DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6500.3
Transmittal Sheet
February 3, 2014

ASSESSMENT, AUTHORIZATION, AND CONTINUOUS MONITORING OF VA INFORMATION SYSTEMS

1. REASON FOR ISSUE: To establish requirements and responsibilities for the Department of Veterans Affairs (VA) to ensure compliance with Assessment and Authorization (A&A) and continuous monitoring requirements for VA information systems as required by the Federal Information Security Management Act of 2002 (FISMA); Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; VA Directive 6500, *Managing Information Security Risk: VA Information Security Program;* and VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program.*

2. SUMMARY OF CONTENTS/MAJOR CHANGES: The enterprise level A&A policy is located in VA Directive and Handbook 6500. This Handbook provides further details for the implementation of A&A in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* In addition, this Handbook provides the framework for VA's Information Security Continuous Monitoring (ISCM) program in accordance with NIST SP 800-37 and NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations.*

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OIT) (005), Information Security (005R), Office of Cyber Security (OCS) (005R2), is responsible for the content of this Handbook.

4. RELATED DIRECTIVE: VA Directive and Handbook 6500

5. RESCISSIONS: VA Handbook 6500.3, *Certification and Accreditation of VA Information Systems*, November 24, 2008.

CERTIFIED BY: BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Stephen W. Warren
Executive in Charge and Chief Information
Officer for Information and Technology

/s/
Stephen W. Warren
Executive in Charge and Chief Information
Officer for Information and Technology

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

ASSESSMENT, AUTHROIZATION, AND CONTINUOUS MONITORING OF VA INFORMATION SYSTEMS

CONTENTS

PARAGRAPH PAGE

ASSESSMENT, AUTHROIZATION, AND CONTINUOUS MONITORING OF VA INFORMATION SYSTEMS

CONTENTS, cont.

APPENDICIES **PAGE**

TABLES **PAGE**

ASSESSMENT, AUTHORIZATION, AND CONTINUOUS MONITORING OF VA INFORMATION SYSTEMS

1. PURPOSE

a. The Department of Veterans Affairs (VA) Directive 6500, Managing Information Security Risk: VA Information Security Program and VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3, VA Information Security Program provide the highest level of policy to ensure VA information systems adhere to and are in compliance with established Federal laws and regulations.

b. This Handbook provides the next level of policy to establish requirements and responsibilities for Assessment and Authorization (A&A) and to establish VA's Information Security Continuous Monitoring (ISCM) program. Additional procedures for A&A and the ISCM program will be distributed by the Office of Information and Technology (OIT).

c. This Handbook is in accordance with Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, Appendix III, and applicable National Institute of Standards and Technology (NIST) Special Publications (SP).

d. This Handbook is designed to include a complete overview of A&A and ISCM to provide specific, consistent policy throughout VA. The intent of this Handbook is to inform readers on A&A and ISCM, specifically:

(1) The requirements of the A&A and ISCM processes;

(2) Which individuals are responsible for specific tasks; and

(3) How other information technology (IT) security activities relate to and/or interact with the A&A and ISCM processes.

2. SCOPE/OVERVIEW

a. Applicability

(1) The policies stated in this Handbook apply to all individuals (VA employees, contractors, researchers, students, volunteers, representatives of Federal, state, local, or tribal agencies, and any others not specifically mentioned in this list) involved in, or in support of, A&A or the ISCM program.

(2) The requirements for A&A apply to information systems used or operated by or on behalf of VA and could include non-VA owned systems storing or processing VA data.

(3) Failure to maintain compliance with A&A and ISCM requirements described in this Handbook may result in denial or revocation of a system's authorization to operate.

b. A&A Background

(1) A&A as it relates to the Risk Management Framework (RMF)

(a) VA has implemented a three-tier approach to risk management, as described in VA Directive and Handbook 6500. Tier 1 addresses risk from a VA perspective, Tier 2 addresses risk from a mission/business process perspective, and Tier 3 addresses risk from the system level through the RMF. VA's adoption of the RMF is addressed in VA Directive and Handbook 6500.

(b) A&A is a dynamic approach to effectively managing information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. The A&A process is an integral part of the NIST-developed six-step RMF, which operates primarily at Tier 3 and promotes a common information security framework for information systems for the Federal government and its contractors.

(c) The six steps of the RMF are:

1. Categorize the information system;

2. Select the security controls;

3. Implement the security controls;

4. Assess the security controls;

5. Authorize the information system; and

6. Monitor the security controls.

(d) The RMF steps of Step 1 – Categorize the Information System, Step 2 – Select the Security Controls, and Step 3 – Implement the Security Controls must be completed before a system enters the A&A process. Step 4 – Assess the Security Controls and Step 5 – Authorize the Information System are central to the A&A process. Step 6 – Monitor the Security Controls is part of the ISCM program, described in the next section. Steps 4, 5, and 6 are the focus of this Handbook. Steps 1, 2, and 3 are described in detail in VA Handbook 6500.

(e) Information systems used or operated by, or on behalf of, VA must be authorized to operate. This authorization is achieved through the process addressed in this Handbook and through this process the system will receive an authority to operate (ATO) or a denial of ATO.

(f) Risk management tasks, including A&A, are performed prior to placing the information system into operation and as part of the information system's continued operation. Performance of the risk management tasks ensures that:

1. Information system-related security risks are being adequately addressed on an ongoing basis; and

2. The Authorizing Official (AO), identified in VA as the Assistant Secretary for Information and Technology and Chief Information Officer (CIO), explicitly understands and accepts the risk to VA operations and assets, individuals, other organizations, and the Nation based on the implementation of a defined set of security controls and the current security state of the information system.

(2) A&A as it relates to the System Development Life Cycle (SDLC)

(a) In accordance with the provisions set forth by FISMA, VA is required to have a VA-wide information security program, which is effectively integrated into VA's business processes and especially into the overall SDLC of every VA IT system.

(b) RMF tasks are executed concurrently with or as a part of SDLC processes to help ensure VA effectively integrates the process of managing information system-related risks with SDLC processes. The SDLC, as developed in NIST SP 800-series and VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle, is a multi-step process specifically focused on implementation of security protections across the life cycle of information systems.

(c) All information systems are in one of the five phases of the SDLC as described in VA Handbook 6500.5:

1. Initiation;

2. Acquisition and Development;

3. Implementation and Assessment;

4. Operations and Maintenance; and

5. Disposal.

(d) The RMF steps of Step 4 – Assess the Security Controls and Step 5 – Authorize the Information System occur primarily in the SDLC phases of Acquisition and Development and Implementation and Assessment. Consistent with a lifecycle approach, assessment requirements should be considered from Initiation through Disposal.

(e) Assessing security controls as early as practicable in the SDLC permits the identification of weaknesses and deficiencies early, validates that controls are implemented correctly and provides the most cost effective method for implementing the system, managing the system, and initiating corrective actions.

(f) For new systems in the Initiation and Acquisition and Development phases, Project Managers are responsible for ensuring that systems receive authorization prior to operational deployment when responsibility for A&A activities shifts to the System Owner. For existing systems, System Owners are responsible for ensuring that the systems for which they are responsible maintain authorization.

(3) A&A as it relates to mission and business processes

(a) Authorization decisions are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business functions.

(b) The authorization package will include information regarding the core mission and business requirements supported by the system and the impact of the system on mission and business operations to be considered by the AO in the authorization decision.

(c) The RMF provides a disciplined and structured process that integrates information security and risk management activities into the SDLC. Through application of the RMF, VA achieves risk-based security that supports organizational mission/business needs. Consideration of the organizational mission, business, and operational requirements and the impact of security decisions on mission and business functions is a part of risk management.

(d) Information security risks are managed consistently across the organization, reflect VA's risk tolerance, and are considered along with other organizational risks affecting mission and business success.

c. ISCM Background

(1) VA will implement an ISCM program to ensure that deployed security controls continue to be effective and that operations remain within stated organization risk tolerance in light of inevitable changes that occur over time.

(2) At Tier 3, ISCM activities address risk management from an information system perspective, including ensuring controls are implemented correctly, operating as intended, producing the desired results, and continuing to be effective in support of ongoing authorization decisions.

(3) At Tier 3, RMF Step 6 – Monitor the Security Controls, the monitoring activities are aligned with the ISCM program and the continuous monitoring supports ongoing authorization of VA information systems.

(4) ISCM activities occur primarily in the SDLC phase of Operations and Maintenance.

3. RESPONSIBILITIES

The responsibilities listed below are specific responsibilities related to A&A and ISCM. For overall information security program responsibilities for these positions, see VA Directive and Handbook 6500.

a. **Assistant Secretary for Information and Technology**, as VA CIO, is responsible for:

(1) Assuming the responsibility as the AO to ensure that systems operate at an acceptable level of risk. The AO is authorized to assume the responsibility and accountability for operating an information system at an acceptable level of risk. The only activity that cannot be delegated by the AO to the Authorizing Official Designated Representative (AODR) is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to VA operations and assets, individuals, other organizations, and the Nation). The AO is responsible for:

(a) Assuming formal responsibility and accountability for the risks associated with operating an information system;

(b) Overseeing budget and business operations of the information system within VA;

(c) Determining the risk to organizational operations (including VA mission, business functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation;

(d) Reviewing and approving the System Security Plan (SSP), memorandums of understanding or agreement (MOU/A), and plan of action and milestones (POA&M) for the information system;

(e) Determining the necessary level of Security Control Assessor independence for security control assessments (SCA);

(f) Determining the acceptability of the residual risk to VA operations and assets, individuals, other organizations, and the Nation based on information generated during the security assessment;

(g) Issuing an ATO for an information system if risks are acceptable and setting any terms and conditions associated with the ATO, if necessary;

(h) Denying an ATO for an information system, or if the system is already operational, halting operations after consulting with the System Owner if unacceptable security risks exist;

(i) Ensuring that all activities and functions associated with security authorizations that are delegated to AODR are carried out; and

(j) Assuming responsibility for ensuring the organization’s ISCM program is applied with respect to a given information system.

(2) Receiving notification of continuous monitoring results which indicate a significant change to the information system or major change to the data collected and maintained to determine if reauthorization is required;

(3) Ensuring the security posture of the information system is maintained, reviewing security status reports and critical security documents, and determining if risk to the organization from the operation of the information system remains acceptable;

(4) Designating a chief information security officer (CISO);

(5) Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;

(6) Overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained;

(7) Assisting senior VA officials concerning their security responsibilities;

(8) Coordinating with other senior officials to report annually to the head of VA on the overall effectiveness of VA's information security program, including progress of remedial actions;

(9) Coordinating with the CISO to ensure:

(a) A VA-wide information security program is effectively implemented resulting in adequate security for all VA information systems and environments of operation for those systems;

(b) Information security considerations are integrated into the programming, planning, and budgeting cycles, Enterprise Architecture, acquisition life cycle, and SDLC;

(c) Information systems are covered by approved security plans and are authorized to operate;

(d) Information security-related activities required across VA are accomplished in an efficient, cost-effective, and timely manner; and

(e) Centralized reporting of appropriate information security-related activities is available;

(10) Determining the appropriate allocation of resources dedicated to the protection of information systems; and

(11) Leading the organization's ISCM program, establishing expectations and requirements for the program.

b. **Deputy Assistant Secretary (DAS) for Information Security** is responsible for:

(1) Serving as the CISO for VA;

(2) Assuming the responsibility of AODR for VA. The AODR can be empowered by the AO to perform the following:

(a) Acting on the AO's behalf in coordinating and performing the necessary activities required for the A&A process of an information system;

(b) Interacting with the System Owner, Project Manager, Information Security Officer (ISO), Security Control Assessors, and other interested parties during the A&A process;

(c) Reviewing all final authorization packages to determine risk to organizational operations (including VA mission, business functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation and making a decision recommendation to the AO to issue an ATO or denial of ATO and recommending any necessary terms and conditions for an ATO;

(d) Checking with the AO to determine if the AO will be empowering the AODR to perform the following:

1. Making decisions with regard to the planning and resources of the A&A activities;

2. Accepting and approving SSPs and SCA plans;

3. Approval and monitoring the implementation of the POA&M; and

4. Assessment and/or determination of risk.

(e) Assisting the AO by recommending a system's operational risk determination.

(3) Carrying out the VA CIO security responsibilities under FISMA;

(4) Establishing, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements related to A&A and continuous monitoring as elements of the Department information security program and ensuring that these elements of the security program are consistently applied across the organization;

(5) Serving as the primary liaison for the VA CIO (AO) to the Information System Owners, Project Managers, and ISOs and, if appropriate, Administration or Program Office officials during the A&A process;

(6) Heading an office with the mission and resources to assist VA in achieving more secure information and information systems in accordance with the requirements in FISMA;

(7) Coordinating privacy-related issues/activities associated with A&A activities;

(8) Developing configuration management guidance for the organization;

(9) Consolidating and analyzing POA&Ms to determine security weaknesses and deficiencies;

(10) Ensuring that risk-related considerations, to include authorization decisions, are viewed from a VA-wide perspective with regard to the overall strategic goals and objectives of VA in carrying out its core missions and business functions;

(11) Ensuring management of information system-related security risk is consistent across VA, reflects VA risk tolerance, and is considered along with other types of risks in order to ensure mission/business success;

(12) Developing an information security risk management strategy for VA providing a strategic view of information security-related risks with regard to VA as a whole, including consideration of the impact on mission and business processes;

(13) Facilitating the sharing of information security risk-related information among the AO and senior VA officials;

(14) Providing oversight for all information security risk management-related activities across VA (e.g., security categorizations of systems) to help ensure consistent and effective risk acceptance decisions;

(15) Ensuring that information regarding the factors necessary for mission and business success are made available for authorization and continuous monitoring decisions;

(16) Providing a VA-wide forum to consider all sources of information security risk (including aggregated risk) to VA operations and assets, individuals, other organizations, and the Nation;

(17) Identifying VA’s risk posture based on the aggregated risk to information from the operation and use of the information systems for which VA is responsible;

(18) Overseeing VA’s ISCM strategy and program;

(19) Establishing, implementing, and maintaining the organization’s ISCM program;

(20) Developing organizational procedures for ISCM of the security program and information systems;

(21) Acquiring or developing and maintaining automated tools to support ISCM and ongoing authorizations;

(22) Ensuring ISCM reports are monitored and events and issues are escalated for appropriate action in accordance with organizational risk tolerance;

(23) Reviewing reports from the ISCM process as input to information security risk posture and risk tolerance decisions; and

(24) Providing support to those with security relevant activities for ISCM and A&A on how to implement ISCM and A&A for their information systems and providing training on the organization's ISCM and A&A program.

c. **Deputy CIO for Architecture, Strategy, and Design** is responsible for:

(1) Ensuring that the information security requirements necessary to protect VA's core missions and business processes are adequately addressed in all aspects of Enterprise Architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes; and

(2) Advising the AO and CISO on security-related issues related to the Enterprise Architecture.

d. **Deputy CIO for Product Development** is responsible for conducting information system security engineering activities. The Deputy CIO for Product Development is responsible for:

(1) Assigning a Project Manager who is responsible for implementing security for software in development;

(2) Capturing and refining information security requirements and ensuring that the requirements are effectively integrated into IT component products and information systems through purposeful security architecting, design, development, and configuration;

(3) Ensuring security requirements for new software are defined and documented in a risk assessment and SSP;

(4) Ensuring each decision to utilize compensating controls or enhance the recommended security controls of the information system is fully documented in the SSP and included in the authorization package submitted to the AO;

(5) Updating software based on findings from ISCM; and

(6) Ensuring software is authorized to operate prior to operational deployment.

e. **Deputy CIO for Service Delivery and Engineering** is responsible for:

(1) Addressing the operational interests of the user community and ensuring compliance with information security requirements;

(2) Procuring, developing, integrating, modifying, operating, and maintaining VA information systems; and

(3) Ensuring that each system is assigned a System Owner who understands his/her role and responsibilities in the A&A process.

f. **Continuous Readiness in Information Security Program Governance Council** is a chartered group sponsored by the Office of Information Security and Service Delivery and Engineering and is responsible for:

(1) Ensuring that the A&A program is developed, reviewed, and maintained to operate efficiently and effectively and complies with FISMA and other related information security requirements;

(2) Reviewing processes, procedures, and policy related to A&A and providing recommendations and/or concurrence;

(3) Identifying process improvement opportunities within the A&A program;

(4) Submitting issues and recommendations regarding the A&A program to the DAS, Office of Information Security and Deputy CIO, Service Delivery and Engineering, for executive decision as necessary;

(5) Ensuring the interests of programs, facilities, and OIT are addressed by the A&A program; and

(6) Ensuring the A&A program is aligned with OIT strategic plans.

g. **Enterprise Risk Management (ERM)** in OIT serves as a Security Control Assessor for onsite SCAs and is responsible for:

(1) Conducting an onsite assessment of the security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., to determine if the documented controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements identified for protecting the system at its specified level of sensitivity);

(2) Using existing or newly requested vulnerability and compliance scans performed by VA Network and Security Operations Center (NSOC) for all technical scanning required for the assessment;

(3) Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation through the onsite assessment and recommending corrective actions to address identified vulnerabilities;

(4) Completing an independent assessment of the SSP as part of the onsite assessment activities to determine if the SSP addresses a set of security controls which are consistent with the Federal Information Processing Standards (FIPS) security categorization and risk assessments completed for the information system. In addition, these security controls must be reviewed for adequacy and must meet all applicable security requirements;

(5) Preparing a security assessment report containing the results, findings, and recommendations from the assessment and providing the results to the System Owner and to the Office of Cyber Security (OCS);

(6) Conducting and/or monitoring risk assessments of continuous monitoring tools;

(7) Providing input to the types of security-related information gathered as part of ISCM; and

(8) Working with OCS to develop SCA test plans.

h. **VA-NSOC** is responsible for:

(1) Performing vulnerability and compliance scans in support of assessment and continuous monitoring activities; and

(2) Performing software assurance assessments and providing the results to the System Owner or Project Manager for remediation.

i. **OCS** is responsible for:

(1) Implementing the A&A process for VA;

(2) Ensuring a comprehensive assessment of the security controls employed within or inherited by an information system is performed to determine the overall effectiveness of the controls (i.e., to determine if the documented controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements identified for protecting the system at its specified level of sensitivity);

(3) Requiring qualified, independent Security Control Assessors to perform SCAs on VA IT systems;

(4) Maintaining an inventory of FISMA reportable systems;

(5) Providing an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommending corrective actions to address identified vulnerabilities;

(6) Ensuring an independent assessment of the SSP is completed as part of the SCA activities to determine if the SSP addresses a set of security controls which are consistent with the Federal Information Processing Standards (FIPS) security categorization and risk assessments completed for the information system. In addition, these security controls must be reviewed for adequacy and must meet all applicable security requirements;

(7) Requiring the Security Control Assessor to prepare a security assessment report containing the results, findings, and recommendations from the assessment and to provide the results to the System Owner and to OCS;

(8) Participating in the development of SCA test plans;

(9) Providing tools, resources, and performance dashboards to plan, schedule, execute, and report on assessments;

(10) Coordinating with the Director, Business Continuity and staff to ensure the Contingency Plan, Disaster Recovery Plan, and Incident Response Plan are included in the overall A&A process and documentation packages;

(11) Facilitating Security Control Assessors' activities, as needed, including notifying ERM of assessments to be conducted, ensuring access to resources to perform the SCA is provided, and supporting onsite assessment activities;

(12) Maintaining SCA processes;

(13) Maintaining and publishing the SCA schedule and the list of required artifacts for the security authorization package; and

(14) Providing results of the SCA to the AO or AODR.

j. **System Owners** are responsible for:

(1) Developing and maintaining system documentation in coordination with Information Owners, system administrators, the ISO, and functional "end user" for any nationally deployed system;

(2) Ensuring the system is deployed and operating according to the agreed-upon security requirements;

(3) Preparing POA&M items in the VA-approved FISMA database to reduce or eliminate vulnerabilities in the information system, including tracking and closing POA&M items in the database;

(4) Ensuring the remediation and updating of the POA&M identified during the authorization process and other reviews, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities;

(5) Informing key VA management officials of the need to conduct a security authorization of the information system, and ensuring appropriate budget and resources are available for the effort, and providing the required information system access, information, and documentation to the Security Control Assessor;

(6) Taking steps to mitigate, reduce or eliminate vulnerabilities identified in the security assessment report, including conducting initial remediation actions on security controls based on the findings and recommendations of the security assessment report;

(7) Updating the SSP and risk assessment based on the findings and recommendations of the SCA and any remediation actions taken;

(8) Assembling the final security authorization package and submitting the package to the AO or AODR for adjudication electronically through the VA-approved FISMA database;

(9) Ensuring the authorization package includes information regarding the core mission and business requirements supported by the system and the impact of the system on mission and business operations;

(10) Ensuring compliance with Federal security regulations and VA security policies;

(11) Ensuring 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;

(12) Performing an analysis of the security impact and risk of changes to identify significant changes to the information system or major changes to the data collected and maintained as part of the ongoing assessment of risk in support of continuous monitoring;

(13) Ensuring the review and update of the SSP when a change requiring reauthorization occurs;

(14) Assisting local system administrators in the identification, implementation, and assessment of security controls;

(15) Ensuring risk assessments are accomplished per the SSP and reviewed and updated periodically and when there is a change to the system requiring reauthorization;

(16) Ensuring each decision to utilize compensating controls or enhance the recommended security controls of the information system is fully documented in the SSP and included in the authorization package submitted to the AO;

(17) Establishing processes and procedures in support of system level implementation of the ISCM program, including developing a continuous monitoring strategy for the information system; and

(18) Completing training on the A&A process and, as part of that training, acknowledging that they understand their A&A responsibilities as outlined in this Handbook and VA's approved A&A training.

k. **Project Managers** are responsible for A&A activities for systems in development. Project Managers are responsible for:

(1) Informing key VA management officials of the need to conduct a security authorization of the information system, ensuring appropriate budget and resources are available for the effort, and providing the required information system access, information, and documentation to the Security Control Assessor;

(2) Taking steps to mitigate, reduce or eliminate vulnerabilities identified in the security assessment report, including conducting initial remediation actions on security controls based on the findings and recommendations of the security assessment report;

(3) Updating the SSP and risk assessment based on the findings and recommendations of the SCA and any remediation actions taken;

(4) Assembling the final security authorization package and submitting the package to the AO or AODR for adjudication electronically through the VA-approved FISMA database;

(5) Ensuring the authorization package includes information regarding the core mission and business requirements supported by the system and the impact of the system on mission and business functions;

(6) Ensuring compliance with Federal security regulations and VA security policies;

(7) Ensuring the information system receives authorization prior to operational deployment;

(8) Ensuring the system is deployed and operating according to the agreed-upon security requirements;

(9) Creating, implementing, and documenting a configuration management plan that controls changes to the software during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation;

(10) Preparing POA&M items in the VA-approved FISMA database to reduce or eliminate vulnerabilities in the information system, including tracking and closing POA&M items in the database;

(11) Assisting developers in the identification, implementation, and assessment of security controls;

(12) Assisting developers in the implementation of secure code and the assessment of the code’s security; and

(13) Ensuring the remediation and updating of the POA&M identified during the authorization process.

l. **Information (Data) Owners** (Network Directors/Facility Directors/Program Managers/Data Stewards) are responsible for:

(1) Establishing the policies and procedures governing the generation, collection, processing, dissemination, and disposal of the data;

(2) Providing input to System Owners or Project Managers regarding the security requirements and the security controls for the information system or systems where the information is processed, stored, or transmitted;

(3) Providing assistance to the VA CIO in identifying the security requirements and appropriate level of security controls for the information system or system(s) where sensitive personal information (SPI) is currently created, collected, processed, disseminated, or subject to disposal;

(4) Determining who has access to the system or systems containing SPI, including types of privileges and access rights based upon expressed job duties; and

(5) Ensuring all POA&M corrective actions are taken by their respective staff, and validating corrective actions taken by the System Owners or Project Managers with whom their data resides.

m. **Local CIOs/System Administrators/Network Administrators** are responsible for day-to-day system operations. The role of a system/network administrator must include security of local area network (LAN) or application administration and account administration. The system/network administrator is responsible for:

(1) Ensuring system operational compliance with Federal security regulations and VA security policies;

(2) Assisting in the development and maintenance of the SSP for any system under his or her responsibility;

(3) Participating in FISMA system self-assessments, external and internal audits of system safeguards and program elements, and in the A&A of the system;

(4) Ensuring the integrity in implementation and operational effectiveness of security controls by conducting technical control testing;

(5) Periodically repeating 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;

(6) Evaluating and developing procedures that assure proper integration of service continuity with other system operations;

(7) Providing information on users and/or the system in support of any reports or documents necessary for oversight and A&A;

(8) Working with local leadership and representatives of the mission and business functions supported by the system to ensure that information regarding the core mission and business requirements supported by the system and the impact of the system on mission and business operations is made available to be considered in the authorization decision; and

(9) Assisting other VA officials who have significant IT responsibilities in the remediation and updating of the POA&Ms identified during the A&A process, periodic compliance validation reviews, and the FISMA annual assessment reporting to reduce or eliminate system vulnerabilities.

n. **ISOs** are assigned responsibility by OIT Field Security Services to ensure the appropriate operational security posture is maintained for an information system or program and, as such, are responsible for:

(1) Serving as the principal staff advisor to the AO, AODR/DAS for Information Security, System Owner, and Project Manager on all matters involving the security of the information system;

(2) Serving as the primary point of contact and coordinator for all security authorization activities within the facilities under their area of responsibility;

(3) Assisting the System Owner and Project Manager in developing and reinforcing security policies for information and the information system;

(4) Participating in the monitoring of a system and its environment of operation, including developing and updating the security plan, managing and controlling changes to the system, and assessing the security impact of those changes;

(5) Assisting the System Owner and Project Manager in managing and controlling changes to the information system, as well as, assessing the security impacts of those changes;

(6) Ensuring compliance with Federal security regulations and VA security policies;

(7) Managing their local information security programs and serving as the principal security advisor to System Owners and Project Managers regarding security considerations in applications, systems, procurement or development, implementation, operation and maintenance, and disposal activities (life cycle management);

(8) Coordinating, advising, and participating, under the guidance of the System Owner and Project Manager, in the development, maintenance, and uploading of the SSP for any systems under their responsibility;

(9) Verifying and validating, in conjunction with System Owners, Project Managers, and VA officials with daily system operating responsibilities, appropriate security measures are implemented and functioning as intended;

(10) Participating in security self-assessments, external and internal audits of system safeguards and program elements, and in A&A of any system supporting the offices and facilities under their responsibility;

(11) Assisting other VA officials, with significant IT responsibilities (system managers, contracting staff, human resources staff, and police) in remediating and updating the POA&Ms identified during the A&A process and completing and reviewing the input of the annual FISMA assessment with the System Owners;

(12) Assisting the System Owner in completing ISCM responsibilities and by participating in the configuration management processes;

(13) Working with local leadership and representatives of the mission and business functions supported by the system to ensure that information regarding the core mission and business requirements supported by the system and the impact of the system on mission and business operations is made available to be considered in the authorization decision; and

(14) Completing training on the A&A process and as part of that training acknowledging that they understand their A&A responsibilities as outlined in this Handbook and VA's approved A&A training.

4. POLICY

a. Fundamental Requirements

(1) Risk Management

(a) VA will view VA program-level (Tier 2/Administration mission/processes) or VA-level (Tier 1) risk from a broader, more strategic view than can be obtained from the more technically focused, system-level view of the information system which results from the assessment.

(b) The AO will make the ultimate mission risk acceptability determinations based on the known vulnerabilities remaining in the information system after the implementation of an agreed-upon set of security controls and the risks to organizational operations (including VA mission, business functions, image, or reputation) and assets, individuals, other organizations, and the Nation resulting from the operation of the information system. As appropriate the AO will consult other individuals within VA, such as the DAS for Information Security, ISO, System Owner, Project Manager, Information Owner, the Security Control Assessor, or Administration or Program Office officials, at any phase in the A&A process or during continuous monitoring to obtain advice on the mission or security of the information system.

(2) Capital Planning

(a) FISMA, SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control* Process, and other Federal regulations charge agencies with integrating information security and Capital Planning and Investment Control processes which have been previously performed independently by security and capital planning practitioners. With increased competition for limited Federal budgets and resources, VA must effectively bridge the gap between information system security and capital planning to help ensure available funding is applied to the highest priority information security and technology investments. Applying funds toward higher priority security investments supports the objective of securing information and information systems, both at the enterprise-wide and system level, commensurate with levels of risk and data sensitivity.

(b) OMB requires VA to prepare budget information for VA-specific investments (including the information system security component) and present the information to OMB on an annual basis using OMB Circular A-11, Exhibits 53 (Information Technology and E-Government) and 300 (Planning, Budgeting, Acquisition, and Management of Capital Assets). VA management prepares budget information for VA-specific investments and contracts incorporating the expenditures necessary to comply with Federal and VA information security standards and requirements as part of the budget preparation process, and throughout the expected life cycle of the budget line item. System Owners or Project Managers may be required to fund assessment efforts from the budget of the operating group in the event of a failure to reach an ATO in the initial A&A process.

(3) Acquisition

(a) VA relies heavily on vendor-provided information technology products and services, as well as cooperative agreements such as MOUs and MOAs. Federal and VA information system security policies and requirements to safeguard the information and information systems are critical in the acquisition of VA products and services and in the awarding of contracts, grants, and cooperative agreements. Management is required to understand the risk and ramifications of purchasing products and awarding contracts, grants, and cooperative agreements.

(b) VA management works with the VA office responsible for procurement through the approved VA IT tracking system. The procurement information contained within the VA IT tracking system is reviewed and approved by the VA OIT Acquisition Team. This group is responsible for ensuring support service contracts and grants are flexible enough to ensure additional security requirements are incorporated quickly and efficiently, as required by law and by VA.

(c) Contractor information systems may require A&A if all of the following conditions are true, as determined by completion of the checklist in VA Handbook 6500.6, *Contract Security*, Appendix A:

1. The acquisition requires use of a contractor-owned IT system or computer assets;

2. The IT system hardware components are located at an offsite contractor facility;

3. The IT system is not connected to a VA network;

4. The contractor has exclusive administrative control to the components; and

5. The purpose of the requirement for the system is to process or store VA information on behalf of VA.

(d) The ISO will notify OCS of any contractor information systems identified in appendix A of VA Handbook 6500.6 as potentially requiring A&A. OCS will review and confirm that the contractor information system requires A&A prior to the requirement for A&A being added to the statement of work or contract.

(4) Media Protection and Document Marking

(a) VA considers information concerning VA IT systems to be VA sensitive information. This includes, but is not limited to the following documents created for and in support of the A&A and ISCM, whether in electronic or hard copy:

1. System (component) inventories;

2. System descriptions;

3. System configurations for servers, desktops, and networking devices;

4. Diagrams;

5. Risk Assessments;

6. SCAs;

7. SSPs;

8. Contingency Plans;

9. Privacy Impact Assessments;

10. POA&Ms;

11. Network monitoring (logs and network/vulnerability scans); and

12. Penetration test reports.

(b) All reports, logs, and records pertaining to A&A and ISCM security issues are also considered VA sensitive information. If the publication of any security related information could diminish or jeopardize the ability of VA to accomplish its mission, that information is also considered VA sensitive information. Documents containing VA sensitive information must be protected in accordance with VA Handbook 6500.

(c) All A&A documentation is considered VA sensitive information regardless of the security categorization (low, moderate, or high) of the system. All users involved with VA sensitive A&A or ISCM information are required to ensure it is secured. All forms of hard copy and electronically stored media are also subject to the security requirements for VA sensitive information.

b. **A&A Process**

(1) A&A is an integral part of VA's information security program. A&A is the process used to ensure information systems have effective security safeguards which have been implemented, planned for, and documented in a security plan. The A&A process is the mechanism by which management provides formal authority for a system to operate and process information. A&A is based on the approval of the AO who is the senior most VA official assigned responsibility for IT systems. A&A is required by information security legislation and Federal regulation and provides a framework for auditing the efficiency and effectiveness of security controls.

(2) Table 1: A&A Associated Tasks, shown on the following page, presents a high-level view of the A&A process. Prior to entering the A&A process, steps 1 through 3 (Categorize the Information System, Select the Security Controls, and Implement the Security Controls) of the RMF are completed; the A&A process parallels steps 4 and 5 of the RMF. Table 1 includes the requirements (tasks) associated with Assess the Security Controls and Authorize the Information System. Following A&A the system is monitored as required in RMF step 6, Monitor the Security Controls, through the ISCM program.

Table 1: A&A Associated Tasks

RMF Step	Tasks
Assess the Security Controls	• Assessment Preparation • Security Control Assessment • Security Assessment Report • Remediation Actions
Authorize the Information System	• Plan of Action and Milestones • Security Authorization Package • Risk Determination • Risk Acceptance

(3) A more detailed overview of the tasks required to assess the security controls and authorize the information system is provided in appendices A and B, respectively.

(4) A&A should not be viewed as an administrative burden. It provides realistic, measurable, and cost-effective benefits for operating a system and protecting its information. Mission and business impacts are considered in the A&A process. The goal is to minimize system risk to an acceptable level for processing information. Risks will always exist; however, identifying weaknesses and prioritizing corrective actions to mitigate vulnerabilities is the foundation of the A&A process.

(5) Authorization is achieved through VA's A&A process.

(a) For systems in development, authorization must be received prior to the system achieving operational or production status. After the initial authorization, the ISCM program supports ongoing authorization.

(b) For information systems already in operation or production the ISCM program supports the ongoing authorization of information systems.

(c) Formal reauthorization is required whenever a system undergoes a significant change or when there is a major change in the information collected or maintained. Prior to implementing a change, the System Owner, with assistance from the ISO and Privacy Officer, will determine if the proposed change is a change requiring reauthorization. Decisions regarding whether a system requires reauthorization will be based on an analysis of risk. A significant change to an information system may include changes to the system itself or to the environment of operation. Significant changes to the information system may include, but are not limited to: installation of a new or upgraded operating system, middleware component, or application; modifications to system ports, protocols, or services; installation of a new or upgraded hardware platform; modifications to cryptographic modules or services; or modifications to security controls. Significant changes to the environment of operation may include, but are not limited to: moving to a new facility; adding new core missions or business functions; modifications to the mission or business use of the system; acquiring specific and credible threat information that the organization is being targeted by a threat source; or establishing new or modified laws, policies or regulations. Major changes to the information collected or maintained are those changes that could result in greater disclosure of information or a change in the way personal data is used.

(6) The RMF steps of Assess the Security Controls and Authorize the Information System consist of a set of well-defined requirements to be completed, as indicated, by VA designated individual(s). These activities are integrated into the SDLC and are broken down into tasks required to complete the step. See VA Handbook 6500.5.

(7) The tasks required to assess and authorize are presented sequentially; however, VA may deviate from the sequential structure to be consistent with existing management and SDLC processes or to be more cost-effective or efficient, as appropriate. Regardless of the ordering of the other tasks, the last step before an information system is placed into operation is the explicit acceptance of risk by the AO. Iterative/incremental assessment methods may be used if it is more practical given development processes or more efficient or cost-effective, for instance, when iterative development processes are employed.

(8) The successful completion of A&A provides VA officials with the necessary confidence that the information system has adequate security controls in place and functioning as intended, any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and appropriate plans and funds have been identified to correct all deficiencies in the information system that can be addressed.

(9) The System Owner or Project Manager is responsible for informing key VA officials such as the DAS for Information Security, OCS Director, ISO, as well as those VA officials with a valid need-to-know of the system requiring A&A. The initial notification of key VA officials is required in writing in the format prescribed by OCS and is an integral part of the system life cycle. This notification also serves as a notification to begin preparing potential participants for the upcoming tasks necessary to plan, organize, and conduct the A&A.

(10) The AO, DAS for Information Security, OCS Director, System Owner, Project Manager, and Security Control Assessor are responsible for determining the level of effort and resources required for the A&A of the information system (including the organization(s) involved) and for preparing a plan of execution.

(11) The level of effort required for security assessment is dependent upon three factors:

(a) The size and complexity of the information system;

(b) The security categorization of the system; and

(c) The security controls employed to protect the system.

(12) For low-impact systems, a streamlined process for assessing the security controls and authorizing the information system may be implemented, if deemed appropriate by OCS.

(13) The AO determines the required degree of independence for Security Control Assessors involved in initial and subsequent authorization and in continuous monitoring. SCAs in support of security authorizations are conducted by independent Security Control Assessors.

(14) Identifying appropriate resources (supporting organizations, funding, and individuals with critical skills) is typically integrated within the system life cycle, capital planning, and budgeting processes.

(15) Training on the A&A process and A&A responsibilities will be available for those with security relevant activities.

(16) VA may choose to accept an authorization package generated by other Federal agencies, Department of Defense, private companies, or the Federal Risk and Authorization Management Program. VA will review the authorization package to determine the risk to VA, considering factors such as the recentness of the authorization results, the environment of operation, the criticality/sensitivity of the information to be processed, stored, or transmitted, and VA’s risk tolerance. OCS will determine the artifacts which must be included in the externally provided authorization package for VA to make an authorization decision and VA may negotiate with the owning organization for additional security measures and/or security related information. The AO will issue an authorization decision document to accept or not accept the risks to VA’s operations and assets, individuals, other organizations, or the Nation. If VA accepts the risk, VA is responsible for the continuous monitoring and ongoing authorization of the system. VA may include as part of the agreement with the owning organization (e.g., contract) a requirement that the owning organization must share results from continuous monitoring activities conducted by the owning organization to maintain the authorization and the terms and conditions (e.g., frequency, format) required for the owning organization to report continuous monitoring results.

c. **ISCM Program**

(1) Development of the ISCM strategy and implementation of an ISCM program provides visibility into VA assets and awareness of threats and vulnerabilities and the effectiveness of deployed security controls. The ISCM strategy and program supports ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner. The ISCM program:

(a) Gives organizational officials access to security-related information on demand, enabling timely risk management decisions;

(b) Facilitates risk-based decision-making regarding the ongoing authorization to operate information systems by providing evolving threat activity or vulnerability information on demand;

(c) Supports frequent updates to security plans, security assessment reports, POA&Ms, hardware and software inventories, and other system information; and

(d) Includes continuous monitoring of all security controls.

(2) VA will follow the process outlined below to develop and implement an ISCM program:

(a) Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

(b) Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.

1. Metrics are organized into meaningful information to support decision-making and reporting requirements.

2. VA will determine the frequency with which each security control or element is assessed for effectiveness and the frequency with which each metric is monitored.

3. The frequency of assessments should be sufficient to assure adequate security commensurate with risk as determined by system categorization and ISCM strategy requirements. When establishing monitoring frequencies for metrics or assessment frequencies for security controls VA will consider:

a. Security control volatility;

b. Security categories;

c. Security controls or specific assessment objects providing critical functions;

d. Security controls with identified weaknesses;

e. Organizational risk tolerance;

f. Threat information;

g. Vulnerability information;

h. Risk assessment results;

i. Output of monitoring strategy reviews;

j. Reporting requirements; and

k. Federal regulations.

4. At the information system level, System Owners will review the minimum monitoring or assessment frequencies established by the ISCM program and determine if the minimum frequencies are adequate for a given information system.

5. Events may occur that trigger the immediate need to assess security controls or verify security status outside of the frequency required by the ISCM strategy.

6. VA will develop architecture to support ISCM that includes data collection, data storage, data analysis capabilities, and reporting capabilities.

(c) Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting.

1. Automate collection, analysis, and reporting of data where possible.

2. Data sources for collecting information include people, processes, technologies, the computing environment, and existing assessment reports.

3. Data collected is assembled for analysis and reported to the stakeholders in accordance with their requirements.

(d) Analyze the data collected and report findings determining the appropriate response.

1. Additional information may be necessary to clarify or supplement existing monitoring data.

2. Output will be formatted to provide information that is specific, measurable, actionable, relevant, and timely.

3. Procedures for analyzing and reporting assessment and monitoring results will include the specific staff/roles to receive ISCM reports, the content and format of the reports, the frequency of reports, and any tools to be used.

4. Information resulting from ISCM is analyzed in the context of stated risk tolerances, the potential impact that vulnerabilities may have on information systems, mission/business processes, and VA as a whole, and the potential impact of mitigation options.

(e) Respond to findings with mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

1. Responses will be in accordance with risk tolerance.

2. Mitigations will be documented in the SSP or added to the POA&M.

(f) Review and update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

1. Factors precipitating change to the monitoring strategy include, but are not limited to:

a. Changes to core missions or business processes;

b. Significant changes in the Enterprise Architecture (including addition or removal of systems);

c. Changes in organizational risk tolerance;

d. Changes in threat information;

e. Changes in vulnerability information;

f. Changes within information systems (including changes in categorization/impact level);

g. Increase/decrease in POA&M related to specific controls;

h. Trend analyses of status reporting output;

i. New Federal laws or regulations; and/or

j. Changes to reporting requirements.

2. Officials examine consolidated POA&M information to determine if there are common weaknesses/deficiencies among the organization's information systems and propose or request solutions, allocate resources, and adjust the monitoring strategy as necessary.

3. VA's ISCM strategy is not static; VA will adjust its ISCM strategy over time as the security program and monitoring capabilities mature.

(3) VA OIT will develop procedures for the implementation of VA's ISCM strategy and program.

d. **Use of Automation**

(1) VA will use automation throughout the A&A and ISCM processes to increase speed, effectiveness, and efficiency of the A&A process and to support the concepts of continuous monitoring and near real-time risk management.

(2) VA will use automation to the maximum extent practicable to:

(a) Conduct SCAs;

(b) Prepare and manage the security authorization package;

(c) Perform continuous monitoring (including use of vulnerability scanning tools, system and network monitoring tools);

(d) Update the authorization package (including use of security management and reporting tools);

(e) Manage changes to the information system or its environment of operation; and

(f) Capture, organize, quantify, visually display, and maintain security status information.

e. **Software Assurance**

(1) VA identifies security defects as early as possible to minimize the cost and disruption of remediating flaws and to avoid deploying flawed software.

(2) VA incorporates software assurance assessment testing with the A&A process. Office of Information Security will determine the scope of the assessments.

(3) The System Owner or Project Manager must submit all source code developed by or for VA for assessment as part of the SCA in support of the initial security authorization.

(4) NSOC will perform software assurance assessments, which may include, but are not limited to penetration testing, static or dynamic application testing, and source code reviews. Results of the assessment will be provided to the System Owner or Project Manager.

(5) All software defects discovered during the assessment must be remediated and the code reassessed to verify remediation prior to the System Owner or Project Manager submitting the system authorization package to the AO for adjudication.

(6) Ongoing assessments of software assurance may be performed in support of the ISCM program.

Appendix A. Terms and Definitions

1. **Adequate Security:** Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of information. SOURCE: SP 800-37

2. **Application:** A software program hosted by an information system. SOURCE: SP 800-137

3. **Assessment Method:** One of three types of actions (examine, interview, test) taken by assessors in obtaining evidence during an assessment. SOURCE: SP 800-137

4. **Assessment Procedure:** A set of assessment objectives and an associated set of assessment methods and assessment objects. SOURCE: SP 800-137

5. **Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: SP 800-53; SP 800-53A; SP 800-27; FIPS 200; 800-137

6. **Authorization/Authorization to Operate (ATO):** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37

7. **Authorization Boundary:** All components of an information system to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the information system is connected. SOURCE: SP 800-37

8. **Authorizing Official (AO):** Senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. In VA, this is the VA CIO. SOURCE: SP 800-53; SP 800-53A; SP 800-37

9. **Authorizing Official Designated Representative (AODR):** An organizational official acting on behalf of an Authorizing Official in carrying out and coordinating the required activities associated with security authorization. SOURCE: CNSSI-4009; SP 800-37; SP 800-53A

10. **Availability:** Ensuring timely and reliable access to and use of information. SOURCE: 38 U.S.C. § 5727

11. Chief Information Officer (CIO): Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure information technology is acquired and information resources are managed in a manner consistent with laws, Executive Orders, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. SOURCE: PL 104-106, Sec. 5125(b); SP 800-37

12. Common Security Control: A security control that is inherited by one or more organizational information systems. These controls affect all VA facilities and systems with operations at the local site(s). SOURCE: SP 800-53 [VA Adapted]

13. Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: 38 U.S.C. § 5727

14. Continuous Monitoring: Maintaining ongoing awareness to support organizational risk decisions. See Information Security Continuous Monitoring. SOURCE: SP 800-137

15. Countermeasures: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. SOURCE: CNSSI 4009; SP 800-37

16. Environment of Operation: The physical surroundings in which an information system processes, stores, and transmits information. SOURCE: SP 800-137

17. High-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. SOURCE: SP 800-37; SP 800-53; SP 800-60; FIPS 200

18. Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The term incident means security incident as defined in 38 U.S.C. 5727(18). SOURCE: 38 U.S.C. 5727

19. Information Owner: An agency official with statutory or operational authority for specified information and responsibility for establishing the control criteria for its creation, collection, processing, dissemination, and disposal which responsibilities may extend to interconnected systems or groups of interconnected systems. SOURCE: 38 U.S.C. § 5727

20. Information Resources: Information in any medium or form and its related resources, such as personnel, equipment, funds, and information technology. SOURCE: 38 U.S.C. § 5727

21. Information Security: A means for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. SOURCE: 38 U.S.C. § 5727

22. Information Security Continuous Monitoring: Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. SOURCE: SP 800-137

23. Information Security Continuous Monitoring Program: A program established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls. SOURCE: SP 800-137

24. Information Security Officer (ISO): Individual working with the senior agency ISO, Authorizing Official, or Information System Owner to help ensure the appropriate operational security posture is maintained for an information system or program. SOURCE: CNSSI 4009 [VA Adapted]

25. Information Security Requirements: Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce, NIST, and OMB, and, as to national security systems, the President. SOURCE: 38 U.S.C. § 5727

26. Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual. SOURCE: 38 U.S.C. § 5727

27. Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: FIPS 200

28. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: SP 800-53; SP 800-53A

29. Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: 38 U.S.C. § 5727

30. Local Area Network (LAN): A datacomm system allowing a number of independent devices to communicate directly with each other, within a moderately sized geographic area over a physical communications channel of moderate rates. SOURCE: FIPS 191

31. Low-Impact System: An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. SOURCE: SP 800-37; SP 800-53; SP 800-60; FIPS 200

32. Major Change: A change to the information collected or maintained that could result in greater disclosure of information or a change in the way personal data is used. SOURCE: VA Adapted

33. Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes; optical disks; magnetic disks; Large-Scale Integration memory chips; and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. SOURCE: FIPS 200; SP 800-53; CNSSI-4009

34. Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this Handbook, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. SOURCE: SP 800-47

35. Moderate-Impact System: An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. SOURCE: SP 800-53; SP 800-60; SP 800-37; FIPS 200

36. Operating Unit: An Operating Unit consists of any and all individuals responsible for the management, operation, maintenance, and security of VA's information and information systems within their area of responsibility. Examples of individuals who are part of the Operating Unit include, but are not limited to, Directors, Program Managers, and Information and Technology staff (system managers, system administrators, and ISOs). SOURCE: VA Adapted

37. Plan of Action and Milestones (POA&M): A plan used as a basis for the quarterly reporting requirements of OMB that includes the following information: (i) A description of the security weakness; (ii) the identity of the office or organization responsible for resolving the weakness; (iii) an estimate of resources required to resolve the weakness by fiscal year; (iv) the scheduled completion date; (v) key milestones with estimated completion dates; (vi) any changes to the original key milestone date; (vii) the source that identified the weakness; (viii) the status of efforts to correct the weakness. SOURCE: 38 U.S.C. § 5727

38. Potential Impact: The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. SOURCE: SP 800-53; SP 800-60; SP 800-37; FIPS 199

39. Privacy Impact Assessment: An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. SOURCE: SP 800-53; SP 800-18; SP 800-122; CNSSI-4009; OMB Memorandum 03-22

40. Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: SP 800-60

41. Risk Assessment: Process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other operations, and the Nation arising from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. SOURCE: SP 800-53; SP 800-53A; SP 800-37

42. Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment techniques and procedures for the continuous monitoring of the security state of the information system. SOURCE: SP 800-53; SP 800-53A; SP 800-37

43. Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result. SOURCE: SP 800-32

44. Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. SOURCE: CNSSI 4009; SP 800-37

45. Sanitization: Process to remove information from media so that information recovery is not possible. It includes removing all labels, markings, and activity logs. SOURCE: FIPS 200

46. Security Assessment Plan: A plan that provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. SOURCE: NIST SP 800-37

47. Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. SOURCE: FIPS 199

48. Security Categorization: The process of determining the security category for information or information system. SOURCE: SP 800-53

49. Security Control Assessment (SCA): The testing and/or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system and/or enterprise. SOURCE: CNSSI-4009

50. Security Control Assessor: The individual, group, or organization responsible for conducting a security control assessment. SOURCE: SP 800-37

51. Security Control Volatility: A measure of how frequently a control is likely to change over time subsequent to its implementation. SOURCE: SP 800-37

52. Security Controls: The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: SP 800-53; SP 800-37; SP 800-53A; SP 800-60; FIPS 200; FIPS 199; CNSSI-4009 [VA Adapted]

53. Security Impact Analysis: The analysis conducted by an organizational official to determine potential security impacts prior to change implementation. SOURCE: SP 800-53 [VA Adapted]

54. Sensitive Personal Information (SPI): The term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual’s identity, including name, social security number, date and place of birth, mother’s maiden name, or biometric records. SPI is a subset of VA Sensitive Information/Data. SOURCE: 38 U.S.C. § 5727.

Note: The term “Sensitive Personal Information” is synonymous and interchangeable with “Personally Identifiable Information.”

55. Significant Change: A significant 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]

56. Software Assurance: Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. SOURCE: CNSSI-4009

57. Subsystem: A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions. SOURCE: SP 800-37

58. System: See “Information System.”

59. System Owner: See “Information System Owner.”

60. System Security Plan (SSP): Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. SOURCE: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; FIPS 200

61. System-Specific Security Control: A security control for an information system that has not been designated as a common security control or a portion of a hybrid control that is to be implemented within an information system. SOURCE: SP 800-37; SP 800-53; SP 800-53A; CNSSI-4009

62. Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009

63. Threat Source: The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidently trigger a vulnerability. Synonymous with threat agent. SOURCE: FIPS 200; SP 800-37

64. Training: A learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge. SOURCE: 38 U.S.C. § 5727

65. Unauthorized Access: Gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access. SOURCE: SP 800-61

66. VA Information/Data: Information owned or in the possession of VA or any entity acting for or on behalf of VA. SOURCE: VA Adapted

67. VA Sensitive Information/Data: All Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions. SOURCE: 38 U.S.C. § 5727

68. Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200

APPENDIX B. ABBREVIATIONS/ACRONYMS USED IN HANDBOOK AND APPENDICES

Abbreviation / Acronym	Description
A&A	Assessment and Authorization
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authority to Operate
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DAS	Deputy Assistant Secretary
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ISO	Information Security Officer
ISCM	Information Security Continuous Monitoring
IT	Information Technology
LAN	Local Area Network
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSOC	Network Security and Operations Center
OCS	Office of Cyber Security
OIT	Office of Information and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework

Abbreviation / Acronym	Description
SCA	Security Control Assessment
SDLC	System Development Life Cycle
SP	Special Publications
SPI	Sensitive Personal Information
SSP	System Security Plan
U.S.C.	United States Code
VA	Department of Veterans Affairs

APPENDIX C. REFERENCES

These requirements comply with established Federal information security laws and regulations, including:

a. 5 U.S.C. 552, § Freedom of Information Act

b. 5 U.S.C. 552a, § Privacy Act of 1974

c. 38 U.S.C.§§ 5721-28, Veteran's Benefits, Information Security

d. 44 U.S.C. § 3541, Federal Information Security Management Act of 2002 (FISMA)

e. CNSSI-1253, *Security Categorization and Control Selection for National Security Systems*

f. CNSSI-4009, *National Information Assurance Glossary*

g. FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*

h. FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*

i. FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*

j. NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*

k. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

l. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

m. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

n. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

o. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*

p. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*

q. NIST SP 800-61, *Computer Security Incident Handling Guide*

r. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*

s. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*

t. NIST SP 800-100, *Information Security Handbook: A Guide for Managers*

u. NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*

v. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

w. NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

x. OMB Circular A -11, *Preparation, Submission, and Execution of the Budget*

y. OMB Circular A -123, *Management's Responsibility for Internal Control*

z. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

aa. OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*

bb. OMB Memorandum M-11-33, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

cc. Pub. L. 104-191 § 264, 110 Stat. 1936, Health Insurance Portability and Accountability Act

dd. Pub. L. 107-347 § 208, 116 Stat. 2899, 2921, E-Government Act of 2002

ee. HIPAA Security and Privacy Rules, 45 C.F.R Part 160 and Part 165, Subparts A, C, D and E

ff. SANS Top 20 Most Critical Internet Security Vulnerabilities List

gg. VA Directive 6001, *Limited Personal Use of Government Office Equipment Including Information Technology*

hh. VA Directive 6004, *Configuration, Change, and Release Management Programs*

ii. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*

jj. VA Directive 6502, *VA Privacy Program* kk. VA Directive 6508, *Privacy Impact Assessments*

ll. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*

mm. VA Handbook 6500.1, *Electronic Media Sanitization*

nn. VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Life Cycle*

oo. VA Handbook 6500.6, *Contract Security* VA Handbook 6508.1, *Privacy Impact Assessment (PIA)*

This page is intentionally blank for the purpose of printing front and back copies.

APPENDIX D. ASSESS THE SECURITY CONTROLS

1. OVERVIEW: ASSESS THE SECURITY CONTROLS

a. The purpose of RMF Step 4 – Assess the Security Controls is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The assessment also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system.

b. Upon successful completion of the assessment, the AO will have the information needed to determine the actual risk to VA operations and assets, individuals, other organizations, and the Nation, and thus, will be able to render an appropriate authorization decision for the information system.

c. The following steps provide the information necessary to assess the security controls:

(1) Assessment Preparation;

(2) Security Control Assessment;

(3) Security Assessment Report; and

(4) Remediation Actions.

d. Table 2: Assess the Security Controls – High-Level Summary of Required Tasks, shown on the following page, contains the high level tasks which must be satisfied in order to assess the security controls, as well as the phases of the SDLC during which these tasks will be performed and the individuals responsible for each task.

Table 2: Assess the Security Controls - High-Level Summary of Required Tasks

Task	SDLC Phase	Primary Responsibility	Supporting Roles	References
Assessment Preparation	Acquisition and Development; Implementation and Assessment	Security Control Assessor	Project Manager or System Owner Information Owner ISO	SP 800-53A
SCA	Acquisition and Development; Implementation and Assessment	Security Control Assessor	Project Manager or System Owner Information Owner ISO	SP 800-53A
Security Assessment Report	Acquisition and Development; Implementation and Assessment	Security Control Assessor	Project Manager or System Owner ISO	SP 800-53A
Remediation Actions	Acquisition and Development; Implementation and Assessment	Project Manager or System Owner Security Control Assessor	AO AODR/DAS for Information Security Information Owner ISO Information System Security Engineer Security Control Assessor	SP 800-30 SP 800-37 SP 800-53A

2. TASKS: ASSESS THE SECURITY CONTROLS

a. Task 1: Assessment Preparation

(1) The Security Control Assessor works with OCS to develop a plan to assess the security controls.

(2) The security assessment plan provides the objectives for the SCA, a detailed roadmap of how to conduct such an assessment, and assessment procedures.

(3) The AO or AODR reviews and approves the security assessment plan to ensure that the plan is consistent with the security objectives of VA, employs state-of-the-practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, employs the appropriate level of resources to the SCA, and is cost-effective with regard to the resources allocated for the assessment. The approved security assessment plan will:

(a) Establish the appropriate expectations for the SCA; and

(b) Identify the level of effort for the SCA to ensure that an appropriate level of resources is applied toward determining security control effectiveness.

(4) The Security Control Assessor must possess the required level of independence and the required skills and technical expertise to successfully carry out assessments including knowledge and experience with the specific hardware, software, and firmware components employed.

(a) The AO or AODR determines the required level of independence for the Security Control Assessor based on the results of the security categorization process for the information system and the ultimate risk to VA operations and assets, individuals, other organizations, and the Nation. The AO determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a risk-based decision on whether to place the information system into operation or to continue its operation.

(b) Independent SCA services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization.

b. Task 2: SCA

(1) The Security Control Assessor assesses the security controls in accordance with the assessment procedures defined in the security assessment plan. Security Control Assessors assess all security controls employed within and inherited by the information system during the initial security authorization.

(2) An SCA determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting

the security requirements for the system. Assessments may also check non-security functions to ensure that they do not contain security vulnerabilities.

(3) The System Owner and Project Manager rely on the technical expertise and judgment of the Security Control Assessor to:

(a) Assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan;

(b) Provide unbiased, factual reporting of the weaknesses and deficiencies discovered during the SCA; and

(c) Provide specific recommendations on how to correct weaknesses or deficiencies in the control and reduce or eliminate identified vulnerabilities.

(4) The System Owner or Project Manager ensures that the Security Control Assessor has access to information systems and environments of operation where the controls are employed, including instances when security controls are provided by an external provider. In addition, the System Owner or Project Manager ensures that the Security Control Assessor has access to appropriate documentation, records, artifacts, test results and other materials, including information regarding security controls provided to an organization by an external provider.

(5) The System Owner or Project Manager documents descriptive information about the information system in the system identification section of the SSP or includes the information by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation are identified as well.

(6) The System Owner or Project Manager obtains any information related to existing assessments that may have been conducted by the external provider and reuses such assessment information whenever possible. When reasonable and appropriate, previous assessment results are reused. Previous assessment results include recent audit information regarding effectiveness of selected security controls and results from programs that test and evaluate the security features of commercial IT products.

c. Task 3: Security Assessment Report

(1) The Security Control Assessor prepares the security assessment report documenting the issues, findings, and recommendations from the SCA.

(2) The Security Control Assessor includes in the security assessment report the information necessary to determine the effectiveness of the security controls employed within or inherited by the information system. The security assessment report is an important factor in an AO’s determination of risk to VA operations and assets, individuals, other organizations, and the Nation. The security assessment report becomes part of the security authorization package developed for the AO.

(3) The Security Control Assessor documents the SCA results at a level of detail appropriate for the type of SCA in accordance with the reporting format prescribed by VA OIT and/or Federal policies.

(4) All security weaknesses and deficiencies identified during the SCA are documented in the security assessment report to maintain an effective audit trail.

(5) The security assessment report is an evolving document that includes assessment results from all relevant phases of the SDLC, including results generated during system development and continuous monitoring.

d. Task 4: Remediation Actions

(1) The System Owner or Project Manager conducts initial remediation actions on security controls based on the findings and recommendations of the security assessment report and the Security Control Assessor reassesses the remediated control(s), as appropriate.

(2) The security assessment report provides visibility into specific weaknesses and deficiencies that were not resolved during system development.

(3) The findings generated during the SCA facilitate a disciplined and structured approach to mitigating risks in accordance with VA priorities.

(a) System Owners or Project Managers, in collaboration with selected VA officials, may decide that certain findings are inconsequential and present no significant risk to VA.

(b) VA officials may decide that certain findings are significant, requiring immediate remediation actions.

(c) In all cases, Operating Units review assessment findings and determine the severity or seriousness of the findings and whether the findings are sufficiently significant to be worthy of further investigation or remediation.

(1) The System Owner or Project Manager updates the risk assessment based on the results of the findings produced during the SCA. The updated risk assessment helps to determine initial remediation actions and the prioritization of such actions.

(2) Senior leadership should ensure that VA’s resources are effectively allocated in accordance with VA priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions and business functions or correcting the deficiencies that pose the greatest degree of risk.

(3) If weaknesses or deficiencies are corrected, the remediated components are reassessed for effectiveness and to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Original assessment results are not changed; the security assessment report is updated with the findings from the reassessment.

(4) The System Owner or Project Manager updates the security plan based on the findings of the SCA and any remediation actions taken. The updated security plan reflects the actual state of the security controls after the initial assessment and any modifications by the System Owner or Project Manager in addressing recommendations for corrective actions. At the completion of the assessment, the security plan contains an accurate list and description of the security controls implemented and a list of residual vulnerabilities.

(5) The System Owner or Project Manager may prepare an optional addendum to the security assessment report that is transmitted to the AO to respond to the initial findings. The addendum may include information regarding initial remediation actions taken by the System Owner or Project Manager in response to the findings or provide an owner's perspective on the findings. The addendum does not change or influence the initial findings provided in the original report.

(6) VA may use an issue resolution process to determine the appropriate actions to take with regard to the security control weaknesses and deficiencies identified during the assessment. Issue resolution can help address vulnerabilities and associated risk, false positive, and other factors that may provide useful information to AOs regarding the security state of the information system including the ongoing effectiveness of system-specific controls, hybrid controls, and common controls. The issue resolution process can also help to ensure that only substantive items are identified and transferred to the POA&M.

APPENDIX E. AUTHORIZE THE INFORMATION SYSTEM

1. OVERVIEW: AUTHORIZE THE INFORMATION SYSTEM

a. The purpose of RMF Step 5 – Authorize the Information System is to ensure the risk to VA operations and assets, individuals, other organizations, and the Nation is acceptable to the AO, and the acceptability of that risk forms the basis of the authorization decision.

b. Upon successful completion of this phase, the system will have received an ATO or Denial of ATO.

c. The following steps provide the information necessary to authorize the information system:

(1) POA&M;

(2) Security Authorization Package;

(3) Risk Determination; and

(4) Risk Acceptance.

d. Table 3: Authorize the Information System – High-Level Summary of Required Tasks, shown on the following page, contains the high level tasks which must be satisfied in order to authorize the information system, as well as the phases of the SDLC during which these tasks will be performed and the individuals responsible for each task.

Table 3: Authorize the Information System - High-Level Summary of Required Tasks

Task	SDLC Phase	Primary Responsibility	Supporting Roles	References
POA&M	Implementation and Assessment	Project Manager or System Owner	Information Owner ISO	SP 800-30 SP 800-37 SP 800-53A OMB Memorandum 02-01 VA Handbook 6500
Security Authorization Package	Implementation and Assessment	Project Manager or System Owner	ISO Security Control Assessor	SP 800-37 OMB Circular A-130, Appendix III
Risk Determination	Implementation and Assessment	AO or AODR	DAS for Information Security	SP 800-30 SP 800-39 VA Handbook 6500
Risk Acceptance	Implementation and Assessment	AO	AODR/DAS for Information Security	SP 800-37 SP 800-39 OMB Circular A-130, Appendix III VA Handbook 6500

2. TASKS: AUTHORIZE THE INFORMATION SYSTEM

a. Task 1: POA&M

(1) The System Owner or Project Manager prepares the POA&M, in a timely and cost-effective fashion, based on the findings and recommendations of the security assessment report.

(2) The POA&M describes the specific tasks that are planned to correct security control weaknesses or deficiencies noted during the assessment and to address residual vulnerabilities in the information system (reduce, eliminate, or accept the vulnerabilities). The POA&M document is based on findings of security assessment report, security impact analysis, and continuous monitoring activities and it identifies:

(a) Tasks to be accomplished with recommendation for completion either before or after information system implementation;

(b) Resources required to accomplish the tasks;

(c) Any milestones in meeting the tasks; and

(d) Scheduled completion dates for the milestones.

(3) The AO uses the POA&M to monitor progress in correcting weaknesses or deficiencies noted during the SCA.

(4) System Owners or Project Managers develop specific POA&Ms based on the results of the SCA and in accordance with applicable laws, Executive Orders, policies, standards, guidance, or regulation and with VA OIT procedures. POA&Ms are not required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the AO.

(5) The content and structure of POA&Ms is informed by VA’s risk management strategy and is consistent with the POA&M process established by OIT and any specific requirements defined in VA OIT procedures, Federal policies, memoranda, or regulations.

(6) VA OIT will define a strategy for developing POA&Ms that facilitates a prioritized approach to risk mitigation that is consistent across VA. The strategy helps to ensure that POA&Ms are based on:

(a) Security categorization of the information system;

(b) Specific weaknesses or deficiencies in the security controls;

(c) Impact of the identified security control weaknesses or deficiencies on the security posture; and

(d) Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources).

(7) Risk assessment guides the prioritization process for items included in the POA&Ms.

(8) OMB issued memorandums provide specific guidance on preparing and submitting the POA&M, and SP 800-30, Risk Management Guide for Information Technology Systems provides guidance on risk mitigation.

b. Task 2: Security Authorization Package

(1) The System Owner or Project Manager assembles the security authorization package and submits the package to the AO for adjudication. The System Owner or Project Manager must submit the package electronically to the VA-approved FISMA database in order for the AO to receive it.

(2) The authorization package provides relevant information on the security state of the information system including the ongoing effectiveness of the security controls employed within or inherited by the system. The security authorization package will also contain any information that may be relevant and affect the final authorization decision, including information on the core mission and business requirements supported by the system and the impact of the system on mission and business functions.

(3) The System Owner or Project Manager ensures the authorization package is secured as VA sensitive information.

(4) The SSP, security assessment report, and POA&M are the three principal documents in the security authorization package. The Contingency Plan, Disaster Recovery Plan, and Incident Response Plan are also required to be included in the authorization package. A complete list of required documents for the authorization package will be posted on the Information Security Portal and updated as necessary.

(5) The authorization package will identify the system authorization boundary.

(6) When security controls are provided by an external provider, the System Owner or Project Manager ensures that the information needed for the AO to make risk-based decisions is made available by the provider.

(7) The AO may request additional information be included in the security authorization package to carry out the authorization action.

(8) The System Owner will update the authorization package as necessary through the life cycle of the system.

c. Task 3: Risk Determination

(1) The AO or AODR determines the risk to VA operations and assets, individuals, other organizations, and the Nation.

(2) The AO or AODR/DAS for Information Security assesses the information provided by the System Owner or Project Manager regarding the current security state of the system and the recommendations for addressing any residual risks.

(3) The AO or AODR may require risk assessments (either formal or informal) be employed to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations.

(4) The DAS for Information Security provides information to the AO that is considered in the final determination of risk to VA operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. Risk-related information includes the criticality of VA missions and/or business functions supported by the information system and the VA risk management strategy.

(5) When making the final risk determination, the AO or AODR considers VA's risk management strategy and the information provided by the System Owner or Project Manager in the security authorization package and the information regarding the effect of the operation and use of a system on VA operations and assets, individuals, and other organizations.

d. Task 4: Risk Acceptance

(1) The AO determines if the risk to VA operations and assets, individuals, other organizations, or the Nation is acceptable by balancing security considerations with mission and operational needs. The AO bases security authorization decisions on the content of the security authorization package and, where appropriate, any inputs received from key VA officials.

(2) The DAS for Information Security provides information to the AO that may be relevant and affect authorization decisions (e.g., VA risk tolerance, specific mission and business requirements, dependencies among information systems, and other types of risks not directly associated with the information system).

(3) After reviewing all of the relevant information the AO then issues an authorization decision for the information system.

(4) The AO conveys the security authorization decision, including relevant information provided from the DAS for Information Security, to the System Owner or Project Manager and makes the decision available to interested parties within VA (e.g., System Owners or Project Managers for interconnected systems, CIOs, Information Owners, senior managers). The authorization decision document contains:

(a) Authorization decision;

(b) Terms and conditions for the authorization, if applicable; and

(c) Authorization termination date, if applicable.

(5) The AO will indicate in the authorization decision document whether the system has received:

(a) ATO – if the AO deems the VA-level risk acceptable, an ATO is issued. The AO may issue an ATO with specific terms and conditions associated with the ATO for up to 36 months.

1. The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the System Owner and/or Project Manager. Terms and conditions will be specified in the authorization decision document.

2. The termination date indicates when the security authorization expires. The authorization termination date is not required when the ISCM program provides the AO with the needed information to conduct ongoing risk determination and risk acceptance activities.

(b) Denial of ATO – if, based on the results of the security assessment, the AO deems the VA-level risk unacceptable; the information system is not authorized for operation. If the system is currently in operation, all activity must cease. The AO will discuss with the System Owner and the Information Owner prior to shutting the system down. Failure to receive an ATO usually indicates the presence of major security control deficiencies in the system.

(6) The AO attaches the authorization decision document to the original security authorization package containing the supporting documentation and transmits it to the System Owner or Project Manager. Upon receipt of the authorization decision document and original authorization package, the System Owner or Project Manager acknowledges and implements the terms and conditions of the authorization and notifies the AO. The System Owner or Project Manager ensures that authorization documents for the information system are made available to appropriate VA officials. Authorization documents, especially information dealing with information system vulnerabilities, are:

(a) Uploaded into the VA-approved FISMA database;

(b) Marked and appropriately protected in accordance with Federal and VA policies;

(c) Retained in accordance with VA’s record retention policy; and

(d) Protected as sensitive in accordance with VA policy.

(7) The AO verifies, on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the System Owner.