



# QUICK START GUIDE

---

## PCI Compliance Assessment Module

Instructions to Perform a PCI Compliance Assessment

# Contents

---

<b>Performing a PCI Compliance Assessment</b> .....	<b>3</b>
<u>PCI Compliance Assessment Overview</u> .....	3
What You Will Need .....	4
Risk Assessment vs. Risk Profile .....	5
PCI Risk Profile Use for Ongoing PCI Compliance Assessments .....	5
<u>Step 1 — Download and Install the Network Detective Application</u> .....	6
<u>Step 2 — Create a New Site</u> .....	6
<u>Step 3 — Start a PCI Compliance Assessment Project</u> .....	7
Use the PCI Compliance Assessment Checklist .....	7
<u>Step 4 — Collect Initial PCI Compliance Assessment Data</u> .....	8
<u>Step 5 — Cardholder Data Environment (CDE) Deep Scan</u> .....	13
<u>Step 6 — Collect Secondary Data</u> .....	14
<u>Step 7 — Document Exceptions</u> .....	14
<u>Step 8 — Generate Reports</u> .....	14
Note on Time to Generate Reports .....	16
<b>PCI Assessment Reports</b> .....	<b>17</b>
<u>Compliance Reports</u> .....	17
<u>Supporting Documentation</u> .....	19
Change Reports .....	21

# Performing a PCI Compliance Assessment

## PCI Compliance Assessment Overview

Network Detective's PCI Compliance Assessment Module combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a PCI Compliance Assessment, you will:

- Download and install the required tools
- Create a site and set up a PCI Compliance Assessment project
- Collect PCI Compliance Assessment data using the Network Detective Checklist
- Generate PCI Compliance Assessment reports

## What You Will Need

In order to perform a PCI Compliance Assessment, you will need the following components:

**Note:** You can access these at <https://www.rapidfiretools.com/nd>.

PCI Compliance Assessment Component	Description
<b>Network Detective</b>	The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites.
<b>PCI Data Collector</b>	The Network Detective PCI Data Collector is a windows application that performs the data collections (network, local 'quick', and local 'deep') for the PCI Compliance Module. Supports both Network and Computer scans.
<b>Push Deploy Tool</b>	The Network Detective Push-Deploy Tool pushes the local data collector to machines in a specified range and saves the scan files to a specified directory (which can also be a network share). The benefit of the tool is that a local scan can be run simultaneously on each computer from a centralized location.
<b>Surveys and Worksheets</b>	Surveys and worksheets contain questions that require investigation outside of an automated scan. You create and manage these documents directly from the Network Detective Application, where you can also import and export your responses to and from Word.

## Risk Assessment vs. Risk Profile

There are two types of PCI Compliance Assessments that can be performed:

Assessment Type	Description
<b>PCI Risk Assessment</b>	<p>A complete assessment that includes all worksheets and surveys.</p> <ul style="list-style-type: none"> <li>• Required at least annually</li> <li>• Recommended quarterly as part of a quarterly compliance review</li> <li>• Requires that all manual worksheets be completed</li> </ul> <p><b>Important:</b> Allow for at least an entire day to perform the assessment on a typical 15 user network</p>
<b>PCI Risk Profile</b>	<p>Updates a Risk Assessment to show progress in avoiding and mitigating risks - and finds new ones that may have otherwise been missed.</p> <ul style="list-style-type: none"> <li>• Does NOT require worksheets</li> <li>• Requires selecting a prior Risk Assessment (will use existing worksheets)</li> <li>• Requires less than 1 hour for a typical 15 user network</li> </ul> <p><b>Note:</b> You can only create a Risk Profile after you have first performed a Risk Assessment.</p>

## PCI Risk Profile Use for Ongoing PCI Compliance Assessments

A PCI Risk Analysis should be done no less than once a year. However, the Network Detective includes an abbreviated version of the PCI Risk Analysis assessment and reporting process within the Network Detective PCI Module. This process is called the PCI Risk Profile.

The PCI Risk Profile is designed to provide interim reporting in a streamlined and almost completely automated manner.

Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.

An important aspect of this abbreviated process is the need that the PCI Module has been already used to perform a PCI Risk Assessment of your customer's Cardholder Data Environment (CDE) on a previous occasion.

Follow these steps to perform a PCI Compliance Assessment:

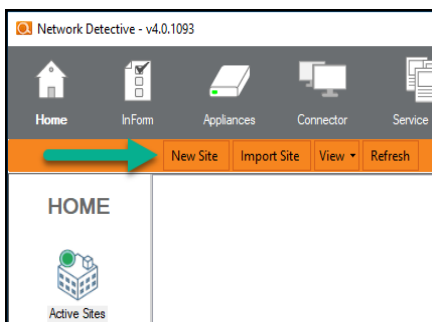
## Step 1 — Download and Install the Network Detective Application

Visit <https://www.rapidfiretools.com/nd>. Download and install the Network Detective Application.

## Step 2 — Create a New Site

To create a new site:

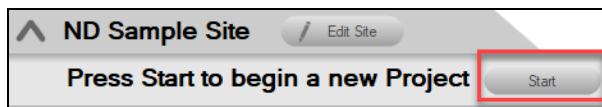
1. Open the Network Detective Application and log in with your credentials.
2. Click **New Site** to create a new Site for your assessment project.



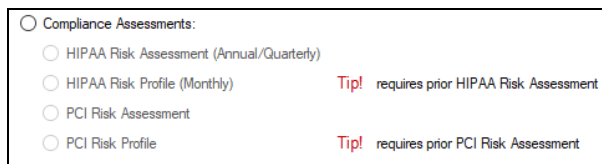
3. Enter a **Site Name** and click **OK**.

## Step 3 — Start a PCI Compliance Assessment Project

1. From within the Site Window, click **Start** to begin the assessment.



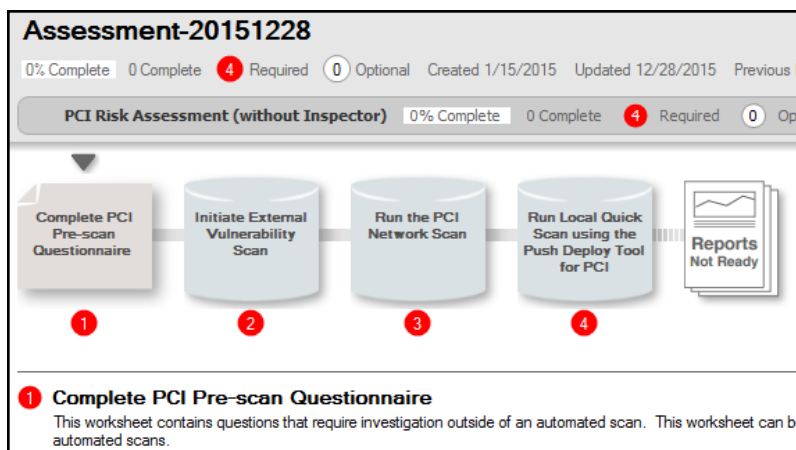
2. Next, select **Compliance Assessments**, and then select your chosen PCI Compliance Assessment.




3. Then follow the prompts presented in the Network Detective Wizard to start the new Assessment.

## Use the PCI Compliance Assessment Checklist

Once you begin the PCI Compliance Assessment, a **Checklist** appears in the Assessment Window. The **Checklist** presents the **Required** 1 and **Optional** 1 steps that are to be performed during the assessment process. The **Checklist** will be updated with additional steps to be performed throughout the assessment process.



Complete the required **Checklist Items** in the exact numerical order presented. Use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

When you complete a step, that item will be updated with a green check mark  in the checklist.



You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.

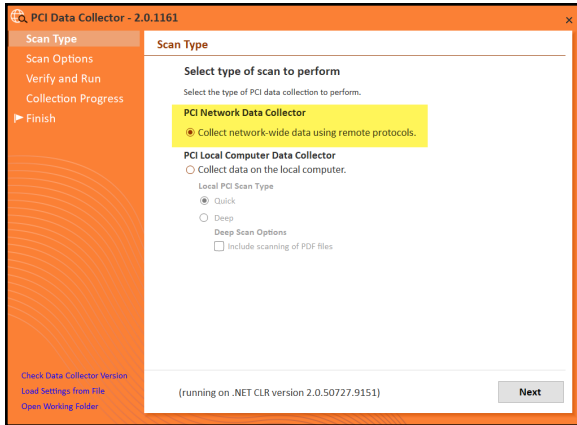


## Step 4 — Collect Initial PCI Compliance Assessment Data

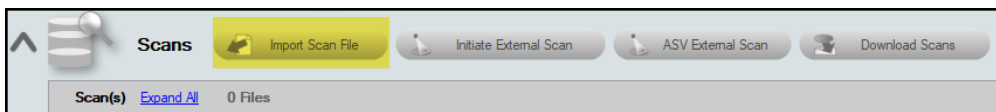
1. First complete the **PCI Pre-Scan Questionnaire**. View the assessment **Checklist** for updates and to track progress.
2. Initiate the **External Vulnerability Scan**.
3. Download, install, and run the **PCI Data Collector** as an Administrator. The PCI Data Collector is available at <https://www.rapidfiretools.com/nd>.
4. Select the **PCI Network Data Collector** option. Follow the prompts and run the PCI Network Scan.

**Note:** Take note of the output file location for the scan. This will be on your computer's Desktop by default.

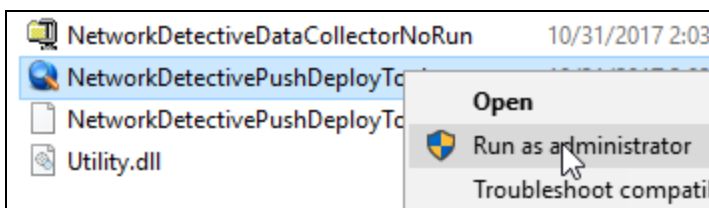




5. Import the **PCI Network Scan** results by clicking **Import Scan File** in the Assessment Window. Select the output file created in the step above.



6. Next, to perform the **PCI “Quick” Local Computer Scans** of computers on the network, download and install the **Push Deploy Tool** on your USB drive from <https://www.rapidfiretools.com/nd>.
7. Extract the contents of the **Push Deploy Tool** .ZIP file to a USB drive or directly to any machine on the target network.
8. Using the Run as Administrator option, run the **NetworkDetectivePushDeployTool.exe** contained within the folder named **NetworkDetectivePushDeployTool**.



**Important:** For the most comprehensive scan, you **MUST** run the Push Deploy Tool as an **ADMINISTRATOR**.

9. From the tool's **Settings and Configuration** window, select the **PCI “Quick” Scan** option. Specify the **Folder** to store resulting computer scan files, and enter the necessary **Administrator Credentials**. Click **Next**.

0.1128

### Settings and Configuration

**Scan Settings**

Storage Folder: \\Desktop\\Network Detective Push Deploy Tool

Scan Type:  Computer Scan  Security Scan Deep Scan Option:  Include the scanning of PDF Files  
 HIPAA Quick  HIPAA Deep  
 **PCI Quick**  PCI Deep  
 BDR Scan  PII Scan

**Credentials**

Access to remote machines to copy files and run collections are required. Username may contain a backslash if you wish to also specify a domain. Credentials will be checked per machine in the order they are specified here. The credentials entered here are not checked until a checkmark is placed next to them.

Username:  Password:

[Add](#)

[Add Current User](#) [Clear All](#)

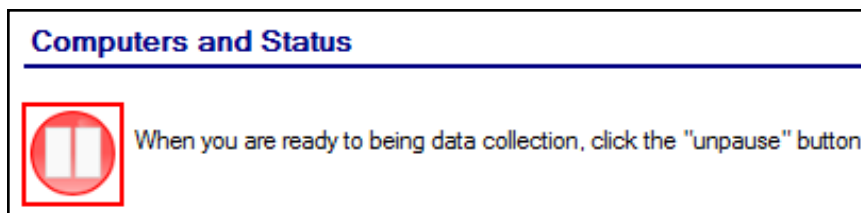
**Important:** For the **Push Deploy Tool** to push local scans to computers throughout the network, ensure that the following prerequisites are met:

- **Ensure that the Windows Management Instrumentation (WMI) service is running** and able to be managed remotely on the computers that you wish to scan. Sometimes Windows Firewall blocks Remote Management of WMI, so this service may need to be allowed to operate through the Firewall.
- **Admin\$ must be present on the computers you wish to scan**, and be accessible with the login credentials you provide for the scan. Push/Deploy relies on using the Admin\$ share to copy and run the data collector locally.
- **File and printer sharing must be enabled** on the computers you wish to scan.
- **For Workgroup based networks, the Administrator credentials for all workstations and servers that are to be scanned are recommended to be the same.** In cases where a Workgroup-based network does not have a one set of Administrator credentials for all machines to be scanned, use the Add option to add all of the Administrator credentials for the Workgroup. Multiple sets of Administrator credentials will be listed in the Credentials box.

**Tip:** For your convenience, create a shared network folder to centralize and store all scan results data files created by the **Push Deploy Tool**. Then reference this folder in the **Storage Folder** field to enable the local computer scan data files to be stored in this central location.

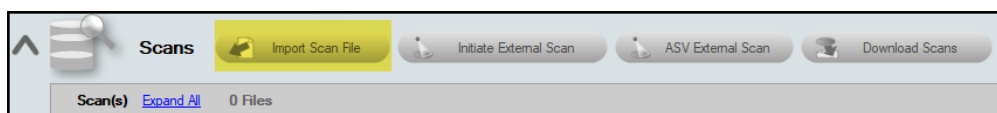
- In the **Computers and Status** window, set the **IP Address range** of the computers to be scanned and then run the scan. After defining the computer **IP Address range**, click the “**unpause**” button as instructed to start your data collection scan.

Alternatively, you can click the **Next** button where you will be prompted to start the data collection process.



After starting the data collection, the **Computers and Status** window will present the status of the scan for each computer selected for scanning.

- When the data collection process is complete, click **Next** to proceed to the **Collected Data Files** window. Click **Finish** to complete the **Push Deploy Tool** data collection process and to access the scan files produced.
- After the **PCI Quick Local Data Scan** is complete, click **Import Scan File** in the Assessment Window to import the scan results into the Assessment.

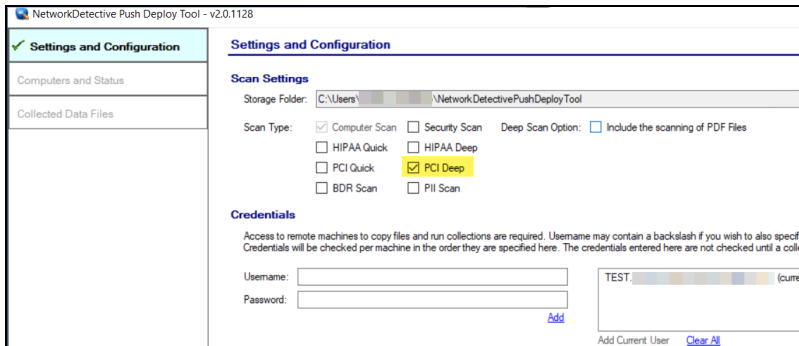


- Run the **PCI Data Collector** selecting **Quick Local Scan** on the computers that were unreachable and **Import** the scan results. This scan is optional if the unreachable computers are not to be a part of the PCI Assessment process.
- Complete the **Gate 1 Completion Worksheet**. The purpose of the Gate 1 Completion Worksheet is to confirm that the initial phase of the PCI assessment has been performed, including all optional scans, before proceeding to the next phase of the assessment process.

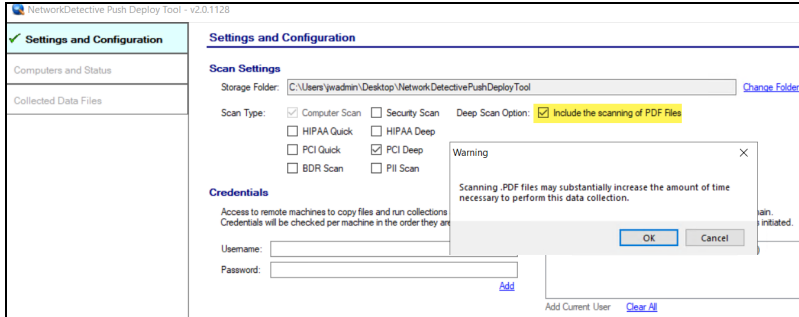
15. Complete the **PCI Post-Scan Questionnaire**.

## Step 5 — Cardholder Data Environment (CDE) Deep Scan

1. Complete the **Cardholder Data Environment ID Worksheet**. In this worksheet, you identify which system components are part of the Cardholder Data Environment.
2. Complete the **Deep Scan Selection Worksheet**. The computers selected in this worksheet will be scanned in the next step.
3. Using the **Push Deploy Tool**, initiate the **PCI Deep Scan** for selected systems.



4. Likewise, choose whether to include PDF files in the scan. Note that this may increase the total scan time.



**Tip:** The Push Deploy Tool is used to push Quick Scan and Deep Scan tasks out to a range of computers on the network. It is recommended that a network share Storage Folder be set up and used to store resulting scans.

5. After the **PCI Deep Scan** is complete, **Import the scan results** into the Assessment. This scan searches the selected local computers' files for cardholder data in the form of Primary Account Number (PAN) information.

6. Complete the **Gate 2 Completion Worksheet**. This worksheet confirms that you have performed the second phase of the PCI assessment before proceeding to the next phase.
7. Run the **PCI Data Collector** selecting the **Deep Local Scan** on the individual computers that were unreachable.

**Note:** Using the **Data Collector** to perform this scan is *Optional* if the unreachable computers are not to be a part of the PCI Assessment process.

## Step 6 — Collect Secondary Data

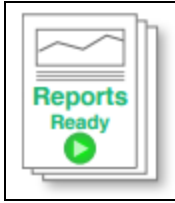
1. Complete the **User ID Worksheet**.
2. Complete the **Anti-Virus Capability Worksheet**.
3. Complete the **Necessary Functions Identification Worksheet**.
4. Complete the **Server Function ID Worksheet**.
5. Complete the **PAN Scan Worksheet**.
6. Complete the **External Port Security Worksheet**.
7. Complete the **PCI Verification Questionnaire**.

## Step 7 — Document Exceptions

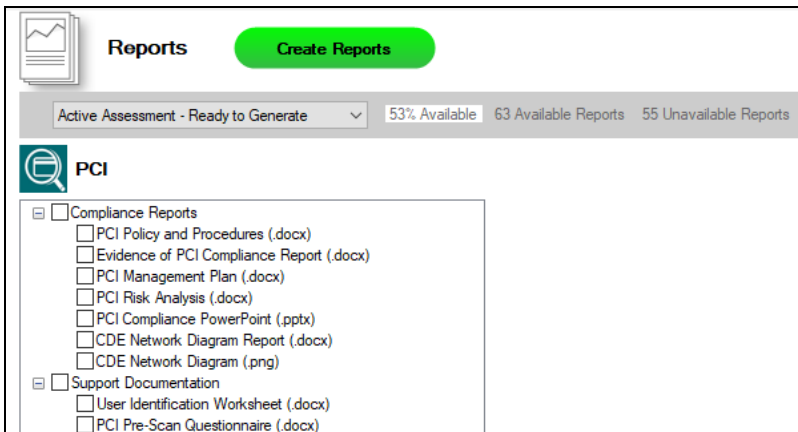
*Optional:* Complete the **Compensating Controls Worksheet**.

## Step 8 — Generate Reports

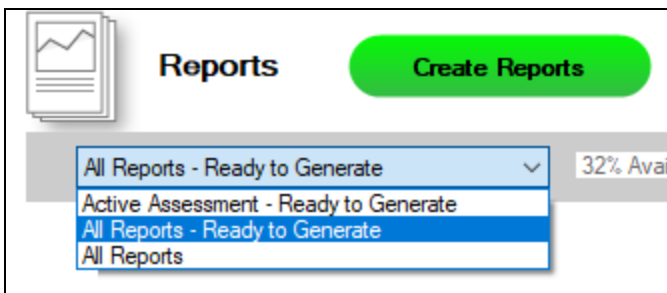
1. Run Network Detective and login with your credentials.
2. Then select the **Site** and go to the **Active Assessment Project**.
3. Click the Reports Ready button at the end of the assessment checklist.



4. Select which of the PCI Compliance Assessment reports that you want to generate.

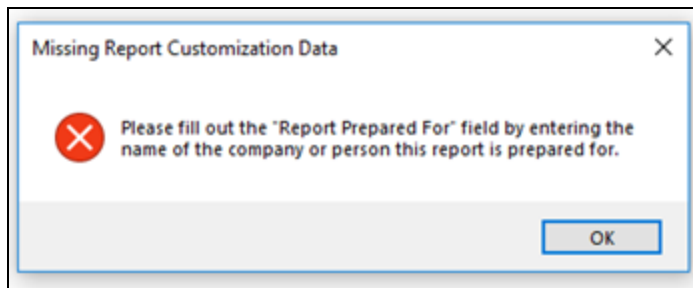


You can use the Reports drop-down menu to filter reports related to the active assessment project, reports that are ready to generate, or to browse all available reports.



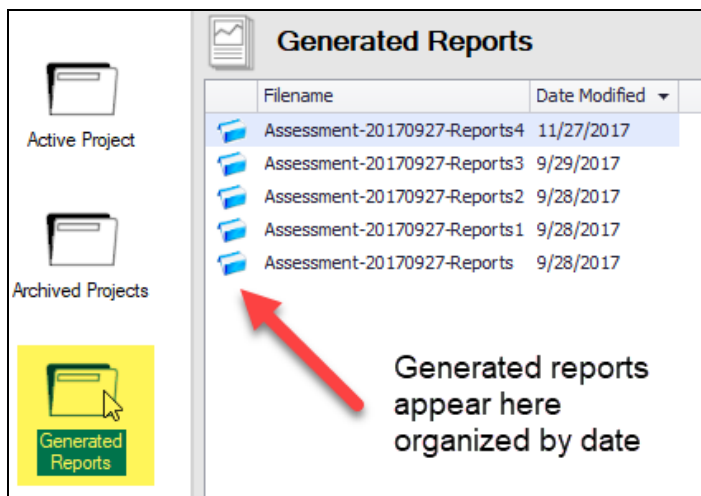
5. Click the **Create Reports** button and follow the prompts to generate the reports you selected.

- i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.



**Tip:** See the [Network Detective User Guide](#) for instructions on how to customize your reports with your company's branding.

Click **Generated Reports** from the left-hand Site menu to access previously generated reports. Double click a set of assessment reports to open the folder in Windows Explorer.



### Note on Time to Generate Reports

**Important:** Larger data sets will require more time to generate reports. If the data set is especially large — in the range of several thousand users, for example — a full set of reports may take several hours to complete.



# PCI Assessment Reports

The PCI Assessment Module can generate the following reports and supporting documents:

## Compliance Reports

These reports show where you are in achieving PCI compliance. In addition, these documents identify and prioritize issues that must be remediated to address PCI related security vulnerabilities through ongoing managed services.

Report Name	Description
<b>Evidence of PCI Compliance</b>	Just performing PCI-compliant tasks is not enough. Audits and investigations require evidence that compliance tasks have been carried out and completed. Documentation must be kept for six years. The Evidence of Compliance includes log-in files, patch analysis, user & computer information, and other source material to support your compliance activities. When all is said and done, the proof to proper documentation is accessibility and the detail to satisfy an auditor or investigator included in this report.
<b>PCI Policies &amp; Procedures Document</b>	<p>The Policy and Procedures are the best practices that our industry experts have formulated to comply with the technical requirements of the PCI DSS. The policies spell out what your organization will do while the procedures detail how you will do it. In the event of a PCI Compliance audit, the first things an auditor will inspect are the Policies and Procedures documentation. This is more than a suggested way of doing business.</p> <p>The Policies and Procedures have been carefully thought out and vetted, referencing specific sections in the PCI DSS Requirements and supported by the other reports include with the PCI Compliance module.</p>
<b>PCI Post-Scan Questionnaire</b>	The Post-Scan Questionnaire contains the documented responses to list of questions that were formulated based on the results of scans that have been performed.
<b>PCI Pre-scan Questionnaire</b>	This questionnaire contains a list of questions about physical and technical security that cannot be gathered automatically. The survey includes questions ranging from how facility controls

Report Name	Description
	access, firewall information, application development, to authentication and change management standards.
<b>PCI Compliance PowerPoint</b>	This PowerPoint slide deck presents a visual overview of the PCI assessment.
<b>PCI Risk Analysis Report</b>	<p>PCI is a risk-based security framework and the production of a Risk Analysis is one of primary requirements for PCI compliance. In fact, a Risk Analysis is the foundation for the entire security program. It identifies the locations of electronic stores of, and/or the transmission of Cardholder Data and vulnerabilities to the security of the data, threats that might act on the vulnerabilities, and estimates both the likelihood and the impact of a threat acting on a vulnerability.</p> <p>The Risk Analysis helps Card Processing Merchants and their 3rd party Service Providers to identify the components of the Cardholder Data Environment (CDE), how the data moves within, and in and out of the organization. It identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of Cardholder Data at rest and/or during its transmission. The Risk Analysis must be run or updated at least annually, more often if anything significant changes that could affect one or more system components in the CDE itself.</p>

## Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
<p><b>Antivirus Capability Identification Worksheet</b></p>	<p>This worksheet enables the PCI readiness specialist to inspect and document the features and capabilities Antivirus Software deployed on computers throughout network both in and out of the Cardholder Data Environment (CDE).</p>
<p><b>Cardholder Data Environment ID Worksheet</b></p>	<p>The Cardholder Data Environment Worksheet takes the list of computers gathered by the Data Collector and lets you identify those that store or access Cardholder Data. This is an effective tool in developing data management strategies including secure storage and encryption.</p>
<p><b>Compensating Controls Worksheet</b></p>	<p>The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to enable PCI compliance. This worksheet allows the PCI Compliance readiness specialist to document explanations on suspect items. The readiness specialist is enabled to document and explain why various discovered items are not true issues and possible false positives.</p> <p>These exceptions can be documented on an item by item level (for example: at the granularity at users, ports, applications, etc.). The Compensating Control Worksheet compiles the issues discovered by the PCI Compliance Data Collection including the completion of the questionnaires and worksheets.</p> <p>The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements. The Compensating Controls Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk. The process is consistent with industry standard PCI assessment and risk management processes.</p>
<p><b>Deep Scan Selection Worksheet</b></p>	<p>The PCI Deep Scan, which includes a Primary Account Number (PAN) scanner used to identify files that are suspected of</p>

Report Type	Description
	containing Cardholder Data. This scan should be run on all computers in the Cardholder Data Environment (CDE) that can be accessed along with a sampling of computers outside the CDE. This worksheet enables the documentation of the computers that should be scanned with the PCI Deep Scan.
<b>External Network Vulnerability Scan Detail by Issue</b>	Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.
<b>External Port Security Worksheet</b>	This worksheet allows you to document business justifications for all of the allowed ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.
<b>Necessary Functions Worksheet</b>	For each server in the Cardholder Data Environment (CDE), this worksheet presents startup applications, services, and other functions, allowing you to identify functions which are unnecessary for the server to fulfill its primary function.
<b>PAN Scan Verification Worksheet</b>	The Deep Scan includes a Personal Account Number (PAN) scanner. The results of the PAN scan are presented in this worksheet, allowing you the opportunity to investigate and verify if the detected numbers are truly an identifying account number/credit card.
<b>PCI Verification Questionnaire</b>	<p>The PCI Verification Worksheet contains a list of PCI compliance assessment issues that were flagged by the PCI Module throughout the assessment process as concerns that required additional information to be documented. This additional documentation was necessary to address risks that were identified or to establish that system components, security measures, and software are PCI compliant.</p> <p>Some of the issues may include: Web-based management interfaces and security, cardholder data environment (CDE) firewall configuration, network diagram verification, security features associated with the use of insecure protocols, and anti-virus verification to just name a few.</p>
<b>Server Function ID Worksheet</b>	Per PCI DSS Requirement 2.1.1, only one function per server can be implemented in order to prevent functions that require

Report Type	Description
	<p>different security levels from co-existing on the same server. The Service Function Identification worksheet enables you to document server roles (web server, database server, DNS server, etc.) and the functions activated on each server (real/physical or virtual) within the Cardholder Data Environment (CDE).</p>
<p><b>User Identification Worksheet</b></p>	<p>The User Identification Worksheet takes the list of users gathered by the Data Collector and lets you identify whether they are an employee or vendor. Users who should have been terminated and should have had their access terminated can also be identified. This is an effective tool to determine if unauthorized users have access to protected information.</p> <p>It also is a good indicator of the efforts the organization goes to so terminated employees and vendors have their access quickly disabled. Another benefit is that you can review the user list to identify generic logons, such as Admin, Billing Office, etc., which are not allowed by PCI since each user is required to be uniquely identified.</p>

## Change Reports

Report Name	Description
<p><b>Baseline PCI Management Plan</b></p>	<p>Based on the findings in the Risk Analysis, the organization must create a Risk Management Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, Network Detective provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Management plan defines the strategies and tactics the organization will use to address its risks.</p>
<p><b>Baseline PCI Risk Profile</b></p>	<p>A Risk Analysis is a snapshot in time, while compliance is an ongoing effort. The Network Detective PCI Risk Profile updates a Risk Analysis to show progress in avoiding and mitigating risks. Whether performed monthly or quarterly, the Risk Profile updates the Risk Analysis and documents progress in addressing previously identified risks, and finds new ones that may have otherwise been missed and resulted in a data breach.</p>