Software 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 Software Acquisition Pathway (SWP) enables organizations to execute rapid and iterative delivery of software capabilities by using modern software development practices and active user engagement. As the Department's operations become increasingly dependent on software, it must ensure software is created in a secure, protected, and controlled environment instilling user confidence that it will perform as designed. Organizations can use the SWP to deploy capability into operations (or operationally representative environments in the embedded sub-path) within 6 months or less, with a bias for as frequent as possible. DoD's goal is to ultimately field capability into production on-demand as required, which may be in hours or days – not months or years. To meet these goals, the SWP emphasizes DevSecOps, continuous authorization to operate (cATO), and implementing the RMF at the speed of relevance.

Whereas DoD Instruction (DoDI) 5000.87, "Operation of the Software Acquisition Pathway," provides the applicable policy and the Adaptive Acquisition Framework website provides detailed procedural information, and acquisition best practices, this RMF Knowledge Service page provides implementation guidance on integrating SWP and RMF processes together thus enabling practitioners to use cybersecurity risk management techniques and tools to enhance SWP activities (reference (c) and (d)).

DoD organizations providing hosting platforms and environments (e.g., DevSecOps) must consider sharing their body of evidence, enable inheritance, and provide residual risk information so that applications hosted, created, and operated in that environment can

evaluate risks of leveraging that environment. As CIO continues to enhance DevSecOps, further guidance will be made available to enhance software acquisition and visibility of risks associated with that software. This page does not supersede or counteract the need to conduct AAF Pathway-specific actions.

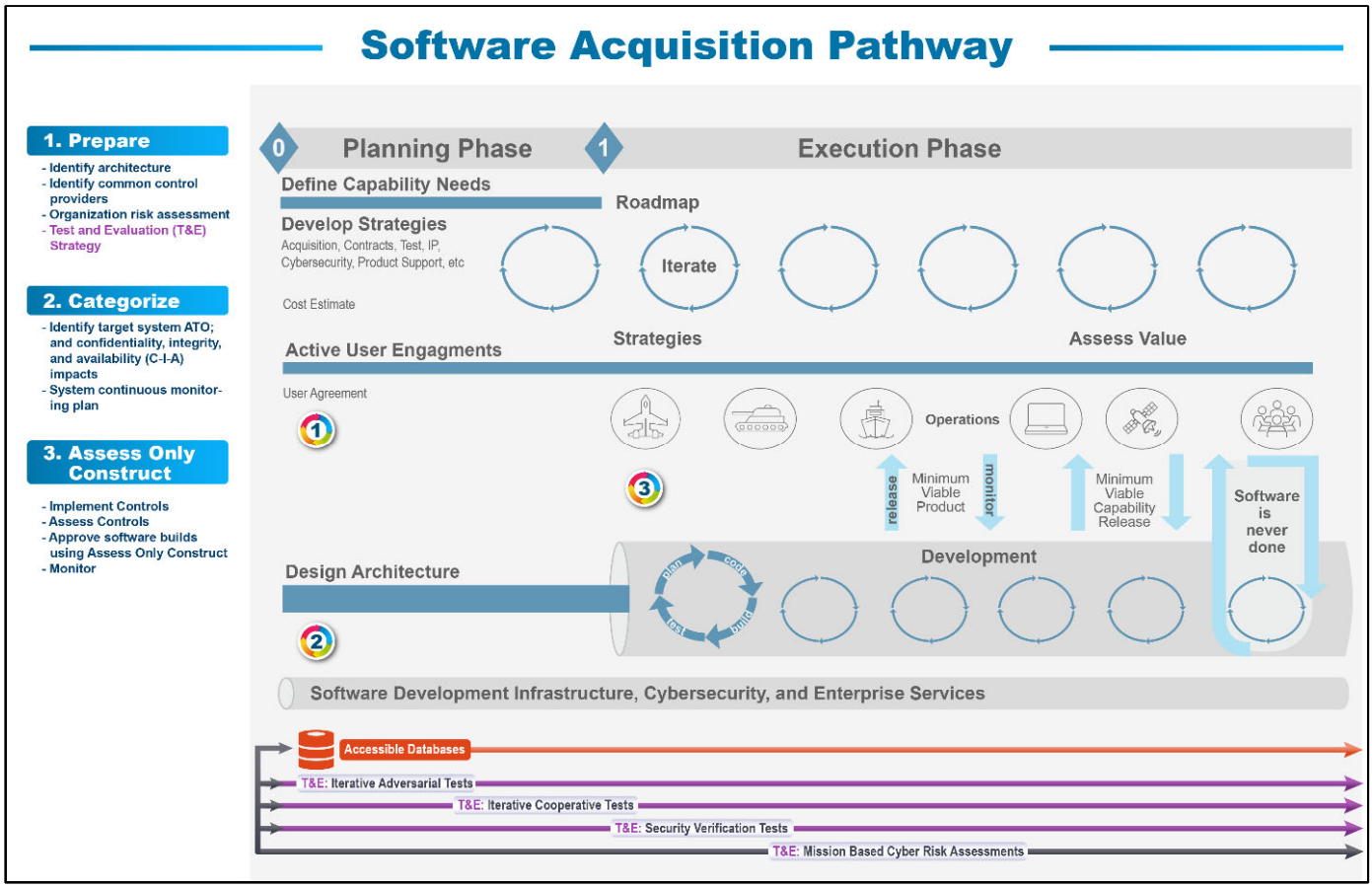

Figure 1. Integrating Assess Only Construct in Software Acquisition Pathway

Planning Phase

As SWP teams proceed through the Planning Phase, they need to establish ties with the appropriate RMF team to help guide the acquisition pathway through the appropriate cybersecurity requirements. RMF activities in this phase coincide with the Prepare Step planning activities from the RMF. In this earliest step, programs identify the environments they will develop and deploy software into so programs can identify any common controls or hybrid controls available to software (reference (e) and (f)). This way, program and RMF personnel can minimize mitigations that are the software's responsibility (either solely or joint) and have the software inherent security control mitigations from the pipeline, hosts/platforms, and

leveraged enterprise services. The testing and mitigation of the inherited controls belongs to the platform and service providers (Prepare Step).

As the SWP and RMF teams identify the mission capabilities and software approach (e.g., web services, infrastructure as code, microservices, containers), they must determine the target system's categorization and continuous monitoring strategies (reference (g) and (h)). This allows the teams to identify any security concerns and appropriately mitigate them.

During this phase and continuing into execution, particular emphasis should be placed on the tooling and automated testing in the development environment (e.g., CI/CD Pipeline, DevSecOps stack, software factory) to facilitate and speedup the process. Program managers should leverage existing development environment platforms and tools – as much as possible – which already have an authorization to operate (ATO) or cATO. The Office of the Secretary of Defense memorandum, "Continuous Authorization to Operate" describes the standards and process necessary to attain a cATO (reference (i)). SWP and RMF teams should work together to leverage reciprocity and automate control verifications to the maximum extent possible. This builds software security into the software development methodology so that the Assess Only process (as with the test and evaluation (T&E) process and establishing an active cyber defense agreement) is done alongside development.

Execution Phase

Because software does not need to undergo the full RMF process, the SWP utilizes the Assess Only construct, which requires due diligence reviews of the software's function, environment, quality control, and data usage and creation. The use of enterprise services allows mission owners to inherit controls and reliable infrastructure, manage a smaller set of controls, and instead focus on innovating and delivering applications.

As software is acquired and continuously integrated into operational environments, the hosting system's Security Plan and other documentation must be accurately updated to account for any changes the software introduces (reference (j)). DevSecOps and cATO are critical elements that support the fast-paced delivery cycle of the SWP.

Because the SWP is an iterative process meant to move at speed, clear communication between the SWP team, the RMF team, and the responsible system authorizing official is key. Also key to this software development is establishing a secure development environment with automated testing and coding standards enforcement for tools and workflows. This ensures programs appropriately capture the correct categorization and cybersecurity standards to assess the software against. Development environments and tools should be secured and continuously monitored for vulnerabilities and intrusions, as a compromise in the development environment could compromise downstream products. Similarly, developers should continuously track and assess upstream supply chain environments or artifacts (such as open-

source libraries) to whatever extent possible, preferably using a software bill of materials (SBOM).

Iterative software development should include mostly-automated pipelines with security testing (e.g., static analysis, dynamic analysis) in-line with best DevSecOps practices. Secure development environments and automated pipelines built with security in mind reduce intentional or unintentional vulnerabilities and compromises of software products and their underlying systems. Because software development is never truly done, the program, RFM team and authorizing official will require continuous interaction and need to maintain lines of communication to review new capabilities and features to assess potential impacts to the security functionality of the hosting system (which may require additional testing and/or analysis). This includes data from hands on iterative adversarial cyber testing and relevant T&E assessment results; failure to have supporting T&E data endangers seamless integration of new software. This ensures changes do not negatively affect the authorization status of host systems or introduce vulnerabilities. Specific T&E requirements and processes are covered by DoDI 5000.89, “Test and Evaluation,” November 19, 2020, and appropriate T&E guidebooks (reference (k)).

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 5000.87, “Operation of the Software Acquisition Pathway,” October 2, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?ver=virAfQj4v_LgN1JxpB_dpA%3D%3D>
(d) Defense Acquisition University, “Software Acquisition,” as amended <https://aaf.dau.edu/aaf/software/>
(e) RMF Knowledge Service, “Common Security Controls and Inheritance,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/securitycontrols/Pages/CommonControls.aspx> (CAC-enabled)
(f) RMF Knowledge Service, “Hybrid Security Controls,” as amended
(g) RMF Knowledge Service, “DoD System Security Categorization Determination,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Categorize/Pages/DoDIS.aspx> (CAC-enabled)
(h) 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=njI4h99LubAZF6DIxsPSwA%3D%3D&b=D546DD5205CB23B2992B715D166AA7665BFC3B215CCCF1F6B51D24FEB0CFE9717710D950A792CAA5A376D53C2F0FB4C2>
(i) 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>
(j) RMF Knowledge Service, “RMF Security Plan,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx> (CAC-enabled)
(k) DoDI 5000.89, “Test and Evaluation,” November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>