Office of Information
and Technology

Assess Only Requirements

Standard Operating Procedures

January 30, 2025 | Version 3.2 | U.S. Department of Veterans Affairs, Office of Information and Technology

FOR INTERNAL USE ONLY

Table of Contents

Figures

Tables

Table 1: Version History

Version	Date	Author	Change Summary
1.0	10/30/2020	OIT OIS	Initial Version
1.1	12/11/2020	OIT OIS	Incorporated requested changes
1.2	3/5/2021	OIT OIS	Updated the Pre-Registration Process and included Major Application System Steward
1.3	3/9/2021	OIT OIS	Updated General Support System to IS Major Application, IS Enclave, and Platform IT System
1.4	5/18/2021	OIT OIS	Incorporated FISMA Reporting guidance
2.0	10/29/2021	OIT OIS	Modified control set information to include the use of Privacy Overlay to add privacy controls to Minor Applications. Updated the System Type
3.0	12/19/2023	OIT OIS	Overhaul of document to match newly implemented Assess Only process.
3.1	2/12/2024	OIT OIS	Updated section 4.7, Risk Review to reflect 70 days. Updated Appendix E, Documentation Requirements to include Network Topology Diagram, Ports, Protocols, and Services, Risk Assessment Report, and System Security Plan as required documents for Assess Only Systems. Added a note to Appendix E identifying artifacts that must be provided to the supporting Platform, Enclave, or Information System.
3.2	1/30/2025	OIT OIS	508 compliance updates Updated last sentence under *Assess Only Prerequisites & Registration* to read: "The Assess Only System Steward / Information System Owner (ISO) and the Assess and Authorize System Steward / ISO are responsible for completing the Pre-Registration process in the Unified System Registry Portal." Updated *Information Types and Impact Levels* section for the *USR Working Group* steps to align with USR portal screenshots. Replaced link for *Configuration Management Plan* with the link on Knowledge Service. (Knowledge Service>Templates>FISMA>CMP).

			Added AO awareness of newly approved Assess Only systems. Added to *Appendix A – Glossary* the Business Impact Analysis (BIA) and Information System Contingency Plan (ISCP) Lite definitions. Added to *Appendix B – Assess Only Control Sets* CP-2-Contingency Plan and CP-9 System Backups to the chart. Updated applicable ***Continuous Monitoring*** sections to clarify when to review and update documentation throughout the SOP.

Introduction

The Standard Operating Procedure (SOP) provides guidelines and requirements for information systems using the Assess Only Registration Type in Enterprise Mission Assurance Support Service (eMASS), VA's Governance, Risk, and Compliance (GRC) tool.

Purpose

The purpose of the procedures will detail specific requirements related to security documentation, GRC system registration, and technical scanning requirements. Refer to Appendix A, terms, definitions, and acronyms used throughout the SOP.

Scope

The procedures outlined in this document apply to information systems and applications that reside within and receive many of their security controls from a supporting Platform, Enclave, or Information System but require attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application or system. Assess Only Criteria:

- Cannot be a standalone application/system;
- Receives majority of its security from the supporting Platform, Enclave, or Information System;
- Federal Information Processing Standard (FIPS) 199 Security Categorization of Low or Moderate;
- Must be associated in eMASS to a supporting Platform, Enclave, or Information System.

Information systems and applications may include, but are not limited to Minor Applications, Special Purpose Systems (SPS), Medical Devices, and Research Systems.

Process Flow Diagram

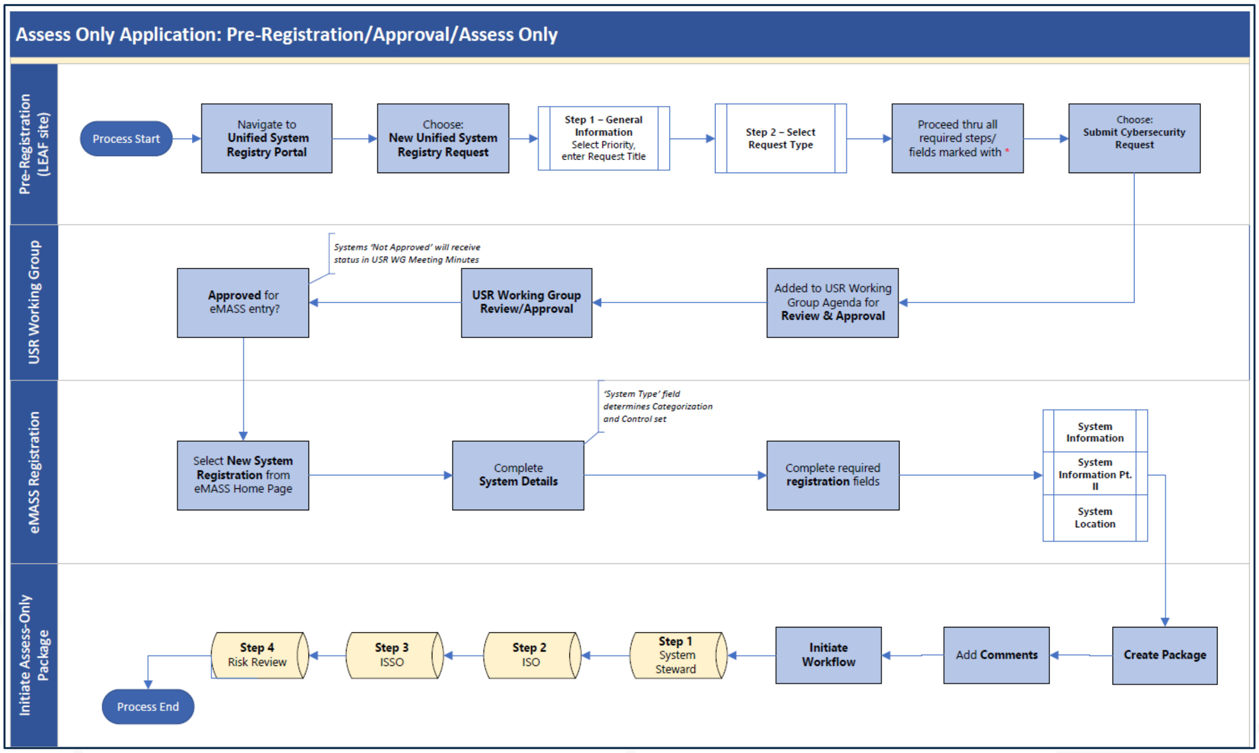

Assess Only Application: Pre-Registration/Approval/Assess Only
Pre-Registration (LEAF site)
Process Start
Navigate to Unified System Registry Portal
Choose: New Unified System Registry Request
Step 1 – General Information Select Priority, enter Request Title
Step 2 – Select Request Type
Proceed thru all required steps/ fields marked with *
Choose: Submit Cybersecurity Request
USR Working Group
Added to USR Working Group Agenda for Review & Approval
USR Working Group Review/Approval
Approved for eMASS entry?
Systems 'Not Approved' will receive status in USR WG Meeting Minutes
eMASS Registration
Select New System Registration from eMASS Home Page
Complete System Details
'System Type' field determines Categorization and Control set
Complete required registration fields
System Information
System Information Pt. II
System Location
Initiate Assess-Only Package
Create Package
Add Comments
Initiate Workflow
Step 1 System Steward
Step 2 ISO
Step 3 ISSO
Step 4 Risk Review
Process End

Figure 1:Process Flow Diagram Screenshot

Assess Only Prerequisites and Registration

Systems using the Assess Only Registration Type must be associated to a supporting Platform, Enclave, or Information System. Communication between the Assess and Authorize System Steward and Assess Only System Steward must occur prior to system registration, as both parties will have to provide detailed information to support Registration. .

The **Assess Only** System Steward / Information System Owner (ISO) and the **Assess and Authorize** System Steward / ISO are responsible for completing the Pre-Registration process in the Unified System Registry Portal.

The prerequisites in this section apply to all information systems requesting approval to use the Assess Only Registration Type in eMASS. These systems must be entered into eMASS and be evaluated for potential risk to the VA. Assess Only packages/artifacts, in addition to any other application/device information, should not leave the VA network.

For any questions regarding system registration, please email the VA OIS USR Taskforce VAOITUSRTaskforce@va.gov for additional guidance.

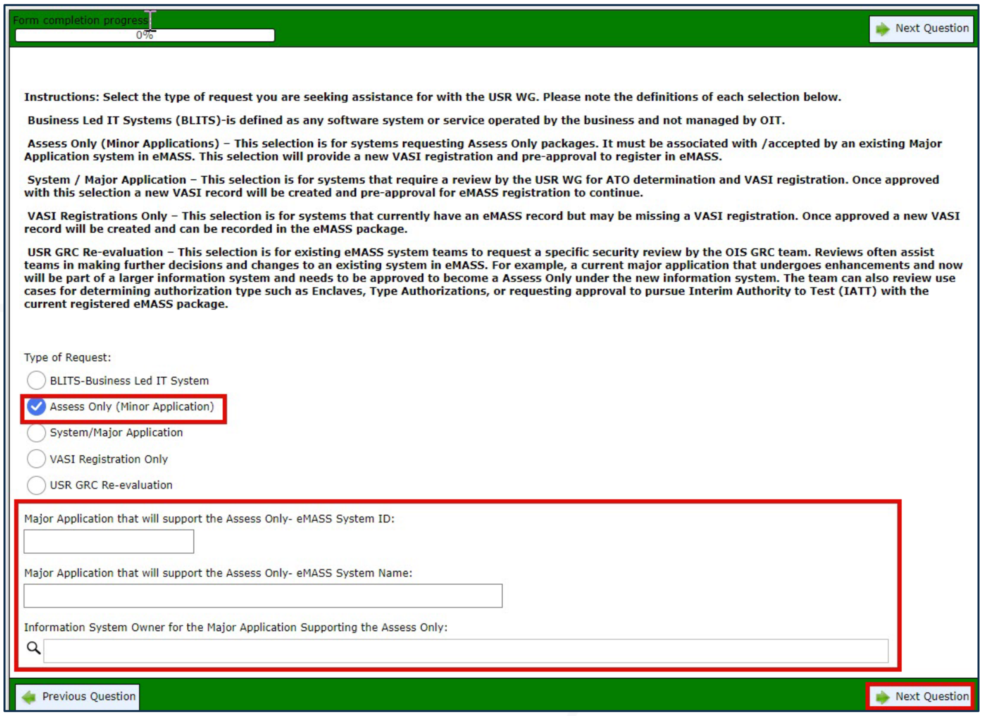
Information Types and Impact Levels

In alignment with NIST 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* are the mandatory standards used by all federal agencies to categorize information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to impact. Systems registering as Assess Only must have a FIPS 199 security category of Low or Moderate. If the information system is categorized as High, the system must be registered as a Major Application using the Assess and Authorize Registration Type. However, if the Assess Only system resides on a system that does not have adequate boundary protection, the Assess Only system must implement the minimum baseline controls required by the host or interconnected system.

Note: *Control selection and overlays may change for the Major Application if the Assess Only system introduces new, unrecognized, risks not covered under the existing ATO.*

USR Working Group Preregistration Steps:

1. Initiate a new Unified System Registry (USR) Intake form by navigating to the Unified System Registry Portal .
2. Select **[New Request]**; the preregistration form will generate once selected.
3. STEP 1-General Information:
    a. Under the **[Priority category]**, choose from drop-down list; Emergency or Normal
    b. Under the **[System Name]**, enter *System Name*.
4. Step 2-Select **[Select type of request]**and **[Select [Click here to Proceed]**
5. Select **[Next Question]** after reading the information presented.
6. Select [**Assess Only]** (Minor Application)



Instructions: Select the type of request you are seeking assistance for with the USR WG. Please note the definitions of each selection below.

Business Led IT Systems (BLITS)-is defined as any software system or service operated by the business and not managed by OIT.

Assess Only (Minor Applications) – This selection is for systems requesting Assess Only packages. It must be associated with /accepted by an existing Major Application system in eMASS. This selection will provide a new VASI registration and pre-approval to register in eMASS.

System / Major Application – This selection is for systems that require a review by the USR WG for ATO determination and VASI registration. Once approved with this selection a new VASI record will be created and pre-approval for eMASS registration to continue.

VASI Registrations Only – This selection is for systems that currently have an eMASS record but may be missing a VASI registration. Once approved a new VASI record will be created and can be recorded in the eMASS package.

USR GRC Re-evaluation – This selection is for existing eMASS system teams to request a specific security review by the OIS GRC team. Reviews often assist teams in making further decisions and changes to an existing system in eMASS. For example, a current major application that undergoes enhancements and now will be part of a larger information system and needs to be approved to become a Assess Only under the new information system. The team can also review use cases for determining authorization type such as Enclaves, Type Authorizations, or requesting approval to pursue Interim Authority to Test (IATT) with the current registered eMASS package.

Type of Request:

○ BLITS-Business Led IT System

● Assess Only (Minor Application)

○ System/Major Application

○ VASI Registration Only

○ USR GRC Re-evaluation

Major Application that will support the Assess Only- eMASS System ID:

Major Application that will support the Assess Only- eMASS System Name:

Information System Owner for the Major Application Supporting the Assess Only:

Figure 2: ISRM Request Screenshot

7. Complete the information requested regarding the supporting Platform, Enclave or Information System already registered in eMASS, then select **[Next Question]** to proceed.

Note: *Required fields in the Roles, System Overview, and Primary System Hosting Location sections contain a * and must be populated with information pertinent to the Assess Only application. If detailed information is not available, or is required but does not apply, please enter N/A or 00000 in the fields.*

8. Once the remaining questions have been addressed, select **[Submit]** in the upper left corner to submit the Intake form to the Unified System Registry Working Group (USR WG) for consideration and review.
    a. Your request will be reviewed by an intake team for assignment of a new Information System Security Officer (ISSO) and the USR WG will include the new information system request for discussion on the weekly meeting agenda, scheduled Tuesdays at 10:00am EST.

b. During the meeting, the USR WG will approve or deny the information system or request additional information before a decision.
c. Once the USR WG approves the new information system request and an eMASS administrator approves the system, an email is automatically generated in eMASS to notify the ISO or delegate of the approval.
d. The System Owner or delegate must then complete the eMASS system registration. Access to eMASS is required to register a new system.

eMASS Registration

The eMASS registration guidance and the required security documents are listed below.

Assess Only Registration Steps:

The Assess Only registration process in eMASS consists of five steps. To begin the New System Registration process, hover over *Authorization* and select **[New System Registration]** from the eMASS *Home* page and complete each step below:

1. *Step 1 – System Information;*
   After selecting **[New System Registration]**, eMASS displays *Step 1 – System Information*. All fields highlighted in red with a red asterisk require input before proceeding. It is important to select "Assess Only" from the "Registration Type" field at the top of the screen. Once all required fields are completed for a section, select**[Save]** at the bottom of the screen.
2. *Step 2 – System Information Pt. II*;
3. *Step 3 – System Location;*
4. *Step 4 – Roles* as applicable.
   Step 5 – Review & Submit. Ensure all data is accurate then at the bottom of the tab, select **[Submit System].**

Note: *Additional details and step-by-step guidelines are available in the eMASS Implementation Guide.*

Once the system is approved, the Assess Only System Steward must complete the data entry process in eMASS. Within eMASS, all required fields are denoted with a red asterisk (*****). In some cases, fields that provide valuable information in the Assess Only registration process may not be identified as required but must be completed.

A response is required in the fields listed below:

Table 2: eMASS Fields

System Registration Location	Field
System Information	Geographical Association
	VA System Type
System Information Pt. II	Personally Identifiable Information (PII)
	Protected Health Information (PHI)
	Data Hosting
	Encryption of Data at Rest
	Segmentation
	Cloud Computing (Note, the following four fields are required if answered Yes)
	CSP FedRAMP Name
	CSP FedRAMP Status
	Cloud FIPS 199 Rating
	Cloud Deployment Model
	Service Models (Select appropriate service model Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Other. If Other is selected, a detailed description is required.
System Location	System Location
	Baseline Location
	Physical Location(s)

Assess Only Requirements-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. If available, template locations for the applicable security artifacts/documents are provided.

All artifacts uploaded into the Artifacts tab or generated through eMASS as part of the assessment package are assumed to have been reviewed/approved by the ISO and/or ISSO when the eMASS workflow is progressed. If the ISO and/or ISSO do not approve an Artifact, the workflow must be returned for rework until approval is received. Contact your ISSO with questions on how to complete the documentation.

Note: *To add applicable security documentation, navigate to the system's Artifacts module. To add a new artifact, select **[Add Artifact]**. On the Artifact Information screen, fill out all applicable information. Further details and step-by-step details about artifacts is available in the eMASS Implementation Guide.*

Business Associate Agreement (BAA)

The Business Associate Agreement (BAA) is mandated by the Health Insurance Portability & Accountability Act and is required if the system provides a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of the VHA and is associated with Protected Health Information (PHI). If the supporting Platform, Enclave, or Information System does not have a BAA that covers the PHI, the Assess Only system will have to complete a BAA.

Continuous Monitoring Requirement

Privacy Officers review local BAA every 2 (two) years from the latest signature date to determine applicability.

The VHA Data Portal provides additional information.

Business Impact Analysis (BIA)

The BIA characterizes the impacts and consequences of a disruption to the system components, supported mission/business processes, and interdependencies. Systems using the Assess Only workflow are required to complete an independent BIA which must also be listed within the supporting Platform, Enclave, or Information Systems BIA.

The BIA should include Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Work Recovery Time (WRT), if known. It is critical that Assess Only systems are considered in the supporting Platform, Enclave, or Information Systems planning to account for potential impacts during an outage and to ensure proper restart of all applications.

Note: *The RTO of the Assess Only system cannot be less than the* supporting Platform, Enclave, or Information System *RTO. ISCP Coordinators cannot complete an ISCP that meets the necessary standards without first completing a BIA.*

The ISO, System Steward, or designee should work with the ISSO, in coordination with the entities identified in the NIST SP 800-34, to complete the BIA using the latest BIA Template and BIA SOP guidance.

Continuous Monitoring Requirement

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

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. The CMP template is available in the FISMA Artifacts menu in the "***Templates"*** section of the Knowledge Service site or 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.

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

Hardware/Software Baseline (HW/SW)

Assess Only systems must complete the Hardware and Software Inventory Import process to ensure all IP Addressable Assets are properly added to their assessment boundary in eMASS.

> **Note:** *All lower environment assets must be inventoried if they are connected to the VA Network. Assets should ONLY be captured in the Assess Only Hardware/Software Inventory if usage and control is held solely by that system. This ensures all IP Addressable Assets are properly added to the responsible authorization boundary in eMASS.*

The FISMA Containerization Asset to Boundary (FCAB) Team aligns all information systems to their FISMA ID. All assets attached to the network are tracked through FCAB, independent of the Registration Type, Assess and Authorize or Assess Only.

- Please refer to *FISMA Containerization Asset to Boundary (FCAB) Important Documents*, on VAs Knowledge Service site for additional guidance such as FAQ's, Charter, and Bulletins.

- 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.

Continuous Monitoring Requirement

The Hardware and Software Inventory must be reviewed on an annual basis or updated when a significant/major change to the system occurs.

ISA/MOU (direct connection with external organization)

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 before an external connection is established. An ISA/MOU must be provided for all external interconnections. 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.

Continuous Monitoring Requirement

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

Information System Contingency Plan (ISCP) - Lite

The ISCP – Lite characterizes interim measures to recover information system services after a disruption, including measures for relocation of information systems and service to an alternate site. Systems using the Assess Only workflow are required to complete an independent ISCP - Lite. The Assess Only system must be listed within the supporting Platform, Enclave, or Information System ISCP.

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed, personnel have been notified, and appropriate teams have been mobilized.

Note: *The Assess Only ISCP process should "pick-up" where the* supporting Platform, Enclave, or Information System *recovery leaves off. The ISCP Coordinator is responsible for notifying and updating the identified personnel with the latest version of this ISCP.*

The ISO, System Steward, or designee should work with the ISSO, in coordination with the entities identified in NIST SP 800-34, to complete the ISCP – Lite using the latest ISCP – Lite Template in the FISMA Artifacts menu in the "***Templates"*** section of the Knowledge Service site.

Continuous Monitoring Requirement

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

Network Topology Diagram

Topology diagrams should depict all hardware within the assessment boundary. The applications and software installed on each hardware or appliance can be identified on the inventory tab. Each port in use needs to be listed at the top of the topology diagram and should depict the traffic flow. The diagram will also need to show if the port data flow direction is inbound, outbound, or bi-directional.

Continuous Monitoring Requirement

The Network Topology Diagram and confirmation of the security assessment boundary, to include all devices and supporting software architecture, should be added to eMASS in the appropriate locations and reviewed annually or updated when a significant/major change in the system occurs.

Ports and Protocols List

The identification of necessary ports, protocols, and services influence the design of the system, system component, or system services and helps avoid or minimize the use of ports, protocols, or services that pose unnecessarily high risks. Each port documented in the diagram must be accounted for in the System's Ports, Protocols, and Services. To manage a System's Ports, Protocols, and Services (PPS) within eMASS, select the **[Assets]** tab and then the **[Ports/Protocols]** sub-tab.

Continuous Monitoring Requirement

VA has defined the frequency to update and review of ports, protocols, and services as quarterly, in alignment with CM-7(1). The system must maintain an audit trail of the reviews.

Refer to the eMASS Implementation Guide for additional details.

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. If a PIA is required as an outcome of the PTA review completed by the Privacy Services Office, a PIA must be completed. The ISO or System Steward is required to upload the PTA/PIA to the Artifacts tab within eMASS.

The ISO will initiate and coordinate the PTA annually (or earlier if there is a major system change) with the assistance of the ISSO and forward to the assigned Privacy Officer for review. Upon completion of an initial review, the Privacy Officer will forward a copy to the VA PIA Support Mail Group for final review. The PTA template is located in the ***Other Helpful Links*** section on the Knowledge Service eMASS page.

Systems using the Assess Only workflow will be included, by name, in the supporting Platform, Enclave, or Information System Privacy Impact Assessment (PIA). The PIA will be uploaded in the Artifacts folder of the Assess Only system. An updated PIA will be required earlier if there are major updates or changes to the systems.

- The PTA/PIA templates and completion processes can be found at Privacy Compliance PTA, and on Privacy Compliance PIA sites.

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.

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.*

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.

Continuous Monitoring Requirement

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

Security Impact Analysis (SIA)

A Security Impact Analysis (SIA) is a tool utilized to determine the extent to which changes to the system could affect the security state of the system. The SIA results will highlight areas where a proposed system change could create additional security requirements necessary to minimize the impact of the proposed system change.

A SIA worksheet template aids in the collection of system information detailing the effort and potential security consequences that must be considered. The Assess Only System Steward/or ISO is responsible for completing the Assess Only Prerequisites and Registration process prior to any SIA submissions.

Note: *Major Changes to the* supporting Platform, Enclave, or Information System *and/or the Assess Only system utilize the same SIA template. The same template can be used for both system types, since the Assess Only System is a dependent system, application or function of the Platform, Enclave, or Information System that requires comprehensive security implementation details and compliance.*

The following documents related to the Security Impact Analysis (SIA) may be found on the Knowledge Service Resources and Important Links page (Templates/Miscellaneous Templates/Security Impact Analysis (SIA)):

- Security Impact Analysis - FAQ's
- Security Impact Analysis (SIA) - Template

Details for completing the Major Change Form may be found within the Authorization Requirements SOP in the eMASS Document Library.

Status of Requirements (SoR)

Assess Only systems will complete the SoR and upload the completed document in the Artifacts section. The same SoR will be provided to the supporting Platform, Enclave, or Information System in support of their authorization package to ensure Assess Only systems are reviewed.

Be sure to include the eMASS ID of the Assess Only system in the *System Name in eMASS* field in the SoR.

Refer to the Status of Security Documents and Technical/Testing Requirements for additional guidance.

System Security Plan (SSP)

The SSP provides an overview of security requirements for Information Systems (IS) and describes controls in place, or planned for implementation, to provide a level of security appropriate for the information processed. The SSP includes user responsibilities, roles and limitations, and general security procedures for users and security personnel.

In addition to the SSP generated in the Reports tab, the System Steward should upload the CCI export to the Artifacts tab within eMASS to be considered an appendix of the SSP. The ISO and ISSO must review the uploaded SSP. Progression of the Assess Only workflow constitutes approval of all information and supporting artifacts, including the SSP.

Refer to the eMASS Implementation Guide for additional details.

Continuous Monitoring Requirement

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

Technical Scans/Requirements

Assess Only systems have identical scanning requirements as Major Applications. Depending on the Assess Only system and components, one or all scans may be required:

Refer to the Authorization Requirements for eMASS Standard Operating Procedure for detailed information.

Database Scan

The Assess Only system must request a database scan if it hosts a dedicated database to store and process system information.

Penetration Test/Application Assessment

A Penetration Test or full Application Assessment, Mobile Application Security Assessment (MASA) and the Web Application Security Assessment (WASA) must be performed if the Assess Only Application is an Internet facing system, processes, uses, or hosts PII and/or financial data. If the Assess Only Application utilizes multiple servers, then a WASA and Penetration Test are required, regardless of the FIPS categorization. If the Internet facing application only uses one server, then only a WASA is required.

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.

Refer to the Authorization Requirements for eMASS Standard Operating Procedure for detailed information.

Continuous Monitoring

Successful completion of OIS Software Assurance scans of libraries and frameworks is additionally 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.

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.

Refer to the Authorization Requirements Standard Operating Procedure for detailed information.

Continuous Monitoring Requirement

Security Configuration Compliance Data must be pulled in accordance with the guidance above on a quarterly basis, or updated 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.

Application Security Testing

Application Security Testing is required for custom-developed VA applications during the development or maintenance phases of a VA application. Successful completion of the software assurance validation of developer-performed scans 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.

Continuous Monitoring Requirement

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.

Application Threat Modeling

Application Threat Modeling is required for all custom developed systems/applications. Application Threat Modeling is not required for VistA systems.

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

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).

Continuous Monitoring Requirement

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

Assess Only - RMF Workflow

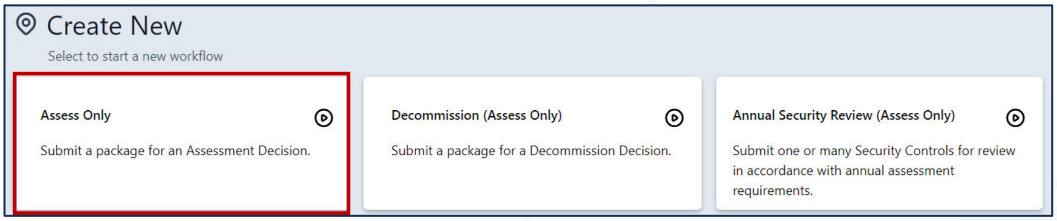
Initiate Assess Only Workflow

The Assess Only workflow does not display RMF Steps systematically in the same manner as the Assess and Authorize workflow. However, the tasks within the RMF Steps are still required for systems using this workflow.

Note: *RMF Steps 1-3 are required for systems using the Assess workflow.*

To initiate new workflow:

1. The System Steward or ISO initiates the Assess Only workflow by navigating to the system on which workflow will be submitted. Select **[Active Workflow Listing]** located within the Workflows main tab.
2. Select **[Assess Only]** to initiate package workflow.



Create New

Select to start a new workflow

Assess Only

Submit a package for an Assessment Decision.

Decommission (Assess Only)

Submit a package for a Decommission Decision.

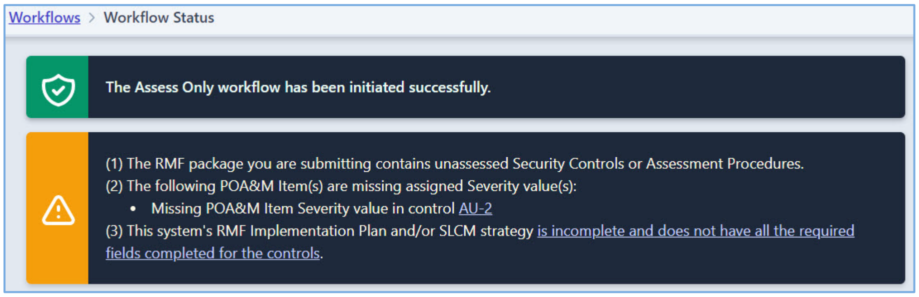
Annual Security Review (Assess Only)

Submit one or many Security Controls for review in accordance with annual assessment requirements.

Figure 3: Creating New Assess Only Workflow Screenshot

3. When the user initiates a new Assess Only package/workflow, a Package Name is required.

   The Package Name should utilize the following format: AssessOnlySystemNameORAcronym_MMYYYY.
4. Select **[Initiate Workflow]**.
5. After initiating the Assess Only workflow, the warning banners will appear. The cautionary warning banner can be ignored, as the workflow was just initiated. This warning banner will disappear once the security controls are reviewed and POA&Ms are developed.



The Assess Only workflow has been initiated successfully.

(1) The RMF package you are submitting contains unassessed Security Controls or Assessment Procedures.
(2) The following POA&M Item(s) are missing assigned Severity value(s):

- Missing POA&M Item Severity value in control AU-2

(3) This system's RMF Implementation Plan and/or SLCM strategy is incomplete and does not have all the required fields completed for the controls.

Figure 4: Assess Only Warning Banner Screenshot

System Details & Categorization

Once the Assess Only workflow has been initiated, System Stewards will complete all tasks normally incorporated within RMF Step 1: Complete System Details and Categorize System.

Refer to eMASS implementation User Guide for specific procedures and guidelines.

System Steward completes following in eMASS.

1. Upon logging into eMASS, the System Steward will see a new workload task on the eMASS home page. Select the hyperlink associated to the Assess Only system in the Task Description to open Workload Tasks.
2. Navigate to the “Details” and select **[Edit]** to complete Assess Only details:
   a. Complete and document system information.
   b. Select **[Save]**.

Note: *All systems using the Assess Only Registration Type are* *<u>NOT</u>* *FISMA Reportable systems but are required to complete the fields within the FISMA tab. The FISMA Reporting field in the FISMA section must reflect* *<u>NO</u>*. *Remaining fields within the FISMA tab must be populated. Assess Only Systems will be included in the FISMA reporting requirements with the supporting Platform, Enclave, or Information System.*

3. Navigate to “Categorization” area in top menu:
   a. Define information types.
   b. Select applicable Confidentiality/Integrity/Availability.
   c. Select **[Save].**

Refer to eMASS implementation User Guide for specific procedures and guidelines.

Security Controls & Implementation Plan

The Assess Only control set is assigned to the system based on the "System Type" selection during the registration process. Appendix B, Assess Only Control Sets, identifies security controls assigned to each system type. The selected controls are designed to determine the sufficiency and effectiveness of a controlled feature or safeguard. The flexibility to manually add controls that are not part of the Low or Moderate control sets is available.

System Steward completes following in eMASS

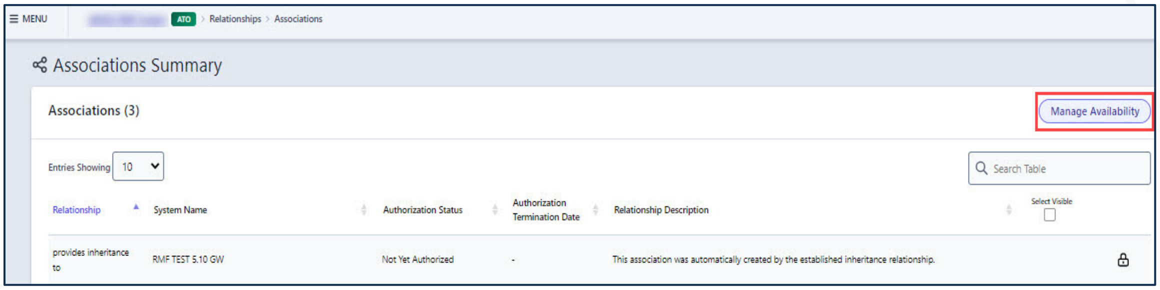
1. Navigate to "Controls" area in top menu:
2. Taylor Security Control Baseline and Apply Overlays:
    a. Add additional controls or enhancements, as necessary, to supplement the Control baseline.
    b. Complete relevant Overlay Questionnaire to determine applicability to system.
3. Navigate to "Implementation Plan" in top menu:
    a. Establish associations and inheritance for common/hybrid/inherited controls.
    b. Complete Implementation Plan.

Step-by-step instructions can be found in the "Add Additional Controls" section of the eMASS Implementation Guide. Refer to Assess Only Control Set to view controls applied to each baseline.

Establishing Association

Assess Only systems establish a two-way relationship with the supporting Platform, Enclave, or Information System through the Associations tab. Association relationships are relegated to the system level and do not exchange Control information. The supporting Platform, Enclave, or Information System will initiate the Association process by selecting the Organization that contains the Assess Only system.

1. Navigate to the *eMASS Menu*, select **[Associations]** under *Relationship* heading.
2. Select **[Manage Availability**]:



Associations Summary

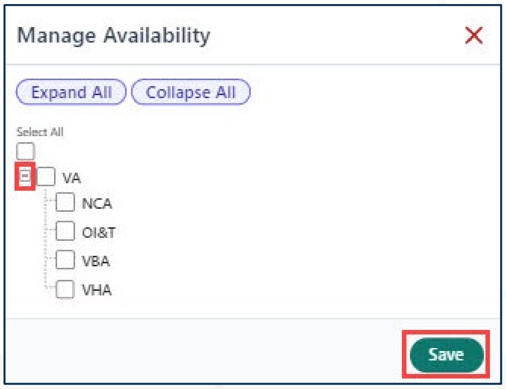
Associations (3)

Entries Showing 10

Relationship	System Name	Authorization Status	Authorization Termination Date	Relationship Description	Select Visible □
provides inheritance to	RMF TEST 5.10 GW	Not Yet Authorized	-	This association was automatically created by the established inheritance relationship.	

Figure 5: Managing Availability for Assess Only Application Screenshot

3. Select the Organization aligned with the Assess Only Application.
4. Select the **[+]** sign to expand the collapsed Organizations.
5. Select **[Save]**.


Manage Availability

Select All

□

⊟ □ VA

□ NCA

□ OI&T

□ VBA

□ VHA

Figure 6: Selecting Assess Only Application Organization Screenshot

6. A notification will appear, confirming that the organization availability was successful:

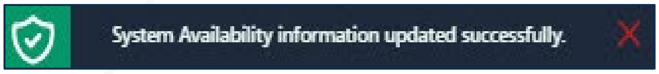

System Availability information updated successfully.

Figure 7: Manage Availability confirmation Screenshot

7. From the *Associations Summary* page, scroll down and select **[Add New Association]**.

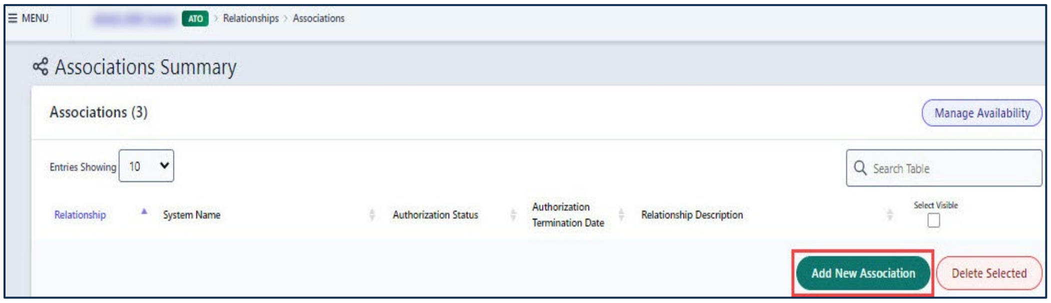
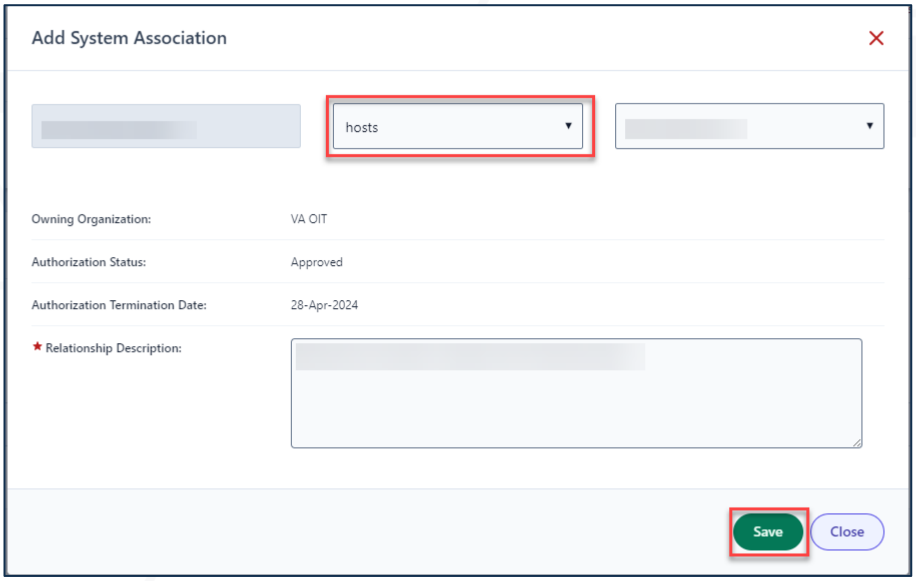


Figure 8: Adding a New Association for Assess Only Application Screenshot

8. Once the Relationship Type and supporting Platform, Enclave, or Information System have been added, the Authorization information will appear.

9. Select **[Save]** after the relationship between both systems has been described.

Note: *The* supporting Platform, Enclave, or Information System *must select "hosts" from the drop-down menu. Assess Only systems are required to have only **one** associated relationship.*



Owning Organization: VA OIT

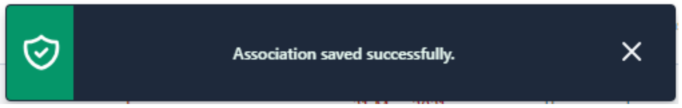
Authorization Status: Approved

Authorization Termination Date: 28-Apr-2024

* Relationship Description:

Figure 9: Saving a New Association for Assess Only Application Screenshot

10. A notification will appear, confirming that the association was successful:



Association saved successfully.

Figure 10: Association relationship confirmation Screenshot

Receiving Inheritance

The supporting Platform, Enclave, or Information System may provide implementation of controls and/or Control Correlation Identifiers (CCIs) assigned to the Assess Only system included in the control set. To document this within eMASS, the system's controls and CCIs must be set up as inheritable.

Inheritance for Assess Only systems utilize the same process as Assess and Authorize Information Systems, as documented in eMASS Implementation Guide.

Note: *It is imperative that the Assess Only System Steward works closely with the Major Application to establish a relationship during the System registration Process. Users cannot search for a supporting Platform, Enclave, or Information System that has not identified their organizational availability.*

Note: *Assess Only systems do not have to inherit from System of Records within eMASS. All inheritance relationships established for the supporting Platform, Enclave, or Information System are assumed for the Assess Only system.*

Refer to the eMASS Implementation Guide for specific steps and additional guidance.

Control Implementation

Systems using the Assess Only workflow will complete *Control Implementation* tasks in the same manner as Major Applications but are not required to initiate this step. Refer to eMASS implementation User Guide for specific procedures and guidelines.

Tasks include documenting implementation of Applicable and Hybrid controls, documenting Test Results per CCI, uploading supporting artifacts to support Test Results, develop initial Plan of Action and Milestones (POA&M) for non-compliant controls, and completion of risk assessments for non-compliant security controls. Assess Only systems must develop POA&Ms to identify tasks required to be completed. POA&Ms must detail resources required to accomplish the elements of the plan, milestones, and scheduled completion dates for the milestones.

Each security artifact uploaded to eMASS should be named using the following format: AssessOnlySystemNameORAcronym_.

Example, technical scan/testing result: AssessOnlySystemNameORAcronym_TechnicalScanName.

> **Note:** *Security Artifacts should not be password protected. eMASS limits access to personnel with a "need to view" for system details and artifacts.*

System Steward completes following in eMASS

1. Implement the Security Controls as documented in the System Security Plan (SSP).
2. Conduct a Self-Assessment:
    a. Conduct testing/self-assessment for applicable security controls.
    b. Complete risk assessments for applicable threat sources and security controls.
3. Develop POA&Ms for non-compliant security controls.
4. Perform Control Implementation review.
5. Once completed, initiate Approval Process (Section 4.5) for Assess Only Package.

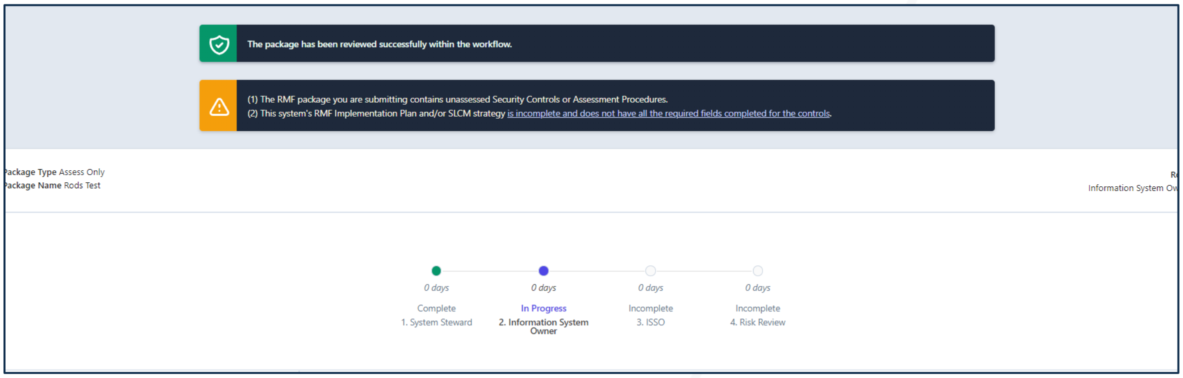
Refer to the POA&M Management Guide and eMASS Implementation Guide for additional details.

Approval Process

System Steward Moves Package to the ISO

Once all tasks, artifacts, and document requirements have been completed, the System Steward will progress the Assess Only Package to the ISO.

1. Open active Workflow Status screen.
2. Choose **[Approve]** under *Select Action drop-down.
3. Enter *Comments in text box provided.
4. Select **[Approve]**.
5. Workflow is now with ISO for review/Approval.



The package has been reviewed successfully within the workflow.

(1) The RMF package you are submitting contains unassessed Security Controls or Assessment Procedures.
(2) This system's RMF Implementation Plan and/or SLCM strategy is incomplete and does not have all the required fields completed for the controls.

ackage Type Assess Only
ackage Name Rods Test

Re
Information System Ow

0 days
Complete
1. System Steward

0 days
In Progress
2. Information System Owner

0 days
Incomplete
3. ISSO

0 days
Incomplete
4. Risk Review

Figure 11: Workflow Status Screenshot

ISO Reviews the Package and Moves to the ISSO

Upon logging into eMASS, the ISO will see a new workload task on the eMASS home page.

1. The ISO reviews the package to ensure necessary actions and tasks have been completed by selecting each category in the task bar; *Workflow, Dashboard, Details, Categorization, Controls, Implementation Plan, Risk Assessment, POA&M, Artifacts, and Reports*.
2. After each section has been completely reviewed, the ISO navigates to **[Menu]**, **[Active Workflow Listing]**, and select Assess Only package name.
3. The ISO chooses the appropriate action in the **Select Action* drop-down.

   To Approve:

   a) Choose **[Approve]** from *Select Action drop-down;

   b) Enter appropriate details in **Comments* box;

   c) Select **[Approve]**.

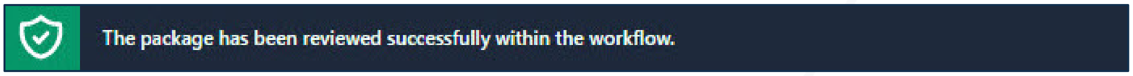
OR

Other Actions:

a) Choose from available actions in *Select Action drop-down;

b) Follow prompts to confirm selected workflow decision.

4. A green notification will appear, indicating that the “ISO” stage has completed.



The package has been reviewed successfully within the workflow.

Figure 12: Information System Owner Validation Screenshot

ISSO Reviews the Package and Moves to Risk Review

Upon logging into eMASS, the ISSO will see a new workload task on the eMASS home page.

1. The ISSO reviews the package to ensure necessary actions and tasks have been completed by selecting each category in the task bar; *Workflow, Dashboard, Details, Categorization, Controls, Implementation Plan, Risk Assessment, POA&M, Artifacts, and Reports*.
2. After each section has been completely reviewed, the ISSO navigates to **[Menu]**, **[Active Workflow Listing]**, and select Assess Only package name.
3. The ISSO chooses the appropriate action in the **Select Action* drop-down.

   To Approve:

   a) Choose **[Approve]** from *****_Select Action drop-down_;

   b) Enter appropriate details in *****_Comments_ box;

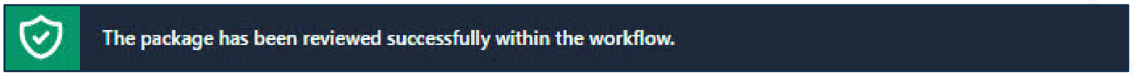
   c) Select **[Approve]**.

   OR

   Other Actions:

   a) Choose from available actions in *****_Select Action drop-down_;

   b) Follow prompts to confirm selected workflow decision.
4. A green notification will appear, indicating that the “ISSO” stage has completed.



The package has been reviewed successfully within the workflow.

Figure 13: Information System Security Officer Validation Screenshot

5. The Assess Only package is now assigned to Risk Review.

Refer to the eMASS Implementation Guide for specific steps and additional guidance.

Control Assessment

Once initial approval is received, the Assess Only system will undergo RMF Step 4 when the supporting Platform, Enclave, or Information System is reauthorized.

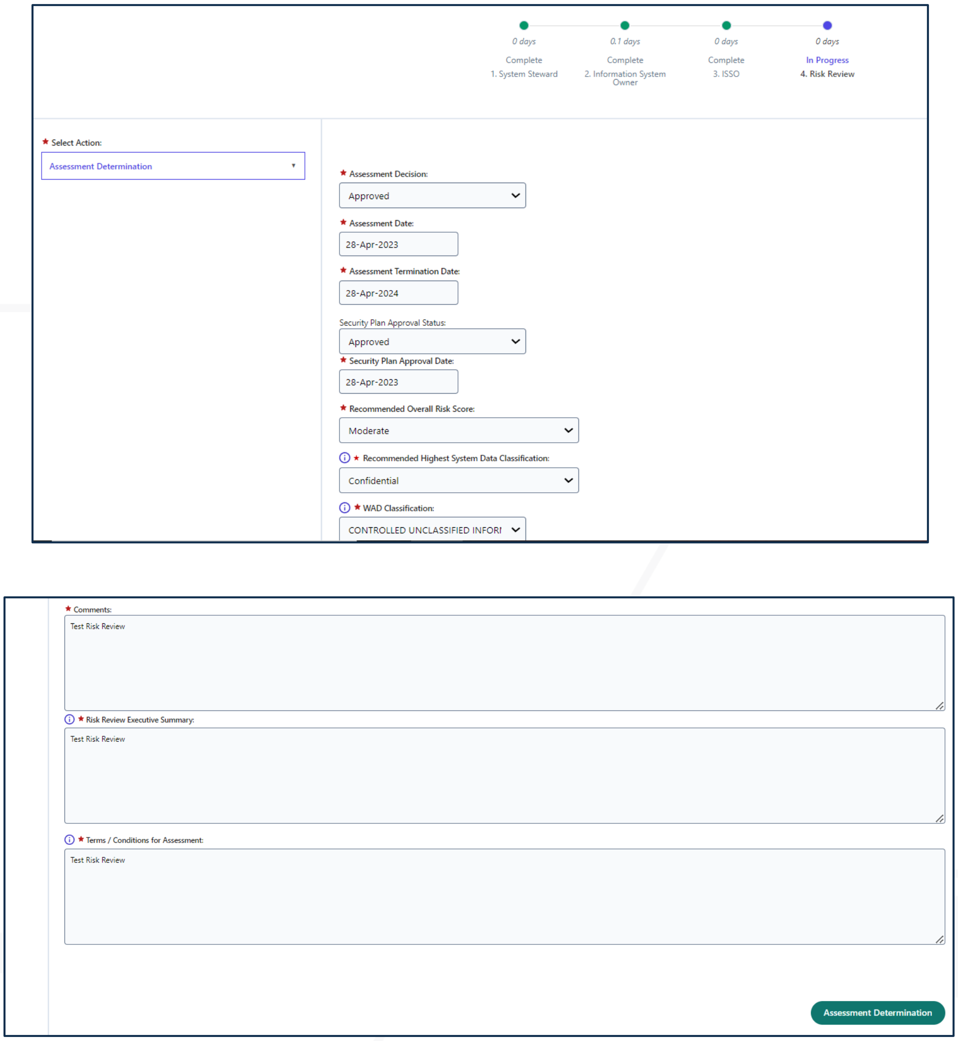
> **Note:** *This stage is performed by the Control Assessor for Major Applications. Systems using the Assess Only workflow are assessed with the Major Application. In this stage, the Control Assessor reviews each control that was previously submitted for validation.*
>
> *The Control Assessor either approves the control's status, indicating agreement with the self-assessment, adds a new test result changing/correcting the prior test result, or returns it for rework.*

Risk Review

> **Note:** *Assess Only systems must be in these stage 70 days prior to Approval Terminal Date (ATD), or "need by date", for initial approvals.*

In this workflow stage, the Risk Reviewer assesses the submitted package and provides an assessment decision based on the presented package. Specifically, this role documents an Executive Summary describing the overall system cybersecurity risk, a recommended assessment decision, and assessment termination date.

1. Choose Risk Review determination from ******Select Action* drop-down.
2. Complete all Risk Review sections below prior to submitting Assessment Decision. All fields with ***** are required fields and must be completed prior to submission:



0 days
Complete
1. System Steward

0.1 days
Complete
2. Information System Owner

0 days
Complete
3. ISSO

0 days
In Progress
4. Risk Review

* Select Action: Assessment Determination

* Assessment Decision: Approved

* Assessment Date: 28-Apr-2023

* Assessment Termination Date: 28-Apr-2024

Security Plan Approval Status: Approved

* Security Plan Approval Date: 28-Apr-2023

* Recommended Overall Risk Score: Moderate

* Recommended Highest System Data Classification: Confidential

* WAD Classification: CONTROLLED UNCLASSIFIED INFORI

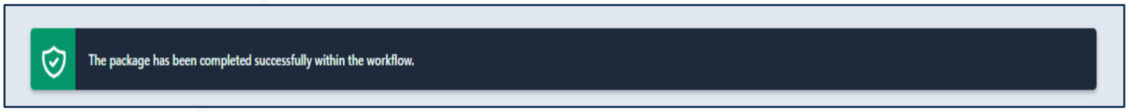
* Comments: Test Risk Review

* Risk Review Executive Summary: Test Risk Review

* Terms / Conditions for Assessment: Test Risk Review

Figure 14: Risk Review Submission Screenshot

3. Select **[Assessment Determination]** to Save/Submit.
4. A confirmation banner stating the package has been successfully completed, along with an assessment summary and Executive Summary will be generated upon completion.



The package has been completed successfully within the workflow.

Figure 15: Risk Review Validation Screenshot

5. The Authorizing Official Designated Representative will brief the Authorizing Official when an associated Assess Only package is approved, informing them of

the impacts to the Assess and Authorize information system, supporting Platform, or Enclave.

Appendix A – Glossary

Table 3: Glossary

Word	Definition
Application	A software program hosted by an information system. SOURCE: NIST SP 800-137.
Authorizing Official	Senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37. In VA, this is the VA CIO.
Availability	Ensuring timely and reliable access to and use of information. SOURCE: NIST 800-53; FIPS 199.
Business Associate Agreement	An entity, including any individual, company, or organization that, performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receipt, maintenance, or transmission of protected health information (PHI), or that provides to or for VHA certain services as specified by the HIPAA Privacy Rule that involves the disclosure of PHI by VHA. SOURCE: 45 C.F.R. § 160.103; VHA Handbook 1605.05.
Business Impact Analysis	An analysis of an IS's requirements, functions and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: NIST 800-34
Common Security Control	Security control that is inherited by one or more organizational information systems. SOURCE: NIST SP 800-53; These controls affect all VA facilities and systems with operations at the local site(s).
Control Set	A Control Set is a group of predefined security controls assigned to systems using the Assess Only workflow based on the System Type the user selects during the System registration process.
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: 44 U.S.C. § 3542.
High Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. SOURCE: NIST SP 800-37; NIST SP

Word	Definition
	800-53; NIST SP 800-60; FIPS 200.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009.
Information Security	A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. SOURCE: 38 U.S.C. § 5727.
Information System Security Officer (ISSO)	Individual working with the senior agency ISO, AO, or Information System Owner to help ensure the appropriate operational security posture is maintained for an information system or program. SOURCE: CNSSI-4009; VA Adapted.
Information Security Requirements	Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce, NIST, and OMB, and, as to national security systems, the President. SOURCE: 38 U.S.C. § 5727.
Information Sensitivity	Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from low, to medium, to high.
Information System Contingency Plan (ISCP)	Management policy and procedures designed to maintain or restore business operations, including computer operations, possible at an alternate location, in the event of emergencies, system failures, or disasters. SOURCE: NIST 800-34
ISCP Lite	Streamlined version of an ISCP that addresses the non-inherited contingency planning controls of an assess only system. It described interim measures to recover information system services after a disruption, including measures for relocation of information systems and service to an alternate site.
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: FIPS 200.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Orders, directive, policy, or regulation.

Word	Definition
	SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C. § 11101 and § 1401.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. SOURCE: 44 U.S.C. § 3542.
Interconnection Security Agreement (ISA)	An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) between the organizations. SOURCE: NIST SP 800-47.
Low Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200.
Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA)	A document established between two or more parties to define their respective responsibilities in accomplishing a goal or mission. In this Handbook, an MOU or MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. SOURCE: NIST SP 800-47.
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Minor Application	An application can be classified as being a Minor Application if it meets the following conditions: it relies upon a major system/enclave for the majority of its security, it is within another system’s authorization boundary, and it does not have its own capital plan. It has an impact level of Low or Moderate.
Moderate Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. SOURCE: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 200.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. SOURCE: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 199.

Word	Definition
Privacy Impact Assessment (PIA)	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. SOURCE: 44 U.S.C. §§ 3541-3549; NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI-4009; OMB Memorandum 03-22.
Protected Health Information (PHI)	Individually identifiable health information held by a covered entity or by a business associate acting on its behalf. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. §§ 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer. Within VA, VHA is the only covered entity. Certain other VA components, such as OI&T, are business associates of VHA. SOURCE: 45 C.F.R. § 160.103; VA Directive 6066.
Security Categorization	The process of determining the security category for information or information system. SOURCE: NIST SP 800-53.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP NIST 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200.

Appendix B – Assess Only Control Sets

Table 4: Assess Only Control Sets

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
AC-1	Access Control Policy And Procedures	X	X	X	X
AC-2	Account Management	X	X	X	X
AC-2 (1)	Automated System Account Management		X		X
AC-2 (2)	Removal Of Temporary / Emergency Accounts		X		X
AC-2 (3)	Disable Inactive Accounts		X		X
AC-2 (4)	Automated Audit Actions		X		X
AC-3	Access Enforcement	X	X	X	X
AC-4	Information Flow Enforcement		X		X
AC-5	Separation Of Duties		X		X
AC-6	Least Privilege		X		X
AC-6 (1)	Authorize Access To Security Functions		X		X
AC-6 (2)	Non-Privileged Access For Nonsecurity Functions		X		X
AC-6 (5)	Privileged Accounts		X		X
AC-6 (9)	Auditing Use Of Privileged Functions		X		X
AC-6 (10)	Prohibit Non-Privileged Users From Executing Privileged Functions		X		X
AC-7	Unsuccessful Logon Attempts	X	X	X	X
AC-8	System Use Notification	X	X	X	X
AC-11	Session Lock		X		X
AC-11 (1)	Pattern-Hiding Displays		X		X
AC-12	Session Termination		X		X
AC-14	Permitted Actions	X	X	X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
	Without Identification Or Authentication				
AC-17	Remote Access	X	X	X	X
AC-20	Use Of External Information Systems	X	X	X	X
AC-20 (1)	Limits On Authorized Use		X		X
AC-21	Information Sharing		X		X
AC-22	Publicly Accessible Content	X	X	X	X
AP-1	Authority To Collect			X	X
AP-2	Purpose Specification			X	X
AR-2	Privacy Impact And Risk Assessment			X	X
AR-3	Privacy Requirements For Contractors And Service Providers			X	X
AR-7	Privacy-Enhanced System Design And Development			X	X
AR-8	Accounting Of Disclosures			X	X
AU-1	Audit And Accountability Policy And Procedures	X	X	X	X
AU-2	Audit Events	X	X	X	X
AU-2 (3)	Reviews And Updates		X		X
AU-3	Content Of Audit Records	X	X	X	X
AU-3 (1)	Additional Audit Information		X		X
AU-4	Audit Storage Capacity	X	X	X	X
AU-5	Response To Audit Processing Failures	X	X	X	X
AU-6	Audit Review, Analysis, And Reporting	X	X	X	X
AU-6 (1)	Process Integration		X		X
AU-6 (3)	Correlate Audit Repositories		X		X
AU-7	Audit Reduction And Report Generation		X		X
AU-7 (1)	Automatic Processing		X		X
AU-8	Time Stamps	X	X	X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
AU-9	Protection Of Audit Information	X	X	X	X
AU-9 (4)	Access By Subset Of Privileged Users		X		X
AU-11	Audit Record Retention	X	X	X	X
AU-12	Audit Generation	X	X	X	X
CA-3	System Interconnections	X	X	X	X
CA-3 (5)	Restrictions On External System Connections		X		X
CA-5	Plan Of Action And Milestones	X	X	X	X
CA-7	Continuous Monitoring	X	X	X	X
CA-9	Internal System Connections	X	X	X	X
CM-1	Configuration Management Policy And Procedures	X	X	X	X
CM-2	Baseline Configuration	X	X	X	X
CM-2 (1)	Reviews And Updates		X		X
CM-2 (]3)	Retention Of Previous Configurations		X		X
CM-2 (7)	Configure Systems, Components, Or Devices For High-Risk Areas		X		X
CM-3	Configuration Change Control		X		X
CM-3 (2)	Test / Validate / Document Changes		X		X
CM-4	Security Impact Analysis	X	X	X	X
CM-5	Access Restrictions For Change		X		X
CM-6	Configuration Settings	X	X	X	X
CM-7	Least Functionality	X	X	X	X
CM-7 (1)	Periodic Review		X		X
CM-7 (2)	Prevent Program Execution		X		X
CM-8	Information System Component Inventory	X	X	X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
CM-8 (1)	Updates During Installations / Removals		X		X
CM-8 (3)	Automated Unauthorized Component Detection		X		X
CM-8 (5)	No Duplicate Accounting Of Components		X		X
CM-9	Configuration Management Plan		X		X
CM-10	Software Usage Restrictions	X	X	X	X
CP-2	Contingency Plan	X	X	X	X
CP-9	System Backups	X	X	X	X
DI-1	Data Quality			X	X
DM-1	Minimization Of Personally Identifiable Information			X	X
DM-2	Data Retention And Disposal			X	X
DM-3	Minimization Of PII Used In Testing, Training, And Research			X	X
IA-1	Identification And Authentication Policy And Procedures	X	X	X	X
IA-5 (2)	PKI-Based Authentication		X		X
IA-7	Cryptographic Module Authentication	X	X	X	X
IA-8	Identification And Authentication (Non-Organizational Users)	X	X	X	X
IA-8 (1)	Acceptance Of PIV Credentials From Other Agencies	X	X	X	X
IA-8 (3)	Use Of Ficam-Approved Products	X	X	X	X
IA-8 (4)	Use Of Ficam-Issued Profiles	X	X	X	X
IP-1	Consent			X	X
IP-2	Individual Access			X	X
IP-3	Redress			X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
IP-4	Complaint Management			X	X
MA-1	System Maintenance Policy And Procedures	X	X	X	X
MA-4	Nonlocal Maintenance	X	X	X	X
MA-4 (2)	Document Nonlocal Maintenance		X		X
MA-5	Maintenance Personnel	X	X	X	X
MA-6	Timely Maintenance		X		X
MP-1	Media Protection Policy And Procedures	X	X	X	X
MP-2	Media Access	X	X	X	X
MP-3	Media Marking		X		X
MP-5	Media Transport		X		X
MP-5 (4)	Cryptographic Protection		X		X
MP-7	Media Use	X	X	X	X
MP-7 (1)	Prohibit Use Without Owner		X		X
PL-8	Information Security Architecture		X		X
RA-3	Risk Assessment	X	X	X	X
RA-5	Vulnerability Scanning	X	X	X	X
RA-5 (5)	Privileged Access		X		X
SA-1	System And Services Acquisition Policy And Procedures	X	X	X	X
SA-2	Allocation Of Resources	X	X	X	X
SA-3	System Development Life Cycle	X	X	X	X
SA-4	Acquisition Process	X	X	X	X
SA-4 (1)	Functional Properties Of Security Controls		X		X
SA-4 (2)	Design / Implementation Information For Security Controls		X		X
SA-4 (9)	Functions / Ports / Protocols / Services In Use		X		X
SA-4 (10)	Use Of Approved PIV	X	X	X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
	Products				
SA-5	Information System Documentation	X	X	X	X
SA-8	Security Engineering Principles		X		X
SA-9	External Information System Services	X	X	X	X
SA-9 (2)	Identification Of Functions / Ports / Protocols / Services		X		X
SA-10	Developer Configuration Management		X		X
SA-11	Developer Security Testing And Evaluation		X		X
SC-2	Application Partitioning		X		X
SC-4	Information In Shared Resources		X		X
SE-1	Inventory Of Personally Identifiable Information			X	X
SE-2	Privacy Incident Response			X	X
SI-2	Flaw Remediation	X	X	X	X
SI-4	Information System Monitoring	X	X	X	X
SI-5	Security Alerts, Advisories, And Directives	X	X	X	X
SI-7	Software, Firmware, And Information Integrity		X		X
SI-7 (1)	Integrity Checks		X		X
SI-7 (7)	Integration Of Detection And Response		X		X
SI-10	Information Input Validation		X		X
SI-11	Error Handling		X		X
SI-12	Information Handling And Retention	X	X	X	X
SI-16	Memory Protection		X		X
TR-1	Privacy Notice			X	X

Control	Title	Low	Moderate	Low with Privacy	Moderate with Privacy
TR-2	System Of Records Notices And Privacy Act Statements			X	X
UL-1	Internal Use			X	X
UL-2	Information Sharing With Third Parties			X	X
Total Controls		**57**	**118**	**77**	138

Appendix C - eMASS Naming Conventions

When the user initiates a new Assess Only package/workflow, a Package Name is required. The Package Name should utilize the following format:

Assess Only Application or Acronym_MMYYYY

Each security artifact uploaded to eMASS should be named using the following format:

Assess Only Application Name or Acronym_<Insert Document Type>

Technical Scan/Testing result **Example:** would be titled:

Assess Only Application Name or Acronym_TechnicalScanName

Appendix D – Standards and Guidelines

The Security Assessment process is developed to document and evaluate the effectiveness of in-place security features, and to determine the extent to which security controls satisfy system-specific requirements specified in the following publications:

- Federal Information Security Modernization (FISMA) Act of 2014
- Privacy Act of 1974, Section 5 U.S.C. 552a, Records Maintained on Individuals
- 38 U.S.C. 5705, Confidentiality of medical quality assurance records
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- OMB Circular A-123 II, Establishing Enterprise Risk Management in Management Practices
- OMB Circular A-130, Managing Information as a Strategic Resource
- VA Directive 6500, VA Cybersecurity Program
- VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program
- VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology
- FIPS 199, Standard for Security Categorization of Federal Information and Information Systems
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST 800-128, Guide for Security-Focused Configuration Management of Information Systems.

Appendix E – Documentation Requirements by System Type

Table 5: Documentation Requirements

Acronym	Documentation/Requirement	Assess Only	Medical Device	Special Purpose System (SPS)	Research Scientific Computing Device (RSCD)
BAA	Business Associate Agreement	X	X	X	X
BIA	Business Impact Analysis	X	X	X	X
CMP	Configuration Management Plan	X			
Control Set	Assigned controls based on "Information Type" selected	X			
ERA	Enterprise Risk Analysis		X	X	X
HW/SW	Hardware/Software Inventory	X	X	X	X
ISA/MOU	Interconnection Security Agreement (ISA)/ Memorandum of Understanding	X	X	X	X
***ISCP - Lite**	Information System Contingency Plan	X	X	X	X
MDCIR	Medical Device Cybersecurity Incident Response		X		
MDS2	Manufacturer Disclosure Statement for Medical Device		X		
Network Topography Diagram	Topography Diagram	X	X	X	X
POA&Ms	Plan of Action and Milestones	X	X	X	X
PPS List	Ports, Protocols, and Services	X	X	X	X
PTA	Privacy Threshold Analysis	X	X	X	X
***PIA**	Privacy Impact Assessment	X	X	X	X
RAR	Risk Assessment Report	X	X	X	X
SIA	Security Impact Analysis	X			
***SoR**	Status of Requirements	X			
SPS Questionnaire	Completed for all procurements of network connected SPS			X	
SSP	System Security Plan	X	X	X	X
Vendor Manufacturer Worksheet	Completed for all procurements of network connected RSCD				X
VA 6550 Directive	VA Directive 6550/Appendix A		X		

Artifacts containing an * must be shared with the supporting Platform, Enclave, or Information System. The supporting Platform, Enclave, or Information System must identify all Assess Only systems by name within their corresponding artifacts.