Initek

Course Project Report

PCI DSS v4.0

Eric Somogyi

CSEC 533 – 11/12/2024

Table of Contents

Executive Summary:

Background and Scope

Initek, currently compliant with Sarbanes-Oxley (SOX) and HIPAA, faces a lack of knowledge in how to achieve compliance with PCI DSS v4.0, which is the Payment Card Industry Data Security Standard taking effect in 2024 worldwide. This is a report in response to the request by the CEO of Initek to provide the company with insight into what it would take to comply with PCI DSS v4.0. This report summarizes the definitions and differences of Sarbanes-Oxley, HIPAA, and PCI DSS v4. It explains why companies choose to be compliant with PCI standards. From the security analyst perspective, it identifies and ranks 4 cybersecurity domains that Initek will need to improve on while becoming PCI DSS v4.0 compliant. It reviews any updates/revisions to current policies, procedures, guidelines, and controls that Initek is confronting. Lastly, this report covers a high-level analysis of the steps and changes that are recommended to be completed by Initek in order to implement PCI DSS v4.0 successfully into the organization.

Call to action

Initek must make several changes within their organization. To lead to successful PCI DSS v4.0 compliance, below are the next steps we recommend to the CEO to take.

1. Conduct a meeting with the board and executive management to review this report in detail through a PowerPoint presentation so everyone can understand.
2. If Initek decides to move forward with the recommendations, move to the planning phase of the project management cycle.
3. Allocate labor hours to employees dictated by executive management to start the assessment phase for investing time in the changes and requirements explained in this report to achieve PSI DSS compliance. This “assess” phase’s goal is for Initek to identify specifically all technology and process vulnerabilities that pose risks to the security of customer cardholder data being transmitted or stored by Initek.
4. If Initek does not currently have the skilled labor to perform action item #3, allocate from the company budget to have a hiring event for new talent to perform these duties.
5. Initek has an option to sign up an employee to attend a PCI DSS training camp for one week to learn everything else in detail in order to ensure efficiency and understanding of all requirements in depth. This employee will be designated as the Team Lead.
6. Discover what the exact costs to order any new hardware, software, tools, or subscriptions/services that are found in the assessment phase that Initek will need to meet the needs of the new Security Architecture.
7. Discover if any, any bad practices that Initek has when *currently* storing and processing cardholder data.
8. Following a completed assessment phase of the PCI DSS cycle, move into the remediate phase to fix any vulnerabilities, technical flaws or any bad practices that were found to be true.
9. When ready, submit all documents to a PCI Qualified Security Assessor (QSA).

Background on PCI DSS v4.0, Sarbanes Oxley, and US HIPPA:

PCI DSS v4.0 stands for, “Payment Card Industry Data Security Standard version 4.0.” This payment standard was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. It provides a baseline of technical and operational requirements designed to protect data but also is used to protect against threats and security overall in the payment ecosystem. It involves three ongoing never-ending phases of assessing, remediating, and reporting to achieve maximum security objective of securing cardholder data.

Sarbanes Oxley, also known as SOX, is a US federal to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. This act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting.

HIPPA stands for, “Health Insurance Portability and Accountability Act” and is a federal law which is meant to protect the privacy of patient’s health information.

Sarbanes Oxley and HIPAA are both legislative controls in the United States while PCI DSS is a global payment industry standard for merchants and vendors.

HIPAA aims to ensure confidentiality, integrity, and availability of protected health information (PHI) of data stored and transferred electronically over the internet and is enforced by the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR). SOX is not aimed at protecting cardholder data but is enforced by the US Securities and Exchange Commission (SEC). PCI DSS is enforced by the Payment Card Industry Security Standards Council (PCI SSC) and payment card companies.

Why companies chose to be compliant with PCI DSS v4.0:

Any company globally that is involved in the processing, collecting, storing, or transfer of personal payment card account data online, in person or on data center servers including “system components” must be PCI DSS v4.0 compliant because it is the globally adopted standard for electronic payment security and is mandatory for all entities. It is the industry standard framework for protecting cardholder data in all environments, while protecting business reputation, and meeting the industry standard requirements by the payment processors for payment security. For any merchant or vendor (online or in person) to accept payment from an end-user from a American Express, Discover Financial Services, JCB International, Mastercard Worldwide, or Visa Inc, they must be compliant with PCI DSS v4.0 which means whichever hardware or software entity process the end users debit/credit card, that entity must be PCI DSSv4.0 compliant. In conclusion, all of these factors enable companies to maintain customer trust in conducting payment transactions.

What cybersecurity domains need to be enhanced?

There are 4 relevant cybersecurity domains that need to be enhanced for Initek to achieve PCI DSSv4.0 compliance. They are Information Security Governance, Security Architecture, Security Awareness Program, and Enterprise Risk Management.

Information Security Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, and verifying that the enterprises' resources are used responsibly.

Security Architecture is the strategic design of systems, policies, and technologies to protect IT and business assets from cyberthreats (Source - Palo Alto Networks). It aligns cybersecurity with the business goals and risk management profile of the organization.

Security Awareness and Program is the education process designed to equip employees, stakeholders, and end users with the knowledge and skills to identify, understand, and mitigate cybersecurity threats and protect information assets.

Enterprise Risk Management is a comprehensive approach and strategic process to identify and managing all the risks that the organization faces.

Ranking of the domains to be implemented and why?

Security architecture is the *most* important domain because what is defined in PCI DSS dictates requirements on how Initek's needs to develop their strategy to achieve key objectives in operations to reduce security breaches, improve operational efficiency and comply with industry regulations and standards in the electronic payment environment.

Information Security Governance is the second most important domain because proper governance involves adding and revising policies, procedures, and programs that shape how Initek will manage and protect its customers cardholder data (CD) and sensitive authentication data (SAD).

Enterprise Risk Management is the third most important domain because by the enterprise understanding *all* the threats that it faces, the vulnerabilities and its risk profile by prioritizing information security risk management, Initek will be able to mitigate risk involving their customer's data assets, while reducing the impact of loss in any incidents. If Initek decides to implement and valid PCI DSS through the *customized approach,* this domain aligns with some of PCI's recommendations to an organization-wide risk management approach to security.

Creating or Continuing a Security Awareness Program (SAP) is fourth because educating and training employees and customers about security is an ongoing process and humans are the highest risk to security. Through a Security Awareness Program, Initek will reduce risk, remain compliant, reduce costs, promote security, and train employees.

What Policies, Standards, Guidelines, & Controls would Initek need to implement?

There are several policies, standards, guidelines, and controls to be implemented or updated and revised. Policies that will need to be updated/revised are the Information Security Policy (ISP), a Data Retention Policy (DRP), an Acceptable Use Policy, a Content Security Policy (CSP), and the Information Security Management Policy.

Policies that will need to be added is the Password/Paraphrase Policy and Cardholder Data Environment Record Identity Policy (CDERIP) and the Security Awareness Program Policy.

Controls that will need to be implemented are Network Security Controls (NSC), a RACI matrix, a File Integrity Monitoring Tool (FIM), disk-level encryption, cryptographic data encryption software, a physical security access control for only authorized personnel.

Controls that will need to have configuration settings adjusted is the Identity and Access Management (IAM) system.

Controls that will need to be adjusted include firewall rules, and the Endpoint Detection and Response (EDR) tool configuration settings.

In addition, designing a Data Network Diagram and Data Flow Diagram is documentation that will need to be produced that supports the guidelines and standards.

The guidelines that will need to be updated is the Incident Response Plan (IRP) to meet the new requirements.

The standards that would need to be implemented per the PCI DSS v4.0 requirements is the NIST SP 800-57 Recommendation for Key Management standard.

If Initek would like to conduct business online or in Europe, ENISA would be a standard that Initek would need to follow.

Initek would need to follow. For online web application security and mobile application security, OWASP is a standard that Initek would want to consider as well.

Further note, all of these above-mentioned items are also identified in Section 5 in what Initek needs to do in order to implement PCI DSSv4.0 successfully.

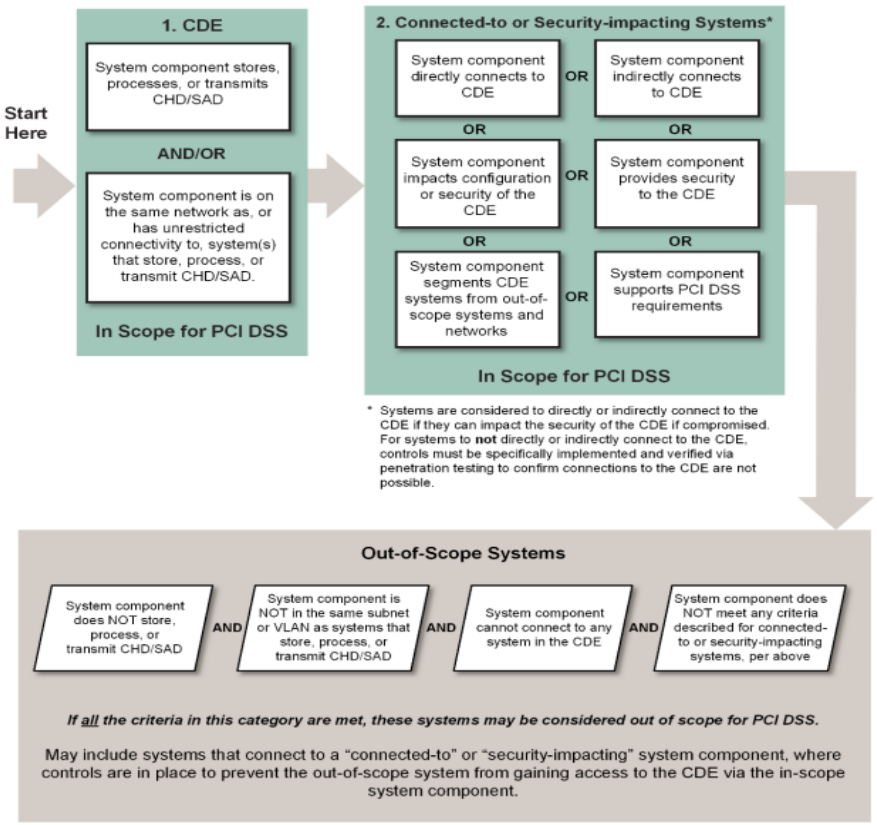
What is needed from Initek to make implementing PCI DSS v4.0 successful?

To go through the PCI DSS v4.0 assessment process, the PCI DSS assessment process includes the following high-level steps:

1. Confirm the scope of the PCI DSS assessment.
2. Perform the PCI DSS assessment of the environment.
3. Complete the applicable report for the assessment according to PCI DSS guidance and instructions
4. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Official Attestations of Compliance are only available on the PCI SSC website.
5. Submit the applicable PCI SSC documentation and the Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those that manage compliance programs such as payment brands and acquirers (for merchants), or other requesters (for service providers).
6. If required, perform remediation to address requirements that are not in place and provide an updated report.

Initek will also need to determine the scope of the environment identifying the cardholder data environment (CDE), which is system component stores, processor transmits of CHD or sensitive authentication data (SAD) or the system components in the same network or has unrestricted connective to systems that store, process, or transmit CHD/SAD. Any system connected to security impacting systems, components directly connections to, and system components impact configuration or security of CDE or system component segments CDE systems from out-of-scope systems and networks.

Figure 1. Understanding PCI DSS Scoping



Initek will use the defined approach, however Initek will have to set their control in place that meets PCI DSS requirements. Initek will schedule an interview with a PCI DSS Qualified Security Assessor (QSA). PCI states that the new PCI DSS security controls will need to be implemented in order ot complete the ROC. Initek will need to determine how many transactions per year they produce. If Initek produces over 6 million transactions per year, that is classified as Level 1 merchant (or 3rd party), then they will be required to produce a PCI DSS Report on Compliance (ROC). If Initek falls above 1 million transactions per year, then they will need to consult the acquiring bank to determine if they need to produce an ROC, otherwise only a Self-Assessment Questionnaire (SAQ) is required. If Initek is under 1 million transactions per year, that would make them a Level 3 or Level 4 merchant (or 3rd party), which only required Initek to produce an annual Self-Assessment Questionnaire (SAQ).

Initek will have to meet 12 PCI DSS requirements which are displayed in Table 1 below:

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

1. Building and Maintaining a Secure Network:

a. Install and Maintain Network Security Controls (NSC)

i. Resources: Personnel - network engineers/administrators. Maintain an up-to-date network diagram. Examine dataflow and network diagrams to verify system components storing cardholder data are not accessible from untrusted networks. After NSC rules are set, confirm network traffic connections are secure and only allowing necessary traffic from all ports.

ii. Software: Integrate Network Security Controls (NSCs) by integrating Firewalls, IDS/IPS, Network Monitoring Tools. These will be placed between environments with different security needs of levels of trust. These NSCs will be a key protection mechanism for our networks.

b. Apply Secure Configuration to All System Components

i. Resources: Personnel - System administrators and security engineers. Any security Policies and operational procedures are updated and known to all parties. Utilize the responsibility assignment matrix (RACI matrix) to ensure roles and responsibilities are documented and assigned. Keep up to date with industry guidance for any security configurations such as new or known CVE vulnerabilities or exploits in any relevant software or third-party platforms. Also refer to NIST, ENISA, and OWASP for guidance.

ii. Software: Use Vulnerability Scanners such as Nessus, Security Information and Event Management (SIEM) systems such as Splunk Enterprise.

2. Protect Stored Account Data:

a. Protect Stored Account Data

i. Resources: Personnel - security architects/administrators. Keep security policies and operational procedures updated. Design a formal Data Retention Policy (DRP). Refer to NIST SP 800-57 Part 1 for recommended Key Management.

ii. Software: Integrate cryptographic data encryption software to encrypt primary account numbers (PAN) that meet the Advanced Encryption Standard (AES) such as SolarWinds.

b. Protect Cardholder Data with strong Cryptography During Transmission over Open, Public Networks

i. Resources: Personnel - security analysts or IT administrators. As of March 31, 2025, confirming that certificates used to safeguard PAN during transmission over open, public networks and are not expired will be required. (PCI DSS Requirement 4.2)

ii. Software: Continue to Use SSL certificates on Initek website and encryption gateways such as Amazon API Gateway. Integrate disk-level encryption for all authentication factors and decryption keys.

3. Maintain a Vulnerability Management Program:

a. Protect all system and Networks from malicious Software

i. Resources: Personnel - security engineers. Refer to security policies and operational procedures.

ii. Software: Use antivirus software/anti-malware software, endpoint detection and response (EDR) tool such as CrowdStrike.

b. Develop and Maintain Secure Systems and Software

i. Resources: Personnel - Software developers

ii. Software: Use any Static or Dynamic Application Security Testing Software to test web application firewalls and applications.

4. **Implement Strong Access Control Measures:**
    a. **Restrict Access to System Components and Cardholder Data by Business need to Know**
    b. **Identify Users and Authenticate Access to System components**
    c. **Restrict Physical Access to Cardholder Data**
        i. Personnel - Retain/employ security administrators. Use the RACI matrix. Define an access control model that is designed to control access to system components. Design a password/paraphrase policy to meet the PCI DSS Requirement 8.3.6 requirement. Enable some physical access security control to only allow authorized personnel based on job function to sensitive areas where CDE is stored.
        ii. Software: Implement MFA solutions for customers online login before payment, integrate identity and access management (IAM) system to control and manage user authentication and access control to any database or application that has the customers' sensitive authentication data (SAD).
5. **Regularly Monitor and Test Networks**
    a. **Log and Monitor All Access to System components and cardholder data**
        i. Resources: Personnel - Security engineers and administrators. Ensure all audit logs meet the requirements of PCI DSS 10.2.1-10.4.1. In the Information Security Management Policy, confirm that all failures of critical security control systems are detected, report, and respond to promptly.
        ii. Software: Utilize SIEM systems and confirm the continued storing of logs.
    b. **Test Security of Systems and Networks Regularly**
        i. Resources: Personnel - Security engineers. Per PCI DSS Requirement 11.3.2 contract out a PCI DSS Approved Scanning Vendor (ASV) to retrieve an external vulnerability scanning report. This is required since Initek is going to be new to PCI DSS compliance. Contract out to a 3rd party Pen-testing firm regularly so security weaknesses are corrected. Use Security policies regularly. Implement a file integrity monitoring (FIM) tool per PCI DSS requirement 11.5.2. Implement a change and tamper detection mechanism such as a Content Security Policy (CSP) per PCI DSS requirement 11.6 to help assist in triggering reporting of changes in HTTP headers.
        ii. Software: Any required software is not required for investment as this is taken care of by the 3rd party Pen-test company.
6. **Maintain an Information Security Policy:**
    a. **Support Information with Organizational Policies and Programs.**
        i. Resources: Personnel - Information Security managers and 24/7 personnel to respond to suspected or confirmed security incidents per PCI DSS requirement 12.10.3. Revise Initek's Information Security Policy with all necessary updates as required in PCI DSS Requirements 12.1 – 12.1.3. Security Awareness Program that includes security awareness education, Acceptable Use Policies. Design a Cardholder Data Environment (CDE) Record Identity Policy (CDERIP) that documents risks identified, evaluated, and managed. Implement of PCI DSS Hardware/Software Technology Record

that documents all technologies vulnerabilities, knowns threats, and include end of life plans, if any, per PCI DSS requirement 12.3.4. Implement an Incident Response Plan (IRP) that is ready to be activated in the event of a confirmed security incident per PCI DSS requirement 12.10. Document PCI DSS Scope conforming to PCI DSS requirements of 12.5.2.

ii. Software: Optional - using a 3rd party security policy management software such as Tenable.io.

Initek is currently not a multi-tenant service provider, however with the new PCI DSS v4.0 requirements post March 2024, any multi-tenant service providers that are a third-party service provider that offers various shared service to merchants and other service providers, where customers share system resources (physical/virtual servers), infrastructure, applications, then there are additional requirements listed in Appendix A1 in the PCI DSSv4.0 standard pdf found here: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf .

If Initek is unable to meet the 12 PCI DSS requirements, then compensating controls may be used and implemented in place of the 12 PCI DSS requirements. Review specifics for compensating controls under Appendix B. If Initek decides to use compensating controls, then the compensating controls results must be documented in a Report on Compliance (ROC) or a Self-Assessment Questionnaire (SAQ). Initek will also need to complete the Compensating Controls Worksheet in Appendix C if they end up using compensating controls due to technological or business constraints to achieve compliance.

If Initek has any struggle with the Self-Assessment, PCI DSS provides contact information of the Qualified Security Assessors' (QSA) on the PCI website http://www.pcisecuritystandards.org/ where they provide training programs to help build awareness for anyone interested in becoming PCI DSS compliant.

Lastly, PCI DSS requires organizations to encrypt user card data with information stored in their databases and the encryption standard to be compliant with is the Advanced Encryptions Standard (AES).