

PCI DSS COMPLIANCE SERVICE

www.redseclabs.com

CONTENT

1	Redseclabs Leading the Way in PCI DSS Compliance	3
2	Why Redseclabs is the Optimal Choice for PCI DSS Compliance	4
	Expertise and Accreditation	4
	Proven Track Record	4
	Customised Client-Centric Approach	4
	Comprehensive Insurance Coverage	4
	Comprehensive Risk Management	4
3	Elevating Your PCI DSS Compliance with Redseclabs	5
	Gap Analysis and Risk Assessment	5
	Remediation Support	5
	Continuous Compliance Monitoring	5
4	The Business Impact of Partnering with Redseclabs	5
	Enhanced Protection for Cardholder Data	5
	Boosted Consumer Confidence	5
	Assurance of Compliance	5
5	Our Skillset	6
	Key Certifications	6
6	Licensed Tools We Use	6
7	Advantages of PCI QSA Accreditation in PCI DSS Compliance	7
8	Customized and Compliant PCI DSS Solutions	7
9	Comprehensive Insurance Coverage	8
10	Benefits of Our Customized Approach	9
11	Risk of Non-Compliance with PCI DSS	10
12	Twelve PCI DSS Requirements in a Nutshell	11
13	Deliverables	11
14	PCI DSS v3.2.1 TO v4.0 Major Changes Summary	12
15	Our Methodology	13
16	Post-Compliance Support and Roadmap	14
17	Our PCI DSS Clients	14



1. Redseclabs Leading the Way in PCI DSS Compliance

Redseclabs stands at the forefront of protecting payment card data and ensuring compliance with the Payment Card Industry Data Security Standard (PCI DSS). As a premier provider of PCI DSS compliance services, EIC leverages its deep understanding of payment security requirements to help clients safeguard sensitive cardholder information and achieve compliance efficiently and effectively



2. Why Redseclabs is the Optimal Choice for PCI DSS Compliance

Expertise and Accreditation

Redseclabs, as a PCI QSA, is highly qualified to navigate your organization through PCI DSS compliance, reflecting our dedication to top-tier security and compliance standards.

Proven Track Record

With years of experience in payment security, Redseclabs has a proven history of helping businesses of all sizes meet rigorous PCI DSS requirements, ensuring that they not only achieve but also maintain compliance over time.

Customised Client-Centric Approach

We understand that each client's environment is unique. Our PCI DSS compliance solutions are tailored to meet the specific needs of your business, ensuring effective coverage and protection of cardholder data.

Comprehensive Insurance Coverage

We maintain comprehensive insurance, including Workers' Compensation, General Liability, Cyber-risk, and Privacy Liability. Our coverage spans millions in limits, reflecting a strong commitment to risk management. This ensures unparalleled protection for our clients and operations.

Comprehensive Risk Management

Our approach includes a thorough assessment of your payment processing environments, identification of vulnerabilities, and implementation of robust security measures designed to protect cardholder data and reduce compliance-related risks.



3. Elevating Your PCI DSS Compliance with Redseclabs

Our services extend beyond simple compliance checks. We perform detailed assessments to identify compliance gaps and potential vulnerabilities in your payment card operations.

Gap Analysis and Risk Assessment

We provide actionable insights and hands-on support to address identified gaps, helping you implement necessary security measures and best practices.

Remediation Support

Redseclabs offers ongoing support and monitoring to ensure your environment remains compliant with PCI DSS standards as they evolve.

Continuous Compliance Monitoring

Our approach is not only about fulfilling requirements but also about enhancing your overall security posture, helping you safeguard against breaches and fraud.



Assurance of Compliance

Meet all PCI DSS requirements confidently with our expert guidance, reducing the risk of costly fines and penalties for non-compliance.



4. The Business Impact of Partnering with Redseclabs

By choosing Redseclabs, you gain:

Enhanced Protection for Cardholder Data

Safeguard your customers' sensitive information against emerging threats and vulnerabilities.

Boosted Consumer Confidence

Enhance your reputation by demonstrating a strong commitment to security, earning trust from customers and partners alike.

5. Our Skillset

Redseclabs provides top tier cybersecurity services, including penetration testing, system auditing, and compliance. With certified experts and a focus on continuous improvement, Redseclabs ensures robust digital asset protection as a trusted industry leader.

Key Certifications



6. Licensed Tools We Use



7. Advantages of PCI QSA Accreditation in PCI DSS Compliance

Assured Quality and Consistency

Our PCI QSA accreditation means our compliance services adhere to the highest standards, ensuring consistent quality and reliability.

Up-to-date Knowledge of Regulations

Being a PCI QSA requires staying current with the latest developments in payment card security, ensuring our team is always equipped with the latest knowledge and techniques.

Global Recognition and Trust

PCI QSA accreditation is recognized worldwide as a mark of superior security expertise in payment card industries. This global recognition builds trust with clients and stakeholders,

8. Customized and Compliant PCI DSS Solutions



Tailored Approach

Our range of certifications, coupled with our PCI QSA accreditation, enables us to offer compliance solutions specifically customized to your organization's payment systems and business needs.



Comprehensive Security Coverage

Our accredited team covers every aspect of your payment card environment, ensuring all components are secure and compliant with PCI DSS requirements.



Conformance to Best Practices

Our methodologies are aligned with industry best practices, helping you not only comply but also strengthen your security environment.

9. Comprehensive Insurance Coverage

At Redseclabs, we understand that robust PCI DSS compliance solutions are part of strong risk management strategies. Our operations are fortified with extensive insurance coverage to back our partnership with you confidently.

Our Insurance Coverages include



Workers' Compensation and Employer's Liability

We maintain statutory Workers' Compensation as required by law and Employer's Liability with a limit of \$1,000,000. This safeguards our team and your organization against any unforeseen circumstances.



Commercial General Liability Insurance

Our policy includes coverage for products, completed operations, advertising injury, personal injury, and contractual liability, with limits of \$1,000,000 per occurrence and a \$2,000,000 annual aggregate. This comprehensive coverage ensures that all aspects of our engagement are protected.



Commercial Automobile Insurance

With a coverage limit of \$1,000,000 per accident, this insurance covers all owned, leased, hired, or non-owned vehicles used during our services.



Technology Errors & Omissions, Cyber Risk, and

Coverage with a \$2,000,000 limit per claim and annual aggregate, protecting against IT service liabilities like data breaches, privacy failures, unauthorized access, and network security incidents.



This comprehensive insurance coverage demonstrates our dedication to mitigating risks for our clients and our business. It reflects our commitment to providing secure, reliable, and trustworthy services, ensuring peace of mind for all stakeholders involved in our engagement.

Customisation and Flexibility at Redseclabs

At Redseclabs, we recognize that every organization has unique compliance needs. Our approach to PCI DSS compliance is anchored in customization and flexibility, ensuring that our services align perfectly with each client's specific requirements.

Customisation and Flexibility Tailoring to Client-Specific Needs

Our PCI DSS compliance services are scalable for businesses of all sizes, ensuring efficient compliance.

Different sectors have unique challenges in securing payment card data, focusing on points of sale or data protection across service points

10. Benefits of Our Customized Approach

Relevance and Efficiency

By tailoring our services, we ensure that our PCI DSS compliance efforts are directly relevant and highly efficient, addressing your specific risks and challenges.

Enhanced Security Posture

Our tailored strategies result in a more robust security posture, addressing the specific vulnerabilities and compliance needs of your industry and business size.

Better Stakeholder Engagement

Tailored strategies foster better engagement from all stakeholders, including employees, management, and vendors. Customized training and clear communication of specific roles in the compliance process increase overall participation and commitment to maintaining security standards.

11. Risk of Non-Compliance with PCI DSS



PCI DSS non-compliance leads to significant financial penalties imposed by payment card brands and acquiring banks.



It increases liability in case of a breach, including legal costs, compensation, and potential damage to reputation.



Legal consequences like investigations and lawsuits can arise from non-compliance with PCI DSS.



Security breaches from non-compliance decrease customer trust, loyalty, and can harm the organization's image.



Non-compliance heightens the risk of card data theft and fraudulent transactions.



Non-compliance may result in lost business opportunities and restricted market access.

12. Twelve PCI DSS Requirements in a Nutshell

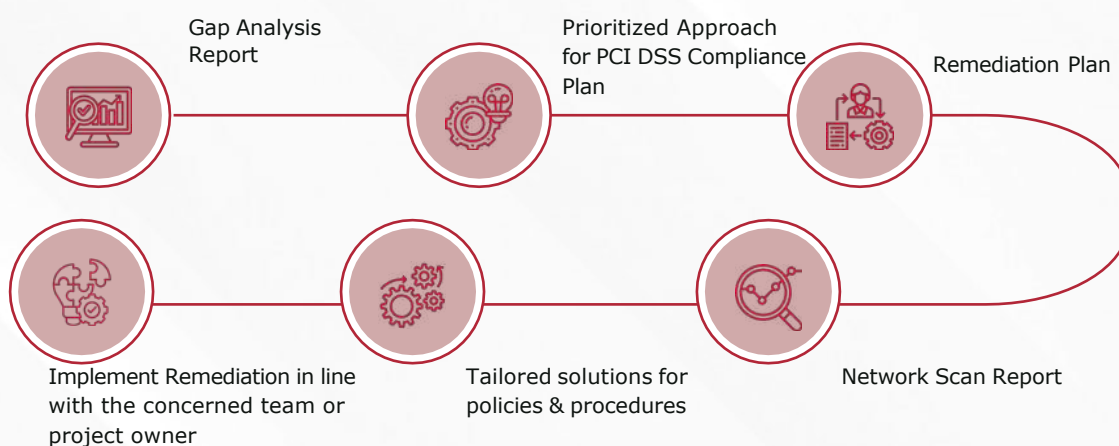
PCI DSS is based on technical and operational requirements related to 12 different areas, performed across six conceptual areas:

- ✓ Build and Maintain a Secure Network and Systems
- ✓ Protect Account Data
- ✓ Maintain a Vulnerability Management Program
- ✓ Implement Strong Access Control Measures
- ✓ Regularly Monitor and Test Networks

13. Deliverables

The major area of concentration throughout the project period will be helping your organization's concerned stakeholders and departments with the process, policy, and guidelines—generating various levels and types of reports in order to make your organization ready for the PCI DSS certification.

Throughout the timeline of the project, following deliverables will be provided:



14. PCI DSS v3.2.1 TO v4.0

Major Changes Summary

Security Protocols



Updated core requirements to allow a broader range of network security technologies beyond traditional firewalls.

Malware Protection



Transition from anti-virus to comprehensive anti-malware programs, expanding coverage across more technologies.

Security Configurations



Shift from default to advanced security configurations for enhanced protection.

Cryptography Practices



Improved cryptography practices to ensure the safety of cardholder data.

Audit Logs:



Replacement of audit traces with more detailed audit logs.

Account Data Security



Strengthened measures to secure account data.

15. Our Methodology

Our PCI compliance approach prioritizes payment card data security by following PCI DSS best practices. The standard includes 12 requirements for any business that stores, processes or transmits cardholder data. These requirements specify the framework for a secure payment environment. Our PCI DSS compliance process includes seven phases. Each phase can be executed independently of the other and followed by reporting.

- **Initiation Meeting:** This initial meeting involves all stakeholders to discuss the project's objectives, timelines, and responsibilities. It's crucial for aligning the project team and ensuring everyone understands the compliance goals and the process ahead.
- **Scope Identification:** This phase defines the boundaries of the PCI DSS assessment, identifying which systems, networks, and data processes handle cardholder data and therefore must comply with PCI DSS requirements.
- **GAP Analysis:** In this stage, the current state of the systems is evaluated against PCI DSS standards to identify shortcomings or 'gaps' in compliance. This analysis helps in planning the necessary corrective actions to achieve full compliance.
- **Remediation Period:** The Remediation Period is a crucial phase in the PCI DSS compliance project, focusing on addressing and resolving the vulnerabilities and compliance gaps identified during the GAP Analysis and vulnerability assessment stages.
 - **ASV Scan and VAPT (External and Internal):** Automated scans and vulnerability assessments are conducted to detect vulnerabilities in both external and internal networks.
 - **Data Center and DR Visit:** Inspection of the data center facilities and disaster recovery site to evaluate physical and environmental security controls.
 - **System & Application Walkthrough:** Detailed reviews of system configurations and applications to ensure they are secured and comply with PCI DSS.
 - **Implement Remediation for VAPT and Identified Gaps:** Addressing the vulnerabilities and gaps found during the assessments to meet PCI DSS standards.
- **Final PCI QSA Audit:** A Qualified Security Assessor (QSA) conducts a comprehensive audit to verify that all PCI DSS requirements have been met and that all remediation actions are effectively implemented.
- **ROC & AOC:** Generation of a Report on Compliance (ROC) and an Attestation of Compliance (AOC) by the QSA. These documents validate the organization's adherence to PCI DSS requirements.
- **Certification:** Upon successful completion of the audit and submission of the ROC and AOC, the organization is awarded the PCI DSS certification, confirming its compliance with all requirements.

16. Post-Compliance Support and Roadmap

We provide comprehensive post-compliance support and a strategic roadmap to guide you beyond the initial PCI DSS certification process:

Timely Resolution and Revalidation

After achieving PCI DSS compliance, we encourage ongoing compliance checks and offer revalidation services to ensure continuous adherence to the standards.

Transparent Progress Tracking

A shared tracking system will be implemented to monitor ongoing compliance status and ensure accountability.

Continuous Monitoring and Updates

Post-compliance, we offer ongoing monitoring and periodic updates on PCI DSS requirement changes, ensuring your defenses remain robust against new threats.

Collaborative Support

Redseclabs will provide collaborative sessions with your team as needed to expedite and clarify the compliance maintenance process.

17. Our PCI DSS Clients

