1. **Use the PCI DSS documentation to answer the following questions:**
   1. **Using the diagram on page 5, list the numbers and corresponding descriptions for all of the items that your company will need to address.**
2. Install and maintain firewall configuration to protect cardholder data
3. Do not use vendor-supplied defaults for system passwords and other security parameters
4. Protect stored cardholder data
5. Encrypt transmission of cardholder data across open, public networks
6. Protect all systems against malware and regularly update anti-virus software or programs
7. Develop and maintain secure systems and applications
8. Restrict access to cardholder data by business need to know
9. Identify and authenticate access to system components
10. Restrict physical access to cardholder data
11. Track and monitor all access to network resources and cardholder data
12. Regularly test security systems and processes
    1. **Select three items from question 1a, and describe why they should be addressed.**
13. Install and maintain firewall configuration to protect cardholder data
    1. Since the IT consultant tested positive for COVID the firewall configuration was never set up. It is mandatory with PCI DSS standards for a storefront to process, store, or transmit credit card information. Without a firewall, we may also have data breaches that put our patient's medical records at risk. There are major consequences if we do not set up a firewall.
14. Protect all systems against malware and regularly update anti-virus software or programs
    1. Since the IT consultant tested positive for COVID he never installed or tested the antivirus. With the lack of antivirus, we are leaving vulnerable to malware. With this vulnerability, we leave sensitive information at risk. This would also leave us out of compliance with PCI DSS and HIPAA making it extremely important to have as we do not want to get fined.
15. Encrypt transmission of cardholder data across open, public networks
    1. As we are only installing servers in one of our locations are using VPNs to transfer data. We need to make sure this data is encrypted. To comply with PCI DSS and protect our customer's personal information. This will help us build a trusting relationship with the patient.
    2. **For each of the items, you selected from 1b, document one PCI DSS Requirement that best matches your company's security gap. See the PCI DSS Requirements column starting on page 20.**

Requirement 1: Install and maintain firewall configuration to protect cardholder data

1.1 Establish and implement firewall and router configuration standards that include the following

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)

Requirement 4: Encrypt transmission of cardholder data across open, public networks

4.1 Use only strong cryptographic and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following.

* The Internet
* Wireless technologies including 802.11 & Bluetooth
* Cellular technologies
* General Packet Radio Service (GPRS)
* Satellite communications

* 1. **For each of the items you selected from 1c, document the best Testing Procedure for your company's situation, using the Testing Procedures column in the chart starting on page 20.**

1.1 Establish and implement firewall and router configuration standards that l include the following

* Examine documented procedures to verify there a formal processes for testing and approval of all network connections and changes to firewall and router configurations
* Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data.
* Examine the data-flow diagram and ensure it shows all cardholder data flows across systems and networks and is kept current and updated as needed upon changes to the environment.
* Verify that the current network diagram is consistent with the firewall configuration standards
* Verify the firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)

* Verify that all operating system types that commonly get affected by malware have anti-virus software deployed on them.
* Review vendor documentation and examine anti-virus configurations
* Examine policies and procedures to verify that anti-virus software and definitions required to be kept up to date
* Verify anti-virus cannot be disabled or altered by users.

4.1 Use only strong cryptographic and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following.

* Identify all locations where cardholder data is transmitted or received over open, public networks. Verify the use of security protocols and strong cryptography for all locations
* Observe a sample of inbound & outbound transmissions to verify the cardholder data is encrypted
* Verify that only trusted keys and/or certificates are accepted
* Ensure the protocol is implemented to use only secure configurations and does not support insecure versions or configurations
* Examine system configuration to verify that the proper encryption strength is implemented for the encryption methodology in use.
  1. **For each of the items you selected from 1c, describe a security control (policy, procedure, hardware, or software) that could be used to resolve the initial issue, and describe how it will help.**

Requirement 1: Install and maintain firewall configuration to protect cardholder data

* Hardware Firewall Implementation and Configuration Management Procedure

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

* Anti-malware software with Automatic Updates and schedule scans

Requirement 4: Encrypt transmission of cardholder data across open, public networks

* End-to-end encryption Solutions and VPN for remote connections
  1. **For each of the items in 1c, research and describe an ideal monitoring technique or tool your company could use to validate that the control is in place.**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

* Next-Generation Firewall with Integrated management Dashboard
  + Palo Alto
  + Cisco

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

* Endpoint Protection Software
  + Crowdstrike
  + SentinelOne

Requirement 4: Encrypt transmission of cardholder data across open, public networks

End-to-end encryption Solutions and VPN for remote connections

* SSL/TLS encryption verification tools & VPN Monitoring Software
  + Manage Engine VPN Monitoring Tool

1. **Use the first non-PCI compliance you identified in question 1 of Week 1's assignment. List four steps you would take to prepare for the audit and why each step is critical.**

* Inventory of Payment Systems:
  + Understanding what payment systems we have so we understand the scope of what we are dealing with.
* Gap Analysis
  + Understanding where we fall short of meeting PCI DSS requirements is critical in understanding what steps we need to take to move forward.
* Replace Non-Compliant Card Machines
  + After we research and understand the best card machines that are compliant with PCI DSS we will replace the old ones.
* Implement Policies and Training:
  + We need to develop policies on how the card information will be handled. We will then have to train staff on these policies
    - Payment card processing policy
    - Access Control Policy
    - Data encryption policy
    - Incident Response Policy
  1. List three security controls that should be implemented (if time and finances are available) by your company before the audit, and describe why you need them.
* Encryption of Transaction Data
  + This is needed since it will ensure that cardholder data is unreadable to unauthorized parties.
* Access Control Measures
  + Not everyone needs to see cardholder data. This will ensure only those who need to see it will be able to.
* Regular Software Updates and Patch Management
  + This is needed to ensure our systems are all up to date, especially payment processing devices.
  1. For the three items you selected in 2. a, describe an ideal monitoring technique or tool your company could use to validate that the control is in place and is meeting policies.
* Encryption of Transaction Data
  + Software to ensure keys are secured
    - Azure Key Vault
    - AWS KMS
    - Google Cloud KMS
* Access Control Measures
  + IAM Systems that provides logging
    - Okta
    - Microsoft EntraID
* Patch management software
  + Tools to ensure systems are up to date
    - ManageEngine Patch Manager Plus