


# How CloudBees® CI/CD Can Support Digital Engineering, Digital Twins and Model-Based System Design



CloudBees provides the leading DevOps platform for compliance-focused organizations. By creating repeatable paths for production deployment of applications, CloudBees helps you get your software into production easily and quickly. Using tools that provide robust control over compliance and governance, developers are empowered to focus on efficiently delivering quality code to meet your mission.

## CloudBees CI/CD also supports best practices for:

- Digital engineering with authoritative repositories for configuration, compliance, and system metrics that scale up to the enterprise level.
- Managing digital twins with a scalable platform that drives both simulations and live systems, so you can develop your CI/CD process at project inception.
- Model Based System Design with tools to facilitate centralized standards, code reuse, and data collection.

## Centralized Release Management

Digital engineering mandates a single “source of truth” for system data that’s integrated across all lifecycle activities like builds, deployments, and releases.

Declarative pipelines go a long way toward building robust, reliable, and repeatable builds. They make it easy to build the same short iterations that make code better for your builds and deploys. But without an easy way to share code and tools to enforce standardization, it’s too easy to fall back on freestyle jobs.

CloudBees Pipeline Templates are tools to enforce consistency and speed development time. Teams create templates with the Pipeline options that are appropriate for their jobs, and developers choose the one that suits their projects.

Pipeline Policies go a step further with tools for setting restrictions that reflect regulatory rules and organizational policies. They are runtime validations for declarative and scripted pipeline code. They can block the execution of jobs that don’t comply with regulations or best practices.



Declarative pipelines go a long way toward building robust, reliable, and repeatable builds.

With CloudBees CI, centralized management goes beyond standardized scripts. It facilitates all aspects of administration, from plugins to cloud resources. This means it's easier to run the CI/CD pipelines for all your systems from a consistent and consolidated platform. So, you can apply the lessons you've learned in simulations to your production systems and create repeatable paths to production across environments with different security levels.

Pipeline Policies go a step further with tools for setting restrictions that reflect regulatory rules and organizational policies. They are runtime validations for declarative and scripted pipeline code. They can block the execution of jobs that don't comply with regulations or best practices.

With CloudBees CI, centralized management goes beyond standardized scripts. It facilitates all aspects of administration, from plugins to cloud resources. This means it's easier to run the CI/CD pipelines for all your systems from a consistent and consolidated platform. So, you can apply the lessons you've learned in simulations to your production systems and create repeatable paths to production across environments with different security levels.

## DevOps Reporting and Analytics

Your single source of truth needs to extend beyond configurations into reporting and analytics. CloudBees Analytics has dashboards and reporting functions with consolidated views for planning, scheduling, and auditing your pipelines. You can watch releases and deployments and collect the data you need to drive continuous improvement at the same time.

CloudBees dashboards employ an extensible model, so you can create different views for different teams. Development teams can have dashboards for their projects, while management can focus on the high-level metrics they need.



Your single source of truth needs to extend beyond configurations into reporting and analytics

## End-to-End Compliance

In order to successfully implement Continuous Authorization To Operate (cATO), your DevOps system needs:

- Continuous visibility into cybersecurity activities inside the system
- An approved DevSecOps design
- Active cyber defense that can respond to threats in real time

There are multiple systems that comprise your capabilities, so you need a system that can assess compliance at more than just a single tier or stage. With CloudBees Compliance, you assemble rules that the system uses to scan your pipelines at every stage, giving you continuous visibility into every component.

A robust DevSecOps design secures your application in development, protects it during delivery, and guards it in production. These practices, like linting code and scanning for threats, are critical to success. The system needs to account for more than just your compiled code, but also for thirdparty libraries, environments, identities, and data. CloudBees facilitates this model with controls and gates that you can map to regulatory frameworks like FedRAMP and NIST for each stage in your pipeline.

Reacting to threats in real time means not just having a way to detect and react to threats, but reacting as quickly as possible, too. In other words, reducing your meantime to recovery (MTTR.) CloudBees Feature Flags act as a kill switch for new features. It's effective for targeting new features to a subset of clients, but it's also a powerful security mechanism, too. If all your applications follow the same build model, you can kill features if they're linked to a threat without killing the user experience or pulling back a new release. This is a process that you can easily practice, and its integral to CloudBees CI/CD.

Learn more at [www.cloudbees.com/federal](https://www.cloudbees.com/federal)