Acquisition of Services Pathway Integration with the 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 Acquisition of Services Pathway allows DoD organizations to acquire contracted services with an estimated value at or above the simplified acquisition threshold as defined in the Code of Federal Regulations. Additional acquisition business practices can be found on the Defense Acquisition University Adaptive Acquisition Framework (AAF) website (reference (c).

Whereas DoDI 5000.74, "Defense Acquisition of Services," provides the applicable policy and the AAF website provides detailed procedural information and acquisition best practices, this page provides implementation guidance on integrating Acquisition of Services and RMF processes together, thus enabling practitioners to use cybersecurity risk management techniques and tools to enhance this Pathway's activities, when appropriate (reference (d)). This Pathway requires minimal additional guidance beyond existing Assess Only guidance (reference (e)). Organizations may also use other means to assess the cybersecurity risks and mitigations for services as long as those reviews are consistent with Assess Only principles found in DoD policy. This page does not supersede or counteract the need to conduct AAF Pathway-specific actions.

Program management offices should apply Prepare Step activities and integrate cybersecurity functional experts in the initial planning for any service that has a cybersecurity consideration. Once cybersecurity considerations have been identified, the Pathway team must leverage its RMF functional experts to execute the Assess Only construct for internal or external services involving systems or system components.

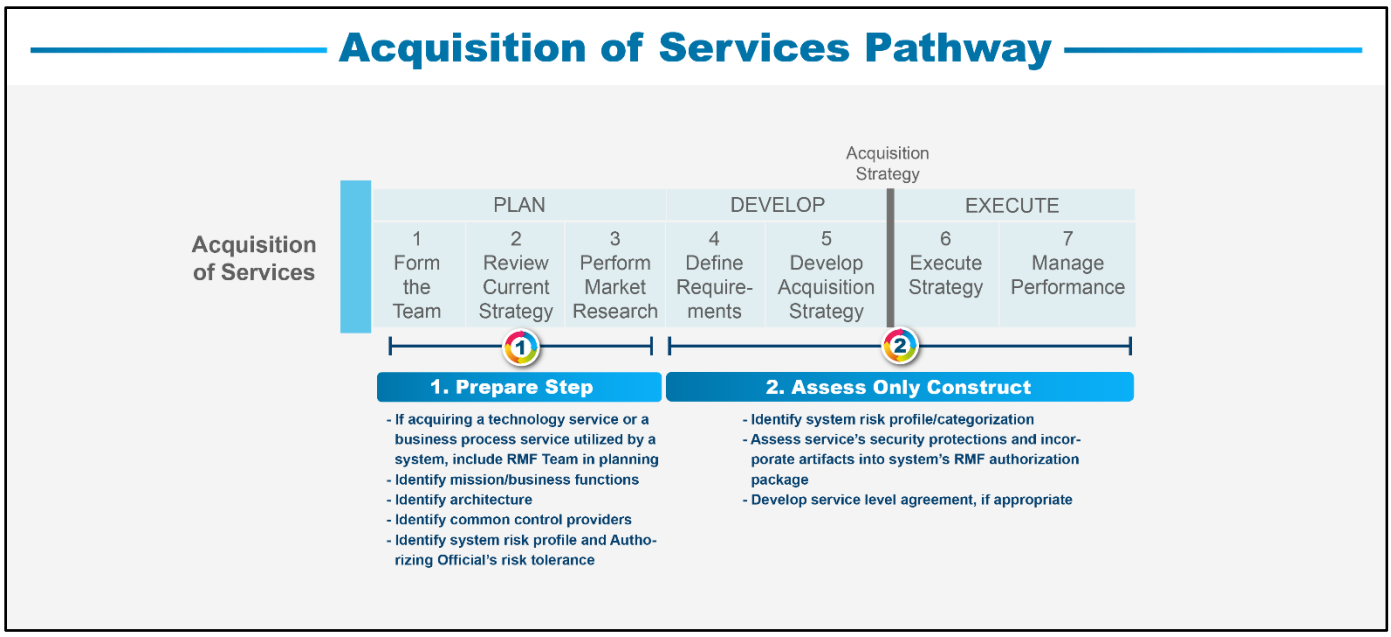

Figure 1. RMF Integration in Acquisition of Services Pathway

Integrating the Assess and Approve Process into Acquisition of Services Pathway

Information technology (IT) services may be a technology service (e.g., point to point Internet protocol data service, satellite communications), or a business process service (e.g., patch management, system monitoring) utilized by a system. IT service users are not responsible for authorizing the system providing the IT services. However, the IT service user must assess the cybersecurity posture of the services prior to using the service. The services are then incorporated into the system boundary. The incorporation of a services into a boundary will vary. As an example, incorporating a service providing a computing environment will differ from the incorporation of a service providing a single technical or process service such as patch management. If the service is satisfying control requirements, the system will inherit those controls from that service. The body of evidence for the using system should reflect these inherited controls. Both the provider and subscriber must understand and specify the responsibilities for any shared or hybrid controls (reference (f)).

The user must ensure security protections of the service are appropriate for the users' system risk profile. IT services should be assessed against an identified standard. For example, commercial cloud service offerings must follow the existing DoD cloud requirements listed in the Cloud Computing Security Requirements Guide published by DoD CIO and DISA (reference (g)). Additionally, the security approach for the IT service is documented in the resulting contract, task order or service level agreement. The user does not re-assess the IT service security results, but uses the evidence provided by the service provider to determine if the service provides the right level of protection for their mission and is meeting contractual obligations.

Specific types of services have established processes for assessing cybersecurity risk (e.g., cloud services). If such a service is being considered, the organization intending to use the service must ensure the service satisfies the assessment requirements associated with the established process for that service type (e.g., complete the cloud provisional authorization process for cloud service offerings). The process below is intended to guide organizations when established processes do not exist.

Internal IT Services

Internal IT Services are delivered by DoD systems or organizations. Examples include Defense Information Systems Agency (DISA)-provided point-to-point Internet protocol data service for connectivity and information transfer, mission partner hosting services, dedicated transport services, satellite communications services, system monitoring services, voice services, cybersecurity service provider services, and cloud services. DoD organizations that use internal IT services must ensure the protection of the system delivering the service is appropriate to the confidentiality, integrity, and availability needs of the information and mission supported.

External IT Services

External IT Services are those services provided by a non-DoD Federal Government agency, a commercial entity, or other non-Federal Government entity. DoD organizations that use external services will develop an interagency agreement, or government statement of work for external IT services containing requirements for service level agreements (SLAs) that include the application of protection requirements appropriate to the confidentiality, integrity, and availability needs of the information and mission supported.

For more information on the Assess Only Construct, see the Assess Only implementation guidance (reference (e)).

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) Defense Acquisition University, “Acquisition of Services,” as amended, <https://aaf.dau.edu/aaf/services/>
(d) DoDI 5000.74, “Defense Acquisition of Services,” January 10, 2020, Change 1 Effective June 24, 2021, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500074p.pdf>
(e) RMF Knowledge Service, “Risk Management Framework (RMF) Assess Only,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Pages/AssessOnly.aspx> (CAC-enabled)
(f) RMF Knowledge Service, “Hybrid Security Controls,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/securitycontrols/Pages/HybridControls.aspx> (CAC-enabled)
(g) Defense Information Systems Agency, “Cloud Computing Security Requirements Guide,” as amended <https://public.cyber.mil/dccs/dccs-documents/>