Defense Business Systems 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).

DoD organizations use the Defense Business System (DBS) Pathway to acquire capabilities and systems supporting DoD business operations. Specific acquisition business processes and the Business Capability Acquisition Cycle (BCAC) mirrors the iterative RMF process.

Whereas DoD Instruction (DoDI) 5000.75, “Business Systems Requirements and Acquisition,” provides the applicable policy and the Adaptive Acquisition Framework website provides acquisition best practices, this page provides implementation guidance on integrating DBS and RMF processes together, thus enabling practitioners to use cybersecurity risk management techniques and tools to enhance acquisition efforts (references (c) and (d)). This page does not supersede or counteract the need to conduct Adaptive Acquisition Framework (AAF) Pathway-specific actions.

Systems developed via the DBS Pathway follow the traditional RMF implementation processes as established on the RMF Knowledge Service (reference (e)). DBS Pathway and unique RMF artifacts can support documentation and artifact creation in both processes. As such, this guidance maps RMF Steps and artifacts to each DBS Pathway phase. Since the DBS Pathway can include acquiring “as-a-service” solutions, use of this Pathway must adhere to approved Cloud Risk Management and the latest Cloud Security Requirements Guide, if acquiring a cloud solution (reference (f) and (g)).

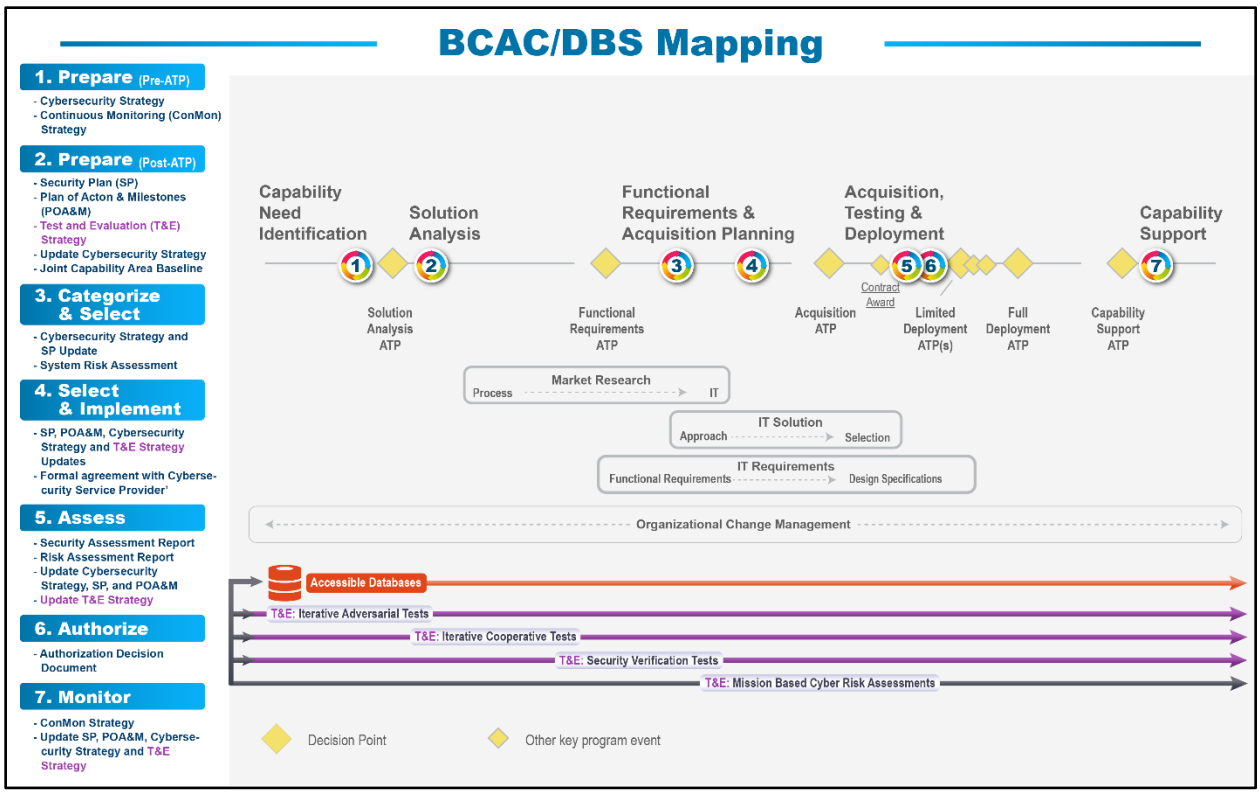

Figure 1. Integrating RMF Steps in the BCAC/DBS Pathway

Capability Need Identification and Solution Analysis

As DoD organizations begin the DBS Pathway, program management office (PMO) and RMF team members (including the Authorizing Official, who, per reference (a), formally assumes responsibility for operating a system at an acceptable level of risk) should begin collaborating as soon as possible. This allows program managers (PMs) to leverage key tasks and artifacts developed for the BCAC process to inform RMF artifacts and vice versa. This close collaboration also ensures DBS/BCAC development includes cybersecurity considerations early – such as the need to establish test and evaluation (T&E) strategies and active cyber defense agreements.

Integrating the Prepare Step in Capability Need Identification and Solution Analysis

Teams should leverage the planning activities in the RMF Prepare Step to identify organization-wide risks and mission/business function risks for the DBS capability. Consistent with DoDI 8510.01, organizations must also begin to apply any Level II control baselines and risk tolerances for their specific mission area, as appropriate. PMs and Functional Leads 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 (Prepare Step). Teams should also begin creating a T&E strategy for continued refinement in later lifecycle stages and ensure RMF artifacts are informed by T&E data. Specific T&E

requirements and processes, throughout the system lifecycle, are covered by DoDI 5000.89, "Test and Evaluation," and appropriate T&E guidebooks (reference (h)). 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 (i)). 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.

Beside the Prepare step activities during the Capability Need Identification phase, RMF and PMO teams should begin creating system artifacts, such as:

- Establishing the system's Cybersecurity Strategy, if relevant;
- Drafting the system's Continuous Monitoring (ConMon) Strategy.

Per DoDI 5000.75, the relevant CIO must approve the Cybersecurity Strategy for any mission-critical, mission-essential systems and Business System Category (BCAT) I programs before any Authority to Proceed (ATP) decision points or contract awards. Any market research conducted in the Solution Analysis phase should inform the organization's system risk management and execution of later assessment activities.

During the Solution Analysis phase, RMF and PMO teams need to coordinate and begin developing the following RMF artifacts, which are consistent with and informed by a T&E Strategy:

- The system's initial Security Plan;
- The system's initial Plan of Action and Milestones (POA&M) (reference (j)).

This close collaboration ensures DBS development includes cybersecurity considerations early. Artifact language reuse may reduce the amount of work needed. These actions prepare the PMO and RMF teams to leverage these artifacts in future lifecycle phases.

Functional Requirements and Acquisition Planning

As PMs lead their teams in the DBS Pathway, RMF teams – per DoDI 8510.01 – must conduct an initial system risk assessment of the DBS capability using NIST SP 800-30, "Guide for Conducting Risk Assessments" (reference (k)). This will inform the PMO and RMF teams of any requirements and improvements needed when delivering the DBS capability.

This assessment, along with the previous information gathered in the previous phases, allows RMF teams to categorize the system and refine the system's security and privacy control baseline by selecting and tailoring needed controls. Organizations use this information and

update their existing Security Plan, POA&M, and strategy documents, as needed. (Categorize and Select Steps).

Integrating the Categorize Step in Functional Requirements and Acquisition Planning

Per DoDI 8510.01, after adopting initial security and privacy control baselines in the Prepare Step, the PMO and RMF teams using the DBS 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 (l)).

Though most DBS are not National Security Systems, RMF and PMO teams must use the same categorization process as any other DoD system, according to DoDI 8510.01 requirements, to address cybersecurity threats. RMF and PMO teams can address any variations needed in control selection via control tailoring considerations in the Select Step. Control tailoring is the norm and is not unique to DBS.

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

RMF artifacts developed in the Categorize Step:

- Further refine the Security Plan, as approved by the system's responsible Authorizing Official (reference (n));
- Update the Cybersecurity Strategy, as needed.

Integrating the Select Step in Functional Requirements and Acquisition Planning

In DBS use cases, RMF integration means selecting security and privacy controls in the Select Step and capturing these in an initial POA&M.

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

PMO and RMF teams should develop 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 system (known as the Subscriber to the CSSP services);

- A draft POA&M;
- An updated Cybersecurity Strategy, as needed.

Acquisition Testing and Deployment

As the DBS capability transitions to functional testing and deployment, RMF teams need to conduct actions found in the Implement Step and the Assess Step before the system can be authorized.

PMO and RMF teams need to collaborate to ensure controls are appropriately implemented and assessed to show that the DBS capability meets appropriate cybersecurity requirements. Evidence of control implementation should be shared with RMF teams before contract award. Assessment activities – the Security Assessment Report and Risk Assessment Report – take place after contracts have been awarded and implementation activities have ended (Implement and Assess Steps).

Integrating the Implement Step in Acquisitions Testing and Deployment

Given initial development has been done, a focus should be given to increasing the automation 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 Implement Step tasks, refer to the guidance pages for control implementation (reference (p)).

Integrating the Assess Step in Acquisitions Testing and Deployment

After contract award, RMF teams can assess the effectiveness of the controls.

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 security and privacy 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 in this phase include:

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

Integrating the Authorize Step in Acquisition, Testing, and Deployment

After teams have adequately proven DBS performance and application of appropriate cybersecurity risk management considerations, the DBS capability is advanced for an authorization decision by the appropriate Authorizing Official. Because the Authorizing Official has been involved since the DBS' inception, Authorizing Officials should be aware of the system and any challenges. This system authorization must take place before any Limited Deployment or Full Deployment ATP (Authorize Step).

Before any deployment ATP is granted, 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 (t)).

Capability Support

After the system's authorization and the Capability Support ATP, organizations must monitor DBS performance – consistent with the Monitor Step from DoDI 8510.01 – to ensure it is operating as expected, and must update the system's documentation – Cybersecurity Strategy, SP, POA&M, or ConMon Strategy – as needed.

Integrating the Monitor Step in Capability Support

Systems developed via the DBS 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 guidance for monitoring systems until decommissioning (reference (u)).

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 5000.75, “Business Systems Requirements and Acquisition,” February 2, 2017, Change 2 Effective January 24, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF>
(d) Defense Acquisition University, “Defense Business Systems (DBS),” as amended <https://aaf.dau.edu/aaf/dbs/>
(e) RMF Knowledge Service, “RMF Implementation,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Pages/default.aspx> (CAC-enabled)
(f) RMF Knowledge Service, “Cloud Risk Management,” as amended <https://rmfks.osd.mil/rmf/RMFforDoDTech/Pages/CloudRiskManagement.aspx> (CAC-enabled);
(g) Defense Information Systems Agency, “Cloud Computing Security Requirements Guide,” as amended <https://public.cyber.mil/dccs/dccs-documents/>
(h) DoDI 5000.89, “Test and Evaluation,” November 19, 2020 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF>
(i) 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>
(j) 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)
(k) National Institute for Standards and Technology, Special Publication 800-30, Revision 1, “Guide for Conducting Risk Assessments,” September 2012, <https://doi.org/10.6028/NIST.SP.800-30r1>
(l) 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>
(m) RMF Knowledge Service, “DoD System Security Categorization,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Categorize/Pages/DoDIS.aspx> (CAC-enabled)
(n) RMF Knowledge Service, “RMF Security Plan,” as amended <https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx > (CAC-enabled)

(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 Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/AssessControls/Pages/default.aspx> (CAC-enabled)
(t) RMF Knowledge Service, “Final Risk Determination and Authorization Decision,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Authorize/Pages/FinalAuthDecision.aspx> (CAC-enabled)
(u) RMF Knowledge Service, “Step 6: Monitor Security Controls,” as amended <https://rmfks.osd.mil/rmf/RMFImplementation/Monitor/Pages/default.aspx> (CAC-enabled)