DevSecOps engagement-Checklist

1. Project Name:
2. Project Sponsor (Director or above):
3. Accounting String to charge time against:

**Application Team Specific**

1. Is this a SOX application?
2. Does the app contain Sensitive/Confidential data? Such as PII
3. Can the application support Blue/Green patching methodology?
4. Is this app Container native? Docker / Kubernetes
   1. If no, can it be?

Confluence:

1. Confluence space name:
2. Confluence space admins:
3. Purpose:

Jira:

1. Project name:
2. Project type:
3. Project key:
4. Roles:
5. Is migration needed from any other issue tracking tool:

Source/Version Control:

1. Number of Developers/Contributors:
2. Any source control being used currently:
3. Familiarity with git operations:
4. Branching strategy:

Artifact Management:

1) Location where artifacts currently being stored:

2) Promotion/demotion process:

3) Versioning process:

Continuous Integration:

1. Any CI being used currently (name, location):
2. Tech stack (.Net, Java, ..etc):
3. Build frequency:
4. Automated unit tests:
5. Unit tests pass rate:
6. Unit tests coverage:
7. Other types of tests (Regression, Integration, Smoke,..etc):

Continuous Delivery/Continuous Deployment:

1. Environments (Staging, QA, Prod,..etc):
2. Frequency of deployment to each environment:
3. Time it takes in current state to deploy to each environment:
4. Planning on using automation to deploy to Production?:

Code inspection/quality:

1. Any code inspection/code quality processes or tools being used currently like Sonarqube:

SAST/DAST

1. Any static/dynamic security scanning being used currently:
2. Fail the build if security scanning didn't pass?: