Governance, Risk, and Compliance - D486

Skerdilaid Hoti

College of Information Technology, Western Governors University

February 2, 2024

Governance, Risk, and Compliance - D486

A.

The security assessment report (SAR) highlights some critical security gaps present in the company's framework. With these gaps present significant risks such as patient data security breaches, compliance issues, and other disruptions to FMCs operations can occur. Addressing these vulnerabilities is essential to mitigate these threats. These gaps currently include lack of security controls and policies, outdated system design, outdated security and privacy plans, and absence of MFA. Depicted in the document is the first issue including access control policies and procedures, account management, least privilege, and security attributesThe first issue is the lack of security controls and policies can lead to unauthorized access, data breaches, insider threats. This can easily lead to exposure of sensitive patient data, compliance violations such as HIPAA, FISMA, and PCI DSS which would lead to regulatory fines, and reputational damage.The next issue is an outdated system design. The outdated system design may include security vulnerabilities and will not meet compliance requirements. Outdated systems can also cause patching issues making them much more vulnerable to malware and intrusion. Another gap in the security framework is outdated security and privacy plans. These outdated plans will likely not be able to correctly address modern and evolving security threats, organization needs. The last gap summarized would be the lack of MFA. MFA is very essential in protecting an organization from unauthorized access. The current system relies solely on passwords making it very vulnerable to various attacks such as phishing, brute force attacks, and credential theft.

B.

Based on the SAR report five critical controls have been identified each with varying levels of risk. By aligning with compliance standards and industry guidelines FMC seeks to enhance its security measures, mitigate potential vulnerabilities, and safeguard sensitive patient data against cyber threats. The first identified risk was least privilege not being enabled. Least privilege ensures that employees and management only have enough access to fulfill their roles and nothing more. As described "Least privilege is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. The principle of least privilege helps protect against insider threats and unauthorized access." (CIS Controls). This is essential in preventing users from having excessive access, reduces the chance of unauthorized access, data breaches, and insider threats. The risk associated with this would be considered high due to a constant risk associated with this vulnerability and also the potential damage it can cause. By remedying this control, FMC ensures that employees and management only have access to the resources necessary to fulfill their roles, reducing the risk of data breaches and insider threats.

The second control was the plans of action and milestones. For this the risk can be considered moderate because while there is no direct threat having a lack of plans one can easily arise and the organization will be equipped to handle it. It can cause the company to struggle with prioritizing security weaknesses and lead to prolonged exposure to vulnerabilities and remediation. By implementing clear plans of action and milestones, FMC can address security

weaknesses promptly, minimize exposure to vulnerabilities, and enhance its overall security posture.

The third control is continuous monitoring. Once again the risk associated can be considered moderate. While not a direct threat to the organization the lack of continuous monitoring will eventually cause a failure to detect and respond to present security incidents prolonging their impact and increasing the risk of critical damage to the organization's data or reputation. By implementing robust continuous monitoring practices, FMC can enhance its ability to detect and respond to security threats promptly, minimizing the potential impact on patient data security and regulatory compliance.

The fourth control is the risk assessment and for this the risk is high. Without a risk assessment FMC can not accurately identify and mitigate risks. It will also impede the process when a breach or attack occurs due to the organization having to waste time finding which systems to work on first and miss out on efficiency that a risk assessment can provide. By conducting regular risk assessments, FMC can proactively identify and address security risks, ensuring compliance with regulatory requirements and safeguarding sensitive patient data effectively.

The fifth control is risk response which would also be considered a high risk. Without documented risk response strategy or an incident response team and plan FMC will struggle to effectively address identified risks. This can lead to delays and prevent mitigation from achieving its goal. By developing and documenting a comprehensive risk response strategy, FMC can enhance its incident response capabilities, minimize the impact of security incidents, and maintain regulatory compliance. "Risk assessments help organizations identify, evaluate, and

prioritize risks to their information assets, allowing for informed decision-making and resource allocation." (ISO/IEC 27005:2018,).

.

C.

Based on the SAR report FMC faces significant security risks. If left unattended these risks could compromise the companies confidentiality, integrity, and availability of patient data and undermine FMCs compliance with regulatory requirements. To mitigate these risks FMC must implement proper remediation strategies for each control area.

For the first control least privilege a strong remediation to this would be the usage of RBAC controls. RBAC controls can provide least privilege by assigning each specific group or individual specific access to only resources required for their job. As described by NIST "RBAC is considered a best practice for managing user permissions and access to sensitive resources. By assigning roles to users based on their responsibilities, organizations can enforce the principle of least privilege, reducing the risk of unauthorized access and potential data breaches" (NIST 800-53). Also it is important to regularly audit and update the access rights to ensure each user only has access to what they are supposed to have and ensure no unauthorized users are present.

The next control would be plans of action and milestones. For this control FMC should develop detailed plans of actions to include actions and milestones that prioritize and address security vulnerabilities identified during risk assessments or security assessments. "The development of a detailed plan of action is critical for organizations to effectively address security vulnerabilities

and weaknesses. This plan should outline specific steps, responsible parties, and timelines for remediation efforts." (NIST 800-37)

The third control was the risk assessment continuous monitoring. For this the best way to remediate would be to include automation technologies at least for the technical part of operations. Tools like SIEM, IDS, IPS, and EDR solutions can provide the necessary automation to help monitor the network and devices continuously. They can also help with ensuring data safety and adherence to compliance. While automation is important it is also essential for the company to conduct manual regular testing and review of systems and logs to ensure they are effective and identify if needed what could be improved on.

For the fourth control or the risk assessment remediation will be for the company to conduct an updated risk assessment. As part of the assessment FMC should identify risks, perform analysis on the risks identified, then mitigation, documentation and reporting, and finally conduct regular reviews and audits. Specific guidelines FMC can use would be NISTs 800-30 guidelines “The National Institute of Standards and Technology (NIST) provides comprehensive guidelines on risk assessment and management. According to NIST SP 800-30 Revision 1, "Risk assessments are foundational for an organization's information security program and are essential for developing an organization-wide risk management process. (NIST 800-30)" It is also that they follow HIPAA and PCI DSS compliance as they conduct the risk assessment.

The last control is the risk response and to remediate this issue FMC will develop and implement a comprehensive risk strategy. First they must define each risk into categories in order to understand what should be remediated first. Such categories include risk acceptance, risk avoidance and mitigation. The first thing the company should implement is an incident response

plan, and a business continuity plan. These two plans will aid and provide guidance to responding to risks. The incident response plan should include an outline for procedures for responding to security incidents, including roles and responsibilities of individuals, communication policy, and escalation procedures.

D.

To ensure compliance and maintain PCI DSS standards FMC will need to develop a PCI-DSS compliant policy. For this policy to be effective it will need to address three concerns explained in section 3.2.4 of the security assessment report. The first issue presented was the inadequate endpoint protection. To adhere to guidelines FMC must ensure that all workstations connected to the network include proper antivirus protection. This includes that all workstations have licensed and active antivirus. Endpoint protection is essential to protecting against malware and other potential threats that could compromise data. The second concern involves implementing MFA. FMC needs to implement MFA on its network to provide another player of protection. An example of an MFA solution would be to use a password and username but also include a SSO. The third control was lack of security controls for the POS system. In order to implement a POS system it requires specific security measures to ensure it is PCI DSS compliant. This would include implementing a secure and maintained network, configuring a firewall, removing vendor specific defaults and including antivirus.

PCI DSS-Compliant Policy

The scope of this policy applies to all employees, contractors, and third-party service providers involved in the processing, storage, or transmission of payment card data involving FMC. The goal of this policy is to ensure FMC is committed to maintaining compliance with PCI DSS standards ensuring the security of payment card data and protecting against data breaches and fraud.

To adhere to this standard roles and responsibilities must be assigned. A PCI compliance officer will be selected who is responsible for overseeing FMCs PCI DSS compliance efforts. The company's ISO or information security officer will be responsible for implementing and maintaining security controls for all processes related to this. System administrators will be responsible for configuring and maintaining systems and applications in adherence to PCI DSS requirements including endpoint protection and firewall settings. Network administrator will be responsible for configuring and maintaining network infrastructure such as securing transmission of payment data and implementing MFA.

The first requirement will be for network administrators to install and maintain a firewall while ensuring proper firewall controls, network segmentation, and removal of vendor supplied defaults. The system administrators will be assigned with implementing stronger control measures including implementation of least privilege, proper authentication, and MFA for all network access. The next requirement involves the system administrators and the ISO in which they will ensure proper encryption methods are being used while the data is at rest and moving.

Proper key management also falls in this category. The last requirement falls under the PCI compliance officer and the iso who will develop and maintain a proper incident response plan. The plan should address all potential security incidents involving payment card cards and include procedures for reporting incidents, escalation, investigating breaches, and notifying relevant stakeholders. The PCI compliance officer will also be in charge of auditing and assessments to monitor compliance. This will include documentation and reports. The compliance officer will also be in charge of maintaining and updating the policy based on changes in technology, regulations or business needs.

References

Your Response Here.

LR's posted in your Learning Resources Tab in the Course of Study – Course Material Section:

Chapple, M., & Seidl, M. (2023). (ISC)2 *CCSP certified cloud security professional official study guide.* Sybex. (3rd ed.) https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud*. (2nd Edition). Springer. https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi(/6/4!/4/2[epubmain]/2[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18]/2/2/1:0)

Estrin, E. (2022). *Cloud security handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site

National Institute of Standards and Technology. (n.d.). NIST *cybersecurity framework (CSF)*. https://www.nist.gov/cyberframework