

Security System Evaluation and Remediation

Governance, Risk, and Compliance

Damian Yates | D486 | August 18, 2024

## **Introduction**

### Fielder Medical Center (FMC) is a federally funded healthcare facility deeply committed to providing high-quality medical services to its community. In its ongoing efforts to modernize operations and increase efficiency, FMC is undertaking a critical initiative to digitize its data management and operational processes. This transition from a paper-based system to a secure digital platform is a step toward streamlining operations and a necessary move to comply with the Federal Information Security Management Act (FISMA) (United States Congress, 2002).

### FISMA mandates that all federal agencies, including entities like FMC that receive federal funding, must ensure the security of their information systems. Non-compliance with FISMA can have severe consequences, including the potential for substantial financial penalties, loss of federal funding, and significant reputational damage. Moreover, failure to comply could expose sensitive patient and staff information to unauthorized access, putting individuals' privacy at risk and undermining the community's trust in FMC.

### As part of its digitization initiative, FMC is implementing advanced systems to manage licensing, certification, and other professional documentation for its medical staff. These efforts are designed to enhance internal operational efficiency and protect sensitive data's confidentiality, integrity, and availability in compliance with FISMA requirements. By ensuring that its digital systems meet these stringent federal security standards, FMC is safeguarding its operations and reinforcing its commitment to secure, efficient, and compliant healthcare services.

### Problem Statement

Fielder Medical Center (FMC) faces several critical vulnerabilities within its security framework, which pose significant risks to the organization's ability to protect sensitive information and maintain compliance with federal regulations. The absence of formalized security policies, such as access control and account management, combined with an outdated System Security Plan (SSP), exposes FMC to potential unauthorized access and data breaches. In addition, the lack of adequate endpoint protection and the absence of multifactor authentication (MFA) further increase the likelihood of cyberattacks.

The proposed Point-of-Sale (POS) system fails to meet Payment Card Industry Data Security Standard (PCI DSS) compliance due to insufficient security measures, placing FMC at risk of costly non-compliance penalties. Furthermore, the system designed to allow secure access for government agencies to verify documents must be more adequately protected, heightening the probability of unauthorized access and data compromise.

The absence of a continuous enterprise monitoring strategy significantly exacerbates these vulnerabilities, undermining FMC’s ability to detect and respond to security incidents in real-time. Such deficiencies threaten FMC’s security posture and regulatory compliance and expose the organization to severe financial and reputational damage.

According to a report by IBM, the healthcare sector's average data breach cost is $9.23 million, the highest across all industries (IBM Security, 2021). A breach at FMC could result in substantial financial losses, potential fines, legal repercussions, and a devastating impact on the trust and confidence of patients, partners, and the community. The reputational harm from a data breach could have long-term consequences, diminishing FMC’s standing in the healthcare sector and eroding its ability to deliver high-quality care. Therefore, addressing these security gaps is imperative for safeguarding FMC’s operations, finances, and reputation.

## **Objective**

This paper aims to develop a comprehensive cybersecurity strategy that will address the critical risks identified in the security assessment of Fielder Medical Center (FMC) and ensure compliance with the Federal Information Security Management Act (FISMA). This strategy will improve FMC's security framework by implementing necessary policy updates, enhancing existing technical controls, and establishing a continuous monitoring process. The goal is to safeguard FMC’s designated sensitive information, mitigate potential threats, and align FMC’s operations with federal regulatory requirements to maintain the organization’s integrity and reputation in the healthcare sector.

### Background

Fielder Medical Center (FMC) is subject to strict federal regulations, including the Federal Information Security Management Act (FISMA), which mandates that all federal agencies and organizations handling federal data implement robust security controls to protect sensitive information. FISMA is particularly relevant to FMC because it directly addresses the protection of Personally Identifiable Information (PII), which includes data such as names, addresses, social security numbers, and other personal details. Given that FMC’s system manages and stores sensitive PII related to its medical staff, compliance with FISMA is not only a legal requirement but also critical to maintaining the trust of medical professionals and the government agencies that rely on the integrity of this data.

FISMA’s importance lies in its comprehensive framework for ensuring that information systems are secure and that risks are managed effectively. By adhering to FISMA standards, FMC can mitigate the risks associated with unauthorized access, data breaches, and other security threats, thereby safeguarding the PII of its doctors and ensuring the organization’s eligibility for federal funding.

## **Overview of the Security Assessment**

To assess FMC’s compliance with FISMA and identify potential vulnerabilities in its security framework, an external security consulting firm, Pruhart Security Consulting, conducted a thorough security assessment. The scope of this assessment included a comprehensive evaluation of FMC’s systems, mainly focusing on the newly implemented system for managing doctor credentials. The evaluation aimed to determine the effectiveness of existing security controls, identify gaps in compliance with FISMA requirements, and recommend necessary improvements to enhance FMC’s overall security posture.

### Methodology

The assessment followed a structured approach aligned with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), specifically adhering to the guidelines outlined in NIST Special Publication 800-53 (National Institute of Standards and Technology, 2020) and NIST Special Publication 800-37 (National Institute of Standards and Technology, 2020). The methodology involved several key steps:

1. **Security Control Evaluation**: The team evaluated FMC’s current security controls as documented in the System Security Plan (SSP), focusing on access control, data protection, and risk management per the NIST SP 800-53 guidelines.
2. **Vulnerability Identification**: A detailed analysis was conducted to identify any vulnerabilities within FMC’s network, systems, and endpoints. This included reviewing the state of endpoint protection, the presence of multifactor authentication, and the overall security of the network infrastructure.
3. **Threat Analysis**: The assessment identified potential threats associated with the vulnerabilities and assessed the likelihood and impact of these threats on FMC’s operations and data security.
4. **Risk Assessment**: The risks identified were analyzed regarding their potential impact on FMC’s ability to protect Personally Identifiable Information (PII) and maintain compliance with the Federal Information Security Management Act (FISMA). This step included a gap analysis to determine where FMC’s current practices fell short of FISMA requirements, following the guidelines in NIST SP 800-37 (National Institute of Standards and Technology, 2020).
5. **Recommendations**: Based on the findings, the consulting team provided detailed recommendations for closing compliance gaps, enhancing security controls, and ensuring continuous monitoring and improvement of FMC’s security posture.

This security assessment provides FMC with a clear understanding of its current security weaknesses and the necessary steps to align with FISMA standards, thereby ensuring the protection of sensitive information and maintaining regulatory compliance.

## **Risk Analysis**

The security assessment report for Fielder Medical Center (FMC) identified several key findings that highlight critical vulnerabilities in the organization’s current security framework. These findings have significant implications for FMC’s ability to protect sensitive information and maintain compliance with government regulatory requirements, particularly under the Federal Information Security Management Act (FISMA).

### Key Findings

* **Lack of Formalized Security Policies:** FMC lacks access control or account management policies. These are foundational elements of any security framework, and their absence leaves the organization vulnerable to unauthorized access to sensitive systems and data.
* **Outdated System Security Plan (SSP):** The existing SSP is outdated and does not reflect the current operational environment or compliance requirements. This gap means that FMC’s security controls may be inadequate to protect against modern threats.
* **Inadequate Endpoint Protection:** The assessment revealed that many workstations connected to FMC’s network either lack antivirus protection or run outdated, unlicensed software. This exposes the organization to a heightened risk of malware infections and cyberattacks.
* **Absence of Multifactor Authentication (MFA):** FMC has not implemented MFA across its systems, which increases the risk of unauthorized access to sensitive personal and professional information. MFA is a critical control for ensuring only authorized individuals can access FMC’s systems.
* **Compliance Gaps Related to PCI DSS:** The planned Point-of-Sale (POS) system lacks necessary security measures, such as firewalls and secure configurations, preventing FMC from meeting PCI DSS compliance standards. This is particularly concerning, given the sensitive nature of financial transactions (PCI Security Standards Council, 2022).
* **Insecure Government Access Portal:** The system that allows government agencies to verify doctor credentials is inadequately protected. The current weak authentication mechanism potentially allows unauthorized access to sensitive information.
* **Lack of Continuous Monitoring:** FMC does not have a continuous monitoring strategy, which is essential for detecting and responding to security incidents in real time. This gap leaves the organization vulnerable to undetected breaches and prolonged exposure to threats.

### Potential Consequences of the Risks Identified

The consequences of these risks, if left unaddressed, could be severe:

* **Data Breaches and Unauthorized Access:** The lack of access control policies, outdated SSP, and absence of MFA significantly increase the likelihood of unauthorized access to FMC’s systems. A data breach involving doctors' personally identifiable information (PII) could lead to identity theft, financial fraud, and legal liabilities for FMC.
* **Malware Infections and Cyberattacks:** Inadequate endpoint protection makes FMC’s network highly susceptible to malware infections, ransomware attacks, and other cyber threats. These could disrupt operations, result in data loss, and compromise sensitive information.
* **Regulatory Non-Compliance and Legal Repercussions:** The gaps in compliance with FISMA and PCI DSS could result in regulatory penalties, loss of federal funding, and damage to FMC’s reputation. Non-compliance with FISMA could jeopardize FMC’s ability to operate as a federally funded healthcare facility.
* **Operational Disruptions:** The absence of continuous monitoring means that security incidents could go undetected for extended periods, leading to prolonged operational disruptions and increased costs associated with incident response and recovery.

### Areas Where Current Security Procedures and Posture Fail to Meet Compliance Requirements

FMC’s current security posture fails to meet government regulatory compliance requirements in several critical areas:

* **Access Control and Account Management:** The lack of formalized policies for access control and account management directly violates FISMA requirements, which mandate strict controls over who can access sensitive information.
* **System Security Plan (SSP):** An outdated SSP that does not align with current operational realities and compliance standards is a significant compliance gap. FISMA requires that the SSP be regularly updated to reflect changes in the system and the threat landscape.
* **Multifactor Authentication (MFA):** FISMA emphasizes the need for robust authentication mechanisms, including MFA, to protect sensitive information. FMC’s failure to implement MFA is a significant compliance issue.
* **Endpoint Protection:** The lack of adequate antivirus and endpoint protection violates essential cybersecurity best practices and fails to meet FISMA’s requirements for protecting federal information systems.
* **Continuous Monitoring:** FISMA mandates continuous monitoring as a vital component of a robust cybersecurity framework. FMC’s lack of a continuous monitoring strategy represents a significant compliance failure.
* **PCI DSS Compliance:** FMC’s planned POS system does not meet the security standards required for PCI DSS compliance, putting the organization at risk of non-compliance with financial regulations.

FMC must address these gaps to mitigate the identified risks, protect sensitive information, and ensure compliance with FISMA and other relevant regulatory requirements.

## **Cyber Strategy Development**

A robust cybersecurity strategy is essential to address the risks identified in the security assessment and bring Fielder Medical Center (FMC) into compliance with FISMA. This strategy will implement vital technical controls, including Multifactor Authentication (MFA), Extended Detection and Response (XDR), and critical network enhancements. These controls will significantly strengthen FMC’s security posture, protect sensitive information, and ensure continuous compliance with federal regulations.

### Technical Controls

1. **Implementation of Multifactor Authentication (MFA)**

One of the most critical measures that FMC must implement is Multifactor Authentication (MFA). MFA adds a layer of security by requiring users to provide two or more forms of authentication before accessing FMC’s systems. This could include something the user knows (e.g., a password), something the user has (e.g., a security token or mobile device), and something the user is (e.g., biometric verification). According to the National Institute of Standards and Technology (NIST), MFA is recognized as a critical security control that significantly enhances the security of information systems by mitigating the risk of unauthorized access (NIST SP 800-63B, 2017).

#### **Benefits of MFA:**

* **Enhanced Security:** By requiring multiple forms of authentication, MFA significantly reduces the risk of unauthorized access, even if one credential is compromised. The Verizon Data Breach Investigations Report (2021) notes that compromised credentials are a leading cause of data breaches, and MFA is an effective measure to mitigate this risk.
* **Regulatory Compliance:** Implementing MFA aligns with FISMA requirements for secure authentication mechanisms, reducing non-compliance likelihood. It also supports compliance with other regulations, such as HIPAA, which mandates the protection of electronic health information (U.S. Department of Health and Human Services, 2013).
* **Protection of Sensitive Information:** MFA is crucial for protecting Personally Identifiable Information (PII) and other sensitive data stored in FMC’s systems. The Health Sector Coordinating Council (HSCC) advocates for MFA as a best practice to protect against unauthorized access to health records and other sensitive data (HSCC, 2020).

#### **Implementation Plan:**

* **Step 1:** Conduct a pilot implementation of MFA on critical systems, such as those that handle PII and financial transactions. This phased approach allows FMC to identify and address any challenges before a full-scale rollout.
* **Step 2:** Gradually roll out MFA across all FMC systems, ensuring all users are equipped and trained to use the new authentication process. User education and training are critical to successfully adopting MFA (Cisco, 2021).
* **Step 3:** Regularly review and update MFA policies and procedures to adapt to new security threats and technological advancements. Continuous evaluation and improvement are essential to maintain the effectiveness of MFA (NIST SP 800-63B, 2017).

1. **Deployment of Extended Detection and Response (XDR)**

To further enhance FMC’s cybersecurity defenses, the deployment of Extended Detection and Response (XDR) is recommended. XDR is an integrated security solution that provides comprehensive visibility, detection, and response across multiple security layers, including endpoints, networks, servers, and cloud environments. Gartner (2020) identifies XDR as a transformative approach to threat detection and response, emphasizing its ability to improve security operations through integrated, automated processes.

#### **Benefits of XDR:**

* **Improved Threat Detection:** XDR enables real-time monitoring and detection of advanced threats across all FMC’s IT environment layers, reducing the time to detect and respond to security incidents. According to Gartner (2020), XDR offers superior detection capabilities compared to traditional security solutions by correlating data across various sources.
* **Centralized Incident Management:** XDR provides a unified platform for managing security incidents, allowing FMC’s security team to investigate and respond to threats from a single interface quickly. This centralized approach streamlines incident management and improves response times (Forrester, 2021).
* **Automated Response Capabilities:** XDR can automate responses to certain types of threats, reducing the burden on FMC’s security team and ensuring rapid containment of potential breaches. Automation is crucial in modern cybersecurity strategies, helping address the growing threats and limited human resources (Gartner, 2020).

#### **Implementation Plan:**

* **Step 1:** Assess FMC’s current security infrastructure and identify gaps that XDR can address. A thorough assessment is necessary to ensure that XDR is effectively integrated with existing systems and processes.
* **Step 2:** Select and deploy an XDR solution that integrates with existing security tools, such as antivirus software and firewalls. Integration with existing tools maximizes the effectiveness of XDR by leveraging already established defenses (Gartner, 2020).
* **Step 3:** Train FMC’s security team on using XDR and establish incident detection, investigation, and response procedures. Practical training ensures that the security team fully utilizes XDR’s capabilities (Forrester, 2021).
* **Step 4:** Continuously monitor the effectiveness of XDR and adjust configurations as needed to respond to evolving threats. Continuous monitoring and adaptation are essential to maintaining a robust security posture (Gartner, 2020).

1. **Network Enhancements**

In addition to MFA and XDR, FMC must implement key network enhancements to protect against unauthorized access and ensure the integrity of its IT environment. These enhancements will address existing vulnerabilities and strengthen the overall security of FMC’s network infrastructure. The Center for Internet Security (CIS) recommends implementing advanced network security measures as part of a comprehensive cybersecurity strategy (Center for Internet Security, 2020).

#### **Key Network Enhancements:**

* **Firewall Upgrades:** FMC must upgrade its existing firewalls to next-generation firewalls (NGFWs) that provide advanced threat protection, including deep packet inspection, intrusion prevention, and application-level filtering. NGFWs are essential for defending against sophisticated cyber threats and ensuring compliance with security standards (Center for Internet Security, 2020).
* **Network Segmentation:** To minimize the impact of potential breaches, FMC should implement network segmentation, dividing the network into distinct security zones. Sensitive data, such as PII, should be isolated from less critical areas of the network. The PCI Security Standards Council (2022) emphasizes network segmentation as a best practice for reducing the scope of security incidents.
* **Secure Remote Access:** With the increasing reliance on remote work, FMC should implement secure remote access solutions, such as Virtual Private Networks (VPNs) with MFA, to ensure that remote connections to the network are secure. Secure remote access is critical for protecting against unauthorized access and maintaining the security of FMC’s IT environment (NIST SP 800-46, 2016).

#### **Implementation Plan:**

* **Step 1:** Conduct a network security audit to identify areas that require enhancement, including outdated firewall configurations and insufficient network segmentation. A comprehensive audit provides the foundation for targeted improvements (Center for Internet Security, 2020).
* **Step 2:** Upgrade firewalls and implement network segmentation based on the data's sensitivity and the systems' criticality. Prioritizing these upgrades ensures that FMC’s most valuable assets are protected first.
* **Step 3:** Establish secure remote access protocols and roll out VPNs with MFA for all remote users. This step is crucial for ensuring remote work does not compromise network security (NIST SP 800-46, 2016).
* **Step 4:** Regularly test and update network security configurations to adapt to new threats and ensure ongoing protection. Continuous testing and updates are vital for maintaining an effective security posture (Center for Internet Security, 2020).

### PCI DSS Compliance Policy Update

To ensure Fielder Medical Center (FMC) achieves and maintains compliance with the Payment Card Industry Data Security Standard (PCI DSS), the following policy addresses the critical concerns outlined in section 3.2.4 of the Security Assessment Report (SAR). These concerns include the lack of proper network segmentation, inadequate firewall configurations, and the absence of antivirus solutions on systems connected to the Point-of-Sale (POS) network. The policy will emphasize network segmentation as a best practice for reducing the scope of security incidents and clearly define the roles and responsibilities of each component involved in achieving PCI DSS compliance.

1. **Network Segmentation**

**Objective:**To reduce the scope of security incidents and limit the impact of potential breaches, FMC will implement network segmentation to isolate systems that handle payment card data from the rest of the network.

#### **Roles and Responsibilities:**

##### Network Security Team:

* + Design and implement network segmentation, ensuring that systems processing, storing, or transmitting payment card data are isolated from non-sensitive areas of the network.
  + Regularly review and update network segmentation configurations to adapt to evolving security threats and business needs.
  + Monitor segmented networks for any unauthorized access attempts and take immediate action to remediate breaches.

##### IT Infrastructure Team:

* + Ensure that all network devices, such as routers and switches, are configured to support and enforce the segmentation policies the Network Security Team established.
  + Maintain documentation of network segmentation architecture and ensure alignment with PCI DSS requirements.
  + Collaborate with the Network Security Team to conduct periodic audits of the segmented network to ensure compliance.

1. **Firewall Configuration**

**Objective:**  
To protect FMC’s POS network from unauthorized access and external threats, robust firewall configurations will be implemented and maintained.

#### **Roles and Responsibilities:**

##### Firewall Management Team (Subset of Network Security Team):

* + Configure firewalls to restrict inbound and outbound traffic to and from the POS network, allowing only necessary and authorized communications.
  + Regularly review and update firewall rules to reflect any changes in network architecture or regulatory requirements.
  + Monitor firewall logs for signs of suspicious activity and work with the Incident Response Team to address potential threats.

##### IT Compliance Officer:

* + Ensure firewall configurations comply with PCI DSS requirements and are appropriately documented.
  + Coordinate with the Firewall Management Team to schedule regular firewall rule reviews and audits.
  + Report on the status of firewall configurations during PCI DSS compliance assessments and audits.

1. **Antivirus Solutions**

Objective:  
To protect FMC’s POS systems from malware infections, all systems connected to the POS network will be equipped with up-to-date antivirus solutions.

#### Roles and Responsibilities:

##### Endpoint Security Team:

* + Deploy and manage antivirus software on all systems within the POS network.
  + Ensure that antivirus definitions are regularly updated and that real-time scanning is enabled on all systems.
  + Monitor antivirus alerts and logs to detect and respond to potential malware threats.

##### System Administrators:

* + Assist the Endpoint Security Team in deploying and configuring antivirus solutions on POS systems.
  + Ensure that any newly added systems to the POS network are promptly equipped with the required antivirus protection.
  + Report any issues or anomalies with antivirus software to the Endpoint Security Team for immediate resolution.

1. **Monitoring and Reporting**

Objective:  
To maintain continuous PCI DSS compliance, FMC will implement regular monitoring and reporting processes to ensure all systems and policies function as intended.

#### Roles and Responsibilities:

##### IT Compliance Officer:

* + Develop and maintain a compliance monitoring schedule that includes regular reviews of network segmentation, firewall configurations, and antivirus software.
  + Prepare reports for senior management detailing the status of PCI DSS compliance efforts, highlighting any areas of concern or improvement.
  + Serve as the primary liaison with external auditors during PCI DSS assessments.

##### Incident Response Team:

* + Collaborate with the Network Security Team, Firewall Management Team, and Endpoint Security Team to respond to any security incidents that may affect PCI DSS compliance.
  + Conduct post-incident reviews to identify gaps in policies or procedures and recommend improvements to prevent future incidents.

This updated PCI DSS policy effectively addresses the concerns identified in the SAR by establishing clear roles and responsibilities for each component involved in maintaining compliance. By emphasizing network segmentation as a best practice, implementing robust firewall configurations, and ensuring the deployment of antivirus solutions, FMC will significantly reduce the scope of security incidents and protect its POS network from potential threats. Regular monitoring and reporting will ensure that all components function as intended, thereby maintaining FMC's compliance with PCI DSS requirements and safeguarding its systems against evolving security challenges.

### Policy and Procedural Updates:

In addition to implementing technical controls, Fielder Medical Center (FMC) must update its policies and procedures to address the deficiencies identified in the security assessment and to align with best practices and regulatory requirements. Key focus areas include establishing Least Privilege Access policies, implementing Continuous Monitoring, and enhancing Risk Assessment and Response procedures. These updates are critical to developing a comprehensive cybersecurity strategy that protects FMC’s sensitive information and ensures ongoing compliance with FISMA.

#### **1. Least Privilege Access**

The principle of Least Privilege Access is a fundamental security concept that dictates that users should only have the minimum level of access necessary to perform their job functions. By restricting access rights, FMC can significantly reduce the risk of unauthorized access to sensitive information, minimize the potential damage from insider threats, and ensure that access to critical systems and data is tightly controlled.

##### Policy Implementation:

* **Access Control Policies**: FMC must establish and enforce access control policies that define the levels of access required for different roles within the organization. These policies should be based on the principle of least privilege and regularly reviewed and updated to reflect changes in job functions or organizational structure.
* **Role-Based Access Control (RBAC)**: Implementing RBAC will allow FMC to assign permissions based on user roles, ensuring that individuals only have access to the resources necessary for their responsibilities. This approach enhances security and simplifies the management of user access rights.
* **Periodic Access Reviews**: FMC should regularly review user access rights to ensure they remain appropriate. This includes revoking access for employees who no longer need it and adjusting permissions as job roles evolve.

#### **2. Continuous Monitoring**

Continuous Monitoring is a critical component of a robust cybersecurity strategy, enabling FMC to maintain real-time awareness of its security posture and respond swiftly to emerging threats. Continuous Monitoring involves the ongoing collection, analysis, and reporting of security-related data, allowing FMC to detect and mitigate security incidents before they can cause significant harm.

##### Policy Implementation:

* **Monitoring Strategy**: FMC must develop a comprehensive continuous monitoring strategy that outlines the specific metrics and indicators to be tracked, the tools and technologies to be used, and the processes for analyzing and responding to security events.
* **Integration with XDR**: By integrating Continuous Monitoring with the Extended Detection and Response (XDR) solution, FMC can achieve enhanced visibility across its IT environment. This integration will enable automated detection and response to threats, reducing the time to identify and mitigate potential security incidents.
* **Incident Reporting and Response Procedures**: FMC should establish clear procedures for reporting and responding to security incidents detected through continuous monitoring. These procedures should include predefined escalation paths, roles and responsibilities, and communication protocols to ensure a coordinated and effective response.

#### **3. Risk Assessment and Response**

Risk Assessment and Response are crucial for identifying, evaluating, and mitigating potential risks to FMC’s information systems and data. A proactive approach to risk management allows FMC to anticipate potential threats, prioritize remediation efforts, and allocate resources effectively to protect against security breaches.

##### Policy Implementation:

* **Regular Risk Assessments**: FMC must conduct regular risk assessments to identify potential vulnerabilities and evaluate the likelihood and impact of various threats. These assessments should consider internal and external factors, including changes in the regulatory environment, technological advancements, and evolving threat landscapes.
* **Risk Mitigation Strategies**: Based on the findings of the risk assessments, FMC should develop and implement risk mitigation strategies that address identified vulnerabilities. This may include technical controls, such as patch management and system hardening, as well as procedural controls, such as employee training and awareness programs.
* **Risk Response Plan**: FMC should establish a formal risk response plan that outlines the steps to be taken during a security incident. This plan should include containment, eradication, recovery procedures, and communication guidelines with stakeholders and regulatory authorities.

Implementing Least Privilege Access, Continuous Monitoring, and enhanced Risk Assessment and Response procedures are essential elements of FMC’s cybersecurity strategy. Together, these policies and procedures create a layered defense that minimizes the risk of unauthorized access, ensures real-time detection and response to security incidents, and provides a proactive approach to managing potential threats. By embedding these practices into its cybersecurity strategy, FMC can strengthen its security posture, protect sensitive information, and maintain compliance with FISMA and other regulatory requirements.

### Governance and Compliance

Effective governance and compliance are foundational to the success of Fielder Medical Center’s (FMC) cybersecurity strategy. To ensure that FMC aligns with regulatory requirements such as the Federal Information Security Management Act (FISMA) and maintains a strong security posture, it is essential to focus on updating the System Security Plan (SSP), implementing comprehensive training programs, and establishing robust documentation and auditing processes. These elements are crucial for maintaining continuous compliance and demonstrating FMC’s commitment to protecting sensitive information.

#### **1. Updating the System Security Plan (SSP)**

The System Security Plan (SSP) is a critical document that outlines FMC’s security controls, procedures, and policies to protect its information systems. An updated SSP is essential for ensuring that FMC’s security framework is aligned with current operational realities and regulatory requirements.

##### Implementation Steps:

* **Review and Revise the SSP**: FMC must thoroughly review its existing SSP to identify outdated sections and areas requiring enhancement. This review should consider changes in the organization’s systems, processes, and compliance requirements since the last update.
* **Incorporate New Security Controls**: The updated SSP should reflect all new security controls and measures that have been implemented, such as Multifactor Authentication (MFA), Extended Detection and Response (XDR), and network enhancements. These additions are critical to demonstrating FMC’s commitment to protecting sensitive data and complying with FISMA.
* **Regular Updates**: FMC should establish a policy for the regular review and updating of the SSP, ensuring that it remains current and reflects any changes in the threat landscape, technology, or regulatory environment. This could be scheduled annually or in response to significant organizational operations changes.

#### **2. Implementing Comprehensive Training Programs**

Training is vital to FMC’s cybersecurity strategy, as human error is often the weakest link in security defenses. By implementing comprehensive training programs, FMC can ensure that all employees know security policies, understand their responsibilities, and are equipped to recognize and respond to potential threats.

##### Implementation Steps:

* **Security Awareness Training**: FMC should develop and deliver regular security awareness training sessions for all employees, covering topics such as recognizing phishing attempts, the importance of strong passwords, and best practices for data protection. This training should be mandatory and tailored to the specific roles and responsibilities of the participants.
* **Specialized Training for IT and Security Staff**: FMC should provide specialized training and general awareness training for its IT and security personnel. This training should focus on implementing and managing the organization’s security controls and incident response procedures and using tools such as XDR.
* **Continuous Learning and Updates**: FMC should encourage a culture of continuous learning by providing regular updates and refresher courses on emerging threats and new security practices. This ensures that employees remain vigilant and up-to-date with the latest security challenges.

#### **3. Proper Documentation and Auditing**

Proper documentation and regular auditing are essential for demonstrating FMC’s compliance with FISMA and other regulatory requirements. Comprehensive documentation provides a clear record of FMC’s security practices, while auditing ensures that these practices are consistently applied and practical.

##### Implementation Steps:

* **Document All Security Procedures and Controls**: FMC must thoroughly document all security procedures, controls, and updates. This includes the detailed configuration of technical controls, access control policies, risk assessments, incident response procedures, and the SSP. Proper documentation is critical for maintaining transparency and accountability.
* **Regular Audits**: FMC should establish a schedule for regular internal and external audits of its security practices. Internal audits will help identify deviations from established procedures, while external audits will independently assess FMC’s compliance with regulatory requirements. These audits should assess the effectiveness of implemented controls, the accuracy of documentation, and the organization’s adherence to the SSP.
* **Audit Readiness**: FMC should maintain a state of audit readiness by ensuring that all security measures are up-to-date, documentation is complete and accurate, and any identified issues are promptly addressed. Preparing for an audit time ensures compliance and reinforces FMC’s commitment to maintaining a solid security posture.

##### **Integration into the Cybersecurity Strategy**

Updating the SSP, implementing comprehensive training programs, and ensuring proper documentation and auditing are crucial components of FMC’s governance and compliance efforts. These measures ensure that FMC’s cybersecurity strategy is effective, sustainable, and compliant with FISMA and other relevant regulations. By embedding these governance and compliance practices into its overall security framework, FMC can demonstrate its commitment to protecting sensitive information, maintaining continuous compliance, and mitigating the risk of regulatory penalties or security breaches.

**Conclusion**

### Summary of the Cybersecurity Strategy

In response to the critical security deficiencies identified in the assessment report, Fielder Medical Center (FMC) will implement a comprehensive cybersecurity strategy to enhance its security posture, protect sensitive information, and ensure compliance with the Federal Information Security Management Act (FISMA). This strategy strengthens technical controls, updates policies and procedures, and reinforces governance and compliance efforts.

To address the technical aspects, FMC will implement Multifactor Authentication (MFA) across all systems, ensuring that only authorized individuals can access sensitive information. This will significantly reduce the risk of unauthorized access. Additionally, FMC will deploy Extended Detection and Response (XDR) to enhance its ability to detect, investigate, and respond to security threats across its IT environment. Network security will be bolstered through firewall upgrades, network segmentation, and establishing secure remote access protocols, protecting the organization against external threats.

FMC will enforce the principle of least privilege on the policy and procedural front by implementing role-based access control and conducting regular access reviews. Continuous monitoring will be developed to maintain real-time awareness of the security posture, enabling swift responses to emerging threats. Regular risk assessments will be conducted, and a formal risk response plan will be established to mitigate identified vulnerabilities and manage security incidents effectively.

Regarding governance and compliance, FMC will review and update its System Security Plan (SSP) to align with current operational realities and incorporate the new security controls. Regular updates to the SSP will be scheduled to ensure ongoing compliance with FISMA. Comprehensive security awareness and specialized training programs will be implemented to equip all employees with the knowledge and skills needed to recognize and respond to security threats. Proper documentation of all security procedures and controls will be maintained, and regular internal and external audits will be conducted to verify compliance and effectiveness.

### Looking Ahead: Future Considerations

As FMC continues to evolve and expand its operations, it will be essential to maintain a proactive approach to cybersecurity. This includes staying informed about emerging threats, regularly reviewing and updating security controls, and adapting to changes in regulatory requirements. FMC should also consider investing in advanced security technologies, such as artificial intelligence (AI) and machine learning (ML), to enhance its threat detection and response capabilities further. Additionally, as the organization grows, expanding the cybersecurity team and fostering a culture of security awareness will be crucial for sustaining a solid security posture.

### Final Reflections

Implementing this comprehensive cybersecurity strategy marks a significant step forward in FMC’s commitment to protecting the sensitive information of its medical staff and maintaining compliance with federal regulations. By addressing the identified security deficiencies and adopting a proactive approach to risk management, FMC is safeguarding its operations and reinforcing its reputation as a trusted healthcare provider. Moving forward, FMC must continue to prioritize cybersecurity as a core aspect of its organizational strategy, ensuring that it remains resilient in the face of evolving threats and maintains the trust of its stakeholders.

## References

Center for Internet Security. (2020). CIS Critical Security Controls. Retrieved from https://learn.cisecurity.org/CIS-Controls-v7.1

IBM Security. (2021). *Cost of a Data Breach Report 2021*. Retrieved from IBM: https://www.ibm.com/security/data-breach

National Institute of Standards and Technology. (2020). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. doi:10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations. doi:10.6028/NIST.SP.800-53r5

PCI Security Standards Council. (2022). Payment card industry data security standard: Requirements and security assessment procedures. (Version 3.2.1). Retrieved from https://www.pcisecuritystandards.org/document\_library

United States Congress. (2002). *E-Government Act of 2002, Public Law 107-347.* Retrieved from https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf