Urgent 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 (TAG) community, the Services, the Office of the Under Secretary of Defense for Acquisition 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 Urgent Capability Acquisiton (UCA) Pathway aggressively streamlines the acquisition process to plan capabilities within weeks and finish development and production within months instead of the more traditional acquisition process. Whereas DoDI 5000.81, “Urgent Capability Acquisition,” provides the applicable policy and the Adaptive Acquisition Framework (AAF) website provides acquisition best business practices, this page provides implementation guidance on integrating the UCA process and the iterative RMF process together (references (c) and (d). This enables practitioners to use cybersecurity risk management techniques and tools to enhance this quick-moving Pathway acquisition. This page does not supersede or counteract the need to conduct AAF Pathway-specific actions.

Pre-Development

Integrating the UCA and RMF processes together needs to begin as early as possible in the UCA pathway because this will allow Program Managers to leverage RMF tools and bodies of knowledge, such as the organization’s Prepare Step activities and Mission Area baselines. In Pre-Development, RMF and UCA program management office (PMO) teams need to begin developing the Cybersecurity Strategy, the system Security Plan, and establishing an active cyber defense agreement (reference (e)). Failure to incorporate cybersecurity stakeholders from the beginning of the UCA Pre-Development stage will likely have unintended side effects to timely deployment of UCA capabilities. This is likely to result in a system that does not have sufficient cybersecurity protections.

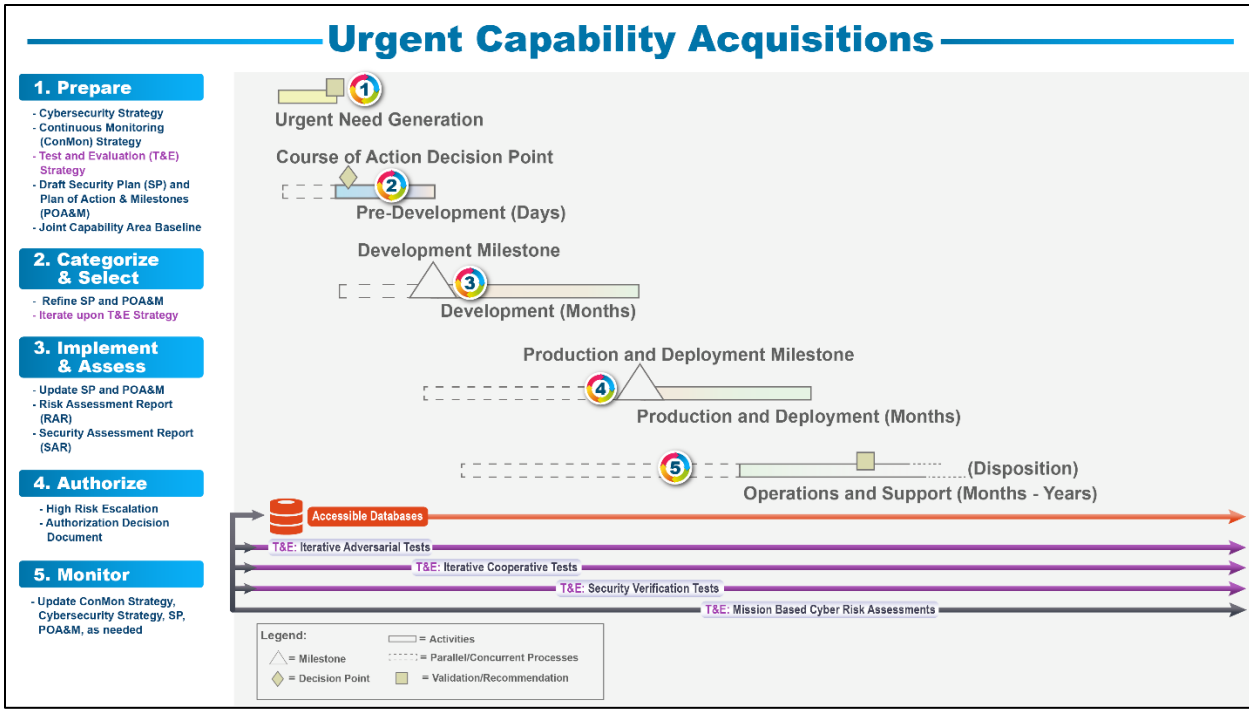

Figure 1. Integrating RMF Steps in the UCA Pathway

Additionally, organizations must also develop a Test and Evaluation (T&E) Strategy for the Pathway capability consistent with DoDI 5000.89, "Test and Evaluation" (reference (f). This strategy and iterative cyber T&E assessments will inform development and authorization of the capability. Specific T&E requirements and processes, throughout the system lifecycle, are covered by DoD Instruction 5000.89 and appropriate T&E guidebooks (Prepare, Categorize, and Select Steps).

Integrating the Prepare Step in Pre-Development

The teams should leverage the planning activities in the RMF Prepare Step to identify organization-wide risks and consider what mission/business functions the UCA capability will fulfill along with risks involved in those functions. Consistent with DoDI 8510.01, organizations must also begin to apply any Level II baselines and risk tolerances for their specific mission area, as appropriate. Program managers and system owners should partner with RMF personnel as early as possible to work Prepare Step activities from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, which – amongst other programmatic elements – is a key indicator of a cyberesecurity program's effectiveness (Prepare Step) (reference (g)). Teams should also begin creating a T&E strategy that incorporates an iterative cyber T&E strategy for continued refinement in later lifecycle stages and ensure RMF artifacts are informed by cyber T&E data. 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.

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, which is forthcoming.

At this point, PMO and RMF teams should begin developing the following artifacts:

- A Cybersecurity Strategy;
- A Continuous Monitoring Strategy;
- A Security Plan;
- An initial Plan of Action and Milestones (POA&M) (reference (h));
- A T&E Strategy, with iterative cyber T&E.

Integrating the Categorize Step in Pre-Development

Per DoDI 8510.01, after adopting initial baselines in the Prepare Step, the PMO and RMF teams using the UCA 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 (i)).

During this categorization, some UCA programs may prioritize major risks to mission/business functions and leave other risk considerations to be addressed in subsequent development in other AAF Pathways or later in the system's current UCA lifecycle. Though not advised, UCA rapidity may necessitate this.

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

Artifacts developed during this lifecycle phase include:

- Refine Security Plan and POA&M
- Continue develop evidence from cyber assessments driven by the T&E Strategy

Integrating the Select Step in Pre-Development

Early RMF integration also means selecting security and privacy controls in the Select Step and capturing these in a POA&M because of the need to rapidly produce and deploy systems. Early RMF integration means RMF and UCA teams can leverage existing evidence from similar DoD systems, commercial capabilities, or iterative cyber T&E assessments – consistent with DoDI 5000.89, "Test and Evaluation" – to inform control selection and POA&M development (reference (k)).

Based on the system categorization, the Select Step explains the process for further refining the security and privacy control baseline established earlier in the Prepare Step – Task P-4 – and selecting a final security 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.

For more details on how to perform tasks in the Select Step, refer to the implementation guidance pages for selecting controls (reference (l)).

Artifacts developed during this lifecycle phase include:

- Refine the Security Plan and POA&M;
- Iterative cyber T&E Strategy assessments.

Development

In this lifecycle phase, RMF and PMO teams need to have open communications as the cybersecurity community develops a POA&M and conducts Risk Assessment and Security Assessment Reports; these artifacts are consistent with the Categorize, Select, Implement, and Assess Steps in the RMF Process. These RMF tools will inform updates to the Acquisition Strategy and ADM, as developed in the Pre-Development phase; and any needed Rapid Acquisition Authority or T&E assessments. Consistent with DoDI 5000.81, urgent needs may need to advance in spite of identified deficiencies or even non-compliant controls; however, it is important that PMO and RMF teams are integrated to the greatest extent possible to ensure that Authorizing Officials' risk tolerance and priorities are addressed during development.

Due to the identified deficiencies or non-compliant controls, Development activities need to include methods of reducing and monitoring system risks. Even with such mitigations, the operation of systems developed using the UCA Pathway may prove high-risk from a cybersecurity perspective because of identified deficiencies or non-compliant controls; however, mission needs may require production and deployment despite such risks. As such, risks need to be well understood and consistent with the relevant Mission Area baseline and risk tolerances established by the appropriate Authorizing Officials, as established in Pre-Development integration.

Integrating the Implement Step in Development

Given initial development has been done, a focus should be given to increasing the automated of security scans and testing, which further streamlines the authorization process. The focus should be on rapidly deploying critical mission functionality and equally on rapidly patching or removing 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.

Programs with large software development efforts should refer to the guidance for the Software Acquisition Pathway for further suggestions on how to address risk management for software development.

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

Key artifacts updated in this phase include:

- Security Plan;
- Plan of Action and Milestones.

Integrating the Assess Step in Development

After selecting and implementing controls, RMF teams can assess the effectiveness of these controls.

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

The SCA also develops a Risk Assessment Report assessing the risk of non-compliant security controls and addresses vulnerabilities displayed in the Security Assessment Report after the security control assessment has been completed (reference (o)). All non-compliant security and privacy controls must be subjected to a risk assessment that considers multiple factors in assigning a residual risk level to each non-compliant security 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 (p)).

Key artifacts developed in this phase include:

- The Security Assessment Report;
- The Risk Assessment Report, if applicable;
- Any updates to the POA&M and Security Plan, if applicable.

High-Risk Escalation Process

Because systems developed in the UCA Pathway are likely to have more cybersecurity risks due to prioritized risk management, organizations should have a high-risk escalation process to quickly review and accept high-risk systems just before the Authorize step and transitioning to the Production and Deployment lifecycle phase. DoD Components will develop a rapid process for demonstrating performance and evaluating UCA systems and system components. This process will leverage the T&E Strategy, included in the Acquisition Strategy, and iterative cyber

T&E test results demonstrating operational performance, to include validation of required cybersecurity, survivability, and resilience requirements and interoperability, as applicable.

This process does not alleviate Authorizing Officials from authorizing systems, but instead it ensures high-risk systems meet appropriate minimum security criteria, have conducted a security assessment report, and have a plan to mitigate system risks so they do not cause additional mission risks. This escalation process should require a multi-level recommendation and approval structure to include operational commanders with cyber threat information, functional leaders in the cybersecurity and acquisition communities, Authorizing Officials, and Mission Owners.

Integrating the Authorize Step in Development

Just before the Production and Deployment Milestone, UCA systems are ready for authorization in the Authorize Step. Because of their early involvement, the Authorizing Official's risk tolerance has been well established and considered in the UCA Pre-Development and Development processes, and the system's high risk has been accepted by an organizational risk escalation structure. As such, the RMF team assembles a Security Authorization Package for transmission to the Authorizing Official (reference (q)).

After the high-risk escalation process, the Authorizing Official will provide an authorization decision to the PM responsible for the UCA system in the Authorize Step. Due to the mission need and pace of the Pathway, an Authoriation to Operate with Conditions is likely if appropriate risk escalation procedures have been followed and appropriate mitigations have been established. These must be recorded in the POA&M. Upon production and fielding of the system, the PMO and RMF teams involved should communicate residual risk levels as well as mitigation methods to the field.

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, iterative adversarial cyber testing; failure to have this supporting T&E data endangers the likelihood of an affirmative authorization decision.

For more details on the Authorize Step, refer to the implementation guidance for authorizing a system (reference (r)).

Production and Deployment and Operations and Support

Systems developed via the UCA Pathway must adhere to limitations of the authorization granted. Additionally, the continuous monitoring artifacts, as required in the Continuous Monitoring Strategy shaped since the Prepare Step, developed in the Monitor Step will support continued operation of the system. At the system's end-of-life, organizations must follow decommissioning guidance. If transitioning to a new program of record, the UCA Pathway must also follow AAF procedures as found in DoDI 5000.81 and leverage the guidance directing how to integrate RMF and AAF artifacts when switching Pathways.

Integrating the Monitor Step in Production and Deployment and Operations and Support

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.

If not transitioning to another Pathway, PMOs and RMF teams must follow decommissioning guidance for systems as required by DoDI 8510.01.

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

References

(a) DoDI 8510.01, “RMF for DoD Systems, July 19, 2022 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=5YnACrAlUCPZ_qeq4T5nlg%3d%3d>
(b) Executive Order 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 16, 2017 <https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>
(c) DoDI 5000.81, “Urgent Capability Acquisition,” December 31, 2019 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500081p.PDF>;
(d) Defense Acquisition University, “Urgent Capability Acquisition,” as amended <https://aaf.dau.edu/aaf/uca/>
(e) RMF Knowledge Servie, “RMF Security Plan,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx> (CAC-enabled)
(f) DoDI 5000.89, “Test and Evaluaiton,” November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>
(g) National Institute for Standards and Technology, Special Publicaiton 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>
(h) RMF Knowledge Service, “RMF Plan of Action and Milestones,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/POAM.aspx> (CAC-enabled)
(i) Committee on National Securit Systems Instruction 1253, “Categorization and Control Selection for National Security Systems,” July 29, 2022 <https://www.cnss.gov/CNSS/openDoc.cfm?a=sLZqUcRxjXmxdGL0h%2BgeSw%3D%3D&b=6DE079AB1D8ACAE7DE40122D566A009DE64B2377FE4BE25753D3346B65282614DA1D8E8E160E6D933CEE1ED0D3B438A8>
(j) RMF Knowledge Service, “DoD System Security Categorization Determination,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Categorize/Pages/DoDIS.aspx> (CAC-enabled)
(k) DoDI 5000.89, “Test and Evaulation,” November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>
(l) RMF Knowledge Service, “Step 2: Select Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Select/Pages/default.aspx> (CAC-enabled)

(m) RMF Knowledge Service, “Step 3: Implement Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/ImplementControls/Pages/default.aspx> (CAC-enabled)
(n) RMF Knowledge Service, “RMF Security Assessment Report,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAR.aspx> (CAC-enabled)
(o) 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)
(p) RMF Knowledge Service, “Step 4: Assess Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/default.aspx> (CAC-enabled)
(q) RMF Knowledge Service, “Introduction to Security Authorization Package,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAPIntro.aspx> (CAC-enabled)
(r) RMF Knowledge Service, “Final Risk Determination and Authorization Decision,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Authorize/Pages/FinalAuthDecision.aspx> (CAC-enabled)
(s) RMF Knowledge Service, “Step 6: Monitor Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/default.aspx> (CAC-enabled)