DevSecOps Continuous Authorization Implementation Guide

Department of Defense, Office of the Chief Information Officer (DoD CIO)

March 2024

Version 1.0

Change History

Version	Date	Change Summary	Author
1.0	21Mar2024	Original version	Mark Smiley, Ph.D.

Contents

Figures

Tables

Introduction

"Real-time or near real-time data analytics for reporting security events is essential to achieve the level of cybersecurity required to combat today's cyber threats and operate in contested spaces." – Continuous Authorization To Operate (cATO) Memo [1].

The exigencies of today demand the agility to respond to changing mission needs by delivering capabilities more rapidly than with traditional DoD processes. To enable such a rapid pace, industry has moved to using DevSecOps software development, often delivering new capabilities multiple times per day. DoD must also modernize its approach to software development and delivery to keep pace with the constantly changing threat so that it can deliver resilient software capability at the speed of relevance.

An integral aspect of this agile modernization is the ability to respond rapidly to changing threats through the continuous integration and delivery of cybersecurity, resiliency, and survivability. The cybersecurity landscape, with its advanced persistent threats and innovative approaches to exploiting vulnerabilities, encourages a movement away from point in time assessments and authorizations, instead moving towards continuous monitoring and assessment of risk, using security automation and security posture dashboards that assist in managing the cybersecurity risk in near real-time.

The modernization approach is delineated in the *DoD Software Modernization Strategy* [2], which includes objectives to advance DevSecOps through enterprise providers, and to accelerate software deployment with continuous authorization.

Many DoD Components identify obtaining an Authorization to Operate (ATO) as the longest step in developing and deploying software. Delivering new features rapidly requires an authorization process that can keep pace with continuous change for a developing capability—called Continuous Authorization to Operate (cATO). 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 moves away from a control assessment point-in-time approach to focusing on *continuous risk determination and authorization through demonstrated continuous assessing, monitoring, and risk management.*

This document focuses on the continuous assessment and authorization of developing and securing application software produced by a software factory that includes a DevSecOps Platform (DSOP), particularly the two use cases described in the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3] and reproduced here in Appendix A. This document identifies the key practices of continuous authorization and describes the method for assessing an organization's readiness to enter continuous authorization. Active risk management, in the form of cATO, is enabled by organizations establishing competencies in managing risk through a risk governance process.

The audience for this document is implementers of systems that seek a cATO. It provides an overview of cATO that includes key practices that must be implemented to achieve a cATO.

What is Continuous Authorization?

> **Continuous Authorization to Operate (cATO)** is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system's cyber posture.

Systems seeking a cATO must have already achieved an Authorization to Operate (ATO) and have entered the Risk Management Framework (RMF) monitor stage.

A cATO is a superset of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) term *ongoing authorization* (see the Glossary for a definition), which has existed for years but lacked the automation to make it effective across a broad community. Continuous authorization for DevSecOps includes additional aspects, such as assessing the team and a DevSecOps Platform for supporting continuous risk monitoring.

The cATO Competencies

The *Continuous Authorization To Operate (cATO) Memo* [1] states: "In order to achieve cATO, the Authorizing Official (AO) must be able to demonstrate three main competencies: On-going visibility of key cybersecurity activities inside of the system boundary with a robust continuous monitoring of RMF controls; the ability to conduct active cyber defense in order to respond to cyber threats in real time; and the adoption and use of an approved DevSecOps reference design."

To summarize, the three competencies are:

- Continuous Monitoring (CONMON) of RMF controls
- Active Cyber Defense (ACD)
- Use of an approved DevSecOps Reference Design.

In addition, the cATO memo calls out the need for a Secure Software Supply Chain (SSSC) and relates that to the third competency, saying: "In order to prevent any combination of human errors, supply chain interdictions, unintended code, and support the creation of a software bill of materials (SBOM), the adoption of an approved software platform and development pipeline(s) are critical."

Evaluation Criteria

The cATO memo states that evolving guidance and related resources will be published on the RMF Knowledge Service (KS) at https://rmfks.osd.mil. An important part of this guidance is the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3] posted there, as well as

in the DoD CIO Library. That document lists activities and documentation to be evaluated by the cATO Authorizing Official.

Approach

Foundational Concepts

To simplify the discussion here are definitions of some key terms.

DevSecOps pipeline – a collection of DevSecOps tools, upon which the DevSecOps process workflows can be created and executed. – DoD Enterprise DevSecOps Fundamentals, Version 2.1 [4].

DevSecOps Platform (DSOP) – the set of tools and automation that enables a software factory. It includes the ability to create DevSecOps pipelines with control gates, and to deploy software into development, test, and staging/pre-production environments. It may also deploy into production, depending on the production environment.

Software Factory – a DSOP combined with the people and processes that support the DSOP, as well as a hosting environment such as a cloud; it includes at least development, test and staging/pre-production environments, and it may include a production environment, as well as other environments such as integration.

The Software Factory is based on one of the *DoD Enterprise DevSecOps Reference Designs (RD)* to be found in the DoD CIO Library. Figure 1 illustrates some of the key components that relate to cATO.

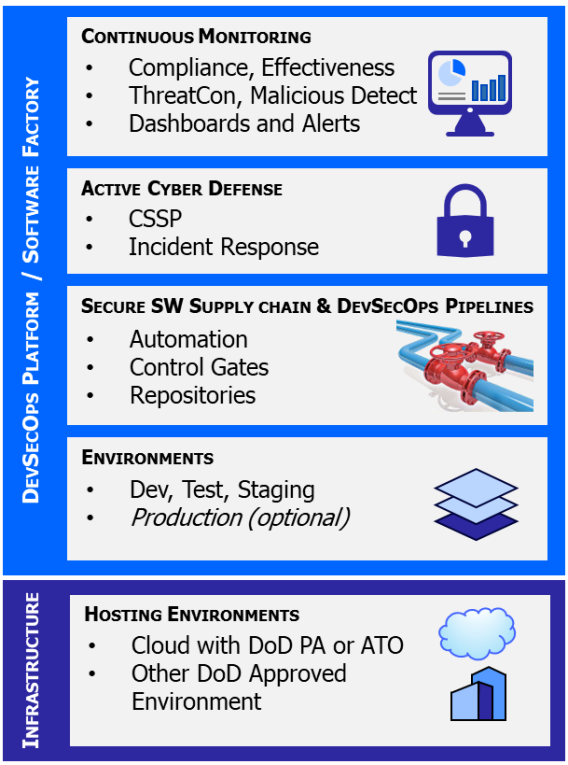

Figure 1. Software Factory: cATO Viewpoint

In the terminology of the NIST Risk Management Framework (RMF), the software factory contains at least one system with a single authorization boundary. This typically contains a development system, a testing system, and a staging (or pre-production) system. It may also contain the production system, or that system may be hosted on a different platform such as in an embedded system. These two use cases are explained in more detail in Appendix A. In either of these cases, the cATO will cover the software developed in the software factory and deployed to the production systems.

The Software Factory should include the following:

- Automation that includes at least one DevSecOps pipeline with automated guardrails and control gates that collect evidence for making continuous risk assessments and determinations during software development
- Built-in dashboards and automated alerts for monitoring and managing the risk in production
    - Must include an active feedback mechanism for both internal and external production environments
- An application hosting environment that uses a modern hyperscale cloud (or other DoD approved environment) to provide development, test, staging, and (optionally) production environments
- A DSOP that is delivered and operated as its own system and provided as a service to application developers
- Input from the risk governance process that provides a common set of acceptable residual risk tolerances for applications moving through the pipeline
    - When the software factory includes the production environment for one or more applications, as in Use Case 1 (Appendix A), the group managing the risk is a collaborative group comprised of the platform team, application teams, AO designated risk assessors, and mission security teams. The cATO is issued to the software factory managing the environment that also has the responsibility for managing the risk for the single authorization boundary that is hosting multiple applications (subsystems)
    - Use case 2 (Appendix A): the production/operational environment is outside the DSOP, such as when the hosting environment is an embedded system or a system of a higher classification than the development environment the risk governance team must work with the authorizing official for the production environment to identify the risk tolerances for applications
- Adherence to DoD CIO DevSecOps guidance, including the DevSecOps Fundamentals Guidebook: Activities and Tools [5]

Assessment Approach

The RMF outlines a risk-based framework for authorizing a system. It includes a mechanism for continuous assessment and authorization, supported by an organization's ability to continuously monitor the ongoing risk and ensure it remains within agreed-to risk tolerances. The program office, mission owners, risk assessors, and authorization official collaboratively develop a set of acceptable risk tolerances. The software factory employs risk thresholds that align to organizational risk management tolerances.

A cATO assessment ensures the software factory includes these features:

a. Continuous security posture (or status) and risk reporting, including dashboards, that aggregate and display results from automated (and possibly manual) security vulnerability analysis, control compliance scans, and security control effectiveness for both the environment and hosted applications
b. Feedback from cyber operations on unexpected changes in security configurations, incident analysis, mitigation effectiveness, change in threat environment, and detection of non-approved behavior is being monitored and used to support the risk response
c. A holistic set of information, along with the DevSecOps guardrails and control gates provides the ability to perform continuous risk analysis against agreed-to risk tolerances in support of continuous risk determinations and authorization decisions

Assessment Method

The assessment process for a cATO involves developing an understanding of the organization's risk management practices in the software factory through the review of evidence of use of the practices, interviews with personnel performing the practices to determine the level of organizational understanding and implementation, and review of results from continuous monitoring activities. The information is used by the assessment team to determine the organization's readiness to manage risk based on evaluation criteria developed by the assessment team. These criteria should be based on the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3].

This assessment method is a fundamental shift from a point-in-time assessment of organizational compliance with security controls to a periodic assessment of an organization's continued readiness for managing risk throughout the application lifecycle from development through operations under continuous integration, delivery, and deployment.

cATO Assessment Method

- Identify the team to perform the process assessment. The skills required to assess DevSecOps platform, process, and people will be different, and the AO will approve the assessment team and their capabilities as part of the authorization process.
- Educate and train the team on the cATO assessment process. Develop the assessment plan and identify key practices, as well as evaluation and weighting criteria. Detailed

cATO evaluation criteria can be found on the KS in the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3]

High Level Evaluation Criteria:

- Practices are defined and documented.
- Evidence exists on the use of risk management and continuous monitoring practices. This evidence includes demonstrations.
- The workforce is knowledgeable on the cATO practices.
- The level of implementation of the cATO practices is measured as defined in Appendix B in Table 2 on cATO requirements targets and objectives.

- Coordinate the assessment with the responsible cATO office; ensure the organization understands the critical practices to be assessed, the assessment process, and the evaluation criteria.
- Review the assessment plan with the AO to ensure key practices and concerns are included.
- Gather and review organization's practice documentation and evidence. For example, evidence may be provided through various types of tracking systems, meeting minutes, and pipeline security scanning reports.
- Identify and schedule interviews with the organization's personnel representing key roles and who are knowledgeable on the cATO DevSecOps (DSO) practices.
- Assess the DSOP, process, and teams against evaluation and weighting criteria. Weighting can be established for the key areas, such as the software factory, process, and teams, down to the actual practices identified in Table 2.
- Develop assessment findings, recommendations, and review them with the organization's office that is responsible for cATO.
- Provide a final organizational readiness risk determination and recommendation for the AO to consider, using an AO cATO decision briefing, including all conditions of the authorization.

cATO Memo Assessment Crosswalk

This section relates the assessment method of evaluating the software factory, processes, and people to the cATO Memo competencies discussed earlier in the cATO Competencies section:

- Continuous Monitoring (CONMON)
- Active Cyber Defense (ACD)
- Use of an Approved DevSecOps Reference Design for a software factory with a Secure Software Supply Chain (SSSC).

These competencies are themes that resonate across the cATO assessment process, as illustrated in Table 1. For example, for CONMON, the software factory must have the automation to generate, analyze and display machine evidence; also, there must be good processes in use (e.g., incident response); and the people must be trained in both the automation and the processes. Similarly, for each of the other competencies.

Table 1: cATO Memo Competencies Assessment Crosswalk

DevSecOps Continuous Authorization to Operate Evaluation Criteria

		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

Key Practices

This section discusses key practices to implement and assess. These are organized into the DevSecOps Platform, cATO Process, and DevSecOps Team (People) practices.

DevSecOps Platform Practices

The DevSecOps Platform must be based on one of the *DoD Enterprise DevSecOps Reference Designs (RD)*. The cATO assessment assumes the DevSecOps platform is already authorized to operate and is in a state of continuous monitoring. The applicable continuous monitoring practices will be inherited for use in the cATO authorization. The intent of this part of the assessment is to ensure the organization responsible for the DevSecOps Platform has effectively instituted the required supporting cATO practices for managing risk of an application traversing the DevSecOps pipeline.

Relative to the DSOP, the following cATO practices apply:

- The DSOP has developed and instituted a continuous monitoring strategy.
- The DSOP uses an established Cybersecurity Service Provider (CSSP) for monitoring the system single authorization boundary for malicious threat actor actions.
- An application or subsystem manager identifies unique application events, develops Security Information and Event Management (SIEM) monitoring analytics, and provides them to the CSSP.
- The production system and its monitoring capabilities are configured for unique application traffic inspection and handling of events.

  - If the system uses containers and the Sidecar Container Security Stack (SCSS) deployed in a Kubernetes pod, it should be configured for unique application traffic inspection and handling of events. (Note that the SCSS is not required; its use depends on the reference design selected.)

- DSOP control inheritance by an application is identified by the DSOP security team.
- Security automation is used for monitoring the application security posture within the production system. In addition, the automation provides for periodic checks of secure configurations.
- Operational risk tolerances are agreed to and implemented in the pipeline control gates with event trigger routing.
- Cyber operations feedback loops are established, and application cybersecurity incidents are reviewed in collaboration with the DevSecOps team.
- The security posture of the application and the DSOP are visualized on the DSOP security dashboard.

cATO Process Practices

The cATO process practices provide for the continuous monitoring, assessment, and management of risk. The objective is to assess the organizational practices to ensure continuous monitoring and response has been instituted for managing production system cyber risk within tolerances. Many of these practices can be automated, including risk determinations and continued ongoing authorization decisions.

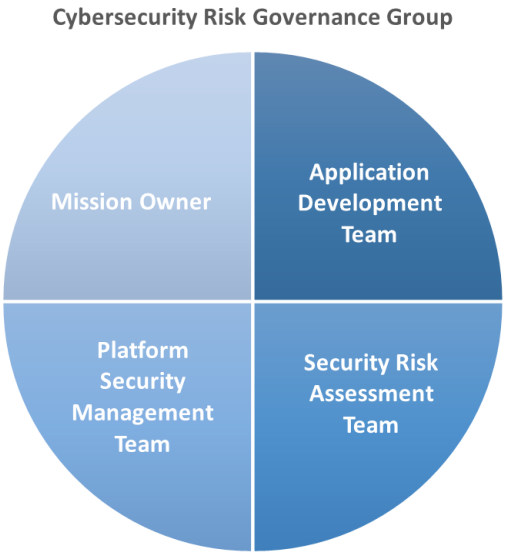

Figure 2. Cybersecurity Risk Governance Group

- The organization establishes a cybersecurity risk governance group comprised of members from the application development team, the Authorizing Official's security risk assessment team, the DSOP security team, and mission owner, as depicted in Figure 2.
- The organization understands and establishes guardrails and control gate risk tolerance promotion rules for making automated risk determinations along with event triggers for escalating resolution.
    - In the case of a DSOP with a single authorization boundary, its risk tolerance should be used to establish the guardrail and control gate promotion rules.
- The DevSecOps team periodically uses dynamic vulnerability tools, threat actor emulation, pen-testing, and analysis from operations to determine security control effectiveness. This is an area in which some of the testing may be manual, such as pen-testing, but the results of which can be used for control gate pass/fail determination.
- The DevSecOps team continuously validates sub-system secure configurations and security control compliance using security automation.
- The DevSecOps team leverages ongoing CSSP monitoring of the production system for non-approved behavior and performing incident forensics to improve the ongoing system security posture. This includes cyber operations intel cell feedback on changes in the threat landscape.
- The DevSecOps team continuously reassesses artifacts in the artifact repository to ensure that the residual risk remains acceptable.
- The DevSecOps team continuously visualizes the security posture and residual risk of the production system.
- The DSOP team establishes the technical security controls and risk tolerances required for applications traversing the pipeline. If stricter tolerances need to be applied, the development team should work with the DSOP cATO team to apply them.

DevSecOps Team Practices

The objective for assessing the DevSecOps teams is to build trust in the team executing the development, performing the security analysis, and the risk management functions. This includes the development team's ability for developing secure code and interpreting vulnerability reports, the security team's ability for managing security control compliance, effectiveness, and risk tolerance, and the DSOP team's ability to instantiate pipelines integrated with security tools and control gates, and to monitor the production environment for possible malicious actions. These teams are an integral part of how the risk management governance group will manage the risk of use of applications within the single authorization boundary. The team assessment reviews the organizational practices that have been put in place to ensure people are educated, trained, and certified accordingly, based on their DevSecOps position's required knowledge, skills, and abilities.

- The organization has a process for ensuring the workforce, based on their role in the organization and DevSecOps platform, is educated, trained, and certified. Possible areas

of training include Agile, DevSecOps, secure coding, security automation tools, interpreting vulnerability scanning reports, and the cATO framework.

    - Leadership education and training should also be available and tracked.
- The organization has an onboarding process for team members based on their role.
- Member(s) of the team have experience in developing security applications, working in a DevSecOps culture, use of security automation tools, and performing application and system authorizations.
- The team members are trained in the cATO method:
    - Trained on the security automation tools, interpretation of resultant scans, and how they are used in the cATO method,
    - Trained on DevSecOps guardrail and control gate promotion rules and risk tolerances,
    - Trained on the resolution and adjudication of security findings that result in exceeding the risk tolerances,
    - Ability to perform root cause analysis of security findings,
    - Trained in continuous monitoring feedback loops for ensuing continuous improvement of system security posture.
    - Trained in the establishment of Plan of Action and Milestones (POA&M) and security dashboard monitoring.
- Organization identifies cultural change challenges and leverages training, collaborative discussion forums, and senior leadership to help address.

Continuous Authorization Metrics

The following metrics provide insight into the effectiveness of the continuous authorization process in maintaining the security, quality and integrity of applications passing through the software factory.

- Cyber hygiene metrics, such as Mean Time to Patch Vulnerabilities – Average time between identification of a vulnerability in the DSOP or application and successful production deployment of a patch. Focus on vulnerabilities with high to moderate impact on application or mission.
- Trend metrics associated with guardrail and control gate results over time to show improvements in development team efforts at developing secure code with each new sprint and the system's continuous improvement in its security posture.
- Feedback Communication Frequency metrics to ensure feedback loops are in place, being used, and trends showing improvement in security posture.
- Metrics associated with continued effectiveness of mitigations against a changing threat landscape.

- Security posture dashboard metrics showing stage of application and its security posture in the context of risk tolerances, security control compliance, and security control effectiveness results.

Other metrics to consider include:

- Container Metrics - measure of the age of containers against the number of times they have been used in a subsystem and its residual risk based on the aggregate set of open security issues.
- Test Metrics - percentage of test coverage passed, percentage of passing functional tests, count of various severity level findings, percentage of threat actor actions mitigated, security findings compared to risk tolerance, and percentage of passing security control compliance.

Practical Implementation Advice

This section offers practical suggestions on how to start to implement an organization and a software factory that can attain a cATO. For details on what to provide in the cATO assessment package, see the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3].

- Choose one of the following options to build out the DSOP.
    - Use an existing DSOP (e.g., Platform One Party Bus).
    - Use a new instance of a DSOP (e.g., Platform One Big Bang).
    - Use an integrated set of cloud-native tools.
    - Use an existing commercial integrated DevSecOps tool.
    - Build a new DSOP using hardened components. This is the most time-consuming approach, and it should be avoided if possible.
- If possible, aim for a DSOP running on a commercial cloud.
    - The cloud may be acquired through the Joint Warfighting Cloud Capability (JWCC) acquisition vehicle, or through other existing DoD vehicles.
    - If the target production environment is not a cloud (use case 2), it may still be useful to perform some development and testing in a cloud.
- Bring security into the team at the start and keep them involved throughout.
    - Set risk tolerances.
    - Implement the risk tolerances in the control gates and guardrails.
    - Ensure cybersecurity best practices are implemented, including separation of duties and least privilege access.
- Create secure agile processes to support the continued delivery of value.
    - Build security into the processes.
- Continuous Monitoring must be implemented in all environments, including development, test, and production.

    - Integrated continuous monitoring with auditing to identify thresholds and triggers for active incident response.
- Active Cyber Defense must be in place, including a local Security Operations Center (SOC) and external CSSP.
    - There must be a detailed incident response plan in place with personnel trained on it.
- Secure Software Supply Chain
    - Create SBOMs for the DSOP and applications passing through it.

The next set of advice is for implementing DevSecOps in an organization. This is part of what is necessary, but it is not part of the cATO package per se.

- Culture change is a critical component of DevSecOps. It may be more challenging to implement than the DSOP, but DevSecOps is not possible without the proper supporting culture.
    - Focus on delivering value.
    - Create good feedback mechanisms.
    - Implement psychological safety. Fail fast, but don't fail the same way twice.
    - Make security everyone's job.
    - Reverse Conway's law and create an organization that mimics the architecture. For example, there will likely be a DSOP team, one or more application teams, and other major components may have associated teams.
- Use agile project management techniques.
    - Create user stories and offer frequent demonstrations, rather than creating comprehensive requirements.
    - To track tasks, use a Kanban board or similar.
    - Do not use a waterfall approach.
    - Do not use a heavy-weight agile process that requires significant overhead to maintain.
- Set up the test (or optional integration) environment early.
    - This may be used for other systems that need to integrate with the software product. This enables continuous integration.
    - This environment may also be used to demonstrate continuous improvement of the product.

Appendix A. Use Cases

This section comes from the *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3]. There are other known use cases, but these two are the focus for this document.

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

Use Case 1 (Software delivery 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 3. 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.*

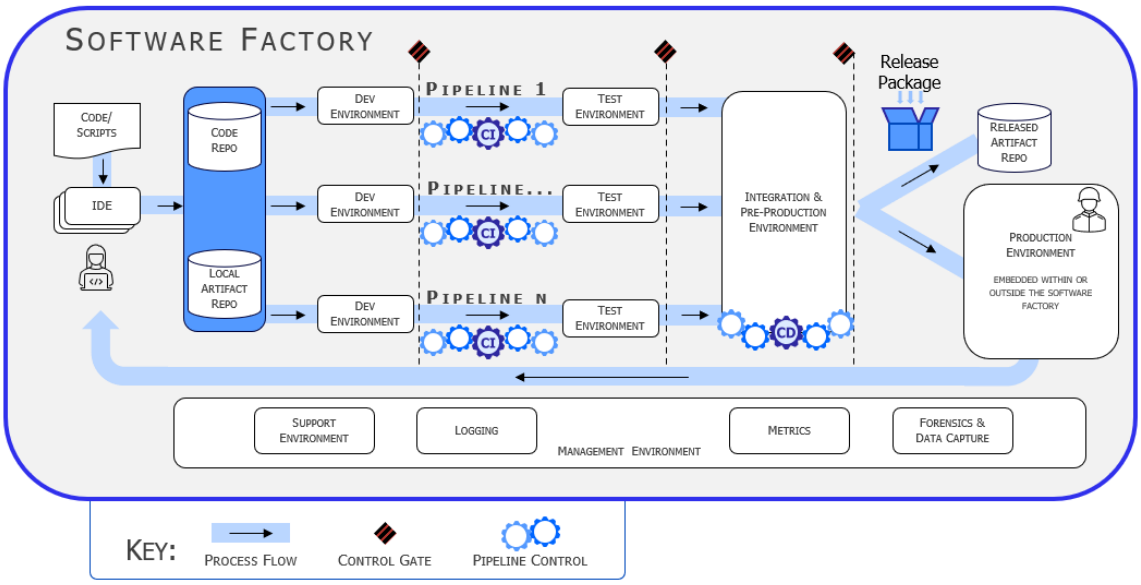

Figure 3. Software Factory with an Integrated Production Environment

Use Case 2 (Software delivery outside the DSOP Boundary): Software is developed by a software factory that already has an ATO, but the software is deployed into another environment (e.g., a weapon system) with its own ATO as depicted in Figure 4. The software factory seeks a cATO for the factory that allows deployment into the production environment. **Error! Reference source not found.**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 an ATO to build software that is then deployed on Navy ships, each of which have their own ATOs.*

An outcome of issuing a cATO for use case 2 is to seamlessly incorporate software factory products through reciprocity agreements into the production environment.

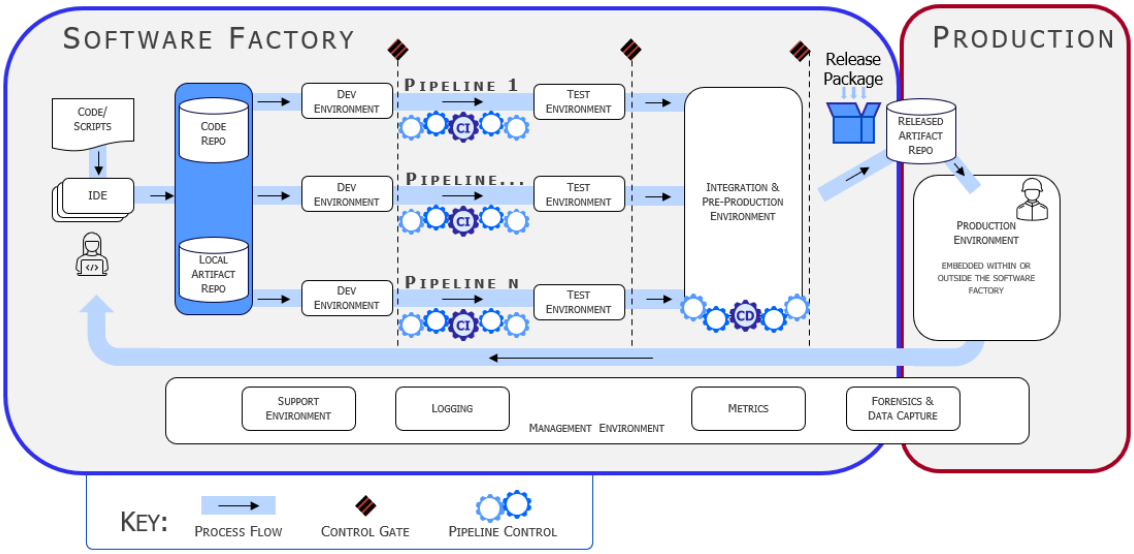

Figure 4. Software Factory with a Separate Production Environment

Appendix B. Requirements

This section summarizes the requirements to assess for a cATO. The intent is to provide an abstraction of the practices to provide flexibility to implementing organizations. It also indicates which requirements are threshold (T) and which are objective (O). A threshold requirement must be met, while an objective requirement is one that should be met, but which may not be fully met initially, while still obtaining a cATO.

The *DevSecOps Continuous Authorization to Operate Evaluation Criteria* [3] provides further details on specific artifacts to include in the cATO assessment package.

The cATO assessment of an organization involves a review of the effectiveness of the methods and practices, such as continuous monitoring, they are using for ongoing management of system and mission risk. The practices ensure continuous risk management, continuous security education and training of DevSecOps teams, and are supported by a DSOP that provides the underpinnings of zero-trust with a software factory.

Table 2 is a list of continuous risk management practices for cATO. The intent is not to say that all these practices need to be implemented, such as in a conformance checklist, but rather organizations typically use these types of practices for continuously managing their risk. An organization could leverage this table for identifying which practices are necessary for their cATO implementation and the assessors would review this implementation to determine its effectiveness.

Table 2: cATO Requirements

ID	Description	Level
IC	**Key cATO Processes and Practices: Information capture practices**	
IC01	Capture mission essential functions, and their supporting assets and data.	T
IC02	Identify and capture risk tolerances and thresholds based on an understanding of the criticality of mission, systems, and key system parameters for cybersecurity, cyber resiliency, and cyber survivability.	T
IC03	Identify cyber threats to network and data architecture, assets supporting essential mission functions and cybersecurity architecture.	T
IC04	Collect evidence for establishing a baseline risk posture.	T
RA	**Reduce the Attack Surface**	
RA01	Leverage DSOP Zero Trust with both ingress/egress and east/west traffic enforcement.	T
RA02	Leverage a Cloud Native Access Point or Boundary Cloud Access Point.	T
SA	**Security Automation risk determination practices**	

ID	Description	Level
SA01	Adjudicate findings, including false positives capture and analysis.	T
SA02	Set guardrail thresholds, control gate risk acceptance tolerances, and notification thresholds.	T
SA03	Automate security control configurations and validation.	O
SA04	Perform security scanning: dependency analysis, static and dynamic application analysis, prioritizing method, and adjudication.	T
SA05	Perform pen-testing and threat emulation: threat modeling, pen-testing methods, and assets.	T
SA06	Perform risk assessments: mission based, threat based, resiliency / survivability based.	T
SA07	Perform verification and validation testing of cybersecurity, cyber resiliency, cyber survivability requirements.	T
SA08	Perform configuration management of system and control configurations.	T
SA09	Perform Security control mitigation effectiveness testing and analysis.	T
SA10	Capture, visualize, and provide feedback on security findings during pipeline runs.	T
CM	**Continuous Monitoring practices**	
CM01	Continuously monitor behavior and implement / improve proactive preventive / resiliency capabilities.	O
CM02	Establish event triggers: on findings / risk tolerances / change in threat / mitigation effectiveness.	T
CM03	Provide availability of findings, plan of action, security posture, and residual risk through DevSecOps dashboards.	T
CM04	Monitor for change in the threat landscape.	O
CM05	Monitor for change in secure configurations.	T
CM06	Monitor control compliance and continued effectiveness of controls against the changing threat.	T
CM07	Establish metrics: identification, collection, and trend analysis.	T
RM	**Continuous Risk Management practices**	
RM01	Establish or assign a group for managing risks. Should include designated AO representative, development security team, DSOP security team, and mission owners	T
RM02	Establish a method for aggregating findings into a risk posture on cybersecurity, cyber resiliency, and cyber survivability	T
RM03	Identify vulnerabilities and perform impact analysis for establishing risk prioritization.	T
RM04	Establish a dashboard visualization of risk information for continuous review.	T

ID	Description	Level
RM05	Establish periodic reviews of risk and risk remediation / adjudication. Establish approach for ad-hoc resolution of risks that exceed thresholds.	T
RM06	Monitor and respond to security posture, status of metrics, change in threat, and effectiveness of controls.	O
PP	**DSOP cATO practices; for a DSOP that already has an authorization; many of these practices will be inherited by the team responsible for cATO.**	
PP01	Compliance with capabilities and practices listed in the *DevSecOps Fundamentals Guidebook: DevSecOps Tools & Activities* [5] and in one of the DoD Enterprise DevSecOps Reference Designs (RD), such as*:* the *DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes* [6].	O
PP02	Implement zero-trust and boundary access point.	T
PP03	Establish a SOC continuous monitoring strategy using the Software Factory.	O
PP04	Establish CSSP application monitoring for non-approved or malicious actions.	T
PP05	Configure the security sidecar for unique application traffic inspection and handling events.	T
PP06	Identify application control inheritance from the DSOP using a shared security model.	T
PP07	Establish the use of security automation for monitoring the application security posture hosted on the DSOP.	T
PP08	Implement agreed-to risk tolerances in the pipeline guardrails and control gates with event trigger routing.	T
PP09	Establish a cyber operations feedback loop and review of application incidents in collaboration with the program office DevSecOps team.	O
PP10	Visualize the security posture of the application and the DSOP on a dashboard.	T
TP	**Organization's development, security, and assessor Team Practices**	
TP01	Establish an organizational DevSecOps position education, certification, and training process.	T
TP02	Establish hiring position descriptions and certification requirements in line with the DoD Cyber Workforce Framework (DCWF).	O
TP03	Establish a training compliance / validation process to ensure team members meet cybersecurity education, certification, and training requirements.	T

ID	Description	Level
TP04	Ensure that members of the team have experience in developing secure applications, working in a DevSecOps culture, and assessing security practices.	O
TP05	Train team members in the cATO method and practices.	T
TP06	Identify cultural change challenges and the change management approach.	T
TP07	Expand the use of (specialized) training programs for senior technology leaders and project managers on software modernization and cATO methods and practices.	T
TP08	Train the team in performing threat actor analysis, mitigation practices, developing secure code, security automation, determining mitigation effectiveness, the software factory, continuous monitoring, and risk management.	O

Appendix C. Glossary

Authorization boundary "All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected." NIST 800-37r2 [7].

Authorizing Official (AO) is "a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation." NIST 800-37r2 [7].

Authorization to Operate (ATO) is "the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems." NIST 800-37r2 [7].

Authorization to Use is "the official management decision given by an authorizing official to authorize the use of an information system, service, or application based on the information in an existing authorization package generated by another organization, and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system, service, or application. Note: An authorization to use typically applies to cloud and shared systems, services, and applications and is employed when an organization (referred to as the customer organization) chooses to accept the information in an existing authorization package generated by another organization (referred to as the provider organization)." NIST 800-37r2 [7].

Continuous Authority to Operate (cATO) is the state achieved when the organization that develops, secures, and operates a system has demonstrated sufficient maturity in their ability to maintain a resilient cybersecurity posture that traditional risk assessments and authorizations become redundant. This organization must have implemented robust information security continuous monitoring capabilities, active cyber defense, and secure software supply chain requirements to enable continuous delivery of capabilities without adversely impacting the system's cyber posture.

Control gate is a defined point in the project lifecycle when specific requirements, called **exit criteria**, must be met to move to the next phase in the lifecycle. Exit criteria include functional, security, and non-functional criteria.

Common Control Provider is "an organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., controls inheritable by organizational systems)." NIST 800-37r2 [7].

DevSecOps is a software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps

is to automate, monitor, and apply security at all phases of software development: plan, develop, build, test, release, deliver, deploy, operate, and monitor [4].

DevSecOps environment a DSOP with a hosting environment such as a cloud; it includes at least development and test environments, and it may include a production environment, as well as other environments such as integration, staging, and pre-production. The environment is based on one of the *DoD Enterprise DevSecOps Reference Designs (RD)* to be found in the DoD CIO Library.

DevSecOps pipeline is a collection of DevSecOps tools, upon which the DevSecOps process workflows can be created and executed [4].

DevSecOps Platform (DSOP) is the set of tools and automation that enables a software factory. It includes the ability to create DevSecOps pipelines with control gates, and to deploy software into development and test environments. It may also deploy into production, depending on the production environment.

Ongoing authorization is defined as "the subsequent (follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process. The authorizing official is provided with the necessary information regarding the near real-time security and privacy posture of the system to determine whether the mission/business risk of continued system operation or the provision of common controls is acceptable. Ongoing authorization is fundamentally related to the ongoing understanding and ongoing acceptance of security and privacy risk and is dependent on a robust continuous monitoring program." NIST 800-37r2 [7].

Platform A platform is a group of resources and capabilities that form a base upon which other capabilities or services are built and operated [4]. A DSOP is a type of platform, but most platforms are not DSOPs.

Software Factory is a software assembly plant that contains multiple pipelines, which are equipped with a set of tools, process workflows, scripts, and environments, to produce a set of software deployable artifacts with minimal human intervention. It automates the activities in the develop, build, test, release, and deliver phases. The software factory supports multi-tenancy [4].

System is any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. NIST 800-37r2 [7].

Appendix D. Acronyms

ACD	Active Cyber Defense
AO	Authorization Official
ATO	Authorization to Operate
cATO	continuous Authorization (to-Operate)
CIO	Chief Information Officer
CM	Continuous Monitoring
CNCF	Cloud Native Computing Foundation
CONMON	Continuous Monitoring
CSSP	CyberSecurity Service Provider
DCWF	DoD Cyber Workforce Framework
DevSecOps	Development Security Operations
DoD	Department of Defense
DSOP	DevSecOps Platform
IC	Information Capture
JWCC	Joint Warfighting Cloud Capability
KS	Knowledge Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
PP	Platform Practices
RA	Reduce the Attack Surface
RD	(DoD Enterprise DevSecOps) Reference Design
RM	Risk Management
RMF	Risk Management Framework
SA	Security Automation
SBOM	Software Bill of Materials
SCSS	Sidecar Container Security Stack
SIEM	Security Information and Event Management
SOC	Security Operations Center
SSSC	Secure Software Supply Chain
TP	Team Practices

Appendix E. References

Useful references to help better understand the cATO method and practices:

1. D. McKeown, “Continuous Authorization To Operate (cATO) Memo.” Feb. 04, 2022, [Online]. Available: https://dodcio.defense.gov/Library/.
2. Department of Defense Software Modernization Strategy, Nov 2021, Version 1.0. Available: https://dodcio.defense.gov/Library/.
3. DevSecOps Continuous Authorization to Operate Evaluation Criteria, DoD CIO, 2024. Available: https://rmfks.osd.mil.
4. Department of Defense CIO, “DoD Enterprise DevSecOps Fundamentals, Version 2.1.” Sep. 2021, [Online]. Available: https://dodcio.defense.gov/Library/.
5. Department of Defense CIO, “DevSecOps Fundamentals Guidebook: Activities and Tools, Version 2.2.” May 25, 2023, [Online]. Available: https://dodcio.defense.gov/Library/.
6. Department of Defense CIO, “DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes, Version 2.1.” Sep. 2021, [Online]. Available: https://dodcio.defense.gov/Library/.
7. National Institute of Standards and Technology, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev. 2).” Dec. 2018, [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.