OFFICE OF

INFORMATION

SECURITY

Authorization Requirements

Standard Operating Procedures

Version 1.47

April 13, 2023

U.S. Department of Veterans Affairs

Office of Information and Technology

Table of Contents

Document Revision History

Revision Date	Summary of Changes	Version	Author
7/22/2019	Initial Draft	1.0	OIS
8/23/2019	Second Draft	1.1	OIS
9/13/2019	Third Draft	1.3	OIS
10/11/2019	Fourth Draft	1.4	OIS
11/13/2019	Updated Premier/VA Network and Platform sections	1.5	OIS
12/13/2019	Updated Application Registration (section 3.2) Changed 'Secure Code Review' sections to 'Application Security Testing' for all applicable boundaries and updated the steps to complete the requirement Removed 'Quality Code Review' requirement Changed 'Secure Design Review' to 'Application Threat Modeling' for all applicable boundaries and updated the steps to complete the requirement Changed 'Status of Artifacts' to 'Status of Requirements' and added link to Status of Requirements template (Section 4) Added Security Impact Analysis (SIA) requirement for systems requiring a major change (Section 4)	1.6	OIS
1/13/2020	Added link for SIA Q&A in Section 4 Updated 'Security Configuration Compliance Data' instructions in all SCCD sections Added Common Control Providers/System of Record (SOR) details (i.e., VA T1SOR, IO SOR, VA Area SOR) in Appendix D and updated SOR verbiage throughout the SOP Updated all 'Application Security Testing' sections with new details on how results are uploaded to eMASS	1.7	OIS

Revision Date	Summary of Changes	Version	Author
2/12/2020	Created Appendix E – New Authorizing Official Guidelines	1.8	OIS
3/13/2020	Changed Major Change Form location to KS eMASS Job Aids (Section 4) and added link Updated verbiage in all technical scan sections to indicate that BOD 19-02 remediation timeline requirements are for Internet accessible systems only Added the Penetration Test/Application Assessment (WASA) requirement for Managed Service (Section 4.2.2.3) and updated the table in Appendix C Clarified scan requirements for FedRAMP (Section 4.3.2 and Section 4.4.2) Revised Step 1 for all Nessus scan sections to include the Hardware/Software SOP Inserted reference to the eMASS Implementation Guide throughout the SOP	1.9	OIS
4/13/2020	Added reference and link to the VA Cloud Security Procedural Guidance in the FedRAMP cloud Non-VAEC boundary (Section 4.4) Created Appendix F – Quick Reference Guide – Continuous Monitoring Changed SCA to Control Assessment to capture security and privacy controls	1.10	OIS

Revision Date	Summary of Changes	Version	Author
5/13/2020	Specified only one POA&M required for each technical scan requirement. Update is within each technical scan section Added requirement that FedRAMP systems must have registered system in eMASS for the FedRAMP and the enterprise/VA boundary. Entry names in eMASS must be same as names listed on FedRAMP.gov. Details in section 4.3 and section 4.4 VAEC link updated with new URL Added a note in section 4.3.2 and section 4.4.2 to ensure Platform-as-a-Service (PaaS) servers/services are not added to the Hardware and Software system inventory	1.11	OIS
6/12/2020	Updated the SIA paragraph in Section 4 Added CMP template link and template contact information to CMP section for all boundaries except for VAEC and Facility. VAEC already has a template and the Facility CMP template is in progress Replaced CM-2 reference with CM-9 within the CMP sections. When uploading the CMP to eMASS, CM-9 should be added as the appropriate security control	1.12	OIS
7/13/2020	ISO Responsibilities and Attestation templates have been added to the KS Job Aids page with link included in Section 3.1 Added a Nessus scan section (Section 4.6.2.1) for the Medical Device boundary	1.13	OIS

Revision Date	Summary of Changes	Version	Author
8/13/2020	Added note to section 2 that VA ATO information should not leave the VA network Added SCCD requirement to Premier/VA Network boundary (section 4.1.2.6) Clarified one POA&M item required for each technical scan performed (e.g., new Nessus scan POA&M item required for each monthly scan). Update is within each technical scan section New section added for Security Boundary Guidance (section 3.3)	1.14	OIS
9/11/2020	Updated ISA/MOU template link	1.15	OIS
10/13/2020	Incorporated latest eMASS update by changing Risk Review stage to RMF Step 5: Stage 3 in section 3.1	1.16	OIS
11/13/2020	Updated URL for the VAEC homepage through section 4.3 Updated FedRAMP package request email address for VA OIS ESA CSA Added Platform as a Service (PaaS) clarification/guidance to FedRAMP Cloud VAEC section 4.3.2 Updated URLs for Medical Device Nessus scans in section 4.6.2.1	1.17	OIS
12/11/2020	Added ISRM Compliance contact information (email address) in Section 1 Clarified that 'system-level' system stewards assist with REEF mitigation in applicable Nessus scan sections	1.18	OIS

Revision Date	Summary of Changes	Version	Author
01/13/2021	Clarified in Penetration Test/Application Assessment sections that VA-CSOC does not perform on-site scans of external systems Updated requirements for Internet facing applications in Penetration Test/Application Assessment sections Added SCCD FAQ link in each SCCD section	1.19	OIS
02/11/2021	Updated section 8.1.1.2 to reference name change from VA IO SOR to VA Enterprise SOR (VA ENTSOR). Updated throughout document Updated Technical Scans section 4.5.2.2 to include new requirement that IA-5.3 will be utilized for POA&M creation where necessary for EDS Updated URL for Knowledge Service eMASS Job Aids pages in section 4.0 to new SharePoint site	1.20	OIS
3/12/2021	Updated the Note in section 3.1 to add Control Review timeline details for RMF Step 4 Added RMF Step 4 Assessment requirement (GRC Bulletin #48) to all Control Review sections	1.21	OIS
03/24/2021	Added Appendix G Type Authorization	1.22	OIS

Revision Date	Summary of Changes	Version	Author
04/13/2021	Addition of section 4.5; FedRAMP Enterprise Cloud Application (-e Systems) procedures Update of Appendix B and C to include FedRAMP Enterprise Cloud Application (-e Systems) Updated all Penetration Test/Application Assessment sections to remove redundant language “and/or internet facing” in first bullet Updated all Nessus scan sections to remove step 5 from completion steps Updated all Application Threat Modeling sections with clarified procedures Updated all Application Security Testing sections with clarified procedures Updated Application Registration section 3.2 with clarified procedures	1.23	OIS

05/13/2021	Update to all System Security Plan (SSP) sections; Step 3: "The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details" Update of SOR definition in Appendix D Updated section 4.3, Application hosted in FedRAMP cloud (VAEC) with additional VA ENTSOR language Updated section 4.3.2, Technical Scans/Testing Requirements with clarified language and VAEC links Updated section 4.3.2.6, Security Configuration Compliance Data (SCCD) with PaaS Note Added IaaS/PaaS to Appendix A0 Acronyms/Definitions table Added additional section 8.1.1.4, Cloud Service Provider SaaS and PaaS SOR to Appendix D, Common Control Providers/System of Record (SOR) Added to section 3.3 Step 10 that devices can only be associated with one FISMA boundary Added to section 4 that the Status of Requirements should be uploaded to the Artifacts tab in eMASS Added note in all SCCD sections to address issues reaching the 90% threshold due to offline devices Added note on how to request an ISSO in section 3.1	1.24	OIS

Revision Date	Summary of Changes	Version	Author
	Moved the note in section 3.1 that references the time requirements to be in RMF Step 4 and RMF Step 5: Stage 3 to Section 4 Added note to section 4.4 and section 4.5 that the -F/-VAF and -e packages must be completed simultaneously in eMASS		
06/11/2021	All ICAMP links have been updated to reflect current Cloud migration Specified which CCI to use for POA&M creation to all Nessus scan, Penetration Test/Application Assessment, and Database Scan sections Moved Application Threat Modeling requirement from Technical Scans/Testing Requirements section to Security Documentation section for each applicable boundary Updated Appendix B and Appendix C to reflect the Application Threat Modeling change	1.25	OIS
07/13/2021	Updated section 4.3 header from “Application hosted in FedRAMP cloud (VAEC)” to “Application Hosted in the VA Enterprise Cloud (VAEC)” Updated section 4.3 “VAEC main page” link to “VAEC Cybersecurity page” Updated section 4.3 to include additional language regarding applications migrating from Traditional/On-Premises/Hybrid applications	1.26	OIS

Revision Date	Summary of Changes	Version	Author
08/11/2021	Updated sections 11.1.3.1 and 11.1.3.2 in Appendix G – Type Authorization Added missing ISCP section to Facility boundary Updated section 4 to include addition of "Information System Change Requests" and clarified guidance for SIA and Significant/Major Changes Updated Configuration Management guidance to include VA ITSM change control system guidance for sections 4.1.1.1, 4.2.1.1, 4.3.1.1, 4.4.1.1, 4.5.1.1, and 4.6.1.1 Added 'IT Service Management (ITSM)' to Appendix A – Acronyms/Definitions table Added 'Software Composition Analysis' requirement to all applicable Technical Scans/Testing sections. New scan/analysis will be completed during the Application Security Testing process Updated Appendix C – Quick Reference Guide – Technical/Testing Requirements to include new 'Software Composition Analysis' requirement Updated all references in section 4.6 Facility from "The ISO or system steward" to "The ISO, system steward, or designee"	1.27	OIS

Revision Date	Summary of Changes	Version	Author
09/10/2021	Removed format suggestion in section 4 to eliminate confusion Added 'validate' to all Control Review sections in paragraph 3 Updated step 5 in all SCCD technical scan sections with "SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort" Replaced 'Software Assurance Request' verbiage with 'Application Security Support' in Application Registration section and all Application Security Testing sections Added language 'Kotlin' to supported programming languages in all Software Composition Analysis sections	1.28	OIS
10/13/2021	Added 'Save As' filename requirement for all monthly Nessus scan/ICAMP reports along with screen capture of how to 'Save As' within ICAMP to all Nessus scan sections (Step 3c)	1.29	OIS
11/12/2021	Added sentence to section 3.3 Step 10 that all lower environments, such as Development and Test, must be added to the Hardware/Software Inventory for vulnerability scanning purposes Removed 'Minor Application Self-Assessment' section. Added reference and link to 'Minor Assessment Requirements for eMASS SOP' in second paragraph of section 4	1.30	OIS

Revision Date	Summary of Changes	Version	Author
12/13/2021	Updated all Application Threat Modeling, Application Security Testing, and Software Composition Analysis sections to eliminate confusion between DevSecOps and Non-DevSecOps environments Added verbiage at beginning of section 4.4 to specify the non-VAEC systems covered in the section Note added in section 4.5 FedRAMP Enterprise Cloud Application to clarify responsibilities for -F, -VAF, and -e packages Updated Roles and Responsibilities within CMP section of the Facility boundary Updated first paragraph in all SCCD sections to include a BigFix alternative if BigFix cannot be installed	1.31	OIS
01/13/2022	Added Appendix H – Provisional ATO Process Updated verbiage in section 3.3 Step 10 for lower environments Added link for IRP template in section 4.6.1.3	1.32	OIS
02/11/2022	Updated verbiage in last sentence of the 'Warning' box in all Software Composition Analysis sections	1.33	OIS

Revision Date	Summary of Changes	Version	Author
03/11/2022	Clarified responsibilities in sections 4.4 and 4.5 for FedRAMP packages and added single instance (-i) verbiage where appropriate Updated FedRAMP header in section 4.5 to include Single Instance (-i) Updated broken links for HW/SW Import SOP throughout document Changed verbiage in all Control Review sections that states the Control Review team will review a sub-set of the top findings found in OIG audits from the past fiscal year audits Added note in P-ATO section 12.2 that -F/-VAF packages must be progressed at the same time as -e/-i packages	1.34	OIS
04/13/2022	Updated MOU/ISA team name in all applicable sections Added Cybersecurity Support request details to Section 3.1 Provided additional clarification to Section 3.3 Step 10 Added single instance (-i) reference to second paragraph of Section 4.4 Updated the Other Federal Agency boundary in Appendix B and Appendix C Added sentence to the end of Section 4.8 Other Federal Agency with a link to the Reciprocity SOP on Knowledge Service Added Appendix I – Action Item Release	1.35	OIS
05/13/2022	Updated CSOC Database Scan Questionnaire link in Sections 4.1.2.2, 4.2.2.2, 4.3.2.2, and 4.4.2.2	1.36	OIS

Revision Date	Summary of Changes	Version	Author
06/10/2022	Removed "Note" for DRP and ISCP due to invalid details in sections 4.1.1.2, 4.1.1.4, 4.2.1.2, 4.2.1.4, 4.3.1.2, 4.3.1.4, 4.4.1.2, 4.4.1.4, 4.5.1.3, 4.6.1.2, 4.6.1.4, 4.9.1.1 Updated MOU/ISA portal links in sections 4.1.1.5, 4.2.1.5, 4.3.1.5, 4.4.1.5, 4.5.1.4, 4.6.1.5, 4.7.1.1, 4.9.1.2	1.37	OIS
07/12/2022	Minor formatting adjustments throughout document	1.38	OIS
08/12/2022	All site and report links updated to reflect new Information Central Analytics Metrics Platform (ICAMP) migration to SharePoint Online site All ICAMP "report export" step and screen captures updated	1.39	OIS
9/13/2022	Updated Appendices B and F to include Disaster Recovery Plan Test, Incident Response Plan Test, and Information System Contingency Plan Test	1.40	OIS
10/13/2022	Added Information System Vulnerability Management Plan (ISVMP) guidance in section 4. Clarified Test document requirements for FedRAMP systems.	1.41	OIS
11/10/2022	Minor formatting adjustments throughout document	1.42	OIS
12/13/2022	Included link to new Templates section of the eMASS Knowledge Service page Updated each Security Configuration Compliance Data (SCCD) section to account for the new report requirements Updated sections 11.1 and 11.2 in Appendix G – Type Authorization	1.43	OIS

Revision Date	Summary of Changes	Version	Author
01/13/2023	Added Information System Contingency Plan and Business Impact Analysis at a requirements for Medical Devices Added link to connections, ports, and protocols template	1.44	OIS
02/13/2023	Removed Appendix I – Action Item Release Updated each section to address ISCP and DRP requirements Added BIA requirement to each section Updated Appendices B and F to add the BIA requirement Updated links to System Owner Attestation and System Owner Responsibilities Added link in Section 3.1 to the eMASS Account Access Request Policy and Procedure SOP	1.45	OIS
03/13/2023	Fixed broken links; Minor formatting adjustments throughout document	1.46	OIS
04/13/2023	Updated POA&M requirements for sections 4.1.2.1, 4.1.2.2, 4.1.2.3, 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.6, 4.3.2.2, 4.3.2.3, 4.4.2.1, 4.4.2.2, 4.4.2.3, and 4.6.2.1 Added verbiage to section 4.3 regarding the transition of a traditional system to a cloud system. Added verbiage to section 4.3.2.2 regarding Database scan requirements	1.47	OIS

1 *Purpose*

To obtain and maintain a Department of Veterans Affairs' (VA) Authorization to Operate (ATO), the authorization requirements included within the contents of this document must be completed. Enterprise Mission Assurance Support Service (eMASS), VA's Governance, Risk and Compliance (GRC) tool, is the authoritative management tool for VA's Assessment and Authorization (A&A) process and Risk Management Framework. All systems will be assessed in

eMASS by the Risk Review team for an authorization recommendation to be submitted to the Authorizing Official (AO) for final ATO consideration. eMASS guidance documentation can be found in the eMASS VA Implementation Guide and eMASS User Guide located on the ***Help*** page within eMASS.

This is a living document based on current federal and VA security policies, standards, and guidance, and is subject to change. For any questions regarding the Authorization Requirements SOP Guide for eMASS, please reach out to ISRM Compliance.

2 *Scope*

These procedures apply to systems that are required to obtain an ATO. These systems must be entered into eMASS and be evaluated for potential risk to the VA. The ATO packages/artifacts and any other ATO information should not leave the VA network.

3 *Authorization Prerequisites and Registration*

3.1 Application Prerequisites

Information System Owners (ISO) for a new information system looking for a determination on an ATO requirement or looking to begin the process to obtain an ATO can submit a request to the GRC Oversight Committee. Follow the steps below to complete the eMASS system pre-registration. For any questions regarding system registration, email the VA OIS GRC Intake Reviewers.

1. Fill out a new Cybersecurity Support request form by going to the Cybersecurity Request Portal.
2. Your request will be reviewed by an intake team for assignment of a new ISSO and the GRC Committee will include the new information system request for discussion on the weekly meeting agenda, scheduled Thursdays at 12:00pm EST. During the meeting, the GRC Committee will approve or deny the information system or request additional information before a decision.
3. Once the GRC Committee approves the new information system request and an eMASS administrator approves the system, an email is automatically generated in eMASS to notify the System Owner or delegate of the approval. The System Owner or delegate must then complete the eMASS system registration. Access to eMASS is required to register a new system.
4. The System Steward completes the eMASS System Registration. The eMASS Account Access Request Policy and Procedure SOP can assist with the registration process. You may also reach out to the ISSO or the VA OIS GRC Intake Reviewers via email with any questions regarding system registration.
5. Once the eMASS system registration has been completed, the GRC Oversight Committee will approve it and the system project team can begin documentation for security and privacy controls and working through the RMF workflow towards an ATO. The ISO must

complete the System Owner Responsibilities and the System Owner Attestation documents then upload both to the Artifacts tab within eMASS.

3.2 Application Registration

Custom-developed VA applications (and deployed instances of Commercial off the Shelf (COTS) and Software as a Service (SaaS) applications at the direction of OIS and/or CSOC), are required to be registered with OIS Software Assurance. The primary goal of registration is to uniquely identify source code for custom-developed applications (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) in anticipation of security testing, and to generate unique identifiers to correlate security testing artifacts.

Application registration guidance is provided below:

- Applications are registered with OIS Software Assurance
- Application registration is a prerequisite to Application Security Testing
- Application Security Testing is in turn a prerequisite to Penetration Testing
- This requirement is not applicable to VistA systems

Application registration completion steps:

1. Navigate to the Your IT Services portal using your web browser.
2. Fill out Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name;
    b. If applicable, update the auto-populated requestor information fields;
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Registration;
    d. In the Application Name field, enter your application's name;
    e. Fill out this PDF form and attach it to the request using the Add attachments link.
3. Click on the Submit button.
4. Make a note of your ticket's request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can view this ticket, or any of your open tickets, through Your IT Services portal.

3.3 System Boundary Guidance

The System Boundary needs to be properly represented in eMASS to ensure the system description, environment, architecture, assets, devices, and hardware and software baselines are recorded accurately.

Roles and Responsibilities

The ISO and system steward should work to document the boundary. The ISSO should review and validate in RMF Step 1 – Security Categorization.

Standards / Guidelines

- NIST SP 800-60
- NIST SP 800-53 (CM-8 Information System Component Inventory, and enhancements)
- FIPS 199, FIPS 200
- VA Handbook 6500
- Hardware and Software System Inventory Import SOP – located in Standard Operating Procedures section of the eMASS Knowledge Service page

Boundary completion steps:

1. On the system information tab, ensure the **System Description** field is accurate. Provide a narrative description of the system, function, and purpose.
2. On the system information tab, ensure the **System Environment** field is accurate. Provide a general description of the technical system. Include the primary hardware, software, and communications equipment. Include any environmental or technical factors that raise special security concerns. Include hosting location name (i.e., Amazon, AITC, the name of the vendor data center).
3. On the system information tab, ensure the **System Authorization Boundary** field is accurate and includes a description of everything within the accreditation boundary of the system. Include Pre-Prod* environments if they will handle production data and ensure to include any minor applications, child applications, and VA custom developed applications covered by the same ATO. Do not include connected system information or systems that are not covered by the scans of this boundary, associated artifacts, or control implementation. (*Note: per step 10, all assets for all lower environments, including the Development, Test, and pred-prod environments, must be added to the Hardware/Software Inventory for vulnerability scanning purposes.)
4. On the system information tab, upload a **System Authorization Boundary diagram**. Select "Choose File" to attach related evidence/diagram. The boundary diagram must include:
    a. all components included in the system boundary;
    b. an authorization boundary drawn around the components indicating that they are within the system's boundary;
    c. any other systems/devices outside of the system's boundary to which the system is directly connected; and
    d. a legend explaining what each shape/icon/line/etc. represents.
5. On the system information tab, ensure the **Hardware / Software / Firmware** field is accurate. List the Hardware/Software/Firmware used by the system.
6. On the system information tab, ensure the **System Enterprise and Information Security Architecture** field is accurate. The security architecture field should accurately and completely describe:
    a. the required security functionality;
    b. the allocation of security controls among physical and logical components; and
    c. expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

7. On the system information tab, upload a **System Enterprise and Information Security** Architecture diagram. The diagram should include an authorization boundary that:
    a. clearly defines services wholly within the boundary;
    b. depicts all major components or groups within the boundary;
    c. identifies all interconnected systems, including the Agency Access Point (e.g., VA.gov);
    d. depicts all major software/virtual components (or groups of) within the boundary; and
    e. is validated against the inventory.
8. On the system information tab, ensure **the Information Flows / Paths** field is accurate. This field should:
    a. identify anywhere Federal data is to be processed, stored, or transmitted;
    b. clearly delineate how data comes into and out of the system boundary; and
    c. depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed, including the use of definitive Agency DNS.
9. On the system information tab, upload an **Information Flows / Paths** diagram. The diagram should:
    a. identify anywhere Federal data is to be processed, stored, or transmitted;
    b. clearly delineate how data comes into and out of the system boundary; and
    c. depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed, including the use of definitive Agency DNS.
10. All systems should complete the **Hardware and Software System Inventory Import** process to ensure all IPs and host names are properly added to eMASS so that scans and integrations with ICAMP, BigFix, and CDM will function. Instructions can be found in the Hardware and Software System Inventory Import SOP. The SOP can also be found by going to the Standard Operating Procedures section of the eMASS Knowledge Service page. The connections, ports, and protocols Template can be found in the Templates section of the eMASS Knowledge Service page. The ISO or system steward must ensure all hostnames for endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the Hardware and Software Inventory Import SOP for managing the Hardware/Software Inventory. Please note, devices can only be associated with one FISMA boundary. If the device or component is shared, it should only be registered with the owning information system responsible for Enclave/OS/Infrastructure ownership and management. Additionally, development assets that process, store, transmit VA data, have an interconnection to a system that has an ATO, and/or external to VA, must be inventoried for vulnerability scanning. These specific types of lower environment assets should already be part of an ATO boundary due to the inclusion of VA sensitive information and/or connection to a production or external to VA environment. All other lower environment assets must also be inventoried for discovery purposes due to being connected to the VA network. These inventory assets should not be included within any part of an ATO process outside of CM-

8 and CM-8(5). They are included solely for discovery purposes at this time. As a reminder, unaccredited lower environments are never allowed to process, store, and/or transmit VA sensitive information without an ATO. All lower environment assets must adhere to VA standards for naming conventions, patching, vulnerability remediation, configuration management, and IP Governance for rapid identification within inventory reports.

11. The BigFix agent **must be** installed to receive Security Configuration Compliance Data as well as communicate with CDM. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.

Continuous Monitoring Requirement

The system boundary must be updated and validated on an annual basis (90 days for medical devices per CM-8.1) or when any change to the system boundary, devices, hardware, or software baselines occurs. Ensure devices are only associated with one FISMA boundary.

Note: Questions about the system boundary guidance or processes should be directed to ISRM.

4 *Assessment and Authorization Requirements*

The Authorization Requirements SOP details the technical scans/testing and security documentation requirements for each boundary. Within each boundary section, details are provided for the required security artifacts, including security document requirements, technical/testing requirements, and Federal/VA guidelines. Additional information related to the parties/OIS organization(s) that can provide additional guidance or assistance for each artifact may also be provided. A Status of Requirements, which is located in the Templates section of the eMASS Knowledge Service page, needs to be completed for each ATO package and indicate if a security document and/or technical/testing requirement is applicable or not applicable. The Status of Requirements should provide details on the latest security documentation and technical/testing requirement results or explain why each security document and/or technical/testing requirement is not applicable or not completed. Once the Status of Requirements is completed, it should be uploaded to the Artifacts tab within eMASS. Security artifacts should not be password protected. eMASS limits access to personnel with a need to view the system details and security artifacts.

For items related to Minor Applications in eMASS, please refer to the eMASS Minor Application Assessment Guide.

Information System Change Requests

According to NIST 800-128; Guide for Security-Focused Configuration Management of Information Systems, a Security Impact Analysis (SIA) is incorporated into the configuration management process to ensure the impact of all changes are documented, analyzed, and evaluated for any adverse impacts on the security posture of the system.

To ensure that the changes have been implemented as approved, a SIA is performed as a part of the Configuration Management Plan (CMP) and supports the implementation of NIST [SP 800-53] control CM-4 and any potential enhancements. If the SIA identifies a significant change(s), the system is required to submit this artifact as part of the CM/CR Process prior to the change going into operation.

Steps for Security Impact Analysis (SIA)

1. Retrieve Major SIA Template from the Templates section of the eMASS Knowledge Service page.
2. Fill out all requested tab information regarding systems current security posture and change details.
3. Submit completed SIA form to the VAOISSIATeam@va.gov for ISRM review.
4. Receive competed SIA spreadsheet with completed Summary Memo detailing the extent changes affect the security posture of the system in relation to the functionality of existing security controls and organizational risk tolerance.

Additional guidance and templates related to SIAs may be found on the Knowledge Service eMASS Job Aids page.

Completion Steps for a Significant/Major Change

If the SIA identifies a significant change(s), the system is required to submit this artifact as part of the CM/CR Process prior to the change going into operation. Once the SIA is completed, reviewed, and returned:

1. The completed SIA must be uploaded to the Artifacts tab in eMASS. The Information System Owner (ISO) is responsible for reviewing this artifact.
2. A completed and signed Significant/Major Change Notification Form should be uploaded to the Artifacts tab in eMASS at least 45 days prior to implementation of the change.
3. According to VA Handbook 6500; Risk Management Framework For VA Information Systems VA Information Security Program, “formal reauthorization is required whenever a system undergoes a significant change or when there is a major change in the information collected or maintained”.

   All RMF steps in eMASS must be completed and all security artifacts need to be updated to reflect the change. To restart the RMF Process in eMASS, please refer to this Authorization Requirements SOP or eMASS Implementation Guide for additional guidance.

Note: For eMASS, the applicable system POCs must request the AODR initiate RMF Step 4 and advance/release controls to the Control Assessor no later than 70 days prior to the Authorization Termination Date (ATD) and/or the scheduled Control Review. The Control Review will be completed within 15 days with the results uploaded to the Artifacts tab in eMASS and the Control Review Team notifying the system stakeholders to close out RMF Step 4.

Additionally, the applicable system POCs must have their authorization package completed and progressed to **RMF Step 5 Authorize: Stage 3 Risk Review in the workflow no less than 45 calendar days** prior to the ATD or date they want their authorization decision to be made if requesting an out of cycle ATO review due to a major change. Once the package has been progressed, a package snapshot will be taken within eMASS for the Risk Review team to analyze for an ATO. After progressing the system to RMF Step 5 Authorize: Stage 3 Risk Review, the system POCs should continue to work on the system requirements within eMASS. Any progress made after the package snapshot will not be able to be viewed by the Risk Review team during their review.

Information System Vulnerability Management Plan (ISVMP)

The Information System Vulnerability Management Plan (ISVMP) establishes a plan for the communication and orchestration of vulnerability management practices at the system-level. It identifies vulnerability management roles and responsibilities, resources, processes, and standards to ensure vulnerabilities are managed throughout the information systems life cycle. ISVMP guidance is provided below.

Roles and Responsibilities

The ISVMP template can be found on the EVMP Knowledge Service (KS) main page.

1. The ISO and system steward should work with the ISSO and applicable service lines, stakeholders, and vendors (if applicable), to complete the ISVMP template.
2. The ISO should validate processes adhere to the ISVMP lifecycles for assessing, prioritizing, remediating, mitigating, and re-assessing vulnerabilities.
3. The ISVMP should include remediation points of contact for those personnel responsible for supporting the remediation activities of the information system and information system components.

Standards / Guidelines

- NIST Cyber Security Framework
- Gartner Vulnerability Management Cycle
- VA Handbook 6500
- POAM Management Guide
- Flaw Remediation SOP
- Vulnerability Management Memo

Completion Steps

1. The ISO and system steward works with the ISSO to complete the ISVMP template.

2. Once the ISVMP template is complete, the ISO or system steward uploads the ISVMP to the Artifacts tab in eMASS, and links to the appropriate security control (SI-2.12) for the ISVMP.

Continuous Monitoring Requirement

The ISVMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.1 Application Hosted On-Premises/VA Network

The On-Premises/VA Network includes applications that are VA managed and utilize an OS platform such as Window, UNIX, or Mainframe. A&A requirements for VAEC and other FedRAMP Cloud applications are addressed separately. **Error! Reference source not found.**

Applications on the On-Premises/VA Network may choose to inherit common control providers from the VA Tier 1 System of Record (T1SOR) and VA Enterprise SOR (VA ENTSOR). Refer to **Error! Reference source not found.** for complete details to help determine if the VA T1SOR or V A ENTSOR is applicable.

4.1.1 Security Documentation

The following sections provide details for each of the required security artifacts including the document requirements, references, and the parties that can provide additional guidance for each artifact. If available, templates for the applicable security artifacts/documents are located in the Templates section of the eMASS Knowledge Service page.

An artifact that is generated through eMASS as part of the authorization package and is reviewed/approved by the ISO and/or Information System Security Officer (ISSO) in the eMASS workflow as part of the authorization package may not require signature(s) and may be valid without signature(s). Contact your ISSO with questions on how to complete the documentation.

4.1.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA IT Service Management (ITSM) change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The CMP template should be used to complete the CMP and is available in the VA OIT Service Management Office's Process Asset Library (PAL). The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

Note: System Level Configuration Management Plans are under the governance of the VA OIT Service Management Office (SMO), Service Configuration Management organization, which collaborates with the Enterprise Program Management Division (EPMD), for continuous maintenance of the template and the availability to the enterprise. Please reach out to the OIT SMO ECRCM Service Configuration Management Staff for any questions about the CMP.

4.1.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. DRP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of system level DRPs.
- The ISO or system steward works with the assigned ISSO and DRP Director to create or revise the DRP. A DRP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS. Guidance on when a DRP is required can be found in the VA Handbook 6500.8.
2. The ISO, DRP Director, or system steward develops or revises the DRP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Disaster Recovery Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7.. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

4.1.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.1.1.4 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.

- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.1.1.5 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an

alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select “Yes” and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as “Contingency Plan”. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.1.1.6 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.

8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.1.1.7 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.1.1.8 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.1.1.9 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.1.1.10 Application Threat Modeling

Application Threat Modeling is a security documentation activity that is conducted before source code is written for custom-developed applications (for entire applications, or e.g., a library, a micro-service, or any application that it has been determined to independently scan and manage the vulnerability data for). Application Threat Modeling may also be conducted before COTS and SaaS applications are deployed or allowed to operate at the direction of OIS and/or CSOC. The goal of threat modeling is to determine where and what type of security controls need to be implemented in source code (or provided by an IT environment) for custom-developed applications. The goal for COTS and SaaS applications is to determine what product or service security configuration is needed (or provided by an IT environment).

Note: Application Threat Modeling is a manual documentation activity where the results are periodically updated, at a minimum annually, to maintain them.

Application Threat Modeling guidance is provided below:

- Custom-developed applications (the entire application, or e.g. a library, a micro-service, or any component that it has been determined to independently scan and manage the vulnerability data for), or instances of COTS and SaaS at the direction of OIS and/or CSOC, is analyzed by VA application developers using the freeware Microsoft Threat Modeling Tool software.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Application Threat Model.
- This requirement is not applicable to VistA systems.

Completion Steps

1. Obtain the freeware Microsoft software from Microsoft Security Development Lifecycle website. Install and configure the Threat Modeling Tool in your local environment.

2. Manually draw whiteboard-like diagrams using the Microsoft Threat Modeling Tool and audit potential threats generated by the tool.
3. Generate a report using the Threat Modeling Tool to use as the security documentation for this activity.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed) for each Application Threat Model (i.e., annually). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.1.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.1.2.1 Nessus Scan

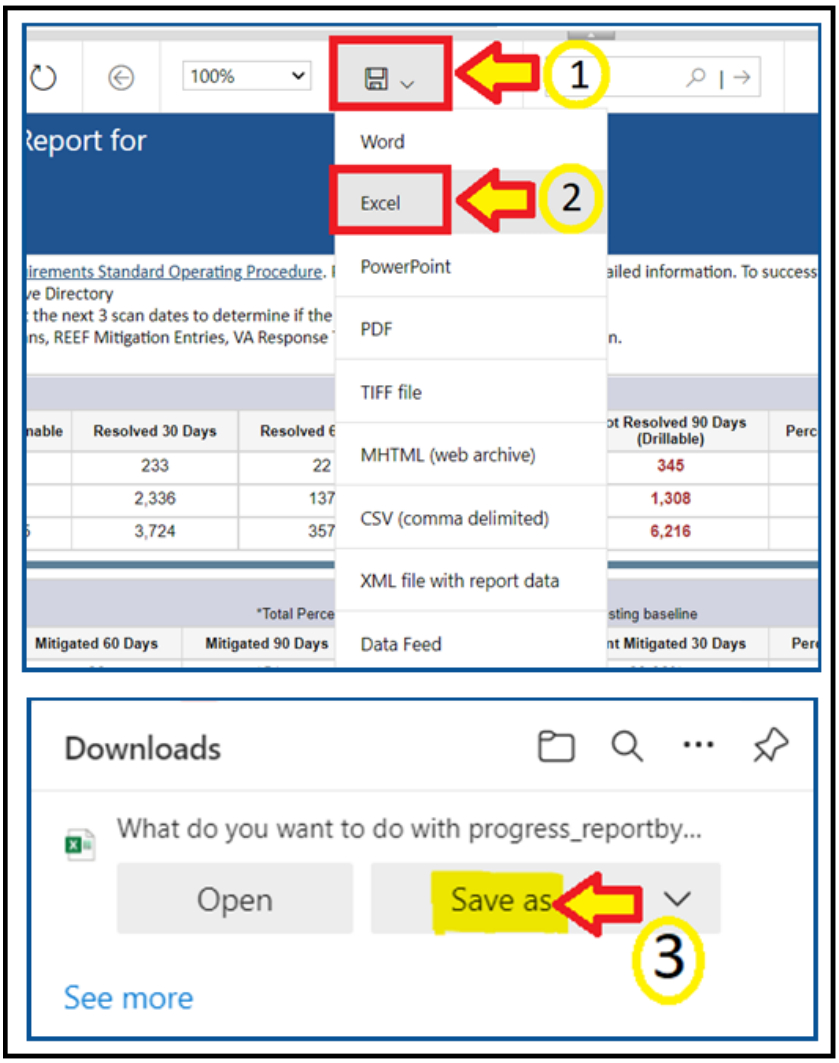
A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. All systems should complete the *Hardware and Software System Inventory Import* process to ensure all IPs are properly added to eMASS and a Nessus scan can be completed. Instructions can be found in the Hardware and Software System Inventory Import SOP, which is in the Standard Operating Procedures section of the eMASS Knowledge Service page.
2. The ISO or system-level system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then record and import the hardware baseline to eMASS (see Step 1 above), so the applicable Nessus data can be recorded.
3. Once the system's Nessus Scan data is accurately recorded, the ISO or system-level system steward follows these steps:
    a. Browse to Information Central Analytics and Metrics Platform (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system-level system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**. See the image below for step-by-step view.



d. The ISO or system-level system steward then uploads the report to the Artifacts tab within eMASS using the naming instructions identified above in step 3c.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system-level system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable

system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
2. Once the Database scan is completed, the summary and raw results must be uploaded to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings.
3. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
4. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For Internet facing applications, a WASA and Penetration Test are required, regardless of the FIPS categorization.

- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.
6. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision,

vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.1.2.4 Application Security Testing

Application Security Testing is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Application Security Testing is also conducted to effectively certify pipelines as part of the software factory life cycle to increase the level of confidence in security testing automation that is relied on for automated deliveries and releases.

Successful completion of Application Security Testing is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

Application Security Testing guidance is provided below:

- Custom-developed application source code (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) is scanned by VA application developers using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) software.
- Final developer performed Fortify scans and mitigations for security issues in production source code are validated by OIS Software Assurance for correctness and completeness.
- Successful completion of Application Security Testing is a prerequisite to Penetration Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Application Security Testing attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is not applicable to VistA systems

The results of OIS Software Assurance Application Security Testing Validation attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another validation attempt must be made. The results of OIS Software Assurance Application Security Testing Validation are also uploaded in an automated fashion to eMASS shortly after completion. A notification email is provided by OIS ISRM GRC Scans after this occurs.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POA&M per scan to document remediation and mitigation activities.

Completion Steps

1. Obtain the OIS-licensed Fortify software from OIS Software Assurance. Install and configure Fortify in your local build environments and also on your build server (if applicable). Perform Fortify scans on source code locally and also on your build server (if applicable) as a scheduled build job.
2. Audit Fortify scan results and implement mitigations in source code as needed to ensure that there are minimally no remaining critical or high severity findings, and that for example the latest version of Fortify software and rulepacks are being used.
3. Upload your submission package materials to your application's share (on the Intranet only), if permissions need to be updated please email OISSwAServiceRequests@va.gov with the Application-ID and VA address(es) needing access.
4. Navigate to the Your IT Services portal using your web browser, and fill out the Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name
    b. If applicable, update the auto-populated requestor information fields
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Security Scan Validation
    d. In the Application Name field, enter your application's name
    e. In the Application ID field, enter your application's VA Software Assurance Program identifier
    f. Fill out this PDF form and attach it to the request using the Add attachments link
    g. Fill out a text file named resubmission.txt that explains changes since any prior submissions and attach it to the request using the Add attachments link
5. Click on the Submit button.
6. Make a note of your ticket’s request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Warning: Upon successful completion of Application Security Testing, security testing results for subsequent automated deliveries and releases must be very carefully monitored locally for changes. There must be build failure criteria for Fortify scans to ensure that the Fortify integration and associated workflows that were certified are being maintained during software factory operation.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- Successful Application Security Testing completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Application Security Testing is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning custom-developed application source code for potential vulnerabilities using the OIS-licensed Fortify tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.1.2.5 Software Composition Analysis

Software Composition Analysis is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Software Composition Analysis focuses on supply chain risk management for custom-developed VA applications. Software Composition Analysis is performed by analyzing underlying libraries and frameworks for potential vulnerabilities as an additional activity during Application Security Testing.

Successful completion of Software Composition Analysis is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process. While Software Composition Analysis is performed as an additional activity during Application Security Testing, separate pass/fail verdicts are returned.

Software Composition Analysis guidance is provided below:

- Libraries and frameworks that use custom-developed applications (e.g., the entire application, a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data) require Software Composition Analysis by OIS Software Assurance as additional activity during Application Security Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Software Composition Analysis attempt for the

period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.

- This requirement is only applicable to custom-developed applications that are written in the following programming languages:
    - .NET Framework
    - .NET Core
    - ASP.NET
    - C#
    - C/C++
    - Classic ASP (with VBScript)
    - Go
    - Java (including Android)
    - JavaScript
    - JSP
    - Kotlin
    - Objective-C/C++
    - PHP
    - Python
    - Ruby
    - Swift
    - Visual Basic (VB.NET)
    - Visual Basic

The results of OIS Software Assurance Software Composition Analysis attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another attempt must be made by making another Application Security Testing request.

Completion Steps

- Software Composition Analysis scans are performed by OIS Software Assurance when Application Security Testing validations are requested.
- Please see the completion steps for Application Security Testing. There are no additional procedures to request Software Composition Analysis scans.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the scan report to the Artifacts tab within eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package. The latest progress should be added to the Status of Requirements. If the scan is not applicable, then list why it's not appliable in the Status of Requirements prior to uploading to the Artifacts tab within eMASS.

Warning: Upon successful completion of Software Composition Analysis, the environments, libraries, and frameworks must be very carefully monitored for

changes. Software Composition Analysis tools, such as OWASP Dependency Check, are strongly recommended to be integrated into pipelines.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally required as follows:

- Successful Software Composition Analysis completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Software Composition Analysis is also required when requested by OIS and/or CSOC.

Note: Additional guidance for Software Composition Analysis can be found on OIT teams. There is an OIS Software Assurance support site in Teams.

4.1.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If BigFix cannot be installed because the system is not supported by BigFix, another VA approved product, such as OpenSCAP, may be used as a substitute until BigFix is compatible with the system. Please refer to the BigFix FAQ and create an incident ticket to be assigned to OIS EV Support Group for approval of other SCCD products. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.

2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. The ISO or System Steward must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.
3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 above, Assessment and Authorization Requirements.
5. The ISO and/or System Steward creates a single POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. A new POA&M item must be created for each required SCCD (i.e., quarterly). Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS. The SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending (Computer Compliance and Check Compliance) and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: If the system cannot reach the 90% threshold due to offline devices, then note this in the SCCD POA&M and Status of Requirements so it can be accounted for in the Risk Review.

4.1.2.7 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review

3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.2 Application Hosted in Managed Service

Managed Service (also known as external systems) are systems that are managed outside the VA network. Technical scans and/or security documents should be provided (as applicable) for each Managed Service. Please refer to section 3.3 for Security Boundary Guidance.

4.2.1 Security Documentation

4.2.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA ITSM change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The CMP template should be used to complete the CMP and is available in the VA OIT Service Management Office's Process Asset Library (PAL). The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

Note: System Level Configuration Management Plans are under the governance of the VA OIT Service Management Office (SMO), Service Configuration Management organization, which collaborates with the Enterprise Program Management Division (EPMD), for continuous maintenance of the template and the availability to the enterprise. Please reach out to the OIT SMO ECRCM Service Configuration Management Staff for any questions about the CMP.

4.2.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. DRP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of system level DRPs.
- The ISO or system steward works with the assigned ISSO and DRP Director to create or revise the DRP. A DRP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS. Guidance on when a DRP is required can be found in the VA Handbook 6500.8.
2. The ISO, DRP Director, or system steward develops or revises the DRP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as “Disaster Recovery Plan”. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

4.2.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.2.1.4 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.2.1.5 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select “Yes” and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the

FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Contingency Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.2.1.6 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.

2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.2.1.7 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the

Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.2.1.8 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.2.1.9 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.2.1.10 Application Threat Modeling

Application Threat Modeling is a security documentation activity that is conducted before source code is written for custom-developed applications (for entire applications, or e.g., a library, a micro-service, or any application that it has been determined to independently scan and manage the vulnerability data for). Application Threat Modeling may also be conducted before COTS and SaaS applications are deployed or allowed to operate at the direction of OIS and/or CSOC. The goal of threat modeling is to determine where and what type of security controls need to be implemented in source code (or provided by an IT environment) for custom-developed applications. The goal for COTS and SaaS applications is to determine what product or service security configuration is needed (or provided by an IT environment).

Note: Application Threat Modeling is a manual documentation activity where the results are periodically updated, at a minimum annually, to maintain them.

Application Threat Modeling guidance is provided below:

- Custom-developed applications (the entire application, or e.g. a library, a micro-service, or any component that it has been determined to independently scan and manage the vulnerability data for), or instances of COTS and SaaS at the direction of OIS and/or CSOC, is analyzed by VA application developers using the freeware Microsoft Threat Modeling Tool software.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Application Threat Model.
- This requirement is not applicable to VistA systems.

Completion Steps

1. Obtain the freeware Microsoft software from Microsoft Security Development Lifecycle website. Install and configure the Threat Modeling Tool in your local environment.
2. Manually draw whiteboard-like diagrams using the Microsoft Threat Modeling Tool and audit potential threats generated by the tool.
3. Generate a report using the Threat Modeling Tool to use as the security documentation for this activity.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed) for each Application Threat Model (i.e., annually). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.2.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.2.2.1 Nessus Scan

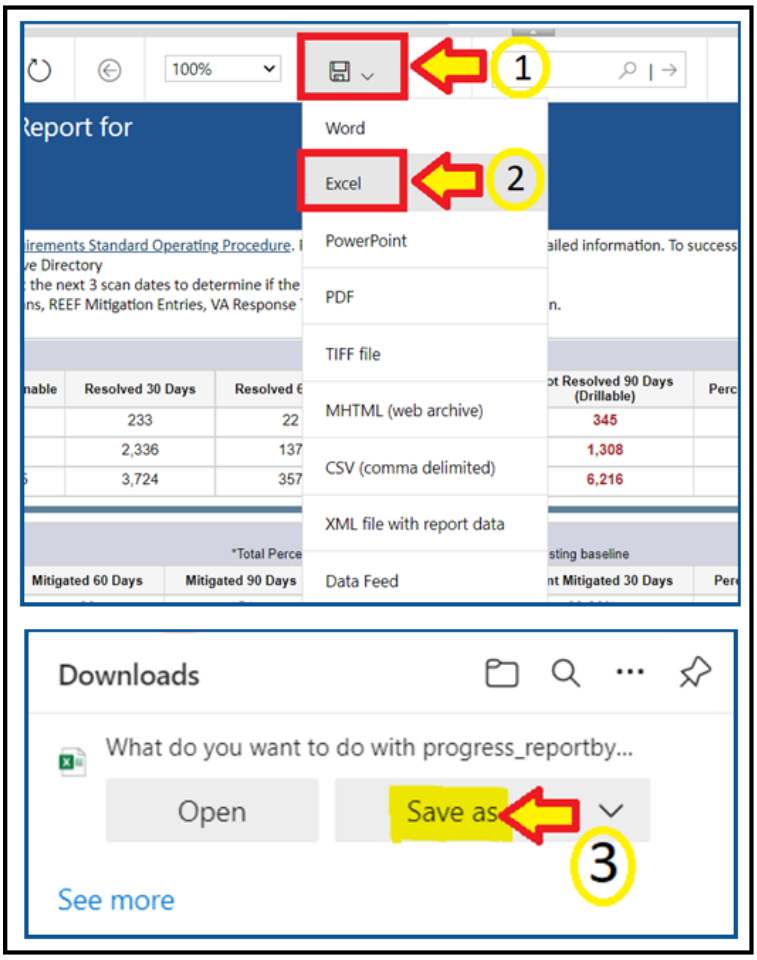
A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. All systems should complete the *Hardware and Software System Inventory Import* process to ensure all IPs are properly added to eMASS and a Nessus scan can be completed. Instructions can be found in the Hardware and Software System Inventory Import SOP, which is in the Standard Operating Procedures section of the eMASS Knowledge Service page.
2. The ISO or system-level system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then record and import the hardware baseline to eMASS (see Step 1 above), so the applicable Nessus data can be recorded.
3. Once the system's Nessus Scan data is accurately recorded, the ISO or system-level system steward follows these steps:
    a. Browse to Information Central Analytics and Metrics Platform (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system-level system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**. See the image below for step-by-step view.



d. The ISO or system-level system steward then uploads the report to the Artifacts tab within eMASS using the naming instructions identified above in step 3c.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system-level system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems and Managed Services. External systems / Managed Services must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary.

4.2.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
2. Once the Database scan is completed, the summary and raw results must be uploaded to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings.
3. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
4. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.2.2.3 Penetration Test/Application Assessment

A full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.

- For Internet facing applications, a WASA and Penetration Test are required, regardless of the FIPS categorization.
- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.
6. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.2.2.4 Application Security Testing

Application Security Testing is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Application Security Testing is also conducted to effectively certify pipelines as part of the software factory life cycle to increase the level of confidence in security testing automation that is relied on for automated deliveries and releases.

Successful completion of Application Security Testing is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

Application Security Testing guidance is provided below:

- Custom-developed application source code (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) is scanned by VA application developers using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) software.
- Final developer performed Fortify scans and mitigations for security issues in production source code are validated by OIS Software Assurance for correctness and completeness.
- Successful completion of Application Security Testing is a prerequisite to Penetration Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Application Security Testing attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is not applicable to VistA systems

The results of OIS Software Assurance Application Security Testing Validation attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another validation attempt must be made. The results of OIS Software Assurance Application Security Testing Validation are also uploaded in an automated fashion to eMASS shortly after completion. A notification email is provided by OIS ISRM GRC Scans after this occurs.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POA&M per scan to document remediation and mitigation activities.

Completion Steps

1. Obtain the OIS-licensed Fortify software from OIS Software Assurance. Install and configure Fortify in your local build environments and also on your build server (if applicable). Perform Fortify scans on source code locally and also on your build server (if applicable) as a scheduled build job.
2. Audit Fortify scan results and implement mitigations in source code as needed to ensure that there are minimally no remaining critical or high severity findings, and that for example the latest version of Fortify software and rulepacks are being used.
3. Upload your submission package materials to your application's share (on the Intranet only), if permissions need to be updated please email OISSwAServiceRequests@va.gov with the Application-ID and VA address(es) needing access.
4. Navigate to the Your IT Services portal using your web browser, and fill out the Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name
    b. If applicable, update the auto-populated requestor information fields
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Security Scan Validation
    d. In the Application Name field, enter your application's name
    e. In the Application ID field, enter your application's VA Software Assurance Program identifier
    f. Fill out this PDF form and attach it to the request using the Add attachments link
    g. Fill out a text file named resubmission.txt that explains changes since any prior submissions and attach it to the request using the Add attachments link
5. Click on the Submit button.
6. Make a note of your ticket’s request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the

explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Warning: Upon successful completion of Application Security Testing, security testing results for subsequent automated deliveries and releases must be very carefully monitored locally for changes. There must be build failure criteria for Fortify scans to ensure that the Fortify integration and associated workflows that were certified are being maintained during software factory operation.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- Successful Application Security Testing completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Application Security Testing is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning custom-developed application source code for potential vulnerabilities using the OIS-licensed Fortify tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.2.2.5 Software Composition Analysis

Software Composition Analysis is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Software Composition Analysis focuses on supply chain risk management for custom-developed VA applications. Software Composition Analysis is performed by analyzing underlying libraries and frameworks for potential vulnerabilities as an additional activity during Application Security Testing.

Successful completion of Software Composition Analysis is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process. While Software Composition Analysis is performed as an additional activity during Application Security Testing, separate pass/fail verdicts are returned.

Software Composition Analysis guidance is provided below:

- Libraries and frameworks that use custom-developed applications (e.g., the entire application, a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data) require Software Composition Analysis by OIS Software Assurance as additional activity during Application Security Testing.

- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Software Composition Analysis attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is only applicable to custom-developed applications that are written in the following programming languages:
    - .NET Framework
    - .NET Core
    - ASP.NET
    - C#
    - C/C++
    - Classic ASP (with VBScript)
    - Go
    - Java (including Android)
    - JavaScript
    - JSP
    - Kotlin
    - Objective-C/C++
    - PHP
    - Python
    - Ruby
    - Swift
    - Visual Basic (VB.NET)
    - Visual Basic

The results of OIS Software Assurance Software Composition Analysis attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another attempt must be made by making another Application Security Testing request.

Completion Steps

- Software Composition Analysis scans are performed by OIS Software Assurance when Application Security Testing validations are requested.
- Please see the completion steps for Application Security Testing. There are no additional procedures to request Software Composition Analysis scans.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the scan report to the Artifacts tab within eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package. The latest progress should be added to the Status of Requirements. If the scan is not applicable, then list why it's not appliable in the Status of Requirements prior to uploading to the Artifacts tab within eMASS.

Warning: Upon successful completion of Software Composition Analysis, the environments, libraries, and frameworks must be very carefully monitored for changes. Software Composition Analysis tools, such as OWASP Dependency Check, are strongly recommended to be integrated into pipelines.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally required as follows:

- Successful Software Composition Analysis completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Software Composition Analysis is also required when requested by OIS and/or CSOC.

Note: Additional guidance for Software Composition Analysis can be found on OIT teams. There is an OIS Software Assurance support site in Teams.

4.2.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If BigFix cannot be installed because the system is not supported by BigFix, another VA approved product, such as OpenSCAP, may be used as a substitute until BigFix is compatible with the system. Please refer to the BigFix FAQ and create an incident ticket to be assigned to OIS EV Support Group for approval of other SCCD products. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.

2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. The ISO or System Steward must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.
3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 above, Assessment and Authorization Requirements.
5. The ISO or system steward will create a POA&M for each failed checklist. The vulnerability description must include the total number of computers that fail the checklist. Please refer to the POAM Management Guide for instructions on creating a POA&M item in eMASS. The SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort.
6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending (Computer Compliance and Check Compliance) and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: If the system cannot reach the 90% threshold due to offline devices, then note this in the SCCD POA&M and Status of Requirements so it can be accounted for in the Risk Review.

4.2.2.7 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review

3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.3 Application Hosted in the VA Enterprise Cloud (VAEC)

Once approval from the GRC Committee has been received and the system has been registered in eMASS with the recognition that it utilizes the VA Enterprise Cloud (VAEC), the System Owner or delegate should work with their VAEC Intake Team and the VAEC Security Team to ensure all

VAEC requirements are met. Information regarding the requirements can be found at the VAEC Cybersecurity page.

The System Owner or delegate should ensure that there is an Enterprise/VA boundary entry in eMASS. The Enterprise/VA boundary entry must address the customer responsible controls and inherit the controls from the VAEC boundary entry (VAEC Microsoft Azure Government High Assessing or VAEC AWS GovCloud High Assessing). Please refer to section 3.3 for Security Boundary Guidance for eMASS.

For applications migrating from Traditional/On-Premises to the VAEC, the eMASS entry for an application in the VAEC should be a **new** eMASS entry in the **Cloud** organization and include only the VAEC boundary information. Security controls common to both the Traditional and Cloud implementation can be exported from the Traditional entry and imported into the Cloud entry. However, to maintain continuity between the Traditional and Cloud systems, the original eMASS package may be used. In this case, the organization must be updated to the **Cloud** organization before VAEC inheritance will be provided. This action currently must be performed by an eMASS administrator.

For Hybrid applications (applications operating with portions in a VA data center and portions in the VAEC – not fully migrating into the VAEC), the existing eMASS entry is used and the VAEC inheritable controls applied. It is the responsibility of the System Steward to determine and document inheritance that comes from the VAEC and inheritance that comes from the data center for all security controls.

The Security Documentation and Technical/Testing requirements listed below are a guideline for the typical requirements to receive an ATO. If the Security Documentation or Technical/Testing requirements is not applicable for the eMASS authorization package, provide an explanation why it's not applicable in the **Status of Requirements** document.

VA OIS leadership has established the VA Tier 1 SOR (T1SOR) and the VA Enterprise SOR (VA ENTSOR) as Common Control Providers (e.g., Hosting Facilities, Organizational Policy Records, etc.) to facilitate the automated establishment of inheritance relationships. Applications in the VAEC that inherit from VAEC AWS or VAEC Microsoft Azure receive VA T1SOR and VA ENTSOR as a pass-through inheritance. Refer to Appendix D – Common Control Providers/System of Record (SOR) for additional details on the VA T1SOR and the VA ENTSOR.

4.3.1 Security Documentation

4.3.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA ITSM change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The CMP template should be used to complete the CMP and is available in the VA OIT Service Management Office's Process Asset Library (PAL). The ISO or system steward should work with the ISSO to complete the CMP. VAEC supplemental guidance can be found at the VAEC Cybersecurity main page.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

4.3.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. DRP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of system level DRPs.
- The VAEC creates or revises the DRP to encompass recovery for all systems hosted within VAEC. A DRP template can be found on the Knowledge Service page.
- Applications within the VAEC will not require a DRP. A DRP is only required if:
    - Your authorization boundary is a VA owned or managed data center.
    - If your authorization boundary contains is a managed service that contains an application and the hosting environment, you may require a DRP.

For applications in the VAEC, the Cloud Service Provider (Microsoft Azure Government or Amazon Web Services GovCloud) is responsible for the DRP. For security reasons, the CSPs do not make their DRP available for review.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. A DRP is not required for individual systems hosted within VAEC. A VAEC wide DRP is developed by the VAEC ISO. Guidance on when a DRP is required can be found in the VA Handbook 6500.8.
2. The VAEC ISO, DRP Director, or system steward develops or revises the DRP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the VAEC ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Disaster Recovery Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the DRP has been uploaded to the FISMA tab, the VAEC ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7.. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change to the system occurs.

4.3.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP. An IRP template for VAEC AWS and VAEC Azure can be found at the VAEC main page.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.3.1.4 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will

monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page. VAEC BIA information is not included in system BIAs as the VAEC is not in a system's authorization boundary.
    - Under Section 3.4 (Identify Resource Requirements) of the BIA, use the following selections for the included table:
        - System Resource/Component: Hosting Infrastructure
        - Platform/OS/Version: VAEC <AWS or Azure>
        - Description: Application resides in VAEC

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts

tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.3.1.5 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page. VAEC ISCP information is not included in system ISCPs as the VAEC is not in a system's authorization boundary.
    - In Appendix K, Associated Plans and Procedures, add the VAEC AWS or Azure ISCP as an additional plan at the end of your list. The VAEC ISCP names are:
        - Department of Veterans Affairs (VA)
          Office of Information Security (OIS)
          Information System Contingency Plan (ISCP)
          VA ENTERPRISE CLOUD (VAEC)
          Amazon Web Services (AWS) GOVCLOUD HIGH

        - Department of Veterans Affairs (VA)
          Office of Information Security (OIS)
          Information System Contingency Plan (ISCP)
          VA ENTERPRISE CLOUD (VAEC)
          MICROSOFT AZURE GOVERNMENT (MAG) HIGH

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500

- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select "Yes" and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Contingency Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

1. .

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.3.1.6 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established, an Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.

- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.3.1.7 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.3.1.8 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.3.1.9 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.3.1.10 Application Threat Modeling

Application Threat Modeling is a security documentation activity that is conducted before source code is written for custom-developed applications (for entire applications, or e.g., a library, a micro-service, or any application that it has been determined to independently scan and manage the vulnerability data for). Application Threat Modeling may also be conducted before COTS and SaaS applications are deployed or allowed to operate at the direction of OIS and/or CSOC. The goal of threat modeling is to determine where and what type of security controls need to be implemented in source code (or provided by an IT environment) for custom-developed applications. The goal for COTS and SaaS applications is to determine what product or service security configuration is needed (or provided by an IT environment).

Note: Application Threat Modeling is a manual documentation activity where the results are periodically updated, at a minimum annually, to maintain them.

Application Threat Modeling guidance is provided below:

- Custom-developed applications (the entire application, or e.g. a library, a micro-service, or any component that it has been determined to independently scan and manage the vulnerability data for), or instances of COTS and SaaS at the direction of OIS and/or CSOC, is analyzed by VA application developers using the freeware Microsoft Threat Modeling Tool software.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Application Threat Model.
- This requirement is not applicable to VistA systems.

Completion Steps

1. Obtain the freeware Microsoft software from Microsoft Security Development Lifecycle website. Install and configure the Threat Modeling Tool in your local environment.
2. Manually draw whiteboard-like diagrams using the Microsoft Threat Modeling Tool and audit potential threats generated by the tool.
3. Generate a report using the Threat Modeling Tool to use as the security documentation for this activity.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed) for each Application Threat Model (i.e., annually). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.3.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

Based on the Service Level Agreements (SLAs) for VAEC AWS and VAEC MAG, the VA can only scan the VA responsible controls. Anything the VA installs in the cloud can be scanned (Infrastructure as a Service). All Cloud Service Provider (CSP) controlled services (Platform as a Service) are covered under the FedRAMP authorization and the 3rd Party Assessment Organization (3PAO) scans. For a specific listing of what is within the VA approved FedRAMP boundary of cloud providers, reference the VAEC Service Catalog on the VAEC Site.

All the services listed are within the FedRAMP boundary and CSP's control; therefore, the VA cannot scan them. These services have been authorized by both FedRAMP and VA. The VA abides by FedRAMP policy and accepts the 3PAO scans. Systems in VAEC Azure that are Platform as a Service (PaaS) can choose to inherit the PaaS controls from the CSP. Specific instructions can be found on the VAEC Site under Cyber Security Resources**.**

Note: Platform as a Service (PaaS) servers should not be added to the Hardware system inventory in eMASS since these are not VA assets. However, the PaaS should be added to the Software system inventory in eMASS.

4.3.2.1 Nessus Scan

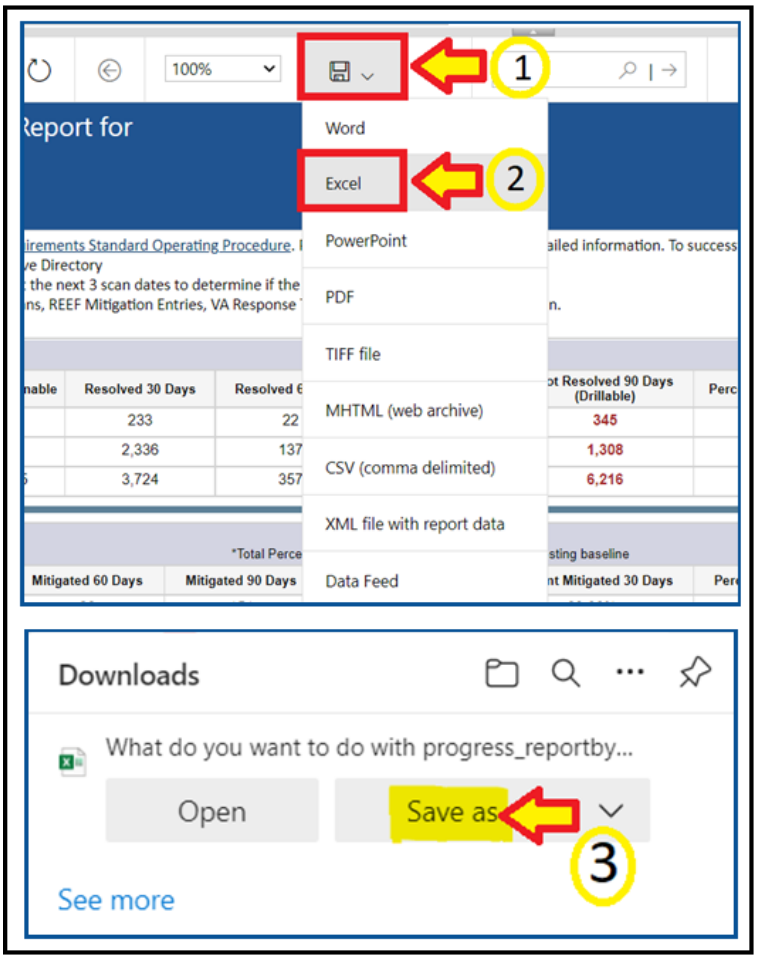
A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems. PaaS servers are not VA owned and cannot be scanned. PaaS servers should not be included in the Hardware system inventory in eMASS.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. All systems should complete the *Hardware and Software System Inventory Import* process to ensure all IPs are properly added to eMASS and a Nessus scan can be completed. Instructions can be found in the Hardware and Software System Inventory Import SOP, which is in the Standard Operating Procedures section of the eMASS Knowledge Service page.
2. The ISO or system-level system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then record and import the hardware baseline to eMASS (see Step 1 above), so the applicable Nessus data can be recorded.
3. Once the system's Nessus Scan data is accurately recorded, the ISO or system-level system steward follows these steps:
    a. Browse to Information Central Analytics and Metrics Platform (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system-level system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**. See the image below for step-by-step view.



d. The ISO or system-level system steward then uploads the report to the Artifacts tab within eMASS using the naming instructions identified above in step 3c.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system-level system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems. External systems must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary. PaaS servers are not VA owned and cannot be scanned. PaaS servers should not be included in the Hardware inventory in eMASS.

4.3.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
2. Once the Database scan is completed, the summary and raw results must be uploaded to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings.
3. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
4. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Database Scan for all VA owned systems. PaaS database servers are not VA owned and cannot be scanned. PaaS servers should not be included in the Hardware inventory in eMASS. However, the database itself must be scanned.

4.3.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High system, considered a major application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For systems residing in a cloud environment or external to the VA network, connections must be in place through the Trust Internet Connection (TIC) prior to assessment to facilitate connectivity from the CSOC internal testing servers.
- For Internet facing applications, a WASA and Penetration Test are required, regardless of the FIPS categorization.
- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/ CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed.
    b. PaaS hosts should not be tested; they are not VA owned services. PaaS hosts are owned by the Cloud Service Provider and all testing and remediation is done by the CSP and their 3PAO for FedRAMP. On the Penetration Test Questionnaire, indicate any PaaS hosts in field "1.17 - Are there any servers, web applications, or network services that should NOT be tested?.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.

a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.

6. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.3.2.4 Application Security Testing

Application Security Testing is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Application Security Testing is also conducted to effectively certify pipelines as part of the software factory life cycle to increase the level of confidence in security testing automation that is relied on for automated deliveries and releases.

Successful completion of Application Security Testing is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

Application Security Testing guidance is provided below:

- Custom-developed application source code (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) is scanned by VA application developers using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) software.
- Final developer performed Fortify scans and mitigations for security issues in production source code are validated by OIS Software Assurance for correctness and completeness.
- Successful completion of Application Security Testing is a prerequisite to Penetration Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Application Security Testing attempt for the period

of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is not applicable to VistA systems

The results of OIS Software Assurance Application Security Testing Validation attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another validation attempt must be made. The results of OIS Software Assurance Application Security Testing Validation are also uploaded in an automated fashion to eMASS shortly after completion. A notification email is provided by OIS ISRM GRC Scans after this occurs.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POA&M per scan to document remediation and mitigation activities.

Completion Steps

1. Obtain the OIS-licensed Fortify software from OIS Software Assurance. Install and configure Fortify in your local build environments and also on your build server (if applicable). Perform Fortify scans on source code locally and also on your build server (if applicable) as a scheduled build job.
2. Audit Fortify scan results and implement mitigations in source code as needed to ensure that there are minimally no remaining critical or high severity findings, and that for example the latest version of Fortify software and rulepacks are being used.
3. Upload your submission package materials to your application's share (on the Intranet only), if permissions need to be updated please email OISSwAServiceRequests@va.gov with the Application-ID and VA address(es) needing access.
4. Navigate to the Your IT Services portal using your web browser, and fill out the Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name
    b. If applicable, update the auto-populated requestor information fields
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Security Scan Validation
    d. In the Application Name field, enter your application's name
    e. In the Application ID field, enter your application's VA Software Assurance Program identifier

f. Fill out this PDF form and attach it to the request using the Add attachments link
g. Fill out a text file named resubmission.txt that explains changes since any prior submissions and attach it to the request using the Add attachments link

5. Click on the Submit button.
6. Make a note of your ticket's request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Warning: Upon successful completion of Application Security Testing, security testing results for subsequent automated deliveries and releases must be very carefully monitored locally for changes. There must be build failure criteria for Fortify scans to ensure that the Fortify integration and associated workflows that were certified are being maintained during software factory operation.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- Successful Application Security Testing completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Application Security Testing is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning custom-developed application source code for potential vulnerabilities using the OIS-licensed Fortify tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.3.2.5 Software Composition Analysis

Software Composition Analysis is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Software Composition Analysis focuses on supply chain risk management for custom-developed VA applications.

Software Composition Analysis is performed by analyzing underlying libraries and frameworks for potential vulnerabilities as an additional activity during Application Security Testing.

Successful completion of Software Composition Analysis is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process. While Software Composition Analysis is performed as an additional activity during Application Security Testing, separate pass/fail verdicts are returned.

Software Composition Analysis guidance is provided below:

- Libraries and frameworks that use custom-developed applications (e.g., the entire application, a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data) require Software Composition Analysis by OIS Software Assurance as additional activity during Application Security Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Software Composition Analysis attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is only applicable to custom-developed applications that are written in the following programming languages:
    - .NET Framework
    - .NET Core
    - ASP.NET
    - C#
    - C/C++
    - Classic ASP (with VBScript)
    - Go
    - Java (including Android)
    - JavaScript
    - JSP
    - Kotlin
    - Objective-C/C++
    - PHP
    - Python
    - Ruby
    - Swift
    - Visual Basic (VB.NET)
    - Visual Basic

The results of OIS Software Assurance Software Composition Analysis attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another attempt must be made by making another Application Security Testing request.

Completion Steps

- Software Composition Analysis scans are performed by OIS Software Assurance when Application Security Testing validations are requested.
- Please see the completion steps for Application Security Testing. There are no additional procedures to request Software Composition Analysis scans.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the scan report to the Artifacts tab within eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package. The latest progress should be added to the Status of Requirements. If the scan is not applicable, then list why it's not appliable in the Status of Requirements prior to uploading to the Artifacts tab within eMASS.

Warning: Upon successful completion of Software Composition Analysis, the environments, libraries, and frameworks must be very carefully monitored for changes. Software Composition Analysis tools, such as OWASP Dependency Check, are strongly recommended to be integrated into pipelines.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally required as follows:

- Successful Software Composition Analysis completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Software Composition Analysis is also required when requested by OIS and/or CSOC.

Note: Additional guidance for Software Composition Analysis can be found on OIT teams. There is an OIS Software Assurance support site in Teams.

4.3.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If BigFix cannot be installed because the system is not supported by BigFix, another VA approved product, such as OpenSCAP, may be used as a substitute until BigFix is compatible with the system. Please refer to the BigFix FAQ and create an incident ticket to be assigned to OIS EV Support Group for approval of other SCCD products. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years. PaaS servers are not VA owned and cannot be scanned. PaaS servers should not be included in the Hardware inventory in eMASS.

Note: Platform as a Service (PaaS) servers should not be added to the Hardware system inventory in eMASS since these are not VA assets. However, the PaaS should be added to the Software system inventory in eMASS.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.
3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 above, Assessment and Authorization Requirements.
5. The ISO and/or System Steward creates a single POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. A new POA&M item must be created for each required SCCD (i.e., quarterly). Please refer to the POA&M Management Guide for

instructions on creating a POA&M item in eMASS. The SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort.

6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending (Computer Compliance and Check Compliance) and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: If the system cannot reach the 90% threshold due to offline devices, then note this in the SCCD POA&M and Status of Requirements so it can be accounted for in the Risk Review.

4.3.2.7 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.

    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.4 Application Hosted in FedRAMP Cloud (Non-VAEC)

This section covers non-VAEC FedRAMP systems and systems that utilize non-VAEC FedRAMP cloud systems for hosting. It can include -F, -VAF, and other cloud hosted systems (e.g., SaaS, non-FedRAMP systems hosted in non-VAEC FedRAMP).

Approval from the GRC Committee must be received with the recognition that it utilizes a non-VAEC FedRAMP cloud. Once approved, the System Owner or delegate should ensure that there's a FedRAMP boundary entry and an enterprise VA boundary or single instance VA boundary entry in eMASS. The enterprise VA boundary or single instance VA boundary entry must address the customer responsible controls and inherit the controls from the FedRAMP boundary entry. The entry names ***must be*** the same as the system names listed on FedRAMP.gov with the added designation of -F for FedRAMP, -VAF for VA sponsored FedRAMP, -e for Enterprise, and -i for single instance. Please refer to section section 3.3 for Security Boundary Guidance in eMASS.

The System Owner or delegate must work to ensure all the Security Documentation and Technical/Testing requirements listed below are completed and included with the eMASS authorization package. If the Security Documentation or Technical/Testing requirements is not applicable for the eMASS authorization package, then the reasons why it's not applicable should be included in the Status of Requirements and be uploaded to the Artifacts tab within eMASS. Please review the VA Cloud Security Procedure Guidance provided by Enterprise Security Architecture to ensure all policy requirements and responsibilities are completed.

The FedRAMP package (-F or -VAF) refers to a government agency sponsored Cloud Service Provider (CSP) or Software-as-a-Service (SaaS) package. They are only visible in eMASS to the assigned cloud or VAEC ISSOs. Non-cloud and non-VAEC ISSOs will only be responsible for the enterprise (-e) or single instance (-i) packages. The field is not responsible for -F or -VAF packages. Sensitive VA records (e.g., PHI/PII) are not contained within the -F or -VAF packages meaning there is no PII/PHI, controls, VA artifacts, or POA&Ms regarding VA Users. The PII/PHI and VA Users are all documented under the associated –E or –I system.

Note: The FedRAMP package (-F or -VAF) and the enterprise package (-e) or single instance (-i) must be completed simultaneously in eMASS and submitted for Risk Review (RMF Step 5: Stage 3) at the same time.

4.4.1 Security Documentation

4.4.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA ITSM change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The CMP template should be used to complete the CMP and is available in the VA OIT Service Management Office's Process Asset Library (PAL). The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

Note: System Level Configuration Management Plans are under the governance of the VA OIT Service Management Office (SMO), Service Configuration Management organization, which collaborates with the Enterprise Program Management Division (EPMD), for continuous maintenance of the template and the availability to the enterprise. Please reach out to the OIT SMO ECRCM Service Configuration Management Staff for any questions about the CMP.

4.4.1.2 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.4.1.3 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

5. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
6. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
7. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
8. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts

tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.4.1.4 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

5. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select “Yes” and then will be required to upload the ISCP to eMASS.
6. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
7. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as “Contingency Plan”. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking

the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

8. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.4.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.

3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.4.1.6 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant

security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.4.1.7 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.4.1.8 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.4.1.9 Application Threat Modeling

Application Threat Modeling is a security documentation activity that is conducted before source code is written for custom-developed applications (for entire applications, or e.g., a library, a micro-service, or any application that it has been determined to independently scan and manage the vulnerability data for). Application Threat Modeling may also be conducted before COTS and SaaS applications are deployed or allowed to operate at the direction of OIS and/or CSOC. The goal of threat modeling is to determine where and what type of security controls need to be implemented in source code (or provided by an IT environment) for custom-developed applications. The goal for COTS and SaaS applications is to determine what product or service security configuration is needed (or provided by an IT environment).

Note: Application Threat Modeling is a manual documentation activity where the results are periodically updated, at a minimum annually, to maintain them.

Application Threat Modeling guidance is provided below:

- Custom-developed applications (the entire application, or e.g. a library, a micro-service, or any component that it has been determined to independently scan and manage the vulnerability data for), or instances of COTS and SaaS at the direction of OIS and/or CSOC, is analyzed by VA application developers using the freeware Microsoft Threat Modeling Tool software.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Application Threat Model.
- This requirement is not applicable to VistA systems.

Completion Steps

1. Obtain the freeware Microsoft software from Microsoft Security Development Lifecycle website. Install and configure the Threat Modeling Tool in your local environment.

2. Manually draw whiteboard-like diagrams using the Microsoft Threat Modeling Tool and audit potential threats generated by the tool.
3. Generate a report using the Threat Modeling Tool to use as the security documentation for this activity.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed) for each Application Threat Model (i.e., annually). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.4.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

For FedRAMP approved systems, the VA can only scan the VA responsible controls. Anything the VA installs in the cloud can be scanned, but all Cloud Service Provider (CSP) controlled services are covered under the FedRAMP authorization and the 3rd Party Assessment Organization (3PAO) scans. For a specific listing of what is within the FedRAMP boundary of cloud providers, review of the FedRAMP package can be requested, or look on the FedRAMP marketplace at the "Service Description" for the cloud provider. For example, to review the services within the FedRAMP boundary of AWS GovCloud, look up AWS GovCloud on the FedRAMP marketplace. All of the services listed are within the FedRAMP boundary and CSP's control; therefore, the VA cannot scan them. These services have been authorized by both FedRAMP and VA. The VA abides by FedRAMP policy and accepts the 3PAO scans. To review the scans, a Package Access Request Form, which can be found on the FedRAMP marketplace page for any service, must be filled out and submitted to VA OIS ESA CSA for approval.

Note: Platform as a Service (PaaS) servers/services should not be added to the Hardware and Software system inventory in eMASS since these are not VA assets.

4.4.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations must be conducted to identify security flaws. When conducting the Nessus Scan, a discovery scan to identify all assets within the authorization boundary must be conducted as a part of the vulnerability scan (a discovery scan will not enumerate any vulnerabilities).

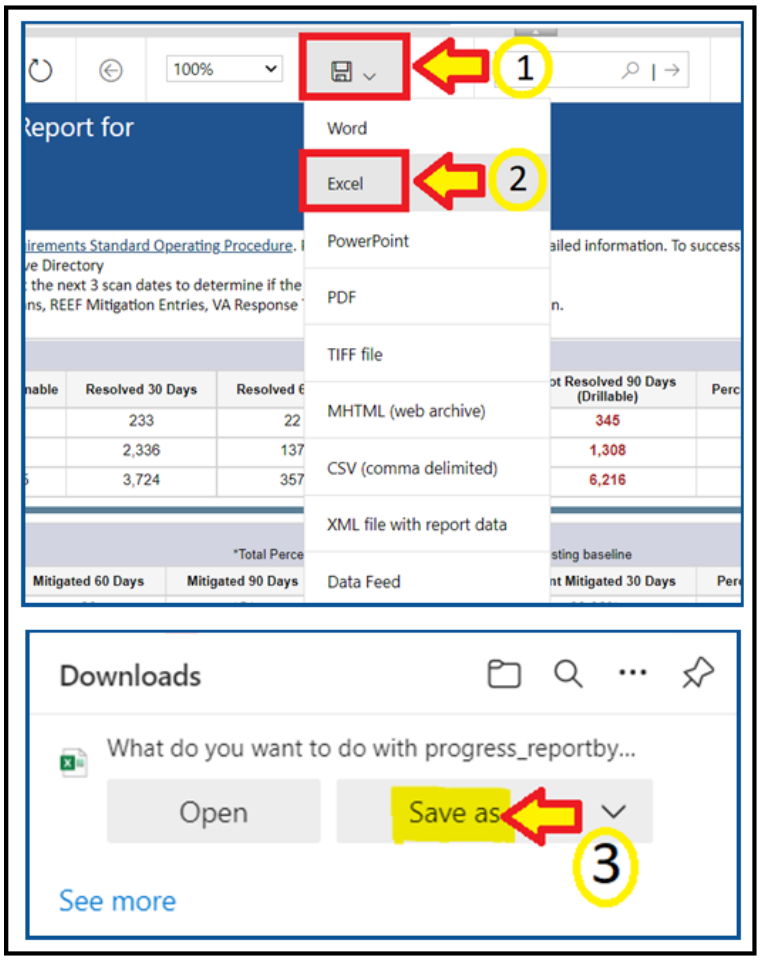
Note: CSOC must conduct an independent Nessus Scan for all VA owned systems.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. All systems should complete the *Hardware and Software System Inventory Import* process to ensure all IPs are properly added to eMASS and a Nessus scan can be completed. Instructions can be found in the Hardware and Software System Inventory Import SOP, which is in the Standard Operating Procedures section of the eMASS Knowledge Service page.
2. The ISO or system-level system steward can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then record and import the hardware baseline to eMASS (see Step 1 above), so the applicable Nessus data can be recorded.
3. Once the system's Nessus Scan data is accurately recorded, the ISO or system-level system steward follows these steps:
    a. Browse to Information Central Analytics and Metrics Platform (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO or system-level system steward creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.

c. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**. See the image below for step-by-step view.



d. The ISO or system-level system steward then uploads the report to the Artifacts tab within eMASS using the naming instructions identified above in step 3c.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.

Note: If raw Nessus Scan data is provided from CSOC, the ISO or system-level system steward needs to upload the actual Nessus Scan results to the Artifacts tab in eMASS along with a mitigation strategy for each finding. Also, within ICAMP, if the ISO/ISSO does not have an option to pull a report for their FISMA reportable system, then contact the VA GRC Service Desk to provide the IP address range of the system authorization boundary to add it to ICAMP to pull the report.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: CSOC must conduct an independent Nessus Scan for all VA owned systems. External systems must have a recent CSOC Nessus scan conducted either via remote connection or by utilizing CSOC staff on-site to perform scans, when necessary.

4.4.2.2 Database Scan

All systems must request a database scan if the project hosts a database to store and process information.

Completion Steps

1. Database scans can be requested at the CSOC Database Scan Questionnaire. For additional information, contact the database scanning team. If a database scan is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
2. Once the Database scan is completed, the summary and raw results must be uploaded to the Artifacts tab within eMASS along with the remediation plan. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings.
3. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
4. A follow-up Database scan should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A Database scan must be completed annually or when a significant/major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.4.2.3 Penetration Test/Application Assessment

A Penetration Test or full Application Assessment (MASA/WASA) must be performed that includes automated and manual assessment tools and techniques for the following:

- A FISMA High system, considered a major or minor application.
- A FISMA Moderate or higher, that processes, uses, or hosts PII and/or financial data.
- For systems residing in a cloud environment or external to the VA network, connections must be in place through the Trust Internet Connection (TIC) prior to assessment to facilitate connectivity from the CSOC internal testing servers.
- For Internet facing applications, a WASA and Penetration Test are required, regardless of the FIPS categorization.
- For systems that are not web-based or host a user presented web application but have middleware or APIs, a Penetration Test and WASA must be performed.
- If a Penetration Test / Application Assessment is not applicable, provide an explanation why it's not applicable in the **Status of Requirements** document.
- The Penetration Test / Application Assessment requirement is not applicable to the VistA authorization boundary.

Completion Steps

1. Systems with custom code must be registered with OIS Software Assurance and receive a "PASS" from the Code Review process prior to requesting an application assessment (MASA/WASA).
2. A system utilizing a COTS product still must register with OIS Software Assurance.
3. The ISO or system steward can request a penetration test/application assessment by completing the CSOC Penetration Test Questionnaire/ CSOC Mobile Application Security Assessment (MASA) Questionnaire/CSOC Web Application Security Assessment (WASA) Questionnaire. Additional scan details can be found at CSOC Scan Documents. Please allow 30 days for CSOC to schedule/conduct the penetration test/application assessment. Questions can be submitted to VA CSOC.
    a. CSOC must conduct an independent penetration test/application assessment for all VA owned applications and Managed Services. CSOC must have visibility into all VA applications where an authorization decision is required, including systems behind firewalls. External systems must also have a recent CSOC penetration test/application assessment performed.
4. CSOC will provide results to the ISO or system steward.
5. The ISO or system steward uploads the summary and raw results to the Artifacts tab in eMASS along with the mitigation / remediation plan for all findings.
    a. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the penetration test to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Findings that must be remediated through or from the vendor should also be documented as part of this analysis and should be documented in either the report of findings provided from VA-CSOC or as a separate document.

6. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.
7. Once the deficiencies have been mitigated, a follow-up Penetration Test/Application Assessment should be requested to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing authorization process.

Continuous Monitoring

A CSOC Penetration Test/Application Assessment is required on an annual basis or when a major change to the system or data occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.4.2.4 Application Security Testing

Application Security Testing is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Application Security Testing is also conducted to effectively certify pipelines as part of the software factory life cycle to increase the level of confidence in security testing automation that is relied on for automated deliveries and releases.

Successful completion of Application Security Testing is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

Application Security Testing guidance is provided below:

- Custom-developed application source code (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) is scanned by VA application developers using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) software.
- Final developer performed Fortify scans and mitigations for security issues in production source code are validated by OIS Software Assurance for correctness and completeness.
- Successful completion of Application Security Testing is a prerequisite to Penetration Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Application Security Testing attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is not applicable to VistA systems

The results of OIS Software Assurance Application Security Testing Validation attempts are returned to VA application developers. A notification email is provided by OIS Software

Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another validation attempt must be made. The results of OIS Software Assurance Application Security Testing Validation are also uploaded in an automated fashion to eMASS shortly after completion. A notification email is provided by OIS ISRM GRC Scans after this occurs.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under "View by" on left side of screen)
- Under the Application Details section, click "Load Details"

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POA&M per scan to document remediation and mitigation activities.

Completion Steps

1. Obtain the OIS-licensed Fortify software from OIS Software Assurance. Install and configure Fortify in your local build environments and also on your build server (if applicable). Perform Fortify scans on source code locally and also on your build server (if applicable) as a scheduled build job.
2. Audit Fortify scan results and implement mitigations in source code as needed to ensure that there are minimally no remaining critical or high severity findings, and that for example the latest version of Fortify software and rulepacks are being used.
3. Upload your submission package materials to your application's share (on the Intranet only), if permissions need to be updated please email OISSwAServiceRequests@va.gov with the Application-ID and VA address(es) needing access.
4. Navigate to the Your IT Services portal using your web browser, and fill out the Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name
    b. If applicable, update the auto-populated requestor information fields
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Security Scan Validation
    d. In the Application Name field, enter your application's name
    e. In the Application ID field, enter your application's VA Software Assurance Program identifier
    f. Fill out this PDF form and attach it to the request using the Add attachments link
    g. Fill out a text file named resubmission.txt that explains changes since any prior submissions and attach it to the request using the Add attachments link
5. Click on the Submit button.
6. Make a note of your ticket's request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Warning: Upon successful completion of Application Security Testing, security testing results for subsequent automated deliveries and releases must be very carefully monitored locally for changes. There must be build failure criteria for Fortify scans to ensure that the Fortify integration and associated workflows that were certified are being maintained during software factory operation.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- Successful Application Security Testing completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Application Security Testing is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning custom-developed application source code for potential vulnerabilities using the OIS-licensed Fortify tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.4.2.5 Software Composition Analysis

Software Composition Analysis is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Software Composition Analysis focuses on supply chain risk management for custom-developed VA applications. Software Composition Analysis is performed by analyzing underlying libraries and frameworks for potential vulnerabilities as an additional activity during Application Security Testing.

Successful completion of Software Composition Analysis is required for all initial production releases OR upon discovery that the application has already been deployed to production and

has not gone through the process. While Software Composition Analysis is performed as an additional activity during Application Security Testing, separate pass/fail verdicts are returned.

Software Composition Analysis guidance is provided below:

- Libraries and frameworks that use custom-developed applications (e.g., the entire application, a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data) require Software Composition Analysis by OIS Software Assurance as additional activity during Application Security Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Software Composition Analysis attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is only applicable to custom-developed applications that are written in the following programming languages:
    - .NET Framework
    - .NET Core
    - ASP.NET
    - C#
    - C/C++
    - Classic ASP (with VBScript)
    - Go
    - Java (including Android)
    - JavaScript
    - JSP
    - Kotlin
    - Objective-C/C++
    - PHP
    - Python
    - Ruby
    - Swift
    - Visual Basic (VB.NET)
    - Visual Basic

The results of OIS Software Assurance Software Composition Analysis attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another attempt must be made by making another Application Security Testing request.

Completion Steps

- Software Composition Analysis scans are performed by OIS Software Assurance when Application Security Testing validations are requested.
- Please see the completion steps for Application Security Testing. There are no additional procedures to request Software Composition Analysis scans.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the scan report to the Artifacts tab within eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package. The latest progress should be added to the Status of Requirements. If the scan is not applicable, then list why it's not appliable in the Status of Requirements prior to uploading to the Artifacts tab within eMASS.

Warning: Upon successful completion of Software Composition Analysis, the environments, libraries, and frameworks must be very carefully monitored for changes. Software Composition Analysis tools, such as OWASP Dependency Check, are strongly recommended to be integrated into pipelines.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally required as follows:

- Successful Software Composition Analysis completion is required after the initial production release, automated producti8on delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Software Composition Analysis is also required when requested by OIS and/or CSOC.

Note: Additional guidance for Software Composition Analysis can be found on OIT teams. There is an OIS Software Assurance support site in Teams.

4.4.2.6 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If BigFix cannot be installed because the system is not supported by BigFix, another VA approved product, such as OpenSCAP, may be used as a substitute until BigFix is compatible with the system. Please refer to the BigFix FAQ and create an incident ticket to be assigned to OIS EV Support Group for approval of other SCCD products. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.
2. The ISO or System Steward is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.
3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO and/or System Steward runs the Security Configuration Compliance Data Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO and/or System Steward uploads the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 above, Assessment and Authorization Requirements.
5. The ISO and/or System Steward creates a single POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. A new POA&M item must be created for each required SCCD (i.e., quarterly). Please refer to the POA&M Management Guide for

instructions on creating a POA&M item in eMASS. The SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort.

6. The ISO and/or System Steward continues to remediate deficiencies identified from the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports.
7. The ISO and/or System Steward uploads new Compliance Trending (Computer Compliance and Check Compliance) and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: If the system cannot reach the 90% threshold due to offline devices, then note this in the SCCD POA&M and Status of Requirements so it can be accounted for in the Risk Review.

4.4.2.7 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE)
    b. for Implementation Guidance for required security controls.

    c. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    d. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level

- Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.5 FedRAMP Enterprise or Single Instance Cloud Application (-e and -i Systems)

The FedRAMP Enterprise Cloud includes applications that are VA managed and utilize Cloud Service Provider (CSP) controlled services that are covered under the FedRAMP authorization boundary. The enterprise or single instance VA boundary entry must address, and upload, the customer responsible matrix (CRM) and inherit the controls from the FedRAMP boundary entry. The –E and –I instances are similar in nature. If contract only allows for a single instance the 'single instance (-I) is to be created along with the FedRAMP (-F/-VAF). After operational if additional locations start using this instance, going to the GRC Committee, and going through the Major Change process should be conducted to be converted to an 'enterprise cloud customer' organizational structure. All –F/-VAF systems should be accompanied by one (1) -E or –I system.

The Security Documentation and Technical/Testing requirements listed below are a guideline for the typical requirements to receive an ATO. If the Security Documentation or Technical/Testing requirements are not applicable for the eMASS authorization package, provide an explanation why it's not applicable in the **Status of Requirements** document.

The FedRAMP package (-F or -VAF) refers to a government agency sponsored Cloud Service Provider (CSP) or Software-as-a-Service (SaaS) package. They are only visible in eMASS to the assigned cloud or VAEC ISSOs. Non-cloud and non-VAEC ISSOs will only be responsible for the enterprise (-e) or single instance (-i) packages. The field is not responsible for -F or -VAF packages. Sensitive VA records (e.g., PHI/PII) are not contained within the -F or -VAF packages meaning there is no PII/PHI, controls, VA artifacts, or POA&Ms regarding VA Users. The PII/PHI and VA Users are all documented under the associated –E or –I system.

Note: The FedRAMP package (-F or -VAF) and the enterprise package (-e) or single instance (-i) must be completed simultaneously in eMASS and submitted for Risk Review (RMF Step 5: Stage 3) at the same time.

4.5.1 Security Documentation

The following sections provide details for each of the required security artifacts including the document requirements, references, and the parties that can provide additional guidance for each artifact. If available, templates for the applicable security artifacts/documents are located in the Templates section of the eMASS Knowledge Service page.

An artifact that is generated through eMASS as part of the authorization package and is reviewed/approved by the ISO and/or Information System Security Officer (ISSO) in the eMASS workflow as part of the authorization package may not require signature(s) and may be valid without signature(s). Contact your ISSO with questions on how to complete the documentation.

4.5.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA ITSM change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The CMP template should be used to complete the CMP and is available in the VA OIT Service Management Office's Process Asset Library (PAL). The ISO or system steward should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO/system steward works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO or system steward uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change to the system occurs.

Note: System Level Configuration Management Plans are under the governance of the VA OIT Service Management Office (SMO), Service Configuration Management organization, which collaborates with the Enterprise Program Management Division (EPMD), for continuous maintenance of the template and the availability to the enterprise. Please reach out to the OIT SMO ECRCM Service Configuration Management Staff for any questions about the CMP.

4.5.1.2 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO or system steward works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an IRP is required. If yes, then the ISO or system steward will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO or system steward uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the IRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change to the system occurs.

4.5.1.3 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select “YES” and then will be required to upload the systems-based BIA to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.

3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.5.1.4 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select "Yes" and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Contingency Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.5.1.5 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.5.1.6 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.5.1.7 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.5.1.8 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,

- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.5.1.9 Customer Responsibility Matrix/ Control Implementation Summary (CRM/CIS)

The CRM/CIS is determined by the CSP and validated by FedRAMP. It identifies and describes agency responsibilities.

Roles and Responsibilities

- The ISO or system steward provides implementation details for all controls and control enhancements identified as customer agency responsibility.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-53
- VA Handbook 6500

Continuous Monitoring Requirement

- Coordinate with the CSP to update the CRM/CIS when a significant/major change to the system occurs.

4.5.1.10 Application Threat Modeling

Application Threat Modeling is a security documentation activity that is conducted before source code is written for custom-developed applications (for entire applications, or e.g., a library, a micro-service, or any application that it has been determined to independently scan and manage the vulnerability data for). Application Threat Modeling may also be conducted before COTS and SaaS applications are deployed or allowed to operate at the direction of OIS and/or CSOC. The goal of threat modeling is to determine where and what type of security

controls need to be implemented in source code (or provided by an IT environment) for custom-developed applications. The goal for COTS and SaaS applications is to determine what product or service security configuration is needed (or provided by an IT environment).

Note: Application Threat Modeling is a manual documentation activity where the results are periodically updated, at a minimum annually, to maintain them.

Application Threat Modeling guidance is provided below:

- Custom-developed applications (the entire application, or e.g. a library, a micro-service, or any component that it has been determined to independently scan and manage the vulnerability data for), or instances of COTS and SaaS at the direction of OIS and/or CSOC, is analyzed by VA application developers using the freeware Microsoft Threat Modeling Tool software.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the Application Threat Model.
- This requirement is not applicable to VistA systems.

Completion Steps

1. Obtain the freeware Microsoft software from Microsoft Security Development Lifecycle website. Install and configure the Threat Modeling Tool in your local environment.
2. Manually draw whiteboard-like diagrams using the Microsoft Threat Modeling Tool and audit potential threats generated by the tool.
3. Generate a report using the Threat Modeling Tool to use as the security documentation for this activity.

After the analysis has been completed, the ISSO, ISO, or System Steward uploads the Application Threat Model to eMASS as part of the authorization package and creates a POA&M item (if needed) for each Application Threat Model (i.e., annually). A remediation plan for any unmitigated findings should be included in the authorization package.

Continuous Monitoring

The Application Threat Model must be updated on an **annual basis** and/or when a significant change in the system or a major change in the application architecture occurs.

Note: Additional guidance for developing and analyzing application threat models using the Microsoft Threat Modeling Tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.5.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the

initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.5.2.1 Application Security Testing

Application Security Testing is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Application Security Testing is also conducted to effectively certify pipelines as part of the software factory life cycle to increase the level of confidence in security testing automation that is relied on for automated deliveries and releases.

Successful completion of Application Security Testing is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process.

Application Security Testing guidance is provided below:

- Custom-developed application source code (the entire application, or e.g., a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data for) is scanned by VA application developers using the OIS-licensed Micro Focus Fortify Static Code Analyzer (SCA) software.
- Final developer performed Fortify scans and mitigations for security issues in production source code are validated by OIS Software Assurance for correctness and completeness.
- Successful completion of Application Security Testing is a prerequisite to Penetration Testing.
- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Application Security Testing attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is not applicable to VistA systems

The results of OIS Software Assurance Application Security Testing Validation attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another validation attempt must be made. The results of OIS Software Assurance Application Security Testing Validation are also uploaded in an automated fashion to eMASS shortly after completion. A notification email is provided by OIS ISRM GRC Scans after this occurs.

To locate application scan result findings in eMASS:

- Go to https://va.emass.apps.mil > [your system] > Assets > Findings > Applications (located under “View by” on left side of screen)
- Under the Application Details section, click “Load Details”

Note: Field staff should ***not*** delete any results, even when remediated. As findings are remediated and subsequent scans are loaded to eMASS, remediated findings will roll off the totals shown on the above page. System owners are responsible for creating at least one POA&M per scan to document remediation and mitigation activities.

Completion Steps

1. Obtain the OIS-licensed Fortify software from OIS Software Assurance. Install and configure Fortify in your local build environments and also on your build server (if applicable). Perform Fortify scans on source code locally and also on your build server (if applicable) as a scheduled build job.
2. Audit Fortify scan results and implement mitigations in source code as needed to ensure that there are minimally no remaining critical or high severity findings, and that for example the latest version of Fortify software and rulepacks are being used.
3. Upload your submission package materials to your application's share (on the Intranet only), if permissions need to be updated please email OISSwAServiceRequests@va.gov with the Application-ID and VA address(es) needing access.
4. Navigate to the Your IT Services portal using your web browser, and fill out the Application Security Support form as follows:
    a. In the REQUESTOR INFORMATION section, in the Requested For field, search for your name
    b. If applicable, update the auto-populated requestor information fields
    c. In the REQUEST DETAILS section, in the Services Request field, select Application Security Scan Validation
    d. In the Application Name field, enter your application's name
    e. In the Application ID field, enter your application's VA Software Assurance Program identifier
    f. Fill out this PDF form and attach it to the request using the Add attachments link
    g. Fill out a text file named resubmission.txt that explains changes since any prior submissions and attach it to the request using the Add attachments link
5. Click on the Submit button.
6. Make a note of your ticket’s request number.

After the request has been made, an OIS Software Assurance team member will follow up. You can then view this ticket, or any of your open tickets, through the Your IT Services portal.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the validation report to eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package.

Note: In the event the application cannot be scanned due to technical issues, or another extenuating circumstance including those that are non-technical, the explanation will need to be documented and uploaded to eMASS as part of the **Status of Requirements** within that authorization package.

Warning: Upon successful completion of Application Security Testing, security testing results for subsequent automated deliveries and releases must be very carefully monitored locally for changes. There must be build failure criteria for Fortify scans to ensure that the Fortify integration and associated workflows that were certified are being maintained during software factory operation.

Continuous Monitoring

Successful completion of the software assurance validation of developer-performed scans is additionally required as follows:

- Successful Application Security Testing completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Application Security Testing is also required when requested by OIS and/or CSOC.

Note: Additional guidance for scanning custom-developed application source code for potential vulnerabilities using the OIS-licensed Fortify tool can be found on OIT Teams. There is an OIS Software Assurance support site in Teams.

4.5.2.2 Software Composition Analysis

Software Composition Analysis is conducted during development and maintenance systems development life cycle phases to improve the ability of VA's business IT systems' custom-developed software components to defend themselves against attacks. Software Composition Analysis focuses on supply chain risk management for custom-developed VA applications. Software Composition Analysis is performed by analyzing underlying libraries and frameworks for potential vulnerabilities as an additional activity during Application Security Testing.

Successful completion of Software Composition Analysis is required for all initial production releases OR upon discovery that the application has already been deployed to production and has not gone through the process. While Software Composition Analysis is performed as an additional activity during Application Security Testing, separate pass/fail verdicts are returned.

Software Composition Analysis guidance is provided below:

- Libraries and frameworks that use custom-developed applications (e.g., the entire application, a library, a micro-service, or any scannable block of code that it has been determined to independently scan and manage the vulnerability data) require Software Composition Analysis by OIS Software Assurance as additional activity during Application Security Testing.

- The ISO or system steward creates one POA&M item and a response in the POA&M tab within eMASS for the results of each Software Composition Analysis attempt for the period of time automated deliveries and releases are allowed. Multiple attempts are usually required to successfully complete the activity.
- This requirement is only applicable to custom-developed applications that are written in the following programming languages:
    - .NET Framework
    - .NET Core
    - ASP.NET
    - C#
    - C/C++
    - Classic ASP (with VBScript)
    - Go
    - Java (including Android)
    - JavaScript
    - JSP
    - Kotlin
    - Objective-C/C++
    - PHP
    - Python
    - Ruby
    - Swift
    - Visual Basic (VB.NET)
    - Visual Basic

The results of OIS Software Assurance Software Composition Analysis attempts are returned to VA application developers. A notification email is provided by OIS Software Assurance and a PDF report is posted to the application's restricted-access OIS Software Assurance share. If a failing verdict is returned, the indicated rework must be performed, and another attempt must be made by making another Application Security Testing request.

Completion Steps

- Software Composition Analysis scans are performed by OIS Software Assurance when Application Security Testing validations are requested.
- Please see the completion steps for Application Security Testing. There are no additional procedures to request Software Composition Analysis scans.

After a passing verdict has been achieved, the ISSO, ISO, or System Steward uploads the scan report to the Artifacts tab within eMASS as part of the authorization package and creates a POA&M item (if needed). A remediation plan for any unmitigated findings should be included in the authorization package. The latest progress should be added to the Status of Requirements. If the scan is not applicable, then list why it's not appliable in the Status of Requirements prior to uploading to the Artifacts tab within eMASS.

Warning: Upon successful completion of Software Composition Analysis, the environments, libraries, and frameworks must be very carefully monitored for changes. Software Composition Analysis tools, such as OWASP Dependency Check, are strongly recommended to be integrated into pipelines.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally required as follows:

- Successful Software Composition Analysis completion is required after the initial production release, automated production delivery, or release on calendar-based intervals, at a minimum annually, and at ISSO direction (which may include additional criteria that affects timing) to effectively certify software factory operation (if applicable).
- Software Composition Analysis is also required when requested by OIS and/or CSOC.

Note: Additional guidance for Software Composition Analysis can be found on OIT teams. There is an OIS Software Assurance support site in Teams.

4.5.2.3 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.

3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.6 Facility

Facility authorizations describe the local processes that differ from enterprise standards, including security control requirements provided by Contingency Planning, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, and System and Information Integrity. Facility authorization boundaries include IT Hardware (i.e., servers, printers, scanners, peripheral devices, desktop computer systems) and any operating systems (OS) software specific to the facility. Please refer to section 3.3 for Security Boundary Guidance.

Facilities may choose to inherit common control providers from the VA T1SOR, VA Enterprise SOR (VA ENTSOR), or VA Area SOR. Refer to Appendix D – Common Control Providers/System of Record (SOR) for complete details to help determine if the VA T1SOR, VA ENTSOR, or VA Area SOR is applicable.

4.6.1 Security Documentation

4.6.1.1 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) identifies configuration management roles and responsibilities, resources, and processes to ensure any changes are evaluated and approved before implementation. CMP guidance is provided below.

As part of the normal configuration/change management of an information system, change requests are entered into the authorized VA ITSM change control system, Your IT Services, for review, approval, and implementation by the appropriate VA OIT organizations or service providers.

Roles and Responsibilities

The Facility team should use the CMP template provided by the field organization. The ISO, system steward, or designee should work with the ISSO to complete the CMP.

Standards / Guidelines

- NIST SP 800-128
- NIST SP 800-53 (CM-9 Configuration Management Plan)
- VA Handbook 6500
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure servers that support the system.
- The CMP should include a current configuration baseline detailing hardware and software associated with the system. Network devices do not apply.

Completion Steps

1. The ISO, system steward, or designee works with the ISSO to complete the CMP.
2. Once the CMP is complete, the ISO, system steward, or designee uploads the CMP to the Artifacts tab in eMASS, and links to the appropriate security control (CM-9) for the Configuration Management Plan.

Continuous Monitoring Requirement

The CMP must be updated on an annual basis or when a significant/major change occurs.

4.6.1.2 Disaster Recovery Plan (DRP)

Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. DRP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of system level DRPs.
- The ISO or system steward works with the assigned ISSO and DRP Director to create or revise the DRP. A DRP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an DRP is required. If yes, then the ISO or system steward will be required to upload the DRP to eMASS. Guidance on when a DRP is required can be found in the VA Handbook 6500.8.
2. The ISO, DRP Director, or system steward develops or revises the DRP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed DRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as “Disaster Recovery Plan”. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the DRP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The DRP must be tested and updated on an annual basis or when a significant/major change occurs.

4.6.1.3 Incident Response Plan (IRP)

An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that were exploited, and restoring computing services. IRP guidance is provided below.

Roles and Responsibilities

- Facilities are responsible for completing the IRP. Systems should upload the facility IRP with the system name added to the title page to indicate the system utilizes the facility IRP.
- The ISO, system steward, or designee works with the assigned ISSO to create or revise the IRP.
- Each site is responsible for developing local level procedures incorporating VA-CSOC area of responsibility.
- A template for the IRP can be found on the Enterprise Security Operations (ESO) document library.

Standards / Guidelines

- NIST SP 800-61
- NIST SP 800-53 (IR-8 Incident Response Plan)
- VA Handbook 6500

Completion Steps

1. During RMF Step 1 within eMASS, the ISO, system steward, or designee will be prompted to indicate whether an IRP is required. If yes, then the ISO, system steward, or designee will be required to upload the IRP to eMASS.
2. The System Owner or delegate develops or revises the IRP using the applicable standards and guidelines.
3. Once completed and tested, the ISO, system steward, or designee uploads the signed IRP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document

within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the IRP has been uploaded to the FISMA tab, the ISO, system steward, or designee must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The IRP must be tested and updated annually or when a significant/major change occurs.

4.6.1.4 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select “YES” and then will be required to upload the systems-based BIA to eMASS.

2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.6.1.5 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select "Yes" and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Contingency Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.6.1.6 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO, system steward, or designee should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the agreement as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.6.1.7 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

ISOs, system stewards, or designees must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO, system steward, or designee will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO, system steward, or designee will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO, system steward, or designee uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO, system steward, or designee must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO, system steward, or

designee uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PIA has been uploaded to the FISMA tab, the ISO, system steward, or designee must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.6.1.8 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, or designee, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, or designee, and ISSO.
- The ISSO validates information added by the ISO, system steward, or designee within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.

4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.6.1.9 System Security Plan (SSP)

Roles and Responsibilities

- The ISO, system steward, or designee completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO, system steward, or designee in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.6.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

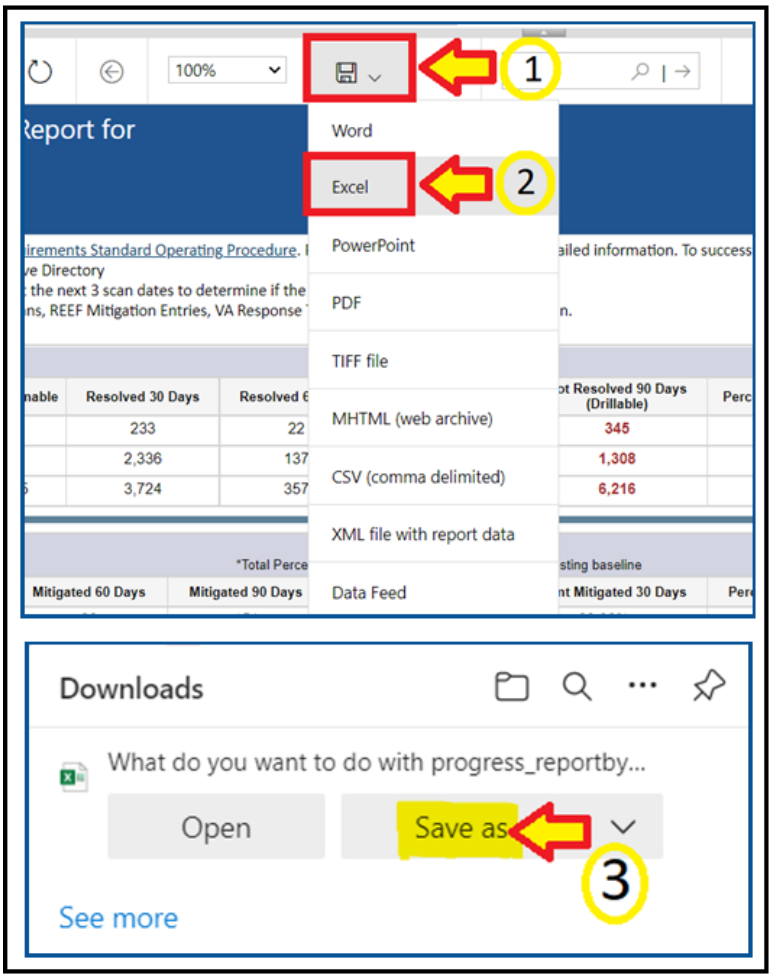
4.6.2.1 Nessus Scan

A credentialed Nessus vulnerability scan against all instances of the operating system and desktop configurations for the facility IP addresses must be conducted to identify security flaws.

Completion Steps

The following steps can be performed to meet the Nessus Scan requirement:

1. All systems should complete the *Hardware and Software System Inventory Import* process to ensure all IPs are properly added to eMASS and a Nessus scan can be completed. Instructions can be found in the Hardware and Software System Inventory Import SOP, which is in the Standard Operating Procedures section of the eMASS Knowledge Service page.
2. The ISO, system steward, or designee can request a Nessus scan using this link. Once the request is completed, ISRM will work with CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices be added to the existing monthly predictive scan. If ISRM/CSOC determine a supplemental scan is required then the results, once received, must be uploaded to the Artifacts tab within eMASS. If decided that the authentication information can be added for the non-Windows devices to the monthly predictive scans conducted by CSOC, then record and import the hardware baseline to eMASS (see Step 1 above), so the applicable Nessus data can be recorded.
3. Once the system's Nessus Scan data is accurately recorded, the ISO, system steward, or designee follows these steps:
    a. Browse to Information Central Analytics and Metrics Platform (ICAMP) and use the Remediation Effort Entry Form (REEF) to document your manual mitigation/remediation effort. For each deficiency identified from the scan, the ISO, system steward, or designee creates a response within REEF for mitigating the deficiencies and/or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within REEF.
    b. Once all manual remediation has been documented within REEF, run this report within ICAMP.
    c. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**. See the image below for step-by-step view.



d. The ISO or system-level system steward then uploads the report to the Artifacts tab within eMASS using the naming instructions identified above in step 3c.
e. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the vulnerability scans to determine and document those findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or from the vendor should also be documented as part of this analysis.

4. The ISO or system steward will follow standard VA Enterprise Vulnerability Management Solutions (EVMS) process for remediation of Nessus scan vulnerabilities. If a POA&M is required, the ISO or system steward creates a POA&M for each unique vulnerability. POA&M responses will follow the POA&M Management Guide.

Continuous Monitoring

CSOC conducts predictive Nessus vulnerability scans on a monthly basis. A supplemental scan is required for A&A purposes when requested by OIS, CSOC, and/or when new vulnerabilities potentially affecting the system/applications are identified and reported. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: Facility boundaries should identify physical specifics and identify hardware/software applicable to each Facility.

4.6.2.2 Enterprise Discovery Scan (EDS)

If required by OIS, an Enterprise Discovery Scan (EDS) against all instances of the operating system and desktop configurations must be conducted to identify security flaws. Any vulnerabilities must be remediated within the approved timelines for the severity of the findings, and a POA&M must be created in eMASS to keep track of the remediation effort.

Completion Steps

1. Browse to the Information Central Analytics and Metrics Platform (ICAMP) and use the EDS input (EDSI) form to document your manual remediation effort. For each deficiency identified from the scan, the ISO, system steward, or designee creates a response within EDSI for mitigating the deficiencies and / or provides evidence that the deficiencies have been mitigated. Also, include the scheduled completion date and status of each deficiency within EDSI.
2. Once all the manual remediation has been documented within EDSI, run this report within ICAMP.
3. Export the report by going to the top of the screen select the Export drop down menu which appears as a computer disc. Choose Excel. 'Save as' **SystemNameORAcronym_Nessus_MMDDYYYY.xlsx**.
4. The ISO, system steward, or designee then uploads the report from step 3 above to the Artifacts tab within eMASS. A mitigation plan should also be uploaded to the Artifacts tab within eMASS.
5. Within the uploaded mitigation strategy, each system should conduct an analysis on the results of the EDS to determine and document the findings that are false positives, not applicable to the system, or otherwise mitigated. Additionally, findings that must be remediated through or by the vendor should be documented as part of this analysis.
6. The ISO, system steward, or designee creates a single POA&M and a response in the POA&M tab within eMASS for the EDS as outlined by the POA&M Management Guide. The EDS will utilize CCI IA-5.3 for POA&M creation where necessary to keep track of the remediation effort.

Continuous Monitoring

CSOC conducts EDS on a quarterly basis. The quarterly results must be pulled in accordance with the guidance above to maintain an ATO. The EDS results must be provided when the tool used receives an upgrade or a major change to the system occurs. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

4.6.2.3 Security Configuration Compliance Data (SCCD)

All accreditation boundaries that contain an operating system are required to provide Security Configuration Compliance Data using BigFix. If BigFix cannot be installed because the system is not supported by BigFix, another VA approved product, such as OpenSCAP, may be used as a substitute until BigFix is compatible with the system. Please refer to the BigFix FAQ and create an incident ticket to be assigned to OIS EV Support Group for approval of other SCCD products. If Security Configuration Compliance Data is not applicable, explain why it's not applicable in the Status of Requirements. The Security Configuration Compliance Data requires at least a 90% compliance to receive an ATO for 3 years.

Completion Steps

The following steps must be performed to meet the Security Configuration Compliance requirement:

1. The BigFix agent **must be** installed to receive Security Configuration Compliance Data. Ensure that the BigFix agent is installed/functioning correctly and confirm that your information system/facility endpoints (i.e., servers/workstations) make up the FISMA boundary. A functioning endpoint is one that is actively communicating with the BigFix core servers and has a last-report-time within the last day or two. Please utilize the Computer Lookup reporting to search for endpoints by hostname(s). If an endpoint is found and has a recent last-report-time, then the BigFix agent is functioning as expected. Please see the BigFix FAQ for help on installing the BigFix agent. If you need assistance with BigFix, please contact the Enterprise Service Desk (ESD) to enter a ticket and assign it to the OIS EV Support Group. Contact the ESD by phone at 1-855-673-4357 or online through Your IT Services portal.
2. The ISO, system steward, or designee is responsible for maintaining an accurate and up-to-date list of the hardware/software for their endpoints/environments. They must ensure all hostnames for the endpoints that comprise the FISMA boundary are listed in the eMASS Hardware/Software Inventory. The hostnames in the Hardware/Software Inventory must **exactly** match the hostnames listed in the BigFix Computer Lookup reporting (e.g., "R03AAASQL99" will be considered a different endpoint than "R03AAASQL99.R03.MED.VA.GOV"). Please use the following instructions for managing the Hardware/Software Inventory. Any questions regarding the management of endpoints in eMASS should be directed to ISRM. The Hardware/Software Inventory is exported once a day from eMASS, at 1:30pm Eastern, to generate the Security Configuration Compliance Data reporting. If you have modified the list of endpoints in eMASS before the 1:30pm cutoff, please run the GRC Boundaries – Computers by Information System report the

following day to verify all of your information system/facility endpoints are being included in Security Configuration Compliance Data reporting. If changes are made after 1:30pm Eastern, the changes won't be available until two days later.

3. After reviewing information system/facility FISMA boundaries for accuracy, the ISO, system steward, or designee runs the Security Configuration Compliance Data Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports and exports them to a PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).
4. The ISO, system steward, or designee uploads the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports to the Artifacts tab within eMASS. Ensure SCCD reports use the naming format identified in Section 4 above, Assessment and Authorization Requirements
5. The ISO, system steward, or designee creates a single POA&M item for the SCCD to serve as a reminder to resolve the deficiencies. A new POA&M item must be created for each required SCCD (i.e., quarterly). Please refer to the POA&M Management Guide for instructions on creating a POA&M item in eMASS. The SCCD will utilize CCI CM-6.7 for POA&M creation where necessary to keep track of the remediation effort.
6. The ISO, system steward, or designee continues to remediate deficiencies identified from the Checklist Trending (Computer Compliance and Check Compliance) and Compliance Trending reports.
7. The ISO, system steward, or designee uploads new Compliance Trending (Computer Compliance and Check Compliance) and Checklist Trending reports to the Artifacts tab within eMASS as evidence of remediation progress.

Note: When running the compliance reports, please select the applicable information system or facility. The boundary data and compliance data are updated nightly.

Continuous Monitoring

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or when changes are made to the approved secure configuration/hardening guides. To maintain the authorization decision, vulnerabilities must be remediated within the approved timelines for the severity of the findings.

Note: If the facility/area cannot reach the 90% threshold due to offline devices, then note this in the SCCD POA&M and Status of Requirements so it can be accounted for in the Risk Review.

4.6.2.4 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- The ISO, system steward, or designee requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD

- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.7 Medical Devices

Medical Devices are MRIs, Pacemakers, X-ray machines, etc. Generally, web applications are not Medical Devices. The Medical Devices boundary consists of required diagrams for all devices (medical devices and special purpose systems (SPSs), where applicable), supporting software architecture, IP ranges, and documentation of all minor applications within the boundary. The ISSO should provide assistance to the ISO or System Steward with Medical Device authorization requirements. Please refer to section 3.3 for Security Boundary Guidance.

4.7.1 Security Documentation

4.7.1.1 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.7.1.2 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select “Yes” and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as “Contingency Plan”. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.7.1.3 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.

6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.7.1.4 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
-]VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.
2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name,

and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change occurs, then a new PTA/PIA must be completed.

4.7.1.5 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.
3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change occurs.

4.7.1.6 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.

- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change occurs.

4.7.2 Technical Scans/Testing Requirements

4.7.2.1 Nessus Scan

The VA Enterprise process for managing Medical Device (MD) and Special Purpose System (SPS) cybersecurity vulnerabilities utilizes Nessus vulnerability scanners and Nessus Network Monitoring hardware for active and passive vulnerability scans. The vulnerability scan results for network connected MDs and SPSs are compiled and analyzed by the Specialized Device Security Division (SDSD), who forward the reports to MD and SPS system owners for remediation action. The Medical Device Vulnerability Management SOP and SPS Vulnerability Management SOP should be reviewed and followed to ensure compliance with the MD and SPS management processes.

4.7.2.2 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.

    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

4.8 Other Federal Agency (Non-eMASS Reciprocity)

An 'Other Federal Agency' system allows the VA to utilize a pre-existing ATO from a Federal Agency and grant a reciprocity based ATO so the VA can utilize the system. The system needs to be approved by the VA GRC Oversight Committee and entered into eMASS. A non-eMASS reciprocity ATO can be granted by the AO once a Risk Review of the system is completed. The review of security artifacts may take place in person by the Risk Review team at the 'Other Federal Agency' facility or virtually if online access can be granted to the Risk Review team. The Risk Review must ensure that the 'Other Federal Agency' ATO meets VA standards. Any VA required security documentation, such as an ISA/MOU or PTA/PIA, must be completed and uploaded to the Artifacts tab within eMASS by the ISO, system steward, and/or ISSO. The Reciprocity SOP should be utilized when working an Other Federal Agency package.

4.9 Platform

The different Platform boundaries throughout the VA require an authorization decision; however, due to the nature of these platforms, there's a limited number of technical scans/testing requirements that can be completed. The following authorization requirements must be completed for IO Network Operations, IO Platform Support Mainframe, IO Platform Support UNIX, and IO Platform Support Windows. Please refer to section 3.3 for Security Boundary Guidance.

Platforms may choose to inherit common control providers from the VA T1SOR and VA Enterprise SOR (VA ENTSOR). Refer to Appendix D – Common Control Providers/System of Record (SOR) for complete details to help determine if the VA T1SOR or VA ENTSOR is applicable.

4.9.1 Security Documentation

4.9.1.1 Systems-Based Business Impact Analysis (BIA)

Systems-based BIAs characterize the impacts and consequences of a disruption to an information system, supported mission / business processes, and interdependencies. They are used as the foundation to determine information system contingency planning requirements and priorities. BIAs are based upon current boundaries established by the Office of Information Security (OIS). Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. BIA guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning guidance for systems-based BIAs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the systems-based BIA. A systems-based BIA template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

5. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a systems-based BIA is required. All VA information systems are required to complete an ISCP and the systems-based BIA is the foundation to determine information system contingency planning requirements and priorities, therefore, the ISO or system steward will select "YES" and then will be required to upload the systems-based BIA to eMASS.
6. The ISO, ISCP Coordinator, or system steward develops or revises the systems-based BIA using the applicable standards and guidelines found on the Knowledge Service.
7. Once completed and tested, the ISO or system steward uploads the signed systems-based BIA to eMASS by going to System > Details > FISMA. After uploading the BIA to the FISMA tab, it needs to be associated to the following controls: CP-2 and CP-7. Please select the Category as "Business Impact Analysis". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

8. Once the systems-based BIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring

The systems-based BIA must be reviewed and updated on an annual basis or when a significant/major change to the system occurs.

4.9.1.2 Information System Contingency Plan (ISCP)

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and service to an alternate site. Plans are based upon current boundaries established by the Office of Information Security (OIS). Each year Each year the OIS Information System Business Continuity Office (OIS ISBC) will monitor systems to make sure they maintain the annual review requirements. ISCP guidance is provided below.

Roles and Responsibilities

- OIS ISBC is the Office of Primary Responsibility (OPR) for oversight of planning and testing of ISCPs.
- The ISO or system steward works with the assigned ISCP Coordinator to create or revise the ISCP. An ISCP template can be found on the Knowledge Service page.

Standards / Guidelines

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53 (CP-2 Contingency Plan)
- VA Handbook 6500
- VA Handbook 6500.8 Information System Contingency Planning

Completion Steps

1. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether an ISCP is required. All VA information systems are required to complete an ISCP, therefore, the ISO or system steward will select “Yes” and then will be required to upload the ISCP to eMASS.
2. The ISO, ISCP Coordinator, or system steward develops or revises the ISCP using the applicable standards and guidelines found on the Knowledge Service.
3. Once completed and tested, the ISO or system steward uploads the signed ISCP to eMASS by going to System > Details > FISMA. By uploading the security document to the

FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Please select the Category as "Contingency Plan". Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.

4. Once the ISCP has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs, including CP-2 and CP-7. To verify, go to the Artifacts tab, type the Artifact Name in the Search box, click on the Artifact Name, associated controls are listed in the Artifact Details section. If security controls are not listed, click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

The ISCP must be tested and updated on an annual basis or when a significant/major change in the system occurs.

4.9.1.3 Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU)

Before an external connection is established with the VA, a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) is required to authorize a connection between information systems that do not share the same Authorizing Official. An ISA/MOU must be provided for all external interconnections.

Roles and Responsibilities

- The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the ISA/MOU.
- A VA review team will assess the documents against a checklist for quality and content.
- The reviewer will work with the ISSO to ensure no documentation deficiencies and notify the ISSO when the document is ready for signatures.
- The ISSO will obtain the appropriate signatures.
- The ISSO will upload the document to the Enterprise Document SharePoint and to the Artifacts tab within eMASS. The ISO or system steward should ensure the correct Artifact Category and Type are selected when uploading to the Artifacts tab.

Standards / Guidelines

- NIST SP 800-47
- VA Handbook 6500

Completion Steps

1. The ISO, in coordination with the entities identified in NIST SP 800-47, will complete the MOU/ISA using the latest template provided at: MOU ISA Template.
2. ISSO will upload all final draft MOU/ISA documents to the MOU ISA Document Portal.
    a. The MOU/ISA Intake Portal User Guide is located on the MOU ISA Document Portal.
3. The OIT OIS ISRM ECSD MOU ISA Team will assess the documents for quality, content, and security.
4. The Enterprise Cybersecurity Support Division (ECSD) reviewer(s) and the ISSO will work collaboratively with the ISO/COR to correct deficiencies found in the documentation.
5. Once all deficiencies have been corrected and accepted, the ECSD reviewer will notify the ISSO via email that the document is ready for signatures.
6. The ISSO will route the document for signatures.
7. Upon receipt of the completed and signed MOU/ISA document, the ISSO will upload the document using the *Publish a Signed Document* feature on the MOU ISA Document Portal.
8. The finalized documents with signatures are linked to the appropriate security controls (CA-3, SA-9) and uploaded to the Artifacts tab within eMASS.

Continuous Monitoring Requirement

The MOU/ISA Annual Review Sheet must be completed annually based on the date of the last signature on the MOU/ISA. If there is a significant change that impacts the architecture as documented, please contact the OIT OIS ISRM ECSD MOU ISA Team.

4.9.1.4 Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)

All ISOs or system stewards must work with the VA Privacy Services Office to complete a PTA for each system. During RMF Step 1 within eMASS, the ISO or system steward will be prompted to indicate whether a PTA/PIA is required. If yes, then the ISO or system steward will be required to upload the PTA/PIA to the Artifacts tab within eMASS.

Privacy Threshold Analysis (PTA)

Roles and Responsibilities

- The ISO, Privacy Officer, ISSO, and Business Owner must work together to submit a PTA, which is reviewed by the Privacy Services Office.
- The PTA requires the Privacy Officer, ISO, and ISSO to sign and date the PTA.
- If the PTA determined a PIA is required, then see the below PIA section to complete the PIA.

Completion Steps

1. The PTA template and the PTA completion process can be found at Privacy Compliance PTA.
2. Once completed, the ISO or system steward uploads the signed PTA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PTA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Privacy Impact Assessment (PIA)

If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed.

Roles and Responsibilities

- The PIA must be submitted to the Privacy Services Office by the Privacy Officer with input from the ISO, ISSO, and any other relevant stakeholders. Additional comments from the PIA support analysts, if any, must also be incorporated.
- The ISO must answer questions related to the PIA in the FISMA tab within eMASS (System > Details > FISMA). Since the Privacy Compliance Dashboard within eMASS can provide reports on these metrics across all systems, the PIA questions must be kept up to date.
- The PIA requires the Privacy Officer, ISO, and ISSO to sign and date the PIA.

Standards / Guidelines

- E-Government Act of 2002
- OMB Circular 03-22
- VA Directive 6502
- VA Directive 6508
- VA Handbook 6508.1
- NIST SP 800-53 (AR-2 Privacy Impact, Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The PIA template and the PIA completion process can be found at Privacy Compliance PIA.

2. Once the PIA is verified as completed by Privacy Services, re-submit the PIA as a PDF file with the required signatures to PIA Support. Additionally, the ISO or system steward uploads the signed PIA to eMASS by going to System > Details > FISMA. By uploading the security document to the FISMA tab, eMASS will automatically add the document to the Artifacts tab and map it to controls. Once uploaded to the FISMA tab, it can be managed (e.g., newer versions) within the Artifacts tab by clicking the Artifact Name. The security document within the FISMA tab should not be deleted or the security document and the history will be deleted.
3. Once the PIA has been uploaded to the FISMA tab, the ISO or system steward must ensure that all documents are appropriately associated as evidence to the relevant security controls and CCIs. To verify, go to the Artifacts tab, click on the Artifact Name, and then click Edit Artifact to add in more security controls or CCIs. Refer to the eMASS Implementation Guide for additional details.

Note: Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIA Support.

Continuous Monitoring Requirement

A PTA must be completed annually. A PIA is valid for 3 years. If a major change to the system occurs, then a new PTA/PIA must be completed.

4.9.1.5 Risk Assessment Report (RAR)

The RAR identifies, estimates, and prioritizes risk involved with organization operations. The RAR is generated within eMASS and utilizes the details provided on control risk, the 40 threats, and any ongoing or risk accepted POA&M items.

Roles and Responsibilities

- The ISO, system steward, and ISSO are responsible for ensuring POA&M items within eMASS are property created and updated.
- The 40 threats must be reviewed by the ISO, system steward, and ISSO.
- The ISSO validates information added by the ISO or system steward within eMASS.

Standards / Guidelines

- NIST SP 800-30
- NIST SP 800-53 (RA-3 Risk Assessment)
- VA Handbook 6500

Completion Steps

1. The ISO and ISSO should complete the Risk Assessment tab within their system.
2. All non-compliant Controls should be addressed for their risk plus any of the 40 threats that are applicable.

3. By default, the Risk Assessment tab will only show Non-Compliant Controls, but the view can be changed using the Filter.
4. The RAR will be included in the snapshot packages created in eMASS. Alternatively, the RAR can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The RA must be updated on an annual basis or when a significant/major change in the system occurs.

4.9.1.6 System Security Plan (SSP)

Roles and Responsibilities

- The ISO or system steward completes the assessments in eMASS and develops POA&M items and responses.
- The ISSO validates information added by the ISO or system steward in eMASS.

Standards / Guidelines

- NIST SP 800-18,
- NIST SP 800-53 (PL-2 System Security Plan)
- VA Handbook 6500

Completion Steps

1. The SSP is developed within eMASS.
2. All required diagrams and confirmation of the security authorization boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations.
3. The system steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. Refer to the eMASS Implementation Guide for additional details.
4. The ISO and ISSO validates information added by the system steward in eMASS.
5. The SSP will be included in the snapshot packages created in eMASS. Alternatively, the SSP can be generated by going to the Reports tab within eMASS.

Continuous Monitoring

The SSP must be updated annually or when a significant/major change to the system occurs.

4.9.2 Technical Scans/Testing Requirements

Findings identified in each technical/testing requirement, also referred to as a technical scan, should be mitigated from the initial detection date within the remediation timeframe specified in the Knowledge Service (i.e.), Critical – 30 days; High – 60 days; Moderate – 90 days; Low – determined by the ISO; Emergent – ASAP. As outlined in BOD 19-02, Internet accessible systems require mitigation of Critical findings within 15 days and High findings within 30 days of the initial detection date. A single POA&M item should be created in eMASS for each of the

applicable scans to track the remediation progress. Every completed scan requires a POA&M item. For example, a new Nessus scan POA&M item must be created every month for each new scan. In addition, a detailed remediation strategy with expected remediation date and status of each vulnerability should be uploaded to the Artifacts tab within eMASS for each of the applicable scans.

4.9.2.1 Control Review

To support compliance with VA policy and Federal requirements, VA systems will be selected to undergo an RMF Step 4 Assessment, whereby an Office of Information Security Risk Management (ISRM) team will review control implementation details and supporting evidence in eMASS during the RMF Step 4 Control Assessment workflow.

The purpose of RMF Step 4 is to determine the extent to which security requirements are implemented correctly, operating as intended, and producing the desired outcome prior to Authority to Operate (ATO) review and determination.

During RMF Step 4, the team will review the system's applicable security controls by testing the implementation details against the supporting artifacts within eMASS to validate and determine compliance with VA policies and guidance. The review team will be targeting a sub-set of the top findings found in the Office of Inspector General (OIG) audits from the past fiscal year audits, but may be adjusted as time progresses.

Completion Steps

1. Completely and accurately progress through RMF Steps 1 – 3.
    a. Utilize the Knowledge Service (KS) Security Controls Explorer (SCE) for Implementation Guidance for required security controls.
    b. Ensure that all requirements are followed from the Authorization Requirements for eMASS SOP.
    c. Confirm steps outlined in the eMASS Implementation User Guide have been followed.
2. Enter self-assessment test results against all the APs assigned to Security Control.
3. Ensure all applicable controls have implementation statements, as well as associated evidence documented.
4. Notify assigned Authorizing Official Designated Representative (AODR) to initiate RMF Step 4.
5. System Steward is to advance the system's workflow to the RMF Step 4 Control Assessor workflow and conduct a bulk release of the identified controls that will be receiving a review **no later than 70 days prior to ATD**.

To bulk release controls ensure to follow the below steps:

1. Controls>Bulk Processing
2. Submit for Review
3. Select controls identified via email communications for review
4. Submit for Review

Workflow Timeline Requirements and Additional Details

- System Steward/Information System Owner requests AODR to initiate RMF Step 4 and advances/releases controls to Control Assessor **no later than (NLT) 70 days prior to ATD and/or scheduled Control Review.**
- Control Review is finished within 15 days, results uploaded to the Artifacts tab within eMASS and a notice is sent to system stakeholders closing out RMF Step 4. During this stage, stakeholders will be unable to make updates to their entities Controls and CCIs.
- RMF Step 5 is initiated
    - Final POA&Ms are created from the Control Review report
    - RMF Step 5.1 has a total of no more than 10 days for completion
- System is required to be to RMF Step 5.3, Risk Review (RR), NLT 45 days prior to ATD
- Communications will be sent to system stakeholders:
    - 90-100 days before the system ATO expiration date to notify system of upcoming Authorization Termination Date (ATD) reminding of requirements.
    - 7 Days prior to the system's upcoming RMF Step 4 Control Review, a reminder will be sent out for the system to complete RMF Steps 1-3 and proceed to RMF Step 4.
    - Close out to summarize results and link report on eMASS under 'Artifacts' tab.
- To avoid non-compliant results, please be sure to provide:
    - Evidence that is current and contains a timestamp
    - Evidence that directly addresses the control objective(s)
    - Artifacts at the CCI level and not at the parent control level
    - Details when uploading artifacts (i.e., page numbers) to direct the assessor to the exact verbiage to satisfy the control

Continuous Monitoring Requirement

As outlined above, once the Control Review is complete, POA&Ms are created in RMF Step 5.1 for the Control Review findings. These POA&Ms should be created and updated as outlined in the POA&M Management Guide.

Note: Questions regarding RMF Step 4 Assessment should be directed to: VAOISControlReviewTeam@va.gov

5 *Appendix A – Acronyms/Definitions*

Acronym	Description
AI	Action Item
A&A	Assessment and Authorization
AO	Authorizing Official
ATO	Authorization to Operate
BIA	Systems-Based Business Impact Analysis
CAE	Common Application Enumeration
CCI	Control Correlation Identifier
CIO	Chief Information Office
CMP	Configuration Management Plan
COTS	Commercial off the Shelf
CRM	Customer Responsibility Matrix
CSOC	Cyber Security Operations Center
DRP	Disaster Recovery Plan
ECSD	Enterprise Cybersecurity Support Division
EDS	Enterprise Discovery Scan
eMASS	Enterprise Mission Assurance Support Service
ENT SOR	Enterprise System of Record
EPR	Emergency Preparedness & Response
FISMA	Federal Information Security Management Act
GRC	Governance, Risk, and Compliance
IaaS	Infrastructure as a Service
ICAMP	Information Central Analytics and Metrics Platform
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISRM	Information Security and Risk Management
ISSO	Information System Security Officer
ITSM	IT Service Management
MASA	Mobile Application Security Assessment
MOU	Memorandum of Understanding
OIS	Office of Information Security
OIT	Office of Information Technology
OPR	Office of Primary Responsibility
PaaS	Platform as a Service
PDAS	Primary Deputy Assistant Secretary
PIA	Privacy Impact Assessment
POA&M	Plan of Actions and Milestones

Acronym	Description
PTA	Privacy Threshold Analysis
RAR	Risk Assessment Report
REEF	Remediation Effort Entry Form
RMF	Risk Management Framework
SaaS	Software-as-a-Service
SCCD	Security Configuration Compliance Data
SIA	Security Impact Analysis
SSP	System Security Plan
SwA	Software Assurance
TIC	Trusted Internet Connection
VAEC	VA Enterprise Cloud
VASI	VA Systems Inventory
VA T1SOR	Veterans Affairs Tier I System of Record
WASA	Web Application Security Assessment

6 *Appendix B – Quick Reference Guide – Security Documentation Requirements*

Boundary	Security Document	Required Y/N
Application hosted On-Premises/ VA Network	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Disaster Recovery Plan Test	Y
	Incident Response Plan	Y
	Incident Response Plan Test	Y
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	Y – if applicable
Application hosted in Managed Service	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Disaster Recovery Plan Test	Y
	Incident Response Plan	Y
	Incident Response Plan Test	Y
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	Y – if applicable
Application hosted in	Configuration Management Plan	Y

Boundary	Security Document	Required Y/N
FedRAMP cloud (VAEC)	Disaster Recovery Plan	Y – for VAEC, N – for systems hosted in VAEC
	Disaster Recovery Plan Test	Y – for VAEC, N – for systems hosted in VAEC
	Incident Response Plan	Y
	Incident Response Plan Test	Y
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	Y – if applicable
Application hosted in FedRAMP cloud (Non-VAEC)	Configuration Management Plan	Y
	Disaster Recovery Plan	N
	Disaster Recovery Plan Test	N
	Incident Response Plan	Y
	Incident Response Plan Test	Y – if applicable
	Systems-Based BIA	Y – if applicable
	Information System Contingency Plan	Y – if applicable
	Information System Contingency Plan Test	Y – if applicable
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y – if applicable
	System Security Plan	Y
	Application Threat Modeling	Y – if applicable
FedRAMP Enterprise Cloud Application (-e Systems)	Configuration Management Plan	Y
	Disaster Recovery Plan	N
	Disaster Recovery Plan Test	N
	Incident Response Plan	Y

Boundary	Security Document	Required Y/N
	Incident Response Plan Test	Y
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Customer Responsibility Matrix	Y
	Application Threat Modeling	Y – if applicable
Facility	Configuration Management Plan	Y
	Disaster Recovery Plan	Y
	Disaster Recovery Plan Test	Y
	Incident Response Plan	Y
	Incident Response Plan Test	Y
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	N
Medical Devices	Configuration Management Plan	N
	Disaster Recovery Plan	N
	Disaster Recovery Plan Test	N
	Incident Response Plan	N
	Incident Response Plan Test	N
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y

Boundary	Security Document	Required Y/N
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	N
	Configuration Management Plan	N
Other Federal Agency (Non-eMASS Reciprocity)	Disaster Recovery Plan	N
	Disaster Recovery Plan Test	N
	Incident Response Plan	N
	Incident Response Plan Test	N
	Systems-Based BIA	N
	Information System Contingency Plan	N
	Information System Contingency Plan Test	N
	Interconnection Security Agreement/ Memorandum of Understanding	N
	Privacy Impact Assessment	N
	Privacy Threshold Analysis	N
	Risk Assessment Report	N
	System Security Plan	N
	Application Threat Modeling	N
	Configuration Management Plan	N
Platform	Disaster Recovery Plan	N
	Disaster Recovery Plan Test	N
	Incident Response Plan	N
	Incident Response Plan Test	N
	Systems-Based BIA	Y
	Information System Contingency Plan	Y
	Information System Contingency Plan Test	Y
	Interconnection Security Agreement/ Memorandum of Understanding	Y – if applicable
	Privacy Impact Assessment	Y – if required following PTA
	Privacy Threshold Analysis	Y
	Risk Assessment Report	Y
	System Security Plan	Y
	Application Threat Modeling	N

Boundary	Security Document	Required Y/N

7 Appendix C – Quick Reference Guide – Technical/Testing Requirements

Boundary	Technical / Testing Requirements	Required Y/N
Application hosted On-Premises/VA Network	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Software Composition Analysis	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Control Review	Y
Application hosted in Managed Service	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y
	Application Security Testing	Y – if applicable
	Software Composition Analysis	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Control Review	Y
Application hosted in FedRAMP cloud (VAEC)	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Software Composition Analysis	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Control Review	Y
Application hosted in FedRAMP cloud (Non-VAEC)	Nessus Scan	Y
	Database Scan	Y – if applicable
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	Y – if applicable
	Application Security Testing	Y – if applicable
	Software Composition Analysis	Y – if applicable
	Security Configuration Compliance Data	Y – if applicable
	Control Review	Y – if applicable

Boundary	Technical / Testing Requirements	Required Y/N
FedRAMP Enterprise Cloud Application (-e Systems)	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	Y – if applicable
	Software Composition Analysis	Y – if applicable
	Security Configuration Compliance Data	N
	Control Review	Y – if applicable
Facility	Nessus Scan	Y
	Database Scan	N
	Enterprise Discovery Scan	Y
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Software Composition Analysis	N
	Security Configuration Compliance Data	Y
	Control Review	Y
Medical Devices	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Software Composition Analysis	N
	Security Configuration Compliance Data	N
	Control Review	Y
Other Federal Agency (Non-eMASS Reciprocity)	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Software Composition Analysis	N
	Security Configuration Compliance Data	N
	Control Review	N
Platforms	Nessus Scan	N
	Database Scan	N
	Enterprise Discovery Scan	N
	Penetration Test/Application Assessment	N
	Application Security Testing	N
	Software Composition Analysis	N
	Security Configuration Compliance Data	N
	Control Review	Y

8 Appendix D – Common Control Providers/System of Record (SOR)

VA Tier1 System of Record (VA T1 SOR), VA Enterprise SOR (VA ENTSOR), and VA Area SOR are common control providers identified as a System of Record (SOR) in the eMASS GRC. A system of record (SOR) is an ISRS (information storage and retrieval system) that is the authoritative source for a particular data element in a system containing multiple sources of the same element. To ensure data integrity, there must be one, and only one, system of record for a given piece of information.

SORs themselves are not actual systems; therefore, they are approved for use by an Authorizing Official, but not Authorized to Operate. Assessment procedures provided by an SOR are assessed in accordance with VA guidance. For additional information on inheritance, refer to the 'Management' section of the eMASS User Guide.

8.1 VA T1SOR

T1SOR is a common control provider in eMASS. T1SOR provides common assessment procedure inheritance for systems within the FISMA Inventory. T1SOR documents test results and test evidence for the assessment procedures that are implemented on an agency-wide basis as directed by OIS policy or other OIS organizations where the implementation applies at a Department level.

Process Providers include:

- VA Policy,
- Information Security Risk Management (ISRM),
- Software Assurance (SwA),
- Security Assessment and Vulnerability Division (SAVD), and
- Cybersecurity Operations Center (CSOC).

Applications on the On-Premises/VA Network, IO Platforms, and Facilities may choose to inherit from T1SOR. Although T1SOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the T1SOR response appropriately describes the security controls in place for their system. As an example, the organization defined time periods cannot be made less stringent. There will be some CCIs that are hybrid, meaning the ISO can further define criteria (i.e., fields audited, devices inventoried, etc.). Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by T1SOR.

8.2 VA Enterprise SOR

VA Enterprise SOR (VA ENTSOR) is a common control provider in eMASS, providing enterprise related NIST SP 800-53 security controls to FISMA systems within the eMASS GRC tool. ENTSOR documents test results and test evidence for the assessment procedures that are implemented on an agency-wide basis by the Enterprise. Enterprise Providers include:

- Business Office,
- Cybersecurity Management,
- Change Management,
- NetsOps,
- Platform Support,
- Solutions Delivery,
- TPS, and
- Unified Communications Infrastructure Support.

Any NON-cloud-based systems on the VA Network may choose to inherit directly from ENTSOR. For applications in the VAEC, ENTSOR test results and evidence are provided via the VAEC provider. Instructions for VAEC AWS or Microsoft Azure can be found on the VAEC site.

Although ENTSOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the ENTSOR response appropriately describes the security controls in place for their system, for example, ENTSOR may not be appropriate for Managed Services or Other Government Agencies. Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by ENTSOR. See the Knowledge Service eMASS Page for additional guidance on inheritance.

8.3 VA Area SOR

VA Districts and Areas are organized into 5 Districts: North Atlantic, Southeast, Midwest, Continental, and Pacific. Within each district, sites such as Regional offices, medical centers, and cemeteries are organized and grouped by Area. The VA Area SOR addresses common processes that are utilized across all Areas.

VA Area SOR is a common control provider in eMASS. VA Area SOR provides common assessment procedure inheritance for VA Areas within the enterprise that utilize VA District Area processes. The VA Area SOR documents test results and test evidence for the assessment procedures implemented across all Areas within the VA.

At present, VA Area SOR includes common Area processes for Configuration Management; other security families will be examined for inclusion.

Areas may choose to inherit from VA Area SOR. Although VA Area SOR is available for inheritance by the listed boundaries within eMASS, it is the responsibility of the requesting system to review each assessment procedure and determine if the VA Area SOR response appropriately describes the security controls in place for their system. Depending on this outcome, System Stewards may choose to selectively inherit all or some of the CCIs provided for inheritance by VA Area SOR.

8.4 Cloud Service Provider SaaS and PaaS SOR

There are currently two additional SORs in eMASS: Microsoft Azure Government SaaS SOR and Microsoft Azure Government PaaS SOR.

In eMASS, the ATO for FedRAMP Microsoft Azure Government covers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, the inheritance is set to the least common denominator, IaaS, to ensure that systems do not receive inheritance not due to them.

These two SORs have been created to address the additional PaaS and SaaS control inheritance for PaaS and SaaS applications.

A PaaS system can inherit first from Microsoft Azure Government or VAEC Azure and then add on the PaaS SOR in order to obtain the additional PaaS inheritable controls. A SaaS system can inherit first from Microsoft Azure Government and then add on the SaaS SOR to obtain the additional SaaS inheritable controls. There are no SaaS applications in the VAEC, so the SaaS SOR is not applicable.

9 *Appendix E – New Authorizing Official (AO) Guidelines*

When an AO leaves the position or when a new AO starts, the systems under his/her purview require a review to continue the current ATO or grant a new ATO. The following steps should be used as guidance to ensure all systems receive an ATO review in a timely manner.

1. When an AO leaves or a new AO is recommended; the *Authorizing Official Appointments Memo* must be updated and signed by the CIO or PDAS prior to the new AO reviewing and providing risk decisions on any authorization packages.
2. The incoming AO to the authorization package will be required to review the package and determine if the system should continue with the current ATO or if a new full review, including a Risk Review, needs to be completed to provide a new ATO.
3. The new AO needs to use the eMASS RMF Step 5 workflow to show approval for the Authorization Boundary within 180 days of the previous AO leaving.

10 *Appendix F – Quick Reference Guide – Continuous Monitoring*

The following quick reference guide for continuous monitoring includes all technical testing and security documentation. Please refer to the specific boundary to verify if the security artifact is required for your system/application. If a major change occurs, all technical testing and security documentation must be re-completed regardless of the required frequency.

Technical Testing / Security Document	Required Frequency
Nessus Scan	Monthly
Database Scan	Annually
Enterprise Discovery Scan	Quarterly
Penetration Test/Application Assessment	Annually
Application Security Testing	Annually
Application Threat Modeling	Annually
Security Configuration Compliance Data	Quarterly
Control Assessment	TBD
Configuration Management Plan	Annually
Disaster Recovery Plan	Annually
Disaster Recovery Plan Test	Annually
Incident Response Plan	Annually
Incident Response Plan Test	Annually
Systems-Based BIA	Annually
Information System Contingency Plan	Annually
Information System Contingency Plan Test	Annually
Interconnection Security Agreement/ Memorandum of Understanding	Annually
Privacy Impact Assessment	Every 3 Years
Privacy Threshold Analysis	Annually
Risk Assessment Report	Annually
System Security Plan	Annually

11 *Appendix G – Type Authorization*

VA Handbook 6500 defines a type authorization as a method, "used to deploy identical copies of an information system or platform IT system. This allows a single security authorization package to be developed for an archetype (i.e., common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave."

Additionally, VA Handbook 6500, page 37, paragraph 8, a, iii explains that, "identical stand-alone information system and platform IT systems that have identical security control implementation and approved baseline are to be deployed to multiple locations may be type authorized."

Note: If the Type Authorization is changed in any way, it is no longer considered a Type Authorization. The originating organization has no responsibility to the receiving organization that is reusing the security testing or assessment results. The receiving organization will request a separate authorization.

11.1 Process

NIST SP 800-37 dictates that when using a Type Authorization, there must be a baseline system and location designated. A baseline will be developed for the archetype (i.e., common) version of a system. This includes hardware, software, or firmware components that are deployed to multiple locations for use in specified environments of operation (e.g., system installation and configuration requirements or operational security and privacy needs provided by the host organization at a specific location).

A Type Authorization is used in conjunction with authorized site-specific controls or with a facility authorization. A Type Authorization is issued by the authorizing official responsible for the development of the system and represents an authorization to operate at the site or facility where the system is deployed. The authorizing official who is responsible for the system at the site or facility accepts the risk of deploying the system and issues an authorization to use.

Authorizing Officials have the capability to set/update the Type Authorization status field within the appropriate Authorization workflow or Security Plan Approval workflow.

Note: A Type Authorization is appropriate when the system is deployed in a defined environment and is comprised of identical instances of system architecture, software, identical information types, functionally identical hardware, information that is processed in the same way, identical control implementations, or identical configurations.

11.2 Requirements

- The archetype system description must state that it is a 'Type Authorization' package and provide the locations of all the identical versions.
- The 'areas' where the archetype or identical version are located must include in the system description that they are hosting a Type Authorized System and list the eMASS ID.
- Only the archetype location will provide hosting facility controls. There is no need to inherit identical version hosting facility common controls.
- The IP addresses (i.e., inventory) of the archetype and identical copies will be documented in the archetype assets tab.
- The deployment location will provide the inventory list to be made 'as part of' the archetype assets.
- Select users/stages prior to the Authorizing Official can set/update a "Recommended Type Authorization" status field for a given system.

11.3 Responsibilities

11.3.1 Responsibilities of Originating Organization

It's the responsibility of the ISO and ISSO of the originating organization to complete the following:

- Maintain deployment locations of the system within originating organizational authorization tracking tool.
- Provide the security authorization package and deployment instructions (or access to it) including a current POA&M, to receiving organizations.
- Communicate all changes to the system during its lifecycle (i.e., different version) to receiving organizations.
- Notify receiving organizations of any new findings (e.g., new threats, discovered vulnerabilities, etc.) throughout the authorization life cycle.
- Gather requirements from potential leveraging organizations before developing the system, to ensure the widest use of a standardized configuration and avoid one-off modifications driving separate authorizations.
- Provide a point of contact (POC) to receiving organizations requesting information.
- Notify receiving organizations at least six months prior to any reauthorization events to ensure consideration of any input from receiving organizations.
- Notify receiving organizations of any plans that may affect their use of the system (e.g., decommissioning, version changes, etc.).
- Identify factors or conditions justifying termination of the MOU/MOA.
- Communicate and provide patches and updates in accordance with VA requirements and timelines.
- Maintain an up to date asset inventory (host/IP) as additional locations are deployed.
- Ensure assignment of an ISSO to maintain continuous monitoring, patch management, Information Assurance Vulnerability Management (IAVM) Program, operational orders, POA&Ms, annual reviews, and/or quarterly/monthly reviews of authorized systems to

include deployed locations. This includes the creation, management, tracking, and reporting of all POA&Ms.

- It’s the originating organizations responsibility to ensure the receiving organization is not deviating from the original baseline.

11.3.2 Responsibilities of Receiving Organization

It's the responsibility of the ISO and ISSO of the receiving organization to complete the following:

- Request Security Authorization Package and deployment instructions (or access to it), including a current POA&M, from the originating organization.
- Accept the originating organization AO's authorization decision.
- Deploy the system using configuration requirements in the security authorization package and deployment instructions.
- Ensuring deployed devices meet the archetype system configurations and are maintained and patched according to originating organization.
- Provide all inherited security controls, mitigations, or support functions required by the type of authorization.
- Obtain any necessary authorization to connect and operate the system within the organization's network.
- Provide a single POC to originating organizations providing information.
- Update necessary authorization tracking tools within the organization.
- Implement required patches and changes in accordance with Project Management (PM) guidance.
- Notify originating organizations of any new findings (e.g., new threats, discovered vulnerabilities) throughout the authorization life cycle.
- Implement mitigations in accordance with the originating Information Technology Security POA&M.
- The receiving organization's ISO/ISSO is responsible for ensuring their POA&Ms are remediated in a timely manner.
- Asset inventory (hosts/IPs) of deployed devices to be made part of archetype boundary at deployment.

It's the responsibility of the ISO and ISSO of the originating organization to complete the following:

-

Note: The responsibilities outlined above are not a comprehensive list. Organizations may need to add or augment these requirements. All agreements, additions, or changes must be agreed upon in writing by the originating and receiving organizations.

11.4 Change Management

All organizations must identify technical POCs as part of their MOU, MOA, and/or SLA to support the management and operation of the Type Authorized system. Organizations must communicate to the Program Manager, any event that may affect the security posture of the Type Authorized system or the installed environment. Agreements must include processes, timing, and notification requirements. Examples of events:

- Security incidents
- Disasters and other contingencies
- Material changes to system configuration
- Personnel changes in critical positions
- New user types (e.g., foreign nationals)
- Changes to the operating environment (e.g., facility was cleared for open storage but is no longer)
- Network the system is connected to is given a Denial of Authorization to Operate (DATO)

Note: Type Authorization systems can be utilized through Reciprocity and/or VA Reuse.

11.5 Identical Instance

The following requirements will be labeled with the location/document type and uploaded to the Artifacts tab of the Archetype system.

- Big Fix/SCCD Configuration baseline scan
- Nessus scan
- Ports and protocol verification (Red Seal)

The base location will be required to track all locations expected to be deployed. As locations are added, the required artifacts will be needed. The ISO/ISSO is responsible to ensure newly implemented systems meet the original configuration baseline using the requirements above.

11.6 Validation of Type Authorization

The identical copied system scans requirements above will be compared to the archetype results to ensure they are, in fact, identical. Any deviations from matching scans will be remediated immediately to ensure all locations are identical to the archetype baseline.

Note: For systems utilizing Type Authorization that will be part of the Office of Electronic Health Record Modernization (OEHRM) and are subject to DHA review, strict adherence to compliance with both VA and DHA policies will be considered.

12 *Appendix H – Provisional ATO Process*

The following process for a Provisional Authority to Operate (P-ATO) has been developed for systems that have an emergent need to go into production very quickly after procurement. Systems that qualify for the P-ATO Process include: Urgent turn around for systems that may have lost prior authorization boundary coverage, Presidential initiatives with the White House, and/or VA CIO visibility.

This process is not available for systems that were delayed due to ESECC, Project Special Forces intake, vendor access to the VA network, or not allowing for planning for all stage timelines of the RMF and eMASS process. eMASS registration must be followed according to **Section 3 Authorization Prerequisites and Registration of the Authorization Requirements SOP**. Detailed steps to register a new system can be found in the eMASS Implementation Guide under **'System Registration'**. **The qualification of the P-ATO process will be decided at the GRC Committee meeting**; ***however, systems with a H/H/H for C/I/A and utilize PII/PHI do not qualify for a P-ATO***.

The requirements to obtain an ATO remain the same for all impact levels of systems as in the body of this document; however, the P-ATO Process will allow for the Information System Owner to provide a shortened list of required artifacts. eMASS will be used for processing and documenting all Authorization Packages. **NOTE: A system may only undergo the P-ATO process for the initial approved stand-up. Any eMASS RMF step skipped during the P-ATO process must be completed after the initial Authorizing Official (AO) decision has been documented in eMASS.**

The P-ATO is expected to be for a very short term (approximately 180 days) to allow the system to follow compliance for being in production, which means the remaining RMF steps, Control and CCI details and test results, technical scans, required evidence, and security artifacts will need to be completed no later than 70 days prior to the decided Authorization Termination Date (ATD) of the granted P-ATO.

The eMASS Implementation User Guide can be used for additional instruction, but inexperienced stakeholders will need to seek out assistance from the DevSecOps team or Enterprise Security Architecture (ESA) Cloud team to ensure quick completion of the requirements set for a P-ATO.

Coordination between the system project team, Information System Owner (ISO), System Steward (SS), Information System Security Officer (ISSO), GRC Committee lead, OIS ISRM Risk Review team, Enterprise Security Architecture team, Authorizing Official Designated Representative (AODR), and Authorizing Official (AO) will be essential to complete the P-ATO Process successfully. Role descriptions of the primary stakeholders are located in VA Directive 6500.

Additional roles not found in VA Directive 6500 are outlined here:

System Project Team	Team comprising of the Project Manager and each stakeholder responsible for project implementation. Including ISO, SS and ISSO.
GRC Committee Lead	OIS ISRM Representative leading the committee and system registration in eMASS
OIS ISRM Risk Review Team	Team assigned to Risk Review (RMF Step 5.3) for full security review to advise of security posture to the AO for P-ATO Decision.
Enterprise Security Architecture Team	Team working with cloud (FedRAMP) systems

With proper notification and coordination between the teams listed above, a **P-ATO is expected to be granted within 13-16 business days of initiation of this process.**

12.1 Provisional ATO Process for systems hosted on the VA Network

This process is specific for applications that will be hosted in a VA owned and managed environment (non-cloud).

- The GRC Committee will process a system outside the normal weekly call, if necessary. Contact the VA OIS GRC Intake Reviewers to plan.
    - Once GRC Committee approves the system to undergo the P-ATO process, meeting minutes showing approval will be uploaded to the System's Artifacts Tab for proof and historical reference
- The assigned System Steward of the package will complete RMF Step 1 – Security Categorization and RMF Step 2 – Control Selection, to include addressing:
    1. Each of the system details tabs
    2. Nessus scans requests
        a. Scan Request must be completed and submitted prior to the P-ATO AO Determination. Upload CSOC Response acknowledging request that is received within 72 hours of request as proof of initiation.
        b. After 30 days the scan will be completed. System Stakeholders are then required to complete the scan upload, POA&M creation and other tasks as outlined in the Authorization Requirements SOP.
    3. Application Security Testing (Fortify)
        a. Application based systems must obtain the OIS-Licensed Fortify software from OIS Software Assurance and install.

b. Submit a request, upload the follow up verification that is received from the OIS Software Assurance team along with the ticket number as proof of initiation.
c. After the results have been received, the SS, ISO or ISSO will upload the validation report to eMASS and create a POA&M item (if needed).

4. Architecture diagram
5. List of Hardware/Software
6. Data flow diagram
    a. How does it go in and out of the system, where is the data coming from, where is it going, what is the use, is there encryption, etc.
    b. Ports, Protocols, and Services Template (PPS)
7. Privacy Threshold Analysis (PTA)

- Once RMF Step 1 and RMF Step 2 are complete, upload the required artifacts and RMF Step 5 can be started.
- In RMF Step 5.1, Finalize System POA&M, the SS/ISO will create one (1) POA&M per control family to document the Plan of Action to address the Control once the P-ATO is obtained.
- Below is the estimated timeline to complete each task in the P-ATO process.

Task	Responsibility	Expected Timeline
GRC Committee	GRC Committee	1 day
RMF Step 1 & 2	System Owner, SS, ISSO	5-7 business days
RMF Step 5	SS/ISO, Risk Review team, AODR, AO	7-8 business days

12.2 Provisional ATO Process for FedRAMP systems (-F/-VAF)

This process is specific for FedRAMP authorized boundaries. All FedRAMP CSP systems will have customer responsible controls identified as a requirement of the FedRAMP process. These controls, along with any additional VA required controls, will be captured in a separate authorization boundary from the FedRAMP boundary. This is the standard process for boundary assignment in eMASS. See section 4.4 for the standard process for FedRAMP systems.

- Appropriate ESECC process for data transfer from VA to the CSP is required.
- Access to the FedRAMP packages for the approved review teams will be expedited.
- The GRC Committee will process a system outside the normal weekly call, if necessary. Contact the VA OIS GRC Intake Reviewers to plan.
    - Once GRC Committee approves the system to undergo the P-ATO process, meeting minutes showing approval will be uploaded to the System's Artifacts Tab for proof and historical reference
- The assigned System Steward of the package will complete RMF Step 1 – Security Categorization and RMF Step 2 – Control Selection, to include addressing:
    1. Each of the system details tabs
    2. Nessus scans requests

a. Scan Request must be completed and submitted prior to the P-ATO AO Determination. Upload CSOC Response acknowledging request that is received within 72 hours of request as proof of initiation.
b. After 30 days the scan will be completed. System Stakeholders are then required to complete the scan upload, POA&M creation and other tasks as outlined in the Authorization Requirements SOP.

3. Application Security Testing (Fortify)
    a. Application based systems must obtain the OIS-Licensed Fortify software from OIS Software Assurance and install.
    b. Submit a request, upload the follow up verification that is received from the OIS Software Assurance team along with the ticket number as proof of initiation.
    c. After the results have been received, the SS, ISO or ISSO will upload the validation report to eMASS and create a POA&M item (if needed).
4. Architecture diagram
5. List of Hardware/Software
6. Data flow diagram
    a. How does it go in and out of the system, where is the data coming from, where is it going, what is the use, is there encryption, etc.
    b. Ports, Protocols, and Services Template (PPS)
7. Privacy Threshold Analysis (PTA)
8. ISA/MOU

- Once RMF Step 1 and RMF Step 2 are complete, upload the required artifacts and RMF Step 5 can be started.
- In RMF Step 5.1, Finalize System POA&M, the SS/ISO will create one (1) POA&M per control family to document the Plan of Action to address the Control once the P-ATO is obtained.
- The Enterprise Security Architecture team and Project Special Forces team will continue their standard review processes for FedRAMP packages and upload the review to the Artifacts tab within eMASS of the FedRAMP authorization boundary.
- The OIS ISRM Risk Review team will review the FedRAMP authorization package along with the Enterprise Security Architecture review and provide a risk summary in eMASS.
- Below is the estimated timeline to complete each task in the P-ATO process.

Task	Responsibility	Expected Timeline
GRC Committee	GRC Committee	1 day
RMF Step 1 & 2	System Owner, SS, ISSO	2-5 business days
RMF 5	SS/ISO, Risk Review team, AODR, AO	7-8 business days

Note: The FedRAMP package (-F or -VAF) and the enterprise package (-e) or single instance (-i) must be completed simultaneously in eMASS and submitted for Risk Review (RMF Step 5: Stage 3) at the same time.

12.3 Provisional ATO Process for SaaS solutions hosted in a non-FedRAMP cloud environment

The Enterprise Security Architecture team will be involved with the system stakeholders to ensure proper flow through the P-ATO Process.

- The GRC Committee will process a system outside the normal weekly call, if necessary. Contact the VA OIS GRC Intake Reviewers to plan.
    - Once GRC Committee approves the system to undergo the P-ATO process, meeting minutes showing approval will be uploaded to the System's Artifacts Tab for proof and historical reference
- The assigned System Steward of the package will complete RMF Step 1 – Security Categorization and RMF Step 2 – Control Selection, to include addressing:
    1. Each of the system details tabs
    2. Nessus scans requests
        a. Scan Request must be completed and submitted prior to the P-ATO AO Determination. Upload CSOC Response acknowledging request that is received within 72 hours of request as proof of initiation.
        b. After 30 days the scan will be completed. System Stakeholders are then required to complete the scan upload, POA&M creation and other tasks as outlined in the Authorization Requirements SOP.
    3. Application Security Testing (Fortify)
        a. Application based systems must obtain the OIS-Licensed Fortify software from OIS Software Assurance and install.
        b. Submit a request, upload the follow up verification that is received from the OIS Software Assurance team along with the ticket number as proof of initiation.
        c. After the results have been received, the SS, ISO or ISSO will upload the validation report to eMASS and create a POA&M item (if needed).
    4. Architecture diagram
    5. List of Hardware/Software
    6. Data flow diagram
        a. How does it go in and out of the system, where is the data coming from, where is it going, what is the use, is there encryption, etc.
        b. Ports, Protocols, and Services Template (PPS)
    7. Privacy Threshold Analysis (PTA)
    8. ISA/MOU
- Once RMF Step 1 and RMF Step 2 are complete, upload the required artifacts and RMF Step 5 can be started.

- In RMF Step 5.1, Finalize System POA&M, the SS/ISO will create one (1) POA&M per control family to document the Plan of Action to address the Control once the P-ATO is obtained.
- Below is the estimated timeline to complete each task in the P-ATO process.

Task	Responsibility	Expected Timeline
GRC Committee	GRC Committee	1 day
RMF Step 1 & 2	System Owner, SS, ISSO	5-7 business days
RMF Step 5	SS/ISO, Risk Review team, AODR, AO	7-8 business days

Note: The Enterprise Security Architecture team will be involved to perform an in-depth risk review of the CSP environment, application, and associated current security configurations upon issuance of initial ATO.

12.4 Provisional ATO Process for Managed Service's (Non-Cloud)

This process is specific for applications that will be hosted in a non-VA owned and managed environment (non-cloud).

- The GRC Committee will process a system outside the normal weekly call, if necessary. Contact the VA OIS GRC Intake Reviewers to plan.
    - Once GRC Committee approves the system to undergo the P-ATO process, meeting minutes showing approval will be uploaded to the System's Artifacts Tab for proof and historical reference
- The assigned System Steward of the package will complete RMF Step 1 – Security Categorization and RMF Step 2 – Control Selection, to include addressing:
    1. Each of the system details tabs
    2. Nessus scans requests
        a. Scan Request must be completed and submitted prior to the P-ATO AO Determination. Upload CSOC Response acknowledging request that is received within 72 hours of request as proof of initiation.
        b. After 30 days the scan will be completed. System Stakeholders are then required to complete the scan upload, POA&M creation and other tasks as outlined in the Authorization Requirements SOP.
    3. Application Security Testing (Fortify)
        a. Application based systems must obtain the OIS-Licensed Fortify software from OIS Software Assurance and install.
        b. Submit a request, upload the follow up verification that is received from the OIS Software Assurance team along with the ticket number as proof of initiation.
        c. After the results have been received, the SS, ISO or ISSO will upload the validation report to eMASS and create a POA&M item (if needed).
    4. Architecture diagram
    5. List of Hardware/Software

6. Data flow diagram
    c. How does it go in and out of the system, where is the data coming from, where is it going, what is the use, is there encryption, etc.
    d. Ports, Protocols, and Services Template (PPS)
7. Privacy Threshold Analysis (PTA)
8. ISA/MOU

- Once RMF Step 1 and RMF Step 2 are complete, upload the required artifacts and RMF Step 5 can be started.
- In RMF Step 5.1, Finalize System POA&M, the SS/ISO will create one (1) POA&M per control family to document the Plan of Action to address the Control once the P-ATO is obtained.
- Below is the estimated timeline to complete each task in the P-ATO process.

Task	Responsibility	Expected Timeline
GRC Committee	GRC Committee	1 day
RMF Step 1 & 2	System Owner, SS, ISSO	5-7 business days
RMF Step 5	SS/ISO, Risk Review team, AODR, AO	7-8 business days

12.5 Provisional ATO Process for Systems with Minor Applications

This process is specific for any applications that are determined to include Minor Application(s). The Major System must follow appropriate guidance from sections 1.1 – 1.4.

The Minor Application will also go through the VA OIS GRC Intake Reviewers for proper determination and alignment with the Major System. Once approved as a Minor:

- The assigned System Steward of the package will complete:
    1. Each of the system details tabs
    2. Association to the Major System
    3. Architecture diagram
    4. List of Hardware/Software
    5. Data flow diagram
        e. How does it go in and out of the system, where is the data coming from, where is it going, what is the use, is there encryption, etc.
        f. Ports, Protocols, and Services Template (PPS)
    6. Privacy Threshold Analysis (PTA)
- As the System Steward completes the above tasks including the upload of the required artifacts the workflow can be progressed forward to the AO to be presented at the same time as the Major System.
    - *NOTE: Steps cannot be passed in here, ensure proper comments are included when progressing the package so the next Stakeholders have an understanding why this must go to the AO with the Major System.*

Once the P-ATO has been granted to the Major System and the Minor is Assessed, the stakeholders of both the Major System and the Minor Application must revisit the

Minor Application Assessment Requirements Standard Operating Procedure following the full process.