Application Lifecycle Management (ALM) Tools Usage Policy for Agency Software Development

The NRC has completed the implementation of the ALM tools (Atlassian Jira, Bitbucket, Bamboo, Invicti, and Octopus Deploy). Office of the Chief Information Officer (OCIO) Leadership wants to ensure that the usage of the agency's approved ALM tools and processes are instituted with a policy that will aid in providing consistent usage and standards for the Continuous Integration (CI) and Continuous Delivery (CD) throughout system and application development, testing, production, and monitoring phases of the agency's system/application lifecycle. This transformation is designed to support and further develop the agency's adoption of agile-based software development practices and DevSecOps methodologies. The paragraphs below provide a high-level description of policy, concepts, processes, requirements, and tools surrounding NRC's ALM capabilities.

There are two methods for developing software at the NRC:

1. Developing an application off-site on vendor provided infrastructure, or
2. Developing an application in the cloud in the Enterprise Development and Test Environment (EDTE).

Either scenario requires application's source code to be **maintained** in a repository in the agency's Source Control Management (SCM) solution, Bitbucket. Also, there must be a defined compile/build process for each software component in the CI tool, Bamboo. This practice:

- Ensures that the software component's source code is continuously validated in the respective project repositories.
- Facilitates and ensures traceability to determine what approved software component source code is running in the Production Operating Environment (POE).
- Software enhancements in development or bugs to be fixed.
- Supports and promotes the adoption of agile-based software development concepts as well as the agency's DevSecOps methodology.
- Ensures source code vulnerability analysis has been completed at specified intervals.

Once the application development team onboards their compile/build processes into the agency's CI tool, the NRC's ALM team will orchestrate the specific automated deployment processes required by each application in order to deploy required artifacts across the pre-production and production environments using the current approved CD tool, Octopus Deploy.

Additionally, NRC requires developers to utilize approved security and functional testing tools (Invicti, Veracode, Selenium, JMeter, and Ranorex, etc.) early in the development process to assist in minimizing security vulnerabilities, thereby avoiding delays at the end of the development process. The use of these tools also orchestrates functional and performance testing for all applications across NRC's enterprise.

System/Application Deployments:

To deploy the application artifacts from the compile/build onto any NRC Production System, the following requirements and artifacts are necessary:

1. A clean Veracode code analysis report and Invicti application security scan result (e.g., All critical and high vulnerabilities must be remediated).
2. A set of release notes providing all relevant information regarding enhancements and bugs being deployed.
3. A test and rollback plan.

The artifacts are required as part of any change request submission to the Change Control Board (CCB) so the CCB members can make educated decisions on approvals of the changes to be deployed into the POE.

NRC DevSecOps Tools:

The following are brief descriptions of the industry leading tools the agency has adopted to support the ALM process. They will help ensure the delivery of quality work products and services in support of NRC mission requirements for application software development:

Jira (Change Management)

Jira is the Agency's official tool used for issue tracking and overall project management functions. The Jira Dashboard will act as the user's central dashboard for tracking all activities in their project. Each team has an initial choice of using three standard workflows (Simple, Standard and Complex) that can be customized for specific needs or business processes. Jira has traceability to Bitbucket (Source Control) and Bamboo (Builds) to identify what code changes were made for each issue, bug, or improvement. Confluence will be used as the agency's application technical documentation repository.

Confluence (Collaboration)

Confluence is the agency ALM workspace where project teams share knowledge and collaborate on projects. It allows project teams to create, capture, and collaborate on any project or idea and provides visibility into institutional knowledge and access to the information needed

Bitbucket (SCM)

Bitbucket is the agency's official source code repository tool. All production source code is required to be actively updated in these repositories as software is being developed and released to production. Bitbucket is a Git based SCM system, the most widely used standard for source control management globally. Sourcetree is the Git client that allows users to push and clone source control repositories and on developer's workstations. Bitbucket provides issue, commit, and build traceability to the other ALM tools.

Bamboo (Build Management/CI)

Bamboo is the agency's official CI tool used to orchestrate software builds and releases across the agency's environment lifecycle. Bamboo organizes the development team's source code builds into plans. This tool orchestrates source code builds, automated testing, and deployments from a single console.

Octopus Deploy (Automated Deployment/CD)

Octopus Deploy is the agency's official CD tool orchestrating the deployments of software release artifacts across the agency's environment lifecycle. The software release lifecycle is dev (EDTE), test, User Acceptance Testing (UAT)/Pre-production (Pre-prod), then production (Prod). Each application will be broken up into components and delivered incrementally through the lifecycle.

Selenium & Ranorex (Automated Testing)

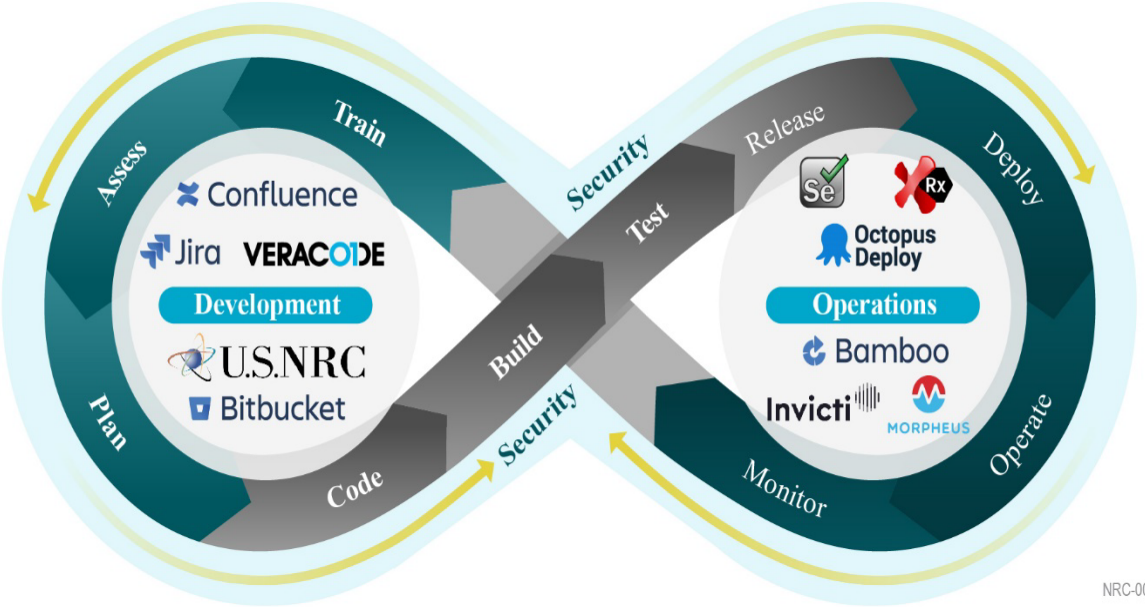
Selenium, JMeter, and Ranorex will be used to orchestrate functional and performance testing for all applications across the agency. Selenium is a browser automation tool that allows for the user to record specific functional tests for web applications. JMeter is a desktop tool that can be configured to test web applications for performance based on usage. Ranorex is a studio desktop application that can test desktop, web, and mobile applications. These tools integrate with Bamboo and Jira to allow for traceability across the entire suite of ALM tools.

Morpheus (Automated Provisioning and Configuration Management)

Morpheus is the agency's cloud governance tool used to implement Infrastructure as Code & Compliance as Code to standardize the application server's configuration across all environments. Morpheus will orchestrate middleware installations and configuration upon instance creation in cloud-based environment.

Invicti (Web App Scanner)

Invicti is an automated, yet fully configurable, web application security scanner that enables you to scan websites, web applications, and web services, and identify security flaws. Invicti can scan all types of web applications, regardless of the platform or the language with which they are built.


Assess
Train
Plan
Code
Build
Security
Test
Release
Deploy
Operate
Monitor
Security
Confluence
Jira
VERACODE
Development
U.S.NRC
Bitbucket
Octopus Deploy
Operations
Bamboo
Invicti
MORPHEUS

NRC-005-v02