Denzel Frimpong

Student ID#: 011480496

Governance, Risk, and Compliance

Security System Evaluation and Remediation

A.

These are the gaps that currently exist in Fielder Medical Center's (FMC)

- **Lack of Security Controls and Policies:** There are deficiencies in access control policies and procedures, account management, most minor privilege enforcement, and security attribute management.
- **Outdated Systems Design:** The current system design must be updated immediately to align with the latest security standards and compliance requirements.
- **Need for Updated Security and Privacy Plans:** The security and privacy plans that require updates encompass the information security program plan.
- **Absence of Multifactor Authentication (MFA):** There is a need to implement MFA and ensure proper identification and authentication of organizational users accessing the network and information systems.

B.

AC-6

The risk rating for the AC-6 Least Privilege is high. The principle of least privilege (PoLP) is a security practice where users, applications, and systems are granted the minimum access necessary to perform their functions. This minimizes the risk of unauthorized access and potential security breaches by ensuring access rights are limited to essential tasks. By implementing PoLP, the organization can reduce the potential damage from security incidents, enforce role-based access control, and regularly audit permissions to maintain a strong security posture.

CA-5

The risk rating for CA-5 Plans of Action and Milestones (POA&M) control is moderate. This is used in project management and cybersecurity to identify, prioritize, and track the resolution of security vulnerabilities and deficiencies. A POA&M outlines specific actions required to address each identified issue, assigns responsibilities, sets deadlines, and establishes milestones to measure progress. FMC needs this structured approach to ensure the organization systematically addresses security gaps, complies with regulatory requirements, and enhances its overall security posture by providing a clear roadmap for remediation efforts and continuous improvement.

CA-7

The risk rating for the CA-7 Continuous Monitoring control is high. FMC should use continuous monitoring to maintain an up-to-date understanding of its security posture, promptly identify and mitigate emerging threats, and ensure compliance with regulatory requirements. Constant monitoring allows for real-time visibility into network activities and system vulnerabilities, enabling proactive responses to potential incidents before they escalate. By constantly evaluating security controls and risks, a company can enhance its resilience, protect sensitive data, and maintain trust with customers and stakeholders.

RA-3

The risk rating for RA-3 Risk Assessment control is moderate. FMC needs risk assessment to systematically identify, evaluate, and prioritize potential threats to its operations, assets, and data. By understanding these risks, FMC can implement effective strategies to mitigate or manage them, ensuring business continuity, protecting against financial losses, and complying with regulatory requirements. Regular risk assessments enable informed decision-making and help build a robust security posture that can adapt to evolving threats and vulnerabilities.

RA-7

The risk rating for the RA-7 Risk Response control is moderate. Risk response is crucial for FMC because it enables the organization to proactively manage and mitigate potential threats that could disrupt operations, cause financial loss, or damage its reputation. A company can minimize the impact of adverse events by identifying and addressing risks through strategies such as avoidance, mitigation, transfer, or acceptance. Effective risk response ensures business continuity, enhances decision-making, and strengthens overall resilience, safeguarding the company's assets and ensuring long-term success.

C.

AC-6

To remediate the principle of least privilege control, organizations should begin by conducting a thorough audit of current access permissions to identify any discrepancies or over-privileged accounts. It is essential to ensure that users have the minimum access necessary to perform their job functions. Implementing role-based access control (RBAC) can streamline permissions assignments by categorizing users into roles with predefined access levels. Regularly reviewing and updating access permissions, especially during role changes or departures, helps maintain adherence to the principle. Additionally, leveraging automated tools can facilitate monitoring and enforcing most minor privilege policies, reducing the risk of human error. Finally, fostering a culture of security awareness through training and clear communication about the importance of least privilege can enhance overall compliance and security posture.

CA-5

To remediate Plans of Action and Milestones (POA&Ms), FMC must comprehensively review all existing plans to identify overdue or incomplete tasks. Prioritize these tasks based on risk and impact to ensure that the most critical issues are addressed first. Assign clear ownership and deadlines for each action item, ensuring accountability. Regularly update the POA&M to reflect progress and changes in priorities or resources. Utilize project management to track milestones and automate reminders for upcoming deadlines. Continuous monitoring and periodic audits can ensure that the POA&M remains aligned with organizational objectives and compliance requirements.

CA-7

FMC should involve implementing a robust strategy that includes real-time data collection, analysis, and response mechanisms. A great example would be an SIEM tool. This process requires deploying automated tools to detect and alert on anomalies or threats, ensuring systems and software are regularly updated to mitigate vulnerabilities, and maintaining thorough documentation and reporting for compliance and audit purposes. Additionally, conducting regular reviews and updates to the monitoring protocols and incorporating feedback from incident responses can enhance the overall effectiveness and resilience of the continuous monitoring system.

RA-3

FMC can start remediation by identifying and prioritizing risks through a comprehensive analysis, then develop and implement targeted mitigation strategies for each identified risk. Regularly update risk assessments to reflect changing threats and vulnerabilities, ensuring all controls are current and influential within the company. Engage stakeholders across the organization to foster a culture of risk awareness and responsibility and establish clear communication channels for reporting and addressing risks. Finally, periodic reviews and audits should be conducted to ensure the ongoing effectiveness and improvement of the risk assessment controls.

RA-7

FMC can begin evaluating the effectiveness of current risk response plans and identifying the gaps or weaknesses. Develop and implement updated response strategies tailored to the identified risks, ensuring they are comprehensive and actionable. Train relevant personnel on these new strategies to provide prompt and effective execution during a risk event. Establish clear communication protocols for timely information sharing and decision-making. Regularly test and review the risk response plans through simulations and drills to ensure they remain effective and make adjustments as necessary based on feedback and evolving risk landscapes.

D.

FMC’s policy for complying with PCI DSS standards covers several critical aspects, including the configuration and upkeep of firewalls, the elimination of default settings provided by vendors, and the implementation of an antivirus solution.

- Firewall: The IT Networking team will be responsible for configuring and maintaining the firewall. The firewall configuration must adhere to PCI DSS requirements. Any requested changes to the firewall must go through established firewall change management process.
- Antivirus Solution: Antivirus (AV) solutions must be installed on all systems and network devices. IT Cybersecurity will conduct an annual evaluation of current AV solution to ensure it meets industry standards. Regular updates and subsequent testing of the AV solution are required for quality assurance. The AV solution should be executed at least once every 24 hours.
- Vendor-Supplied Defaults: IT Networking is responsible for changing all vendor-supplied defaults to protect the infrastructure from publicly accessible credentials. It is strongly recommended to conduct testing to confirm that no vendor-supplied defaults remain.