Blueprint for
PCI Compliance-as-a-Service

By Win Pham, Vice President Development

RapidFireTools®
A Kaseya COMPANY

Introduction

The topic of PCI compliance is often misunderstood by both MSPs and their clients. The most common misconception is that PCI compliance means only having to pass a certified external vulnerability scan. In the industry, this type of scan is performed by an Approved Scan Vendor (ASV). While this is an important part of achieving compliance, it is only one component. PCI compliance is broken into 12 major segments nicknamed the dirty dozen. Of these sections, the ASV scan only represents compliance with section 11.2.

Another common misconception is that PCI compliance is an “IT Project” with a beginning and end. The fact is that PCI Compliance is an ongoing process of assessment, remediation, and reporting. While small and medium sized businesses are technically “allowed” to assess themselves, few of them will have the tools, technical knowledge, or objectivity to “self-assess.”

As an MSP, you are in a prime position to educate your clients about their obligations under PCI and to deliver a high-value, ongoing “PCI Compliance-as-a-Service.” In this white paper, we provide you with a blueprint for helping your clients become PCI compliant and continue to maintain that compliance on an ongoing basis.

What gets submitted and to whom?

Most businesses begin their PCI Compliance journey when they are asked to submit documentation of PCI compliance to their merchant bank or to a verifier.

What is submitted typically depends on the classification of your clients’ businesses and how they take and process credit cards. Most businesses will only need to submit a Self-Assessment Questionnaire (SAQ), an Attestation of Compliance (AoC), and evidence of passing quarterly external vulnerability scans performed by an Approved Scan Vendor (ASV). None of these requirements are intuitive for an untrained client, but all can be easily provided by you as a service.

Some larger vendors—or those working with a Qualified Security Assessor (QSA) —will also have to submit evidence that they have performed quarterly internal vulnerability scans and have remediated high-risk vulnerabilities. This is often accompanied by rescans as proof that all of the identified high-risk vulnerabilities have been addressed.

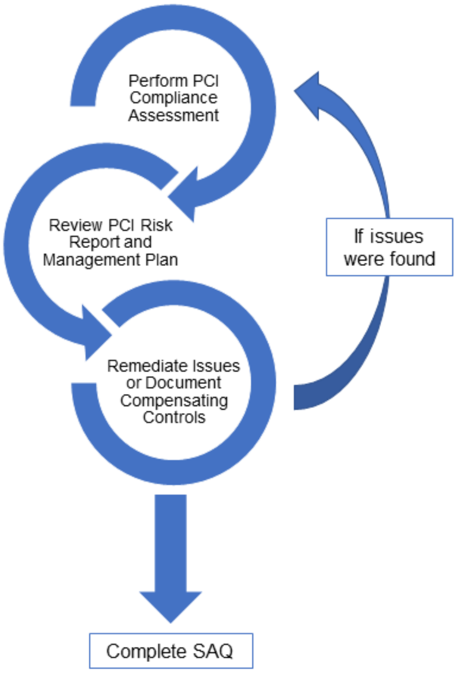
Initial SAQ Submission

Now that we have seen what is needed for submission, let’s jump back to the beginning and walk through the tasks you need to perform for your client. To prepare for the initial submission, you will need to gather the appropriate Self-Assessment Questionnaire to complete. Typically, your client’s merchant bank will indicate which form you need to complete. These are typically formulated in questions that require affirmative answers to confirm compliance.

Help your clients avoid the pitfall of “lying to comply” by helping them understand that there are negative ramifications to ignoring PCI compliance. If they experience a breach, the mandatory post-breach investigation will likely uncover the lies, exposing the client to much greater fines and potential lawsuits.

Rather than relying on a cumbersome and unwieldy paper questionnaire, use the PCI Compliance module from Network Detective to automatically identify issues and address them with your client. The module will automatically produce an Evidence of Compliance document, along with a corresponding Risk Assessment, providing the facts to help answer the SAQ and provide documentation to demonstrate the responses were made in a fact-based manner.

PCI requires addressing identified issues or documenting compensating controls. The process you should follow to complete the SAQ should follow the flow below:


Perform PCI Compliance Assessment
Review PCI Risk Report and Management Plan
Remediate Issues or Document Compensating Controls
If issues were found
Complete SAQ

The associated documents, including the Evidence of Compliance, should be stored for clients in case there’s an audit or request for documentation.

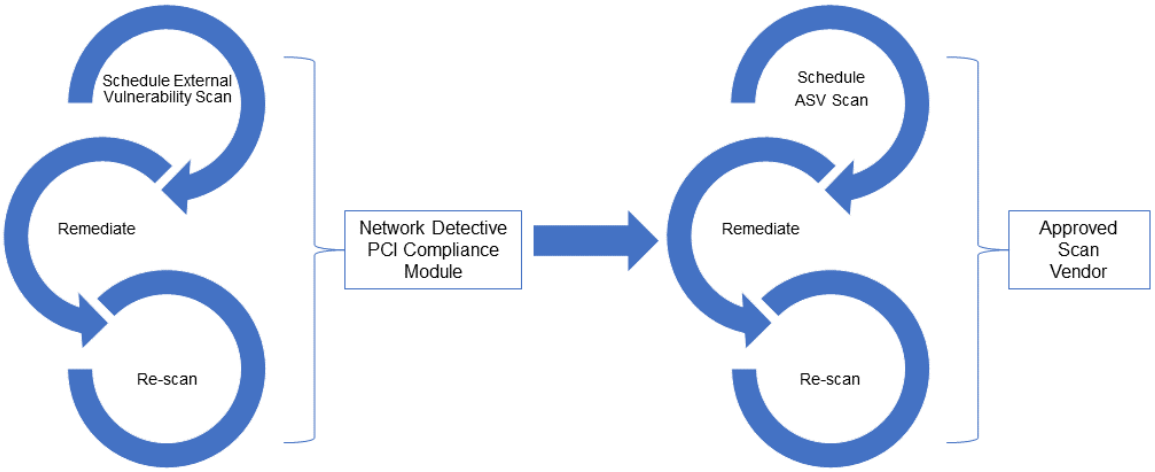
Initial ASV Scan Submission

Most PCI compliance submissions will require you submit an Authorized Scan Vendor (ASV) scan with an accompanying Attestation of Compliance. In order to obtain your Attestation, the results of your scan must not include any issues of medium severity or higher (CVSS score 4.0-10). If such issues are revealed by your scan, you must remediate those issues and continue to run additional scans and remediate until you have a passing scan.

The ASV scan must be performed by one of a handful of Approved Scan Vendors, and the cost of the service can range widely, from a few hundred to thousands of dollars. If you use the Network Detective PCI Compliance module to deliver your PCI Compliance service, there is a built-in option to schedule and run ASV scans provided by our scan partner, Server Scan. The scanning service is provided at a discounted rate, allowing you to add a mark-up when you pass the cost onto your client as part of the service fee. When your scan passes, the fee you pay includes the required Attestation of Compliance. If it does not pass, you can perform the necessary remediation and rescan the same network as many times as needed at no additional cost until it passes.

Typically, quarterly scans are required to maintain PCI compliance. Once you set up your client for an ASV scan in Network Detective, the settings are saved and can be scheduled to take place automatically.

Before you schedule an ASV scan for your client, we strongly recommend running the Network Detective external vulnerability scan (available for free unlimited use with the PCI compliance module). You can scan as many IP addresses as needed as often as necessary before scheduling your ASV scan. ASV scans are more intense than the Network Detective external vulnerability scan, but by reviewing the results from the Network Detective scan, you can quickly remediate many issues before your ASV scan.


Schedule External Vulnerability Scan
Remediate
Re-scan
Network Detective PCI Compliance Module
Schedule ASV Scan
Remediate
Re-scan
Approved Scan Vendor

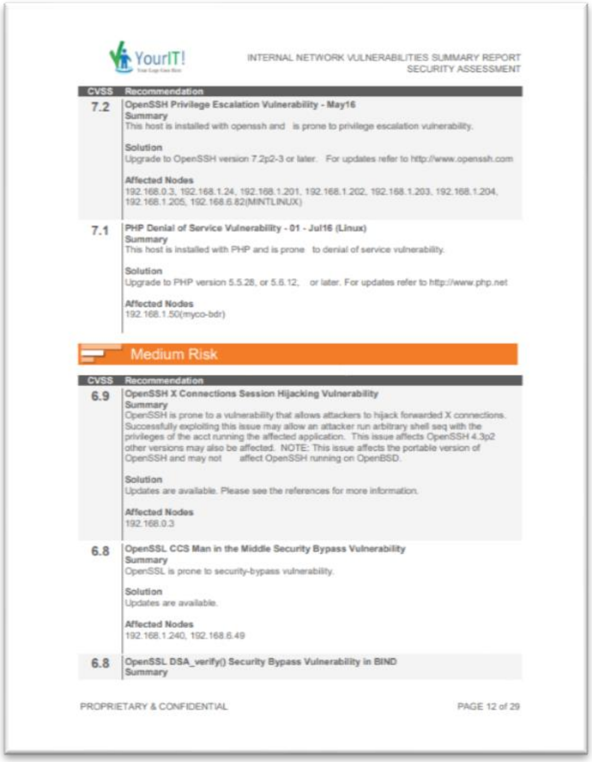
There are several advantages to performing Network Detective external vulnerability scans before scheduling your ASV scan. Typically, issues will be found during the scan. In some cases, the time it takes to remediate, and re-scan is taken away from the length of time that an Attestation is valid.

Because unlimited external vulnerability scans are included with the Network Detective PCI compliance module subscription, you can help your clients address most common issues before having a formal ASV scan performed. A common mistake is to submit an incorrect IP address that's not owned by your client. With Network Detective, you can validate that the IP addresses and hosts you are scanning are valid and owned by your client, and firewall misconfigurations can be addressed quickly.

Initial Internal Vulnerability Scan Submission

In some cases, you will need to perform and submit the results from your Internal Vulnerability Scan and re-scans to show that medium and high-risk severities have been addressed.

Using the Network Detective Inspector or Cyber Hawk, you can perform an internal vulnerability scan, review the results, and address all issues with CVSS scores of 4.0 or greater. To assist with identification of which issues should be remediated, the report "Internal Network Vulnerabilities Summary" from Inspector lists all issues sorted by CVSS score along with all affected nodes.



YourIT!

INTERNAL NETWORK VULNERABILITIES SUMMARY REPORT
SECURITY ASSESSMENT

CVSS	Recommendation
7.2	**OpenSSH Privilege Escalation Vulnerability - May16** **Summary** This host is installed with openssh and is prone to privilege escalation vulnerability. **Solution** Upgrade to OpenSSH version 7.2p2-3 or later. For updates refer to http://www.openssh.com **Affected Nodes** 192.168.0.3, 192.168.1.24, 192.168.1.201, 192.168.1.202, 192.168.1.203, 192.168.1.204, 192.168.1.205, 192.168.6.82(MINTLINUX)
7.1	**PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)** **Summary** This host is installed with PHP and is prone to denial of service vulnerability. **Solution** Upgrade to PHP version 5.5.28, or 5.6.12, or later. For updates refer to http://www.php.net **Affected Nodes** 192.168.1.50(myco-bdr)

Medium Risk

CVSS	Recommendation
6.9	**OpenSSH X Connections Session Hijacking Vulnerability** **Summary** OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded X connections. Successfully exploiting this issue may allow an attacker run arbitrary shell seq with the privileges of the acct running the affected application. This issue affects OpenSSH 4.3p2 other versions may also be affected. NOTE: This issue affects the portable version of OpenSSH and may not affect OpenSSH running on OpenBSD. **Solution** Updates are available. Please see the references for more information. **Affected Nodes** 192.168.0.3
6.8	**OpenSSL CCS Man in the Middle Security Bypass Vulnerability** **Summary** OpenSSL is prone to security-bypass vulnerability. **Solution** Updates are available. **Affected Nodes** 192.168.1.240, 192.168.6.49
6.8	**OpenSSL DSA_verify() Security Bypass Vulnerability in BIND** **Summary**

PROPRIETARY & CONFIDENTIAL

PAGE 12 of 29

Ongoing Compliance

Although the initial submission of proof of a passed Internal Vulnerability Scan is required for compliance, it is not enough. Remember: compliance is much more than a ‘project’ with a beginning and end; it’s an ongoing process of assessment, remediation, and reporting. To achieve true compliance, you should engage your client in a continual cycle of regular assessments and remediation.

Adding a Cyber Hawk appliance to your IT Compliance toolbox can help automate this process. Cyber Hawk will scan the network daily and perform weekly internal vulnerability scans to help identify new security issues that arise between your main assessments. The policy-based approach of Cyber Hawk makes it easy to configure and tailor for each client’s specific environment and can help discover inappropriate access to cardholder data environment (CDE) systems.

While ASV scans are only required quarterly, you can offer more security by scheduling external vulnerability scans that can occur between the required quarterly ASV scans. These scans are easily scheduled using another Network Detective tool called Reporter™, which can also generate intermediate risk profile assessments and associated management plans. To maintain compliance and stay ahead of compliance drift, we recommend reviewing the management plans monthly and addressing issues routinely.

Services and Required Components

	Minimal	Recommended
Initial Submission	• PCI Compliance Module • ASV Scan	• PCI Compliance Module • ASV Scan • Inspector or Cyber Hawk
Ongoing Compliance	• PCI Compliance Module • ASV Scans • Cyber Hawk	• PCI Compliance Module • ASV Scans • Cyber Hawk • Reporter

Cost of Delivery for Multiple Service Configurations

While you can charge thousands of dollars for PCI Compliance services, your sunk cost of goods to deliver them is minimal using Network Detective. Below is a list that itemizes the cost of the most popular configurations used by MSPs. Please note all prices shown are for 36-month subscriptions. Subscription fees are subject to change.

Configuration 1 typically involves the purchase of a single Inspector appliance that can be moved from location to location to perform the required internal vulnerability scans.

Configuration 1 – Initial Submission Preparation

PCI Scan Module	$249/month
ASV Scan	$49/IP address
Inspector	$99/month – 1 appliance

Configuration 2 is designed to deliver PCI Compliance-as-a-Service. You'll need Cyber Hawk, which includes an unlimited number of Cyber Hawk appliances, and can be used for the required initial vulnerability scans. Unlike the Inspector, Cyber Hawk appliances are left connected to each client's network and provide daily alerts of discovered internal vulnerabilities, which assists with daily support.

Configuration 2 – Initial Submission Preparation and Ongoing Compliance

PCI Scan Module	$249/month – unlimited clients
ASV Scan	$49/IP address
Cyber Hawk	$499/month – unlimited clients

Configuration 3 augments Configuration 2 by adding automated reporting, which allows for automation of external vulnerability scans as well. With automated reporting, intermediate compliance reporting and documentation can be created with minimal effort on a regular basis (monthly if desired).

Configuration 3 – Initial Submission Preparation and Ongoing Compliance with Automation

PCI Scan Module	$249/month – unlimited clients
ASV Scan	$49/IP address
Cyber Hawk	$499/month – unlimited clients
Reporter	$250/month – unlimited clients

Deliverables and Suggested Service Pricing

	Minimal	Recommended
Initial Submission	PCI Compliance Reports External Scan Results Attestation of Compliance $1,500 - $5,000 for report preparation + $59/external IP address (ASV Scan) + hourly rate for remediation	PCI Compliance Reports External Scan Results Internal Scan Results Attestation of Compliance $2,500 - $10,000 for report preparation + $59/external IP address (ASV Scan) + hourly rate for remediation
Ongoing Compliance	Policy Violation Detection Quarterly Attestation of Compliance $250+/month + $59/external IP (quarterly ASV Scan) + hourly rate for remediation	Policy Violation Detection Automated Monthly PCI Report Updates Automated Monthly External Vulnerability Scans Quarterly Attestation of Compliance $500+/month + $59/external IP (quarterly ASV Scan) + hourly rate for remediation

The range for pricing provided above is broad, because the biggest cost to you will be how much time you have to invest to deliver the service. Here is a list of the different tasks that typically vary by the size of the organization and approximate time estimates to perform:

- Review of Users – 2 minutes per user
- Review of Computers – 5 minutes per computer
- Deep Scans on CDE Computers – 10 minutes per computer in CDE

In the case of ongoing compliance, you should account for the number of locations as well. Note that we recommend that you charge a separate hourly rate for remediation services as the required tasks may vary greatly and some involve infrastructure additions and changes.

Conclusion

There are millions of business in North America that are subject to PCI, and a large percentage of their owners are unaware of the requirements and/or are operating under the mistaken belief that they are in compliance.

As an MSP, you are in a prime position to educate your clients about their obligations under PCI, and also to deliver a high-value, ongoing “PCI Compliance-as-a-Service” using affordable, purpose-built tools.

RapidFire Tools, a Kaseya company, creates innovative business-building technology tools for Managed Service Providers (MSPs). More than 8,000 technology service professionals worldwide use our products to close more business, offer more services, keep more customers, and make more money. Our offerings include **Network Detective®**, a complete suite of IT assessment, documentation, and reporting tools; **Cyber Hawk™**, an insider cyber threat detection and alerting tool; and **Compliance Manager™**, an automated security and privacy compliance platform.

Our flagship product, Network Detective, is the #1 non-intrusive IT assessment and reporting tool. With it, MSPs can quickly and easily capture a vast amount of network assets, users, configurations, and vulnerabilities without installing any software, probes, or agents. Our proprietary algorithm analyzes the data to generate dozens of professionally designed, completely brandable reports in minutes. Network Detective includes six modules for different kinds of IT assessments. We also offer the Reporter add-on, which dramatically reduces time and labor by automating the network scans and report generation process. The subscriptions include an unlimited number of scans, on an unrestricted number of networks.

RapidFire Tools also offers Cyber Hawk, the first IT security tool designed to detect insider cybersecurity threats and generate daily alerts of suspicious network changes an anomalous end-user behavior. Cyber Hawk empowers MSPs to create custom, brandable, and unique cybersecurity services at an affordable rate.

Rounding out our offerings is Compliance Manager, a unique compliance process automation tool, with built-in modules to support the delivery of Compliance-as-a-Service solutions. Specific standards supported including HIPAA, GDPR, the NIST Cybersecurity Framework, as well as a specialized module for compliance with the security provisions of most cyber liability insurance policies. MSPs use Compliance Manager to ensure that the IT policies and procedures required by industry or government regulations are being followed and, critically important, documented.

To learn more, visit www.rapidfiretools.com or call 678-323-1300.