QUICK START GUIDE

PCI Compliance Assessment Module with Inspector

Instructions to Perform a PCI Compliance Assessment
Contents

Performing a PCI Compliance Assessment (with Inspector) ...... 3

PCI Compliance Assessment Overview ......................................................... 3
   What You Will Need ................................................................................. 4
   Risk Assessment vs. Risk Profile ......................................................... 5
   PCI Risk Profile Use for Ongoing PCI Compliance Assessments ...................... 5

Step 1 — Download and Install the Network Detective Application .................. 6

Step 2 — Create a New Site ......................................................................... 6

Step 3 — Add Inspector Appliance .................................................................. 7

Step 4 — Start a PCI Compliance Assessment Project .................................... 8
   Use the PCI Compliance Assessment Checklist ........................................... 8

Step 5 — Collect Initial PCI Compliance Assessment Data ............................ 9

Step 6 — Cardholder Data Environment (CDE) Deep Scan ................................ 11

Step 7 — Collect Secondary Data .................................................................. 11

Step 8 — Document Exceptions ................................................................... 12

Step 9 — Generate Reports ......................................................................... 12

Performing an ASV Scan and Downloading ASV Scan Reports .................... 15
   Setting Up and Performing an ASV Scan ............................................... 15
   Setting Up Access to Your ServerScan ASV Scan Account to View and Download Reports ................................................................. 19
   Setting Up Your ASV Reports to include your Company Information ........... 21
   Notification that Your ASV Scan has Started .......................................... 22
   Viewing the Results of your ASV Scan .................................................. 22
   Performing an ASV Rescan using ServerScan .......................................... 26

PCI Assessment Reports .............................................................................. 31

   Compliance Reports ................................................................................. 31

   Supporting Documentation ....................................................................... 34
Performing a PCI Compliance Assessment (with Inspector)

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](https://www.rapidfiretools.com/nd).

<table>
<thead>
<tr>
<th>PCI Compliance Assessment Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Detective</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PCI Data Collector</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Inspector Appliance</strong></td>
<td>The Inspector Appliance is an appliance-based system used for performing scheduled IT assessment scans and deeper dive diagnostics. The Inspector performs scans from the point-of-view of the client’s internal network.</td>
</tr>
<tr>
<td><strong>Surveys and Worksheets</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Risk Assessment vs. Risk Profile

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

<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Risk Assessment</td>
<td>A complete assessment that includes all worksheets and surveys.</td>
</tr>
<tr>
<td></td>
<td>• Required at least annually</td>
</tr>
<tr>
<td></td>
<td>• Recommended quarterly as part of a quarterly compliance review</td>
</tr>
<tr>
<td></td>
<td>• Requires that all manual worksheets be completed</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> Allow for at least an entire day to perform the assessment on a typical 15 user network</td>
</tr>
<tr>
<td>PCI Risk Profile</td>
<td>Updates a Risk Assessment to show progress in avoiding and mitigating risks - and finds new ones that may have otherwise been missed.</td>
</tr>
<tr>
<td></td>
<td>• Does NOT require worksheets</td>
</tr>
<tr>
<td></td>
<td>• Requires selecting a prior Risk Assessment (will use existing worksheets)</td>
</tr>
<tr>
<td></td>
<td>• Requires less than 1 hour for a typical 15 user network</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can only create a Risk Profile after you have first performed a Risk Assessment.</td>
</tr>
</tbody>
</table>

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 — Add Inspector Appliance

Next, associate an Inspector with the Site. To do this:

1. From within the newly created Site, click the chevron button to show the Site Configuration Options.

2. Next, click **Add**. The Add Appliance window will appear.

3. Use the drop-down menu to select the Appliance you wish to associate with the site.

**Important:** Before starting your first assessment using the PCI Module, be sure to update your Inspector device to the latest version.
Step 4 — Start a PCI Compliance Assessment Project

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

   ![Start button](image)

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** and **Optional** 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.

![Checklist](image)
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.

![Checklist](image)

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

---

### Step 5 — 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**.

   **Note:** In cases where your client requires an External Vulnerability Scan to be completed by a PCI DSS Approved Scanning Vendor (ASV), based on availability, an ASV Scan may be initiated from the PCI Module’s Assessment Window. See "**Performing an ASV Scan and Downloading ASV Scan Reports**" on page 15 for more information.

3. **Optional:** Initiate the **Internal Vulnerability Scan** on the Inspector Appliance and download the results using the **Download Scans** feature.

   **EXAMPLE:**
   To initiate scans using an appliance, follow these steps:
i. From the Scans bar, click **Initiate Appliance Scan**.

   ![Initiate Appliance Scan](image)

ii. Click **Create Scan Task**.

   ![Create Scan Task](image)

iii. Select your desired scan task and follow all prompts until the scan has been scheduled or initiated.

   ![Select Scan Task](image)

iv. When the scan has finished, download the scan results into the Assessment using the **Download Scans** button.

   ![Download Scans](image)

4. Initiate the **PCI Network Scan with Layer 2/3 Discovery** on the Inspector appliance and download the scans results into the Assessment using the **Download Scans** feature.

5. Initiate the **Push Quick Local Scans for PCI** on the Inspector appliance and download the scans results into the Assessment using the **Download Scans** feature.

6. **Optional:** Using the **Run as Administrator** option, run the **PCI Data Collector** selecting Quick Local Scan on the computers that were unreachable and Import the scan files into the Assessment.

7. Complete the **Gate 1 Completion Verification 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.

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

### Step 6 — 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. Initiate the **Push Deep Local Scan for PCI** for selected systems and download scans using the **Download Scans** feature. This scan searches the selected local computers' files for cardholder data in the form of Primary Account Number (PAN) information.

4. 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.

5. 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.

### Step 7 — 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 8 — Document Exceptions

*Optional: Complete the Compensating Controls Worksheet.*

Step 9 — 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 before generating reports.

   ![Missing Report Customization Data](image)

   **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.
Generated reports appear here organized by date
Performing an ASV Scan and Downloading ASV Scan Reports

In cases where your client requires an **External Vulnerability Scan** to be completed by a PCI DSS Approved Scanning Vendor (ASV), based on availability, an **ASV Scan** may be initiated from the PCI Module’s **Assessment window**. **ServerScan**, a RapidFire Tools, Inc. partner, will be performing the **ASV External Vulnerability Scan** on the Host/IP Address Range you specify in an **ASV Scan Request** as outlined in the process below.

**Note:** Prior to performing an ASV Scan, it is recommended that you perform an External Vulnerability Scan using the PCI Assessment Module as a part of your PCI Assessment and remediate any identified vulnerabilities.

Setting Up and Performing an ASV Scan

Follow these steps to use the PCI Assessment Module to initiate a request for an **ASV Scan**:

1. Select **ASV External Scan** option to request that an **External Scan** be performed.
   
   ![Request ASV External Scan](image)

   The **Request ASV External Scan** window is displayed.

2. Select the Add Host/IP link and the **Add IP Address or Host** window is displayed.

3. Enter the **IP Address** and select **Add**.
Confirm that the IP Address is added to list in the Request ASV External Scan window.

4. Then select the Next button to proceed to the next step.

5. In the Request ASV External Scan window, enter in your Email, Telephone Number, and any Special instructions, and select the Authorize the Scan Affirmation.

6. Next, select the Submit button to submit your ASV Scan Request.
If you have used the Network Detective **ASV Scan** feature before and have a ServerScan account, use the email address that you have associated with this account.

7. You will be presented with a Confirm window stating that you should check the **Host/IP Addresses** that you have selected for your ASV Scan(s) before finalizing with your **ASV Scan request**.

![Confirm window](image)

8. Select the **OK** button to proceed. You may select **Cancel** to go to the previous step.

   The **Submitting Scan Request** window will be displayed noting your submissions progress while your **ASV Scan Request** is submitted.

![Submitting Scan Request window](image)

Upon acceptance of the **Scan Request's** submission, you will receive confirmation that your scan has been submitted.

![ASV External Scan Request Submitted](image)

**Important:** It may take up to 30-60 minutes during the business hours of 9am-5pm Mountain Time (MT) for your ASV Scan request submission to be confirmed. Any scan requests submitted outside of these business hours will be processed the next business day.
Tip: If you already have used the ASV Scan feature in the past and have a ServerScan ASV Scan account, please proceed to "Notification that Your ASV Scan has Started" on page 22.

After your ASV Scan Request has been submitted, you will receive an email notification from RapidFire Tools, Inc. stating that your ASV Scan Request has been submitted to ServerScan for processing.

A listing of your ASV Scan Request will also be listed under the Scans Bar in the PCI Assessment window.

9. ServerScan, a RapidFire Tools, Inc. partner, will be performing the ASV External Vulnerability Scan on the IP Range you specified.
After the **ServerScan** system reviews the details of your scan request and you are using the **ASV Scan** service for the first time, you will receive an email notification about setting up your **ASV Scan** account at **ServerScan**.

The purpose of this account is so that you can download the results of your scan.

After receiving this email from **ServerScan**, you should proceed to "**Setting Up Access to Your ServerScan ASV Scan Account to View and Download Reports**" below to configure access to your **ASV Scan** account and the reports that are made available after your **ASV Scan** is complete.

**Setting Up Access to Your ServerScan ASV Scan Account to View and Download Reports**

If you are using the ASV Scan feature for the first time and have received an email notification from **ServerScan** welcoming you to the **ServerScan ASV Scan** service, proceed to the steps immediately below.

If you already have a **ServerScan ASV Scan** account, please proceed to the next section entitled "**Notification that Your ASV Scan has Started**" on page 22.

Follow these steps to complete the set up of your **ServerScan** account.
1. Set up your **Password** for your PCI/ASV Scanning Account at **ServerScan** by selecting the link contained within the **Welcome to ServerScan** email notification that you received.

2. Following the instructions on the **ServerScan** website to log into your account used to access details about your **ASV Scan** results and to manage **ASV Rescans**.

3. Assign your password to the **ServerScan account** created for your **ASV Scan Management, Reports, and Scan Attestation document(s)**.
A confirmation that your new **Password** has been assigned to your **ServerScan** account will be presented.

Setting Up Your ASV Reports to include your Company Information

Next set up the reports that will be generated to include your company's specific information. To do this:

1. **Access the ServerScan My Settings feature.**

2. **Enter the Company Name and Address** details in the My Settings page.

3. **Your settings are saved after you navigate away from the My Settings page.**
4. Exit the **ServerScan** website by selecting the **Logout** link.

   ![ServerScan Account Home](image)

**Notification that Your ASV Scan has Started**

After your **ASV Scan** has been initiated by **ServerScan**, you will receive a notification by email that your **PCI Server Scan Started**.

Upon completion of your **ASV Scan**, you will receive an email notifying you that the **PCI Server Scan** you requested is complete.

![Sample Email Notification](image)

After receiving the **PCI Server Scan Complete** notification by email, you will access your **ServerScan** account to view the results. To view the results of your **ASV Scan**, proceed to the next section.

**Viewing the Results of your ASV Scan**

After your **ASV Scan** is complete, you will receive an email notification stating that the scan has completed. The **PCI Server Scan Complete** email notification will contain a summary of your **ASV Scan** results.
To view the results of your ASV Scan, follow the steps below.

1. Log into your ServerScan ASV Scan account by visiting www.serverscan.com and selecting the MY ACCOUNT link.

   ![User Account login window](image)

   The User Account login window will be displayed.

2. Enter your Email Address and Password and select the Log In button to access your account.
After logging into your account, the **Go to Scan Manager** option will be displayed.

3. Select the **Go to Scan Manager** option to view the results of your **ASV Scan**.

The **Scan Manager** window will be displayed.
4. Select the **View Compliance Reports** link.

The **Compliance Reports** window will be displayed.

5. Using the **Download Reports** option(s), download and view the **ASV Scan Reports**.

6. Based on the outcome of your **ASV Scan** (in terms of the identified vulnerabilities), download and view the **Executive Scan Report**, the **Detailed ASV Scan Report**, and **Attestation** documents.

7. Log out of the **ServerScan Portal**.
Review the Executive and Detailed reports for the ASV Scan performed by ServerScan.

If your ASV Scan revealed security vulnerabilities that prevent your Merchant client from passing its PCI External Network Vulnerability Protection requirements, after the identified vulnerabilities are remediated, you may want to perform a "Rescan" using the ServerScan service.

Proceed to the next section to learn how to use the ServerScan Rescan option to run another ASV Scan on your client's network.

Performing an ASV Rescan using ServerScan

To run another ASV Scan (i.e. Rescan) to check for external vulnerabilities on your client's network perimeter, follow these steps:

1. Log into your ServerScan account visit the ServerScan website at www.serverscan.com and select the MY ACCOUNT link.

2. Enter in your Username and Password and select the Log In option to log into your ServerScan account:

3. Select the ServerScan Go to the Scan Manager button.
The **Scan Manager** window will be displayed.

4. Select the **View Compliance Reports** link.

The **Compliance Reports** window will be displayed.
5. To start the **Rescan** in the **Compliance Reports** window, select the **Rescan** icon that is present in a previous scan's results entry.

![Rescan Icon]

The **New Scan** settings window will be displayed to enable you to schedule your **Rescan**.

6. Set up and **Submit** the **Rescan**.

   Review the **Name**, **Email**, and **Target Hosts** fields to verify that the preloaded information from your original **ASV Scan** is correct.

![New Scan Settings Window]

7. Select the **Schedule Options**, **Run This Scan On Date and Time**, and **Time Window** settings.

   After defining the scan's settings, select the **Submit** button.

   The **Scheduled Scan** confirmation window will be displayed.
Once your Rescan submission has been verified by the ServerScan system, you will receive a notification by email stating that your ASV Scan has been scheduled and started.

8. Log out of your ServerScan account.

9. Upon receipt, view the email Notification that confirms that your ASV Rescan has been scheduled and started.

10. After your Rescan is complete, you will receive an email Notification that the ASV Scan is complete.

   Upon the completion of the Rescan, you can log into your ServerScan account to download and view the reports containing the results of the ASV Scan.
11. To view the results of your scan, log into your **ServerScan** account. Then select the **ServerScan View Compliance Reports** option.
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.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline PCI Management Plan</td>
<td>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.</td>
</tr>
<tr>
<td>Baseline PCI Risk Profile</td>
<td>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.</td>
</tr>
<tr>
<td>Cardholder Data Environment (CDE) Network Diagram and Details Report*</td>
<td>This report allows you to completely visualize how system components are connected within the Cardholder Data Environment (CDE) being assessed. This high-level report shows a layer 2/3 diagram and mapping with section blow-ups that list all major network devices, and segmented diagrams of connected devices. Additional information is also provided to identify which operating systems and device types were found. CDE details include a list of all discovered computers and network devices including those that we were unable to find connectivity information (denoted in gray text within the report).</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Devices where connectivity information is unavailable may be due to a lack of responsiveness of the computer itself or other &quot;hidden&quot; network devices (i.e., network devices that did not respond to SNMP requests). *Requires the Network Detective Inspector appliance.</td>
<td></td>
</tr>
<tr>
<td>Evidence of PCI Compliance</td>
<td>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 &amp; 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.</td>
</tr>
<tr>
<td>PCI Policies &amp; Procedures Document</td>
<td>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. 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.</td>
</tr>
<tr>
<td>PCI Post-Scan Questionnaire</td>
<td>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.</td>
</tr>
<tr>
<td>PCI Pre-scan Questionnaire</td>
<td>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 access, firewall information, application development, to authentication and change management standards.</td>
</tr>
<tr>
<td>PCI Risk Analysis Report</td>
<td>PCI is a risk-based security framework and the production of a Risk Analysis is one of primary requirements for PCI</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>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. 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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Capability Identification Worksheet</td>
<td>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).</td>
</tr>
<tr>
<td>Cardholder Data Environment ID Worksheet</td>
<td>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.</td>
</tr>
<tr>
<td>Compensating Controls Worksheet</td>
<td>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. 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. 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.</td>
</tr>
<tr>
<td>Deep Scan Selection Worksheet</td>
<td>The PCI Deep Scan, which includes a Primary Account Number (PAN) scanner used to identify files that are suspected of</td>
</tr>
<tr>
<td>Report Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Report Type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>** 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.**</td>
<td></td>
</tr>
<tr>
<td><strong>External Network Vulnerability Scan Detail by Issue</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>External Port Security Worksheet</strong></td>
<td>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.</td>
</tr>
<tr>
<td><em><em>Internal Network Vulnerability Scan</em> by Details</em>*</td>
<td>Detailed reports showing security holes and warnings, informational items including CVSS scores as scanned from inside the target network. Closing internal vulnerabilities helps prevent external attackers, once inside a network, and internal users from exploiting weaknesses typically protected by external firewalls. *Requires the Network Detective Inspector appliance.</td>
</tr>
<tr>
<td><strong>Necessary Functions Worksheet</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PAN Scan Verification Worksheet</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PCI Layer 2/3 Diagram</strong>*</td>
<td>This diagram shows the various components discovered along with their Layer 2 and Layer 3 connections. Systems and devices that are part of the Cardholder Data Environment (CDE) are highlighted. Having a representation of the components in the CDE along with their connectivity to the global network is a requirement of PCI. *Requires the Network Detective Inspector.</td>
</tr>
<tr>
<td>Report Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PCI Verification Questionnaire</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Server Function ID Worksheet</td>
<td>Per PCI DSS Requirement 2.1.1, only one function per server can be implemented in order to prevent functions that require 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).</td>
</tr>
<tr>
<td>User Identification Worksheet</td>
<td>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. 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.</td>
</tr>
</tbody>
</table>