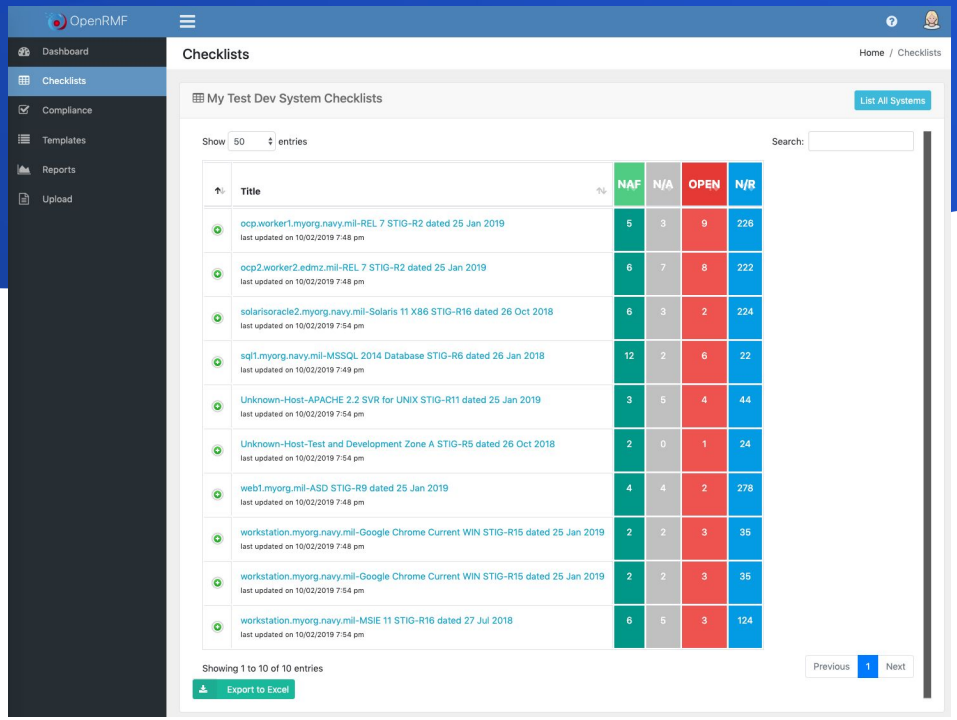
OpenRMF - Innovation and Automation for DISA STIGs and NIST Controls

https://www.openrmf.io

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

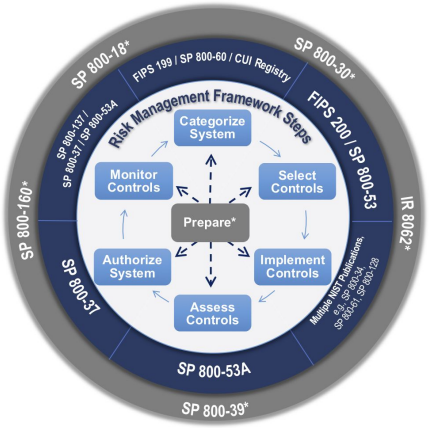
- Upload Checklists (XML or XCCDF SCAP)
- Run Compliance Reports
- Filter on Open Items remaining
- Manage Checklists by System



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

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

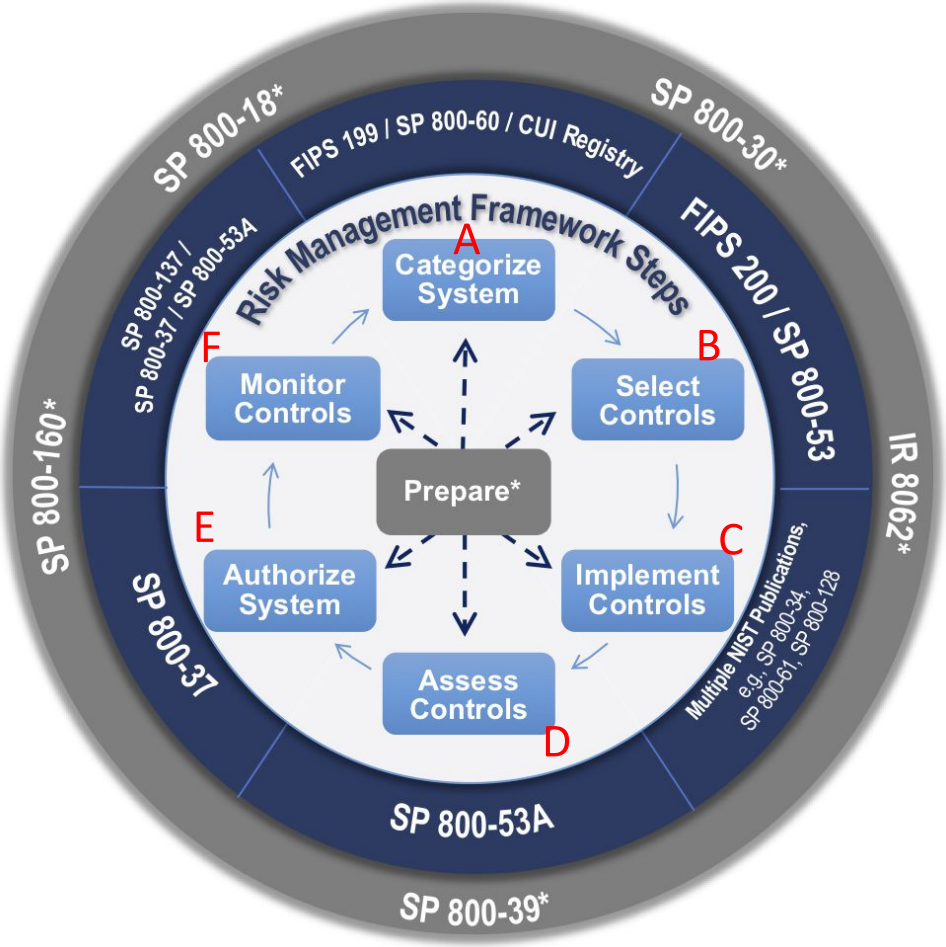


© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

The RMF Process – 6 Steps

Time Consumers

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



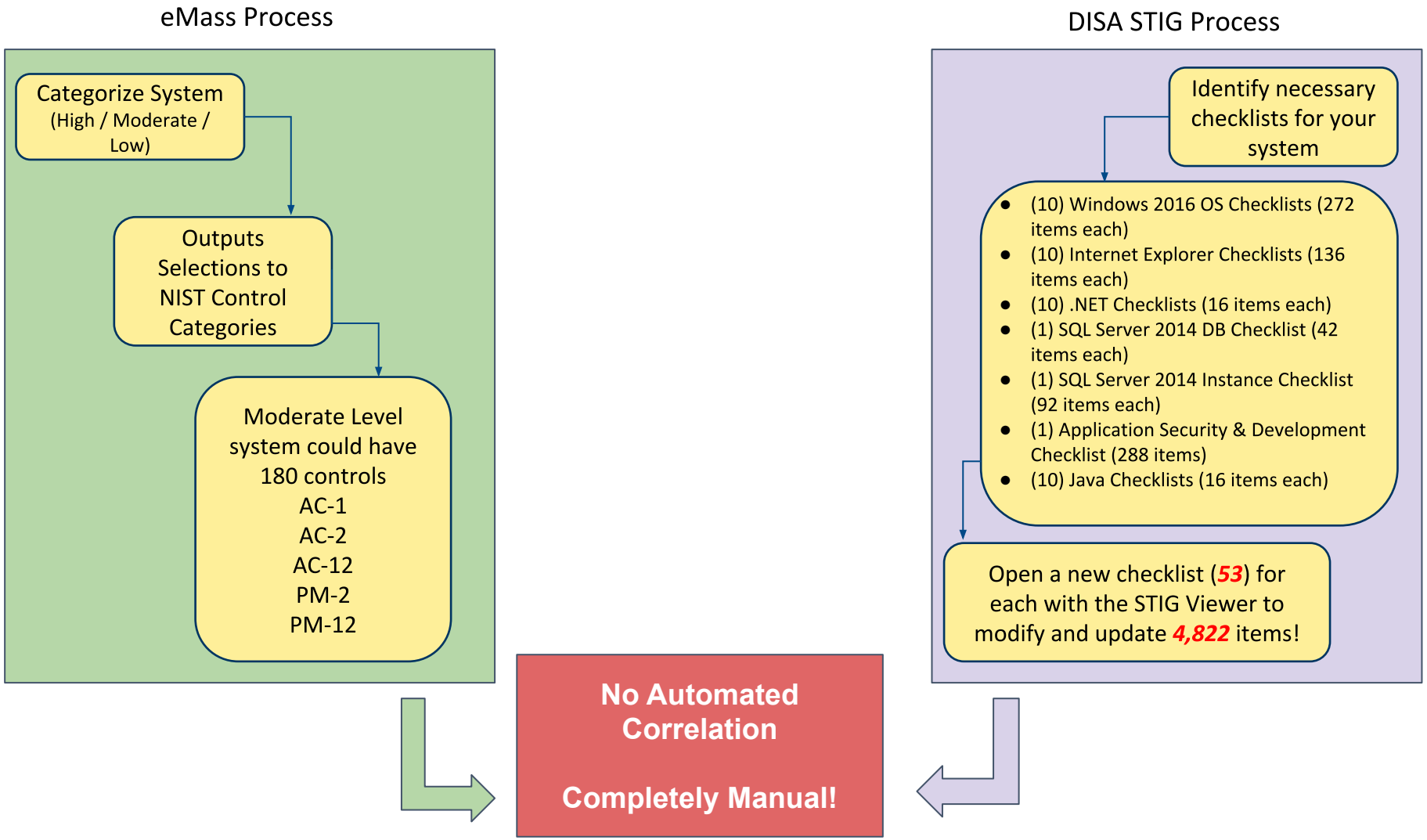
Current Timeframe

	A	B	C	D	E	F
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
OpenRMF	A	B	C	D	E	F

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

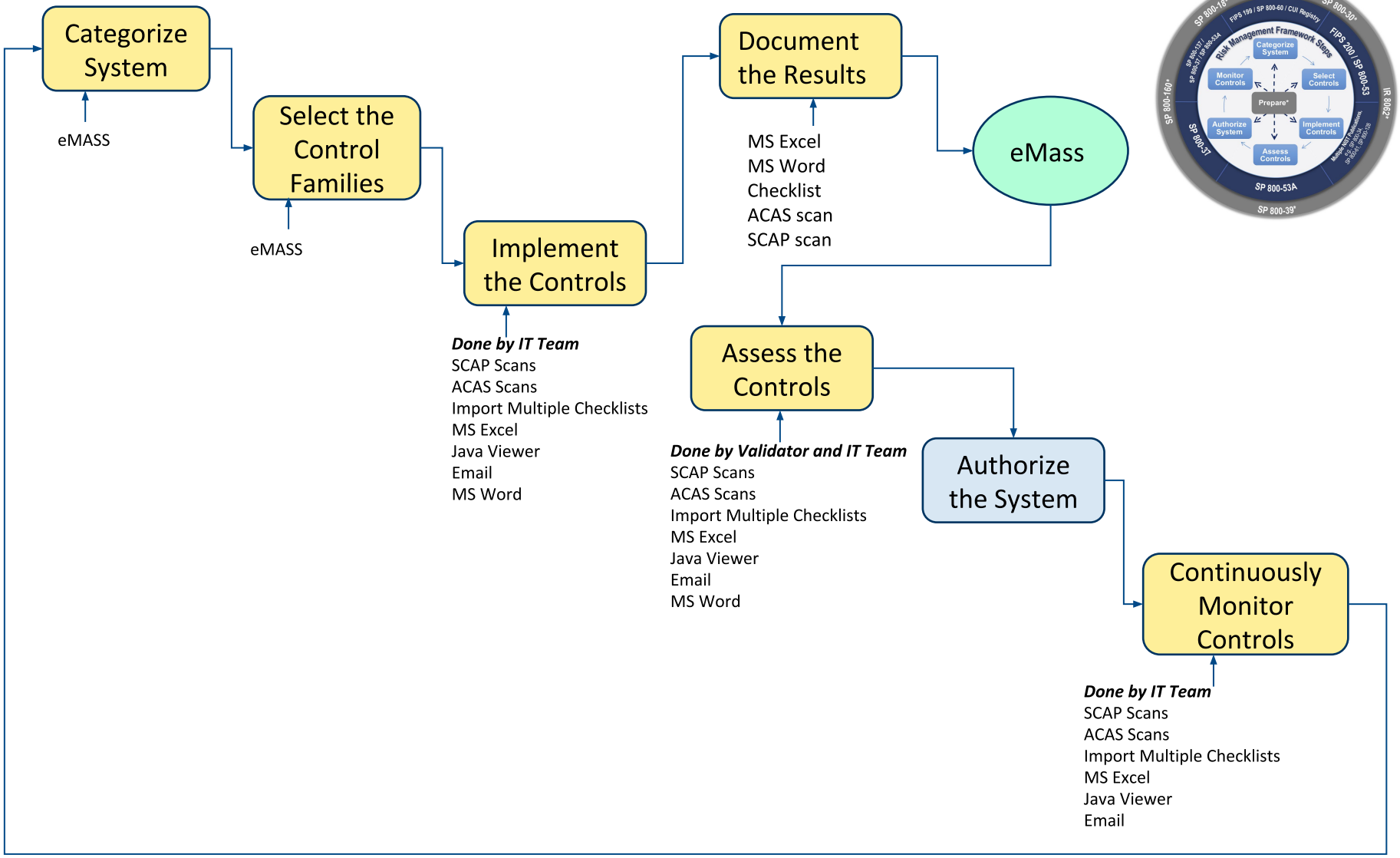
Complexity of RMF in your System

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



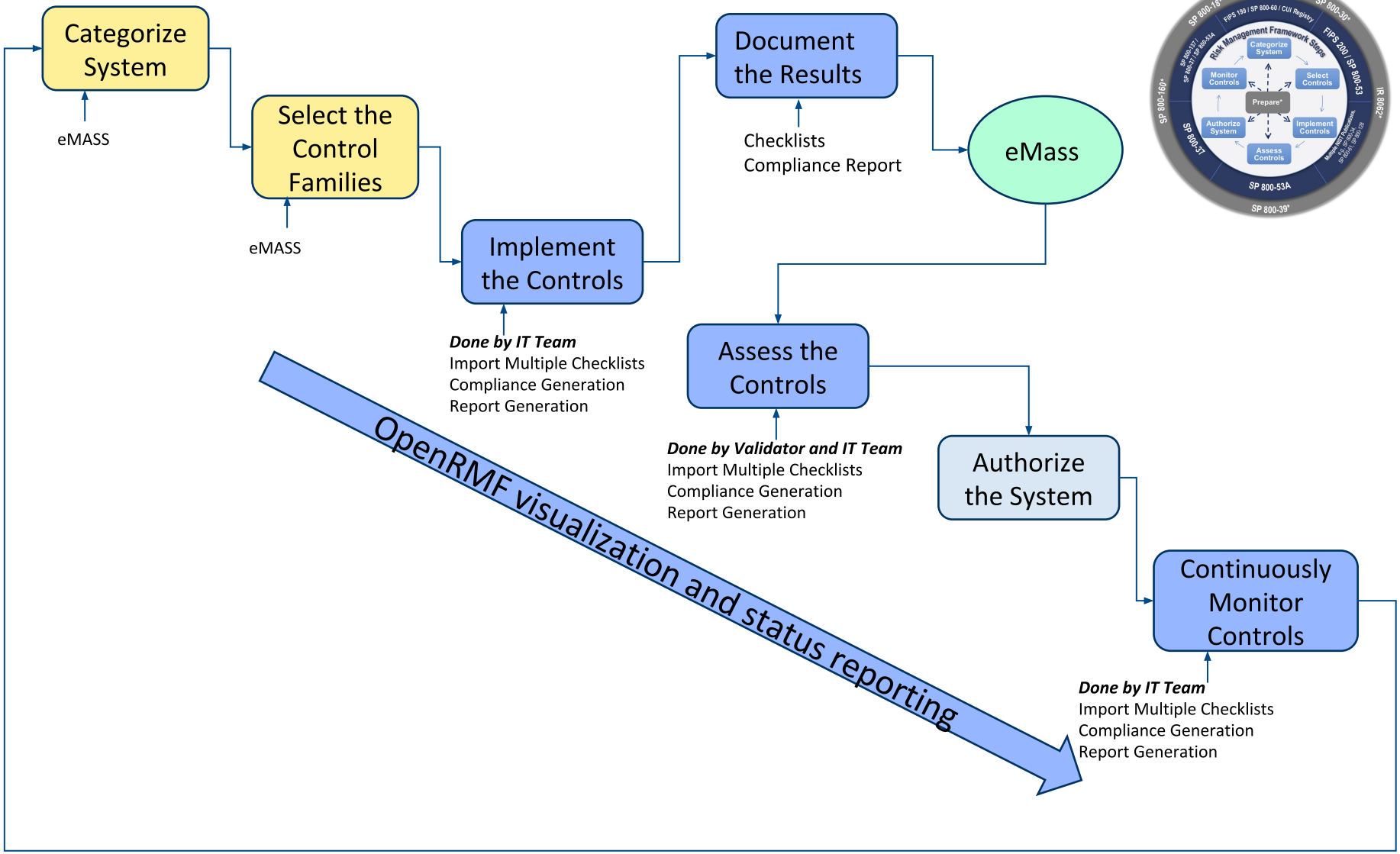
© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

Current RMF Process



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

RMF Process with OpenRMF Automation



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

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/

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

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
- January 2020 v 0.10
  - ACAS scan results
  - Single Source of Truth for all ACAS scan results
- 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

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

OpenRMF v 0.9 Screenshots

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

OpenRMF Testimonials

“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

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

Screen Shots – OpenRMF Checklist Upload

OpenRMF

Dashboard
Checklists
Compliance
Templates
Reports
Upload

Checklist file upload

Home / New checklist upload

Checklist Upload

Add a new System

New System Name

My New System

Enter a new system if not in the list above

Checklist Files (up to 5 at a time)

4 files were chosen | Choose Files

sqlserver2014database.ckl
size: 304 KB type: ckl

RHL7-worker2-edmz.ckl
size: 1.25 MB type: ckl

GoogleChrome.ckl
size: 206 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 Cingular LLC. © 2019 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Checklists by System

OpenRMF

- Dashboard
- Checklists
- Compliance
- Templates
- Reports
- Upload

Checklists

Home / Checklists

My Test Dev System Checklists

List All Systems

Show 50 entries

Search:

Title	NAF	N/A	OPEN	N/R
ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019 last updated on 10/02/2019 7:48 pm	5	3	9	226
ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019 last updated on 10/02/2019 7:48 pm	6	7	8	222
solarisoracle2.myorg.navy.mil-Solaris 11 X86 STIG-R16 dated 26 Oct 2018 last updated on 10/02/2019 7:54 pm	6	3	2	224
sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018 last updated on 10/02/2019 7:49 pm	12	2	6	22
Unknown-Host-APACHE 2.2 SVR for UNIX STIG-R11 dated 25 Jan 2019 last updated on 10/02/2019 7:54 pm	3	5	4	44
Unknown-Host-Test and Development Zone A STIG-R5 dated 26 Oct 2018 last updated on 10/02/2019 7:54 pm	2	0	1	24
web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019 last updated on 10/02/2019 7:48 pm	4	4	2	278
workstation.myorg.navy.mil-Google Chrome Current WIN STIG-R15 dated 25 Jan 2019 last updated on 10/02/2019 7:48 pm	2	2	3	35
workstation.myorg.navy.mil-Google Chrome Current WIN STIG-R15 dated 25 Jan 2019 last updated on 10/02/2019 7:54 pm	2	2	3	35
workstation.myorg.navy.mil-MSIE 11 STIG-R16 dated 27 Jul 2018 last updated on 10/02/2019 7:54 pm	6	5	3	124

Showing 1 to 10 of 10 entries

Previous 1 Next

Export to Excel

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

Screen Shots – OpenRMF Individual Checklist

OpenRMF

- Dashboard
- Checklists
- Compliance
- Templates
- Reports
- Upload

My Checklist

Home / Checklist

ocp.worker1.myorg.navy.mil-REL 7 STIG-R2 dated 25 Jan 2019

Update Checklist Data

	NOT A FINDING	NOT APPLICABLE	OPEN	NOT REVIEWED
Total	5	3	9	226
CAT 1	1	0	0	29
CAT 2	4	3	8	184
CAT 3	0	0	1	13

Last Updated on 10/02/2019 7:48 pm

Download | Export to Excel | Delete Checklist

STIG Information

Title: Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Release: Release: 2 Benchmark Date: 25 Jan 2019
Description: This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Asset Information

System: My Test Dev System
Host: ocp.worker1.myorg.navy.mil
FQDN: worker1.ocp.edmz.mydomain.mil
Tech Area: Application Review
Asset Type: Computing
Role: Member Server

Vuln Ids

Open N/A
NaF NR

V-71849
V-71855
V-71859
V-71861

Vulnerability Details

VULN ID: V-71861
STIG ID: RHEL-07-010040
Status: Open
Severity: medium
Rule ID: SV-86485r4_rule
Rule Name: SRG-OS-000023-GPOS-00006
CCLID: CCI-000048

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

Screen Shots – OpenRMF Generate Compliance

OpenRMF

- Dashboard
- Checklists
- Compliance
- Templates
- Reports
- Upload

Compliance

Home / Compliance

Compliance Generator

System Filter

My New System

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 Results

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

Show 50 entries

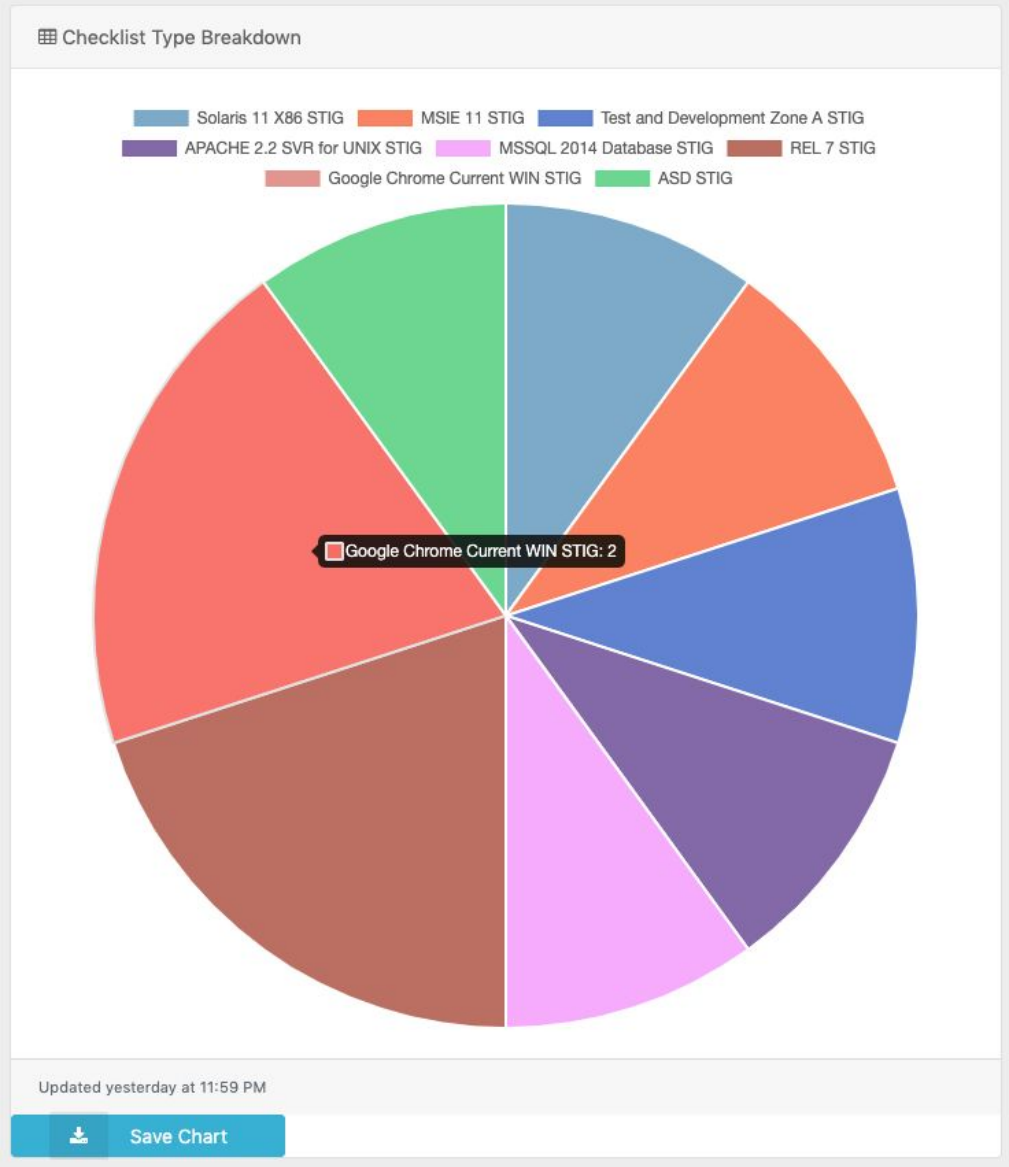
View your OpenRMF Dashboard

Search:

#	Control	Title	Checklists
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	
2	AC-2	ACCOUNT MANAGEMENT	• ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019 • web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
3	AC-3	ACCESS ENFORCEMENT	• ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019 • sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018 • web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
4	AC-4	INFORMATION FLOW ENFORCEMENT	• web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019 • workstation.myorg.navy.mil-Google Chrome Current WIN STIG-R15 dated 25 Jan 2019 • workstation.myorg.navy.mil-MSIE 11 STIG-R16 dated 27 Jul 2018

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

Screen Shots – OpenRMF Reports



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