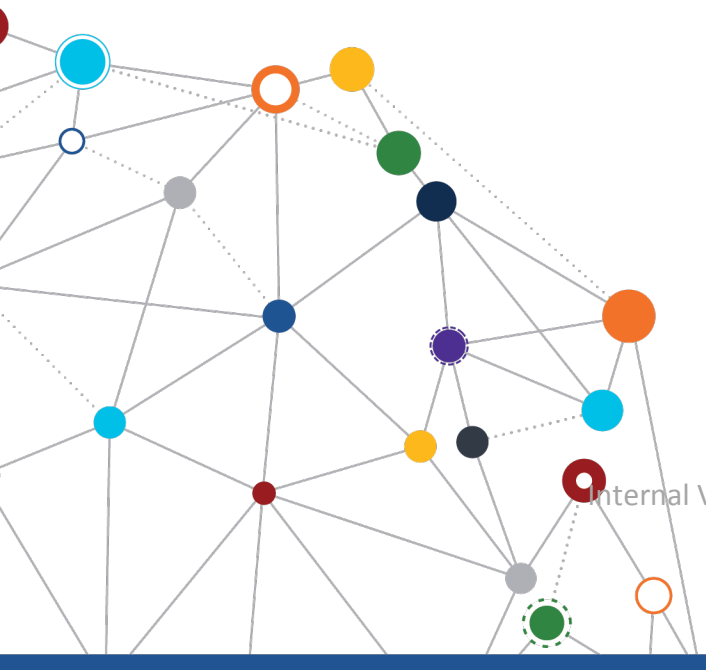
OFFICE OF
INFORMATION
SECURITY

Department of Veterans Affairs Cloud Authority to Operate (ATO) Process

Version 2.0

November 19, 2018 | Cybersecurity Architecture Office



VA

U.S. Department of Veterans Affairs
Office of Information and Technology
Office of Information Security

Revision History

Date	Version	Description	Author
10/08/2018	1.0	Initial Draft	IMC / UNISYS
10/26/2018	1.1	Updated Draft	VAEC COMS Team/Cognosante
11/19/2018	2.0	Updated and finalize for signature	VAEC COMS Team/Cognosante

We, the undersigned, approve the content of this ATO Cloud Security Process for the VA Enterprise Cloud (VAEC) Microsoft Azure Government High and Amazon Web Services (AWS) GovCloud High.

_____

David Catanoso

Director

Enterprise Cloud Solutions Office (ECSO)

_____

Joseph Fourcade
Program Manager
Enterprise Cloud Solutions Office (ECSO)

Table of Contents

VA Cloud Authority to Operate Process Summary

1 Background

Obtaining an Authority to Operate (ATO) for a cloud-leveraged Department of Veteran Affairs (VA) information system changes the ATO process applied historically at VA. Cloud Service Providers (CSPs) have gone to great lengths to secure their infrastructure, utilizing world-class security tools and employing in-house security teams with deep expertise. Most importantly, CSP's use a **shared responsibility model** for providing defense-in-depth security.

As detailed in *Figure 1* below, the specific cloud service delivery mechanisms that a customer selects (whether on-premises, IaaS, PaaS, or SaaS) will define and determine customer-specific responsibilities.

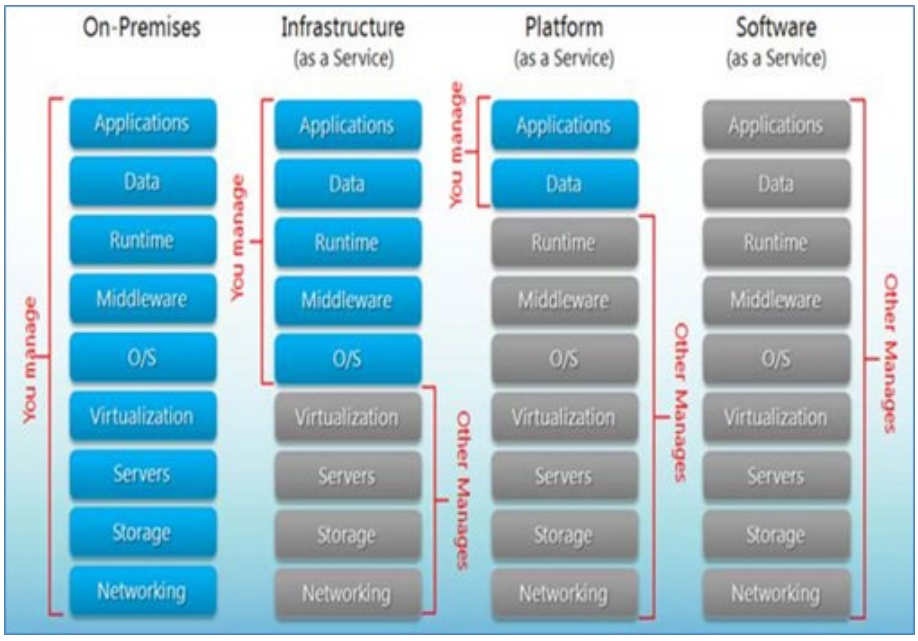


Figure 1: Shared Responsibility for different Cloud Service Modes https://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/

There are three primary cloud service models based on the NIST SP 800-145, *The NIST Definition of Cloud Computing*:

- Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
- Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications.

Customers deploying in the VA Enterprise Cloud (VAEC) can take advantage of the *shared responsibility model* and accelerate more secure deployment of IT assets and accelerate the ATO process.

Specifically, customers utilizing the shared-responsibility model can take advantage of control inheritance. The CSPs are responsible for ensuring they have gone through the FedRAMP process and obtained an ATO. As part of the FedRAMP process, the CSP will document in the Controls Implementation Summary (CIS) the responsibilities of the CSPs and the customer. The majority of VA cloud-leveraged systems will rely on not only their own ATO but the ATO of their Cloud Service Provider (CSP) and the ATO of the VA Enterprise Cloud (VAEC) with each representing a potential source of security control inheritance.

The VAEC provides a set of common General Support Services (GSS) to simplify support and development. The services that are part of the VA GSS ATO provided to within the VAEC Azure an AWS deployments are the following:

- Common Services
  - Active Directory
  - PKI Services
  - Ansible
  - Backup
  - CA Unified Infrastructure Management (CA UIM)
  - Disaster Recovery
  - GitHub
  - Jump Boxes
  - SMTP Relays
- Security and Scanning Tools
  - BigFix
  - McAfee (HIPS, HIDS, Antivirus)
  - Nessus
  - Splunk

2 Purpose

This document is intended to standardize the process flow and expectations for obtaining ATO for a VA cloud-leveraged system. It will be enhanced in future iterations to standardize the process flow for authorizing individual cloud services including Software-as-a-Service (SaaS) which presents unique challenges of its own. Linked to the process flow are potential metrics that can be measured and presented during Planning, Migration, and Operation of the VA cloud-leveraged information system. It will also be updated as the VA migrates from RiskVision to eMASS for RMF assessment recording.

3 Scope

The VA Enterprise Cloud (VAEC) CSP Environments have a US Federal Risk and Authorization Management Program (FedRAMP) High Certified VA ATO. VAEC provides access to the FedRAMP certified services of each CSP.

The ATO for an application or system residing in the VAEC is separate from the VAEC CSP Environment ATO. Each project team is responsible for its application or system level ATO.

System Owners and Information Security Officers (ISO) will follow the Risk Management Framework for VA Information System (VA Handbook 6500). This guide presents the overall process flow to achieve an ATO for a VA cloud-leveraged information system. The process is linked to the RMF as described above and contains distinct procedures to ensure the appropriate security concerns and compliance requirements are considered throughout the RMF. Currently, the VA utilizes RiskVision (https://vaww.grc.va.gov/spc/page.jsp) as their Governance, Risk, and Compliance (GRC) tool to capture security and compliance requirements.

VA has partnered with the Defense Information Systems Agency (DISA) to transition to a new GRC tool. This tool, Enterprise Mission Assurance Support Service (eMASS) is a web-based Government off-the-shelf (GOTS) service for Risk Management Framework (RMF) Assessment and Authorization activities. DISA will deploy and maintain eMASS on behalf of the VA.

Please refer to the VAEC CSP's website (VAEC Site) to determine which services are in scope and have been fully assessed by third party auditors, resulting in a FedRAMP Certification, attestation of compliance, or ATO.

Customers deploying in the VAEC can take advantage of the common controls that are being provided by the CSP, VAEC, and from the VA to accelerate more secure deployment of IT assets and accelerate the ATO process. Common controls are security controls whose implementation results in a security capability that is *inheritable* by one or more organizational information systems. The inheritable controls from the CSP have been assessed with an accredited Third-Party Assessment Organization (3PAO) as part of the FedRAMP ATO process. This means the System Owner has less controls that they are responsible for implementing and validating. This will help to accelerate the authorization process.

When submitting an authorization package within RiskVision, the ISO will work with the System Owner to provide guidance on those controls that are inheritable and do not require a response.

Figure 2 Controls Inheritance Summary

4 VA Cloud ATO Process – VA Cloud-Leveraged System

The overview provided below illustrates the Risk Management Framework (RMF) process to obtain a system-specific ATO when the system leverages a cloud service (or multiple cloud services). The process flow follows the NIST and VA RMF by identifying specific procedural tasks for each of the following RMF steps (as applicable):

1. Categorize
2. Select
3. Implement
4. Assess
5. Authorize
6. Monitor

Figure 3 Risk Management Framework (RMF)

Note: As this is a document specific to the process and procedures required to achieve ATO for cloud services and VA cloud-leveraged information systems, the processes associated with implementation and assessment are abbreviated while referencing the appropriate legacy process for completing the action.

The System Owner, ISO, and other designated stewards must complete the following to successfully submit for an Authorization package (see Appendix A – Cloud ATO Checklist):

- ☐ Designate an Information Security Officer and coordinate assignment of an Enterprise Program Management Office (EPMO) Information Assurance (IA) Security Analyst (see Section 5.1)
- ☐ Submit for a Veteran -Focused Integration Process Request (VIPR) ID (see Section 5.2)
- ☐ Complete the RiskVision (to be replaced by eMASS) System Inventory Checklist (see Section 5.3)
- ☐ Register with the VA Software Assurance Program Office (see Section 5.4)
- ☐ Submit for a Secure Design Review (see Section 5.5)

- ☐ Submit a Privacy Threshold Analysis to determine if a Privacy Impact Analysis (PIA) is required (see Section 5.6 and Section 6.1.5)
- ☐ Prepare PIA if required (see Section 5.6)
- ☐ Prepare System Security Plan (see Section 6.1.1)
- ☐ Prepare Incident Response Plan (see Section 6.1.2)
- ☐ Prepare Disaster Recovery Plan (see Section 6.1.3)
- ☐ Prepare Information Security Contingency Plan (ISCP) (see Section 6.1.4)
- ☐ Prepare Interconnection Security Agreement/Memorandum of Understanding (see Section 6.1.6)
- ☐ Prepare Configuration Management Plan (see Section 6.1.7)
- ☐ Prepare Signatory Authority document (see Section 6.1.8)
- ☐ Document control implementation evidence in RiskVision (or eMASS) (see Section 6.1.9)
- ☐ Prepare Risk Assessment (see Section 6.1.10)
- ☐ Request Nessus Scan (see Section 6.2.1)
- ☐ If project includes a database, schedule Database scan (see Section 6.2.2)
- ☐ Request Quality Code Review validation (see Section 6.2.3)
- ☐ Request Secure Code Review validation (see Section 6.2.4)
- ☐ Request Penetration Test/Web Application Security Assessment (see Section 6.2.5)
- ☐ Request Security Compliance Configuration Data (SCCD) scan (see Section 6.2.6)
- ☐ Prepare Plan of Action and Milestones (see Section 6.3)
- ☐ Prepare Authorizing Official System Brief (AOSB) to be submitted with ATO Packet (see Section 6.4)

For the ATO to be reviewed for authorization by the VA, the package must be completed and uploaded into RiskVision and progressed to "CA Provide Certification Recommendation" no less than 45 calendar days before the date of the requested authorization decision. More detailed information can be found in the Office of Information Security document "Authorization Requirements Standard Operating Procedures Version 3.27", dated September 28, 2018.

5 Authorization Prerequisites

5.1 Information Security Officer (ISO) Designation

If an ISO is not yet assigned to the system/application, the System Owner must submit the required form to request ISO Support.

Form Link:	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/ATO%20Documents/FSS_ISO%20Support_Request.pdf
E-mail Address:	VAFSSISORequests@va.gov

Once an ISO is assigned, coordinate with the ISO to get an assigned Security Analyst from the EPMO IA office.

5.2 Veteran – Focused Integration Process Request (VIPR) Identification (ID)

If an effort touches the VA network, regardless of whether it spends government funds from VA's Congressional IT Appropriation or any other appropriation, the VIP Framework is mandated per the Veteran-focused Integration Process (VIP) Memorandum signed on Dec. 31, 2015 by Laverne Council, Assistant Secretary for Information Technology.

The Veteran-focused Integration Process (VIP), a Lean-Agile framework, services the interest of Veterans through the efficient streamlining of activities occurring within the IT enterprise. This effort prioritizes the increasing value to the Veteran, information security, portfolio management, and continuous organizational learning and improvement within VA.

The primary goal of VIP is to increase the speed of delivering high-quality, secure, and sustainable IT capabilities to benefit the Veteran.

The system owner will submit Epics to OIT to begin the process.

VIP Link:	**VIP SharePoint**: https://vaww.vaco.portal.va.gov/sites/OIT/epmo/vip/Pages/HomePage.aspx
E-mail Address:	**VIP Business Office**: vavip@va.gov **Assistance with Alignment Epics**: epics@va.gov **Release Readiness Office**: OITEPMOTRSRROReleaseAgents@va.gov

5.3 RiskVision Entry for Application or System

System Owner or delegate completes the RiskVision (RV) System Inventory Checklist. Reach out to the ISO or the RiskVision Working Group (RVWG) with any questions regarding checklist completion. Once the RVWG approves the Application/System for a RiskVision entry, the System Owner or delegate will be notified by OIS via e-mail from the GRC Service Desk.

RV Checklist Link:	https://vaww.portal2.va.gov/sites/infosecurity/ca/RV_NewSystemRequest.aspx
E-mail Address:	**RiskVision Working Group:** VARiskVisionWG@va.gov **GRC Service Desk**: vaGRCservicedesk@va.gov

5.4 Application Registration

Custom developed and COTS VA applications are required to be registered with the VA Software Assurance Program Office. Registration is necessary to maintain an inventory of the total population of VA custom and COTS applications, by type and business line according to the VA Common Application Enumeration (CAE) to ensure application-level security considerations are taken into account when determining readiness and performance.

Detailed instructions on the registration process can be found on the VA Software Assurance Developer Support Site.

Application Registration Link:	https://wiki.mobilehealth.va.gov/display/OISSWA/How+to+open+an+NSD+ticket+to+register+a+VA+application
E-mail Address:	**OIS Software Assurance:** OISSwAServiceRequests@va.gov

5.5 Secure Design Review

Secure design reviews of VA custom-developed applications are conducted during development and during authorization processes. Secure design reviews, unlike secure code reviews, may be performed before any code is written.

If the application has not already been registered (Section 5.2), then the custom-developed application will need to be registered. After the registration has been completed, an Application-ID and upload/report directory will be provided. **COTS applications do not need to be submitted for Secure Design Review**. Next, request a sample VA Application Threat Model by sending an email to OIS Software Assurance with the following:

- Subject: Request sample threat models
- Body: Include the Application-ID for which the models are being requested in support of.

Secure Design Review Link:	**Application Threat Model**: https://wiki.mobilehealth.va.gov/display/OISSWA/How+to+open+an+NSD+ticket+to+request+an+initial+application+threat+model **VA Secure Design Review SOP**: https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Secure%20Design%20Review%20SOP.pdf?api=v2
E-mail Address:	**OIS Software Assurance**: OISSwAServiceRequests@va.gov

5.6 Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)

The System Owner (SO), Privacy Officer (PO), and ISO will need to work together to submit a PTA to determine if Personally Identifiable Information (PII) is being collected by the Application/System. If the PTA determines that is no PII being collected:

1. The System Owner, PO, and ISO will be notified that no further action is required.
2. A copy of the PTA will be provided to the System Owner, PO and ISO as privacy compliance and risk management document indicating the system has been assessed for privacy implications.
3. Upload a copy of the PTA into RiskVision.

If the PTA indicates that PII is being collected:

1. A copy of the PTA will be provided to the SO, PO and ISO as privacy compliance and risk management documentation indicating an IT system has been assessed for privacy implications and a PIA is required.
2. The PO will coordinate with the ISO and System Owner to ensure all data and associated risks are identified and documented in the PIA submission. The ISO and System Owner will review and draft the PIA and work with the PO for any chances.
3. The PIA will require electronic signature from the PO, ISO and SO prior to submission to the Chief Information Officer (CIO) for review and signature. Once the CIO reviews and signs the PIA, it is officially approved and completed.
4. The SO, PO and ISO will be notified of the approval and approved PIA will be incorporated into the System's A&A package by the ISO.
5. The System Owner or delegate uploads the PIA into RiskVision.

PTA / PIA Template Link:	https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FVA%20A%20and%20A%20Templates&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View=%7b5FCA9CEF-1C50-441D-A2FE-28D536ED0098%7d
E-mail Address:	**Privacy Office**: PIASupport@va.gov

6 Assessment & Authorization (A&A) Requirements

6.1 Security Documentation

6.1.1 System Security Plan (SSP)

The SSP is the 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.

The SSP is developed within RiskVision.

Continuous Monitoring Requirement – The SSP must be updated on an **annual basis** or when a significant change in the system or a major change in the data occurs.

RiskVision Link:	**National Release GRC Instance:** https://vaww.grc.va.gov/spc/index.jsp **Enterprise Operations GRC Instance**: https://vaww.eogrc.va.gov/spc/index.jsp
E-mail Address:	**GRC Service Desk:** vaGRCservicedesk@va.gov

6.1.2 Incident Response Plan (IRP)

IRP guidance is provided below:

- Facilities are responsible for completing the IRP.
- An IRP is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.
- IRP guidance can be found in NIST SP 800-61.
- Tools and websites that can be useful in IRP creation:
  - Agiliance RiskVision Enterprise Operations GRC Instance
  - Agiliance RiskVision National Release GRC Instance
  - OIS Cyber Security Portal
- The System Owner works with the assigned ISO to create the IRP.
- Once completed and tested, the System Owner or designee uploads the signed IRP into RiskVision.
- Each site is responsible for developing local level procedures incorporating VA-CSOC areas of responsibility.
- The Incident Response Plan must meet the following standards in creation:
  - Information Access and Privacy Program
  - NIST Special Publication 800-61 - Computer Security Incident Handling Guide
  - VA Handbook 6500.3, Certification and Authorization of Federal Information Systems

Continuous Monitoring Requirement – The IRP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

6.1.3 Disaster Recovery Plan (DRP)

DRP guidance is provided below:

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- Disaster Recovery planning refers to measures to recover information system services to an alternate location after a disruption.
- The System Owner or delegate develops or revises the DRP.
- Questions about the planning process, plan templates, or testing process should contact the EPR team (OITITOPSSPECOECCDRCOOPAllStaff@va.gov).
- The System Owner or delegate uploads the DRP into RiskVision.

- The DRP must meet the following standards:
    - NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems Agiliance RiskVision Enterprise Operations GRC Instance
    - Office of Information Security, Authorization Requirements Guide Standard Operating Procedures

Continuous Monitoring Requirement – The DRP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

6.1.4 Information Security Contingency Plan (ISCP)

ISCP guidance is provided below:

- Emergency Preparedness & Response (EPR) underneath DR/COOP is the Office of Primary Responsibility (OPR) for planning and testing of plans.
- Plans are based upon current boundaries established by OIS. Each year EPR will provide planning and testing guidance through an action item.
- Contingency planning refers to interim measures to recover information system services after a disruption.
- The System Owner or delegate develops or revises the Information System Contingency Plan.
- Questions about the planning process, plan templates, or testing process should contact the EPR team (OITITOPSSPECOECCDRCOOPAllStaff@va.gov).
- The System Owner or delegate uploads the Information System Contingency Plan into RiskVision.
- The ISCP must meet the following standards:
    - NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems Agiliance RiskVision Enterprise Operations GRC Instance
    - Office of Information Security, Authorization Requirements Guide Standard Operating Procedures

Continuous Monitoring Requirement – The ISCP must be tested and updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

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

The **Privacy Threshold Analysis (PTA)** should be updated, signed and uploaded in the *Documents tab* in RiskVision. If required, the **Privacy Impact Assessment (PIA)** should be updated, signed and uploaded in the *Documents tab* in RiskVision.

Continuous Monitoring Requirement – A PTA must be submitted **on Annual Basis**. A PIA must be submitted **Every Three Years**. (A&A SOP, 4.2.9)

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

ISA/MOU guidance is provided below:

- Before an external connection can be granted, a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) are 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.
- ISA/MOU guidance can be found in NIST SP 800-47 and VA Handbook 6500.
- Additional guidance for completion of the ISA/MOU can be found in the Field Security Service (FSS) Bulletin # 269 or by contacting the Health Information Security Division at vafsshisd@va.gov or the OIT Enterprise Risk Management (ERM) CRISP Team at Sharon.mcallister@va.gov.

ISA/MOU completion steps:

1. System Owner in coordination with the entities identified in NIST SP 800-47 will complete the ISA/MOU using the latest template provided at: OIS Portal or A&A Home Documents.
2. ISO will upload all final draft MOU/ISA documents to the MOU/ISA Review Submissions SharePoint site for a review prior to requesting signatures.
3. A VA review team will assess the documents against a checklist for quality and content.
4. The reviewer and the ISO will work collaboratively to correct deficiencies found in the documentation.
5. The reviewer will notify the ISO via email informing them that the document is ready for signatures.
6. The ISO will process the document for signature.
7. Upon receipt of the completed and signed MOU/ISA document, the ISO will upload the document to the Enterprise Document SharePoint.
8. The finalized document should also be added to the existing A&A artifacts in RiskVision.

Continuous Monitoring Requirement – The ISA/MOU Review Sheet must be completed on an **annual** basis. If there is a significant change, which impacts the architecture, please contact the Health Information Security Division at vafsshisd@va.gov to determine if an update to the ISA/MOU is necessary.

6.1.7 Configuration Management Plan (CMP)

CMP guidance is provided below:

- Facilities are responsible for completing the CMP (pending clarification on requirement for systems).
- CMP guidance can be found in NIST SP 800-128 and VA Handbook 6500.
- Additional guidance for completion of the CMP can be provided by OIS.
- The CMP should include processes for managing configuration and change management.
- The CMP should include infrastructure devices and baseline configurations (e.g., switches, routers, firewalls).
- The CMP should include a configuration file for each operating system(s), database(s), application(s), and network device(s) to validate compliance with baseline configuration.

CMP completion steps:

1. System Owner or delegate completes the CMP using the template provided at A&A Home Documents.
2. ISO, System Owner or delegate/System Steward uploads the CMP to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The CMP must be updated on an **annual** basis or when a significant change in the system or a major change in the data occurs.

6.1.8 Signatory Authority

Signatory Authority guidance is provided below:

- The Signatory Authority must be signed and dated by the appropriate parties.
- Additional guidance for completion of the Signatory Authority can be provided by OIS.

Signatory Authority completion steps:

1. System Owner or delegate completes the Signatory Authority using the template provided at A&A Home Documents.
2. System Owner, ISO or delegate/System Steward uploads the Signatory Authority to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – The Signatory Authority must be completed on an **annual** basis or when a significant change in the system or a major change in the data occurs.

6.1.9 Control Implementation Evidence

All control implementation statements evaluated as part of the RiskVision Assessment Workflow need to contain evidence that demonstrates the control was tested, how it was tested, and the results. The evidence will be required for all controls that are documented to be in place and the

results can be documented by going to the appropriate assessment and clicking on the General tab. From the General tab, select each control in the Control Test column to document how a control was tested, the results, any associated findings, and any supporting documentation.

6.1.10 Risk Assessment (RA)

The Risk Assessment (RA) should be uploaded in the Documents tab in RiskVision. Follow the steps below to complete the action item.

1. The System Steward completes the assessment in RiskVision.

2. The ISO validates information added by the System Steward in RiskVision.

3. The ISO, System Owner or delegate/System Steward exports the RA from RiskVision and uploads the document to the Documents tab in RiskVision

Continuous Monitoring Requirement – The RA must be updated on an Annual Basis or when a significant change in the system or a major change in the data occurs (A&A SOP, 4.2.4).

6.2 Scanning and Testing

6.2.1 Nessus Scan

A credentialed 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). All Critical and High deficiencies should be mitigated with documented mitigation evidence provided, and Moderate and Low deficiencies should be mitigated or have a documented mitigation plan.

The System Owner or delegate will need to request a Nessus scan. Once the request is completed, CPO will work with ISRM/CSOC to determine if a separate supplemental vulnerability scan shall be conducted or authentication information for the non-Windows devices (e.g., SSH credentials for Linus/Unix servers) be added to the existing monthly predictive scan (conducted by NSOC).

Upload the results to the **Documents** tab within RiskVision when results are sent to you. Next, please provide the IP Ranges to ISRM, so the applicable Nessus data can be entered in TVM within RiskVision.

If a system's Nessus Scan data is not currently displayed in the TVM within RiskVision, refer to the TVM guidance material located on the OIS portal.

Once the system's Nessus Scan data is accurately shown in TVM within RiskVision, System Owner or delegate needs to follow these steps:

a) Browse to Nessus Enterprise Web Tool (NEWT) and use the Remediation Effort Entry Form (REEF) to document your manual remediation effort. For each deficiency identified from the scan, the System Owner or delegate 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 https://spsites.cdw.va.gov/sites/FODW_PVT/Progress%20Reports/Progress_ReportbyRegion_Chart.rdl within NEWT.

c) Export the report by going to the upper left side of the screen select the Actions Menu. Choose Export and select Excel. Save the file.

d) System Owner or delegate then uploads the report from step 3 above to the Documents tab within RiskVision. Mitigation information can also be provided in the Vulnerabilities tab within RiskVision.

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.

Continuous Monitoring Requirement – CSOC conducts predictive Nessus vulnerability scans monthly. 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, the system must meet this continuous monitoring requirement.

Nessus Links:	**Nessus Scan Request:** https://vaww.portal2.va.gov/sites/infosecurity/ca/Lists/Supplemental%20Scan%20Request/AllItems.aspx **OIS Portal GRC Training**: https://vaww.portal2.va.gov/sites/infosecurity/projects/GRC%20Tool/GRC%20Tool%20Training%20Materials/Forms/AllItems.aspx **Nessus Enterprise Web Tool (NEWT**: https://spsites.cdw.va.gov/sites/FODW_PVT/
E-mail Address:	**ISRM**: vaoisisrmrmf@va.gov

6.2.2 Database Scan

If this project includes a database host, a full database scan must be scheduled with the VA-CSOC. Once the database scan results are received, all findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision.

To maintain the authorization decision for the system, any findings must be remediated within the approved timelines for the severity of the findings, and a Plan of Action and Milestones (POA&M) must be created in RiskVision to keep track of the remediation effort. Database scans can be requested by visiting the link listed below.

If a Database scan is not applicable, upload document to the documents tab explaining why a Database scan is not applicable.

Continuous Monitoring Requirement – The Database scan must be conducted on an **annual** basis or when a significant change to the configuration.

VA CSOC DB Scan Questionnaire	https://vaww.portal2.va.gov/sites/infosecurity/ca/Lists/VA%20NSOC%20DB%20Questionnaire/AllItems.aspx
E-mail Address:	**Database Scanning Team:** VANSOCDBScans@va.gov

6.2.3 Verification & Validation (V&V) Quality Code Review

Quality code reviews of VA enterprise applications are conducted during development. Quality code reviews conducted during development are performed both during component testing and during A&A processes. If the application has not be registered, then the VA Application Developer will need to open a VA National Service Desk (NSD) ticket to register their application with the VA SwA Program Office.

V&V reviews are conducted during the A&A process to obtain an Authority to Operate (ATO) or Temporary Authority to Operate (TATO). VA Application Developers scan their own application source code and deliver the scan results to the VA SwA Program Office for review.

- Subject: "Request quality code review validation"
- Body: Include the Application-ID and attach the V&V Quality Code Review Request Form

Secure Design Review Link:	**V&V Quality Code Review**: https://wiki.mobilehealth.va.gov/pages/viewpage.action?pageId=63837464 **V&V Quality Code Review Request Form**: https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Quality%20Code%20Review%20Validation%20Request%20Form.pdf **V&V Quality Code Review SOP**: https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Quality%20Code%20Review%20SOP.pdf?api=v2
E-mail Address:	**OIS Software Assurance**: OISSwAServiceRequests@va.gov

6.2.4 Secure Code Review

Secure code reviews of custom developed VA applications using the approved VA static code analysis tool should be conducted to identify vulnerabilities, coding, and design flaws within VA applications. Applications written in languages that are not supported, such as MUMPS, shall be targeted for manual review of testing with other applicable tools. If a Secure Code Review is not applicable, upload a document to the Documents tab within RiskVision explaining why a Secure Code Review is not applicable.

Note there are two types of code reviews, which are not the same and are not interchangeable from an authorization perspective. There are different, separate A&A SOP technical/testing requirements for each. Secure code review has to do with following up mainly on potential critical and high severity findings. Compared to quality code review which has to do with following up on potential quality-specific findings.

As part of the process for the secure code review, the Fortify .fpr scan file(s) and zip(s) of scanned code to your applications will need to be uploaded to the report directory on the VA network. An email will need to be sent to the OIS Software Assurance with the Secure Code Request form attached, and the following:

- Subject: "Request secure code review validation"
- Body: Please include the Application-ID and attach the Secure Code Review Request form.

Continuous Monitoring Requirement – The Secure Design Review must be updated on an **Annual Basis** or when a significant change in the system or a major change in the application architecture occurs. (A&A SOP, 4.2.11)

Secure Design Review Link:	**V&V Secure Code Review**: https://wiki.mobilehealth.va.gov/pages/viewpage.action?pageId=26774489 **V&V Secure Code Review Request Form**: https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Quality%20Code%20Review%20Validation%20Request%20Form.pdf **V&V Secure Code Review SOP**: https://wiki.mobilehealth.va.gov/download/attachments/24482308/VA%20Secure%20Code%20Review%20SOP.pdf?api=v2
E-mail Address:	**OIS Software Assurance**: OISSwAServiceRequests@va.gov

6.2.5 Penetration Test / Web Application Security Assessment (WASA)

The System Owner or delegate requests a penetration test or a WASA by completing the CSOC Penetration Test / CSOC WASA form found at NSOC Scan Documents to request penetration test/application assessment from CSOC.

The CSOC Penetration Test / NSOC Web Application Security Assessment (WASA) must be uploaded in the *Documents tab* on RiskVision and updated Annually.

Continuous Monitoring Requirement – A CSOC Penetration Test / CSOC WASA is required on an Annual Basis to maintain an ATO and/or when a major change to the system or upgrades to the tools used occurs. In addition, OI&T conducts penetration testing quarterly on one-fourth of the total number of VA High Systems and/or internet facing systems. (A&A SOP, 4.2.11)

Pen Test / WASA Link:	**Pen Test / WASA Request**: https://vaww.portal2.va.gov/sites/infosecurity/ca/CA%20Home%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Fca%2FCA%20Home%20Documents%2FCSOC%20Scan%20Documents&FolderCTID=0x012000CB0DD849BEA0AB4FA5FEE491047C852D&View=%7B5FCA9CEF-1C50-441D-A2FE-28D536ED0098%7D

6.2.6 Security Compliance Configuration Data (SCCD)

The System Owner or delegate contacts ISRM at vaoisisrmrmf@va.gov to ensure the IP addresses or system names that make up their system(s) are appropriately tagged or accounted for in RiskVision.

After reviewing information system boundaries for accuracy, System Owner/Delegate should run the Security Configuration Compliance Data (SCCD) **Checklist Trending** and **Compliance Trending** reports and export them to PDF from the EVVM Dashboard (https://dashboard.tic.va.gov > Enterprise > All Systems > Authorization & Accreditation).

System Owner or Delegate uploads the Compliance Trending and Checklist Trending reports to the Documents tab in RiskVision. The Compliance Trending and Checklist Trending reports can be found at https://dashboard.tic.va.gov/s/28U/ and https://dashboard.tic.va.gov/s/28T/, respectively.

Important: If the IS environment changes, the System Owner will need to contact ISRM to ensure the correct system(s) are tagged/untagged in RiskVision. Not informing ISRM of system inventory changes will result with incorrect SCCD scan reports.

Continuous Monitoring Requirement – 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, or when requested by OIS.(A&A SOP, 4.3.5)

Checklist Trending reports	Regional GSS: https://dashboard.tic.va.gov/s/28T/ Facility GSS: https://dashboard.tic.va.gov/s/28V/ System: https://dashboard.tic.va.gov/s/28X/
Compliance Trending reports	Regional GSS: https://dashboard.tic.va.gov/s/28U/ Facility GSS: https://dashboard.tic.va.gov/s/28W/ System: https://dashboard.tic.va.gov/s/28Y/

6.3 Plan of Action and Milestone (POA&M) Remediation

The System Owner or delegate will address all weaknesses that have been identified during the assessment and scanning of the applicable application or system within RiskVision prior to submission for ATO. The System Owner or delegate will need to provide responses for the weakness that includes the remediation activities for the corrective actions or mitigation activities with associated milestones to correct the weaknesses.

6.4 Authorizing Official System Brief (AOSB)

The completion of the AOSB process is automated. EPMOIA will send out the AOSB link that is specific to the system typically two weeks prior to the "45-Day" ATO expiration date. The system's AOSB link is sent to the System Owner and ISO. For further information, contact EPMOIA@va.gov.

Initial ATOs will go through a similar process. The progression of the RiskVision workflow will prompt for an AOSB to be completed.

Appendix A Cloud ATO Checklist

CLOUD AUTHORIZATION CHECKLIST FOR DEPLOYMENTS WITHIN THE VAEC	
Activity	**Status**
Authorization Prerequisites	
Information Security Officer (ISO) Designation and EPMO IA Security Analyst assigned	
Focused Integration Process Request (VIPR) Identification (ID)	
RiskVision Entry for Application or System	
Application Registration	
Secure Design Review	
Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)	
Assessment & Authorization (A&A) Requirements	
Security Documentation (RMF Step 3)	
System Security Plan (SSP)	
Incident Response Plan (IRP)	
Disaster Recovery Plan (DRP)	
Information Security Contingency Plan (ISCP)	
Interconnection Security Agreement (ISA) / Memorandum of Understanding (MOU) – (if required)	
Configuration Management Plan (CMP)	
Signatory Authority	
Control Implementation Evidence	
Risk Assessment (RA) (RMF Step 4)	
Scanning and Testing (RMF Step 4) – Request as soon as possible after CRISP compliance	
Nessus Scan	
Database Scan (if required)	
Verification & Validation (V&V) Quality Code Review	
Secure Code Review	
Penetration Test / Web Application Security Assessment (WASA)	
Security Compliance Configuration Data (SCCD)	
Plan of Action and Milestone (POA&M) Remediation	
Authorizing Official System Brief (AOSB)	
Authorization Package Submission	
Authorization to Operate (ATO) Issuance (RMF Step 5)	
Continuous Monitoring (RMF Step 6)	

APPENDIX B VA Cloud ATO Report and Dashboard (Sample Mockup)

All VA systems are required to register in VA's Information System Inventory (VASI) and cloud-leveraged systems are no exception. Information about each system will be captured in RiskVision and periodically fed to VASI. VA's Enterprise Architecture (EA) Security Domain produces an ATO Report and Dashboard as illustrated in **Figure 4**, that can be leveraged to produce results filtered to show only cloud-leveraged systems.

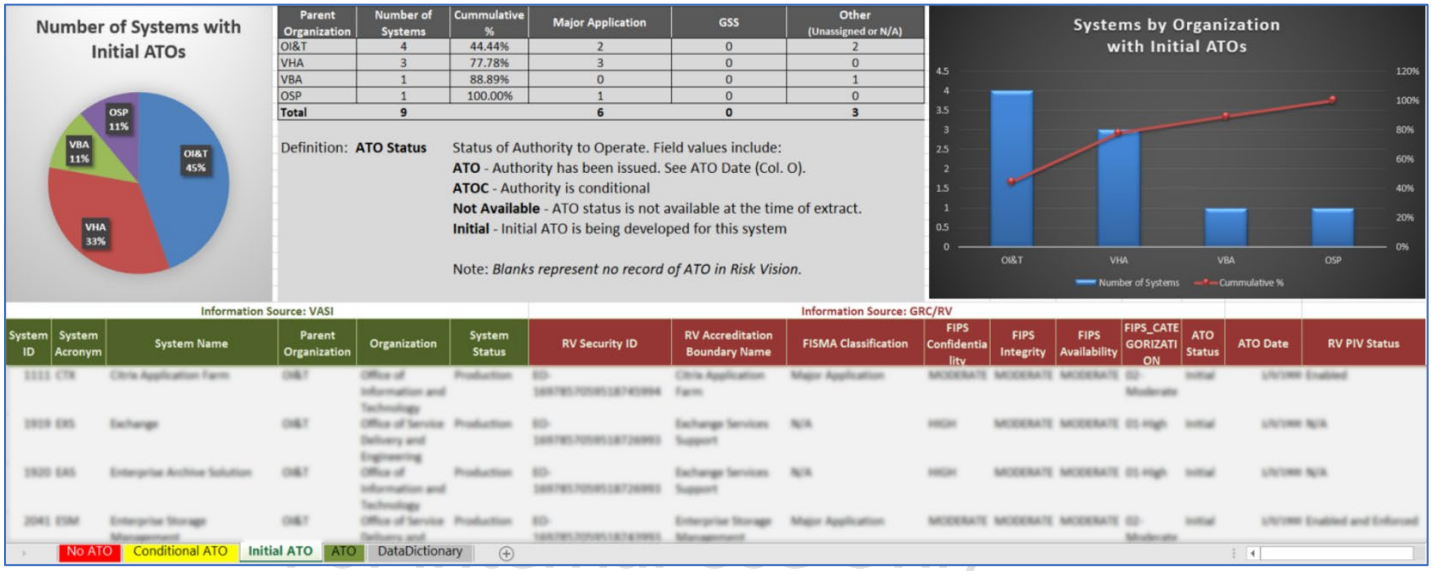


Figure 4: ATO Report and Dashboard Sample Mockup

Appendix C System Owner Policy Mandated Responsibilities

In accordance with VA policy, System Owners/System Stewards have policy mandated responsibilities spanning from information system security to day-to-day system operations. The responsibilities in this checklist pertain to System Owners/Stewards responsibilities as outlined in VA Handbook 6500 and system accreditation requirements. (Source: Office of Information Security System Owner Accountability Model, Model Criteria Version 1.0, dated January 2016)

#	Responsibility	Designee	Completed?	
1.	Develop in RiskVision: - SSP - Risk Assessment - Configuration Management Plan (CMP) - Incident Response Plan (IRP) - Information System Contingency Plan (ISCP) - Disaster Recovery Plan (DRP) - Privacy Impact Assessment (PIA) - Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
2.	Review and update the SSP as required by OCS and when a significant change to the system occurs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
3.	Review, update and test the system contingency plan as specified in the SSP and when a significant change to the system occurs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
4.	Ensure risk assessments are accomplished per the SSP, regularly reviewed/updated, and when there is a major change to the system, reviewed and updated as required.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
5.	Conduct PIA with the assistance of the PO, as required.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
6.	Develop and maintain an IT system Configuration, Change, and Release Management Plan.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
7.	Ensure that technical testing is coordinated with the appropriate organizational entities and completed as scheduled (i.e., Nessus scans, secure code reviews, penetration test/application assessments, security control assessments (SCA), and security configuration compliance data).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
8.	Ensure each system has developed a secure baseline of security controls by scoping, tailoring, compensating, and supplementing the controls as outlined in the VA Handbook 6500.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
9.	Ensure each system secure baseline configuration outlined above is documented in	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	the SSP and approved by the VA CIO (as the AO) or designee prior to implementation.			
10.	Provide appropriate access to VA systems (including types of privileges or access), in coordination with VA managers and ISOs.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
11.	Ensure the development and maintenance of SSPs and contingency plans are in coordination with local information owners, the local system administrators, ISO, and functional "end user" for nationally deployed systems.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
12.	Ensure system users and support personnel receive required security training.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
13.	Assist the local system administrators in the identification, implementation, and assessment of security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
14.	Ensure the information system receives authorization prior to operational deployment, is reauthorized when a significant change in the system or a major change in the data occurs, and is continuously monitored.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
15.	Assist other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the plan of action and milestones (POA&M) and updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
16.	Ensure continuous monitoring activities are performed.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
17.	Notify the responsible VA ISO, PO, VA Network Security Operations Center (VA-NSOC) and the OIG as appropriate per VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), of any suspected incidents immediately upon identifying that an incident has occurred and	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	assisting in the investigation of incidents, as necessary.			
18.	Ensure compliance with the Enterprise and Security Architecture throughout the system life cycle.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
19.	Charter, organize, and maintain VA's Patch and Vulnerability Team (PVT) Program.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
20.	Collaborate with VA Identity Safety Service to monitor for identity theft, when appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
21.	Nominate a COR for all contracts impacted by this directive and ensuring CORs complete the required COR training.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
22.	Ensure security requirements and security specifications are explicitly included in VA contracts, as appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
23.	Work with the ISO and PO to ensure contracts contain the required security language necessary for compliance with FISMA and 38 U.S.C. 5721-5728 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing the VA Contractor ROB.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
24.	Ensure contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
25.	Ensure contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
26.	Monitor the contract to ensure that security requirements are met, consulting the ISO and PO as necessary.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
27.	Ensure compliance with Federal security requirements and VA security policies.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

28.	Participate in self-assessments, external and internal audits of system safeguards and program elements, including A&A of the system.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
29.	Evaluate proposed technical security controls to assure proper integration with other system operations.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
30.	Identify requirements for resources needed to effectively implement technical security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
31.	Ensure the integrity in implementation and operational effectiveness of technical security controls by conducting technical control testing.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
32.	Serve as owner for all local systems (e.g., tenant systems, guest networks) for which he/she is assigned, establishing standards (based on Federal requirements and VA security policies) for operating the systems within a VA facility, and removing non-compliant systems from use at the VA facility.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
33.	Periodically repeat selected test procedures from the system's security authorization to ensure the security controls continue to operate effectively at the proper levels of assurance per NIST guidance and over the life cycle of the system.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
34.	Assist other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
35.	Collaborate with VA Identity Safety Service to provide training on identity theft and fraud prevention and mitigation and to assist in the prevention and mitigation of potential identity theft and fraud.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

36.	Consult with the AO or designee, the local CIO and ISO when establishing or changing system boundaries. Additional guidance regarding the determination of system boundaries is outlined in NIST SP 800-37 and should be used if there are questions regarding a system's boundary.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
37.	In coordination with Information Owners and the ISO, categorize information systems as low-, moderate-, or high-impact for the security objectives of confidentiality, integrity, and availability.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
38.	Continue with VA's Risk Management Framework by: (1) selecting the initial baseline of security controls, (2) tailoring the initial baseline of security controls, and (3) supplementing the baseline controls as outlined in VA Handbook 6500.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
39.	Implement and test the security controls specified in the approved SSP.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
40.	Implement the VA-approved U.S. Government Configuration Baseline (USGCB) controls, formerly known as the Federal Desktop Core Configuration (FDCC), or Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG).	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
41.	Ensure assessors have access to the information system and environment of operation where the security controls are employed, and the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
42.	Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated controls, as appropriate.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
43.	Prepare the POA&M based on the findings and recommendations of various security	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

	assessment reports excluding any remediation actions taken.			
44.	Assemble the security authorization package and submits the package to the AO for adjudication.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
45.	Follow the security authorization process defined in VA Handbook 6500.3.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
46.	Determine the security impact of proposed or actual changes to the information system and its environment of operation.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
47.	Conducts remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
48.	Update the SSP, security assessment report, and POA&M based on the results of the continuous monitoring process.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
49.	Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate VA officials on an ongoing basis in accordance with the monitoring strategy.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
50.	Follow VA Handbook 6500.1, Electronic Media Sanitization requirements when a system is removed from service.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
51.	Follow additional information regarding continuous monitoring in VA Handbook 6500.3.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐
52.	Implement and follow additional System Owner/Steward responsibilities as outlined in the VA Handbook 6500's security control details.	[*populate with name of actual designee, as appropriate*]	Yes ☐	No ☐

The list of System Owner responsibilities is subject to change as federal and VA security policies, standards and guidance are modified.

Appendix D References and Supporting Documentation

VA Handbook 6500

Office of Information Security document “Authorization Requirements Standard Operating Procedures Version 3.27”, dated September 28, 2018

Assessment and Authorization, Process Asset Library, Office of Information and Technology, undated.

Other ATO documents can be found at:

NSOC ATO Scan Forms

Appendix E Acronyms

Acronym	Definition
3PAO	Third-Party Assessment Organization
A&A	Assessment and Authorization
AO	Authorizing Official
AOSB	Authorizing Official System Brief
ATO	Authority to Operate
CA	Certification Authority
CA UIM	Computer Associates Unified Infrastructure Management
CAE	Common Application Enumeration
CIO	Chief Information Officer
CIS	Controls Implementation Summary
CMP	Continuous Monitoring Requirement
COOP	Continuity of Operations Plan
COTS	Commercial Off-The-Shelf
CPO	Certification Program Office
CRISP	Continuous Readiness in Information Security Program
CSOC	Cybersecurity Operations Center
CSP	Cloud Service Provider
DB	Database
DRP	Disaster Recovery Plan
eMASS	Enterprise Mission Assurance Support Service
ERM	Enterprise Risk Management
ERP	Emergency Response Plan
EVVM	Enterprise Visibility and Vulnerability Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSS	Field Security Service
GRC	Governance, Risk and Compliance
GSS	General Support Services
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HISD	Health Information Security Division
IaaS	Infrastructure as a Service
ID	Identification
IP	Internet Protocol (Usually refers to IP Address)
IRP	Incident Response Plan

ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISO	Information Security Officer
ISRM	Information and Security Risk Management
IT	Information Technology
MOU	Memorandum of Understanding
MUMPS	Massachusetts General Hospital Utility Multi-Programming System
NEWT	Nessus Enterprise Web Tool
NIST	National Institute of Standards and Technology
NSD	National Service Desk
NSOC	Network and Security Operations Center
OIS	Office of Information Security
OIT	Office of Information Technology
OPR	Office of Primary Responsibility
PaaS	Platform as a Service
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PO	Privacy Officer
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
RA	Risk Assessment
REEF	Remediation Effort Entry Form
RMF	Risk Management Framework
RV	RiskVision
RVWG	RiskVision Working Group
SaaS	Software as a Service
SCCD	Security Compliance Configuration Data
SO	System Owner
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
SwA	Software Assurance
TATO	Temporary Authority to Operate
TVM	Threat and Vulnerability Manager
V&V	Verification & Validation
VA	Veteran Affairs
VAEC	Veteran Affairs Enterprise Cloud
VIP	Veteran-focused Integration Process

VIPR	VA IT Process Request
WASA	Web Application Security Assessment