Aric Allen
Fall 2025 BINS 4331

Final Term Project

Pete's Pizzeria processes numerous payment card transactions daily. As a merchant handling sensitive cardholder data, the organization must comply with Payment Card Industry Data Security Standard (PCI DSS) to protect customers, maintain trust, and avoid potential financial penalties. Due to the IT department having limited resources, our strategy is to prioritize four PCI DSS requirements from the six easiest to implement.

The 4 PCI DSS requirements we will be selecting are: Protect cardholder data with strong cryptography during transmission, restrict access to system components and cardholder data by business "need-to-know", restrict physical access to cardholder data, and protect all systems and networks from malicious software. These four are selected for their high compliance rates, impact on data protection, and feasibility within our current infrastructure.

Protect cardholder data with strong cryptography during transmission is selected because it provides the highest protection against data interception and is relatively easy to implement with current POS and network tools. Restrict access to system components and cardholder data by business "need-to-know" is selected because it limits internal threats by ensuring only authorized employees can access sensitive systems. Restrict physical access to cardholder data is selected because it is a simple and cost-effective measure to prevent unauthorized on-site data access. Protect all systems and networks from malicious software is selected because it is an essential defense to block malware that could compromise customer payment data.

For protecting cardholder data with strong cryptography during transmission, some processes/controls are: Establishing a data encryption process for all payment transmission and configuring an automatic rejection of insecure protocols on firewalls and routers. For restricting

access to system components and cardholder data by business “need-to-know”, some processes/controls are: Develop and maintain a role-based access control policy that limits user access to only the data required for their job and enabling multi-factor authentication for all users accessing systems that handle cardholder data.

For restricting physical access to cardholder data, some processes/controls are: Establishing a visitor management process that logs, identifies, and escorts all non-staff in sensitive areas and deploy CCTV monitoring to record and review access to sensitive data areas. For protecting all systems and networks from malicious software, some processes/controls are: Implementing an anti-malware management process that includes daily updates, scanning schedules, and quarantine procedures and also installing enterprise-grade antivirus/EDR software with automatic updates.

To implement the processes and controls for protecting cardholder data with strong cryptography during transmission, we will configure all point-of-sale (POS) systems and online ordering systems to transmit cardholder data using Transport Layer Security (TLS) 1.3. We will also update all routers and network firewalls to block insecure protocols (HTTP, FTP, Telnet, etc.) and force encrypted connections.

To implement the processes and controls for restricting access to system components and cardholder data by business “need-to-know”, we will develop a role based access control by defining access levels for key departments (e.g., cashiers, managers, kitchen staff, IT, finance). We will configure these user roles in the active directory or POS management system to ensure only authorized employees can access customer payment or order data. We will also implement Multi-Factor Authentication on systems used by management, accounting, and IT to access the payment environment and document these MFA logs for annual PCI DSS audits.

To implement restricting physical access to cardholder data, we will establish a visitor management system by installing keycard access locks on server and POS back-office areas and also create a visitor logbook at the main office entrance to track all non-staff entries (e.g., vendors, maintenance, etc.). We will also establish CCTV cameras to monitor all activity in the building especially in the sensitive data areas to ensure only authorized personnel are in those locations.

To protect all systems and networks from malicious software, we will implement an anti-malware and patch management process by deploying enterprise antivirus software (e.g., CrowdStrike, Bitdefender, or Windows Defender for Business) and also configuring automatic updates and daily malware scans. We will also develop a patch management schedule to install OS and application security updates every two weeks.

By executing these tactical actions, Pete's Pizza will establish a secure, compliant environment for processing cardholder data. The IT Department's approach will balance feasibility, cost-effectiveness, and risk reduction, ensuring that PCI DSS controls are both implemented and sustained through continuous monitoring and staff training. This plan will serve as the foundation for Pete's Pizza's long-term goal of achieving full PCI DSS v4.0 compliance, enhancing customer trust, and protecting the company's reputation.