DevSecOps Continuous Authority to Operate Evaluation Criteria

Executive Summary

To maintain a competitive advantage, the Department of Defense (DoD) must develop and deploy software with increasing speed and agility, while improving security. The DoD must have the ability to respond quickly to rapidly changing threats through the continuous integration and delivery of capabilities, cybersecurity, resiliency, and survivability. The capability to mitigate threats early during software development as well as during operations is necessary. To prepare DoD software development efforts to do this the Department will implement a new approach to system authorizations; Continuous Authority to Operate (cATO).

Continuous Authorization to Operate (cATO) is a modernized authorization process designed to work with programs that want to move faster and that are willing to adopt the necessary culture change. While a cATO raises the security standard over a traditional Authorization to Operate (ATO), the benefits are the ability to deploy updated software more rapidly to the field, while improving security and continuously managing the risk.

Continuous Authorization moves away from a control assessment point-in-time document-based approach (though some documents are still required), towards focusing on continuous risk determination and authorization through continuous assessing, monitoring, and risk management.

Continuous Authorization is an organizational risk management process designed to keep pace with modern software development. An organization with a cATO is allowed to continuously assess and deploy subsystems that meet the risk tolerances for use within a system authorization boundary.

A cATO is based on continual assessment of three things: the processes, the skills of their teams, and the use of an authorized DevSecOps (DSO) Platform. This assessment must incorporate automation, continuous monitoring, and active cyber defense.

Overview

This cATO Evaluation Criteria establishes the use cases and guidelines for evaluating a request for continuous authorization from a DevSecOps platform or software factory. Additionally, it provides DoD software factories the recommended processes and information required to generate a cATO package and send to DCIO (CS) for review / approval. Appendix A outlines the two use cases where requesting a DSO cATO is appropriate. Appendix B highlights the baseline guidance and assessment overview as well as the specific information required for the cATO request.

Appendix A

Continuous Authorization: Scope for General Use Cases for Applying DevSecOps

Programs or systems applying for a cATO should already be in one of the following use case categories.

Use Case 1 (Inside the DevSecOps Platform (DSOP) Boundary): A software factory already has an ATO. Software is developed in that factory and deployed within its production environment (i.e., within its system boundary) as depicted in Figure 1. The software factory seeks a cATO that includes its production environment. This is the main use case for a DevSecOps Platform (DSOP) leveraging cATO. *Example: Software developed and put into production using the Platform One (P1) Party Bus.*

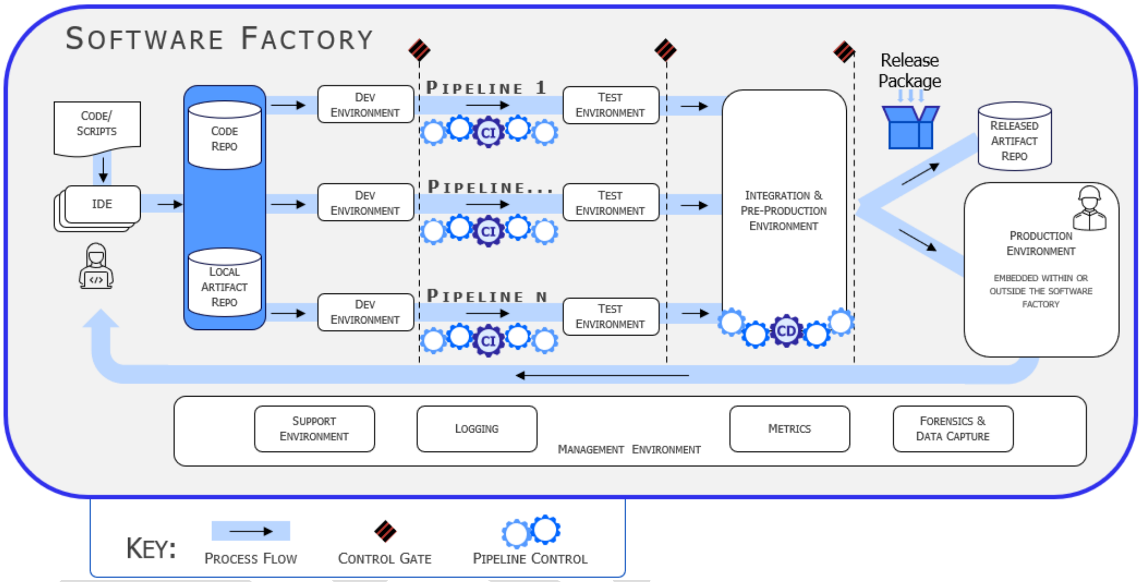


Figure 1. Software Factory Embedded System

Use Case 2 (Outside the DSOP Boundary): Software is developed by a software factory that already has an ATO, but it is deployed into another environment (e.g., a weapon system) with its own ATO as depicted in Figure 2. The software factory seeks a cATO for the factory that allows deployment into the production environment. This involves at least 2 authorization boundaries and there must be agreements in place to pass software across the boundary and subsequently pass results and feedback back to the software factory. *Example: The Forge Software Factory has a ATO to build software that is then deployed on Navy ships, each of which have their own ATOs.*

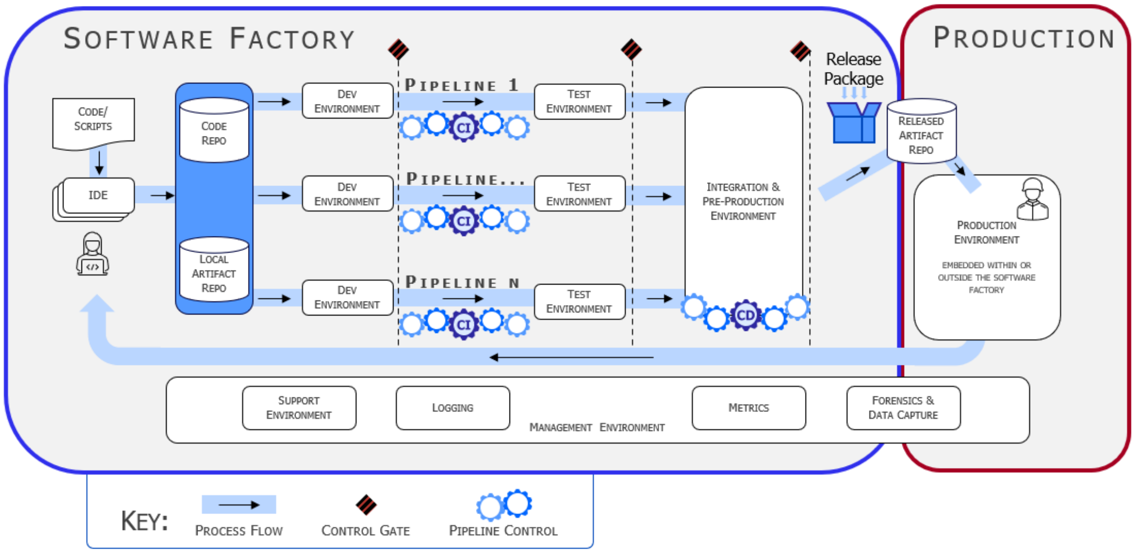


Figure 2. Software Factory in the Cloud

An outcome of issuing a cATO is to seamlessly incorporate software factory products through reciprocity agreements into the production environment.

Figure 3 shows the DevSecOps continual development process and the delineation between the software factory that is primarily responsible for creating the software product and the associated production environment where the software will execute.

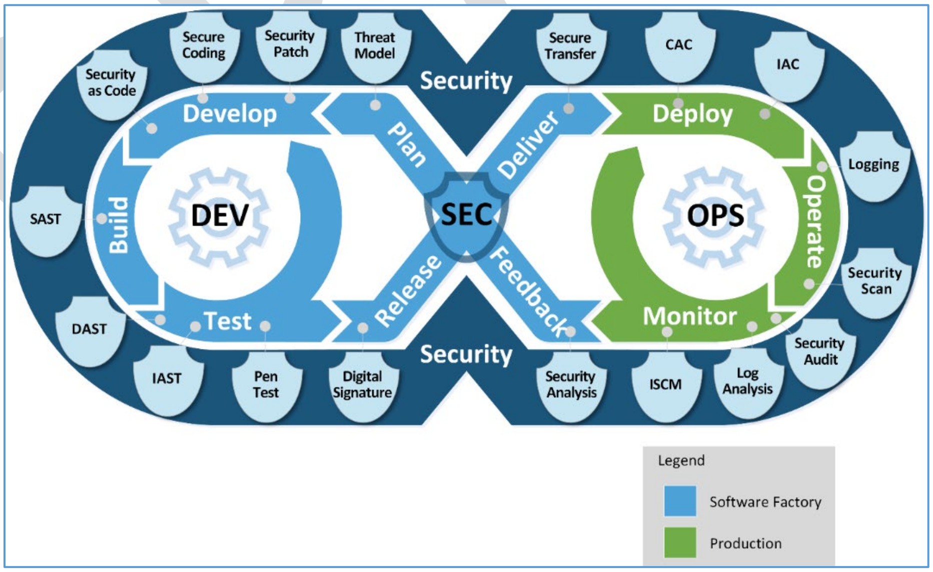


Figure 3. Software Factory/Production boundary

Appendix B

Continuous Authorization: DevSecOps Implementation Guidance and Evaluation Criteria

While the DoD RMF Knowledge Service is the authoritative source for cATO implementation guidance, this appendix provides an overview of how to assess a DevSecOps environment for cATO along with the requirements to deploy applications outside of the DSOP in accordance with NIST guidance.

Figure 4 depicts an overview of the cATO assessment method. The top row shows the related Risk Management Framework (RMF) steps: prepare, assess, authorize, and monitor. Other RMF steps (i.e., categorize, select, and implement) take place outside the review process. The next row, with chevrons, indicates the steps in the assessment process: identify assessors, develop an assessment plan, assess the DSOP, assess the teams, assess the processes, develop a cATO authorization recommendation, authorize the cATO, and constantly monitor the risk. Note that Figure 4 illustrates the assessment process; this process should not be confused with the software development lifecycle of Figure 3.

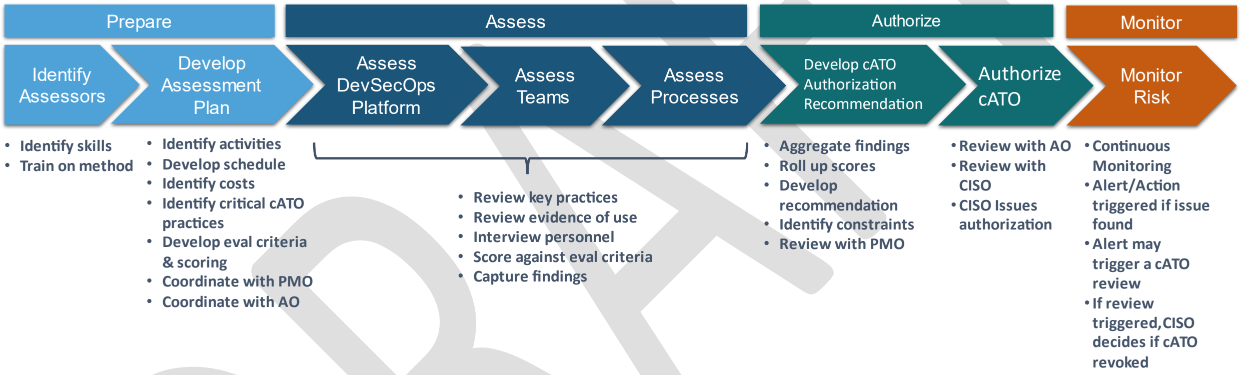


Figure 41. Assessment Method Overview

DevSecOps Platform practices required for cATO are informed by the existing RMF authority to operate assessment and implement continuous monitoring of the DSOP. This assumes that before applying for a cATO, the DSOP has already progressed through the monitor phase of RMF and has a valid ATO. The cATO assessment further evaluates the ‘Prepare’, ‘Assess’, and ‘Authorize’ RMF phases. However, the key to receiving a cATO is having a robust continuous monitoring strategy that includes automated triggers based on approved thresholds within the auditing and incident management plans. The automated triggers and approved thresholds should include both internal and external threats. Additionally, a complete understanding and implementation (or planned implementation) of the shift security left and shield right concept that incorporates vulnerability scanning and compliance checking with detection and response activities to security incidents in real time. This includes tight integration with a CSSP. Hosting any environment (development, test, staging, production, etc.) on a cloud requires the deployment of a Cloud Native Application Protection Platform (CNAPP). Once the Chief Information Security Officer (CISO) grants a cATO, continuous monitoring practices (including the CSSP) monitor the risk. Upon identification of an issue or anomaly the CSSP, along with the

SCA, shall investigate and mitigate as necessary. If the issue or anomaly is outside of agreed upon thresholds, the CSSP and/or SCA may initiate a review of the cATO. If so, the CISO may decide to revoke the cATO. However, with the approval of the previous authorizing official the system can revert to its original ATO.

The approval to implement cATO process within a DevSecOps environment is granted by following the RMF guidelines identified in CNSSI 1253, NIST SP 800-53 and DoDI 8510.01. In order to receive an approved cATO, the organization must have a current ATO with no 'High' or 'Very High' findings. The cATO analysis will review the existing authorization, further evaluate the continuous monitoring strategy, ensure active cyber defense is implemented properly, assess the DevSecOps processes, and validate they are following secure software supply chain guidance in accordance with guidance from the current version of NIST SP 800-161r1.

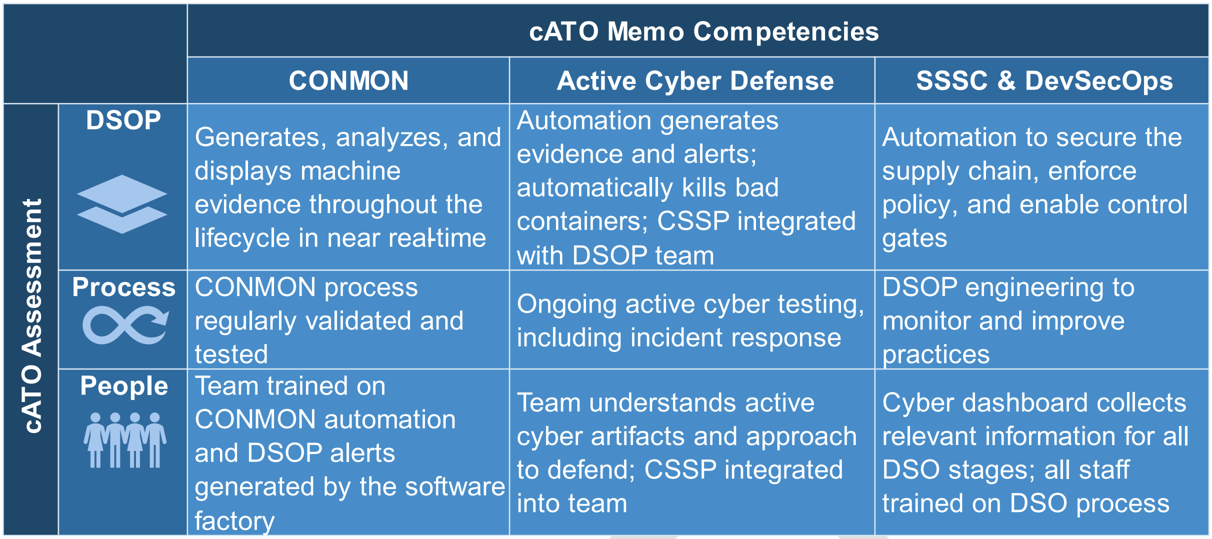
cATO Assessment Overview for DevSecOps

The three competencies indicated in the cATO memo are Continuous Monitoring (CONMON), Active Cyber Defense (ACD) and Secure Software Supply Chain (SSSC). However, the assessment is organized into evaluating the DevSecOps Platform, Processes, and People (Teams). This section discusses how to reconcile these two sets of concepts. To be considered for cATO, the DevSecOps environment must ensure:

1) The DevSecOps Platform (DSOP) contains essential automation to enable CONMON, ACD, and to support DevSecOps (DSO) tooling for a Secure Software Supply Chain (SSSC).
2) Processes are defined for people using, operating, and maintaining the DSOP.
3) People are trained on the DSOP and its processes.

The cATO applies to the DSOP and to software produced by the software factory and hosted within an approved repository. The processes for using the DSOP must be clear, and the people must be familiar with all aspects of the DevSecOps environment.

Figure 5 depicts a high-level crosswalk between these two sets of concepts, showing how they relate. The main columns represent the three competencies, while the rows show the three aspects of the cATO Assessment.



		cATO Memo Competencies		
		CONMON	Active Cyber Defense	SSSC & DevSecOps
cATO Assessment	DSOP	Generates, analyzes, and displays machine evidence throughout the lifecycle in near real-time	Automation generates evidence and alerts; automatically kills bad containers; CSSP integrated with DSOP team	Automation to secure the supply chain, enforce policy, and enable control gates
	Process	CONMON process regularly validated and tested	Ongoing active cyber testing, including incident response	DSOP engineering to monitor and improve practices
	People	Team trained on CONMON automation and DSOP alerts generated by the software factory	Team understands active cyber artifacts and approach to defend; CSSP integrated into team	Cyber dashboard collects relevant information for all DSO stages; all staff trained on DSO process

Figure 52. cATO Memo Competency Assessment Crosswalk

cATO Evaluation Criteria

The following list of activities associated with the Continuous Authorization (cATO) competencies are what the DoD CISO considers when Component CISOs present systems that are requesting to move into a cATO state.

The presence of these activities will be partly determined through demonstrated use of system-level dashboards, which are a culmination of information received from logging, testing, and the following activities, providing a real-time view of the environment. Components are not limited to the way they conduct the following activities; however, this document offers guidelines to achieving a proper cATO environment through the integration of the above cATO competencies.

Items in **bold** in this section indicate documents or artifacts that must be delivered as part of the application for cATO package.

Continuous Monitoring

- **cATO Risk Management Strategy**
  - Must include establishment of cATO risk tolerances based on the Components' risk posture guidance
  - Must include process, management, and tracking of insider and external threats
  - IAW DoDI 8510.01
- **System CONMON Strategy**
  - Will be assessed IAW organizational Risk Management Strategy
  - Includes plan to continuously assess and track vulnerabilities on all the system assets within the infrastructure

- Includes determination of metrics (measures) to establish patterns and discern threats such as:
  - Implementation measures to measure execution of security policy
  - Effectiveness/efficiency measures to measure results of security services delivery
  - Impact measures to measure business or mission consequences of security events
- Includes timelines for continuous monitoring of security controls (automated every hour, minute, second; manual once a year, etc.)
- Includes tight coupling with auditing and incident management strategies

- **System Authorization Boundary Diagram**
  - Include data flows (including PII)
  - Include detailed information for all external connections IAW Appendix E Diagram Requirements of the DISA Connection Process Guide
- **Business Rules**
  - The following are examples of the type of business rules to be established by the system:
    - Closely involve DoD 8510-level certified cybersecurity experts throughout the life of the program
    - Define and assign cybersecurity roles and responsibilities
    - Identify and retain Subject Matter Experts to ensure the cybersecurity risk posture of the system is maintained during operations
    - Establish a vulnerability coordination Point of Contact
    - Align staffing to address detected and identified vulnerabilities
    - AO and designated cybersecurity personnel must have real-time access to the results of testing, scanning, monitoring, and performance metrics at the platform or application level in a mutually agreeable format (i.e., dashboards, alerts, etc.)
    - Identify, assess, prioritize, and share risk information in real-time
    - Identify risks in real-time and initiate corrective action plans to mitigate them
- **Automated Monitoring Information**
  - Status of dashboarding activities, including a demonstration of the dashboard in operation
  - Must be readily available and as near real time as feasible
  - Includes a dashboard with relevant current information that helps security personnel perform their tasks
  - Must publish master endpoint record and endpoint data required elements to JFHQ-DODIN-directed repositories in accordance with JFHQ-DODIN OPORD 8600-22 or its successor
    - Must include implementation of the operational attribution tags as defined in the DoD Operational Attribute Guidebook and required per JFHQ-

DODIN CTO 22-01, JFHQ-DODIN CTO 22-083, and JFHQ-DODIN OPORD 8600-22

  - Includes an alerting capability that contacts security personnel when appropriate
  - Demonstrate which security controls are fed into a system-level dashboard view, providing a real time and robust mechanism for AOs to view the environment
  - To help secure the software supply chain, the software development pipeline and its environment must be monitored as well

- **System Authorization Package Documentation (leveraged from the Component's RMF Inventory Tool)**
  - Security Assessment Plan (SAP)
  - Risk Assessment Report (RAR)
  - System Security Plan (SSP)
  - ATO memo (Signed)
  - Plan of Action and Milestones (POA&Ms)
  - Update documents in response to CONMON process
    - Security Assessment Plan
      - Ensure it covers the DSOP supporting full lifecycle, including the delivery pipeline and addresses:
        - Threat modeling and vulnerability analysis
        - Independent verification of assessment plans and evidence
        - Penetration testing
        - Attack surface reviews
        - Manual code reviews
        - Verifying the scope of Testing and Evaluation (T&E)
        - Static Application Security Testing (SAST)
        - Dynamic Application Security Testing (DAST)
        - Interactive Application Security Testing (IAST)
- **Continuity of Operations Plan (COOP) / Disaster Recovery Plan (DRP)**
  - **Evidence of ConOps testing**
    - Examples include:
      - Read-throughs, walk-throughs, simulations etc.
      - Backup activities
      - Restoration plan
- **Incident Response Plan**
  - Incident Response Management
    - Evidence of a program in place that includes:
      - Policies
      - Plans
      - Procedures
      - Defined roles
      - Training
      - Proof of communication efforts
    - Examples of evidence include:

        - Read-throughs, walk-throughs, simulations etc.
        - Tabletop exercise
      - Capabilities to detect and respond to attackers
        - Behavior Monitoring evidence
        - Intrusion Detection/Prevention Systems evidence
- **Continuous Vulnerability Management Documentation**
  - Evidence of mitigation
    - Published expectations and timelines for corrective action plans and remediation efforts
    - Published plan to ensure availability of staff and resources
    - Findings tracked using Deficiency Reports and system-level POA&Ms
  - Vulnerability scanning procedures IAW DoDI 8530.01
  - Leverage process and automation to enable identification of highest priority items and vulnerabilities to remediate (verified through documentation and demonstration)
  - Monitor for new threat and vulnerability information IAW DoD and Component level Information Security Continuous Monitoring (ISCM) strategies. Critical and moderate vulnerabilities are documented upon discovery and mitigated within a timeframe acceptable to the AO
- **Audit log analysis**
  - Collect, analyze, alert, review, and retain audit logs IAW NIST SP 800-53 security controls
  - Evaluation of events that could help detect, understand, or recover from an attack, as described in Appendix A of OMB M-21-31
- **cATO Approval Memo (located on the RMF KS)**
  - While cATO approval authority resides with the DoD CISO, this template will be filled out by the cATO Assessment Methodology Working Group and submitted with the Components' cATO package

Active Cyber Defense (ACD)

- **Certified Cybersecurity Service Provider (CSSP)**
  - IAW DoDI 8530.01,Meeting the Evaluator's Scoring Metrics requirements
  - External - CSSP Service Level Agreement (SLA) for both on premises and cloud systems
  - Internal – Documentation of methodology supporting ACD
  - Inherited – Agreements/documentation where integration occurs
  - Outline scope and parameters of CSSP support for on-prem and cloud systems
  - Employ CSSP sensors and tools to detect vulnerabilities
- **External Assessment Results and Remediation Evidence**
  - A penetration test must be completed on development and operational environments by a qualified 3rd party within 90 days and annually thereafter.

        - Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in the cybersecurity defense posture (people, processes, and technology), and simulating the objectives and actions of an attacker.
        - Test the authorization boundary IAW DoDI 8531.01, searching for weaknesses that would allow unauthorized access.
        - Activities include:
            - Red/Blue/Purple Teaming Events
            - Automated testing
    - Provide a Vulnerability and Penetration Assessment
    - AO provided results with findings and planned mitigations.
    - Updated document POA&Ms where appropriate
    - Lessons Learned Tracking
- **Security Testing and Documentation**
    - Security testing should be conducted on an ongoing basis and test against adversary tactics and techniques based on real-world observations
    - Strategy and budget for automated cybersecurity testing resources
    - Documentation of the ongoing iterations of cybersecurity analysis and penetration testing
    - Documentation and evaluation of the impact of system or environment changes to the cybersecurity defense posture

Secure Software Supply Chain (SSSC) and DevSecOps

Authorize the DevSecOps Platform

- **Use of a DevSecOps Platform (DSOP) that implements an approved DevSecOps Reference Design, or implementation of an approved DevSecOps Reference Design**
    - Identify the DevSecOps Reference Design to which the DSOP adheres
    - Approved DevSecOps Reference Designs are posted to the DoD CIO public library
- **Software Bill of Materials (SBOM)**
    - Provide a SBOM for the DSOP with a statement of how it was developed
    - Provide an automated export of the SBOM for applications/products passing through the DSOP
    - Specify the SBOM format and how often it is generated
        - SBOM should be in one of the common formats:
            - Software Package Data Exchange (SPDX)
            - Software Identification Tags (SWID)
            - CycloneDX
            - However, the format has not yet been mandated. SBOM is currently undergoing regulatory action, Defense Information

Systems Agency (DISA) Federal Acquisition Regulation (FAR) is the lead

  - Maintain an archive of SBOMs for products passing through pipelines. This can be kept in the same area as the assessment evidence (e.g., results of security tests) for the products
  - Explain how the SBOMs are analyzed. If a new cybersecurity vulnerability appears in the Common Vulnerabilities and Exposures (CVE®) system, explain how the organization applies it to the SBOMs
- **Activities and Tools Mapping**
  - Based on the DevSecOps Activities and Tools Guidebook, provide the mapping of the required and preferred DevSecOps activities to the system's implementation.
  - Include any additional documentation listed with the mapped activities in the Activities and Tools Guidebook
  - Provide Activities and Tools Mapping POA&Ms/Roadmap to show continuous improvement
  - Provide demonstration of various activities listed within the Activities and Tools Guidebook (selected activities determined during the cATO evaluation)
- **Cloud Native Application Protection Program -** Employ an integrated set of security and compliance capabilities to secure and protect cloud-native applications across development and production to include:
    - Artifact Scanning:
      - Software Composition Analysis to review artifacts to find open-source libraries included. This should be addressed in the creation of the SBOMs.
      - Application Security Testing such as SAST, DAST, and IAST
    - Cloud Configuration:
      - Cloud Security Posture Management (CSPM) for continuous monitoring, detection, and remediation of cloud security misconfigurations.
      - Cloud Infrastructure Entitlement Management (CIEM) for management of access rights, permissions, or privileges for the identities of a single or multi-cloud environment.
      - Infrastructure as Code (IaC) Scanning to find security flaws before pushing to production.
    - Runtime Protection:
      - Cloud Workload Protection (CWPP) to provide runtime enforcement
    - Cloud Detection and Response (CDR) to provide advanced threat detection, incident response, and continuous monitoring capabilities specifically designed for cloud environments.

Authorize the Process

- Reliance on Infrastructure as Code (IaC) and Configuration as Code (CaC) to avoid environment drift
- **Control Gate and Guardrail Analysis**
    - These processes should be described in the Incident Response Management section above
    - Provide a description of each control gate and what triggers cause the gate to close and open. This should include what triggers an alert and how to respond to that alert
    - Demonstrate each control gate in action (this may be in a non-production environment) or provide screen shots of control gate output as displayed in a dashboard
    - Provide a description of each guardrail and the process that occurs when something is out of the risk tolerance for the guardrail

Authorize the People

- **Verification of appropriate training for each member of the team(s), based on their role**
    - Provide an organization chart showing the roles within the DSO Team
    - Demonstrate appropriate separation of duties and least privilege are applied to all personnel
    - Periodically conduct Tabletop Exercises with the whole team and produce **After Action Reports**
        - Exercises should include:
            - Security incident response procedures
            - Standard procedures for the DSOP, including how to respond when a control gate triggers
            - How to respond to a security alert
            - Requests for elevated privileges
- **The organizational DevSecOps education, certification, and training process is documented.** Documentation need not be text documents but may be in online learning management tools that assessors can view. Possible areas of training include Agile, DevSecOps, secure coding, security automation tools, interpreting vulnerability scanning reports, cATO method, etc.

    - The team members are trained in the cATO method:

        - Trained on the appropriate version of the DoD Enterprise DevSecOps Reference Design.
        - Trained on the security automation tools and how they are used.

        - Trained on the CI/CD control gates, promotion rules, and the established risk tolerances.
        - Trained on the resolution / adjudication of security findings that result in exceeding the risk tolerances.
        - Ability to perform root cause analysis of “critical” and “substantive” security findings.
        - Trained in continuous monitoring feedback loops for ensuing continuous risk monitoring against tolerances.
        - Trained in the establishment of POA&M and security dashboard monitoring in a DevSecOps environment.
    - Verification of appropriate training for each member based on their role on the Product/Application Team
    - Verification of cybersecurity team member qualifications in accordance with DoD 8570.01-M
    - Document cross-functional team training and shadowing
- **Insider Threat Monitoring**
    - Validate an insider threat working group is established, active, and chaired by senior leadership
        - Validate insider threat working group identifies critical areas for review along with thresholds for analysis
    - The below concepts can be used to protect against insider threats:
        - Separation of duties
        - Paired programming
        - Least privilege management with respect to containers/cloud environments
- **Onboarding/Offboarding**
    - An onboarding/offboarding process is defined for new team members based on their role.
    - Show evidence that all personnel have gone through the onboarding/offboarding process, without regard to their rank or position.