

SHIP-HATS Compliance Framework Transition

Jason Kwan, Senior Software Engineer, GovTech

Geok Rong, Software Engineer (II), GovTech

CLASSIFICATION

Agenda

- Compliance Pipeline Removal
- What will happen in GitLab 19.0
- Transition to Pipeline Execution Policy
- Transition: Action to take
- Demo
- Q&A

Compliance Pipeline Removal

Compliance Pipeline

- **Status:** Deprecated (since [GitLab 17.3 in Sep 2024](#))
- **Scheduled for Removal:** GitLab 19.0 (24th June 2026)

Who is impacted?

Projects and users using ship-hats compliance framework

GitLab 19.0 (24th June 2026)

Background:

Our Compliance Frameworks were configured to use Compliance Pipelines. The EOL of Compliance Pipelines meant we needed to transit to a new framework.

What happens if no action is taken:

- **Compliance Framework Label will remain** on project (Reason: Compliance Framework is NOT deprecated/removed, this feature remains in Compliance Center)
- **Compliance Pipeline is non-functional**, meaning Compliance Framework is just a label that serves no purpose to your pipelines

Impact:

- It may break users' pipelines if there are dependencies on ship-hats compliance framework's jobs.
- Jobs from SHIP-HATS Compliance Framework will be missing from users' pipelines.

After version 19, existing SHIP-HATS Compliance Frameworks will cease to function if no action is taken.

Transition from Compliance Pipelines to Pipeline Execution Policy



SHIP-HATS has created a Security Policy Project ([stored in Innersource, linked to WOG](#)) with **Pipeline Execution Policy** as a replacement of existing SHIP-HATS Compliance Frameworks

Caveats:

- This Pipeline Execution Policy (PEP) is based off the **SHIP-HATS Catch All Compliance Framework** with **standardization** in mind – modifications are required on users' pipeline configurations
 - This PEP is designed to **replace all 5 flavors of existing compliance framework** (e.g ship-hats-docker-multi-service-compliance, ship-hats-webapp-compliance, ship-hats-single-service-compliance, ship-hats-docker-ci-compliance and ship-hats-catch-all-compliance)

Considerations before embarking on the transition:

- Are the **stages** aligned between your GitLab configuration and PEP?
- Is **.parallel-matrix-vars** defined in your GitLab configuration file?
- Are there **scans** that need to be **excluded** from your pipeline?

Transition: What is the process?

Before GitLab 19.0

5 Compliance Frameworks with Compliance Pipeline (v1.0.1 to v1.1.7)

1. ship-hats-docker-multi-service-compliance
2. ship-hats-webapp-compliance
3. ship-hats-single-service-compliance
4. ship-hats-docker-ci-compliance
5. ship-hats-catch-all-compliance

Users need to make the transition before **24th June** to avoid impact of CF change

After GitLab 19.0

Compliance Frameworks with Compliance Pipelines (v1.0.1 to v1.1.7)

Non-Functional

Removed

1 single Catch all Compliance Framework linked to Pipeline Execution Policy (PEP)

- ship-hats-pipeline-execution-policy

Will continue to work

Options to manage the Compliance Pipeline Removal

1. Switch to pipeline execution policy with new compliance framework (**recommended**)
 - `ship-hats-pipeline-execution-policy`
2. Use "include" with existing template (**only supported for next 6 months**)

```
include:  
- project: "innersource/sgts/ship-hats/ship-hats-compliance"  
  ref: "main"  
  file:  
  - /v1.1.7/compliance-templates/webapp-compliance.yml
```

Transition: Action to take to use PEP

1. In your gitlab configuration,
 - a) it should include build, static-test, runtime-test, sign, deploy-to-prod stages
 - Rearrange stages
 - Update Job stage
 - b) configure .parallel-matrix-vars
 - c) additional variables may be needed for certain use cases
2. Store project's CICD variables to exclude scans that are not applicable to your project
 - a) Example:
 - CONTAINER_SCANNING_DISABLED = true
 - RUNTIME_TEST_DISABLED = true
3. Include the PEP configuration files for testing and remove them once testing is finished.
4. Switch the compliance framework applied on your project to **ship-hats-pipeline-execution-policy**.

More details: [Innersource / SGTS / SHIP-HATS / WOG - Security Policy Project · GitLab](#)

Recap

What are you using?	Action to Take	When?
Compliance Framework	Move to either: 1. Pipeline Execution Policy (recommended) 2. Compliance Framework Templates (6 months)	Before 24 June 2026
Compliance Framework Templates (via "include")	Move to Pipeline Execution Policy	Before Dec 2026

1. Switch to pipeline execution policy with new compliance framework (**recommended**)
 - `ship-hats-pipeline-execution-policy`
2. Use "include" with existing template (**only supported for 6 months after 24 June 2026 – compliance framework templates will no longer be maintained after Dec 2026.**)

```
include:  
- project: "innersource/sgts/ship-hats/ship-hats-compliance"  
  ref: "main"  
file:  
- /v1.1.7/compliance-templates/webapp-compliance.yml
```



Thank you.