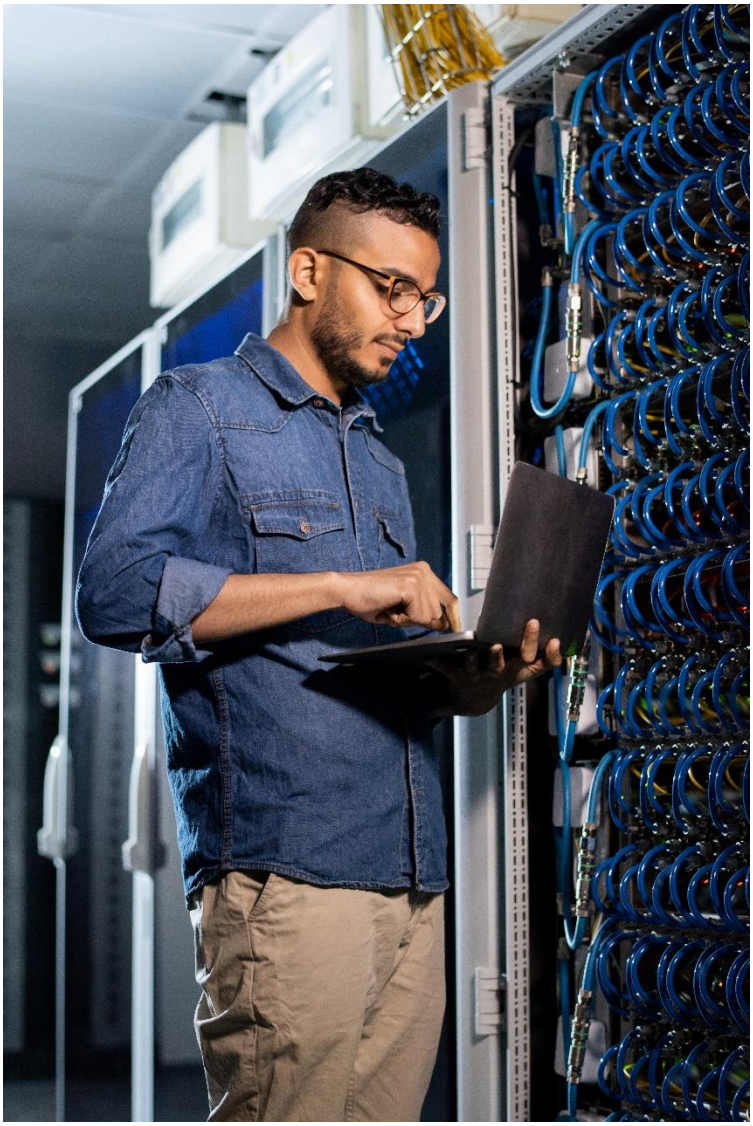
Expanding Your Service Offerings with Recurring IT Assessments



By Win Pham, Vice President Development

RapidFireTools®
A Kaseya COMPANY

Overview

Recurring IT assessments provides you, the managed service provider (MSP), with a means to reduce client churn and create new revenue offerings, while further differentiating you from your competition. Performing recurring IT assessments is an important way for you to catch small issues before they cause big problems, but more important, it provides you a way to help your clients see and understand the value of your services.

Regular assessments can provide your clients with a more secure and reliable infrastructure, help them avoid hefty compliance fines, and give both you and your clients the ability to be proactive in managing and maintaining their strategic IT assets.

Unfortunately, most MSPs don't perform assessments frequently enough. The typical reasons are:

- there isn't enough time
- there's something more pressing to do
- the lack of understanding about the value obtained for the effort

The good news is that there are enabling technologies now available that make regular and ongoing IT assessments feasible from a resource and cost perspective.

The purpose of this document is to present a blueprint for incorporating recurring IT assessments into your standard service offerings.

Three Tiers of Assessment Frequency & Depth

While the benefits of IT assessments are plentiful, not all clients will require the same level of review and scrutiny. Ideally, you will be able to determine both the complexity of your clients' networks, and their value of their business to you, and create your own unique and branded assessment service.

In this paper, we present three tiers of service that should allow you to match the level of effort with the needs and opportunities of most of your clients. For each of the blueprints, we provide you with the recommended frequency and purpose of each of the assessment types, the specific Network Detective tools that you will need to perform the assessments, and what your deliverables will be.

Basic Level Assessment Blueprint

The Basic Level assessment service is designed for most SMB companies typically served by most small MSPs. These businesses generally don't have sophisticated compliance needs, don't have internal IT staff, and may not be able to afford or require any type of enhanced services.

This blueprint balances the level of effort required for you to perform the assessment on a regular basis, with the recurring revenue levels you are likely to be receiving. The incremental extra effort needed to perform assessments at this level is well worth the additional benefits both you and your client will enjoy.

Frequency	Network Detective Component	Deliverable	Purpose
Initial Annual	Network Security Reporter	Network & Security Risk Reports Management Plans Full Detail Report External Vulnerability Summary	Establish a baseline assessment Refresh the baseline on annual basis Provides network documentation
Monthly	Network Security Reporter	Baseline Management Plan Risk Reports (Change) Management Plans (Change) Full Detail Change Report External Vulnerability Summary	Show progress in issue remediation with baseline reports Show new issues and re-prioritize with change reports Identify significant network changes that may affect monitoring and management
Quarterly	Network Security Reporter	Network & Security PowerPoints Quarterly Business Review Report	Interactive review of significant changes in a digestible fashion Identify new projects and initiatives

Required Tasks

All work for the Basic Blueprint can be performed remotely. This significantly minimizes the cost of performing the assessments.

Estimated Time

There are advanced tools available that can automate most of the work, but if performed manually, the required technician time would be typically 30-60 minutes per month per client, with one hour each quarter for the interactive review. Additional automation techniques can reduce the required effort to only the interactive review.

Perform Scans

Initial/Annual/Monthly/Quarterly

1. Remote onto a server or workstation in the client's network
2. Download and run the Network/Security Data Collector to perform a Network Scan
3. Download and run the Network/Security Push Data Collector to run local data collections on the connected computer
4. Initiate an External Vulnerability scan from the Network Detective application

Note: Monthly/quarterly/annual steps are automated with the installation of Reporter on a single computer at the client's location during the initial visit

Scheduling Techniques

Implementation of the blueprint requires proper scheduling of tasks. Scheduling can be performed manually using Outlook reminders or with recurring tickets through your PSA system.

By using Reporter, scanning and report generation/delivery can be fully automated by installing a Remote Data Collector application at each client location, then setting the desired frequency. If you prefer no installation at the target locations, Reporter gives you the option to script the data collection process and have it run on a schedule using your RMM or Windows Task Scheduler.

Report Review and Delivery

Reports should be generated per the blueprint based on the frequency. The Initial/Annual and Quarterly reviews should be done interactively either in person or online. Monthly reports can be delivered electronically to your client and reviewed as needed. On a monthly basis, a technician should review the set of generated reports, focusing mostly on the change reports, and looking for new issues in the Management Plans.

Enhanced Level Assessment Blueprint

The Enhanced Level assessment blueprint is designed for your more sophisticated clients and network environments. These clients may have needs for higher levels of IT security or specialized services. This level allows for the inclusion of added-value assessments, like SQL Server and MS Exchange, along with network diagraming and internal vulnerability detection. Unlike the Basic Level blueprint, this blueprint does require an annual on-site visit.

Frequency	Network Detective Component	Deliverable	Purpose
Initial Annual	Network Security Inspector Reporter	Network & Security Risk Reports Management Plans Full Detail Report External Vulnerability Summary Internal Vulnerability Summary Layer 2/3 Diagram & Detail	Establish a baseline assessment Refresh the baseline on annual basis Provides network documentation Enhanced security from identifying internal network vulnerabilities
Monthly	Network Security SQL Server Reporter	Baseline Management Plan Risk Reports (Change) Management Plans (Change) Full Detail Change Report External Vulnerability Summary SQL Server Health Reports	Show progress in issue remediation with baseline reports Show new issues and re-prioritize with change reports Identify significant network changes that may affect monitoring and management
Quarterly	Network Security Exchange Reporter	Network & Security PowerPoints Quarterly Business Review Report Exchange Risk/Detail Reports	Interactive review of significant changes in a digestible fashion Identify new projects and initiatives Provide additional documentation for disaster recovery

Required Tasks

On an annual basis, an on-site visit with an Inspector appliance is required to perform the Internal Vulnerability and Layer 2/3 scan. All other scans (Monthly and Quarterly) can be performed remotely.

Estimated Time

Implementing the Enhanced Blueprint manually would take about the same time as the Basic Blueprint, but will require additional six hours of time per year:

- two hours for the on-site visit to connect and remove the Inspector
- four extra hours of time to scan and generate Exchange and SQL Server reports

Automation would also significantly reduce the time to implement the Enhanced Blueprint as well.

Perform Scans

Initial/Annual

1. Go on-site
2. Connect the Inspector appliance
3. From the Network Detective application, setup the Inspector appliance to initiate an Internal Vulnerability scan, Layer 2/3 scan, Network Scan, and Local Push for Network and Security
4. Initiate an External Vulnerability scan from the Network Detective application

Monthly/Quarterly

1. Remote onto a server or workstation in the client's network
2. Download and run the Network/Security Data Collector to perform a Network Scan
3. Download and run the Network/Security Push Data Collector to run local data collection on the connected computers
4. Download and run SQL Server collection (monthly, if applicable)
5. Download and run Exchange data collection (quarterly, if applicable)
6. Initiate an External Vulnerability scan from the Network Detective application

Note: Monthly and quarterly steps are automated with the installation of Reporter on a single computer at the client's location during the initial visit; annual internal vulnerability scans require an on-site visit.

Scheduling Techniques

Implementation of the blueprint requires proper scheduling of tasks. Scheduling can be performed manually using Outlook reminders or with recurring tickets through your PSA system.

By using Reporter, scanning and report generation/delivery can be fully automated by installing a Remote Data Collector application at each client location, then setting the desired frequency. If you prefer no installation at the target locations, Reporter gives you the option to script the data collection process and have it run on a schedule using your RMM or Windows Task Scheduler.

Report Review and Delivery

Reports should be generated per the blueprint based on the frequency. The Initial/Annual and Quarterly reviews should be done interactively, in person or online. Monthly reports can be delivered electronically to your client and reviewed as needed. On a monthly basis, a technician should review the set of generated reports, focusing on the change reports and looking for new issues in the Management Plans.

Premium Level Assessment Blueprint

The Premium Level Blueprint is designed for larger companies and those with compliance needs. Compliance requires not only an Annual Risk Analysis, but also proof of on-going efforts. The Premium Level provides a framework for how to demonstrate and document on-going efforts. The Premium Level assessment can be performed using either the HIPAA or PCI Compliance module (or both in situations where you have larger healthcare clients).

Frequency	Network Detective Component	Deliverable	Purpose
Initial Annual	HIPAA/PCI Inspector Reporter	All Compliance Reports	Provides annual Evidence of Compliance and proof of risk analysis
Monthly	HIPAA/PCI Reporter	HIPAA/PCI Risk Profile HIPAA/PCI Management Plan (Change) External Vulnerability Summary	Demonstrates on-going compliance and remediation activity
Quarterly	Inspector Reporter	Internal Vulnerability Summary	Perform the quarterly vulnerability scans required by various compliance standards

Required Tasks

On a quarterly basis, an on-site visit with an Inspector appliance is required to perform the Internal Vulnerability and Layer 2/3 scan, as well as performing the on-site survey.

Estimated Time

The cost to implement the Premium Blueprint varies greatly with the size of the organization. Most of the effort will consist of the following:

- annual Risk Analysis (8+ hours annually)
- quarterly Inspector scans (8 hours annually)
- monthly scans (1 hour monthly)

Perform Scans

Initial/Annual

1. Go on-site
2. Perform complete HIPAA/PCI Compliance assessments

Monthly

1. Remote onto a server or workstation in the client's network
2. Perform the HIPAA and PCI scans for use with the Risk Profiles (utilizing worksheets from the previous annual assessment)

Quarterly

1. Go on-site
2. Connect the Inspector appliance
3. Initiate an Internal Vulnerability Scan
4. After scan completion, remove the Inspector

Note: Annual and monthly steps are automated with the installation of Reporter on a single computer at the client's location during the initial visit; quarterly internal vulnerability scans require an on-site visit.

Scheduling Techniques

Implementation of the blueprint requires proper scheduling of tasks. Scheduling can be performed manually using Outlook reminders or with recurring tickets through your PSA system.

By using Reporter, scanning and report generation/delivery can be fully automated by installing a Remote Data Collector application at each client location, then setting the desired frequency. If you prefer no installation at the target locations, Reporter gives you the option to script the data collection process and have it run on a schedule using your RMM or Windows Task Scheduler.

Report Review and Delivery

Reports should be generated per the blueprint based on the frequency. The Initial/Annual and Quarterly reviews should be done interactively, in person or online. Monthly reports can be delivered electronically to your client and reviewed as needed. On a monthly basis, a technician should review the set of generated reports, focusing on the change reports and looking for new issues in the Management Plans. For compliance purposes, all primary and supporting reports should be archived.

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.