**Governance, Risk, and Compliance**

Western Governors University

February 2, 2025

**A.  RISK ANALYSIS**

There are currently gaps which exist in the current companies’ security framework which were noted in the Security Assessment report. By highlighting these we can create awareness for the company regarding existing vulnerabilities. This will allow them to take proper action to mitigate risk. The objective is to protect sensitive information, adjust to current times with more modern technology, and help the company to avoid fines for lack of compliance.

The client is currently lacking security controls and policies. They are missing access control policies and procedures. There is no account enforcement or principle of least privilege. In addition, the security controls need to be more clearly defined. The current systems are outdated and lack posture. The system security plan is aligned with compliance laws and is currently outdated. They have not had a risk assessment to assess the current landscape. The client does not have a continuous security monitoring strategy in place. They have weak authentication and access management. MFA has not been set up in the current environment for account or network access. Doctors are uploading PII in an outdated insecure method. Authorized government agencies require secure access to the web portal, but the current authentication method does allow secure access in this environment. Workstations lack proper anti-virus software. This is important to detect, prevent, and remove possible malware. The firewall is also outdated, creating a major security vulnerability. This could allow malicious actors to bypass and gain access to the current network. Plans of action and milestones are missing. This can inhibit effective remediation (CMS Information Security Privacy Group, 2024). The client is planning to establish a POS system at their physical location. The current state of the network infrastructure would prevent the client from being PCI DSS compliant if a POS system was installed. They need to create more security measures: firewalls, segmentation, and authentication.

**B1. CONTROL RISKS**

There were five controls mentioned in Section 3.3 of the SAR which can help to mitigate risk. AC-6, which is related to the principle of lease privilege I give a risk rating of high. Without this control the risk of unauthorized access is increased. This increases the risk of insider threat as disgruntled employees may have access to files that they shouldn’t, allowing a larger attack surface. In addition, if an account is compromised this can lead to easy privilege escalation (CSF Tools, 2025). Lack of least privilege can directly impact confidentiality and integrity of the systems, including the systems containing PII and healthcare data.

The client lacks CA-5, Plans of Actions and Milestones. I rank this risk as moderate as not have a plans in place can lead to delays when vulnerabilities are detected. In order to comply with FISMA it is important that the client has a plan of action in place. This will help with remediation. (CMS CyberGeek, 2025).

Without a continuous monitoring strategy set in place, CA-7, the client is risking having breaches undetected. It is easier to minimize damage if a threat is detected early on. Because of this I rank this risk rating as high. This control is essential for integrity and availability in federally regulated environments. Real time oversight is required to meet Fisma and NIST 800 53 Standards. (NIST, 2025).

The client has not recently conducted a risk assessment RA-3. This risk is ranked as high as it can impact confidentiality, integrity, and availability. Without this control their ability to identify and prioritize risks is limited.

The client does not have a structured approach to risk response RA-7. This is like plans of action. I would rank this risk as moderate. There should be a method in place for mitigating, accepting, or transferring risk.

**B2.  RESPONSE JUSTIFICATIONS**

Accepting the risk associated with the five recommendations for controls could result in fines, legal action, and reputational damage. This would result from a lack of compliance with FISMA, PCI DSS, and HIPAA.

Least privilege is very important when it comes to restricting user access. The HIPAA security rule requires role-based access when dealing with electronic protected health information (US Department of HHS, 2021).

The client must implement Plans of Action and Milestones to remain FISMA compliant, avoid failures in security audits, and assist with risk mitigation (CMS, CyberGeek2025). In addition, NIST 800 37 mentions that remediation tracking is required to mitigate identified threats (NIST, 2025).

Continuous monitoring will enable threat time detection and incident response. This risk cannot be accepted as PCI DSS requires real time logging and security monitoring (UCSF controller’s office, 2023). The lack of this control would increase the likelihood of undetected breaches. This could result in the compromise of highly sensitive information.

Risk Assessment RA-3 must be conducted to comply with federal (FISMA) and industry regulations (CMS Information and Security Group, 2024). Failure to conduct risk assessments could result in penalties for non-compliance. According to NIST 800 30 Risk assessments are crucial in reducing threat impact. HIPAA also requires regular assessment (US Department of HHS, 2024.

It is important that the company creates a response plan. This will ensure that they have a system in which they accept, transfer, or mitigate risk. The client cannot accept unmanaged risk as this can result in breach of data. It is important the client determines their risk appetite and act accordingly. Because they are federally funded and deal with PHI there is very little room as to what is acceptable for data exposure. They need to take preventative measures to ensure that this data is secure and protected. Otherwise, they will be subject to fines from FISMA and HIPAA (CMS Information and Security Privacy Group 2025).

**C.  RISK REMEDIATION**

Now that we have discussed the risks associated with the controls and the justifications for not accepting the risk, we will discuss how the client can begin to enact proper remediations.

Currently unauthorized users can access sensitive data. This can increase the likelihood of a breach and fines from regulatory noncompliance. To create this the company will use Identity access management and Active Directory. This will allow us to define users and create Role Based Access Control. In addition, to make it more difficult for malicious actors to compromise accounts we will enforce Multi Factor Authentication. In addition, we will audit to ensure there are no weak configurations.

The company needs to have plans of action and milestones. To achieve this, we will recommend a reference for the NIST Risk Management Framework. In addition, we can use software which can keep track. The company can also create a designated security compliance team. They can assign ownership, schedule regular reviews, and integrate risk remediation into their current plan.

To detect real-time threats continuous monitoring will be set up. For this it is recommended the company utilize software & systems such as: Security Information and Event Management, Endpoint Detection and Response, and Vulnerability Management Systems. They can use tools such as: Splunk, CrowdStrike, and Nessus, to accomplish these goals.

In order to properly reduce threats, the company will need to conduct Risk Assessment. To accomplish this, they will utilize a risk assessment framework such as: NIST 800 30 or ISO 27005. They can use automated tools and potentially create a team that is dedicated to assessing risk. They should perform a full risk assessment and begin classifying and prioritizing risks utilizing FIPS 199 risk categorization. They should also schedule risk assessments.

Placing a risk response plan will allow the client to formalize an incident response plan. This will help them to become more organized and assess their risk appetite. They can utilize a risk management framework from NIST or ISO in order to help them accomplish this goal. They should be very clear about the goals and align with FISMA, HIPAA, and PCI DSS.

**D.  PCI DSS POLICY**

Since the client has decided to install POS systems on site it is important that they remain compliant with PCI DSS. In order to achieve compliance, we will establish a policy. The policy will enforce three requirements: Firewall Implementation and Maintenance, Elimination of Vendor-Supplied Defaults, and Deployment of Antivirus Solutions.

It is important setup and maintain a firewall to protect cardholder data from unauthorized access. We will deploy a PCI-DSS compliant firewall and segment the POS network from other networks. The firewall should be configured so only necessary traffic can go to and from the systems. The firewall logs should be maintained and reviewed. The IT security team will be responsible for configuring and managing the firewalls. The compliance officer will ensure that the settings comply with PCI DSS.

We will change all default passwords and security settings in the POS devices. All of the default usernames, passwords, and SNMP settings will be reset before the systems go into production. We will implement strong password policies. We will regularly audit the system accounts to ensure compliance. System Administrators will update and manage the configurations. The IT security team will conduct regular audits. The compliance officer will maintain documentation.

A secure Antivirus solution will be deployed and maintained. This will protect the POS system from malware and cyber threats. PCI DSS approved software will be deployed on all of the devices. Logging and alerting will be enabled. In addition, the logs will be reviewed quarterly. The IT Security Team will deploy and manage the software. System Administrators will monitor alerts and take remediation actions. The compliance officer will ensure that the software complies with PCI DSS and receives regular updates. (UCSF Controllers Office, 2024)

Internal Audits will be conducted every three months to ensure compliance with the created policy. Any incident or noncompliance issue should be reported immediately. Employees working with the devices are required to attend annual training and awareness.

**E.  SOURCES**

CMS Information and Security Privacy Group. (2024). Federal Information Security

Modernization Act. https://security.cms.gov/learn/federal-information-

security-modernization-act-fisma

UCSF Controllers Office. (2023). Understanding PCI DSS.

https://controller.ucsf.edu/how-to-guides/accounting-reporting/understanding-payment- card-industry-data-security-standard-pci

CSF Tools. (2025). AC-6 Least Privilege

<https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-6/>

CMS CyberGeek. 2025. Plan of Action and Milestones

https://security.cms.gov/learn/plan-action-and-milestones-poam

National Institute of Standards and Technology. 2025 Security and Privacy

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

US Department of HHS. 2021 Controlling Access to ePHI

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

National Institute of Standards and Technology. 2025 RMF Information Systems and Org

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

US Department of HHS. 2024. Summary of the HIPAA Security Rule

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html