

# OpenRMF - Innovation and Automation for DISA STIGs and NIST Controls

<https://www.openrmf.io>

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

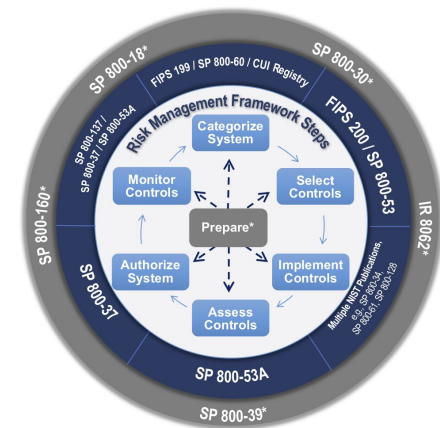
- Upload Checklists (XML or XCCDF SCAP)
- Run Compliance Reports
- Filter on Open Items remaining
- Manage Checklists by System

The screenshot displays the OpenRMF web application interface. On the left is a dark sidebar with navigation links: Dashboard, Systems (selected), Compliance, Templates, Reports, and Upload. The main content area is titled 'System Information and Checklists' and includes a breadcrumb trail 'Home / System / Checklists'. Below the title are two tabs: 'System Information' (active) and 'Audit Information'. The 'System Information' tab shows details for a system named 'OpenRMF Production PaaS', including the number of checklists (10), a description, Nessus scan status (N/A), and latest POA&M and risk assessment reports (both future). The 'Audit Information' tab shows creation and last update timestamps. Below these tabs is a 'Checklists' section with a table of 50 entries. The table has columns for Title, NAF, N/A, OPEN, and N/R. The first six rows of the table are visible, showing various STIGs and their compliance counts.

Title	NAF	N/A	OPEN	N/R
ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	5	3	9	226
ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	6	7	8	222
solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	6	3	2	224
sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	12	2	6	22
Unknown-Host-APACHE 2.2 SVR for UNIX STIG-R11 dated 25 Jan 2019 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	3	5	4	44
Unknown-Host-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019 last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	5	3	5	54

# Current Challenges Implementing RMF

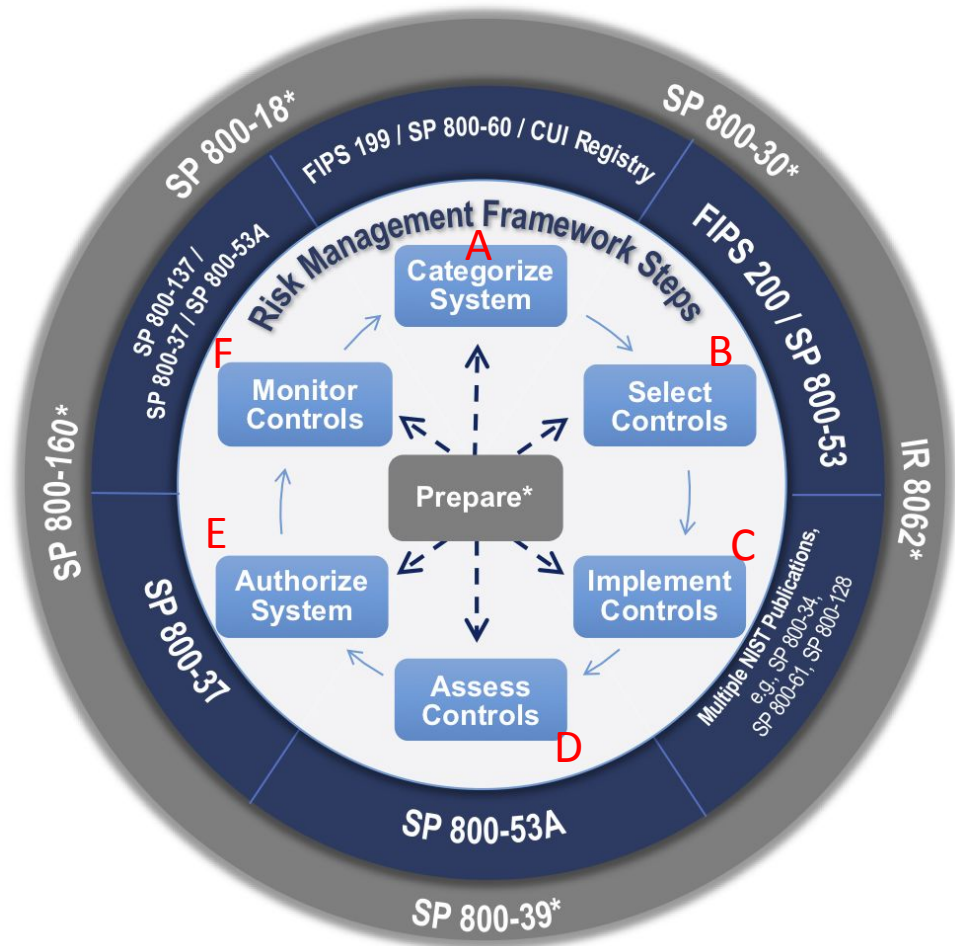
- Slow process driven by disparate systems
- Compliance with STIGs means checklists are numerous and not related directly to NIST control families
- Information shared via Email, DISA STIG Viewer, Excel, and shared folders – no single source of truth
- Limited management oversight into the IA status and security posture
- Must install Java to use the DISA STIG viewer
- IT Teams must manage the checklists manually
- Checklists are managed manually, one at a time
- Leadership sees Cybersecurity as “black magic” and “too hard”
- Leadership does not see value in Cybersecurity – only hardship
- No correlation of errors and deltas across checklists



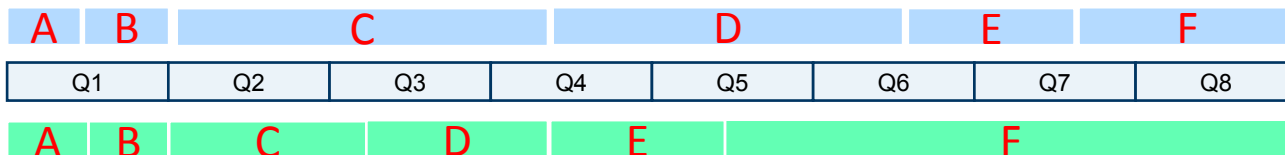
# The RMF Process – 6 Steps

## 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



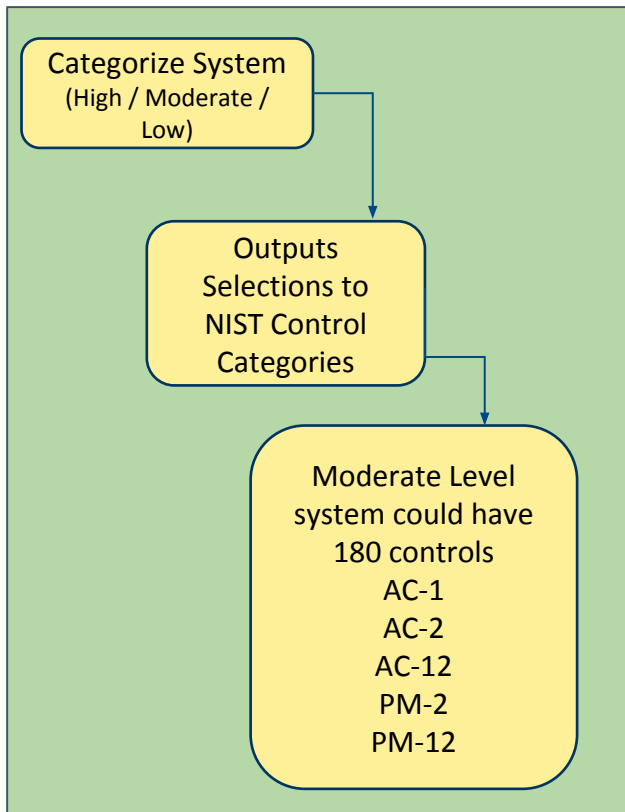
## Current Timeframe



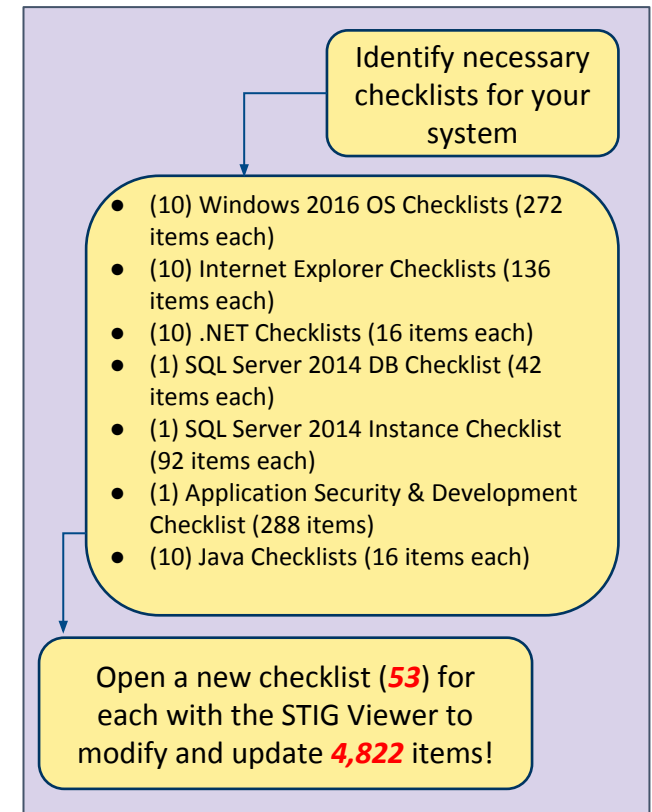
# Complexity of RMF in your System

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

## eMass Process



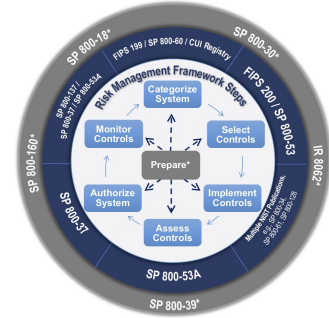
## DISA STIG Process



**No Automated  
Correlation**

**Completely Manual!**





# 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
- Browser based
- Role Based Access Control
- Easily Find Errors and Deltas Across Checklists
- Removes the IA Mystery!

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

# Coming Soon...

- Nov 2019 v 0.9
  - SCAP scan import to create/update a checklist
  - Single Source of Truth for all SCAP scan results
  - Automated update of checklist from scan results
- December 2019 v 0.10
  - ACAS scan results
  - Single Source of Truth for all ACAS scan results
  - Manage your System for all Checklists
- March 2020 v 0.11
  - Logging and Auditing across systems
- May 2020 v 0.12
  - Live Editing of Checklists Online
- December 2020 - v 1.0 Enterprise Features
  - Versioning of Checklists
  - More Detailed Reporting
  - Multi-Tenant
  - Risk Assessment Report generation
  - POA&M generation



# OpenRMF v 0.10 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



OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

System Information and Checklists

Home / System / Checklists

System Information

Update System

List All Systems

Title: OpenRMF Production PaaS

Checklists: 10

Description: The AWS production Platform as a Service for OpenRMF beta

Nessus Scan: N/A

Latest POA&M: (future)

Last Risk Assessment Report: (future)

Audit Information

Created: 12/01/2019 11:31 am

Last Updated: 12/01/2019 2:35 pm

Last Compliance Check: 12/01/2019 11:38 am

Checklists

Show 50 entries

Search:

↑↓	Title	NAF	N/A	OPEN	N/R
+	<a href="#">ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	5	3	9	226
+	<a href="#">ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	6	7	8	222
+	<a href="#">solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	6	3	2	224
+	<a href="#">sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	12	2	6	22
+	<a href="#">Unknown-Host-APACHE 2.2 SVR for UNIX STIG-R11 dated 25 Jan 2019</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	3	5	4	44
+	<a href="#">Unknown-Host-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019</a> last updated on 12/01/2019 2:35 pm <a href="#">delete</a>	5	3	5	54

# Screen Shots – OpenRMF Individual Checklist



OpenRMF

Dashboard

Systems

Compliance

Templates

Reports

Upload

My Checklist

Home / Checklist

Asset Information

Update Checklist Data

List All Checklists

System: OpenRMF Production PaaS

Host: sql1.myorg.navy.mil

Title: MS SQL Server 2014 Database Security Technical Implementation Guide

Release: Release: 6 Benchmark Date: 26 Jan 2018

FQDN: sql1.navair.navy.mil

Tech Area:

Asset Type: Computing

Role: Member Server

Last Updated on 12/01/2019 2:35 pm

Download

Export to Excel

Delete Checklist

Severity Breakdown

Open

Not a Finding

Not Applicable

Not Reviewed

52%

29%

14%

5%

Last Updated on 12/01/2019 2:35 pm

Save Chart

Category Breakdown

CAT I

CAT II

CAT III

95%

5%

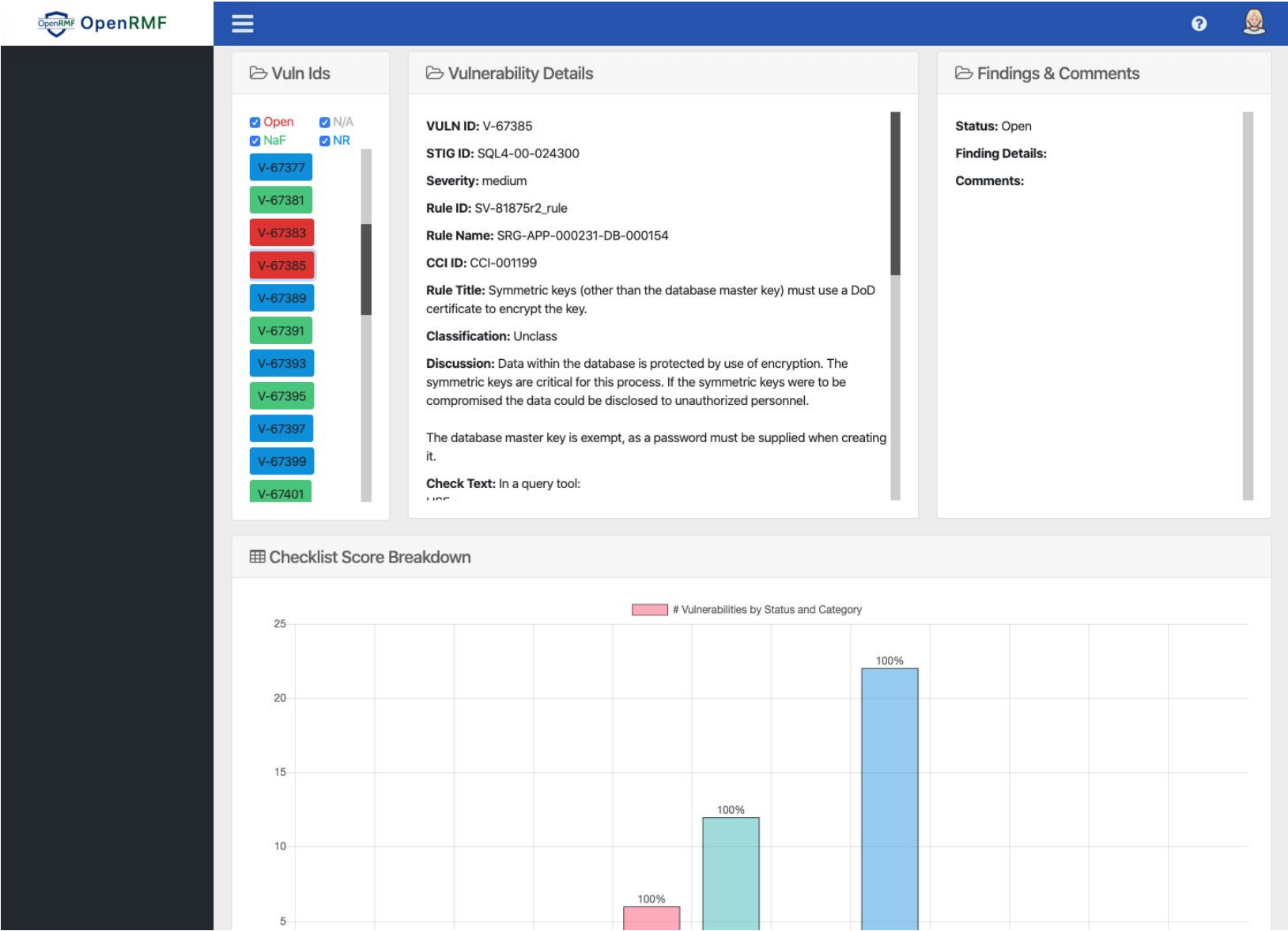
Last Updated on 12/01/2019 2:35 pm

Save Chart

sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018

	NOT A FINDING	NOT APPLICABLE	OPEN	NOT REVIEWED
Total	12	2	6	22
CAT 1	0	0	0	0
CAT 2	12	2	6	22
CAT 3	0	0	0	0

# 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	

# 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

