Security System Evaluation and Remediation

By: Jordan Biggs

Part A:

The Security Assessment Report shows several gaps in the Fielder Medical Center's(FMC) framework. The report outlines that the gaps mainly stem from the outdated systems and failure to comply with federal & industry standards. FMC's security posture is weak in several areas: Governance, Endpoint Protection, and Risk Management. A fundamental lack of comprehensive security controls governs Access Control (AC), account management, and the Principle of Least Privilege (PoLP). Operational security is weak. The network lacks Multifactor Authentication (MFA). Endpoints lack proper, licensed Antivirus (AV) protection. This technical weakness is aggravated by organizational failure. Security plans are outdated. FMC lacks a current system inventory/asset list. FMC fails to implement continuous Risk Assessment (RA-3) or Plans of Action and Milestones (POA&M) tracking (CA-5). This means FMC cannot formally track or remediate known risks. Critical infrastructure is vulnerable. The network relies on an End-of-Life (EoL) firewall. FMC lacks secure processes to authenticate doctors. These issues create high-risk compliance gaps.

Part B:

B1:

Control Identifier	Control / Control Enhancement	Rating	Reason
AC-6	Least Privilege	High	Compromised accounts have excessive access to PII and critical systems. This causes maximum potential impact from unauthorized disclosure.
CA-5	Plans of Action and Milestones	High	FMC fails to develop and track remediation actions. Known high-risk vulnerabilities persist. This leads to an unacceptable likelihood of compromise and violates FISMA compliance.
CA-7	Continuous Monitoring	High	FMC cannot rapidly detect new threats or security incidents. This increases attacker dwell time and violates FISMA's continuous assessment mandate.
RA-3	Risk Assessment	High	Absent risk assessment prevents executive leadership from making informed decisions. This results in misallocated resources and failure to prioritize critical PII risks.
RA-7	Risk Response	High	Missing a formal risk rationale causes inconsistent security. FMC cannot demonstrate due diligence to government auditors. This creates severe legal and compliance risk.

B2:

These are five control risks that FMC needs to fix. Acceptance is not allowed because of federal compliance and healthcare security standards. In order to be in compliance with mandatory controls, such as AC-6, CA-5, CA-7, RA-3, and RA-7

of FISMA and NIST SP 800-53, regulatory requirements are outlined for access, authorization, and risk management. Without compliance, consequences will include a non-compliance finding, the loss of Authorization to Operate, and possibly even the loss of federal funding or other legal penalties. You have mandates you must meet in order to remain compliant. FMC also handles sensitive data, including PII and SSNs. Industry standards such as HIPAA, along with the CIA Triad, prohibit risks that threaten confidentiality or integrity. Finding Least Privilege and Continuous Monitoring weaknesses raises the likelihood of a breach. You must remediate these issues in order to protect data and maintain compliance.

Part C:

Control Identifier	Remediation plan
AC-6	FMC must implement a Role-Based Access Control (RBAC) model. This requires a full audit of all current user and service account permissions. Actions: Map user job duties to defined roles (e.g., "Doctor," "Admin"). Assets/Changes: Deploy a Privileged Access Management (PAM) tool to control administrative accounts. Remove unnecessary admin rights from standard accounts immediately
CA-5	FMC must formalize a process for tracking security deficiencies. Actions: Log every SAR finding as a POA&M item. Assign a responsible owner, a due date, and specific resources to each task. Assets/Changes: Adopt a GRC Platform or an existing IT ticketing system to log, track, and report POA&M status to the Board on a quarterly basis.
CA-7	FMC must establish real-time visibility into network activity. Actions: Define key security performance indicators (KPMs) and security metrics to monitor. Assets/Changes: Implement a Security Information and Event Management (SIEM) solution. Centralize all log data from endpoints, switches, and the firewall to detect anomalies and generate proactive alerts.
RA-3	FMC must replace the outdated risk assessment with a formalized process. Actions: Adopt a methodology, such as NIST SP 800-30. Analyze threats, vulnerabilities, and the likelihood/impact of each risk. Assets/Changes: Conduct a new risk assessment after implementing baseline security controls like the firewall and MFA. This accurately reflects the new security posture.
RA-7	FMC needs a documented process for addressing and justifying risk decisions. Actions: Create a formal Risk Register. Document all identified risks, their scores, and the corresponding response (Mitigate, Accept, Transfer, Avoid). Mandate that any Moderate or High risk accepted must be formally documented and signed off by the CISO or a Board member. Assets/Changes: Integrate the Risk Register into the GRC or POA&M tracking system for auditability.

Part D:

PCI Requirement 5 (Malware Protection)

This requirement encompasses Endpoint and Antivirus (AV) Management. All systems connected to the network, including workstations and the POS system, must deploy and maintain actively licensed, centrally managed Antivirus/Anti-Malware software. AV signature files must be automatically updated at least once daily. The IT/System Admin shall be responsible for installation, ensuring licenses, and performing daily verification of AV operational status on all endpoints. The Security Team shall monitor AV reporting logs for unlicensed or inactive endpoints.

PCI Requirement 8.3 (MFA)

This requirement necessitates Multi-Factor Authentication. MFA shall be utilized for every non-console access to the CDE. MFA shall be in place for any remote access by employees and third parties into the network. This includes the web portal used by Doctors and Government Agencies. The Security Team shall plan, deploy, and enforce the MFA solution at all authentication points. All Users shall be responsible for enrollment in and use of MFA for all necessary system access

PCI Requirement 2 (Vendor Defaults)

This requirement addresses Vendor Defaults and Hardening. All vendor-supplied defaults for passwords, security parameters, and unnecessary accounts on all systems must be changed or disabled immediately upon installation. Secure configuration standards must be documented and applied. The IT/System Admin is responsible for ensuring no default passwords are used. You must execute a hardening checklist upon system setup. The Security Team is responsible for conducting annual audits to verify that no vendor-supplied defaults are active.

PCI Requirement 1 (Firewall)

This requirement covers Firewall Configuration and Maintenance. A firewall must be implemented and maintained. This creates a secure perimeter for the Cardholder Data Environment (CDE). The firewall must be actively supported. Configure the firewall to deny all traffic not explicitly required for business functions (deny-all approach). The IT/System Admin is responsible for replacing the EoL firewall with a currently supported model. You must manage firewall rule sets. The Security Team is responsible for performing a mandatory quarterly review of firewall rules. This ensures they align with the CDE's documented security policies.