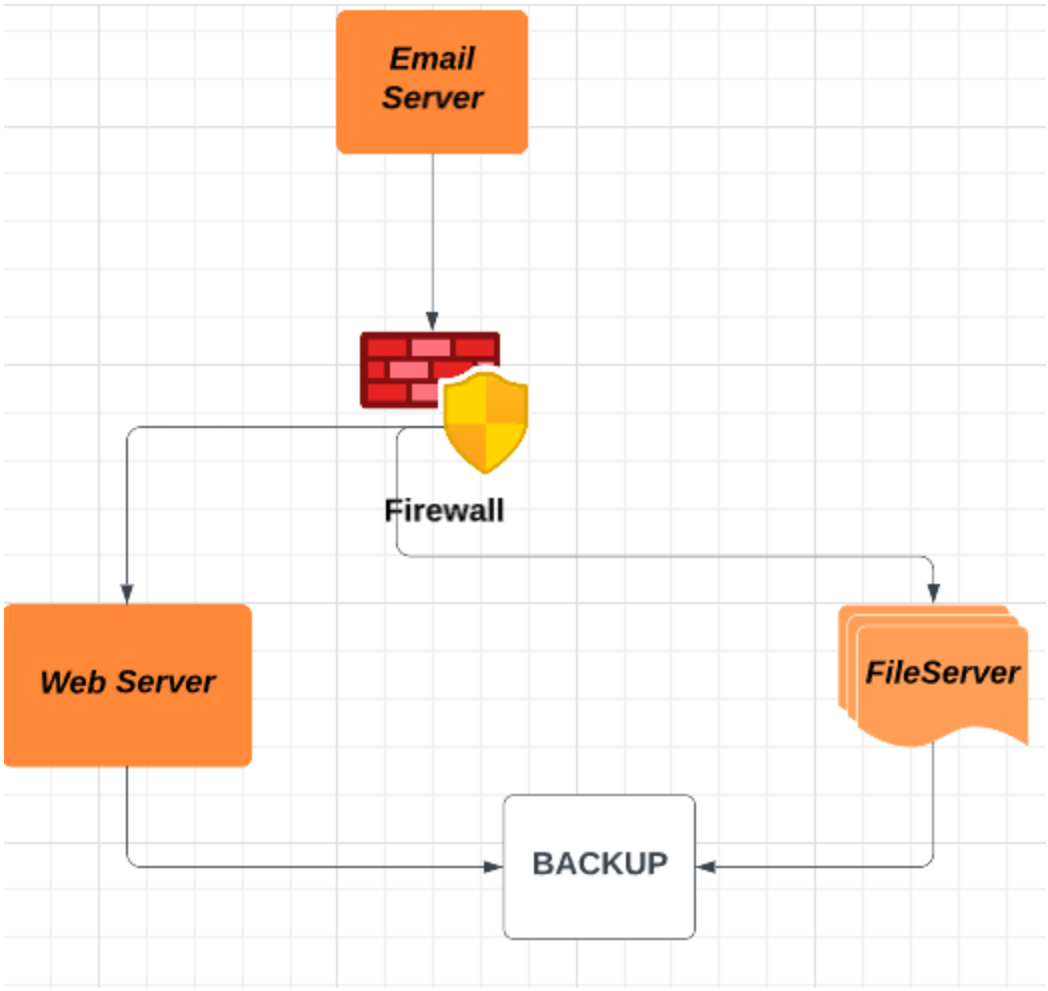


Diagram 2



Task 4. Conduct a Risk Analysis

There is no need to include this in your journal, as it will be in your project submission.