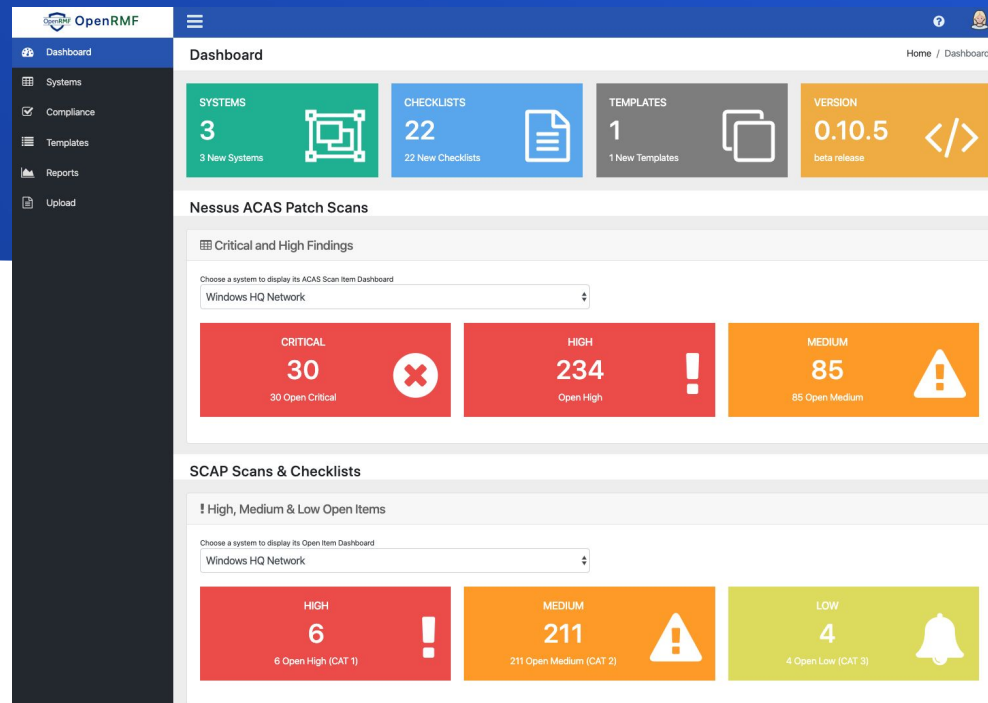


# OpenRMF - Innovation and Automation for DISA STIGs, Nessus scans and NIST Controls

<https://www.openrmf.io>

The only web-based open source tool to help you manage your DISA STIGs, Nessus Scans, NIST Controls, and correlate them automatically!

- Upload Checklists (CKL or XCCDF SCAP)
- Run Compliance and Information Reports
- Filter on Open Items remaining
- Manage Checklists by System

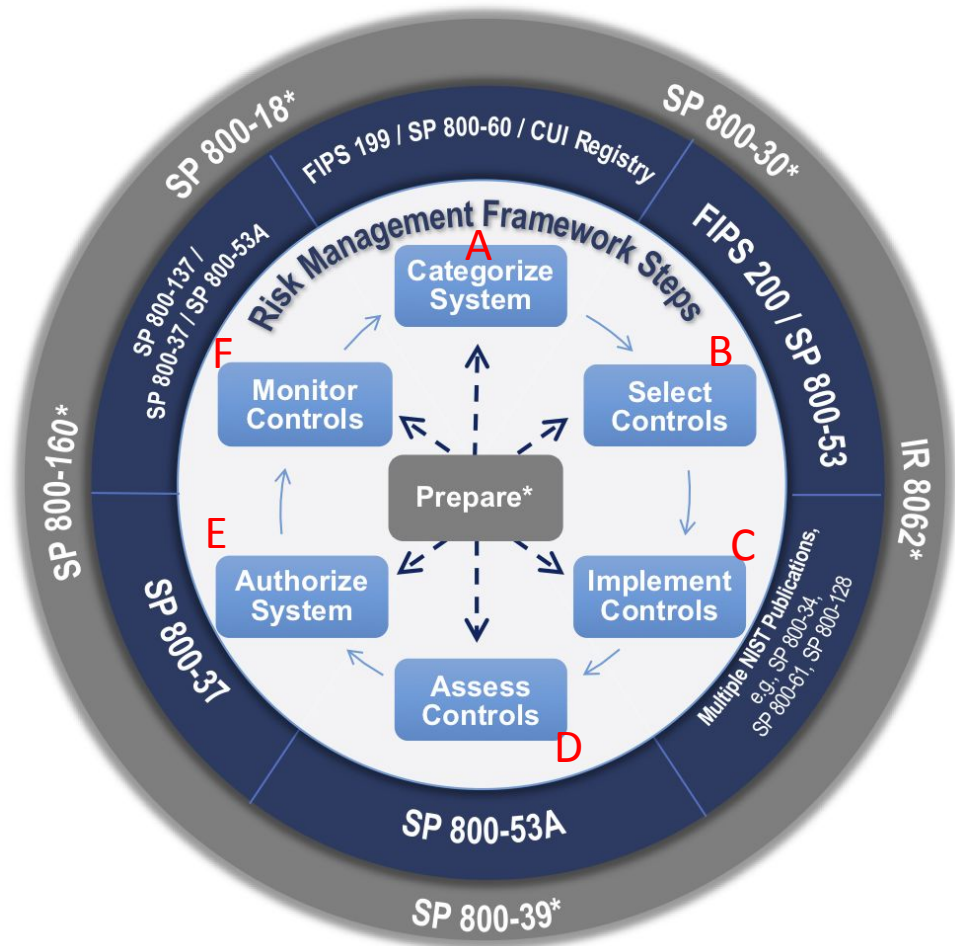


- 
- The diagram illustrates the Risk Management Framework (RMF) steps and their associated NIST Special Publications (SP) and Framework Interim Reports (IR). The central circle contains the steps: Prepare\* (grey), Monitor Controls (blue), Select Controls (blue), Implement Controls (blue), Assess Controls (blue), and Authorize System (blue). Arrows indicate a clockwise flow from Prepare\* to Monitor Controls, then to Select Controls, Implement Controls, Assess Controls, Authorize System, and back to Prepare\*. A dashed double-headed arrow connects Prepare\* to the other steps. The outer ring lists the following publications:
- SP 800-137 / SP 800-53A
  - SP 800-160\*
  - SP 800-37
  - SP 800-53A
  - SP 800-39\*
  - SP 800-30\*
  - FIPS 199 / SP 800-60 / CUI Registry
  - IR 8062\*
  - Multiple NIST Publications, e.g., SP 800-123, SP 800-138, SP 800-139

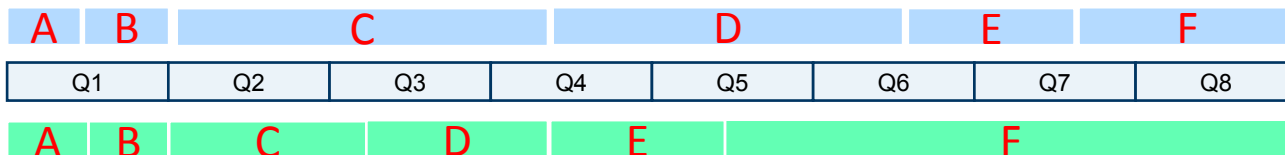
# The RMF Process – 6 Steps

## Time Consumers

- OpenRMF here → A. Categorize the System
- OpenRMF here → B. Select the Control Families
- OpenRMF here → C. Implement the Controls
- OpenRMF here → D. Assess the Controls
- OpenRMF here → E. Authorize the System
- OpenRMF here → F. Monitor Controls



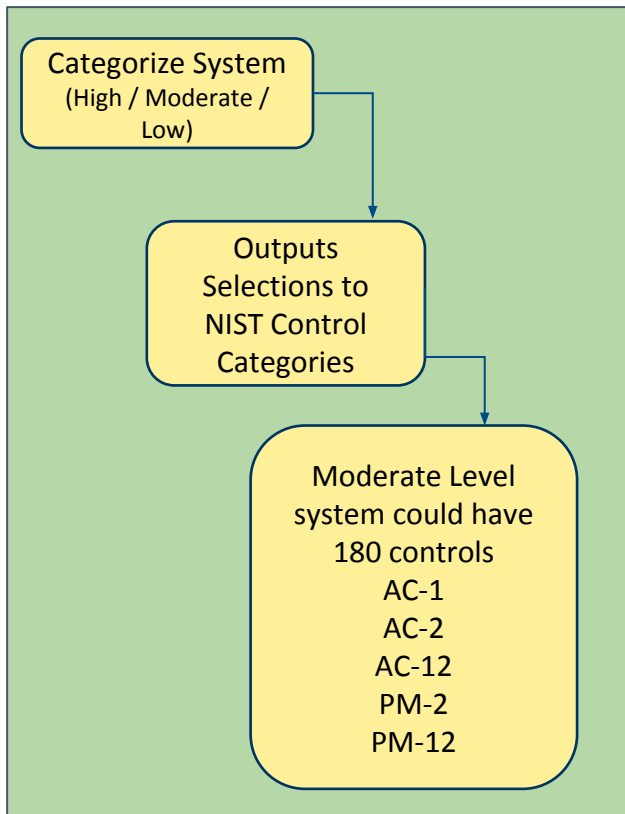
## Current Timeframe



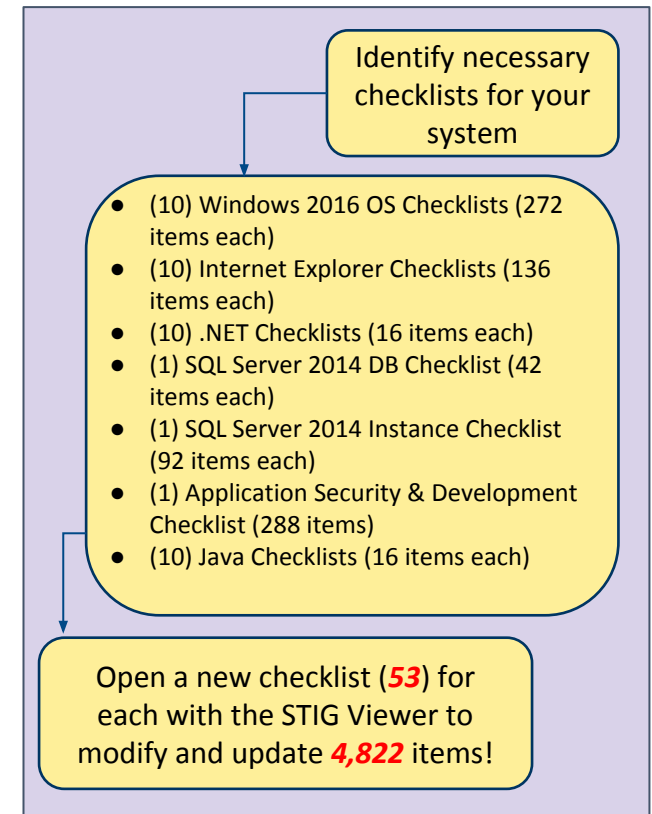
# Complexity of RMF in your System

Example: 1 system consisting of 10 Windows Servers with 1 Application

## eMass Process

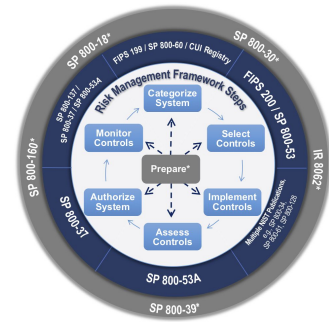


## DISA STIG Process

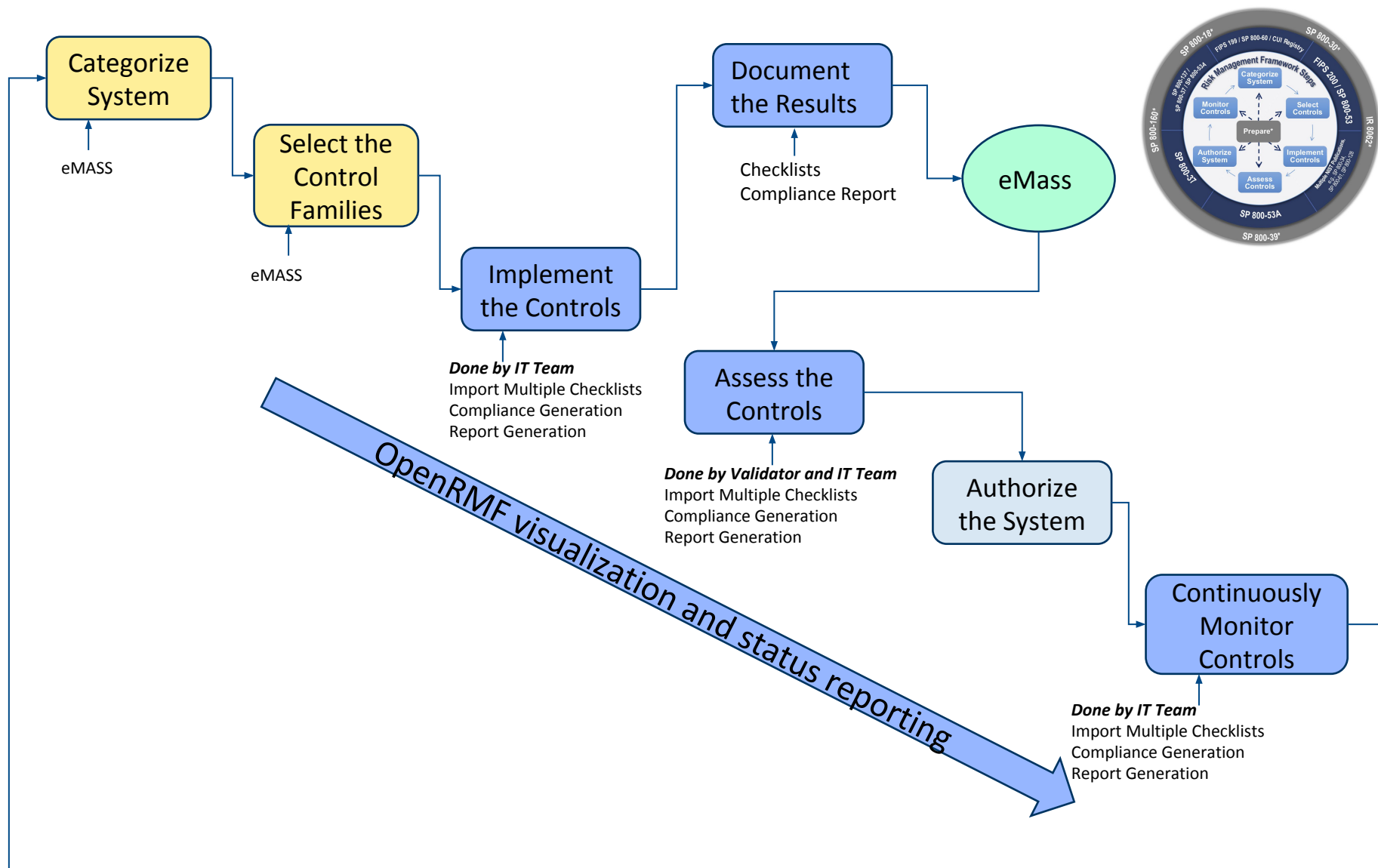


**No Automated  
Correlation**

**Completely Manual!**



# RMF Process with OpenRMF Automation



# OpenRMF Features

- 100% Open Source tool
- Automatically Relate DISA STIGs with NIST RMF Control Families and Categories Seamlessly
- Automatically Organize Checklists by System
- Single Source of Truth for all System Checklists
- Management Insight into IA Status and Security Posture
- On premise, local machine, or in the cloud
- 100% Browser based
- Role Based Access Control
- Easily Find Errors and Deltas Across Checklists
- Run Nessus scan, Checklist, and Controls reports
- Removes the IA Mystery!

More information at <https://www.openrmf.io/>

# Coming Soon...

- March 2020 v 0.12
  - Automatically create your Test Plan
  - Automatically create your POA&M
  - Automatically create your Risk Assessment Report
  - Live Editing of Checklists Online
  - Better reporting and filtering of data
  - Edit vulnerability status across multiple checklists in an instant
- ~ August 2020 - v 1.0 Enterprise Features
  - Versioning of Checklists
  - More Detailed Reporting
  - Multi-Tenant
  - Versioning and Merging of Nessus ACAS scan data
  - Enterprise Connectors to external systems



# OpenRMF v 0.11 Screenshots

“Using the OpenRMF tool, we reduced the three weeks to generate our compliance report down to 5 minutes. And OpenRMF found an error in our compliance we did manually.” – former employee of MSG

“With the OpenRMF Tool, we quickly found 2 servers with the exact same hostname we did not see by looking at each checklist individually.” - Neany

“Using the list of checklists per system, we were able to update management on our number of open items across all checklists within our system in seconds.” - Tutela

# Screen Shots – OpenRMF Checklist Upload



OpenRMF

Dashboard

Checklists

Compliance

Templates

Reports

Upload

Checklist file upload

Home / New checklist upload

Checklist Upload

System Name

My New System

Select the system this belongs to, or 'None'

Add a new System

Checklist Files (up to 5 at a time)

3 files were chosen

Choose Files

DEGTHAT\_SCC-5.0.1\_2019-04-1...

size: 27.2 KB type: xml

sqlserver2014database.ckl

size: 304 KB type: ckl

ASD-application1.ckl

size: 1.58 MB type: ckl

Upload and Save

Checklist Upload Help

Use this form to upload a new \*.CKL STIG checklist file or SCAP Scan XCCDF \*.XML to the system for scoring, indexing, and managing your DoD STIG information. Select your system (if any) and then select up to five (5) \*.CKL or \*.XML files to upload at a time.

All fields are mandatory.

\* Please fill in the **Host** field on your Checklist file CKL! All checklists are named by SYSTEM-HOSTNAME-STIGTYPE-REVISION.

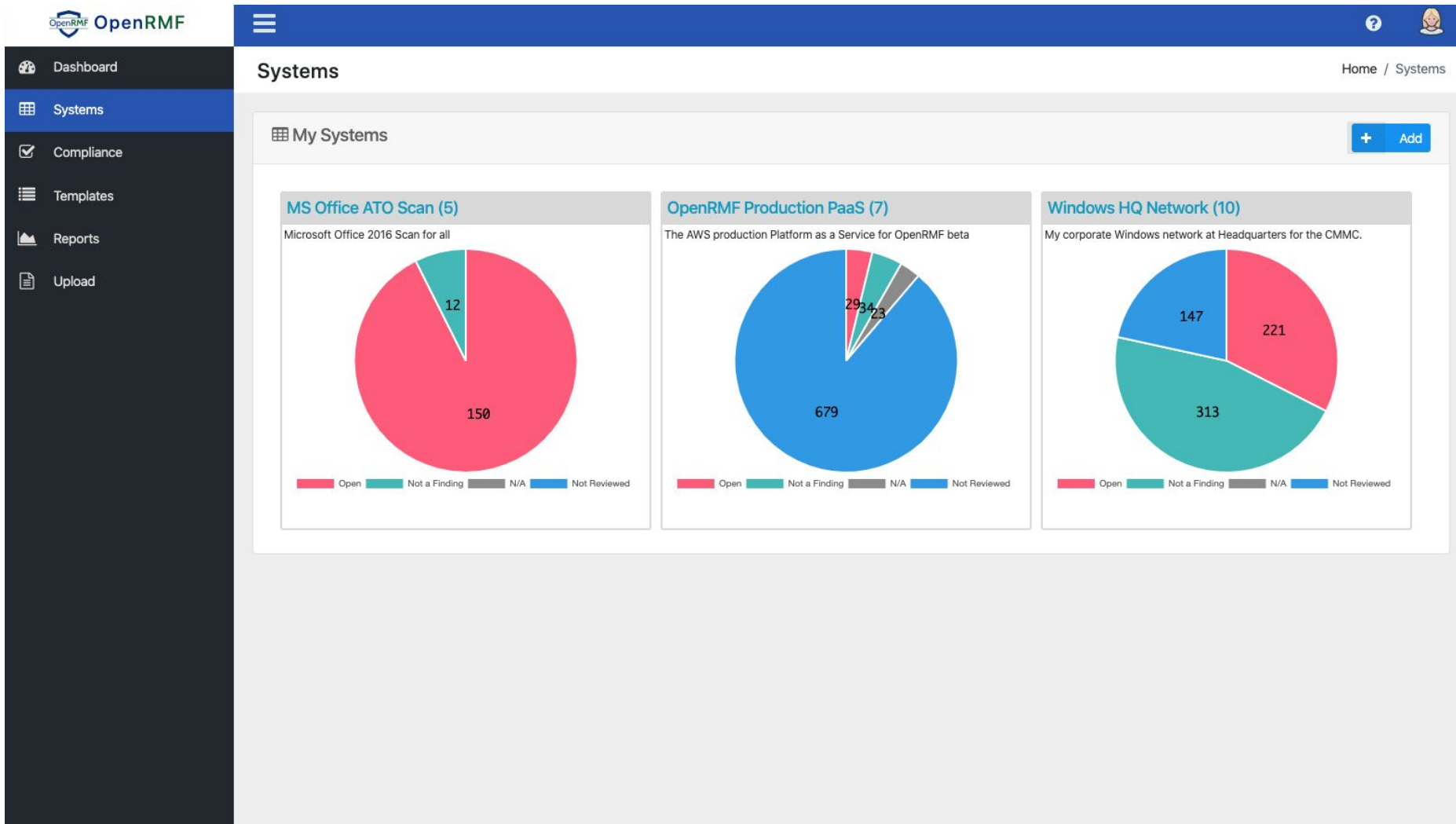
i.e. PAL Platform - ca2335.myorg.navy.mil - Google Chrome Current Windows STIG - Release: 15 Benchmark Date: 25 Jan 2019

© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

<https://www.openrmf.io>

11

# Screen Shots – OpenRMF Checklists by System



# Screen Shots – OpenRMF System Record

OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

System Information and Checklists

Home / System / Checklists

System Information

List All Systems

**Title:** Windows HQ Network

**Checklists:** 10

**Description:** My corporate Windows network at Headquarters for the CMMC.

**Nessus Scan:** Yes [\(xml\)](#) [\(xlsx\)](#)

**Latest POA&M:** (future)

**Last Risk Assessment Report:** (future)

**Audit Information:**

**Created:** 12/01/2019 11:45 am

**Last Updated:** 12/29/2019 10:20 am

**Last Compliance Check:** 12/27/2019 9:07 am

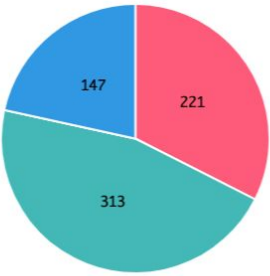
Edit

Compliance

Upload

Delete

System Status



Open 221, Not a Finding 313, N/A, Not Reviewed 147

Save Chart

Checklists

Show 50 entries

Search:

	Title	OPEN	NAF	N/A	N/R
<input type="checkbox"/>	<div>DEGTHAT-Google Chrome Current WIN STIG-R17 dated 25 Oct 2019</div> <div>last updated on 12/01/2019 11:46 am</div> <div>delete</div>	19	6	0	18
	CAT 1:	1	0	0	0
	CAT 2:	16	6	0	17
	CAT 3:	2	0	0	1
<input type="checkbox"/>	<div>DEGTHAT-Microsoft DotNet Framework 4.0 STIG-R9 dated 25 Oct 2019</div> <div>last updated on 12/01/2019 11:46 am</div> <div>delete</div>	1	2	0	13
<input type="checkbox"/>	<div>DEGTHAT-Microsoft Office System 2016 STIG-R1 dated 14 Nov 2016</div> <div>last updated on 12/01/2019 11:46 am</div> <div>delete</div>	18	2	0	0

# Screen Shots – OpenRMF Individual Checklist



OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

My Checklist

Home / Checklist

Asset Information

List All Checklists

**System:** Windows HQ Network  
**Host:** DEGTHAT  
**Title:** Google Chrome Current Windows Security Technical Implementation Guide  
**Release:** Release: 17 Benchmark Date: 25 Oct 2019  
**FQDN:**  
**Tech Area:**  
**Asset Type:** Computing  
**Role:** None

Last Updated on 12/01/2019 11:46 am

Edit

Download

Export

Delete

DEGTHAT-Google Chrome Current WIN STIG-R17 dated 25 Oct 2019

	OPEN	NOT A FINDING	NOT APPLICABLE	NOT REVIEWED
Total	19	6	0	18
CAT 1	1	0	0	0
CAT 2	16	6	0	17
CAT 3	2	0	0	1

Severity Breakdown

Open

Not a Finding

Not Reviewed

Last Updated on 12/01/2019 11:46 am

Save Chart

Category Breakdown

CAT I

CAT II

CAT III

Last Updated on 12/01/2019 11:46 am

Save Chart

Vuln Ids

Open

NaF

V-44711

N/A

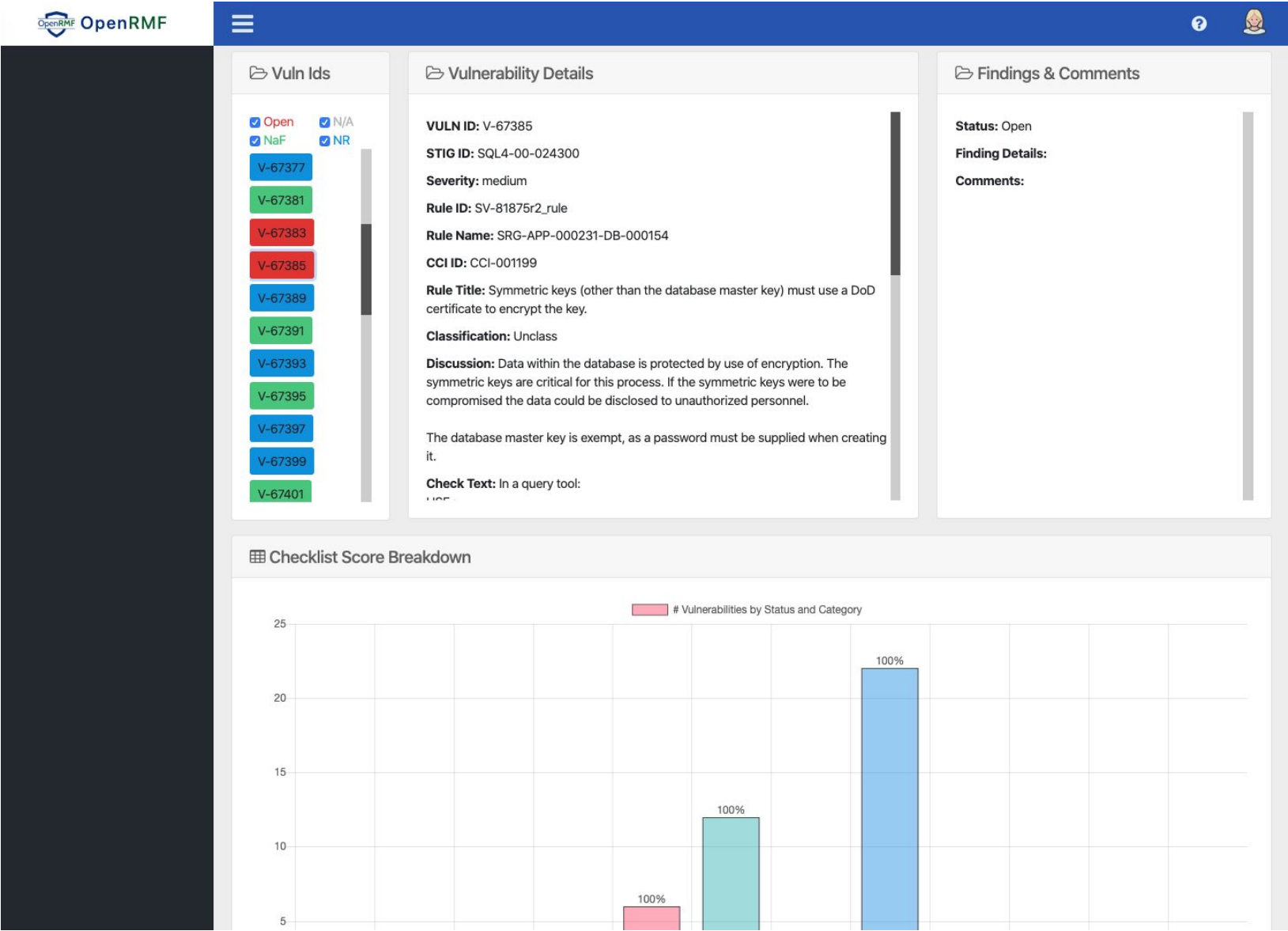
NR

Vulnerability Details

Please select a Vulnerability ID to view its details.

Findings & Comments

# Screen Shots – OpenRMF Individual Checklist



# Screen Shots – OpenRMF Generate Compliance



OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

Compliance

Home / Compliance

Compliance Generator

System Filter

OpenRMF Production PaaS

System Impact Level

Moderate

Contains PII / Privacy Data?

☒

Generate

Compliance Help

Generate a Compliance Report across all the checklists in your system to verify your status on satisfying all relevant controls. Follow the steps below to generate and validate your checklists for the chosen Impact Level.

1. Choose your System

2. Choose your Impact Level (Low, Moderate, High)

3. Check if you contain PII, PHI, or Privacy Data

4. Click the Generate button

5. Review the controls and checklists

6. Click the checklist to view the Vulnerabilities for that control

7. Page through the results at the bottom of the table

8. Use the Search box to filter results as you type

Compliance Summary

Summary per family for your System Compliance. Details are below in the next section.

✓ Green = Not A Finding / Not Applicable. ◯ Blue = Not Reviewed. ✗ Red = Open.

✗ AC

◯ AP

◯ AR

◯ AT

✗ AU

◯ CA

✗ CM

◯ CP

◯ DI

◯ DM

✗ IA

◯ IP

◯ IR

✗ MA

◯ MP

◯ PE

◯ PL

◯ PM

◯ PS

◯ RA

◯ SA

✗ SC

◯ SE

✗ SI

◯ TR

Compliance Details

Below find the results. Green = Not A Finding / Not Applicable. Blue = Not Reviewed. Red = Open.

Show 50 entries

Search:

#	Control	Title	Checklists
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	

© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

<https://www.openrmf.io>

16



# Screen Shots – OpenRMF Compliance Details

Compliance Details			
Below find the results. Green = Not A Finding / Not Applicable. Blue = Not Reviewed. Red = Open.			
Show 50 entries		Search: <input type="text"/>	
# ↑↓	Control ↑↓	Title ↑↓	Checklists ↑↓
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	
2	AC-2	ACCOUNT MANAGEMENT	<ul style="list-style-type: none"><li>ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018</li><li>web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019</li></ul>
3	AC-3	ACCESS ENFORCEMENT	<ul style="list-style-type: none"><li>ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018</li><li>Unknown-Host-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019</li><li>web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019</li></ul>
4	AC-4	INFORMATION FLOW ENFORCEMENT	<ul style="list-style-type: none"><li>web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019</li><li>workstation.myorg.navy.mil-Google Chrome Current WIN STIG-R15 dated 25 Jan 2019</li><li>workstation.myorg.navy.mil-MSIE 11 STIG-R16 dated 27 Jul 2018</li></ul>
5	AC-5	SEPARATION OF DUTIES	
6	AC-6	LEAST PRIVILEGE	<ul style="list-style-type: none"><li>ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018</li><li>Unknown-Host-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019</li><li>web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019</li></ul>
7	AC-7	UNSUCCESSFUL LOGON ATTEMPTS	<ul style="list-style-type: none"><li>ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018</li><li>web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019</li></ul>
8	AC-8	SYSTEM USE NOTIFICATION	<ul style="list-style-type: none"><li>ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</li><li>ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</li></ul>

# Screen Shots – OpenRMF Reports

A screenshot of the OpenRMF web application interface. The left sidebar is dark blue with white text and icons for navigation: Dashboard, Systems, Compliance, Templates, Reports (highlighted), and Upload. The top header is blue with the OpenRMF logo, a menu icon, a help icon, and a user profile icon. The main content area is titled "Reports" and shows a section for "Available Reports" with three cards: "Nessus Patch Listing" (with a grid icon), "System Pie Charts" (with a pie chart icon), and "System Checklist Listing" (with a checkmark icon). Each card has a green "Run Report" button at the bottom. The breadcrumb "Home / Reports" is visible in the top right of the main area.

OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

Reports

Home / Reports

Available Reports

Nessus Patch Listing

System Pie Charts









System Checklist Listing

Run Report

Run Report

Run Report

# Screen Shots – OpenRMF Nessus Reports



Reports - Nessus Scan Report

Home / Reports

Filters

System Filter: OpenRMF Production PaaS [Run Report](#)

**Choose your System and click Run Report**

Nessus Scan Report: 168.138.17.78

Show 50 entries

	Host	Plugin Id	Plugin Name	Family	Severity
+	168.138.17.78	57690	Terminal Services Encryption Level is Medium or Low	Misc.	2 - Medium
-	168.138.17.78	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	2 - Medium

Click the + to get more detailed information

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Plugin Type

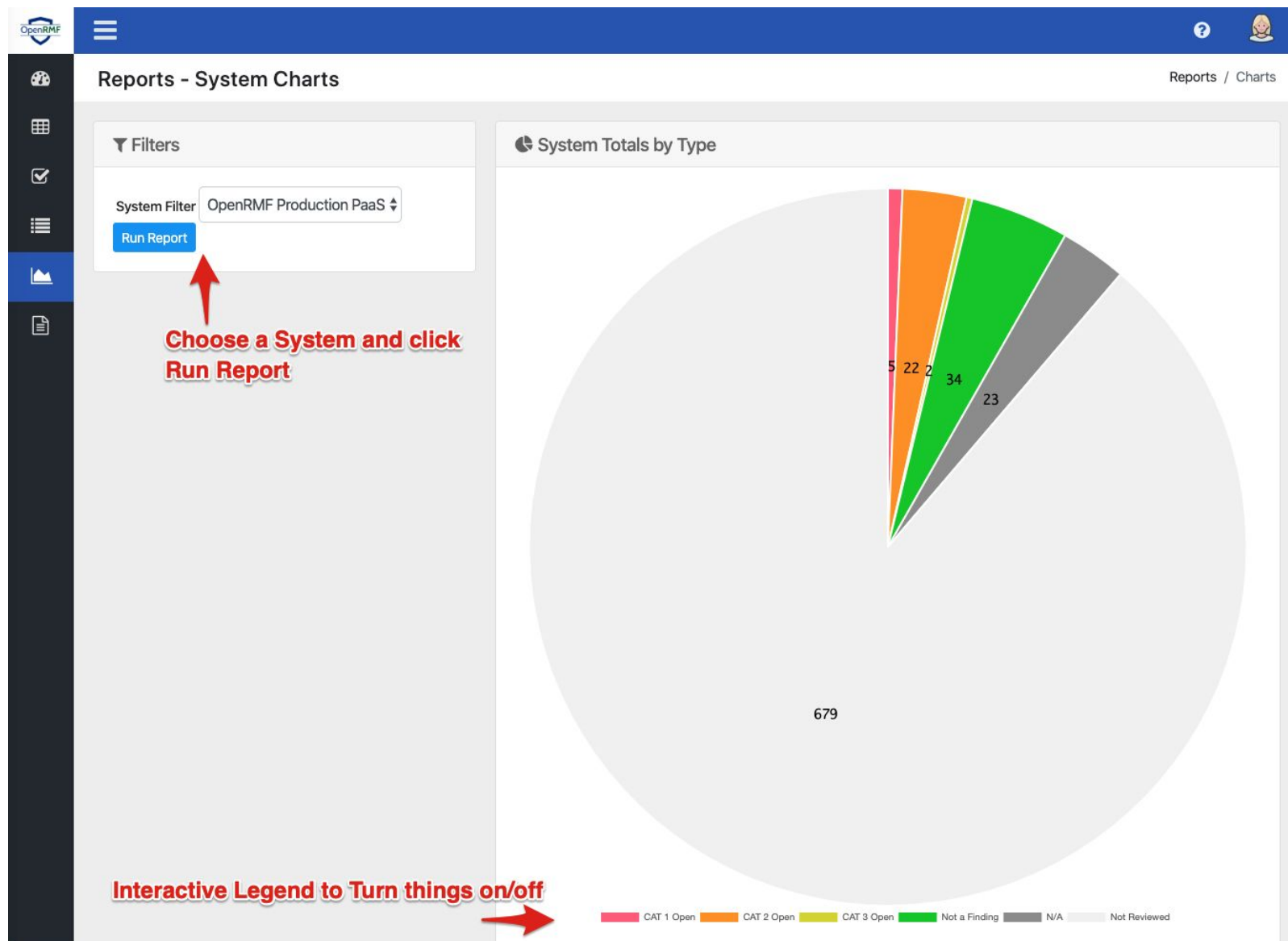
remote

Publication Date

2005/06/01

+	168.138.17.78	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2 - Medium
+	168.138.17.78	57688	SSL Self-Signed Certificates	General	2 - Medium

# Screen Shots – OpenRMF System Reports



# Screen Shots – OpenRMF Checklist Reports



Home / Reports

Reports - Checklist Report

Filters

System Filter  
OpenRMF Production PaaS

Checklist  
web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019

Run Report

Asset Information

**System:** OpenRMF Production PaaS  
**Host:** web1.myorg.mil  
**Title:** Application Security and Development Security Technical Implementation Guide  
**Release:** Release: 9 Benchmark Date: 25 Jan 2019  
**FQDN:**  
**Tech Area:**  
**Asset Type:** Computing  
**Role:** None

Show 50 entries

Search:

	Vuln ID	Severity	Rule ID	STIG ID	Status	Title	CCI
+	V-69239	medium	SV-83861r1_rule	APSC-DV-000010	Open	The application must provide a capability to limit the number of logon sessions per user.	CCI-000054
-	V-69241	medium	SV-83863r1_rule	APSC-DV-000060	Not Reviewed	The application must clear temporary storage and cookies when the session is terminated.	CCI-002361

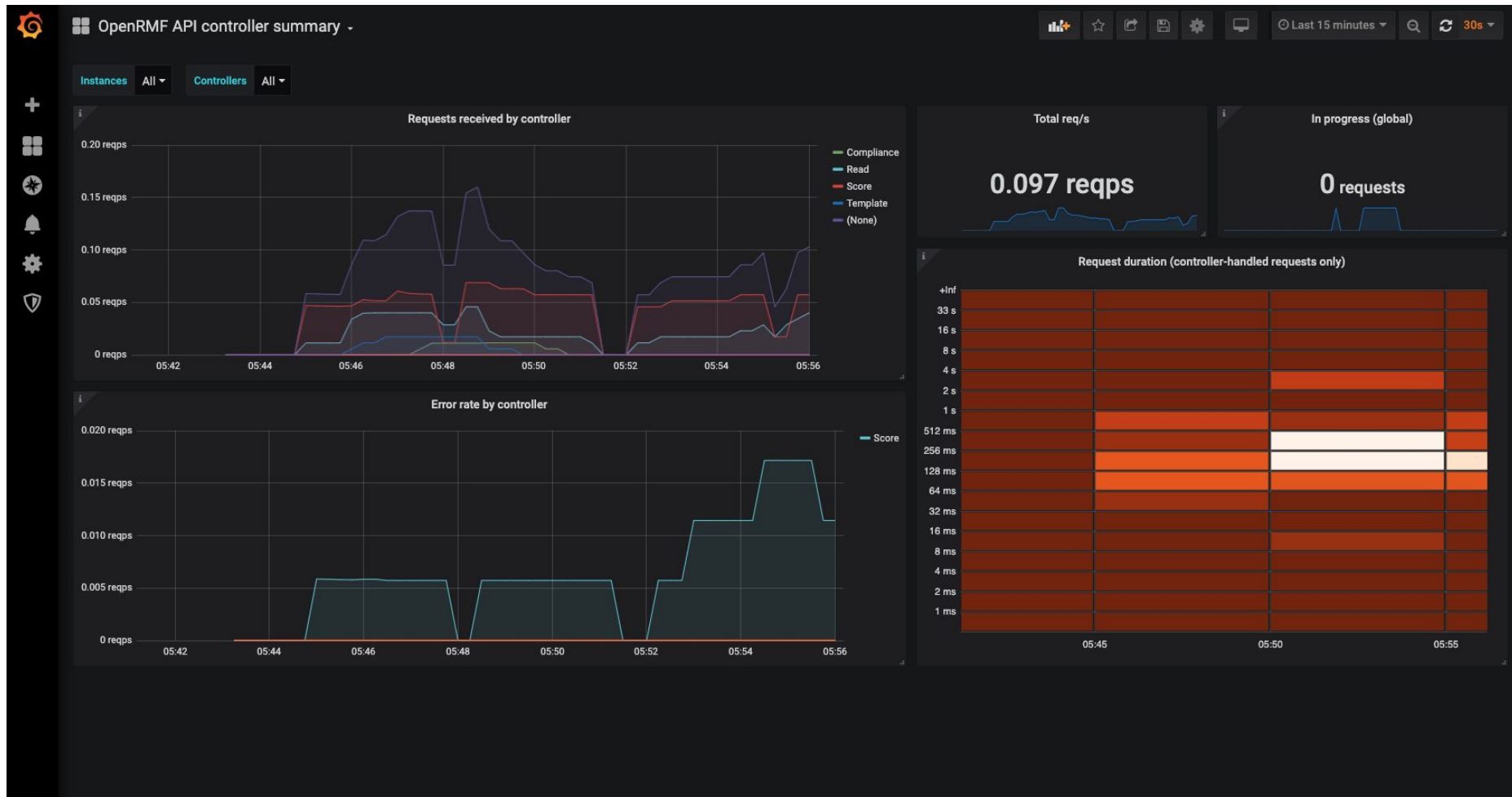
Discussion

Persistent cookies are a primary means by which a web application will store application state and user information. Since HTTP is a stateless protocol, this persistence allows the web application developer to provide a robust and customizable user experience. However, if a web application stores user authentication information within a persistent cookie or other temporary storage mechanism, this information can be stolen and used to compromise the users account. Likewise, HTML 5 provides the developer with a client storage capability where application data larger than the 4K cookie size limit can be stored on the local client. While this can be beneficial to the developer, this is considered insecure storage and should not be used for storing sensitive session or security tokens. A cross site scripting attack can put this data at risk. Web applications must clear sensitive data from files and storage areas on the client when the session is terminated.

Check Content

Review application design documentation and interview application administrator to identify how the application makes use of temporary client storage and cookies. Identify cookie and web storage locations on the client. Clear all browser cookies and web cache. Log on to the application and perform several standard operations, noting if the application ever prompts the user to accept a cookie. If prompted by the browser to save the user ID and password (decline to save the user ID and password), this is a finding. Log out of the application and close the browser. Reopen the browser and examine the stored cookies. The cookies displayed should be related to the application website. The procedure to view cookies will vary according to the browser used. Some modern browsers are making use of SQLite databases to store cookie data so use of a SQLite db reader/browser may be required. Open the cookies related to the application website and search for any identification or authentication information. While authentication information can vary on a per application basis, this is most often specified as "username=" or "password=" If the web application prompts the user to save their password or if a username or password value exists within a cookie or

# Screen Shots – OpenRMF Metrics (Grafana)





# Screen Shots – OpenRMF Metrics (Grafana)



# Screen Shots – OpenRMF Metrics (Grafana)

