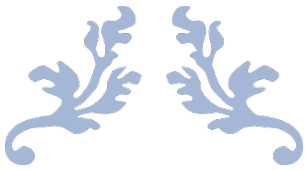

GOVERNANCE, RISK AND COMPLIANCE

Jamal Rizki

Table of Contents

Summary of Current Gaps Found in Fielder Medical Center's Security Framework

Endpoint Security – The assessment report notes that many workstations do not have adequate antivirus protection. Many of the workstations either run unlicensed software or none at all. Consequently, the systems are exposed to malware infections and their associated risks.

Weak IAM controls and policies – It was found that multi-factor authentication is absent across the network infrastructure. The current controls also fail to include an adequate implementation of least-privilege principles, and the access-control policies are lacking. Without enforcement of these controls, systems can be left vulnerable to unauthorized access by a threat actor.

Missing satisfactory governance and documentation – The current system security plan is outdated and lacks adequate regulatory compliance. It either lacks or contains outdated documentation, including an inventory/asset list and an up-to-date risk assessment.

Aging infrastructure – It was noted that archaic systems were in use and in need of review. The use of legacy software and hardware introduces vulnerabilities that are often widely known to threat actors.

Lack of PCI DSS compliance – To achieve compliance for the POS system at its physical location, Fielder Medical Center needs to implement firewalls, deploy an antivirus solution, and update its systems to meet regulatory requirements.

Lacking data protection for personally identifiable information (PII) – Because Fielder Medical Center is a federally funded healthcare facility, it must comply with FISMA; however, its current authentication processes are inadequate to meet these requirements.

Associated Risk Ratings and Analysis

ID	Control	Rating	Explanation
AC-6	Least Privilege	High	Accounts currently have more access than necessary for their functions. If least privilege is not enforced, a threat actor who compromises an account can more easily access sensitive material. A lack of least-privilege controls also expands the scope of internal threats.
CA-5	Plans of Action and Milestones	Moderate	Without a plan of action and milestones, there are no defined steps or processes to

			correct or eliminate discovered vulnerabilities.
CA-7	Continuous Monitoring	High	By not implementing continuous monitoring, systems become vulnerable because anomalies are not detected as they occur.
RA-3	Risk Assessment	High	The current risk and asset assessments are antiquated, meaning that current threats and assets may not have been taken into account.
RA-7	Risk Response	Moderate	There is no documented process for accepting, mitigating, avoiding, or transferring risk. This can lead to errors when developing the correct response.

Justifications for remediation:

Least privilege (AC-6) – FISMA requires federal systems to enforce strict access controls; Fielder Medical Center must remediate this gap to align with AC-6 in *NIST SP 800-53 Revision 5* (National Institute of Standards and Technology [NIST], 2020).

Plan of action and milestones (CA-5) – To meet the requirements under FISMA, Fielder Medical Center must provide a plan of action and milestones as outlined in *NIST SP 800-53 Revision 5* (NIST, 2020)

Continuous monitoring (CA-7) – To remain compliant with FISMA, Fielder Medical Center needs to implement a monitoring program outlined in *NIST SP 800-53 Revision 5* (NIST, 2020)

Risk assessment (RA-3) – An up-to-date risk assessment is a requirement of *NIST SP 800-53 Revision 5* (NIST, 2020); to be in compliance with FISMA, Fielder Medical Center will need to remediate this oversight.

Risk response (RA-7) – FISMA requires that decisions regarding whether to mitigate, transfer, accept, or avoid risk be documented. This has been mandated in *NIST SP 800-53 Revision 5* (NIST, 2020).

Plans For Remediation

Least privilege (AC-6) – To implement least privilege, Fielder Medical Center should create role-based access-control groups and apply the minimum amount of privileges to each job description. There should also be an annual evaluation of these access entitlements.

Plan of action and milestones (CA-5) – The creation of a NIST aligned plan of action and milestones template should be drawn up. This should include all weaknesses found, list the person responsible, and specify a completion date. The plan should also be reviewed regularly.

Continuous monitoring (CA-7) – Fielder Medical Center should collect security event logs and monitor these logs in a centralized location. Logs should be analyzed regularly. Periodic vulnerability scans should also be run, and the results documented and analyzed.

Risk assessment (RA-3) – It is recommended that the risk assessment be updated; this should include the asset inventory, current threats and vulnerabilities, likelihood, and impact data. The assessment should be reassessed regularly to remain current.

Risk response (RA-7) – Fielder Medical Center should document all identified risks and categorize these risks and their responses based on likelihood and impact. This document should be reviewed regularly to ensure compliance.

PCI DSS Policy

Purpose

Fielder Medical Center's upcoming point-of-sale environment requires PCI DSS compliance to ensure the safeguarding of consumers' credit card data.

Scope

All system components, people, and processes, including Fielder Medical Center employees and contractors, third-party providers and any other entities that store, process and transmit cardholder data.

Policy and Assigned Roles

1. Network Security Controls (PCI Requirement 1) – To align with PCI-DSS Requirement 1 (PCI Security Standards Council [PCI SSC], 2022, Requirement 1). Network traffic flows in both directions must be restricted to business necessary scope only, and all non-business traffic is denied by default. To accomplish this, network security controls such

as firewalls will be deployed at every Internet boundary. This policy will be evaluated quarterly to accommodate necessary changes.
Responsible: Network Engineering
Accountable: CISO

2. Secure System Configuration (PCI Requirement 2) – Before any point-of-sale equipment goes into production, all vendor default accounts will be identified and all default passwords changed to meet PCI-DSS requirement 2 compliance (PCI SSC, 2022, Requirement 2).
Responsible: Network Engineering
Accountable: CISO
3. Protecting Systems from Malicious Software (PCI Requirement 5) – To meet the requirements outlined in PCI DSS 5 (PCI SSC, 2022, Requirement 5), an anti-virus solution will be implemented across the network. This anti-malware solution will be actively maintained and updated to ensure protection against evolving threats.
Responsible: Desktop Support
Accountable: CISO

Policy Reviews and Maintenance

This policy will be reviewed annually but is subject to revision should PCI DSS guidance change. This ensures the policy remains fit for purpose.

Works Cited

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5).* https://doi.org/10.6028/NIST.SP.800-53r5

PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and testing procedures, version 4.0*. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf