PCI DSS COMPLIANCE SOLUTIONS

PCI SCOPE ASSESSMENT | PREPAREDNESS ASSESSMENT | REMEDIATION | ONSITE | MAINTENANCE

Streamline Your Compliance

The Payment Card Industry Data Security Standard (PCI DSS) specifies technical and operational requirements for all organizations that store, process or transmit credit card data. From the world's largest corporations to the smallest brick-and-mortar store, if you handle credit card data, then PCI DSS applies to you.

PCI DSS version 3.2.1 was retired on March 31, 2024 and PCI DSS 4.0 took effect April 1, 2024.

There are **64** new requirements. Of those 64,

- 53 apply to all entities.
- 11 new requirements for Service Providers only.
- 13 will be required immediately for all v4.0 validations – new roles and responsibilities, scoping exercise and a Targeted Risk Analysis (TRA) if using the customized approach.
- 51 are future dated best practices until March of 2025.

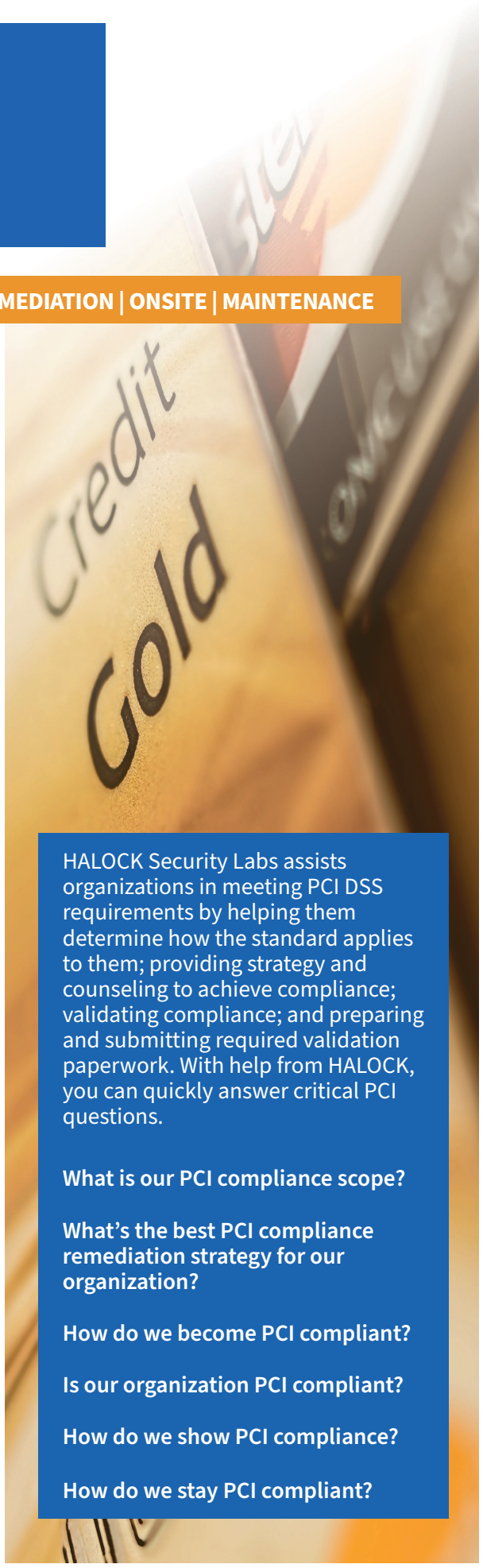
PCI DSS v4.0 introduces the Customized Approach validation option.

For entities that cannot meet the PCI DSS' stated requirement, the Customize Approach Objective provides an alternative. Organizations will have to:

- Document a Controls Matrix Template and perform a Targeted Risk Analysis for each customized control.
- Perform testing, monitoring of controls and provide completed matrix(es), targeted risk analysis, testing and effectiveness evidence to assessors for validation.
- Have clearly explained cadences used throughout the standard and that "periodic" control cadences are determined based on risk analysis (testing high-risk controls more frequently).

PCI DSS is emphasizing (more than ever) business as usual activities to implement and maintain layered security controls for protecting cardholder data. The introduction of the customized approach and targeted risk analyses provide organizations the opportunity to use their existing risk assessment methodology to analyze and justify controls. Every organization that has a PCI DSS obligation will have ***at least 1 targeted risk analysis*** to complete for their 4.0 compliance.

HALOCK has been working with litigators, regulators, judges, and standards bodies to agree on a definition for reasonable controls, and we can help you in the process.



HALOCK Security Labs assists organizations in meeting PCI DSS requirements by helping them determine how the standard applies to them; providing strategy and counseling to achieve compliance; validating compliance; and preparing and submitting required validation paperwork. With help from HALOCK, you can quickly answer critical PCI questions.

What is our PCI compliance scope?

What's the best PCI compliance remediation strategy for our organization?

How do we become PCI compliant?

Is our organization PCI compliant?

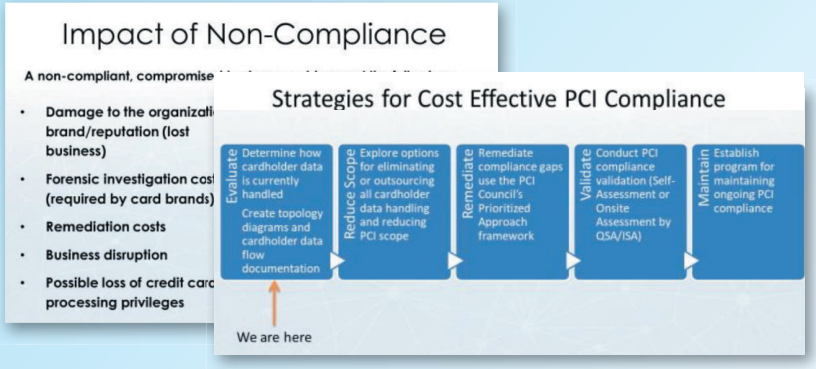
How do we show PCI compliance?

How do we stay PCI compliant?

HALOCK®

PCI DSS EDUCATION

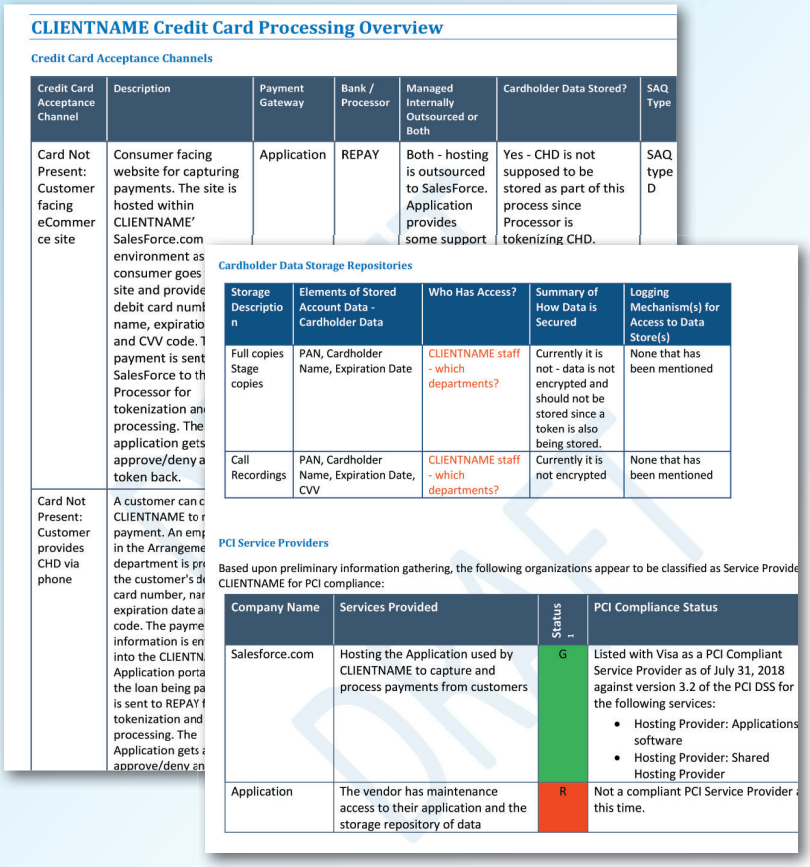
HALOCK's **PCI Overview presentations** provides stakeholders with valuable education about the PCI Data Security Standard, validation requirements, and potential consequences for non-compliance. Our clients understand what is involved in achieving PCI compliance and how best to approach the process.



PCI DSS SCOPE ASSESSMENT

Serving in an advisory capacity, one or more of HALOCK's QSAs work with a client's staff to identify and document all interactions with cardholder data and the flow of credit card data through the network and systems in the assessed environment. This information is used to determine preliminary **scope of a client's PCI DSS cardholder data environment** (including all connected-to and management components) and applicable requirements.

Every organization has unique drivers, goals, requirements and cultures, all of which need to be considered when determining how to take on compliance. There are also a lot of different approaches to addressing PCI compliance. Therefore, after completing the **Scope assessment, HALOCK conducts a Strategic Remediation Planning session** to help the organization think through the impact of different remediation strategies and determine what approach will be the best fit.


CLIENTNAME Credit Card Processing Overview

Credit Card Acceptance Channels

Credit Card Acceptance Channel	Description	Payment Gateway	Bank / Processor	Managed Internally Outsourced or Both	Cardholder Data Stored?	SAQ Type
Card Not Present: Customer facing eCommerce site	Consumer facing website for capturing payments. The site is hosted within CLIENTNAME' SalesForce.com environment as consumer goes site and provide debit card numb name, expiratio and CVV code. T payment is sent SalesForce to th Processor for tokenization an processing. The application gets approve/deny a token back.	Application	REPAY	Both - hosting is outsourced to SalesForce. Application provides some support	Yes - CHD is not supposed to be stored as part of this process since Processor is tokenizing CHD.	SAQ type D
Card Not Present: Customer provides CHD via phone	A customer can c CLIENTNAME to payment. An emp in the Arrangeme department is pr the customer's d card number, nar expiration date a code. The payme information is en into the CLIENTN Application porta the loan being pa is sent to REPAY tokenization and processing. The Application gets approve/deny en					

Cardholder Data Storage Repositories

Storage Description	Elements of Stored Account Data - Cardholder Data	Who Has Access?	Summary of How Data is Secured	Logging Mechanism(s) for Access to Data Store(s)
Full copies Stage copies	PAN, Cardholder Name, Expiration Date	CLIENTNAME staff - which departments?	Currently it is not - data is not encrypted and should not be stored since a token is also being stored.	None that has been mentioned
Call Recordings	PAN, Cardholder Name, Expiration Date, CVV	CLIENTNAME staff - which departments?	Currently it is not encrypted	None that has been mentioned

PCI Service Providers

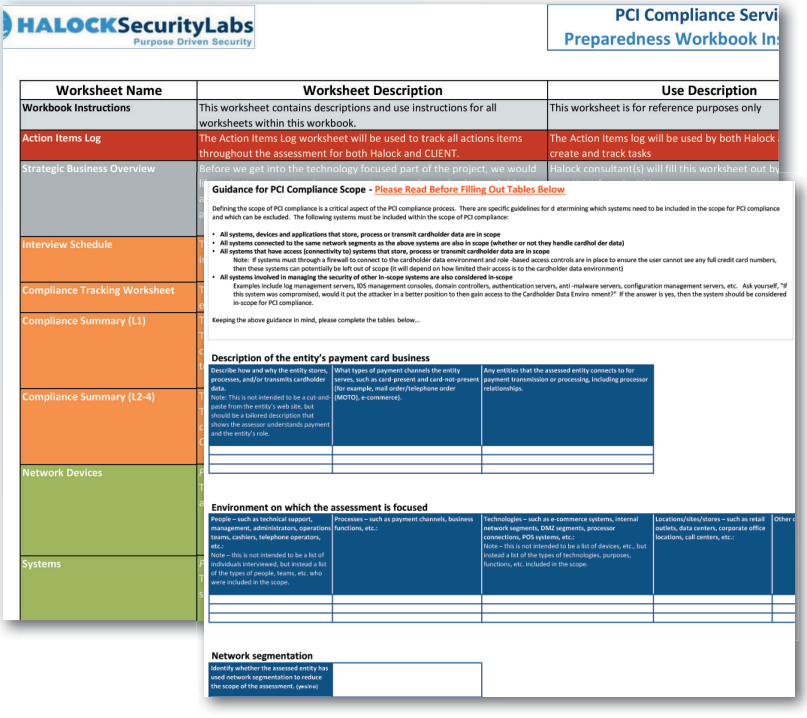
Based upon preliminary information gathering, the following organizations appear to be classified as Service Provide CLIENTNAME for PCI compliance:

Company Name	Services Provided	Status 1	PCI Compliance Status
Salesforce.com	Hosting the Application used by CLIENTNAME to capture and process payments from customers	G	Listed with Visa as a PCI Compliant Service Provider as of July 31, 2018 against version 3.2 of the PCI DSS for the following services: • Hosting Provider: Applications software • Hosting Provider: Shared Hosting Provider
Application	The vendor has maintenance access to their application and the storage repository of data	R	Not a compliant PCI Service Provider this time.

PCI DSS PREPAREDNESS ASSESSMENT

A PCI DSS Preparedness Assessment is designed to **uncover elements of the existing environment** and security controls that are not in line with the PCI Data Security Standard by **evaluating whether each of the 250+ specific requirements within the PCI DSS** are being addressed appropriately.

Using the PCI audit framework as a guide, this assessment consists of data gathering and interview-style reviews of the existing environment. A hands-on analysis of systems on a sampling basis can also be included. By gathering information about the present configuration of systems and security controls, HALOCK can determine where issues exist and will **provide appropriate recommendations** for correcting those issues.


HALOCKSecurityLabs
Purpose Driven Security

PCI Compliance Servi
Preparedness Workbook In

Worksheet Name	Worksheet Description	Use Description
Workbook Instructions	This worksheet contains descriptions and use instructions for all worksheets within this workbook.	This worksheet is for reference purposes only
Action Items Log	The Action Items Log worksheet will be used to track all actions items throughout the assessment for both Halock and CLIENT.	The Action Items log will be used by both Halock create and track tasks
Strategic Business Overview	Before we get into the technology focused part of the project, we would	Halock consultant(s) will fill this worksheet out by
Interview Schedule		
Compliance Tracking Worksheet		
Compliance Summary (L1)		
Compliance Summary (L2-4)		
Network Devices		
Systems		

Guidance for PCI Compliance Scope - Please Read Before Filling Out Tables Below

Defining the scope of PCI compliance is a critical aspect of the PCI compliance process. There are specific guidelines for d etermining which systems need to be included in the scope for PCI compliance and which can be excluded. The following systems must be included within the scope of PCI compliance:

- All systems, devices and applications that store, process or transmit cardholder data are in scope
- All systems connected to the same network segments as the above systems are also in scope (whether or not they handle cardhol der data)
- All systems that have access (connectivity to) systems that store, process or transmit cardholder data are in scope
  Note: If systems must through a firewall to connect to the cardholder data environment and role -based access controls are in place to ensure the user cannot see any full credit card numbers, then these systems can potentially be left out of scope (it will depend on how limited their access is to the cardholder data environment)
- All systems involved in managing the security of other in-scope systems are also considered in-scope
  Examples include log management servers, IDS management consoles, domain controllers, authentication servers, anti -malware servers, configuration management servers, etc. Ask yourself, "If this system was compromised, would it put the attacker in a better position to then gain access to the Cardholder Data Enviro nment?" If the answer is yes, then the system should be considered in-scope for PCI compliance.

Keeping the above guidance in mind, please complete the tables below...

Description of the entity's payment card business

Describe how and why the entity stores, processes, and/or transmits cardholder data. Note: This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.	What types of payment channels the entity serves, such as card-present and card-not-present (for example, mail order/telephone order (MOTO), e-commerce).	Any entities that the assessed entity connects to for payment transmission or processing, including processor relationships.

Environment on which the assessment is focused

People – such as technical support, management, administrators, operations teams, cashiers, telephone operators, etc.: Note – this is not intended to be a list of individuals interviewed, but instead a list of the types of people, teams, etc. who were included in the scope.	Processes – such as payment channels, business functions, etc.:	Technologies – such as e-commerce systems, internal network segments, DMZ segments, processor connections, POS systems, etc.: Note – this is not intended to be a list of devices, etc., but instead a list of the types of technologies, purposes, functions, etc. included in the scope.	Locations/sites/stores – such as retail outlets, data centers, corporate office locations, call centers, etc.:	Other c

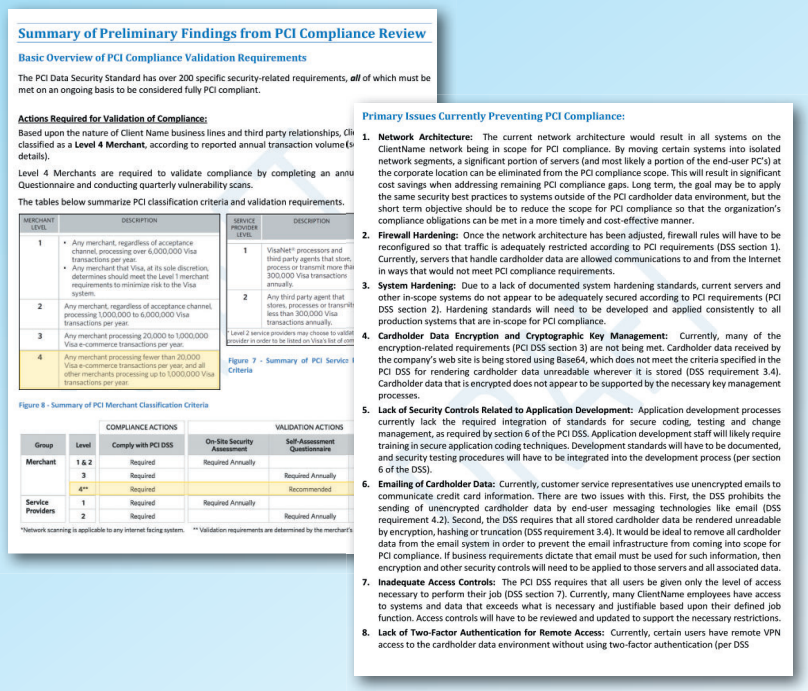
Network segmentation

Identify whether the assessed entity has used network segmentation to reduce the scope of the assessment. (yes/no)	

PCI DSS REMEDIATION PROGRAM MANAGEMENT

You've assessed your PCI profile and have identified the gaps preventing you from being PCI compliant. How do you get from here to the finish line? HALOCK offers a full suite of PCI compliance remediation and security program management solutions to **help you identify and close those PCI compliance gaps**.

HALOCK's security engineers work closely with your staff to identify, design, and/or implement the appropriate technical solutions to achieve your goal. Plus, we help you manage remediation efforts via security project and portfolio management, business analysis, process improvement, or even our Virtual Chief Information Security Officer (vCISO) service.



Summary of Preliminary Findings from PCI Compliance Review

Basic Overview of PCI Compliance Validation Requirements

The PCI Data Security Standard has over 200 specific security-related requirements, ***all*** of which must be met on an ongoing basis to be considered fully PCI compliant.

Actions Required for Validation of Compliance:

Based upon the nature of Client Name business lines and third party relationships, Cli… classified as a **Level 4 Merchant**, according to reported annual transaction volume (s… details).

Level 4 Merchants are required to validate compliance by completing an annu… Questionnaire and conducting quarterly vulnerability scans.

The tables below summarize PCI classification criteria and validation requirements.

MERCHANT LEVEL	DESCRIPTION
1	• Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa transactions per year. • Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1,000,000 Visa transactions per year.

SERVICE PROVIDER LEVEL	DESCRIPTION
1	VisaNet† processors and third party agents that store, process or transmit more tha… 300,000 Visa transactions annually.
2	Any third party agent that stores, processes or transmits… less than 300,000 Visa transactions annually.

Level 2 service providers may choose to validate… provider in order to be listed on Visa's list of com…

Figure 7 - Summary of PCI Service … Criteria

Figure 8 - Summary of PCI Merchant Classification Criteria

		COMPLIANCE ACTIONS	VALIDATION ACTIONS	
Group	Level	Comply with PCI DSS	On-Site Security Assessment	Self-Assessment Questionnaire
Merchant	1 & 2	Required	Required Annually	
	3	Required		Required Annually
	4**	Required		Recommended
Service Providers	1	Required	Required Annually	
	2	Required		Required Annually

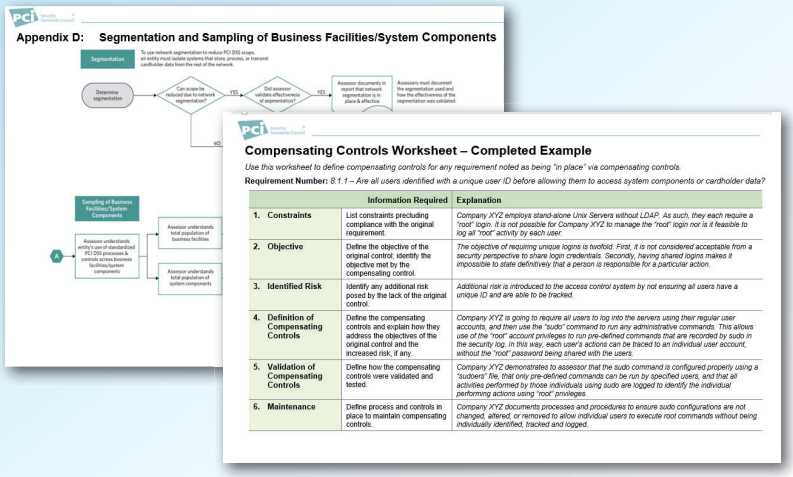
*Network scanning is applicable to any internet facing system. ** Validation requirements are determined by the merchant's …

Primary Issues Currently Preventing PCI Compliance:

1. **Network Architecture:** The current network architecture would result in all systems on the ClientName network being in scope for PCI compliance. By moving certain systems into isolated network segments, a significant portion of servers (and most likely a portion of the end-user PC's) at the corporate location can be eliminated from the PCI compliance scope. This will result in significant cost savings when addressing remaining PCI compliance gaps. Long term, the goal may be to apply the same security best practices to systems outside of the PCI cardholder data environment, but the short term objective should be to reduce the scope for PCI compliance so that the organization's compliance obligations can be met in a more timely and cost-effective manner.
2. **Firewall Hardening:** Once the network architecture has been adjusted, firewall rules will have to be reconfigured so that traffic is adequately restricted according to PCI requirements (DSS section 1). Currently, servers that handle cardholder data are allowed communications to and from the Internet in ways that would not meet PCI compliance requirements.
3. **System Hardening:** Due to a lack of documented system hardening standards, current servers and other in-scope systems do not appear to be adequately secured according to PCI requirements (PCI DSS section 2). Hardening standards will need to be developed and applied consistently to all production systems that are in-scope for PCI compliance.
4. **Cardholder Data Encryption and Cryptographic Key Management:** Currently, many of the encryption-related requirements (PCI DSS section 3) are not being met. Cardholder data received by the company's web site is being stored using Base64, which does not meet the criteria specified in the PCI DSS for rendering cardholder data unreadable wherever it is stored (DSS requirement 3.4). Cardholder data that is encrypted does not appear to be supported by the necessary key management processes.
5. **Lack of Security Controls Related to Application Development:** Application development processes currently lack the required integration of standards for secure coding, testing and change management, as required by section 6 of the PCI DSS. Application development staff will likely require training in secure application coding techniques. Development standards will have to be documented, and security testing procedures will have to be integrated into the development process (per section 6 of the DSS).
6. **Emailing of Cardholder Data:** Currently, customer service representatives use unencrypted emails to communicate credit card information. There are two issues with this. First, the DSS prohibits the sending of unencrypted cardholder data by end-user messaging technologies like email (DSS requirement 4.2). Second, the DSS requires that all stored cardholder data be rendered unreadable by encryption, hashing or truncation (DSS requirement 3.4). It would be ideal to remove all cardholder data from the email system in order to prevent the email infrastructure from coming into scope for PCI compliance. If business requirements dictate that email must be used for such information, then encryption and other security controls will need to be applied to those servers and all associated data.
7. **Inadequate Access Controls:** The PCI DSS requires that all users be given only the level of access necessary to perform their job (DSS section 7). Currently, many ClientName employees have access to systems and data that exceeds what is necessary and justifiable based upon their defined job function. Access controls will have to be reviewed and updated to support the necessary restrictions.
8. **Lack of Two-Factor Authentication for Remote Access:** Currently, certain users have remote VPN access to the cardholder data environment without using two-factor authentication (per DSS

PCI VALIDATION

Validation takes place through an Onsite Assessment and Report on Compliance (for organizations with a large transaction volume), or a Self-Assessment Questionnaire. Regardless of which requirement applies to you, our Qualified Security Advisors (QSAs) can help you compile the required evidence, audit security controls, and **author the appropriate compliance reports to register and demonstrate your PCI compliance**.



Appendix D: Segmentation and Sampling of Business Facilities/System Components

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as being "in place" via compensating controls.

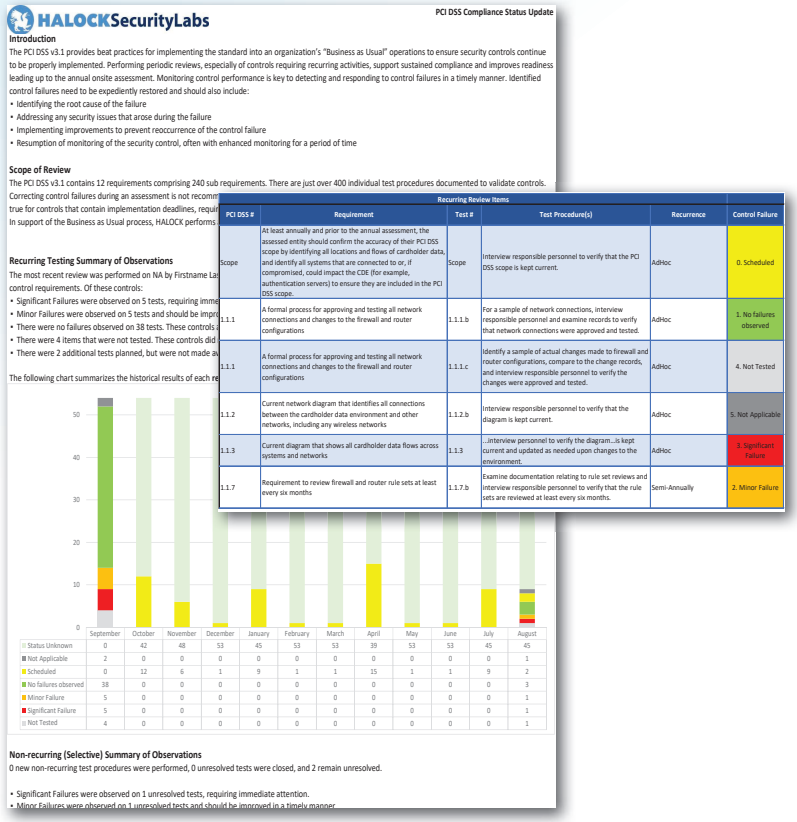
Requirement Number: *8.1.1 – Are all users identified with a unique user ID before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers using their regular user accounts, and then use the "sudo" command to run any administrative commands. This allows use of the "root" account privileges to run pre-defined commands that are recorded by sudo in the security log. In this way, each user's actions can be traced to an individual user account, without the "root" password being shared with the users.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the sudo command is configured properly using a "sudoers" file, that only pre-defined commands can be run by specified users, and that all activities performed by those individuals using sudo are logged to identify the individual performing actions using "root" privileges.*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure sudo configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually identified, tracked and logged.*

PCI COMPLIANCE MAINTENANCE

With the new PCI DSS v4.0, there are compliance activities that specifically require ongoing operational requirements. The most common causes for noncompliance during the annual onsite validation are control failures related to these activities. The Compliance Maintenance Program is conducted on a regular basis to monitor and assess those requirements and tasks. The efforts performed under this program support PCI DSS "Business as Usual" activities, establish a proactive approach to validating required compliance tasks, and identify control failures in a timely manner that otherwise would result in non-compliance.

The HALOCK PCI DSS Compliance Program provides a process for achieving and maintaining PCI compliance that controls costs, maximizes return on security investment, and provides measurable indicators of progress. It is available as a one year program with monthly, bi-monthly or quarterly sessions.



HALOCKSecurityLabs

PCI DSS Compliance Status Update

Introduction

The PCI DSS v3.1 provides best practices for implementing the standard into an organization's "Business as Usual" operations to ensure security controls continue to be properly implemented. Performing periodic reviews, especially of controls requiring recurring activities, support sustained compliance and improves readiness leading up to the annual onsite assessment. Monitoring control performance is key to detecting and responding to control failures in a timely manner. Identified control failures need to be expediently restored and should also include:

- Identifying the root cause of the failure
- Addressing any security issues that arose during the failure
- Implementing improvements to prevent reoccurrence of the control failure
- Resumption of monitoring of the security control, often with enhanced monitoring for a period of time

Scope of Review

The PCI DSS v3.1 contains 12 requirements comprising 240 sub requirements. There are just over 400 individual test procedures documented to validate controls.

Correcting control failures during an assessment is not recomm… true for controls that contain implementation deadlines, requi…

In support of the Business as Usual process, HALOCK performs …

Recurring Testing Summary of Observations

The most recent review was performed on NA by Firstname La… control requirements. Of these controls:

- Significant Failures were observed on 5 tests, requiring imme…
- Minor Failures were observed on 5 tests and should be impro…
- There were no failures observed on 38 tests. These controls …
- There were 4 items that were not tested. These controls did …
- There were 2 additional tests planned, but were not made av…

The following chart summarizes the historical results of each re…

Recurring Review Items

PCI DSS #	Requirement	Test #	Test Procedure(s)	Recurrence	Control Failure
Scope	At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope.	Scope	Interview responsible personnel to verify that the PCI DSS scope is kept current.	AdHoc	0. Scheduled
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.b	For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	AdHoc	1. No failures observed
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.c	Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	AdHoc	4. Not Tested
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.b	Interview responsible personnel to verify that the diagram is kept current.	AdHoc	5. Not Applicable
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	1.1.3	…interview personnel to verify the diagram…is kept current and updated as needed upon changes to the environment.	AdHoc	3. Significant Failure
1.1.7	Requirement to review firewall and router rule sets at least every six months	1.1.7.b	Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	Semi-Annually	2. Minor Failure

	September	October	November	December	January	February	March	April	May	June	July	August
Status Unknown	0	42	48	53	45	53	53	39	53	53	45	45
Not Applicable	2	0	0	0	0	0	0	0	0	0	0	1
Scheduled	0	12	6	1	9	1	1	15	1	1	9	2
No failures observed	38	0	0	0	0	0	0	0	0	0	0	3
Minor Failure	5	0	0	0	0	0	0	0	0	0	0	1
Significant Failure	5	0	0	0	0	0	0	0	0	0	0	1
Not Tested	4	0	0	0	0	0	0	0	0	0	0	1

Non-recurring (Selective) Summary of Observations

0 new non-recurring test procedures were performed, 0 unresolved tests were closed, and 2 remain unresolved.

- Significant Failures were observed on 1 unresolved tests, requiring immediate attention.
- Minor Failures were observed on 1 unresolved tests and should be improved in a timely manner.

HELPING YOU STAY COMPLIANT AND PROTECT YOUR DATA

Why HALOCK?

Our professional team makes the process easier for you. Benefit from an independent, experienced assessment that provides practical and actionable intelligence for a safer business environment.

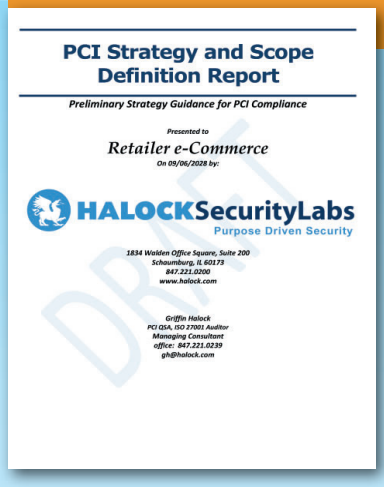
- Deep technical and operational understanding of PCI DSS requirements
- Proven methods, efficient tools and a tested delivery process
- Dedicated QSAs for your assessment program
- Integration with the HALOCK Penetration Testing team
- **Purpose Driven Security®** that focuses our attention on the underlying intent of each requirement as it relates to the particular circumstances of your business.

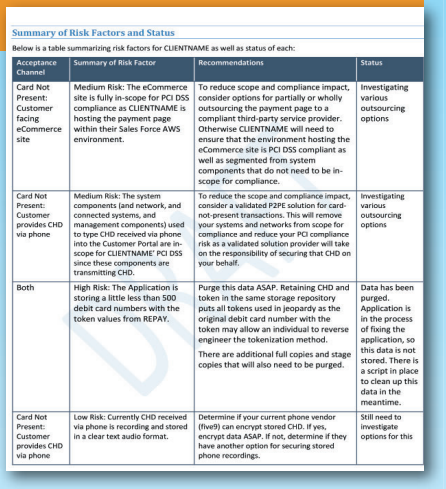
About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, and Security Engineering.

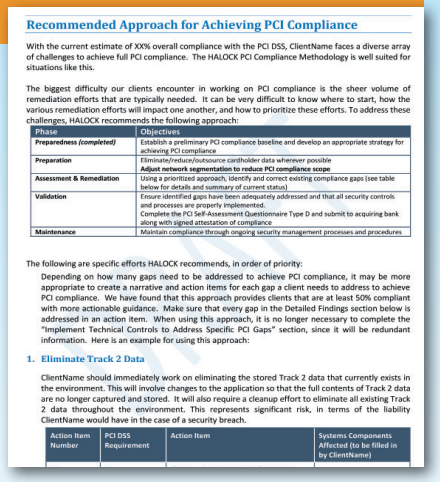
EDUCATION

STRATEGY





ASSESSMENT



VALIDATION

DELIVERABLES THAT MAKE SENSE.

HALOCK develops **comprehensive reports** that are fully customized for you. The reports outline PCI compliance issues identified during PCI compliance assessments and provides Recommendations for effective countermeasures if any controls are found to be missing or insufficient.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

halock.com