GOVERNANCE, RISK, AND COMPLIANCE – D486

DFN1 TASK 1: Security System Evaluation and Remediation

Shane M. Deitle

Western Governors University

A: Summarize the gaps that currently exist in the company's security framework as described in the attached "Security Assessment Report for Fielder Medical Center" (SAR).

1. **Lack of Security Controls and Policies:** The report identifies a deficiency in security controls and policies. The deficiencies include the following: account management, access control, security attributes, as well as least privilege. These gaps pose a significant risk to Fielder Medical Center 's overall security posture.
2. **Outdated Systems Design:** Fielder Medical Center's systems design is considered outdated, creating a mismatch between the existing systems security plan (SSP) and current compliance requirements. Immediate attention is required to bridge these gaps and ensure alignment with regulatory standards.
3. **Security and Privacy Plans Need Updating:** The security assessment emphasizes the need for updating security and privacy plans at Fielder Medical Center. The development of an information security program plan based on compliance as well as organizational needs, the updating of the system inventory/asset list, and the conducting of a risk assessment that coincides with the new controls in the network and information systems are all included.
4. **Absence of Multifactor Authentication (MFA):** Fielder Medical Center lacks multifactor authentication, which is a critical security measure. The report recommends implementing MFA to enhance the authentication process and strengthen overall network security.

B1: For each of the five identified controls within the SAR, identify the associated risk rating as low, moderate, or high and explain the risk. ("Risk" and "Explanation")

& B2: For each of the five identified controls within the SAR, justify FMC's decision to remediate the risk associated with the identified control instead of accepting the risk based on compliance and industry guidelines and support the justification with industry-respected sources. ("Justification")

& C: Discuss how FMC should remediate the risks with each of the five controls identified in Section 3.3 of the SAR. For each risk, include any assets, actions, or changes that will be needed for remediation. ("Remediation Strategy")

1. AC-6
   - Risk: Moderate
   - Explanation:
     - Least privilege is a fundamental security principle that aims to restrict user access rights to the minimum levels necessary for performing job functions. In the context of Fielder Medical Center, the absence of least privilege implies that users may have unnecessary access permissions, which could lead to sensitive information being accessed without authorization. This risk is moderate because while it poses a threat to data confidentiality and integrity, it may not result in severe consequences immediately. However, over time, unauthorized access could potentially escalate to more critical security incidents.
   - Justification:
     - Fielder Medical Center decided to remediate this risk to make sure the principle of least privilege is enforced, reducing the likelihood of unauthorized access. Compliance with industry standards emphasizes the importance of least privilege to limit access to only what is necessary for the job duties of users to be performed, thereby reducing the attack surface (NIST SP 800-53 Rev. 5.1.1, AC-6).
   - Remediation Strategy:
     - To address the lack of least privilege, Fielder Medical Center should implement a comprehensive access control policy that adheres to the principle of least privilege. This involves reviewing and adjusting user permissions based on their job roles and responsibilities. Access rights should be limited to the minimum necessary for users to perform their duties. Fielder Medical Center should conduct regular access reviews and audits to ensure ongoing compliance with the least privilege principle.
     - Assets/Actions/Changes
       1. Conduct an inventory of user roles and permissions.
       2. Define access levels based on job roles and responsibilities.
       3. Implement a regular review process for user access.
       4. Utilize automated tools for access control and monitoring.

2. CA-5
   - Risk: High
   - Explanation:
     - A lack of comprehensive plans for addressing security vulnerabilities and weaknesses increases the likelihood of unaddressed issues persisting within the system. This high-risk rating is attributed to the potential for security vulnerabilities to remain exploitable, leading to security incidents and data breaches. Without a structured plan to identify, prioritize, and remediate vulnerabilities, Fielder Medical Center faces increased exposure to cyber threats and potential regulatory non-compliance.
   - Justification:
     - Fielder Medical Center opted to remediate this risk to establish and track planned remediation actions systematically. Compliance with NIST SP 800-53 mandates the development of plans of action and milestones to address weaknesses promptly, aligning with best practices in risk management (NIST SP 800-53 Rev. 5.1.1, CA-5).
   - Remediation Strategy:
     - To address the absence of a robust plan of action and milestones, Fielder Medical Center should establish a structured process for identifying, prioritizing, and remediating security vulnerabilities. This involves creating detailed plans of action with clear milestones for each identified vulnerability. Fielder Medical Center should prioritize remediation efforts based on risk assessment outcomes and allocate resources accordingly.
     - Assets/Actions/Changes Needed for Remediation:
       1. Develop a comprehensive plan of action and milestones.
       2. Prioritize vulnerabilities based on risk assessments.
       3. Allocate resources for timely remediation.
       4. Establish a mechanism for tracking and reporting progress.

3. CA-7
    - Risk: Moderate
    - Explanation:
        - Continuous monitoring is critical for the timely detection of security incidents and anomalies. The moderate risk rating indicates that while there is a risk of delayed detection and response to security events, the immediate impact may not be severe. However, over time, the lack of continuous monitoring could result in extended periods of undetected malicious activity, potentially leading to more significant security breaches.
    - Justification:
        - Fielder Medical Center chose to remediate this risk by implementing a continuous monitoring strategy. Continuous monitoring is a fundamental aspect of risk management (NIST SP 800-53 Rev. 5.1.1, CA-7).
    - Remediation Strategy:
        - To address insufficient continuous monitoring, Fielder Medical Center should implement a robust continuous monitoring strategy. This involves deploying automated tools for real-time threat detection, incident response, and system performance monitoring. Fielder Medical Center should establish protocols for timely incident reporting and response, ensuring that security events are promptly addressed.
        - Assets/Actions/Changes Needed for Remediation:
            1. Deploy continuous monitoring tools and systems.
            2. Establish incident response protocols.
            3. Train personnel on continuous monitoring practices.
            4. Regularly review and update monitoring configurations.

4. RA-3
   - Risk: High
   - Explanation:
     - An outdated risk assessment may fail to identify and address new and evolving risks associated with the changes in Fielder Medical Center 's systems. The high-risk rating reflects the potential for unidentified risks to impact the confidentiality, integrity, and availability of Fielder Medical Center 's information assets. Without an updated risk assessment, Fielder Medical Center may not be adequately prepared to implement effective risk mitigation strategies, leaving the organization vulnerable to a range of security threats.
   - Justification:
     - Fielder Medical Center decided to remediate by conducting an updated risk assessment. Industry standards, such as NIST SP 800-53, emphasize the need for periodic risk assessments to identify and manage risks effectively (NIST SP 800-53 Rev. 5.1.1, RA-3).
   - Remediation Strategy:
     - To address the risk associated with an outdated risk assessment, Fielder Medical Center should conduct a comprehensive and updated risk assessment. This involves identifying and analyzing potential risks associated with changes in Fielder Medical Center 's systems, processes, and technologies. Fielder Medical Center should use the findings to update the risk assessment and develop strategies for mitigating identified risks.
     - Assets/Actions/Changes Needed for Remediation:
       1. Conduct a thorough risk assessment.
       2. Identify and analyze new and evolving risks.
       3. Update the risk assessment documentation.
       4. Develop and implement risk mitigation strategies.

5. RA-7
   - Risk: High
   - Explanation:
     - Without a clear and well-documented rationale for risk response decisions, Fielder Medical Center may struggle to implement effective risk mitigation measures. The high-risk rating underscores the importance of transparent and justified decision-making in risk response, ensuring that chosen strategies align with the organization's goals, compliance requirements, and industry best practices. Inadequate justification increases the likelihood of ineffective risk management, potentially exposing Fielder Medical Center to avoidable security incidents.
   - Justification:
     - Fielder Medical Center chose to remediate this risk by providing adequate justification for risk response strategies. Complying with industry standards ensures a comprehensive approach to risk response (NIST SP 800-53 Rev. 5.1.1, RA-7).
   - Remediation Strategy:
     - To address the risk associated with inadequate justification for risk response strategies, Fielder Medical Center should establish a transparent and well-documented process for making risk response decisions. This involves clearly articulating the rationale behind chosen risk response strategies and ensuring alignment with organizational goals, compliance requirements, and industry best practices.
     - Assets/Actions/Changes Needed for Remediation:
       1. Establish a documented risk response process.
       2. Clearly articulate the rationale for risk response decisions.
       3. Align risk response with organizational goals and compliance.
       4. Train personnel on the approved risk response procedures.

D: Develop a PCI DSS–compliant policy to address the three concerns identified in Section 3.2.4 of the SAR, including the roles and responsibilities associated for each requirement identified within the SAR to meet PCI DSS compliance.

1. Firewall Concern
   - Policy Title
     - Firewall Configuration Policy
   - Roles/Responsibilities:
     1. Network Security Team: Configure and manage firewalls with specific attention to PCI DSS requirements, including default-deny rules and intrusion prevention.
     2. System Administrators: Collaborate with the Network Security Team to implement and maintain firewall rules and configurations.
     3. Compliance Officer: Regularly assess and verify that firewall configurations align with PCI DSS requirements.
2. Password Policy Concern
   - Policy Title
     - Password Management and Authentication Policy
   - Roles/Responsibilities:
     1. IT Security Officer: Develop and enforce password policies in accordance with PCI DSS standards.
     2. System Administrators: Ensure the removal of vendor-supplied defaults and enforce strong password requirements for all system accounts.
     3. Security Awareness Training Coordinator: Include password security training in awareness programs for all employees.
3. Antivirus Solution Concern
   - Policy Title
     - Antivirus Protection Policy
   - Roles/Responsibilities:
     1. System Administrators: Ensure all workstations have a PCI DSS-compliant antivirus solution installed and configured properly.
     2. Security Officers: Oversee the implementation of antivirus protection policies and conduct regular audits to ensure compliance.
     3. End Users: Promptly report any issues related to antivirus protection on their workstations to the IT support team.

E. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

NIST. (2023, November 11). *Security and Privacy Controls for Information Systems and Organizations*. CSRC - COMPUTER SECURITY RESOURCE CENTER. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1

NIST. (2023, November 11). *CSRC - COMPUTER SECURITY RESOURCE CENTER*. Access CPRT - Cybersecurity and Privacy Reference Tool; AC-6. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC-06

NIST. (2023, November 11). *CSRC - COMPUTER SECURITY RESOURCE CENTER*. Access CPRT - Cybersecurity and Privacy Reference Tool; CA-5. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CA-05

NIST. (2023, November 11). *CSRC - COMPUTER SECURITY RESOURCE CENTER*. Access CPRT - Cybersecurity and Privacy Reference Tool; CA-7. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CA-07

NIST. (2023, November 11). *CSRC - COMPUTER SECURITY RESOURCE CENTER*. Access CPRT - Cybersecurity and Privacy Reference Tool; RA-3. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=RA-03

NIST. (2023, November 11). *CSRC - COMPUTER SECURITY RESOURCE CENTER*. Access CPRT - Cybersecurity and Privacy Reference Tool; RA-7. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=RA-07