Securing Small Business Payment Systems:

A Governance, Risk, and Compliance (GRC) Assessment and PCI DSS Compliance Roadmap

Dry Clean Super Center of Lafayette

Quentin Jackson

Cybersecurity/April Cohort

Institute of Data

October 11, 2025

Table of Contents

7. Proposed Roadmap to PCI DSS Compliance
    7.1 Plan of Action & Milestones
    7.2 Short Term (0-3 months)
    7.3 Mid Term (3-6 months)
    7.4 Long Term (6-12 months)
8. Implementation Plan and Cost Estimation
    8.1 Estimated Costs
    8.2 Return on Security Investment (ROSI)
9. Challenges, Risks, and Mitigation Strategies
    9.1 Common Small Business Constraints
    9.2 Potential Risks During Transition
    9.3 Mitigation Plans
10. Conclusions
11. Recommendations
12. References

1. Executive Summary

Dry Clean Super Center of Lafayette (DCSC) operates in a competitive market providing garment care services throughout the Lafayette area, including washing, dry cleaning, pressing, stain spotting, and specialty garment treatments, with a convenient drive through service. With increasing digital payments and concerns about data breaches, DCSC seeks to assess their current payment system's security posture and align with industry-accepted standards to protect both their customers and themselves from financial, reputational, and legal harm.

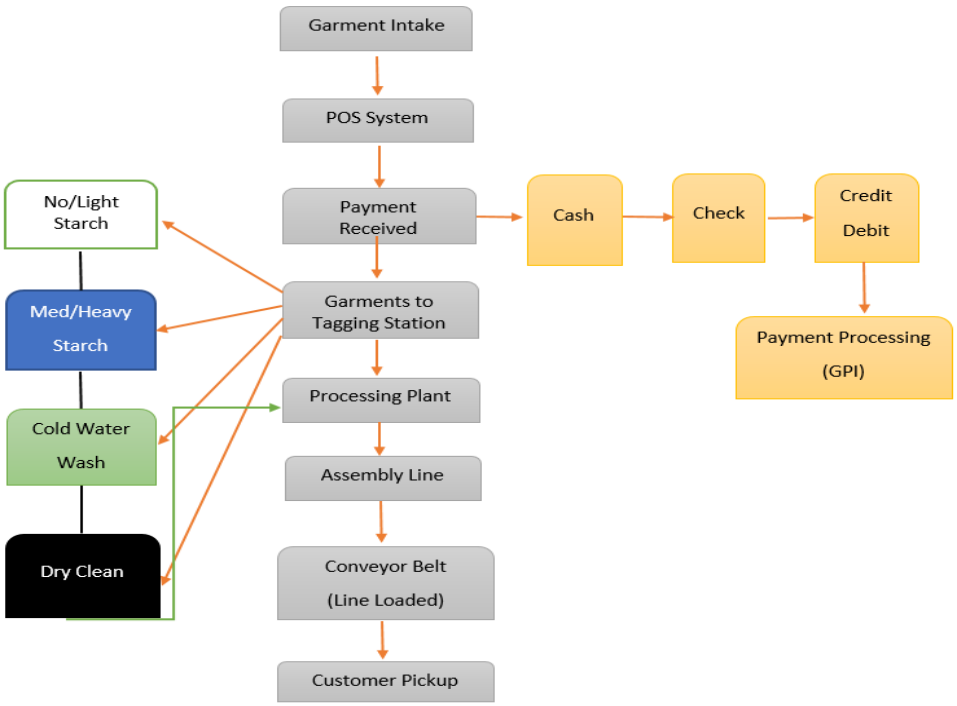
This capstone presents a Governance, Risk, and Compliance (GRC) assessment of Dry Clean Super Center's payment systems, identifies gaps relative to the Payment Card Industry Data Security Standard (PCI DSS), and proposes a roadmap to full compliance. Recommendations include strengthening governance and policies, implementing robust technical controls, enhancing risk management practices, instituting continuous monitoring, training staff, and upgrading hardware where necessary.

2. Introduction

2.1 Background and Context

The shift toward cashless transactions and customer demand for convenience have made credit and debit card payments integral to small business operations. However, along with this convenience comes the risk of data breaches, fraud, and non-compliance penalties. Payment card data is a high-value target for cybercriminals. Ensuring compliance with PCI DSS is essential for businesses that store, process, or transmit cardholder data.

J & P Jabez LLC (dba Dry Clean Super Center of Lafayette), was established in 2003, and has an additional location in Opelousas, Louisiana. Dry Clean Super Center of Lafayette (DCSC) performs in-person and point-of-sale (POS) transactions. Ensuring its POS infrastructure, network, policies, and staff practices meet security expectations is essential not only for regulatory compliance but for customer trust and business continuity. Being a small business creates multiple constraints related to cybersecurity, due to limited financial and human resources. DCSC lacks the budget to invest in advanced security tools, manage security services, and dedicated IT staff, leaving DCSC more vulnerable to threats. Time is also a constraint, as the owners and employees are focused on core business operations rather than monitoring networks and patching systems. In addition, DCSC struggles with the lack of cybersecurity expertise, making it difficult to implement best practices, maintain compliance, and respond effectively to incidents. These constraints often result in reliance on outdated software, weak security configurations, and insufficient employee training, all of which increase the risk of cyberattacks. A high turnover rate in DCSC also poses serious cybersecurity risks because it disrupts consistency in current security practices and increases the likelihood of human error. Frequent employee departures may lead to delays or oversights in deactivating user accounts, leaving behind unused credentials that attackers can exploit. New hires may not receive adequate training in security protocols due to time and resource limitations, resulting in weak password practices or unsafe handling of customer data. Additionally, constant staff changes can strain DCSC's ability to enforce security policies consistently, making it harder to build a culture of security awareness. This instability not only heightens the risk of data breaches but also makes it more difficult to detect and respond to threats effectively inside and out. Below is a flow diagram of the whole garment process from customer intake, to the customer pickup.



2.2 Purpose and Scope

The purpose of this Governance, Risk, and Compliance (GRC) assessment for DCSC is to evaluate how well the organization manages risks, protects sensitive customer and financial data, and complies with the relevant regulations and industry standards. Its scope will include reviewing policies, processes, and technical safeguards related to areas such as payment card security, employee access controls, data privacy, and business continuity planning. This assessment will help identify gaps in cybersecurity practices, operational risks, or regulatory obligations that may expose the business to financial loss, reputational harm, or legal penalties. For DCSC, the GRC assessment is tailored to its scale, focusing on practical, cost-effective measures that ensure secure handling of customer information, maintain trust, and support long-term business resilience.

2.3 Research Questions

1. What is the current GRC posture of DCSC with respect to payment system security?
2. Where are the gaps relative to PCI DSS requirements?
3. What roadmap (governance, technical, organizational) is needed for DCSC to achieve compliance?
4. What are the costs, challenges, and anticipated benefits associated with compliance, and updating hardware/software?

3. Literature Review

3.1 PCI DSS Overview

The Payment Card Industry Data Security Standard (PCI DSS), currently at version 4.0.1, is a global framework designed to safeguard payment card data and mitigate the risk of breaches for organizations that store, process, or transmit cardholder information. PCI DSS is structured around six major objectives: building and maintaining a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy (PCI Security Standards Council [PCI SSC], 2024). To achieve these objectives, the standard outlines 12 core requirements:

1. Install and maintain network security controls
2. Apply secure configurations to all system components
3. Protect stored account data
4. Protect card holder data with strong cryptography during transmission over open, public networks

5. Protect systems and networks from malicious software
6. Develop and maintain secure systems and applications
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
10. Log and monitor all access to system components and cardholder data
11. Test security of systems and networks regularly
12. Support information security with organizational policies and programs (PCI SSC, 2024)

Collectively, these requirements provide businesses of all sizes with a structured approach to protecting sensitive information, ensuring compliance with industry expectations, and maintaining customer trust.

3.2 GRC Frameworks (PCI DSS and NIST CSF)

Governance, Risk, and Compliance (GRC) frameworks provides organizations with a structured approach to aligning business objectives with risk management practices and regulatory requirements. For small business, GRC serves as a practical method to identify operational and cybersecurity risks, establish internal controls, and ensure compliance with standards such as PCI DSS and the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). PCI DSS focuses specifically on safeguarding payment card data through twelve core requirements and six overarching objectives, mentioned above, while the NIST CSF provides a flexible, risked-based model organized into five core functions: Identify, Protect, Detect, Respond, and Recover, this helps organizations of all sizes manage cybersecurity risks (PCI Security Standards Council [PCI SSC], 2024; National Institute of

Standards and Technology [NIST], 2018). For a small business such as DCSC that accepts credit card payments, and stores them, adopting a GRC framework enables integration of PCI DSS compliance into daily operations while using the NIST CSF to guide broader cybersecurity maturity. This combined approach helps prioritize limited resources, reduce regulatory exposure, and strengthen customer trust through a more resilient security posture. Here is a table mapping PCI DSS requirements against the NIST CSF functions:

PCI DSS Objective / Requirements	Corresponding NIST CSF Function(s)	Small Business Implementation Notes
Build and Maintain a Secure Network and Systems	Identify, Protect	Configure firewalls, secure Wi-Fi, segment networks; small business can use managed firewall solutions
1. Install and maintain network security controls	Protect	Use hardware/software firewalls and intrusion prevention
2. Apply secure configurations to all system components	Protect	Change default passwords, disable unnecessary services, apply patches regularly
Protect Cardholder Data	Protect	Encrypt stored cardholder data and transmissions; train staff on safe data handling
3. Protect stored account data	Protect	Implement encryption and access controls
4. Encrypt transmission of cardholder data over open networks	Protect	Use TLS/SSL or secure VPNs for data transmission
Maintain a Vulnerability Management Program	Identify, Protect, Detect	Regularly scan for malware and vulnerabilities; small businesses can leverage free or low-cost scanning tools
5. Protect systems and networks from malicious software	Detect, Protect	Install antivirus/anti-malware, schedule regular scans
6. Develop and maintain secure systems and applications	Protect	Apply software updates and secure development practices
Implement Strong Access Control Measures	Protect, Detect	Limit access to cardholder data; assign unique IDs; enforce MFA
7. Restrict access by business need-to-know	Protect	Role-based access control
8. Identify and authenticate users	Protect	Strong passwords, multifactor authentication
9. Restrict physical access to cardholder data	Protect	Lock storage areas, restrict office access
Regularly Monitor and Test Networks	Detect, Respond	Log network activity, monitor for anomalies, conduct periodic audits

10. Track and monitor all access to system and networks regularly	Detect	Enable logging, review logs regularly
11. Test security of systems and networks regularly	Detect, Respond	Conduct vulnerability scans and penetration testing
Maintain an Information Security Policy	Identify, Protect, Respond, Recover	Document security policies, train staff, establish incident response plan
12. Support information security with organizational policies	Identify, Protect, Respond, Recover	Policies guide employees behavior and response procedures

3.3 Small Business Payment System Threat Landscape

A small business like DCSC faces a unique payment systems threat landscape due to their frequent handling and storage of customer payment information, including credit and debit card data. Point-of-sale (POS) terminals, mobile payment devices, and possible online booking platforms are all potential attack vectors for cybercriminals seeking to steal cardholder data. Common threats include malware targeting POS systems, skimming devices on card readers, phishing attacks aimed at employees, and weak internal access controls that allow unauthorized access to sensitive payment data. Because many small businesses operate with limited IT resources, they are especially vulnerable to unpatched software, outdated terminals, and insufficient employee training on secure payment handling. Additionally, storing customer payment information for recurring services increases risk exposure, as a breach could compromise multiple customer accounts simultaneously. Overall, small payment systems in the dry cleaning business must contend with a combination of technical, operational, and human-centric threats that could lead to financial loss and reputational damage.

4. Methodology

4.1 Data Collection

For a Governance, Risk, and Compliance assessment of DCSC, effective data collection is critical to understand the operational, technical, and regulatory landscape. Key questions for DCSC's management should focus on business practices, such as: How is customer payment information collected, stored and retained? What internal controls exist to restrict access to sensitive data? Are employees trained on secure payments handling and incident reporting procedures? For the POS software provider, WinCleaners, important questions include: How does the system encrypt cardholder data both at rest and in transit? What mechanisms exist for patch management and vulnerability monitoring? Are audit logs maintained and accessible for review? For the payment processing company, Global Payments Integrated, questions should address transaction security and compliance, including: How are payments tokenized or encrypted? What fraud detection and monitoring capabilities are in place? How is PCI DSS compliance validated, and what reporting is available to the merchant? Collecting responses to these targeted questions enables a comprehensive understanding of potential risks and informs the design of controls that align with both PCI DSS and NIST CSF frameworks.

4.2 Point-of-Sale software (WinCleaners v 10.1.15)

WinCleaners (v 10.1.15) is a specialized point-of-sale (POS) software designed for the dry cleaning industry, providing both operational efficiency and secure payment processing. The system employs strong security measures, including tokenization and end-to-end encryption, to safeguard cardholder data during transactions. When a customer initiates payment, the card data is immediately encrypted within the POS terminal, ensuring that sensitive information cannot be intercepted in transit. This encrypted data is then tokenized, replacing the primary account

number (PAN) with secure, non-sensitive tokens that can be stored for future transactions without exposing cardholder information. The tokenized and encrypted data is securely transmitted through WinCleaner's payment gateway to Global Payments Integrated (GPI), the merchant processing partner, where authorization and settlement occur. This streamlined flow of information ensures compliance with PCI DSS requirements while reducing the risk of fraud and maintaining the customer trust.

4.3 Payment Processing (Global Payments Integrated)

When Global Payment Integrated (GPI) is used in conjunction with WinCleaners point-of-sale (POS) system, the payment process is designed to protect sensitive cardholder data through multiple layers of security. Once a customer's card is swiped, dipped, or tapped, the cardholder data is immediately encrypted within the POS terminal, ensuring the primary account number (PAN) cannot be intercepted during transmission (Global Payments Integrated, 2020a). This encrypted data is then sent to GPI, where tokenization replaces the PAN with a unique, non-sensitive token that can be safely stored in the merchant environment for recurring transactions, refunds, or customer profiles without exposing actual card data (Global Payments Integrated, 2020b; PCI Security Standards Council, 2011). The original card data is stored only in Global Payment's secure, PCI DSS-compliant data centers, ensuring merchants never handle or retain raw cardholder information (PCI Security Standards Council, 2015). By combining point-to-point (P2PE), tokenization, and secure off-site data storage, the integration between WinCleaners and Global Payments Integrated provides end-to-end protection, reduces PCI DSS compliance scope for DCSC, and mitigates the risk of fraud or data breaches (Global Payments, n.d.).

Here is a table mapping the division of responsibility between GPI and the Merchant

Security Task	GPI	Merchant
Encrypting Card Data	Yes	No
Tokenization and Storage	Yes	No
PCI DSS Compliance of Platform	Yes	No
PCI Self-Assessment Questionnaire (SAQ)	No	Yes
Securing Merchant Network/ Devices	No	Yes
Fraud Monitoring Tools	Yes	No
Training Staff	No	Yes
Chargeback Response	No	Yes

5. Current State Assessment of Dry Clean Super Center

5.1 Business Profile and Payment Environment

Dry Clean Super Center maintains a strong payment environment supported by its specialized point-of-sale system, WinCleaners, and its integration with Global Payments Integrated, a leading merchant processor. The WinCleaners POS enhances security by encrypting customer card data at the point of entry, transmitting it securely, and relying on tokenization to protect stored transaction information, while Global Payments Integrated ensures that sensitive data is housed only in its PCI DSS-compliant data centers (Global Payments Integrated, 2015). Together, these systems establish a robust security posture that mitigates the risk of fraud, reduces PCI DSS scope for the business, and aligns with industry best practices for safeguarding cardholder data. However, despite these strong technical and procedural controls, DCSC is rendered non-compliant due solely to its failure to complete the Self-Assessment Questionnaire (SAQ) required annually by Global Payments Integrated, underscoring that the compliance is not only about technology but also about administrative obligations (PCI Security Standards

Council, 2011). In addition to this, there are various controls that can and must be implemented to the physical location at DCSC that would render sensitive business files safer than current practices. Due to a lack of personnel, there is not an administrative employee on duty at all times during business hours (7:30 AM – 6 PM M-F). Due to the lack of presence, some offices must remain unlocked to give front end employees access to petty cash and other various documents that may be needed throughout their shifts. This access to the administrative office unfortunately leaves some sensitive documentation unsecure, which violates the control of least privilege. DCSC also lacks an emergency and recovery plan in the event that a natural disaster should effect the business. This lack of planning could hinder business continuity and cause the complete shutdown of operations until such a time that DCSC could recover from damages rendered.

DCSC has eight counter stations all equipped with business towers, credit card scanners, touchscreen monitors, thermal printers, and ticket printers. All stations operate on Windows 11, except for three workstations. The three outstanding systems operate on Windows 7, 8, and 10 respectively. This presents an immediate issue, because Windows 7 and 8 have been rendered obsolete, and Windows 10 is slated for end of life October 31, 2025. This is relevant because there will be no more support via security patches for Windows 10, as there is no longer support for Window 7 and 8 currently. This hardware and software must be upgraded immediately, as this is a current exposure in DCSC's cybersecurity posture. Three Dell business systems with WinCleaner's upgrades and Windows 11 upgrades should cost an estimated $7,500-$8,500. Dry Clean Super Center's hardware was found to be up to date, with the exception of these three CPUs in use for front counter operations. The CPUs that were in use were found to be outdated because of the use of i3 core processors, which Windows 11 does not support. The only solution

to remedy this issue is to upgrade the hardware and subsequently upgrade and update the operating system to Windows 11. This should be done post haste, to close this open attack vector.

5.2 Governance Structure and Policies

Although DCSC maintains a secure payment environment through the use of WinCleaners POS and its integration with Global Payment Integrated, the organization's governance structure and policy framework remain underdeveloped. The business has not established formal, written security policies related to payment operations, such as acceptable use policy for staff or a documented data retention policy for cardholder information. While these omissions do not compromise the technical security of payment transactions, they reveal a lack of standardized governance practices. In addition, decision-making regarding payment hardware and software is conducted informally by management, without the oversight of a dedicated risk or compliance committee. This approach highlights a strong technical foundation for payment security but underscores the need for more formalized governance and policy processes to ensure long-term resilience and regulatory compliance.

5.3 Risk Management Practices

Dry Clean Super Center currently exhibits immature risk management practices that limit its ability to proactively address payment security and compliance challenges. The organization does not maintain a formal risk register or conduct regular risk assessments, resulting in a lack of structured visibility into potential threats and vulnerabilities. Security incidents are logged informally, without a standardized process for documentation, escalation, or analysis, and there is no formal incident response plan to guide coordinated actions in the event of a breach or

system compromise. Additionally, staff training related to information security and PCI DSS compliance is minimal, leaving employees with limited awareness of their responsibilities in protecting cardholder data. As a result, while DCSC's payment systems remain technically secure, the absence of formalized risk management practices increases organizational exposure to regulatory non-compliance and operational disruption.

5.4 Gap Analysis

A gap analysis of Dry Clean Super Center reveals that while the business benefits from a strong technical payment environment through its use of WinCleaners POS and Global Payments Integrated-both of which provide encryption, tokenization, and PCI DSS-compliant data storage-its governance and administrative practices are significantly underdeveloped. DCSC lacks formal written policies governing payment security, including acceptable use and data retention policies, and decision-making authority is fragmented, with management making ad hoc choices without the guidance of a risk compliance committee. Risk management processes are similarly weak, as the organization does not maintain a risk register, conduct regular risk assessments, or implement a formal incident response plan; security incidents are tracked informally, and staff training on PCI DSS requirements is minimal, leaving employees underprepared. Finally, although payment systems themselves are secure, DCSC remains out of compliance with PCI DSS because it has not completed the required Self-Assessment Questionnaire (SAQ) for GPI. Together, these findings indicate that DCSC's primary gaps lie not in technical safeguards but in governance, policy development, and compliance administration, all of which must be addressed to achieve full regulatory alignment and long-term resilience.

6. Regulatory and Compliance Requirements

6.1 Other Relevant Laws & Regulations

In addition to PCI DSS compliance, Dry Clean Super Center must consider other relevant laws and regulations that govern the handling of payment and personal data. At the federal level, DCSC is subject to consumer protection regulations such as the Gramm-Leach-Bailey Act (GLBA) for safeguarding customer financial information and the Federal Trade Commission (FTC) guidelines on data security and breach notification. State-specific requirements in Louisiana further obligate businesses to protect personal identifying information (PII) under the Louisiana Database Security Breach Notification Law (La. Rev. Stat. 51:3071), which mandates prompt notification to affected individuals and the attorney general in the event of a security breach involving sensitive data. Additionally, general consumer protection statutes and privacy obligations require that organizations implement reasonable administrative, technical, and physical safeguards for the data they collect. Compliance with these regulations, in combination with PCI DSS standards, ensures that DCSC not only secures payment information but also meets broader legal obligations, reducing the risk of penalties, litigation, and reputational harm.

7. Proposed Roadmap to PCI DSS Compliance

7.1 Plan of Action & Milestones (POA&M)

To strengthen its compliance posture, DCSC should pursue a phased roadmap that prioritizes immediate compliance requirements while building sustainable governance and risk management practices. By following this phased approach, DCSC can address immediate

compliance obligations, institutionalize governance and risk management practices, and build a culture of ongoing security and compliance.

7.2 Short-Term (0-3 months)

Establish formal written security policies aligned with PCI DSS requirements, including an acceptable use policy, data retention policy, and procedures for handling cardholder data. Complete and submit the SAQ required by Global Payments Integrated to close the most critical compliance gap. There is an immediate need to upgrade the 3 outdated CPUs with the i3 core processors running Windows 7, 8, and 10. Support is no longer given for the Windows 7 and 8 OS, and will be ending this month for Windows 10 OS, making this an immediate need for DCSC. This is a hardware/software gap that must be closed as soon as possible, to further limit attack vectors within the DCSC system.

7.3 Mid-Term (3-6 months)

Implement a formal risk management framework by developing a risk register, conducting initial risk assessments, and introducing a standardized process for documenting and escalating incidents. Draft and adopt formal incident response plan to ensure preparedness in the event of a payment security incident

7.4 Long-Term (6-12 months)

Launch recurring employee training programs to raise awareness of PCI DSS obligations and reinforce secure practices across all staff. Establish a governance structure, such as a compliance or risk committee, to provide oversight for payment system decisions and ensue

ongoing alignment with PCI DSS requirements. Conduct annual reviews of policies, risk assessments, and training effectiveness to sustain compliance and resilience.

8. Implementation Plan and Cost Estimation

8.1 Estimated Costs

The implementation plan for Dry Clean Super Center focuses on strengthening governance, risk management, and compliance administration while leveraging the existing secure payment infrastructure provided by Wincleaners POS and Global Payments Integrated. In the first phase, DCSC should upgrade the three workstation's hardware and OS, as well as engage a compliance consultant to assist with drafting formal policies, developing a risk register, and completing the required GPI SAQ, an effort estimated at $5,000-$7,500 in consulting and administrative costs. Costs of hardware and software upgrades are estimated to be $7,500-$8,500. In the second phase, the business should invest in creating and testing a formal incident response plan, conducting initial employee training sessions, and implementing risk assessment procedures, which can be achieved with modest training and documentation software investments of approximately $3,000-$5,000. Finally, establishing an ongoing compliance and governance structure-such as annual risk reviews, refresher training, and periodic policy updates-is expected to require an annual recurring cost of $2,000-$4,000. Once hardware and software upgrade costs are included, overall, the total implementation plan is projected $17,500-$23,500 in initial costs, with minimal recurring expenses, making PCI DSS compliance an achievable and sustainable goal for DCSC while significantly reducing organizational and regulatory risks.

8.2 Return on Security Investment (ROSI)

The return on security investment (ROSI) for Dry Clean Super Center is substantial because the organization already benefits from a strong technical payment environment through its WinCleaners POS and integration with Global Payments Integrated, both of which provide tokenization, encryption, and PCI DSS-compliant storage. The primary costs of compliance are there for limited to administrative and governance improvements-such as policy development, risk management process, incident response planning, and employee training-rather than expensive overhauls of core payment infrastructure. By investing an estimated $17,500-$23,500 in these initiates, DCSC can achieve full PCI DSS compliance, significantly reduce the risk of regulatory fines, avoid potential breach-related costs, and strengthen customer trust in its payment security practices. Compared with the average cost of a data breach in small businesses, which can reach hundreds of thousands of dollars in remediation and lost revenue, DCSC's investment yields a high return by mitigating financial exposure, protecting reputation, and ensuring long-term resilience in payment operations.

9. Challenges, Risks, and Mitigation Strategies

9.1 Common Small Business Constraint

Small businesses often face a range of constraints that can limit their operational efficiency, growth, and security posture. Financial resources are typically limited, making investments in technology, security, and compliance more challenging compared with large organizations. Staffing constraints are also common, with employees often required to wear multiple hats, which can dilute expertise in specialized areas such as cybersecurity, risk management, or

regulatory compliance. Time constraints further exacerbate these challenges, as day-to-day operational demands leave little bandwidth for strategic planning, policy development, or staff training. Additionally, small businesses may lack access to advanced tools, technical expertise, or formal governance structures, which can hinder the implementation of robust security controls and adherence to regulatory frameworks such as PCI DSS. These constraints necessitate careful prioritization and efficient use of resources to maintain secure, compliant, and resilient operations.

9.2 Potential Risks During Transition

During the transition to full PCI DSS compliance, and hardware/software upgrades, DCSC may encounter several potential risks that could impact operations, security, and compliance. Implementation of new governance structures, policies, hardware/software, and risk management processes may temporarily disrupt routine business activities or slow transaction processing as staff adapt to updated procedures and equipment. Incomplete or inconsistent staff training could result in accidental mishandling of cardholder data, creating vulnerabilities despite the strong technical security of WinCleaners POS and Global Payment Integrated. Additionally, the migration of documentation, risk registers, and incident response protocols carries the risk of gaps or errors if not carefully managed and validated. Failure to meet internal deadlines or accurately complete the SAQ could prolong non-compliance, exposing DCSC to regulatory scrutiny. These transitional risks highlight the need for careful planning, phased implementation, and ongoing monitoring to ensure that improvements in governance, policy, and risk management strengthen the organization without introducing unintended operational or security challenges.

9.3 Mitigation Plans

To mitigate potential risks during the transition to PCI DSS compliance, Dry Clean Super Center should adopt a structured and phased implementation approach. Clear timelines and milestones should be established for policy development, risks management processes, and completion of the Self-Assessment Questionnaire to prevent delays and ensure accountability. Comprehensive staff training programs should be conducted prior to and throughout the transition, emphasizing proper handling of cardholder data and adherence to updated procedures, reducing the likelihood of human error. All documentation, including risk registers, incident response plans, and policies, should be carefully reviewed and validated to ensure completeness and accuracy. Additionally, pilot testing of new processes and periodic progress reviews by a designated compliance or risk committee can identify gaps early, allowing corrective actions to be taken before full deployment. By combining phased implementation, structured oversight, and continuous monitoring, DCSC can minimize operational disruption, strengthen its governance framework, and achieve PCI DSS compliance in a controlled and effective manner.

10. Conclusions

Dry Clean Super Center of Lafayette is at a stage where proactive measures can substantially reduce risk and align the company with industry standards. While several gaps exist relative to PCI DSS requirements—especially in governance, technical controls, and monitoring—the path to compliance is feasible with phased implementation, management commitment, and reasonable investment. Achieving PCI DSS compliance not only helps avoid regulatory and financial penalties but builds customer trust and protects the business's long-term

viability. Upgrading hardware immediately closes the gaps in the technical lapses. Immediate upgrade of OS to Windows 11 will ensure continuous support and constant security patches, significantly reducing the opportunities for a breach of any kind. While hardware and software upgrades significantly reduce attack vectors used by bad actors.

11. References

- PCI Security Standards Council. (2022). *PCI DSS Version 4.0: Requirements and Security Assessment Procedures.*
- Smith, A., & Jones, B. (2021). "Small Business Cybersecurity: Challenges and Best Practices." *Journal of Information Security*, 12(2), 101-118.
- Louisiana Legislature. (2020). *Louisiana Data Breach Notification Law.*
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*.
- Payment Card Industry Security Standards Council. (n.d.). "Tokenization Guidelines."
- Global Payments Integrated. (2020, March 4) PCI DSS Requirements for Tokenization and Encryption. Global Payments Integrated. https://www.globalpaymentsintegrated.com/en-us/blog/2020/03/24/pci-dss-requirements-for-tokenization-and-encryption
- PCI Security Standards Council. (2011, August). Information supplement: PCI DSS tokenization guidelines. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

- Global Payments. (n.d.). Network tokens -Overview. Global Payments Developer Portal. https://developer.globalpay.com/ecommerce/networks-tokens
- ISACA (2020) Governance, Risk, and Compliance: Principles and Practices, ISACA.
- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, v1.1. US Department of Commerce https://doi.org/10.6028/NIST.cswp.04162018
- PCI Security Standards Council. (2024). Payment Card Industry Data Security Standard, v 4.0.1 https://www.pcisecuritystandards.org