ATTACHMENT B - ATO Requirements

The Office of Cyber Security (OCS) offers comprehensive guidance and support services to facilitate the Assessment and Authorization (A&A) of VA systems. Proper planning and implementation of the A&A process ensures that applicable security requirements are integrated into development and operational processes to safeguard veterans' information.

All VA systems that require A&A must meet the following requirements prior to Authority to Operate (ATO) determination.

ATO Requirements	
Technical / Testing Requirements	

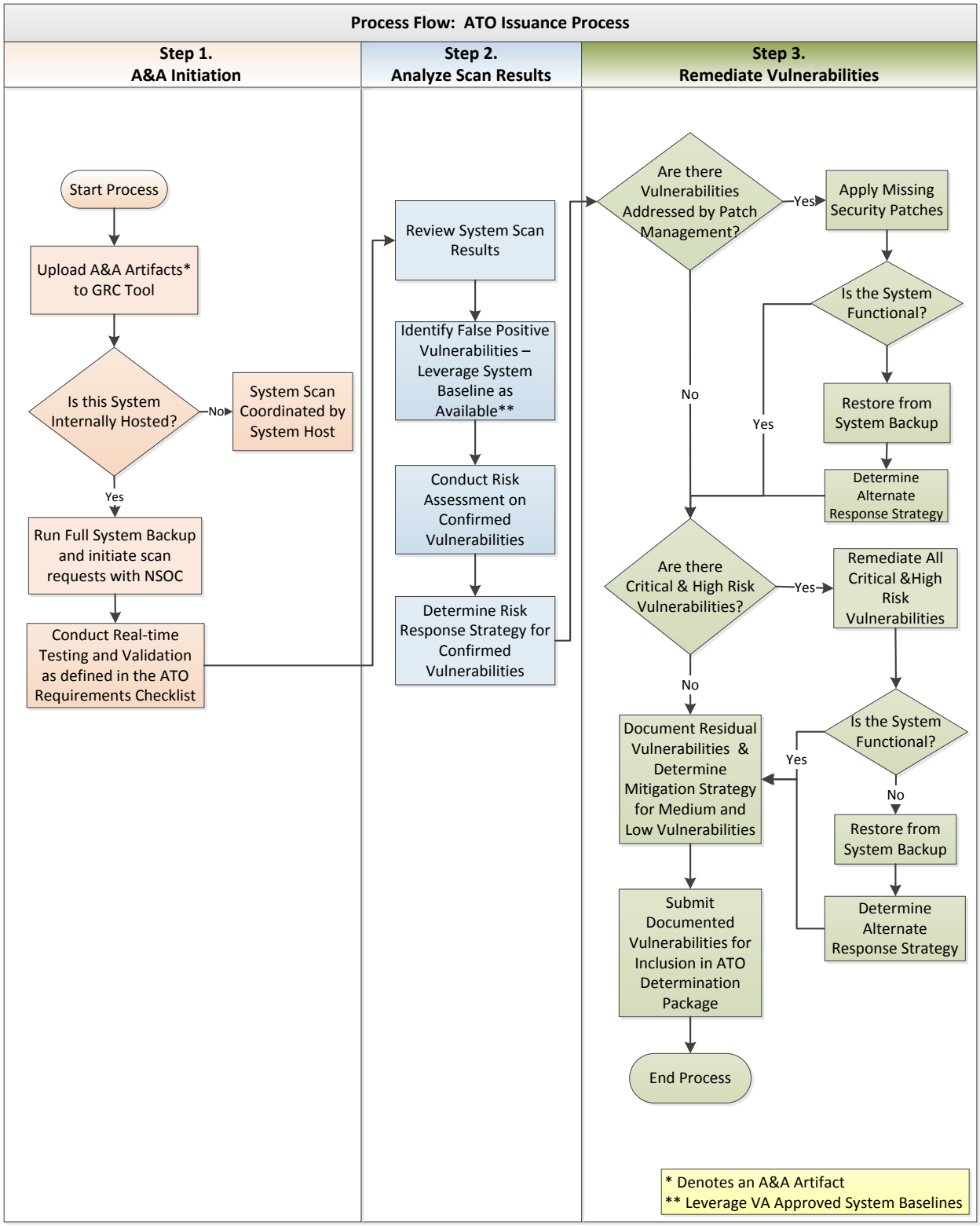
☐	**Baseline Platform Image**
	• For each host, there must be an approved baseline platform (operating system, database, etc.) image installed
	• Platforms should be limited to one baseline build. Any exceptions must be documented and approved
	• All baseline image builds must be configured using approved hardening guidance for the following:
	  ○ Operating Systems (DISA STIG, NIST USGCB, Microsoft)
	  ○ Databases (DISA STIG, NIST USGCB, Microsoft)
	  ○ Network Devices (NSA SNAC Configuration Guides)
	• Baseline image must be managed through the Change Management process with changes approved through a Change Control Board

☐	**Nmap Scan** • A network discovery scan must be conducted to include all IP addresses within the system boundary mapped back to specific components within the system architecture • Actual scan results must be provided for analysis
☐	**Tenable Nessus Scan** • A vulnerability scan against all instantiations of the operating system must be conducted to identify security flaws • Actual scan results must be provided for analysis • All vulnerability scans that identify Critical and/or High findings should be remediated or have a documented mitigation plan
☐	**HP Fortify Static Code Analyzer** • A Fortify Static Code Analyzer must be conducted to identify security vulnerabilities, coding, and design flaws within applications • Actual scan results must be provided for analysis • All terminal findings (e.g., STIG Cat I/II, Fortify Critical/High, OWASP) must be remediated

☐	**Security Configuration Compliance Scan**
	• Compliance scans must check against approved hardening guidance for the following:
	  ○ Operating Systems (DISA STIG, NIST USGCB, Microsoft)
	  ○ Databases (DISA STIG, NIST USGCB, Microsoft)
	  ○ Network Devices (NSA SNAC Configuration Guides)
	• Actual scan results must be provided for analysis
	• A compliance scan using an SCAP validated scanning tool must be conducted with a passing result (> 80% compliant)
	• All compliance scans with failing results should have a documented mitigation plan

☐	**Application Assessment / Pen Test** • Full application assessment or penetration test must be performed that includes automated & manual assessment tools and techniques • An IBM App Scan should be performed against all web applications to identify security vulnerabilities • Actual scan results must be provided for analysis • All Critical and/or High findings should be remediated or have a documented mitigation plan
Documentation Requirements	

☐	**System Security Plan (SSP)** • The SSP must include a network diagram and confirmation of the security accreditation boundary to include all devices and supporting software architecture • The SSP will be generated through the Agiliance RiskVision OpenGRC tool • Guidance is found in NIST SP 800-18 • The SSP is authored locally, but may contain inserts that are inherited, National or Common, in nature • The SSP template is available on the OIS Portal
☐	**Risk Assessment (RA)** • The RA will be generated through the Agiliance RiskVision OpenGRC tool • Guidance is found in NIST SP 800-30 • The RA template is available on the OIS Portal
☐	**Configuration Management Plan (CMP)** • 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 • Guidance is found in NIST SP 800-70 and VA Handbook 6500 • Inclusion of a CMP as a separate document is required for all VA systems per VA Handbook 6500 • The CMP template is available on the OIS Portal
☐	**Incident Response Plan (IRP)** • Guidance is found in NIST SP 800-61 and VA Handbook 6500.2 • Inclusion of an IRP as a separate document is required for all VA systems per VA Handbook 6500 • VA-NSOC is responsible for National level tasks associated with incident response. Each site is responsible for developing local level procedures incorporating VA-NSOC areas or responsibility • The IRP template is available on the OIS Portal
☐	**Signatory Authority** • Guidance is found in NIST SP 800-18 • All package submissions must include this document signed and dated by the appropriate parties • The Signatory Authority template is available on the OIS Portal
☐	**Information Security Contingency Plan (ISCP)** • Guidance is found in NIST SP 800-34 and VA Handbook 6500.8 • Inclusion of an ISCP as a separate document is required for all VA systems per VA Handbook 6500 • The ISCP template is available on the OIS Portal
☐	**Privacy Impact Assessment (PIA)** • Authority is found in OMB Circular 03-22 • The VA requires that Operating Units conduct a PIA on applicable systems – VA Handbook 6500 • The PIA template is available on the OIS Portal
☐	**Interconnection Security Agreement (ISA) / Memorandum of Understanding (MOU) (if applicable)** • Guidance is found in NIST SP 800-47 and VA Handbook 6500 • Inclusion of ISAs / MOUs as separate documents is required for all VA systems per VA Handbook 6500 • The ISA and MOU templates are available on the OIS Portal
☐	**Security Configuration Checklists** • Guidance is found in NIST SP 800-70 • This document is a product of the CMP and lists the security configurations that are required for the devices within the boundary of the system • The Security Configuration Checklist template is available on the OIS Portal
☐	**Disaster Recovery Plan (DRP)** • Guidance is found in NIST SP 800-34 and VA Handbook 6500.8 • Inclusion of a DRP as a separate document is required for all VA systems per VA Handbook 6500 • The DRP template is available on the OIS Portal
☐	**Change Management Waiver (if applicable)** • Deviations from approved configuration baselines need to be justified in a waiver
☐	**Remediation Evidence / Mitigation Plans** • All Critical and High risk POA&Ms / vulnerabilities must be remediated with supporting evidence of the remediation efforts • POA&Ms as a result of the SCA and Technical Scans must have a mitigation plan and/or remediation evidence


Process Flow: ATO Issuance Process
Step 1.
A&A Initiation
Step 2.
Analyze Scan Results
Step 3.
Remediate Vulnerabilities
Start Process
Upload A&A Artifacts* to GRC Tool
Is this System Internally Hosted?
No
System Scan Coordinated by System Host
Yes
Run Full System Backup and initiate scan requests with NSOC
Conduct Real-time Testing and Validation as defined in the ATO Requirements Checklist
Review System Scan Results
Identify False Positive Vulnerabilities – Leverage System Baseline as Available**
Conduct Risk Assessment on Confirmed Vulnerabilities
Determine Risk Response Strategy for Confirmed Vulnerabilities
Are there Vulnerabilities Addressed by Patch Management?
Yes
Apply Missing Security Patches
Is the System Functional?
Yes
Restore from System Backup
Determine Alternate Response Strategy
No
Are there Critical & High Risk Vulnerabilities?
Yes
Remediate All Critical &High Risk Vulnerabilities
Is the System Functional?
Yes
No
Restore from System Backup
Determine Alternate Response Strategy
No
Document Residual Vulnerabilities & Determine Mitigation Strategy for Medium and Low Vulnerabilities
Submit Documented Vulnerabilities for Inclusion in ATO Determination Package
End Process
* Denotes an A&A Artifact
** Leverage VA Approved System Baselines