STUDENT WORKSHEET: Capstone 2, Scenario 2

Name: Chijioke Ejim

Scenario 2

Remediate Audit Findings

Read the scenario below. For each issue identified from the security audit, identify either an administrative, technical, or physical control to remediate the issue. You can use the example scenario below to guide your answers.

Example scenario:

You are a cybersecurity analyst for a publicly traded investment company. Recently, there has been an increase in the number of cyberattacks conducted on similar organizations. The leadership of your organization has decided to have a security audit performed on the organization's network in order to prepare for these cyberattacks.

The audit discovered several deficiencies in the security controls of the organization.

Review each finding below, which includes a prompt for a technical, administrative, or physical control. Your response will be a recommendation for a control or controls that fall into that category

Exemplar 1

Finding	**Controls Recommended**
Storage rooms containing sensitive data were not locked or access to the room audited. Identify a phyisical control to remediate the room access violations.	RFID ID Card access applied to the rooms containing sensitive data

Exemplar 2

Finding	**Controls Recommended**
Company financial data can be accessed by anyone. Identify a technical control to remediate the Sarbanes Oxley violation for financial data control.	Data Loss Prevention tools implemented where financial data is stored.

Scenario 2

Remediate Audit Findings

You are an analyst for a large healthcare organization.

The organization is responsible for providing patient care to over 1 million patients annually. It is a national leader in providing patient care to a major metropolitan area. Recently, a data breach occurred within the healthcare organization's computer network resulting in significant patient information being breached and leaked onto the dark web. The breach is suspected to be a result of a SQL Injection attack on the organization's patient portal webpage.

This event became publicly known and the hospital's reputation has been tarnished as a result. To remediate, the organization has allocated significant funds to overhaul their computer network and cyber security program.

The organization's IT architecture consists of a campus WAN with three main office buildings operating inside of the campus network: the main hospital, the children's hospital, and the administrative building. Close to 15% of administrative employees work remote.

It is your responsibility to provide recommendations for each of the audit findings below.

Review each finding below, which includes a prompt for a technical, administrative, or physical control. Your response will be a recommendation for a control or controls that fall into that category

1.

Finding	**Controls Recommended**
There were HIPAA violations around PHI data security, storage and handling identified in the file servers of the administrative building. Identify an <u>administrative</u> control to remediate the HIPAA violations.	Implement workforce security measures, by: Implementing policies and procedures to: Ensure that all members of the workforce have appropriate access to electronic protected health information; and Prevent those workforce members who are not given access to ePHI, from obtaining such access. Implement policies and procedures for authorizing access to electronic protected health information.

	Implement a security awareness and training program for all workforce members, including management.

2.

Finding	**Controls Recommended**
Most network accounts contained privileges above the user's job requirements. Identify a technical control to remediate this issue.	Implement granular access controls that enforce least-privilege.

3.

Finding	**Controls Recommended**
Sensitive areas of the environment were not segregated from the rest of the network. Identify a technical control to remediate the flat network design.	Implement network segmentation. The network can be segmented by department, function, or even type of network.

4.

Finding	**Controls Recommended**
Remote employees had direct access to the internal network from outside the organization without the use of secure access. Identify a technical control to remediate external access control issues found during the audit.	Implement the use of VPN to access the network from outside the organization. Recommend training of employees on how to use VPN to access organization's network

5.

Finding	**Controls Recommended**
Physical areas of the IT facilities were not secured or otherwise easily accessible. Identify a technical control to remediate Physical Security control issues found during the audit.	Implement use of CCTV, alarms, locks and fencing.

6.

Finding	Controls Recommended
Hundreds of endpoints were not updated with the latest OS and patches. Identify an administrative control to remediate outdated operating system and patches.	Implement patch management.

7.

Finding	Controls Recommended
Weak passwords are being used for user accounts and default passwords in use across the network with no multi-factor authentication. Identify an administrative control to remediate password issues.	Enforce strong password policies like ensuring that users have strong passwords with no maximum character limits. Make sure a password is a combination of uppercase and lowercase letters, symbols, and numbers. Enforce multi-factor authentication.

8.

Finding	Controls Recommended
The customer relationship management (CRM) application contained several user input fields that did not have parameters to control number or type of characters. Identify an administrative control.	Enforce character escaping and input validation