Major Capability Acquisition Pathway Integration with Risk Management Framework

The content on this page is implementation guidance and best practices describing the policy found in DoD Instruction (DoDI) 8510.01 (reference (a)). Policy requirements are cited where appropriate. DoD Components may implement Risk Management Framework (RMF) requirements in a manner they choose consistent with DoDI 8510.01 and Executive Order 13800 (reference (b)).

This page was developed in collaboration with the RMF Technical Advisory Group community, the Services, the Office of the Under Secretary of Defense for Acquisitions and Sustainment, and the Office of the Under Secretary of Defense for Research and Engineering. For more information regarding policy and best practices, please contact the RMF TAG Secretariat (NIPR e-mail: OSD.RMFTAG-Secretariat@mail.mil).

The Major Capability Acquisition (MCA) Pathway is designed to acquire and modernize military unique systems that provide enduring capability. To adequately address cybersecurity risks in MCA activities, effective integration between Adaptive Acquisition Framework (AAF) and RMF teams needs is required.

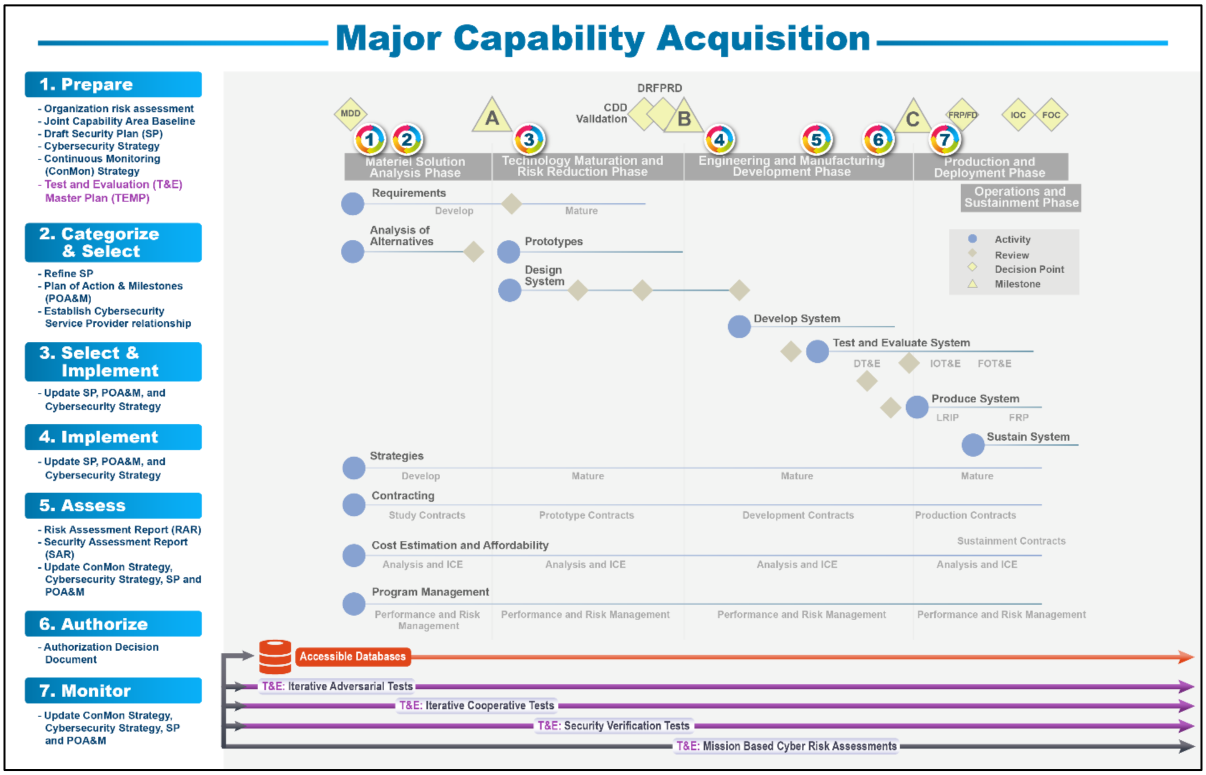
Major Capability Acquisition
1. Prepare
- Organization risk assessment
- Joint Capability Area Baseline
- Draft Security Plan (SP)
- Cybersecurity Strategy
- Continuous Monitoring (ConMon) Strategy
- Test and Evaluation (T&E) Master Plan (TEMP)
2. Categorize & Select
- Refine SP
- Plan of Action & Milestones (POA&M)
- Establish Cybersecurity Service Provider relationship
3. Select & Implement
- Update SP, POA&M, and Cybersecurity Strategy
4. Implement
- Update SP, POA&M, and Cybersecurity Strategy
5. Assess
- Risk Assessment Report (RAR)
- Security Assessment Report (SAR)
- Update ConMon Strategy, Cybersecurity Strategy, SP and POA&M
6. Authorize
- Authorization Decision Document
7. Monitor
- Update ConMon Strategy, Cybersecurity Strategy, SP and POA&M
MDD
A
DRFPRD
CDD Validation
B
C
FRP/FD
IOC
FOC
1
2
3
4
5
6
7
Materiel Solution Analysis Phase
Technology Maturation and Risk Reduction Phase
Engineering and Manufacturing Development Phase
Production and Deployment Phase
Operations and Sustainment Phase
Requirements
Develop
Mature
Analysis of Alternatives
Prototypes
Design System
Develop System
Test and Evaluate System
DT&E
IOT&E
FOT&E
Produce System
LRIP
FRP
Sustain System
Activity
Review
Decision Point
Milestone
Strategies
Develop
Mature
Mature
Mature
Contracting
Study Contracts
Prototype Contracts
Development Contracts
Production Contracts
Sustainment Contracts
Cost Estimation and Affordability
Analysis and ICE
Analysis and ICE
Analysis and ICE
Analysis and ICE
Program Management
Performance and Risk Management
Performance and Risk Management
Performance and Risk Management
Performance and Risk Management
Accessible Databases
T&E: Iterative Adversarial Tests
T&E: Iterative Cooperative Tests
T&E: Security Verification Tests
T&E: Mission Based Cyber Risk Assessments

Figure 1. Integrating RMF Steps in the MCA Pathway

Whereas DoDI 5000.85, “Major Capability Acquisition,” details the applicable policy and the AAF website provides acquisition best business practice, this page provides implementation guidance on integrating MCA and RMF processes thus enabling program office staff to use cybersecurity risk management techniques and tools to enhance major capability acquisition efforts (references (c) and (d)). This page does not supersede or eliminate the requirement to conduct AAF Pathway-specific actions.

Systems developed via the MCA Pathway follow the traditional RMF implementation processes as established in DoDI 8510.01 and on the RMF Knowledge Service (reference (a) and (e)). Unique AAF and RMF artifacts can support documentation and artifact creation in both processes. As such, this guidance maps RMF Steps, which are iterative in nature, and artifacts to each MCA phase.

Material Solution and Analysis Phase (MSA) (Pre-Milestone A)

The MSA phase includes planning activities and coincides with Prepare Step tasks that support subsequent RMF steps.

If practical, the program management office (PMO) should consider its digital engineering (DE) strategy and how this will support cybersecurity risk management. Use of DE helps teams identify security boundaries and potential attack surfaces. Teams can also configure DE environments to automatically create or populate some RMF artifacts.

It is also critical to begin thinking about how software will be developed and deployed, which can radically impact the planned RMF posture and selected controls as well as how RMF artifacts are developed and reviewed. Things like the use of government versus contractor software development environments, DevSecOps, and the use of continuous integration/continuous delivery (CI/CD) pipelines will impact controls and security boundaries.

Program management office (PMO) staff and RMF team members should begin collaborating as soon as possible as this allows program managers (PMs) to leverage key tasks and artifacts developed for the AAF process to inform RMF artifacts and vice versa. This close collaboration ensures MCA development includes cybersecurity considerations early – such as the need to establish test and evaluation strategies and active cyber defense agreements – and artifact reuse may reduce the amount of work needed. Early integration should also include organizational risk planning, system categorization, and establishing a control baseline based on organizations’ business/mission functions and Authorizing Officials’ risk tolerance (Prepare, Categorize, and Select Steps).

Integrating the Prepare Step in the MSA Phase

An organization’s adoption of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 standards – amongst other programmatic elements – is a key indicator of a cybersecurity program’s effectiveness. This adoption allows organizations to increase system development and authorization speed by standardizing security and privacy plan content. Prepare Step tasks vary as some are organization-wide focused while others are system-specific focused. According to DoD adoption of NIST standards in DoDI 8510.01, Appendix E, Table E-1, Prepare Tasks, Responsibilities, and Supporting Roles, in NIST SP 800-37, Revision 2 assigns roles for performing Prepare Step tasks (reference (f)).

This table in NIST 800-37 identifies who performs Prepare Step tasks. PMs and system owners should integrate with RMF teams early to ensure their acquisition activity leverages the organization's Prepare Step activities (Tasks P-1 through P-7) and appropriately coordinates the system level tasks (P-8 through P-18) for the specific system being developed. For an in-depth review of the Prepare Step, please refer to NIST SP 800-37, Revision 2, and the DoD-specific Prepare Step implementation guidance on the RMF Knowledge Service, which is forthcoming.

As PMO teams work through the MSA Phase, they need to work with RMF teams on Tasks P-8 through P-18. Specifically, the Prepare Step allows PMOs and RMF teams to have a holistic understanding of the risks posed to organizations' and systems' mission/business functions. This understanding will allow RMF and PMO teams to adopt control baselines as starting points so that when an operational need arises, organization's already have the organizational risks and baselines well understood and easily transferrable to system artifacts.

At this point, RMF teams need to start developing initial artifacts needed to support a later authorization decision. In addition to the risk management activities specified in DoDI 5000.85, cybersecurity risk planning in this phase needs to include:

- Completing an initial organizational cybersecurity risk assessment as part of the Prepare Step (NIST SP 800-30); ideally organizations have a risk assessment and NIST Cybersecurity Framework Profile already completed for MCA teams to leverage (reference (g) and (h));
- Establishing baseline security and privacy controls based on the organization's risk tolerance, Level II mission area owner guidance, and common or hybrid control inheritance to record in the Security Plan (reference (i));
- Registering the system in all relevant tracking databases (e.g., Enterprise Mission Assurance Support Service, DoD Information Technology Portfolio Repository) and capturing this information in the Security Plan;
- Preparing a draft system-level Continuous Monitoring (ConMon) Strategy;
- Establishing a Cybersecurity Strategy, as approved by the cognizant Chief Information Officer;
- Defining requirements through the Joint Capabilities Integration and Development System process and the Cyber Survivability Endorsement Key Performance Parameters.

Integrating the Categorize Step in the MSA Phase

Per DoDI 8510.01, after adopting initial baselines in the Prepare Step, the PMO and RMF team using the MCA Pathway must categorize the system in the Categorize Step. Categorization for

DoD systems parallels the system life cycle. RMF team members categorize the system per CNSSI 1253, "Categorization and Control Selection for National Security Systems," and document the results of this categorization in the Security Plan (reference (j)).

For more details on how to perform tasks in the Categorize Step, refer to the implementation guidance for system categorization (reference (k)).

Key artifacts developed in the Categorize Step:

- Further refine the Security Plan, as approved by the system's responsible Authorizing Official;
- Establish a Test and Evaluation Master Plan (TEMP) consistent with DoDI 5000.89, "Test and Evaluation," that includes early, iterative cyber testing. Specific test and evaluation (T&E) requirements and processes, throughout the system lifecycle, are covered by DoD Instruction 5000.89, "Test and Evaluation," and appropriate T&E guidebooks (reference (l)).

Integrating the Select Step in the MSA Phase

In MCA use cases, early RMF integration also means selecting security and privacy controls in the Select Step and capturing these in an initial Plan of Action and Milestones (POA&M) (reference (m)).

Based on the system categorization, the Select Step explains the process for further refining the control baseline established in Task P-4 and selecting a final control set for DoD systems, as found in CNSSI 1253, "Categorization and Control Selection for National Security Systems", with further discussion and detail in DoDI 8510.01 (reference (j)).

For MCA capabilities that have a significant amount of developed software (applications), AAF teams should consider separating the software development and utilizing the Software Acquisition Pathway. In planning for development, consider the software development plan and whether the use of a software factory and DevSecOps pipeline with an existing continuous Authorization to Operate (cATO) is viable (reference (n)).

For more details on how to perform tasks in the Select Step, refer to the implementation guidance pages for control selection (reference (o)).

PMO and RMF teams should have developed the following artifacts in the Select Step:

- An updated Security Plan;
- A formal agreement between a cybersecurity service provider (CSSP) and the organization developing the MCA system (known as the Subscriber to the CSSP services);
- A draft POA&M.

Technology Maturation and Risk Reduction Phase (Milestone A to Milestone B)

RMF and PMO team members, per DoDI 8510.01, must conduct a risk assessment consistent with NIST SP 800-30 on the system being developed, and continue to refine the baseline established in the Prepare and Select Steps as the system matures. In addition, per DoDI 8510.01, RMF teams must identify these security and privacy control updates in the system's Security Plan (Select and Implement Steps).

Integrating the Implement Step in the Technology Maturation and Risk Reduction Phase

AAF and RMF teams can start implementing controls during system designing and prototyping in the MCA Technology Maturation and Risk Reduction Phase. PMOs and RMF teams should require development contractors to decompose the high-level technical controls into detailed system performance specifications and designs in system specifications at level 3 and, depending on the system involved, down into levels 4 and 5. This decomposition enables contractors to implement technical control specifications and develop technical performance measures for each level so that they can demonstrate relevant implementation starting at each component/subcomponent level.

Failure to decompose controls like this in TMRR could result in significant challenges in later lifecycle phases. PMOs and RMF teams need to jointly develop contract language, which decomposes the RMF controls needed for a system. Failure to do this may leave key areas of DoD concern unaddressed by contractor selection of controls. By collaborating in this decomposition, PMOs and RMF teams can understand where controls may not be implementable. This can also identify how other engineering requirements may conflict with controls thus resulting in certain implementation not being realistic.

For more details on how to perform Implement Step tasks, refer to the implementation guidance on how to implement controls (reference (p)).

At this point, PMO teams should have the following RMF artifacts:

- An updated Security Plan;
- An updated Cybersecurity Strategy, as needed.

Engineering and Manufacturing Development (EMD) Phase

During this phase, RMF and PMO teams need to update their system's POA&M, Security Plan, and Cybersecurity Strategy based on the maturity of the technology. Such updates should include corrective actions on any feedback from the CSSP. After completing these updates, the RMF and PMO teams need to complete a Security Assessment Report and Risk Assessment Report as well as update the ConMon Strategy (Implement and Assess Steps).

Integrating the Assess Step in the EMD Phase

After the critical design review and test readiness review events, system development testing and evaluation begins. Teams finalize Implement Step activities during system development and should begin Assess Step actions during system test and evaluation. RMF teams can only assess the effectiveness of controls after they have been selected and implemented.

The security assessment plan approval process establishes the appropriate expectations for the control assessment and establishes the control assessment's level of effort. An approved security assessment plan, as developed by the Security Control Assessor (SCA), ensures the organization uses the appropriate resources to determine control effectiveness.

Per DoDI 8510.01, even if a compelling mission or business need requires the rapid introduction of a new system, assessment activity and a Security Assessment Report are still required (reference (q)).

The SCA also develops a Risk Assessment Report assessing the risk of non-compliant controls and addresses vulnerabilities displayed in the Security Assessment Report after the control assessment has been completed (reference (r)). All non-compliant controls must be subjected to a risk assessment that considers multiple factors in assigning a residual risk level to each non-compliant control. The individual risk levels are then used to inform the SCA’s recommendation (i.e., Security Assessment Report executive summary) to the Authorizing Official on acceptance of the cybersecurity risk of operating the system.

For more details on how to perform Assess Step tasks, refer to the assessment guidance pages, Security Assessment Report template, and Risk Assessment Report template (reference (s)).

Key artifacts developed during this phase include:

- The Security Assessment Report;
- The Risk Assessment Report, if applicable;
- Any updates to the POA&M, Security Plan, and ConMon Strategy, if applicable.
- Any updates to the cyber T&E Strategy need to be documented in the TEMP.

Integrating the Authorize Step in EMD Phase

Before exiting the EMD Phase, the system being developed must receive an authorization decision before moving into the Production and Deployment Phase (Authorize Step). Because of their early involvement, the Authorizing Official’s risk tolerance has been well established and considered in the MCA development process. As such, the RMF team assembles a Security Authorization Package for transmission to the Authorizing Official (reference (t)).

Before transitioning to operations and sustainment, consistent with DoDI 8510.01, every system used in the Department must have an Authorizing Official responsible for authorizing the system’s operation based on achieving and maintaining an acceptable risk posture. All authorization decisions should also be supported by data from relevant T&E assessments results, to include early and iterative adversarial cyber testing; failure to have this supporting T&E data endangers the likelihood of an affirmative authorization decision.

For more details on Authorize Step tasks, please refer to the implementation guidance for authorizing systems (reference (u)).

Production and Deployment Phase (Post-Milestone C)

After an authorization decision has been issued, the system is produced and deployed. Accompanying this deployment is the system-level ConMon Strategy that communicates requirements to monitor the system's performance and produce artifacts for reauthorization of the system.

As the program matures, a focus should be given to increasing the automation of security scans and testing, and further streamlining the authorization to operate (ATO) process. The focus should be on being able to rapidly deploy not only critical mission functionality, but also to rapidly patch or remove vulnerabilities across the full deployed environment and supply chain. As with preceding phases, continue to leverage DoD enterprise service and repositories to maximize reuse and leverage reciprocity, where possible.

For programs with large software development efforts, refer to the guidance for the Software Acquisition Pathway for further suggestions on how to address RMF for the software.

Operations and Sustainment Phase (Post-Full Rate Production or Full Deployment Decision)

As the system's lifecycle progresses, so too does the system's RMF process. In Operations and Sustainment, organizations must maintain the system's body of evidence and monitor the system's controls, per DoDI 8510.01, to ensure changes to the security status are documented in the POA&M and appropriate changes are made to the ConMon Strategy. Earlier RMF processes should be iterated upon as systems take on new capabilities or undergo significant changes.

Ensure support contracts include the use of automation for security implementation and testing to reduce the time and increase efficiency for those activities. The focus should continue to be on being able to rapidly deploy not only critical mission functionality, but also to rapidly patch or remove vulnerabilities across the full deployed environment and supply chain. Enabling continuous monitoring of applications and infrastructure is key to DevSecOps and will be of particular importance in this phase. Programs will probably be releasing software updates and patches independent of, and more frequently than, hardware changes. Ensure the ATO approach supports that capability. Again, leverage DoD enterprise services and repositories to maximize reuse and leverage reciprocity, where possible.

For programs with large software development, refer to the guidance for the Software Acquisition Pathway for further suggestions on how to address RMF for the software.

Integrating the Monitor Step in the Operations and Sustainment Phase

Systems developed via the MCA Pathway, as with all DoD systems, must adhere to limitations of the authorization determination, as established by DoDI 8510.01. Additionally, the continuous monitoring artifacts, as required in the ConMon Strategy, will support continued operation of the system via the Monitor Step.

The Monitor Step focuses on monitoring security and privacy controls associated with the system. The objective is to conduct continuous monitoring of the security of an organization's networks, information, and systems in accordance with organizational and system-level information security continuous monitoring (ISCM) strategies, and respond by accepting, avoiding, mitigating, sharing, or transferring risk as situations change. Monitoring is the phase of the RMF that supports the complementary goals of Federal Information Security Modernization Act (FISMA) of 2014 compliance and maintaining ongoing system security.

ISCM in and of itself, does not provide a comprehensive, enterprise-wide risk management approach. Rather, ISCM activities help Authorizing Officials make better informed risk-based decisions. Robust ISCM allows a move toward ongoing authorization but until such time as the DoD CIO determines that the DoD ISCM program is mature and robust enough to support ongoing authorization, DoD will continue to minimally require 3-year re-authorization.

Automation can make the process of ISCM more cost-effective, consistent, and efficient. Many of the controls defined in NIST SP 800-53 – especially in the technical families of Access Control, Auditing and Accountability, Identification and Authentication, and Systems and Communications Protection – are good candidates for monitoring using automated tools and techniques. Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those selected controls. It is also important to recognize that with any comprehensive information security program, all implemented controls, including management and operational controls, must be regularly assessed for effectiveness, even if monitoring them is not easily automated.

Monitoring activities track:

- System and Environment Changes;
- Ongoing Security Control Assessments;
- Ongoing Remediation Actions;
- Key Updates;
- Security Status Reporting;
- Ongoing Risk Determination and Acceptance;
- System Removal and Disposal.

For more information on Monitor Step tasks, refer to the guidance for monitoring systems (reference (v)).

Decommissioning, Demilitarization, and Disposal

At the system’s end-of-life, organizations must follow the decommissioning guidance in the Monitor Step, per DoDI 8510.01, to execute required actions when a system is removed from service. In the MCA Pathway, decommissioning is better known as demilitarization.

For more information on decommissioning/demilitarizing tasks, refer to the implementation guidance for system decommissioning (reference (w)).

References

(a) DoDI 8510.01, “RMF for DoD Systems,” July 19, 2022

(b) Executive Oder 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017

(c) DoDI 5000.85, “Major Capability Acquisition,” August 6, 2020, Change 1 Effective November 4, 2021

(d) Defense Acquisition University, “Major Capability Acquisition,” as amended <https://aaf.dau.edu/aaf/mca/>

(e) RMF Knowledge Service, “RMF Implementation,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Pages/default.aspx> (CAC-enabled)

(f) National Institute for Standards and Technology, Special Publication 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018 <https://doi.org/10.6028/NIST.SP.800-37r2>

(g) National Institute for Standards and Technology, Special Publication 800-30, Revision 1, “Guide for Conducting Risk Assessments,” September 2012 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>;

(h) National Institute for Standards and Technology, “Cybersecurity Framework,” as amended <https://www.nist.gov/cyberframework/framework>

(i) RMF Knowledge Service, “RMF Security Plan,” as amended https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx (CAC-enabled)

(j) Committee on National Security Systems Instruction 1253, “Categorization and Control Selection for National Security Systems,” July 29, 2022 <https://www.cnss.gov/CNSS/openDoc.cfm?a=eVuxLh6gL147vpwzMn2Upg%3D%3D&b=1036F8BB907D6C6E578A3D4D4443DE9293E7058752CD380FCA445F86B737DCB3E4DBC6DDF6BA4BD84DDED21095040EF8>

(k) RMF Knowledge Service, “DoD System Security Categorization Determination,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Categorize/Pages/DoDIS.aspx> (CAC-enabled)

(l) DoDI 5000.89, “Test and Evaluation,” November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>

(m) RMF Knowledge Service, “RMF Plan of Action and Milestones (POA&M),” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/POAM.aspx>

(n) Office of the Secretary of Defense Memorandum, “Continuous Authorization to Operate (cATO),” February 2, 2022 <https://dodcio.defense.gov/Portals/0/Documents/Library/20220204-cATO-memo.PDF>

(o) RMF Knowledge Service, “Step 2: Select Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Select/Pages/default.aspx> (CAC-enabled)

(p) RMF Knowledge Service, “Step 3: Implement Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/ImplementControls/Pages/default.aspx> (CAC-enabled)

(q) RMF Knowledge Service, “RMF Security Assessment Report,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAR.aspx> (CAC-enabled)

(r) RMF Knowledge Service, “RMF Risk Assessment Report (RAR) for Non-Compliant Security Controls,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/RiskAssessment.aspx> (CAC-enabled)

(s) RMF Knowledge Service, “Step 4: Assess Security Control,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/default.aspx> (CAC-enabled)

(t) RMF Knowledge Service, “Introduction to Security Authorization Package,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAPIntro.aspx> (CAC-enabled)

(u) RMF Knowledge Service, “Final Risk Determination and Authorization Decision,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Authorize/Pages/FinalAuthDecision.aspx> (CAC-enabled)

(v) RMF Knowledge Service, “Monitor Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/MonitorControls.aspx> (CAC-enabled)

(w) RMF Knowledge Service, “Decommission,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/Decommission.aspx> (CAC-enabled)