OFFICE OF INFORMATION SECURITY

Accreditation Requirements Guide

Standard Operating Procedures

JANUARY 2014

Office of Information Security

Table of Contents

1. Background

To obtain and maintain an Authority to Operate (ATO), the accreditation requirements included within the contents of this document must be completed. The Accreditation Requirements section outlines the technical/testing and security documentation requirements that are necessary to support an accreditation decision. The Governance, Risk and Compliance (GRC) tool (RiskVision) will act as the management tool for the Assessment and Authorization (A&A) process, and systems will be assessed in RiskVision by an OCS representative [Certification Agent (CA)] for an accreditation recommendation to be submitted to the OIS Chief Information Security Officer (CISO) and VA Chief Information Officer (CIO) [Designated Approval Authorities (DAAs)] for final review and determination. RiskVision guidance documentation can be found on the OIS Portal (Click here).

In addition to the descriptions and procedures in this document, the accreditation requirements are listed in the *Accreditation Requirements Quick Link Reference Guide* located on the OIS Portal at http://go.va.gov/j8vn and in Appendix A of this document.

This document is based on current federal and VA security policies, standards and guidance, and is subject to change as VA and federal policy is modified.

2. Accreditation Prerequisites

The following steps need to be followed once a system is identified as needing a VA accreditation decision:

1. System Owner or delegate ensures an Information Security Officer (ISO) is assigned to the system. If an ISO is not yet assigned, designate an ISO by completing the following steps:

   a) The System Owner requests the VA ISO Support Request form from VAFSSISORequests@va.gov.

   b) Complete and submit the VA ISO Support Request form to VAFSSISORequests@va.gov.

   c) The ISO will help facilitate and coordinate accreditation requirements to the project team and answer cyber security questions throughout the System Development Life Cycle (SDLC).

2. System Owner or delegate requests the RiskVision Working Group at VARiskVisionWG@va.gov to include the system in the agenda for an upcoming RiskVision Working Group Meeting (meetings occur every Thursday at 12:00 PM EST when an agenda item exists), and that the applicable system points of contact (POCs) receive access to RiskVision. The RiskVision Working Group will provide any necessary forms that must be completed and submitted prior to the meeting.

3. During the meeting, a decision will either be made to move forward with the addition of the system into RiskVision or a recommendation to remediate any assigned action items with the assistance of the RiskVision Working Group.

4. Once the RiskVision Working Group approves the system entry into RiskVision, the System Owner or delegate will be notified by OCS that the system has been added. The applicable

system POCs will receive notification from the GRC Service Desk (vaGRCservicedesk@va.gov) stating that they have received access to the applicable instance of RiskVision:

    a. National Release GRC Instance: https://vaww.grc.va.gov/spc/index.jsp

    b. Enterprise Operations GRC Instance: https://vaww.eogrc.va.gov/spc/index.jsp

5. Once the applicable parties have access to RiskVision and the system resides in the tool, the System Owner or delegate shall contact OCS to review the accreditation requirements and determine if certain requirements are not applicable based on the type of system in question.

    a. Contact the Certification Program Office (CPO) at CertificationPMO@va.gov to review the accreditation requirements with an OCS CPO resource.

The applicable system POCs must have their accreditation package completed and uploaded to RiskVision no less than fifteen calendar days prior to the date they want their accreditation decision to be made.

3. Accreditation Requirements

The accreditation requirements include technical/testing, security documentation, and security control compliance requirements. If a required security control is not implemented, the project team must establish a Risk Based Decision (RBD) by following the applicable steps provided in Section 3.2.10.

If a system goes through a significant (major) change (as defined below) after an ATO determination is made, the system is required to re-complete the accreditation requirements, including updating all security documentation to reflect the change.

Significant Change Definition: Per the current 'draft' VA Handbook 6500.3, Assessment, Authorization, And Continuous Monitoring of VA Information Systems, the definition of 'significant change' is as follows: A significant (major) change to an information system or environment of operation is a change that is likely to affect the security state of the information system. Significant changes to an information system may include, but are not limited to, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include, but are not limited to, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, policies, or regulations. Source: SP 800-37 [VA Adapted].

3.1 Technical/Testing Requirements

The following section provides details on each of the technical/testing requirements including a description of the requirements and the parties/OIS organization(s) that will assist in the completion of the requirements.

3.1.1 Nessus Scan / [Discovery Scan (part of Nessus scan)]

A credentialed vulnerability scan against all instantiations 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 accreditation 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 following steps must be performed to meet the Nessus Scan requirement:

1. System Owner or delegate contacts CPO at CertificationPMO@va.gov to request system scan from NSOC. System Owner or delegate can contact NSOC directly with the applicable form(s) instead of reaching out to CPO, if preferred.

   a) NSOC must conduct an independent Nessus scan for all VA owned systems. NSOC has visibility into Enterprise Operations (EO) systems and Managed Services in most cases and has the ability to perform Nessus scans in coordination with system personnel. External systems must also have a recent NSOC Nessus scan conducted either via remote connection or by utilizing NSOC staff on-site to perform scans, when necessary. Sites and systems that have previously leveraged local Nessus scan capabilities (scans not officially run by NSOC), can still continue to leverage those scans and mitigate findings in accordance with OCS guidance, however, NSOC will have visibility into the scan server or results and has the final approving authority. In addition to this requirement, OIS may request that NSOC conduct a follow-up scan, where necessary. NSOC has the ability to provide an assessment of scan results and recommendations prior to an accreditation determination.

2. NSOC will provide results to system POCs.

3. System Owner or delegate uploads actual Nessus scan results to the *Documents* tab in RiskVision.

4. For each deficiency identified from the scan, the System Owner or delegate creates a response 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. Information should be provided in Excel or Word format (refer to the OCS preferred template located on the OIS Portal at: http://go.va.gov/plgx). System Owner or delegate uploads the aforementioned document to the *Documents* tab in RiskVision.

5. System Owner or delegate creates one finding and a response in the *Findings* tab within RiskVision for the Nessus scan to serve as a reminder to resolve the deficiencies.

Note: A follow-up Nessus scan may be requested by OIS to ensure deficiencies have been mitigated and new deficiencies do not exist as part of the ongoing accreditation process.

Continuous Monitoring Requirement – An NSOC or NSOC approved Nessus scan must be performed on a *monthly* basis and/or when new vulnerabilities potentially affecting the system/applications are identified and reported (NIST 800-53r4). To maintain the accreditation decision, the system must meet this continuous monitoring requirement.

3.1.2 Code Review

Code reviews of custom developed VA applications using the current approved VA static code analysis tool should be conducted to identify security 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 or testing with other applicable tools (notify OCS if this is the case at OISSwASupportGroup@va.gov). 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 following steps must be performed to meet the Code Review requirement:

1. System Owner or delegate contacts the Product Development (PD) Fortify Support Team at FORTIFY@va.gov with a Cc to Julie Harvey (PD) at Julie.Harvey@va.gov and requests a Fortify license. Once the license is received, the System Owner or delegate conducts the initial Fortify scan and provides the test result files (such as the Fortify Project or .fpr files), along with the complete and buildable source code for the inventoried applications for independent source code review and analysis to the OCS Software Assurance Team at OISSwASupportGroup@va.gov.

   a) Managed Services can conduct the code review locally but OIS can request that the applicable internal OIS party conducts a follow-up code review. NSOC will have the ability to provide an assessment of code review results prior to accreditation determination.

2. System Owner or delegate uploads test results to the **Documents** tab in RiskVision.

3. For each deficiency identified from the code review, System Owner or delegate creates a response 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. Information should be provided in Excel or Word format (refer to the OCS preferred template located on the OIS Portal at: http://go.va.gov/plgx). System Owner or delegate uploads the aforementioned document to the **Documents** tab in RiskVision.

4. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the code review to serve as a reminder to resolve the deficiencies.

Continuous Monitoring Requirement – An OIS or OIS approved Code Review is required when changes to the application or upgrades to the tool (i.e., Fortify) occur.

3.1.3 Penetration Test/Application Assessment

A penetration test or full application assessment must be performed that includes automated and manual assessment tools and techniques on *Internet Facing and/or High Impact Applications.* 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 following steps must be performed to meet the Penetration Test/Application Assessment requirement:

1. System Owner or delegate contacts CPO at CertificationPMO@va.gov to request penetration test/application assessment from NSOC. System Owner or delegate can contact NSOC directly with the applicable form(s) instead of reaching out to CPO, if preferred. Please allow 30 days for NSOC to schedule/conduct the penetration test/application assessment.

    a) NSOC must conduct an independent penetration test/application assessment for all VA owned applications. NSOC must have visibility into all VA applications where an accreditation decision is required. External systems must also have a recent NSOC penetration test/application assessment performed either remotely or by utilizing NSOC staff on-site to perform scans, when necessary. In situations where a site, application team, or external vendor has had a recent penetration test/application assessment that was not performed by NSOC, validation of those results and approval of the external assessment rests with NSOC and OIS leadership. In addition to this requirement, OIS may request that NSOC conduct a follow-up penetration test/application assessment, where necessary. NSOC has the ability to provide an assessment of the results or conduct the final penetration test/application assessment, if deemed necessary, prior to the accreditation determination.

2. NSOC will provide results to system POCs.

3. System Owner or delegate uploads actual results to the *Documents* tab in RiskVision.

4. For each deficiency identified from the penetration test/application assessment, the System Owner or delegate creates a response 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. Information should be provided in Excel or Word format (refer to the OCS preferred template located on the OIS Portal at: http://go.va.gov/plgx). System Owner or delegate uploads the aforementioned document to the *Documents* tab in RiskVision.

5. System Owner or delegate creates one finding and a response in the *Findings* tab within RiskVision for the Penetration Test/Application Assessment to serve as a reminder to resolve the deficiencies.

Continuous Monitoring Requirement – An NSOC or NSOC approved penetration test/application assessment is required when changes to the application or upgrades to the tools used occurs.

3.1.4 Security Control Assessment (SCA)

If appropriate, an SCA will be required by OCS. If an SCA is required, all Critical and High POA&Ms should be mitigated with documented mitigation evidence provided, and Moderate and Low POA&Ms should be mitigated or have a documented mitigation plan.

The following steps must be performed to meet the SCA requirement:

1. Once notified by OCS that an SCA is required, OIT Enterprise Risk Management (ERM) will be notified by OCS to schedule the assessment.

2. OIT ERM will conduct the SCA.

3. Once SCA results are received from OIT ERM (POA&Ms and SCA Report), System Owner or delegate must upload the results and POA&Ms to the **Documents** tab in RiskVision, along with a response for mitigating the POA&Ms and/or evidence that the POA&Ms have been mitigated.

4. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the SCA to serve as a reminder to resolve the deficiencies.

Continuous Monitoring Requirement – An SCA will be performed based on the criticality of the system and/or if circumstances arise that require an onsite SCA under the discretion of OCS.

3.1.5 Security Configuration Compliance Scan

Compliance scans must be performed against all Windows hosts (NSOC only has Windows Compliance scan capabilities) and must check against VA approved hardening guidance for all Operating Systems, Databases, Networks, and Security Devices, where guidance exists.

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

1. System Owner or delegate contacts CPO at CertificationPMO@va.gov to request compliance scan from NSOC. System Owner or delegate can contact NSOC directly with the applicable form(s) instead of reaching out to CPO, if preferred.

    a) NSOC must conduct an independent compliance scan for all VA owned systems. NSOC has visibility into EO systems and Managed Services in most cases and has the ability to perform compliance scans in coordination with system personnel. External systems must also have a recent NSOC compliance scan conducted either via remote connection or by utilizing NSOC staff on-site to perform scans, when necessary. Sites and systems that have previously leveraged local compliance scan capabilities (scans not officially run by NSOC), can still continue to leverage those and mitigate findings in accordance with OCS guidance. NSOC must have visibility into those scan server(s) or results and has the final approving authority. In addition to this requirement, OIS may request that NSOC conduct a follow-up compliance scan, where necessary. NSOC has the ability to provide an assessment of compliance scan results and recommendations prior to an accreditation determination.

2. NSOC will provide results to system POCs.

3. System Owner or delegate uploads actual results to the **Documents** tab in RiskVision.

4. For each deficiency identified from the compliance scan, System Owner or delegate creates a response for mitigating the deficiencies and / or provides evidence that the deficiencies have been mitigated. Include the scheduled completion date and status of each deficiency. Information should be provided in Excel or Word format (refer to the OCS preferred template located on the OIS Portal at: http://go.va.gov/plgx). System Owner or delegate uploads the aforementioned document to the **Documents** tab in RiskVision.

5. System Owner or delegate creates one finding and a response in the **Findings** tab within RiskVision for the compliance scan to serve as a reminder to resolve the deficiencies.

Continuous Monitoring Requirement – An NSOC or NSOC approved Security Configuration Compliance Scan must be performed on a *quarterly* basis, or when changes are made to the approved secure configuration/hardening guides.

3.2 Security Documentation Requirements

The following section provides details on each of the required security artifacts including the document requirements, references, and the parties/OIS organization(s) that can provide additional guidance for each artifact.

Templates for the applicable security artifacts/documents mentioned below are available on the OIS Portal at http://go.va.gov/plgx. To access the templates on the OIS Portal, select "Cyber Security" in the left column, then the "VA A and A Templates" folder on the right column, and then select the appropriate template from the list of available templates. Contact your ISO for questions on how to complete the documentation.

3.2.1 System Security Plan (SSP)

SSP guidance is provided below:

- The SSP is developed within RiskVision and a word document/template is no longer necessary.
- All required diagrams and confirmation of the security accreditation boundary to include all devices and supporting software architecture should be included.
- All controls must be addressed. A finding will need to be created in RiskVision for every control that is not in place.
- SSP guidance is found in NIST SP 800-18 and VA Handbook 6500.3.
- Additional guidance for completion of the SSP can be provided by OCS.

SSP completion steps:

1. The System Steward completes the assessments in RiskVision and develops findings and responses in the *Findings* tab for controls not in place.
2. The ISO validates information added by the System Steward in RiskVision.

Continuous Monitoring Requirement – The SSP must be updated on an *annual* basis or when a significant change is made to the system.

3.2.2 Signatory Authority

Signatory Authority guidance is provided below:

- The Signatory Authority must be signed and dated by the appropriate parties.
- Signatory Authority guidance can be found in NIST SP 800-18.
- Additional guidance for completion of the Signatory Authority can be provided by OCS.

Signatory Authority completion steps:

1. System Owner or delegate completes the Signatory Authority using the template provided at: http://go.va.gov/plgx.

2. System Owner 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 the SSP is updated due to a significant change.

3.2.3 Risk Assessment (RA)

RA guidance is provided below:

- The RA is developed within RiskVision and a word document/template is no longer necessary.

- RA guidance is found in NIST SP 800-30.

- Additional guidance for completion of the RA can be provided by the Office of Risk Management and Incident Reporting (RMIR)/OCS.

RA completion steps:

1. The System Steward completes the assessment in RiskVision.

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

Continuous Monitoring Requirement – The RA must be updated on an *annual* basis or when a significant change is made to the system.

3.2.4 Configuration Management Plan (CMP)

CMP guidance is provided below:

- 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 guidance can be found in NIST SP 800-70 and VA Handbook 6500.

- Additional guidance for completion of the CMP can be provided by OCS.

CMP completion steps:

1. System Owner or delegate completes the CMP using the template provided at: http://go.va.gov/plgx.
2. 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 is made to the system.

3.2.5 Incident Response Plan (IRP)

IRP guidance is provided below:

- The ISCP Assessment (ISCPA) tool will be the entry point for plan creation.
- Each site is responsible for developing local level procedures incorporating VA-NSOC areas of responsibility.
- IRP guidance can be found in NIST SP 800-61.
- Additional guidance for completion of the IRP can be provided by the Office of Business Continuity (OBC).

IRP completion steps:

1. Applicable facility/data center POCs must ensure they have completed the ISCPA training provided in TMS and by OBC.
2. Applicable facility/data center POCs complete the IRP via the ISCPA Tool.

Continuous Monitoring Requirement – The IRP must be updated on an **annual** basis or when a significant change is made.

3.2.6 Information Security Contingency Plan (ISCP)

ISCP guidance is provided below:

- The ISCP Assessment (ISCPA) tool will be the entry point for plan creation.
- The ISCPA tool will create both the facility and data center plans.
- Additional guidance for completion of the ISCP can be provided by OBC and located on the OIS Portal at: https://vaww.portal2.va.gov/sites/infosecurity/bc/default.aspx.

ISCP completion steps:

1. Applicable facility/data center POCs must ensure they have completed the ISCPA training provided in TMS and by OBC.
2. Applicable facility/data center POCs complete the ISCP via the ISCPA Tool.

Continuous Monitoring Requirement – The ISCP must be updated on an *annual* basis or when a significant change is made.

3.2.7 Disaster Recovery Plan (DRP)

DRP guidance is provided below:

- The ISCP Assessment (ISCPA) tool will be the entry point for plan creation.
- The ISCPA tool will create both the facility and data center plans.
- Additional guidance for completion of the DRP can be provided by OBC and located on the OIS Portal at: https://vaww.portal2.va.gov/sites/infosecurity/bc/default.aspx.

DRP completion steps:

1. Applicable facility/data center POCs must ensure they have completed the ISCPA training provided in TMS and by OBC.
2. Applicable facility/data center POCs completes the DRP via the ISCPA Tool.

Continuous Monitoring Requirement – The DRP must be updated on an *annual* basis or when a significant change is made.

3.2.8 Privacy Impact Assessment (PIA)

PIA guidance is provided below:

- A complete PIA must have:
    o A previously completed Privacy Threshold Analysis (PTA).
    o Been completed in the most up-to-date and Privacy Services approved template for both the PTA and PIA. The PTA and PIA template can be found at: http://go.va.gov/plgx.
    o Been completed in coordination with the VA Privacy Services Office.
    o Been signed by the System Owner, Privacy Officer, and ISO.
    o Been re-submitted whenever there are significant (major) changes to the system or within 3 years.
- Authority is found in E-Government Act of 2002, OMB Circular 03-22, VA Directive 6502, VA Directive 6508, and VA Handbook 6508.1.
- Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIASupport@va.gov.

PIA completion steps:

1. System Owner, Privacy Officer, and ISO work together to submit a PTA, which is reviewed by the Privacy Services Office.

2. After review and determination by analysts, the PTA must be signed by the System Owner, Privacy Officer, ISO, and any other relevant stakeholders and re-submitted to the Privacy Services Office via PIASupport@va.gov.

3. If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed and submitted to the Privacy Services Office and then comments by the analysts, if any, must be incorporated.

4. Once the PIA is verified as complete by Privacy Services, re-submit the PIA as a PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to PIASupport@va.gov.

5. The PIA must then be uploaded into the GRC tool as an artifact. System Owner or delegate/System Steward uploads the PIA to the **Documents** tab in RiskVision.

Continuous Monitoring Requirement – A PTA must be submitted every year. The PIA is valid for 3 years if there are no significant changes to the system.

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

ISA/MOU guidance is provided below:

- 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 provided within the MOU/ISA Field Security Service (FSS) Bulletin located at: https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/FSS%20Bulletins/124_MOU%20ISA%20Document%20Processing%20FINAL%20Guidance_080113.pdf 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, delegate or ISO will complete the ISA/MOU using the template provided at: http://go.va.gov/plgx.

2. ISO will upload all ISA/MOU documents to the following new SharePoint site for review, prior to requesting signatures: https://vaww.portal2.va.gov/sites/fss/HISD/ISAMOU/SitePages/Home2.aspx\.

3. The OIT Enterprise Risk Management (ERM) Team will review the documents against a checklist for quality and content.

4. OIT ERM and the ISO will work collaboratively to correct deficiencies found in the documentation.

5. OIT ERM will return the document to the ISO informing them it is ready for signatures.

6. ISO will submit the document for signature and return to the ISA/MOU Review Submission SharePoint to enter the date the document was sent for signature.

7. Upon receipt of the completed (all signatures received) ISA/MOU document, the ISO will return for one final time to the SharePoint site and update the original entry by placing a date in the Final Approval Received field.

Continuous Monitoring Requirement – The ISA/MOU must be completed on an ***annual*** basis or when a significant change is made to the system.

3.2.10   RBD Process

Note: RBD materials are located on the OIS Portal at: https://vaww.portal2.va.gov/sites/infosecurity/ca/VA_6500_Waiver.aspx. Approved RBDs must be uploaded to the ***Documents*** tab in RiskVision by the System Owner or delegate/System Steward.

- Local RBD: The System Owner has the flexibility to not implement a security control based on the system's specific environment or technical requirements.
    - Develop RBD Memorandum to describe justification why a security control is not implemented.
    - System Owner signs memorandum and uploads it to RiskVision.

- OIS/National RBD: The System Owner will provide justification as to why a common control or hybrid control cannot be implemented and include a recommended action including any compensating controls.
    - Complete OIS/National RBD Memorandum template to describe justification as to why a common control or hybrid control is not implemented.
    - System Owner signs memorandum.
    - System Owner coordinates with ISO to have the Deputy Assistant Secretary, Information Security review and sign the memorandum.
    - System Owner or delegate/System Steward uploads the signed memorandum to RiskVision.

3.3 Closing

Once all of the above requirements are either met or deemed inappropriate by OIS, the completed package will be submitted to the DAA by OCS/CA with one of the following three recommendations:

- Denial of ATO (DATO) – An accreditation decision allowing the authority to halt an existing operational or new system because unacceptable security risks exist.

- Temporary ATO (TATO) with Conditions – An accreditation decision authorizing a system to temporarily operate for a set amount of time while certain terms and conditions must be met.

- ATO – An accreditation decision authorizing a system to operate.

Appendix A – Accreditation Requirements Quick Reference Guide

Accreditation Requirements		
Requirement	**Roles / Responsibilities**	**References**
Technical/Testing Requirements		
Nessus Scan • A credentialed vulnerability scan against all instantiations of the operating system and desktop configurations must be conducted to identify security flaws. • When conducting the Nessus Scan, a discovery scan (a discovery scan will not enumerate any vulnerabilities) must be conducted as a part of the vulnerability scan. • Actual scan results must be provided for analysis. • 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.	• <u>System Owner or delegate</u> contacts CPO at CertificationPMO@va.gov to request system scan from NSOC. System Owner or delegate can contact NSOC with the applicable form(s) instead of reaching out to CPO, if preferred. • <u>NSOC</u> conducts scans and provides results to system POCs. • <u>System Owner or delegate</u> is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the scan results to RiskVision under Entity Details: Documents tab. • <u>System Owner or delegate</u> creates one finding and a response in the Findings tab within RiskVision for the Nessus scan to serve as a reminder to resolve the deficiencies.	• Contact the Office of Cyber Security (OCS) at: CertificationPMO@va.gov and/or NSOC with any questions
Code Review • Code reviews of custom developed VA applications using the current approved VA static code analysis tool should be conducted to identify security 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 or testing with other applicable tools (notify OCS if this is the case). • 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.	• <u>System Owner or delegate</u> contacts the Product Development (PD) Fortify Support Team at FORTIFY@va.gov and Cc Julie Harvey (PD) at Julie.Harvey@va.gov and requests a Fortify license. • Once license is received, the <u>System Owner or delegate</u> conducts the initial Fortify scan and provides the test result files (such as the Fortify Project or .fpr files), along with the complete and buildable source code for the inventoried applications for independent source code review and analysis to the <u>OCS Software Assurance Team</u> at OISSwASupportGroup@va.gov. • <u>System Owner or delegate</u> is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the code review results to RiskVision under Entity Details: Documents tab.	• Contact the OCS Software Assurance Team at OISSwASupportGroup@va.gov with any questions

☐		• System Owner or delegate creates one finding and a response in the Findings tab within RiskVision for the Code Review to serve as a reminder to resolve the deficiencies.	
☐	**Penetration Test/Application Assessment** • A full penetration test/application assessment must be performed that includes automated and manual assessment tools and techniques on *Internet Facing and/or High Impact Applications*. • Actual test results must be provided for analysis. • 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.	• System Owner or delegate contacts CPO at CertificationPMO@va.gov to request penetration test/application assessment from NSOC. System Owner or delegate can also contact NSOC with the applicable form(s) instead of reaching out to CPO, if preferred. • NSOC conducts penetration test/application assessment and provides results to system POCs. *Please allow 30 days for NSOC to schedule/conduct the penetration test/application assessment.* • System Owner or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the test results to RiskVision under Entity Details: Documents tab. • System Owner or delegate creates one finding and a response in the Findings tab within RiskVision for the penetration test/application assessment to serve as a reminder to resolve the deficiencies.	• Contact OCS at: CertificationPMO@va.gov and/or NSOC with any questions
☐	**Security Control Assessment (SCA)** *(if applicable)* • An SCA will be required only upon request from OCS. • If an SCA is required, all Critical and High POA&Ms should be mitigated with documented mitigation evidence provided, and Moderate and Low POA&Ms should be mitigated or have a documented mitigation plan.	• OIT Enterprise Risk Management (ERM) will be notified by OCS to schedule and conduct the SCA, and will provide the results to the system POCs once the SCA is completed. • System Owner or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them along with the test results to RiskVision under Entity Details: Documents tab. • System Owner or delegate creates one finding and a response in the Findings tab within RiskVision for the SCA to serve as a reminder to resolve the deficiencies.	• Contact OCS at: CertificationPMO@va.gov and/or OIT ERM
☐	**Security Configuration Compliance Scan** • Compliance scans must be performed against all Windows hosts (NSOC only has Windows Compliance scan capabilities) and must check against VA approved hardening guidance for all Operating Systems, Databases, Networks, and	• System Owner or delegate contacts CPO at CertificationPMO@va.gov to request system scan from NSOC. System Owner or delegate can also contact NSOC with the applicable form(s) instead of reaching out to CPO if preferred. • NSOC conducts scans and provides results to system	• Contact OCS at: CertificationPMO@va.gov and/or NSOC with any questions

Requirement	Roles / Responsibilities	References
Security Devices, where guidance exists. • Operating Systems (DISA STIG, NIST USGCB, Microsoft) • Databases (DISA STIG, NIST USGCB, Microsoft) • Network / Security Devices (NSA SNAC Configuration Guides) • All compliance scans with failing results should have a documented mitigation plan.	POCs. • System Owner or delegate is responsible for coordinating the mitigation of deficiencies, documenting the mitigation plans, and uploading them to RiskVision under Entity Details: Documents tab, along with the scan results. • System Owner or delegate creates one finding and a response in the Findings tab within RiskVision for the security configuration compliance scan to serve as a reminder to resolve the deficiencies.	
Requirement	**Roles / Responsibilities**	**References**
Security Documentation Requirements		
System Security Plan (SSP) • The SSP is developed within RiskVision. • All required diagrams, and confirmation of the security accreditation boundary to include all devices and supporting software architecture should be included. • All controls must be addressed. A finding will need to be created in RiskVision for every control that is not in place.	• System Steward completes the assessments in RiskVision and develops findings and responses in the *Findings* tab for controls not in place. • ISO validates information added by the System Steward in RiskVision.	• NIST SP 800-18 and VA Handbook 6500.3 • Additional guidance for completion of the SSP can be provided by OCS
Signatory Authority • The Signatory Authority must be signed and dated by the appropriate parties.	• System Owner or delegate completes the Signatory Authority using the template provided at: http://go.va.gov/plgx and uploads the Signatory Authority to RiskVision under Entity Details: Documents tab.	• NIST SP 800-18 • Additional guidance for completion of the Signatory Authority can be provided by OCS
Risk Assessment (RA) • The RA is developed within RiskVision.	• System Steward completes the assessments in RiskVision. • ISO validates information added by the System Steward in RiskVision.	• NIST SP 800-30 • Additional guidance for completion of the RA can be provided by the Office of Risk Management and Incident Reporting (RMIR)/OCS
Configuration Management Plan (CMP) • The CMP should include processes for managing configuration and change management. • The CMP should include infrastructure devices and	• System Owner or delegate completes the CMP using the template provided at: http://go.va.gov/plgx and uploads the CMP as evidence to RiskVision under Entity Details: Documents tab.	• NIST SP 800-70 and VA Handbook 6500 • Additional guidance for completion of the CMP can

	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.		be provided by OCS
☐	**Incident Response Plan (IRP)** • The ISCP Assessment (ISCPA) tool will be the entry point for plan creation. • Each site is responsible for developing local level procedures incorporating VA-NSOC areas of responsibility.	• <u>Applicable facility / data center POCs</u> must ensure they have completed the ISCPA training provided in TMS and by OBC and can then complete the IRP via the ISCPA Tool.	• NIST SP 800-61 • Additional guidance for completion of the IRP can be provided by the Office of Business Continuity (OBC)
☐	**Information Security Contingency Plan (ISCP)** • The ISCPA tool will be the entry point for plan creation. • The ISCPA tool will create both the facility and data center plans.	• <u>Applicable facility / data center POCs</u> must ensure they have completed the ISCPA training provided in TMS and by OBC and can then complete the ISCP via the ISCPA Tool.	• Additional guidance for completion of the ISCP can be provided by OBC and located on the OIS Portal at: https://vaww.portal2.va.gov/sites/infosecurity/bc/default.aspx
☐	**Disaster Recovery Plan (DRP)** • The ISCPA tool will be the entry point for plan creation. • The ISCPA tool will create both the facility and data center plans.	• <u>Applicable facility / data center POCs</u> must ensure they have completed the ISCPA training provided in TMS and by OBC and can then complete the DRP via the ISCPA Tool.	• Additional guidance for completion of the DRP can be provided by OBC and located on the OIS Portal at: https://vaww.portal2.va.gov/sites/infosecurity/bc/default.aspx

OFFICE OF INFORMATION SECURITY

☐	**Privacy Impact Assessment (PIA)**
	• A complete PIA must have:
	  • A previously completed Privacy Threshold Analysis (PTA).
	  • Been completed in the most up-to-date and Privacy Services approved template for both the PTA and PIA. The PTA and PIA template can be found at: http://go.va.gov/plgx.
	  • Been completed in coordination with the VA Privacy Services Office.
	  • Been signed by the System Owner, Privacy Officer, and ISO.
	  • Been re-submitted whenever there are major changes to the system or within 3 years.
		• System Owner, Privacy Officer, and ISO work together to submit a PTA, which is reviewed by the Privacy Services Office. After review and determination by analysts, the PTA must be signed by the System Owner, Privacy Officer, ISO, and any other relevant stakeholders and re-submitted to the Privacy Services Office via PIASupport@va.gov. If a PIA is required as an outcome of the PTA analysis by the Privacy Services Office, a PIA must be completed and submitted to the Privacy Services Office and then comments by the analysts, if any, must be incorporated.
		• Privacy Services verifies PIA and provides results.
		• System Owner or delegate re-submits the PIA as a PDF file with the signatures of the System Owner, Privacy Officer, ISO, and any other relevant stakeholders to PIASupport@va.gov.
		• System Owner or delegate uploads the PIA to RiskVision under Entity Details: Documents tab.
			• Authority is found in E-Government Act of 2002, OMB Circular 03-22, VA Directive 6502, VA Directive 6508, and VA Handbook 6508.1
			• Additional guidance for completion of the PIA/PTA can be provided by the Privacy Services Office. Any questions may be sent to PIASupport@va.gov

☐	**Interconnection Security Agreement (ISA)/ Memorandum of Understanding (MOU)** • An ISA/MOU must be provided for all external interconnections.	• System Owner or delegate or ISO will complete the ISA/MOU using the template provided at: http://go.va.gov/plgx. • ISO will upload all ISA/MOU documents to the following new SharePoint site for a review, prior to requesting signatures: https://vaww.portal2.va.gov/sites/fss/HISD/ISAMOU/SitePages/Home2.aspx\. • OIT Enterprise Risk Management (ERM) Team will review the documents against a checklist for quality and content. OIT ERM and ISO will work collaboratively to correct deficiencies found in the documentation. OIT ERM will return the document to the ISO informing them it is ready for signatures. • ISO will submit the document for signature and return to the ISA/MOU Review Submission SharePoint site and enter the date the document was sent for signature. Upon receipt of the completed (all signatures received) ISA/MOU document, the ISO will return for one final time to the SharePoint site and update the original entry	• NIST SP 800-47 and VA Handbook 6500 • Additional guidance for completion of the ISA/MOU can be provided within the MOU/ISA Field Security Service (FSS) Bulletin located at: https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/FSS%20Bulletins/124_MOU%20ISA%20Document%20Processing%20FINAL%20Guidance_080113.pdf • Additional guidance can be provided by the Health Information Security Division at vafsshisd@va.gov or the OIT ERM CRISP Team at

		by placing a date in the Final Approval Received field.	Sharon.mcallister@va.gov

Appendix B – Accreditation Flowchart

Accreditation Process Flow

Accreditation Prerequisites

Start Process

Is an ISO assigned to the system? —No→ System Owner contacts FSS* and completes the VA ISO Support Request Form

↓ Yes

System Owner contacts RiskVision Working Group** for system addition to the tool and RiskVision access

System Owner contacts the Certification Program Office (CPO)*** to determine applicability of accreditation requirements

* VAFSSISORequests@va.gov
** VARiskVisionWG@va.gov
*** CertificationPMO@va.gov

Documentation Requirements

System Steward completes the SSP, develops a finding for each control not in place, and completes the RA all in RiskVision

ISO validates information added by the System Steward in RiskVision

System Owner or delegate completes Signatory Authority, CMP, PIA, and ISA/MOU (if applicable) and uploads the documentation as evidence to the '1-3 VA System Documentation' question in RiskVision; and the applicable facility / data center POCs complete the IRP, ISCP, and DRP in the ISCP Assessment (ISCPA) tool and uploads the documentation as evidence to the '1-3 VA System Documentation' question in RiskVision

Technical / Testing Requirements

System Owner works with CPO* to initiate Nessus scan and NSOC to perform the Nessus scan. Upload results to RiskVision

System Owner works with CPO* to initiate Security Configuration Compliance scan and NSOC to perform the Compliance scan. Upload results to RiskVision

Is the system a custom developed VA application? —Yes→ System Owner requests Fortify license for Code Review**. Upload results to RiskVision

↓ No

Is the system a High impact or internet facing system? —Yes→ System Owner works with CPO* to initiate Pen Test/ Application Assessment and NSOC to perform the test. Upload results to RiskVision

↓ No

Did OCS require a Security Control Assessment (SCA)? —Yes→ System Owner works with CPO and ERM to schedule and conduct SCA. Upload results to RiskVision

↓ No

Did the technical/testing requirement identify deficiencies? —Yes→ Develop mitigation plan*** and upload to Documents tab in RiskVision

Accreditation Package submitted for ATO decision in RiskVision

* CertificationPMO@va.gov
** FORTIFY@va.gov, cc: Julie.Harvey@va.gov
*** Mitigation template found at: http://go.va.gov/plgx