Middle Tier of 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 Middle Tier of Acquisition (MTA) Pathway allows organizations to rapidly prototype systems that already have existing maturity or to accelerate system maturation for rapid fielding or transfer to another long-term Pathway.

Whereas DoDI 5000.80, “Operation of the MTA,” provides policy and the Adaptive Acquisition Framework (AAF) website provides acquisition best practices, this page provides implementation guidance on integrating MTA and RMF processes together thus enabling practitioners to use cybersecurity risk management techniques and tools to enhance this Pathway’s activities (reference (c) and (d)).

This Pathway requires minimal additional guidance beyond the need to move fast so both processes Rapid Prototyping and Rapid Fielding should follow the traditional DoD RMF process, which is iterative in nature. This page does not supersede or counteract the need to conduct AAF Pathway-specific actions.

MTA Planning

In order to move at speed within the rapid MTA Pathway, organizations should have mature cybersecurity risk management processes in place per DoD’s adoption of National Institute of Standards and Technology (NIST) tools as an integrated enterprise-wide risk decision structure per DoDI 8510.01.

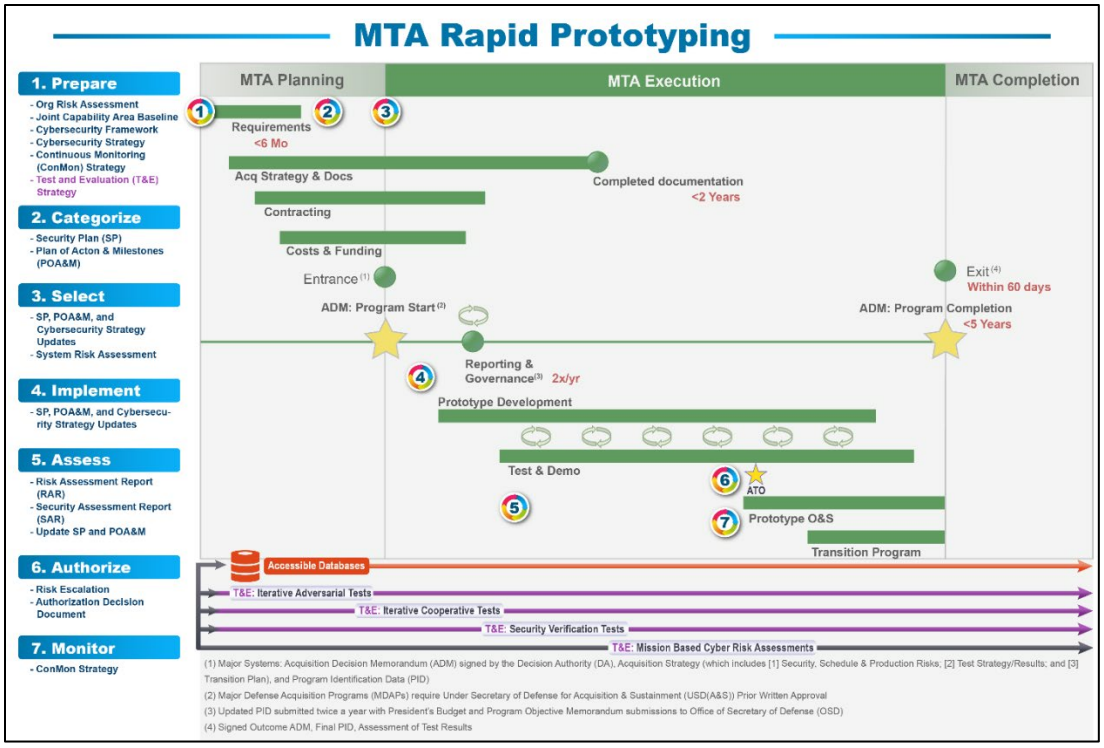

Figure 1. Integrating RMF Steps in the MTA Rapid Prototyping

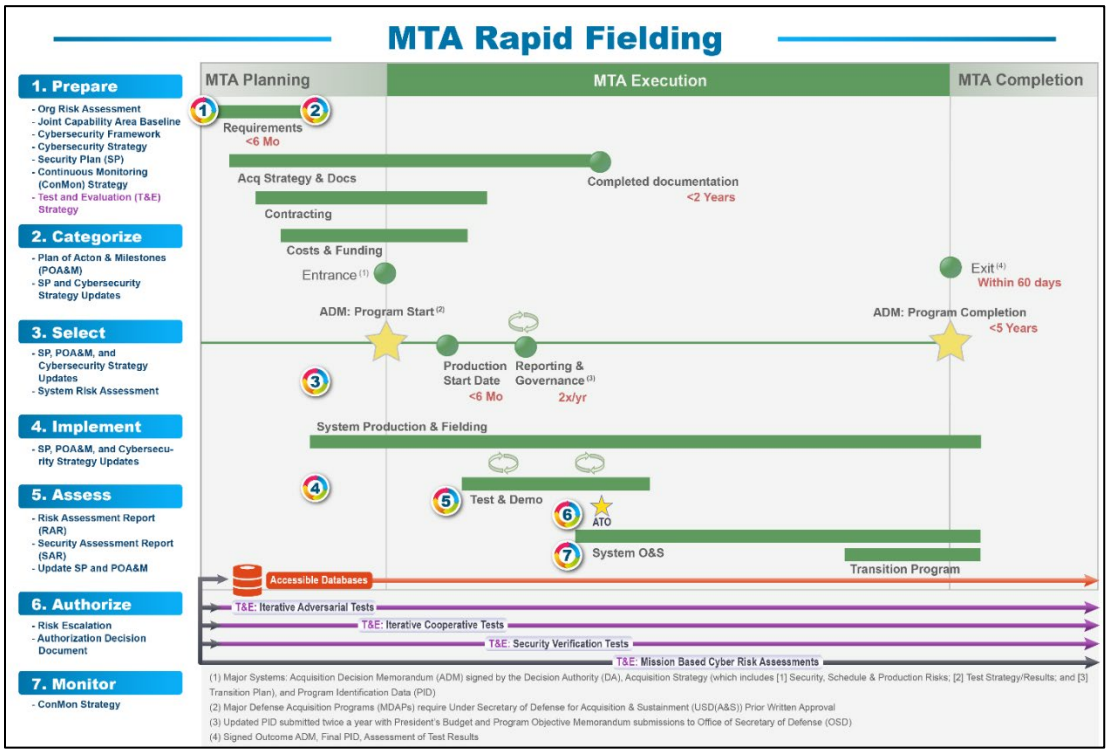

Figure 2. Integrating RMF Steps in the MTA Rapid Fielding Pathway

Integrating the Prepare Step in Prototyping and Rapid Fielding

One such indicator of cybersecurity program maturity – among other key programmatic elements – is organization's adoption of the NIST Special Publication (SP) 800-37, Revision 2, Prepare Step, consistent with DoDI 8510.01. 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. Table E-1, Prepare Tasks, Responsibilities, and Supporting Roles in Appendix E of NIST SP 800-37, Revision 2 identifies who performs Prepare Step tasks. Program Managers 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. This early collaboration also ensures MTA development includes cybersecurity considerations early – such as the need to establish test and evaluation strategies and active cyber defense agreements. 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 (reference (e)).

As AAF teams work through MTA Planning, they need to work with RMF teams on Tasks P-8 through P-18. Specifically, the Prepare Step allows program management offices (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 security 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.

If practical, the 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. At this point, RMF teams need to start developing initial artifacts needed to support later a later authorization decision. These include:

- Completing an initial cybersecurity risk assessment (NIST SP 800-30) (reference (f));
- Establishing initial control baseline based on both Level II mission area owner guidance and the organization's unique Cybersecurity Framework profile, if applicable;
- Establishing a Cybersecurity Strategy;
- Establishing a Security Plan (reference (g));
- Begin developing a Plan of Action and Milestones (POA&M) (reference (h));
- Developing a draft system-level Continuous Monitoring (ConMon) Strategy.

Integrating the Categorize Step in Prototyping and Rapid Fielding

Per DoDI 8510.01, after adopting initial baselines in the Prepare Step, the PMO and RMF teams using the MTA Pathway must categorize the system in the Categorize Step 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 MTA 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 MTA lifecycle. Though not advised, MTA rapidity may necessitate this.

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

Key artifacts developed during this lifecycle phase:

- Refine Security Plan and Plan of Action and Milestones (POA&M);
- Establishing a Test and Evaluation (T&E) Strategy, that includes an iterative cyber T&E Strategy. Specific T&E requirements and processes, throughout the system lifecycle, are covered by DoDI 5000.89, "Test and Evaluation," November 19, 2020, and appropriate T&E guidebooks (reference (k)).

Integrating the Select Step in Prototyping and Rapid Fielding

In both MTA use cases – Prototyping and Rapid Fielding – 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. In the Rapid Prototyping use case, early RMF integration means RMF and MTA teams can leverage existing evidence from similar DoD systems, commercial capabilities, and iterative cyber T&E assessments – consistent with DoDI 5000.89, "Test and Evaluation" – to inform control selection, authorization, and POA&M development.

Based on the system categorization, the Select Step explains the process for further refining the security control baseline established in 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 prototypes that have a significant amount of developed software (applications), PMOs should consider separating this 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 (l)).

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

Integrating the Implement Step in Rapid Fielding

Because a previous body of evidence exists for systems being developed in the Rapid Fielding use case, PMO and RMF teams can immediately start implementing controls when system production and fielding begins in the MTA Planning phase.

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 Implement Step tasks, refer to the implementation guidance for implementing controls (reference (n)).

MTA Execution

Integrating the Select Step in Prototyping

In the Prototyping lifecycle, as the MTA team develops acquisition and funding strategies, RMF teams register the system in the appropriate tracking systems and continue their work to refine the existing POA&M and control selections, as previously discussed, with the available evidence as the Acquisition Strategy is developed.

Integrating the Implement Step in Prototyping

At the Acquisition Decision Memorandum Program Start in the Prototyping use case, the PMO and RMF team can begin the Implement Step, as previously discussed, as they develop prototypes, implement controls for these systems, and assess their effectiveness. RMF and PMO teams should coordinate efforts with T&E to inform continued updates to the POA&M and other relevant artifacts.

Implementing the Assess Step in Prototyping and Rapid Fielding

After prototype development or rapid fielding production begins, RMF teams can assess the effectiveness of the controls after they have been selected and implemented.

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 (o)).

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 (p)). 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 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 the Assess Step, refer to the implementation guidance for assessing controls (reference (q)).

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

If system development in the MTA Pathway only focuses on major, prioritized cybersecurity risks and not holistic cybersecurity risks, this MTA system may be considered high-risk. In such cases, DoD Components will develop a process for demonstrating performance and evaluating MTA 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. Organizations need to have a rigorous organizational level risk acceptance process to review high-risk systems right before an Authorizing Official can authorize the system for operations and sustainment. This high-risk

escalation process ensures system development and authorization has sufficient information on cyber threats, functional needs, and mission priorities.

This escalation process can be unique to each organization; however, before the risk escalation workflow can begin, RMF and MTA teams need to meet certain organization-defined minimum security criteria, have a Security Assessment Report, an up to date POA&M explaining how risks will be mitigated, and a ConMon Strategy explaining the frequency and level of monitoring the system will receive.

If an MTA system's high-risk is accepted by the multi-level recommendation and approval structure, the system can advance to the Authorizing Official for an authorization decision. If the system's high-risk is not accepted, the system needs to reenter development and testing to drive down risk before returning to the risk escalation process. This risk management process does not alleviate Authorizing Officials from authorizing systems, but instead ensures high-risk systems have plans to mitigate system risks that could cause additional mission risks.

Integrating the Authorize Step in Prototyping and Rapid Fielding

At this point, MTA 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 MTA development process, and the system's high-risk has been accepted, if applicable, by an organizational risk escalation structure. As such, the RMF team assembles a Security Authorization Package for transmission to the Authorizing Official (reference (r)).

Before transitioning to operations and sustainment, consistent with DoDI 8510.01, every system used in the Department – including those in Rapid Prototyping Programs, Rapid Fielding Programs, and MTA Programs that have transitioned to the Major Capability Acquisition pathway – 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. If granted an IATT, at the conclusion of the IATT, systems should have the body of evidence to further inform future actions, such as continued development or fielding with a new authorization decision.

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

Integrating the Monitor Step in Prototyping and Rapid Fielding Operations and Sustainment

Systems developed via the MTA 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 established in the Prepare Step, 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 implementation guidance for monitoring systems (reference (t)).

MTA Completion

If transitioning to a new AAF Pathway, the MTA Pathway team must also follow AAF procedures as found in DoDI 5000.80 and leverage the guidance directing how to integrate RMF and MTA artifacts when switching Pathways.

If at the system's end-of-life, organizations must follow the decommissioning guidance in the Monitor Step to execute required actions when a system is removed from service (reference (u)).

See the decommissioning guidance for more details on performing this task or if transferring to another Pathway, see the guidance on switching Pathways.

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 5000.80, "Operation of the Middle Tier of Acquisition (MTA)," December 30, 2019 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500080p.PDF>;

(d) Defense Acquisition University, "Middle Tier of Acquisition (MTA)," as amended <https://aaf.dau.edu/aaf/mta/>

(e) 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>

(f) 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>

(g) RMF Knowledge Service, "RMF Security Plan," as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx> (CAC-enabled)

(h) RMF Knowledge Service, "RMF Plan of Action and Milestones (POA&M)," as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/POAM.aspx> (CAC-enabled)

(i) 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=q2kjpkLxUvHH8vvqvPDyHQ%3D%3D&b=2F87494A837B20C8A2F64441E5BBB7817781D4F75126374CF1D1BD96F166A5EC0ECEBED2460D91C66F66631842F77B9B>

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

(k) DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>

(l) 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>

(m) RMF Knowledge Service, “Step 2: Select Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Select/Pages/default.aspx> (CAC-enabled)
(n) RMF Knowledge Service, “Step 3: Implement Security Controls,” as amended (CAC-enabled)
(o) RMF Knowledge Service, “RMF Security Assessment Report,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAR.aspx> (CAC-enabled)
(p) 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)
(q) RMF Knowledge Service, “Step 4: Assess Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/default.aspx> (CAC-enabled)
(r) RMF Knowledge Service, “Introduction to Security Authorization Package,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAPIntro.aspx> (CAC-enabled)
(s) RMF Knowledge Service, “Final Risk Determination and Authorization Decision,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Authorize/Pages/FinalAuthDecision.aspx> (CAC-enabled)
(t) RMF Knowledge Service, “Monitor Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/MonitorControls.aspx> (CAC-enabled)
(u) RMF Knowledge Service, “Decommission,” <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/Decommission.aspx> (CAC-enabled)