CLAMP R3 - M4 Code Freeze Milestone Checklist

The following items are expected to be completed for the project to Pass the M4 Code Freeze Milestone.

M4 Release Code Freeze Milestone overview is available in wiki.

Practice Area	Checkpoint	Yes /No	Evidences	How to?
Product Management	Have all JIRA Stories supporting the release use case been implemented?	Yes	17 issues	
	List the Stories that will not be implemented in this current Release.	Yes	31 issues	
	Are committed Sprint Backlog Stories been coded and marked as "Closed" in Jira?	Yes	80 issues	
	Are all tasks associated with committed Sprint Backlog Stories been marked as "Closed" in Jira?	Yes	18 issues	
Release Management	Have all issues pertaining to FOSS been addressed?	Yes		
	Have all findings from previous milestones been addressed?	Yes	No specific findings	For M2 and M3 Milestones, ensure all findings have been closed.
	Has the Project Team reviewed and understood the most recent license scan reports from the LF, for both (a) licenses within the codebase and (b) licenses for third-party build time dependencies?	Yes		
	For both (a) and (b), have all high priority non-Project Licenses been either removed or escalated as likely exception requests?	Yes	Nexus IQ report	
Development	Are all Defects of priority Highest and High in status "Closed" in Jira?	Yes	3 issues	
	Has the project team reach the Automated Unit Test Code Coverage expectation? (Refer to artifacts available in Sonar)	Yes	Goal: 50% for Incubation project in Beijing	For evidences, provide link(s) to Gerrit repos by providing the URL as shown in this example clamp gerrit sonar link
	Is there any binaries (jar, war, tar, gz, gzip, zip files) in Gerrit project repository?	No		Refer to CI Development Best Practices
	Is there any pending commit request older than 36 hours in Gerrit?	No		
	Provide the "% Achived" on the CII Best Practices program.	98%	cii best practices in progress 98%	As documented in CII Badging Program, teams have to fill out CII Best Practices
	Is there any Critical and Severe level security vulnerabilities older than 60 days old in the third party libraries used within your project unaddressed? Nexus-IQ classifies level as the following: • Critical is level 7 to 10 • Severe is level 4 to 6 • Moderate is level 1 to 3 which is complaint with CVSS V2.0 rating.	Yes	In the case critical known vulnerability are still showing in the report, fill out the Security Vulnerability Threat Template in your project. nexus IQ report	Ensure the Nexus-IQ report from "Jenkins CLM" shows 0 critical security vulnerability. Open the Nexus-IQ report for the details on each repo.
	Are all the Jenkins jobs successfully passed (verify + merge jobs)?	Yes	CLAMP jenkins tab	
	Have all OOM Staging Healtcheck related to your project passed?	Yes		
	Are all snapshot binaries available in Nexus-staging?	Yes	Provide link to clamp Nexus	
	Do you have a clear plan to implement the Independent Versioning and Release Process by RC0?	Yes		Contact the upstream teams to make sure they will release their artifacts (in Nexus Release repo) so you can build by depending on these released artifacts by RC0.

Integration and Testing	Have 100% of Continuous System Integration Testing (CSIT) Use Cases been implemented successfully in Jenkins?	Yes	Jenkins CLAMP tab	
	Is there a Docker images available for your project deliverable?	Yes	Nexus 3 clamp docker repo	
	Has the project code successfully passed the Daily Build process?	Yes	Jenkins CLAMP tab	Goal is to ensure the latest project commit has not broken the Integration Daily Build
Doc	Has the team created a docs folder and Development and Release Notes documentation templates in Readthedocs?	Yes	CLAMP readthedocs link	
	Is the API documentation section populated?	Yes	CLAMP documentation	API doc included in Online doc Note that CLAMP is now integrated with SWAGGER and MSB