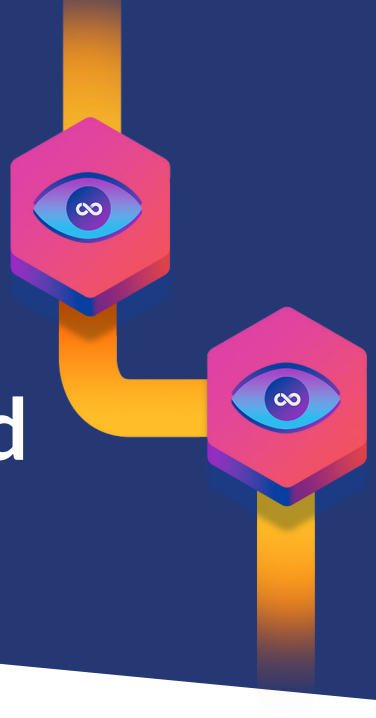
CloudBees® | Solution Brief

Continuous Compliance for Trustworthy DevSecOps and ATO Certainty



Your Burning Compliance Questions

1. How do I consistently ensure RMF compliance across systems and programs, even while modifying controls on the fly?
2. How do I gain the confidence in real time to say that an application complies with standards both internal (organizational policies) and external (regulatory frameworks)?
3. Do I have up-to-date evidence that gives me the ability to do on-going authorizations as we build toward Continuous ATO?
4. How do we know that our investments in security, compliance, and audit are being enforced across the software delivery lifecycle and are producing the desired outcomes for the program and overall mission?

A Path to Continuous ATO

In February 2022, Secretary of Defense released a memorandum highlighting some key factors for organizations seeking cATO.

“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.”

CloudBees® Compliance provides the on-going visibility by continuously monitoring those RMF controls – plus any applicable controls you choose – in order to ensure the adopted DevSecOps reference design is properly implemented and the compensating controls are effective.

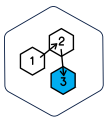
> *Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached.*

CloudBees Compliance:

- Provides the ability for AOs to DECLARATIVELY STATE what "safe and secure" means for the program or mission, and then map that policy prose to automation.
- Runs continuously across the entire organization and SDLC, including production, to create a single source of compliance truth and transparency.
- Provides context of the threat/problem in relation to the SDLC and in relation to the impact on the mission's critical services and applications.

Security teams set program-wide compliance standards for the digital estate (code, binaries, pipelines, environments, identities, and data) without having to train developers or write controls into every tool.

Developers get clear, actionable directions on what needs to be fixed so they can stay focused on delivering mission capabilities.



AOs can make defensible decisions in real time based on contextual risk – without having to wade through alert storms and mountains of false positives or worry about gaps.

Helping Answer Your Burning Questions On:

- Visibility and Trust: Defensible Decisions that Drive Mission Outcomes
- Accelerating Secure and Compliant Software Delivery
- Track and Measure Program Outcomes

Contact public-sector@cloudbees.com for more information.

CloudBees.

CloudBees, Inc.
4 North Second Street | Suite 1270
San Jose, CA 95113
United States
www.cloudbees.com
info@cloudbees.com