6 Pillars of DevSecOps
— a SAFECode / Cloud Security Alliance partnership —

These pillars provide a framework that blends the traditionally siloed operations: development, infrastructure operations, and information security, into a cohesive whole that facilitates the creation of secure software.

Lead Authors and Contributors:
John Martin, Setumadhav Kulkarni, Ronald Tse, Michael Roza, Sean Heide, David Lewis, Eric Gauthier, Lee Szilagyi

Published Pillars: Automation and Collective Responsibility. Four papers are in work and open to contribution.
6 Pillars of DevSecOps

Pillar 1: Collective Responsibility
- Security is fundamental
- CSO team leads, but everyone must be aware and contribute
- Users and developers the first line of defense

Pillar 2: Collaboration and Integration
- Team members must share their expertise
- Awareness and cooperation are necessary to avoid or mitigate incident

Pillar 3: Pragmatic Implementation
- Security must be integrated into development practices and toolchain
- No one-size-fits-all solution – practices must be tailored to target system
- Usability is key to success
6 Pillars of DevSecOps

Pillar 4: Bridging Compliance & and Development
- Compliance requirements help to identify appropriate controls
- Translate controls to software measures that can be automated and measured

Pillar 5: Automation
- Automated practices are core to process efficiency
- Seek to automate development and operational security tasks wherever feasible

Pillar 6: Measure, Monitor, Report & and Action
- We can’t manage what we don’t know
- Measure during development and operations

Summary
Measures in SAFECode/CSA document are key to successful DevSecOps execution