D486

Governance, Risk, and Compliance

BY:	Christobel Nweke
DATE:	July 8, 2025

Security System Evaluation and Remediation

Introduction

Based off of the Security Assessment report for FMC(Fielder Medical Center) conducted by Dr. Sophia Martin of Pruhart security Consulating, there exist multiple glaring security flaws within FMC.

FMC is required to provide PII(Personally identifiable information) about its doctors to authorized government agencies for validation of information, and securing federal funds on a recurring annual basis. We (FMC) also need to allow a gateway for the Doctors to be able to upload sensitive PII information to prove that they are up to date in their licensing practice. However, as it stands currently we dont have proper controls in place to authentic access to the database where the Doctors PII is stored, which exposes our PII to potential data breach.

we also has several end-of-life systems in place that need to be updated, most notably our current firewall infrastructure which is no longer being supported by the vendor. FMC, also has several workstations without proper Antivirus(AV) software licenses installed. There does not seem to be continuous monitoring at the network or host levels due to the lack of Network/Host Intrusion Detection Systems (IDS). There also does not seem to be proper encryption of data in transit, or data at rest controls being put in place.

FMC has a point of sale (POS) system that requires compliance with PCI DSS. Network segmentation is one requirement needed to ensure PCI DSS compliance. Currently, the FMC POS shares a similar network space as the workstations FMC owns. The POS system also relies on a firewall that is no longer supported.

Figure 1 below provides a high level summary of FMC network topology, which highlights the systems current security posture needing to be improved.

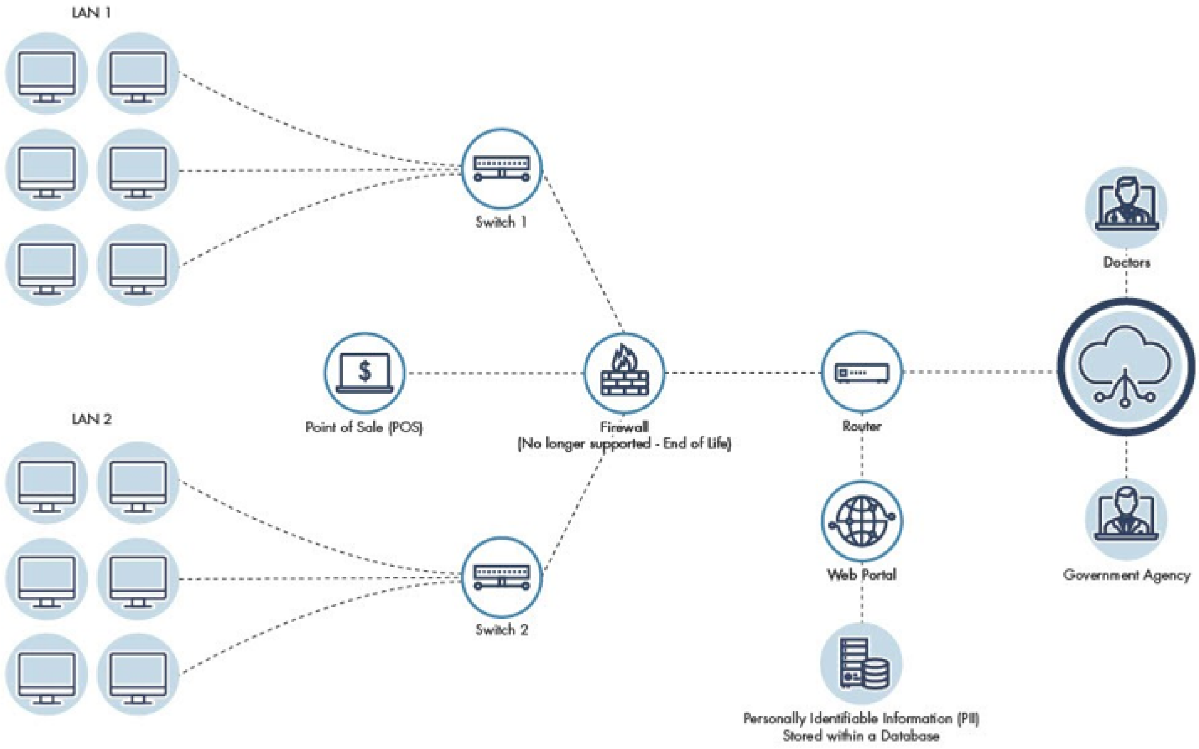

Figure 1: FMC Network Topology Based off Security Assessment Report

SAR Controls Review

To aid in classifying the associated risks from Section 3.3 of the SAR i will be mostly taking a qualitative approach. The method for qualitative assessment will be an impact/probability graph pulling inspiration from Figure 3-4 of Fundamentals of Information Systems Security by David Kim, and Michael G Solomon.

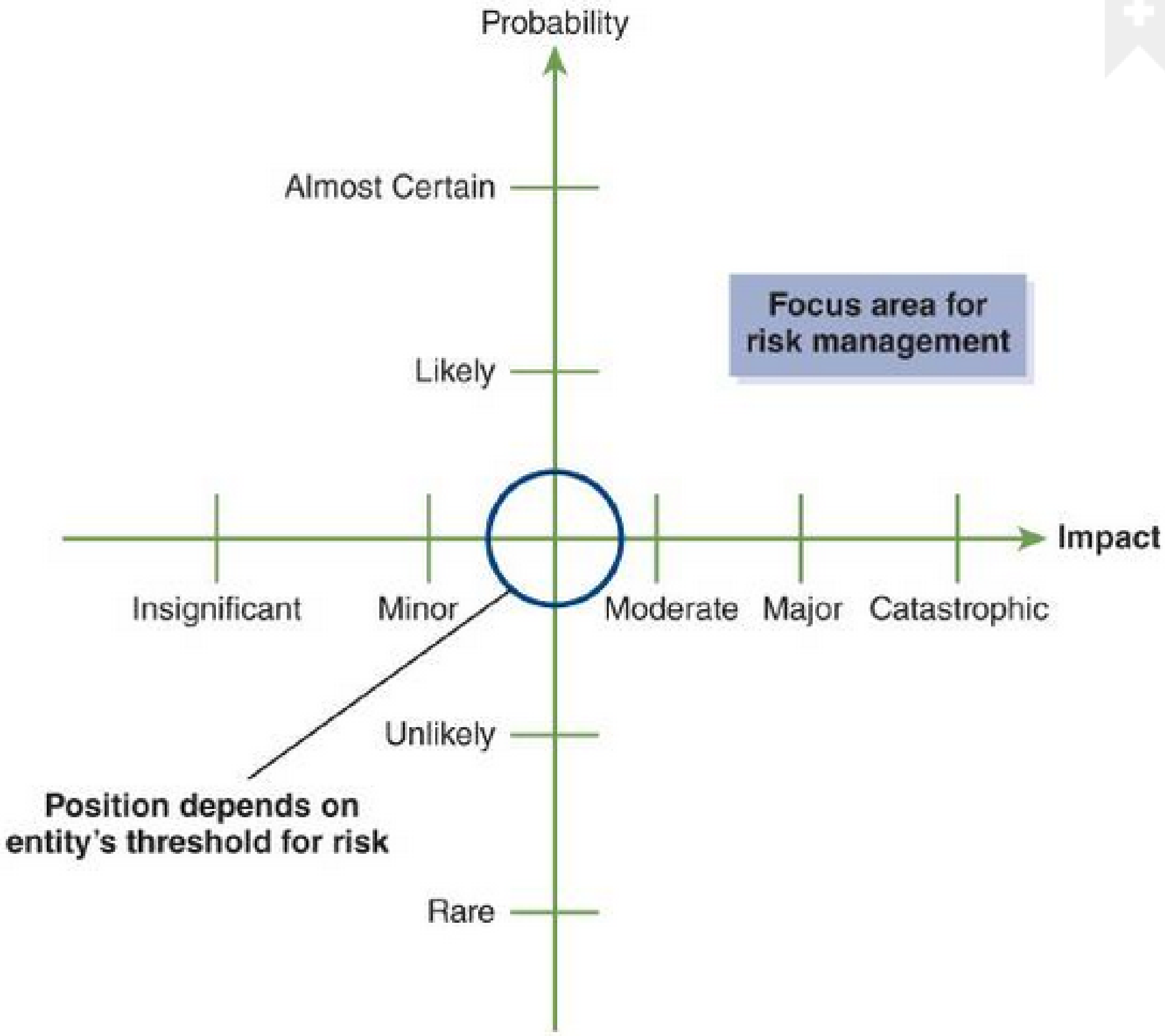

FIGURE 3-4 Qualitative risk assessment.

Figure 2: Impact probability qualitative assessment

AC-6 Least privilege Control Review

Given the current security posture of FMC, the likelihood that privileged actions could be performed by non privileged users is extremely high. Based off FMC current network topology we can see that there is little protection for the database that stores the PII of the doctors at FMC. Therefore, not only can other doctors potentially access the PII of their colleagues, but there isn't a mechanism in place for authentication to even prevent external users who aren't authorized from accessing that database. The web portal acting as a buffer to the database isnt protected, so a lot of privilege escalation exploits could occur The probability of this vulnerability being exploited is high and practically certain. Couple this with the impact, which could not only lead to databreach of sensitive PII of the doctors but this could also affect FMC's ability to gain further funding if the confidentiality of the PII databse for verifying the doctors information is compromised. Therefore i would prioritize this control as being of high importance falling into the top right quadrant of the probability impact graph. This means that it takes high priority in addressing. This would be a risk that would need to be remediated until the residual risk falls to a risk tolerance level that addresses FISMA compliance requirements

A Remediation for AC-6 includes, Implementing an Identity and Access Management System paired with role based access control functionality. This addresses authorization issues by only allowing the authorized personals access to the PII Database. Therefore if a bad actor somehow obtains the credentials of a non authorized internal user, they at least wouldn't have easy access to the PII database. The web portal also needs to be hardened in accordance with OWASP top 10, which highlights the top 10 web vulnerability categories. This is because if the web portal is vulnerable to input validation for example, a bad actor could do a lot. They could obtain doctor information directly from the PII database and disturb the integrity of the database by changing the data stored via SQL injection, and even directly execute commands with cross site scripting.

Pairing the above hardening of the web portal a Web Application Firewall (WAF) i believe would help reduce overall attack surface as it'll act as another extra security layer for filtering, monitoring, and even blocking troublesome traffic to the web portal. Additionally ensuring that all endpoints have an antivirus capable of preventing, detecting, and removing malware could help protect against attacks that could lead to privilege escalation exploits.

CA-5 Plans of Action and Milestones Control Review/Remediaton

Not having a plan of action and milesstone control review in place is definitely detrimental because having such a consistent system in place helps keep track of identified vulnerabilities and ensures those vulnerabilities aren't lost and forgotten which could lead to future exploitation. Such a control is also a requirement for organizations required to be in compliance with government regulations like FISMA, FEDRAMP etc. The impact of not having this control implemented i would say is major but the likelihood of exploitation is unlikely. FMC is required to have this implemented but considering that FMC doesn't handle classified government data, it's more accurate to classify this control as a moderate risk that does need to be remediated due to its requirement as part of FISMA compliance but that could also take less priority over for example, AC-6 Least privilege Control.

To remediate this risk, we will needs to implement a process for handling the creation of Plans of Actions and Milestones (POA&M). This would help with organization and effectiveness in tracking and remediating found vulnerabilities, and would also help ensure we at FMC meet compliance quicker. Inspiration for guides/templates on how to go about this can be drawn from OMB A-130 guidelines. Assigning/Training an individual responsible for overseeing the entire plan and who can then delegate/train other owners on a per staff/team basis is crucial and would also help ensure a smooth flowing process for instituting POA&Ms.

CA-7 Continous Monitoring Control Review

Lack of continuous monitoring control can lead to confidentiality issues in the PII database the doctors upload to. Given the fact that government agencies also need access to the same database ensuring that the full scope of the CIA triad isn't violated is very important. The implementation of this control helps address that. Loss of reputation, loss of federal funding, Doctor PII possibly being breached, and the probability of exploitation is high given the current state of our network topology which has no preventative measures on the web portal access to the database/the database itself. Therefore, i would assign this a risk rating of High. Lack of a continious monitoring solution is crucial, because if an exploitation were to occur it could go undetected for weeks, months or even years which can be catastrophic for the organization as a whole.

A good remediation for this would be to first, use the Nist SP 800-137 to develop a consistent strategy. Once developed, we can employ the use of Security Information and Event Management (SIEM) tools like Datadog, to monitor critical endpoints like the PII database. Using SIEM tools like DataDog allows automated monitoring of the connection endpoints that the Doctors/Government Agency connect to, which allows for us to monitor for suspicious activity. SIEM tools like Datadog these days i have learned are robust enough to even be configured to detect against a large number of up-to-date attack threats in real time, and can even serve as a first response for prevention in addition to detection if needed.

RA-3/RA-7 Risk Assessment/Risk Response Controls Review

In order to keep receiving funding we at FMC need to continously stay in compliance. Therefore there is a need to have a Risk Assessment framework/plan in place that helps ensure that areas of noncompliance can be found via RA-3 controls and then also addressed via RA-7 Risk Response controls. Both go hand in hand, and lack of proper implementation of both can lead to organizational reputation loss in addition to loss of federal funding and breach of data. Therefore i would assign both controls a risk rating of High over moderate just to emphasize the importance of implementing both controls correctly to avoid failing future audits and falling out of compliance. The lack of both controls in the system is one that definitely needs to be remediated, because FISMA mandates it. It is not a risk that can be transfered, or avoided or we would risk losing federal funding.

For RA-3 Risk Assessment a good remediation step would be taking thought process from NIST SP 800-30. NIST SP 800-30 details an in-depth guide on preparing, and conducting an actual risk assessment (Chapter 3.1-3.2). For example we can identify the firewall as an asset needing to be Risk Assessed. Then apply the

Risk Assessment steps carefully detailed in NIST SP 800-30, EX: identify threat sources, identify threat events, identify vulnerabilities etc.

For RA-7 Risk Response i'll pull inspiration from NIST SP 800-39 (Chapter 3.3 - Responding to risk). Following the prior example for RA-3 Risk Assessment, the response for the firewall risk assessment could fall under, Risk Acceptance, Risk Avoidance, Risk Mitigation, Risk Sharing or Transfer. In this case a Risk Mitigation response would be appropriate. This would require decommissioning the End of Life (EoL) firewall system and upgrading to a Newer Firewall preferrable a Next-Gen Firewall for better capabilities. To take it even further NIST SP 800-39 calls for integrating risk management in a continuous fashion, which would be beneficial in the future for us as it would reduce the number of compliance issues needing to be dealt with at a time. So, in the case of the firewall we can implement a continuous risk assessment methodology that evaluates End of Life (EoL) systems and alerts for its replacement sooner.

PCI DSS-compliant policy

In order to address the POS system PCI DSS compliance, we can do the following, building and maintaining a secure network, secure configuration of all system components, and addition of a good Antivirus solution. Building and maintaining a secure network, requires maintaining a secure firewall configuration to protect cardholder data. The Networking team at FMC should opt for Next-Gen Firewall over a regular fireall, as it provides more security features like deep packet inspection, more granular control and even Intrusion Prevention Capabilities which can better secure Card Payment Data.
Below highlights the minimum firewall configuration that the Networking team needs to ensure is met to satisfy PCI DSS compliance:

- Change default firewall password provided by vendor,
- Restrict in/outbound traffic to POS to only what's necessary,
- Avoid use of "Any" in firewall allow rules,
- "Deny all" traffic that you dont specifically authorize,
- Permit only established connections into network,
- Turn on intrusion detect and intrusion blocking if available,
- Turn on notifications,
- Turn on Network address translation to hide internal addressed from the internet,
- Check for and install firewall updates or patches to address new vulnerabilities, as soon as available

To meet the secure configuration of all system components the Systems Administrator in charge of change configuration management would need to ensure that as part of FMC's POS system configuration management policy all default passwords on the POS systems are changed as well as the removal of unnecessary software, functions, and accounts on the system.

Lastly, the FMC IT Security team should ensure that a proper Antivirus program is being employed on the POS system. The Antivirus program needs to be continuous, up to date with the latest signatures in order to prevent malware on the POS system, and also be capable of detecting/removing malware.

Bibliography

[1] NIST US Department of Commerce. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* 2011. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[2] NIST US Department of Commerce. *Guide for Conducting Risk Assessments.* 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[3] OMB. *CIRCULAR NO. A-130.* 2016. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[4] PCI Security Standards Council. *PCI Firewall Basics.* 2018. URL: https://www.pcisecuritystandards.org/wp-content/uploads/2022/05/Small-Merchant-Firewall-Basics.pdf (visited on 2018).

[5] Joint Task Force. *NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations.* 2018. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[6] Joint Task Force. *TABLE C-4: ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY.* 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[7] David Kim and Solomon Michael G. *Chapter 3, "Risks, Threats, and Vulnerabilities".* 2021. URL: https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/reader.action?docID=6741186&ppg=740.

[8] David Kim and Solomon Michael G. *Fundamentals of Information Systems Security.* 2021. URL: https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/reader.action?docID=6741186&ppg=740.

[9] OWASP. *OWASP Top 10.* 2024. URL: https://owasp.org/www-project-top-ten/.

[10] PCI Security Standards Council. *PCI DSS v4.x Quick Reference Guide.* 2025. URL: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4_x-QRG.pdf.

[11] DATADOG. *Security Cloud SIEM.* 2025. URL: https://www.datadoghq.com/product/cloud-siem/ (visited on 2025).