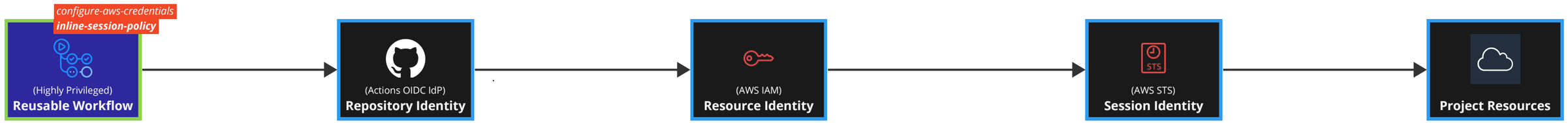
# Introduce a reusable workflow that enforces resource naming




**GitHub Docs**
*github context*

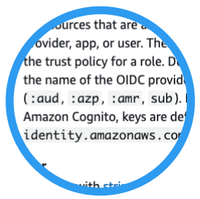
- calling repo details available at runtime

👀 - a highly privileged Reusable Workflow could dynamically template an inline-session-policy, only allowing access to resources owned by the calling repo

**GitHub Docs**
Example: Requiring a reusable workflow

🔐 - OIDC claims are cryptographically signed

- includes details for the calling action & its repo



**AWS Docs**
*Available keys for AWS web identity federation*

can only access OIDC claims for:
- :aud
- :azp
- :amr
- :sub

🙌 can enforce only our (highly privileged) Reusable Workflow is able to use an inline-session-policy through a customised `sub` claim in GitHub

**configure-aws-credentials Docs**
*Session tagging*

🚀 - through the inline-session-policy assumed by our Reusable Workflow, AWS IAM+STS can identify a runner as acting on a particular project and restrict resource access

🎉 - configure-aws-credentials' role session naming allows repo details to show in CloudTrail

**_Infrastructure Team_ Managed Resource**
with load-bearing security responsibilities

**Externally Managed Resource**
with load-bearing security responsibilities