**Case Study: ISeeU Eyecare**

**1. Compliance Needs**

**What are all of the specific compliances your company needs to meet?**

* **HIPAA Compliance**: Protects patient information such as medical records, insurance details, and examination images.
* **PCI DSS Compliance**: Ensures secure handling of credit card transactions.

**Why does your company need to meet these compliances?**

* HIPAA is mandatory due to the sensitive nature of patient data.
* PCI DSS compliance is necessary to securely process and store credit card information, ensuring customer trust and financial security.

**List the compliance organizations you need to work with.**

* **HIPAA**: Partners like CVS or other pharmacies must also meet HIPAA standards for shared patient data.
* **PCI DSS**: Vendors processing payments need to align with PCI DSS requirements to ensure safe transactions.

**2. Credit Card Issues and PCI DSS**

**What credit card issues prevent compliance with PCI DSS?**

* The company’s current credit card systems are non-compliant, posing a significant barrier to PCI DSS adherence.

**Concerns related to questionable credit card items:**

* Logs of product purchases, returns, exchanges, and warranties are necessary for inventory management but must be secured under PCI DSS standards.

**3. Technology Issues**

**Identify three technology gaps to address immediately:**

1. Non-compliant credit card systems.
2. Insufficient IAM (Identity and Access Management).
3. Lack of HIPAA compliance measures.

**Proposed fixes:**

* **PCI DSS Compliance**:
  + Determine PCI level and complete a self-assessment questionnaire (SAQ).
  + Replace outdated systems with PCI-certified credit card machines.
* **IAM**:
  + Implement tools like Splunk or ManageEngine for auditing and monitoring.
  + Establish Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA).
* **HIPAA Compliance**:
  + Train employees on privacy procedures and implement monitoring systems.
  + Develop privacy policies and ensure oversight by a dedicated compliance officer.

**4. Compliance Audit Preparation**

**Four items to prepare for an auditor:**

1. Documentation of policies and procedures.
2. Audit trails and logs.
3. Evidence and examples of compliance.
4. Reports on vendor compliance.

**5. NIST 800-53 Framework**

**Three areas to implement:**

1. **Access Control**: Lockdown sensitive patient data using IAM systems.
2. **Incident Response**: Develop and test a comprehensive response plan.
3. **Information Protection**: Encrypt sensitive information and create regular backups.

**Framework solutions for company issues:**

* **IAM Implementation**:
  + Introduce tools for active directory monitoring and user management.
* **Incident Response**:
  + Formulate a recovery plan and simulate scenarios to ensure readiness.
* **Data Encryption**:
  + Adopt secure cryptographic protocols to protect data-at-rest and data-in-transit.

**6. PCI DSS Detailed Documentation**

**1. PCI DSS Requirements**

**List of requirements to address:**

1. Install and maintain firewall configurations.
2. Protect all systems against malware and regularly update antivirus programs.
3. Encrypt transmission of cardholder data across public networks.

**Selected Testing Procedures:**

* **Firewalls**: Examine diagrams and verify firewall configurations.
* **Antivirus**: Ensure systems have updated antivirus programs.
* **Encryption**: Validate the use of strong cryptography for all transmissions.

**Ideal Monitoring Tools:**

* Firewalls: Palo Alto, Cisco firewalls.
* Antivirus: Endpoint protection tools like CrowdStrike.
* Encryption: VPN monitoring software and SSL/TLS verification tools.

**7. NIST Privacy Framework Implementation**

**Functions and Benefits**

1. **Identify-P**: Inventory and map data processing activities.
2. **Govern-P**: Establish privacy policies for consistent practice.
3. **Control-P**: Manage data with specific policies to secure patient records.
4. **Communicate-P**: Build transparency and trust through clear communication.
5. **Protect-P**: Implement robust access controls and encryption to safeguard sensitive data.

**Selected Categories and Subcategories**

* **Governance Policies**: Develop privacy training programs for employees.
* **Identity Management**: Deploy Role-Based Access Control (RBAC) systems.
* **Data Security**: Use encryption to protect sensitive data.

**8. IT Domain Analysis**

**Domains Used by ISeeU Eyecare**

1. **User Domain**: Access control and user training.
2. **Workstation Domain**: Secure desktops and laptops.
3. **LAN Domain**: Facilitate secure internal data flow.
4. **LAN-to-WAN Domain**: Protect data shared externally.
5. **WAN Domain**: Enable secure connectivity between locations.
6. **Remote Access Domain**: Provide secure access for remote workers.
7. **System/Application Domain**: Manage sensitive data and transactions.

**Priority Domains**

* **System/Application Domain**: Critical for managing sensitive patient and financial data.
* **LAN-to-WAN Domain**: Essential for securing data in transit.

**Domains Deprioritized with Zero Trust**

* **LAN Domain**: Perimeter defenses become less critical as Zero Trust relies on identity-based controls.
* **Remote Access Domain**: Uniform access controls reduce reliance on traditional remote access systems.

**9. Digital Forensics Reporting**

**Ransomware Case**

1. **Incident Logs**: Identify the ransomware’s entry and timeline.
2. **Backup Files**: Assess damage and aid recovery.
3. **System Images**: Analyze the strain and scope of the ransomware.

**Data Breach Case**

1. **Access Logs**: Track unauthorized access attempts.
2. **Network Traffic Logs**: Detect unusual data flows.
3. **Data Inventory Documentation**: Identify compromised data and guide mitigation efforts.