SEI WEBINAR SERIES | Keeping you informed of the latest solutions

Software Engineering Institute | Carnegie Mellon University

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003515

Continuous Integration
Secure DevOps

Hasan Yasar,

Technical Manager

Secure Lifecycle Solutions

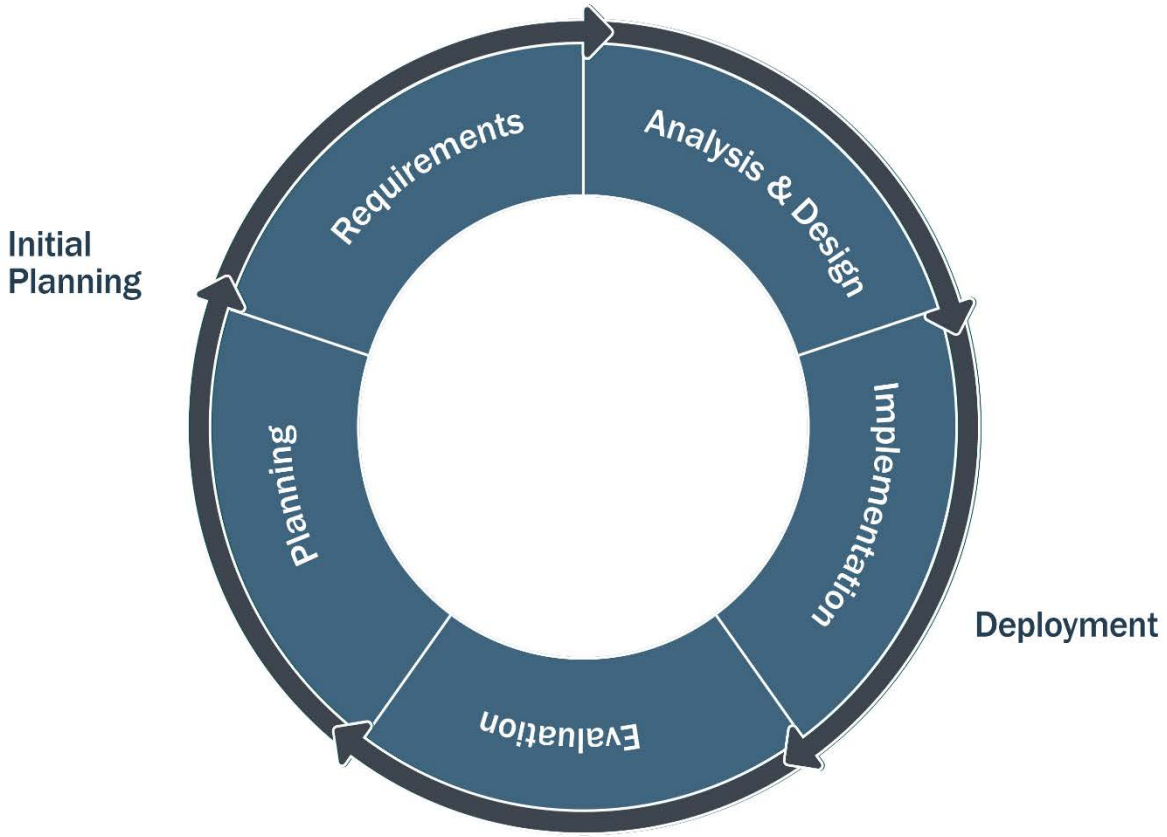
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

What Is DevOps?

The DevOps Movement Began as a Reaction …

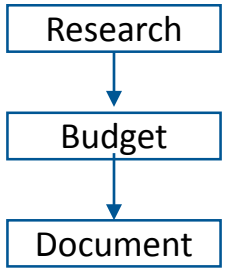
to years of disconnect between Development and Operations that began to manifest itself as conflict and inefficiency

Agile Method

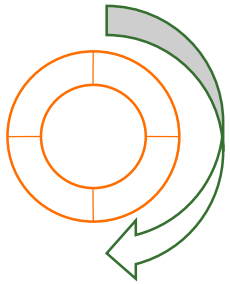


Water - Scrum - Fall

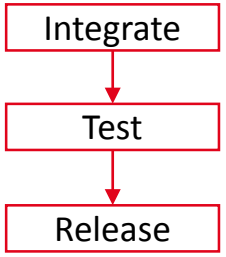
Business



Development

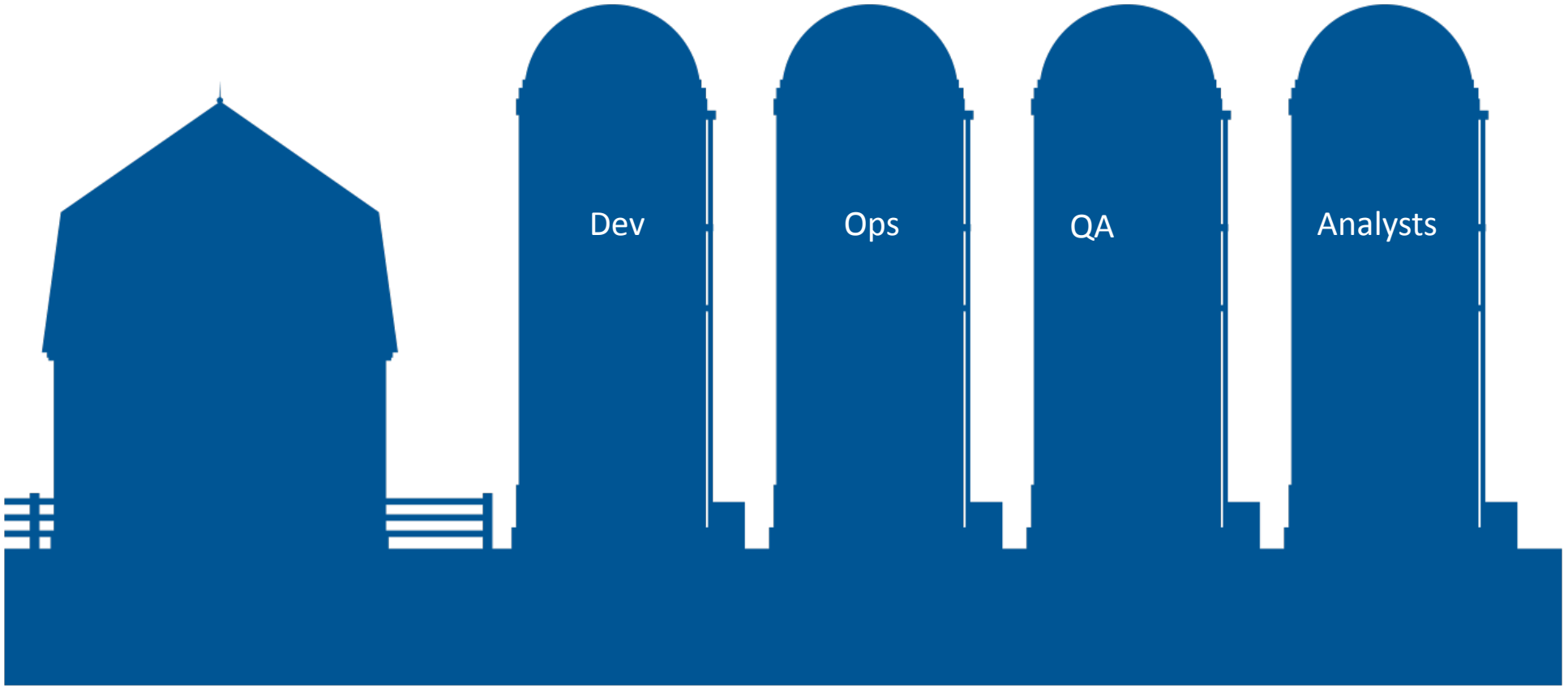


QA
Operations

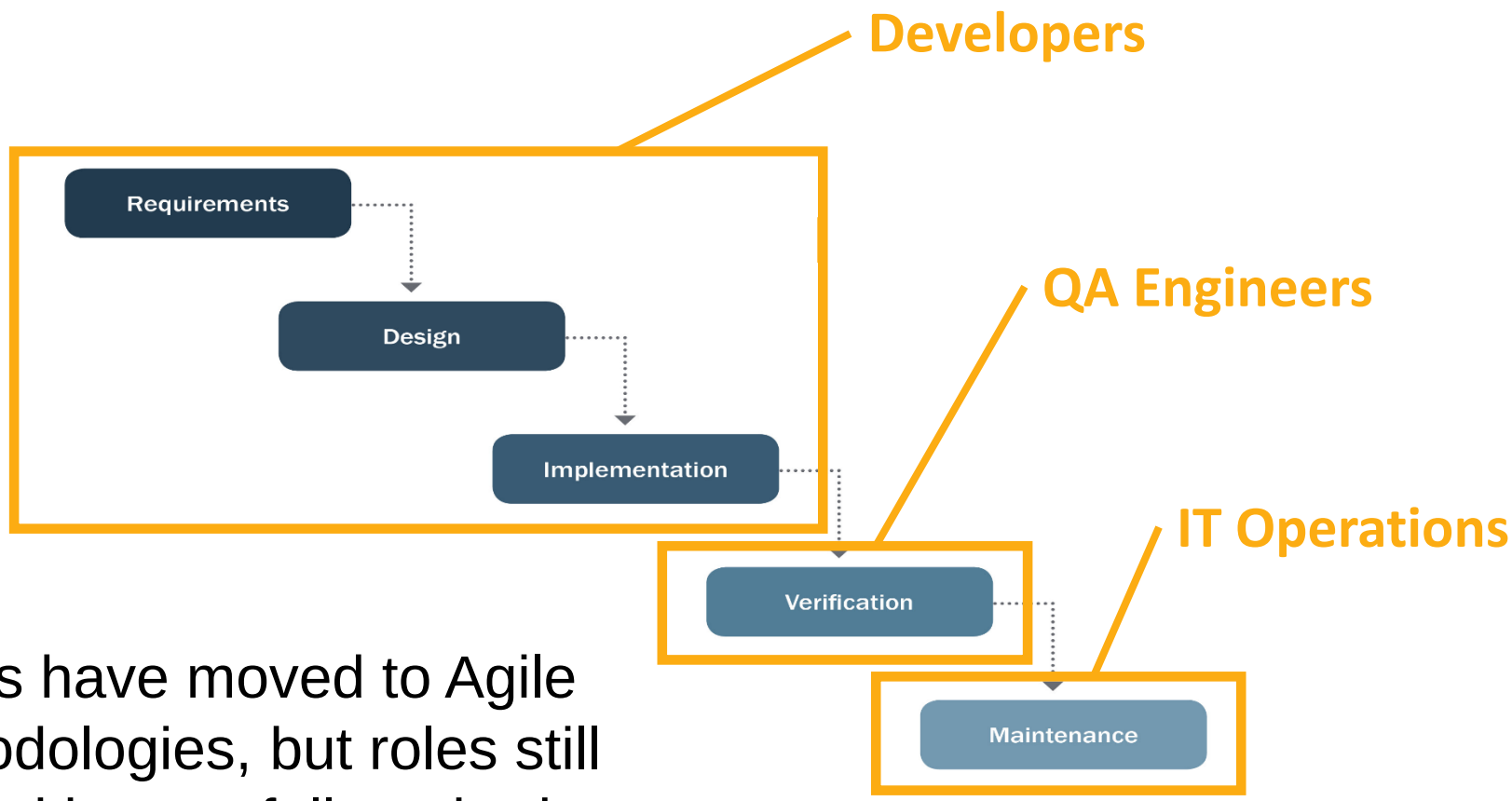


Jez Humble, https://youtu.be/L1w2_AY82WY
Dave West, http://sdtimes.com/analyst-watch-water-scrum-fall-is-the-reality-of-agile/

Silos Block Collaboration



Silos Reinforce Waterfall



Teams have moved to Agile methodologies, but roles still align with waterfall methods

Polling Question

Would you like more information about DevOps?

1. Yes
2. No

DevOps is an Extension of Agile Thinking

Agile

Embrace constant change

Embed Customer in team to internalize expertise on requirements and domain

DevOps

Embrace constant testing, delivery

Embed Operations in team to internalize expertise on deployment and maintenance

DevOps Aims to Increase…

…the pace of **innovation**

…**responsiveness** to business needs

…**collaboration**

…software **quality**

DevOps Has Four Primary Focus Areas

Collaboration between project team roles

Infrastructure as Code: Scripted Infrastructure Configuration

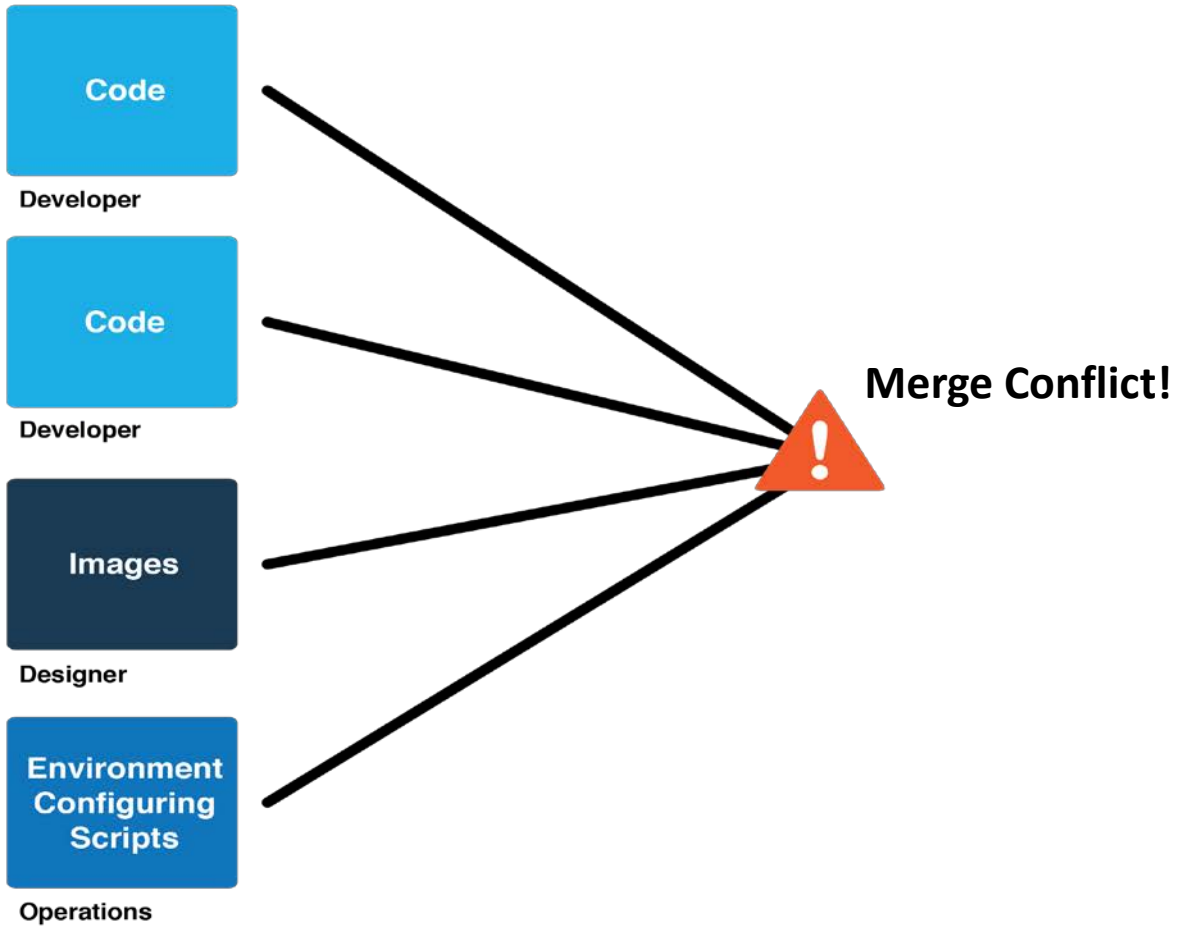
Automation of Tasks / Processes / Workflows

Monitoring Applications and Infrastructure

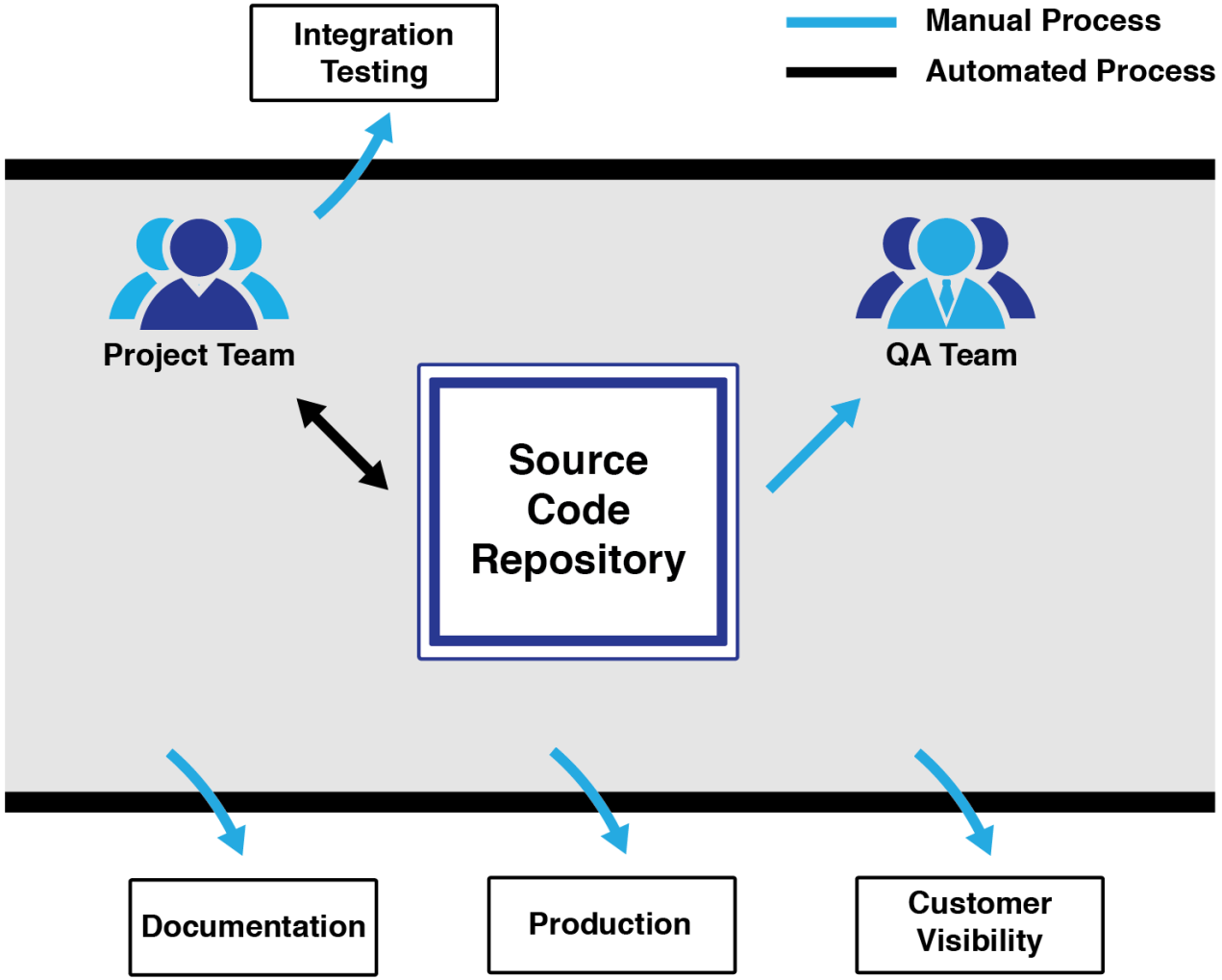
Continuous Integration

Software projects consist of many artifacts

Integration can be challenging



This is often a manual process



Manual Integration is Flawed

Human-driven processes are…

- Infrequent
- Expensive
- Repetitive
- Error-prone

This leads to:

Disjointed activities / components

Slow, unreliable, costly reporting and failure recognition

Lack of transparency of problems

Integration Hell

Polling Question

Do you currently implement Continuous Integration in your development cycle ?

1. Yes
2. No

Automating Integration Fixes These Issues

Automation…

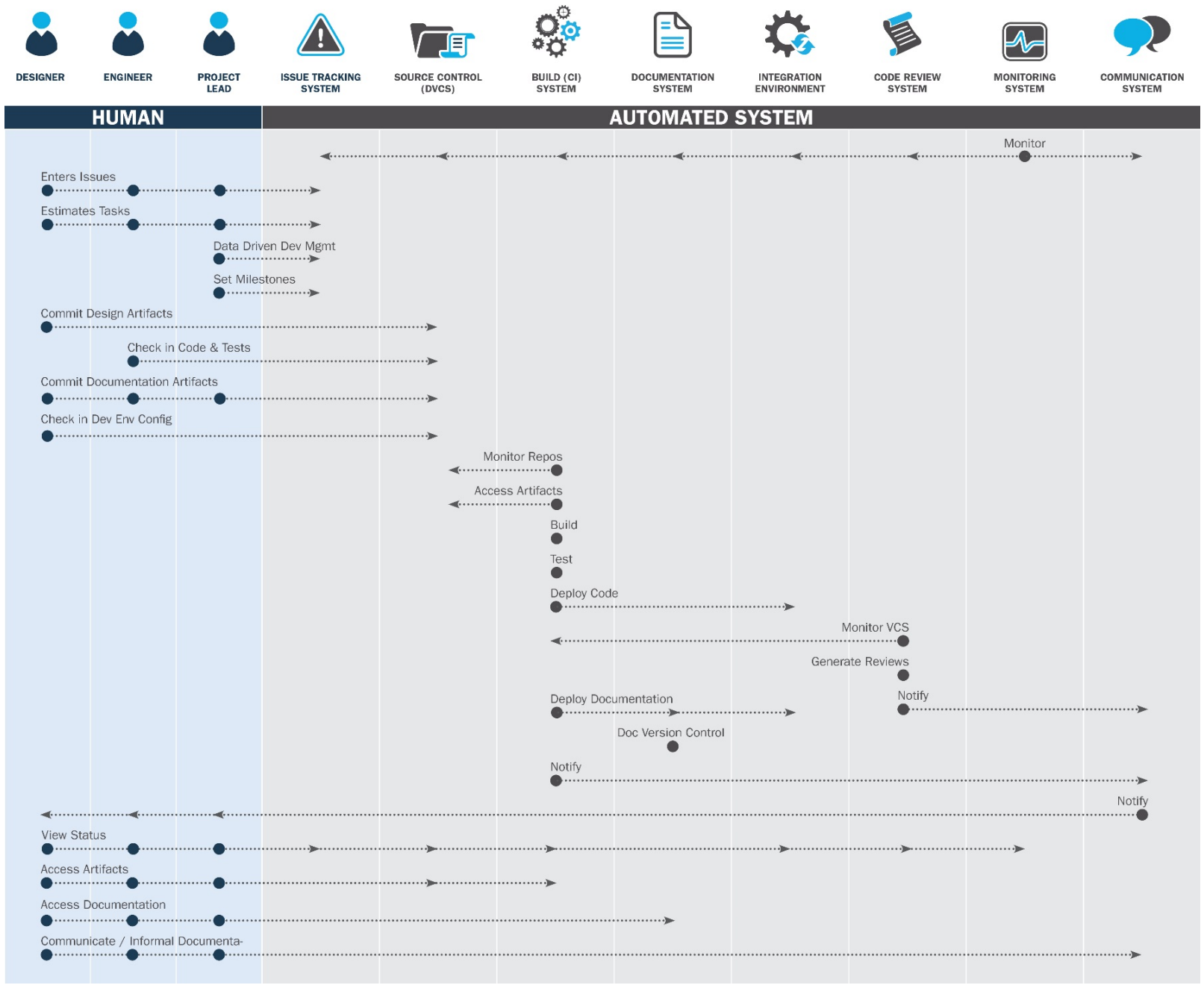
Removes inefficiencies due to human-driven process

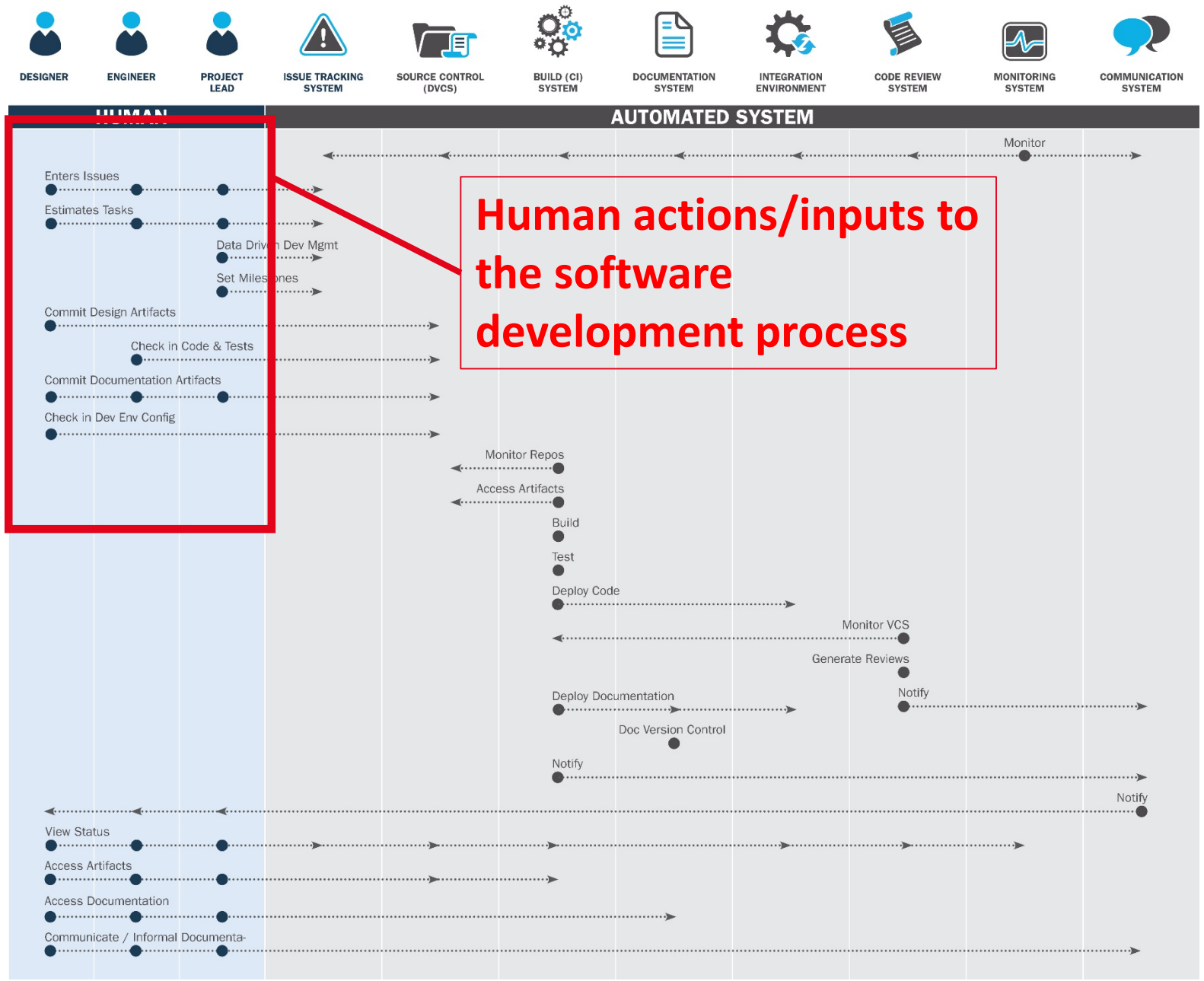
Standardizes artifact submission process

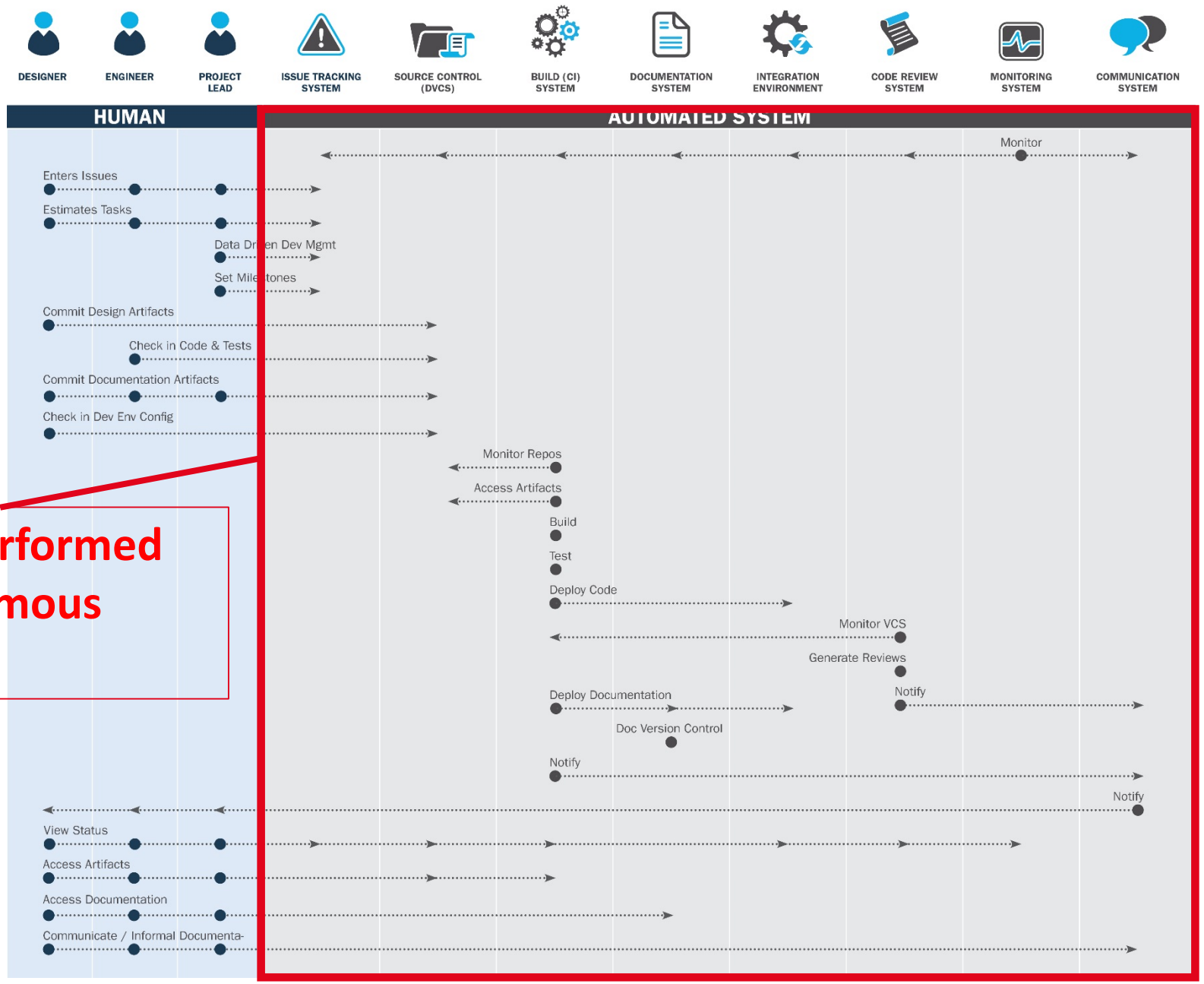
Guarantees **consistent results**

Allows team to **fail fast** (and fix fast)

Reduces pain of integration







Actions performed by autonomous systems

Continuous Integration is Even Better

Continuous Integration uses a **build server** to…

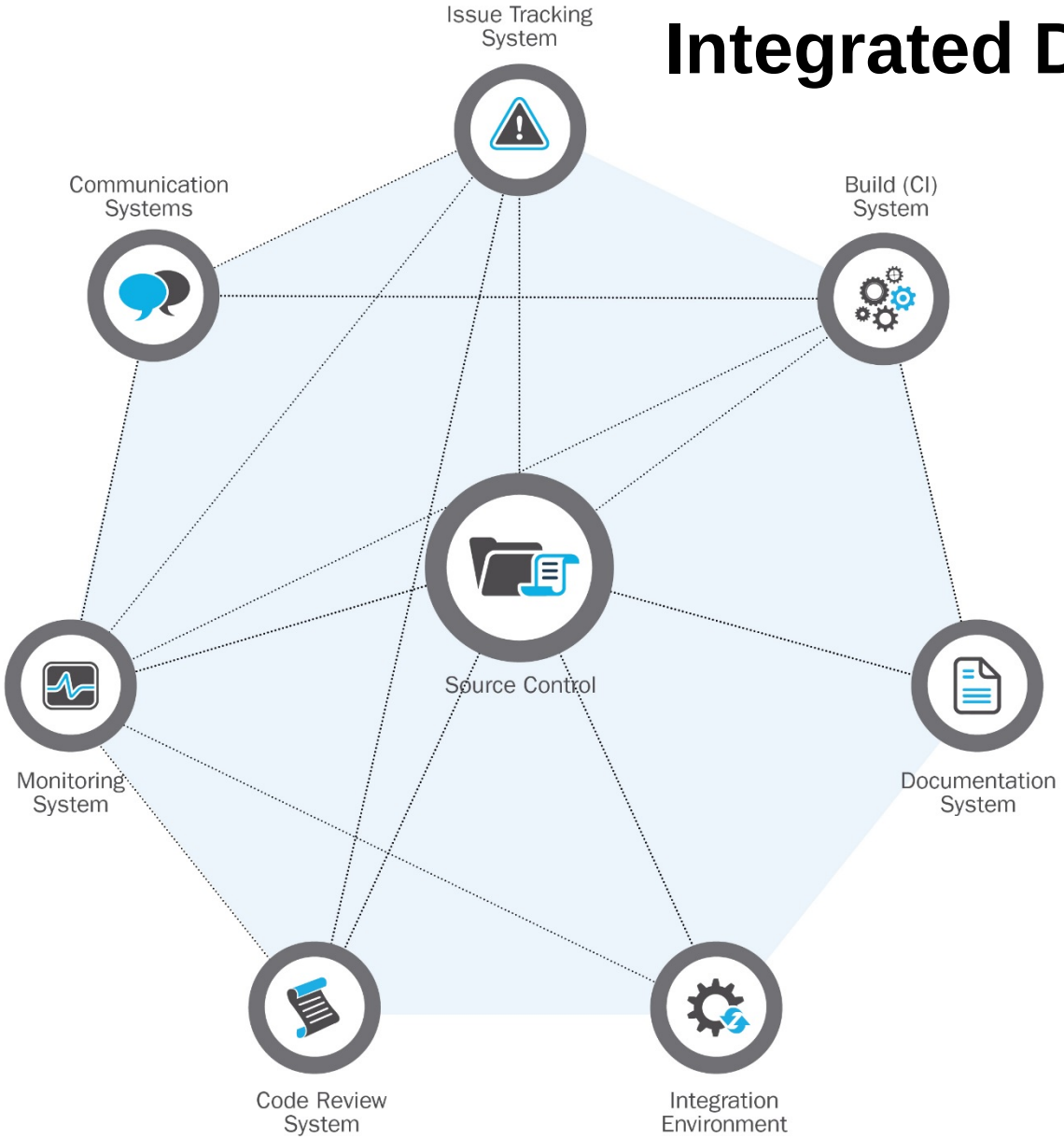
Integrate artifacts on **every change**

Give team with **immediate notification** of failure or success

Require issues be fixed before moving forward

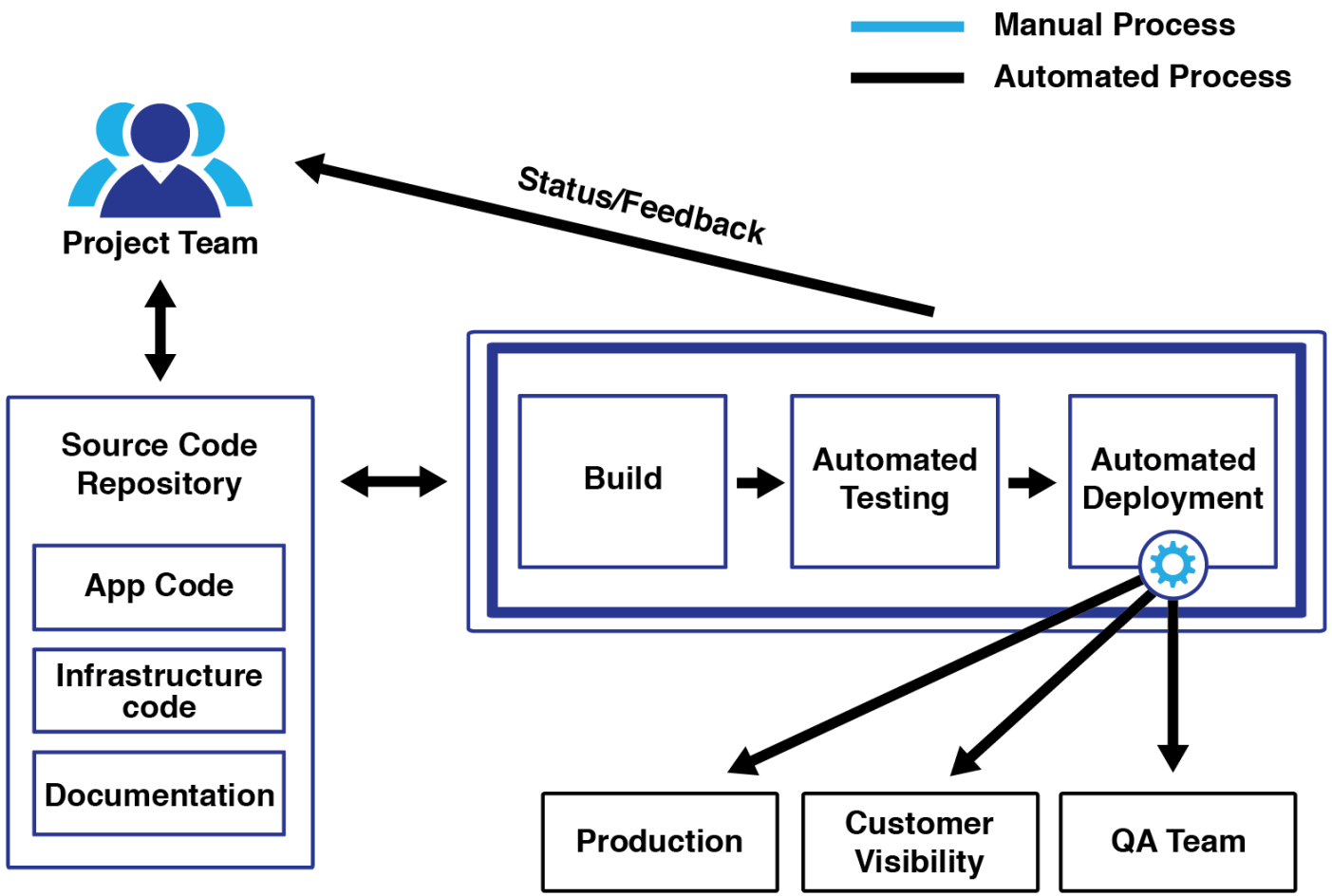
Enforce standards (can fail based on quality as well as functionality)

Integrated Development pipeline



Integration and communication, even among tools, is the key!

Continuous Integration (CI) Model



Fail the Build When Software is Not Good Enough

Don’t just configure failure for compile/build errors!

Want 90% test coverage? **Fail the build if code base is <90% covered**

Want all DB queries < 2sec? **Test them, and fail the build otherwise**

Want to make sure code conforms to style guide? **You guessed it…**

CI is your best tool to enforce quality standards

Secure DevOps

Integrating Security practices into DevOps

Team Composition

Developers

Features

Quality Attributes

Efficiency

Performance

Users

Authentication

Authorization

IT Ops

- Deployment
- Maintenance
- Updates
- Change policy
- Failure
- Data loss
- Risk prevention

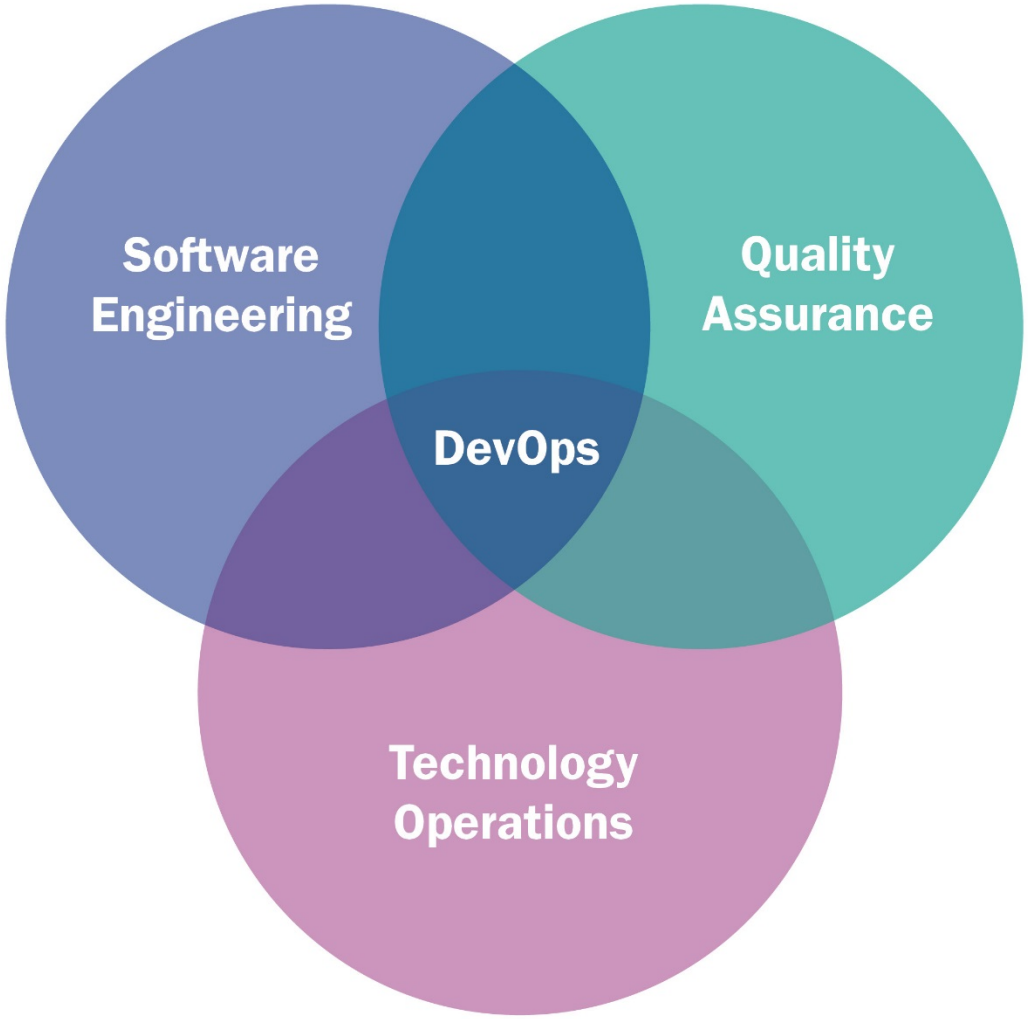
QA

- Testable
- Issue tracking
- Bug Reports
- Usability
- Help Desk

Security Team

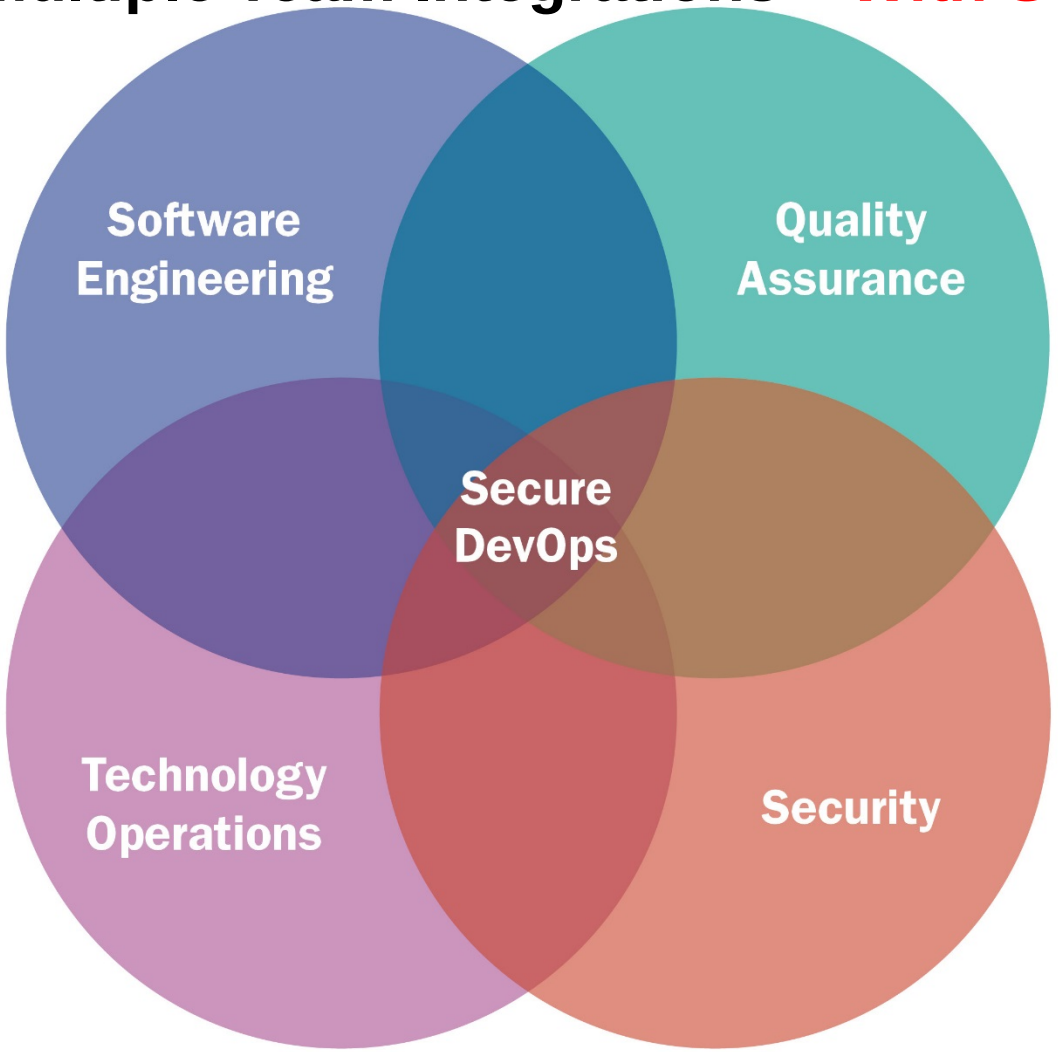
- Data Privacy
- Intrusion detection
- Threat vectors
- CVEs
- Package security
- Authentication
- Authorization
- Security Standards Compliance

DevOps: Multiple Team Integrations



DevOps: Multiple Team Integrations + *With Security Team*

DevOps: Multiple Team Integrations + *With Security Team*

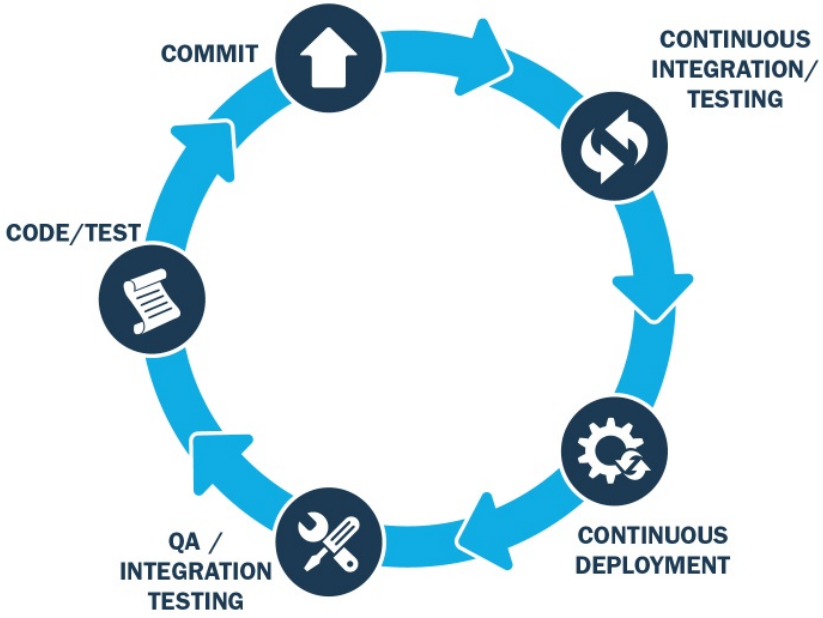


Polling Question

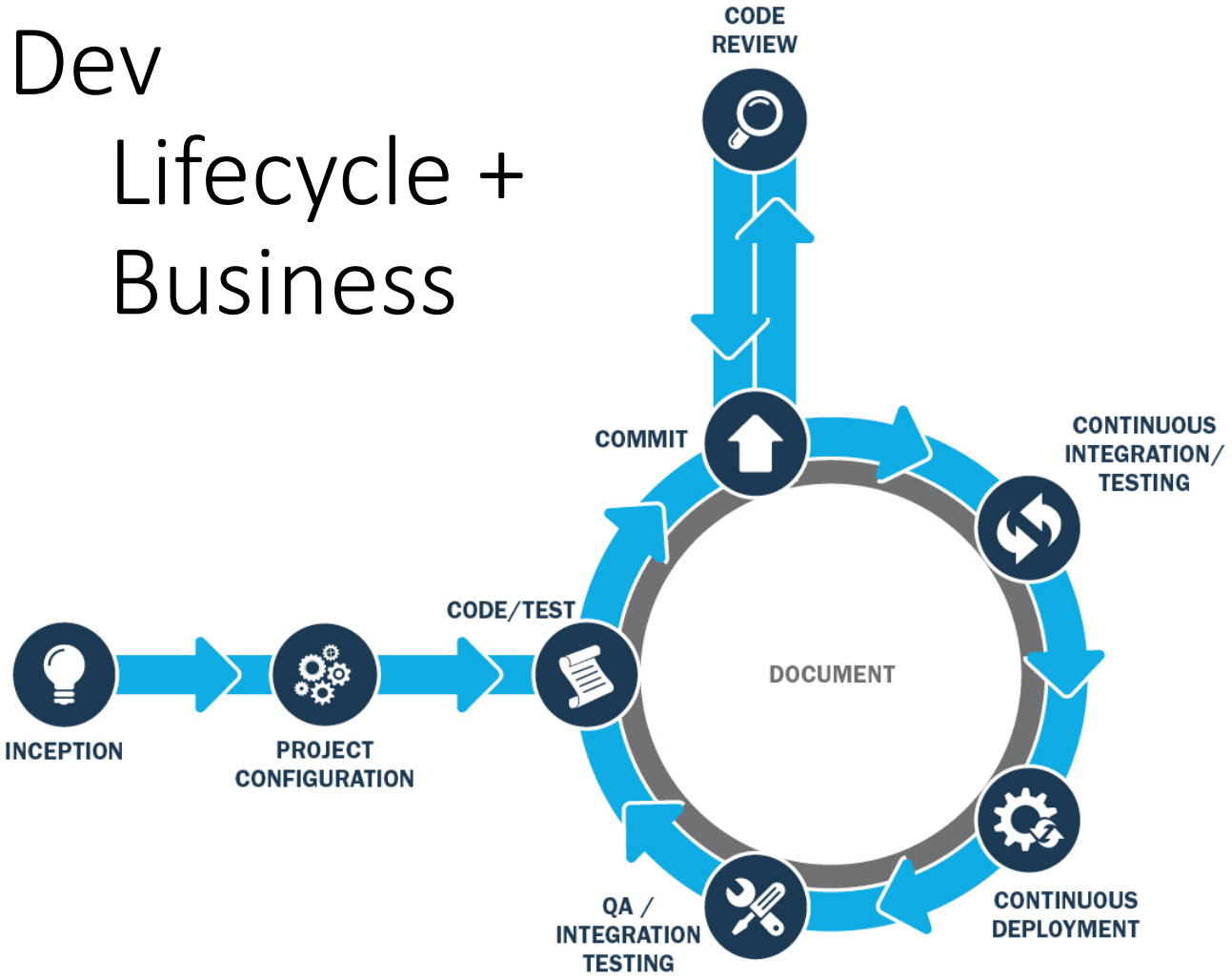
At what point do you consider security?

a. At the very beginning
b. Sometimes in the middle
c. Toward the end
d. Not at all

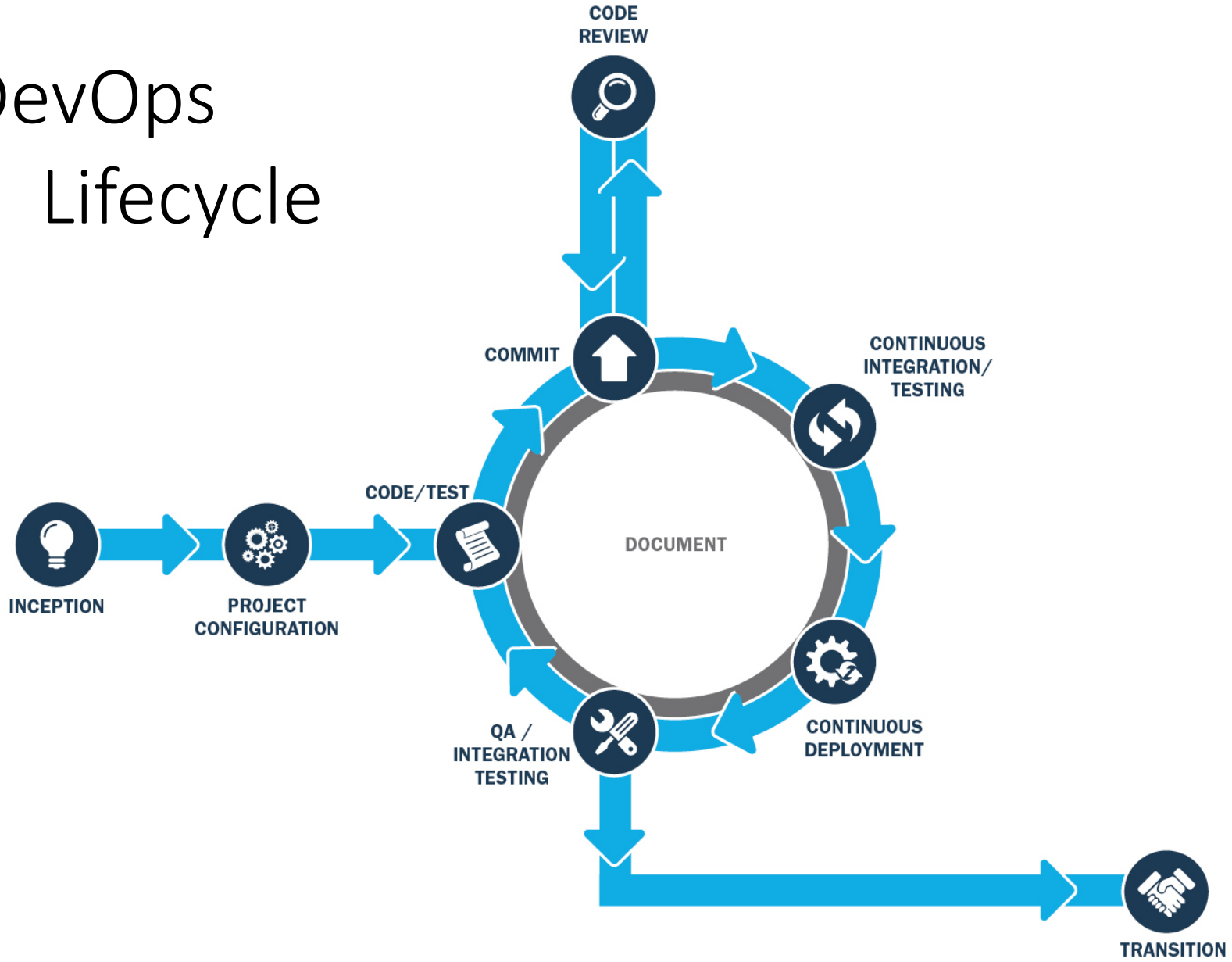
Dev Lifecycle



Dev Lifecycle + Business

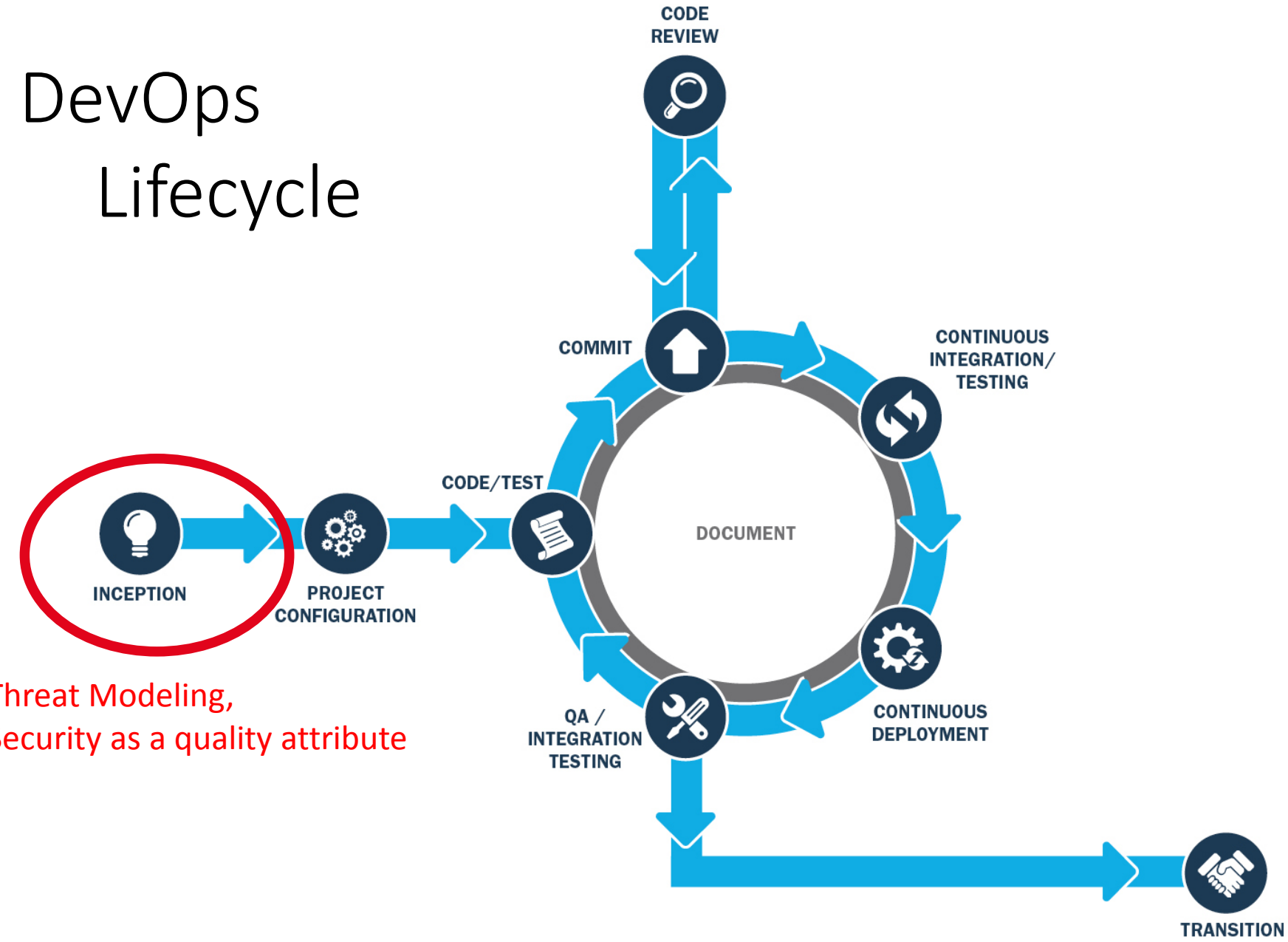


DevOps Lifecycle



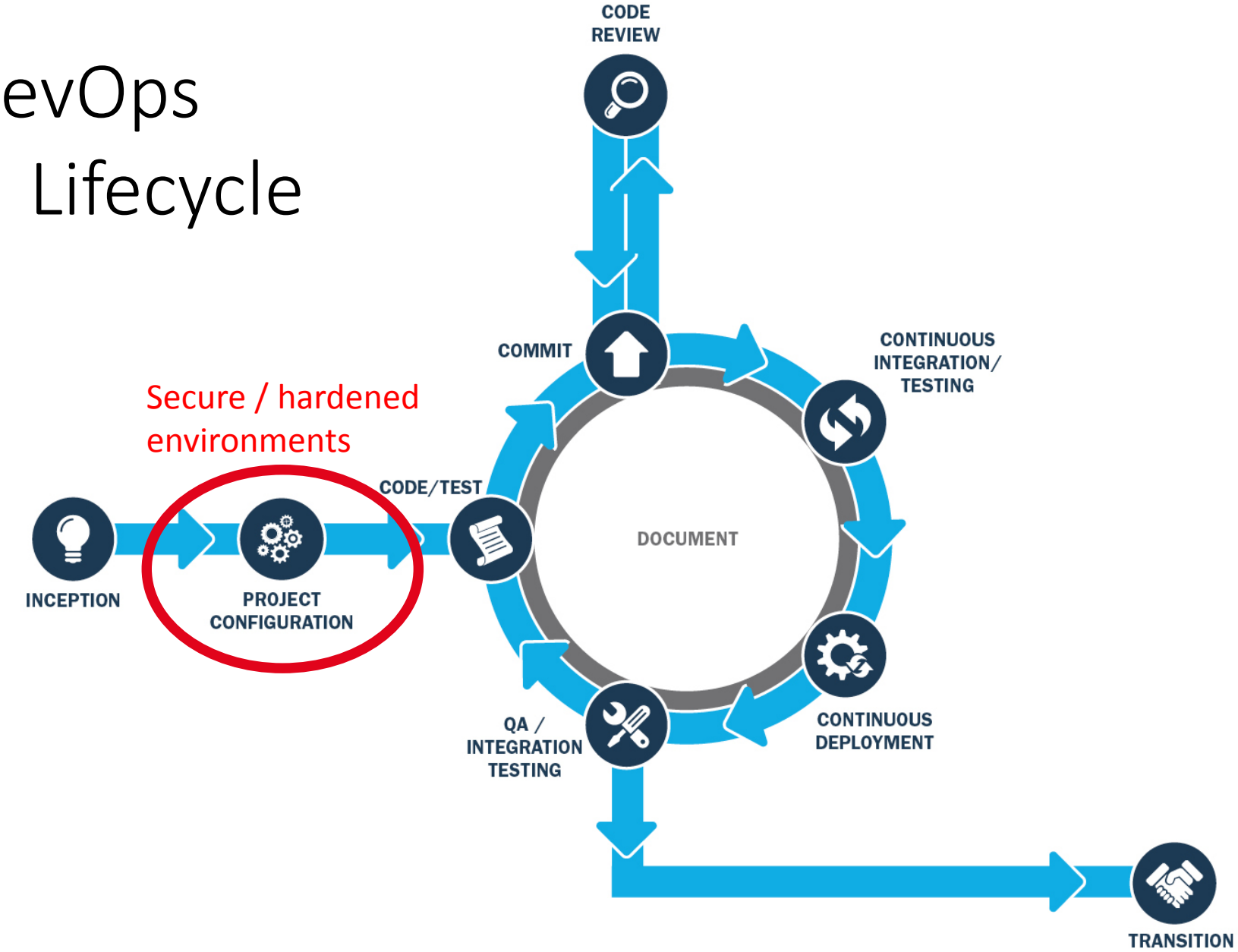
Where are opportunities for *security processes*?

DevOps Lifecycle



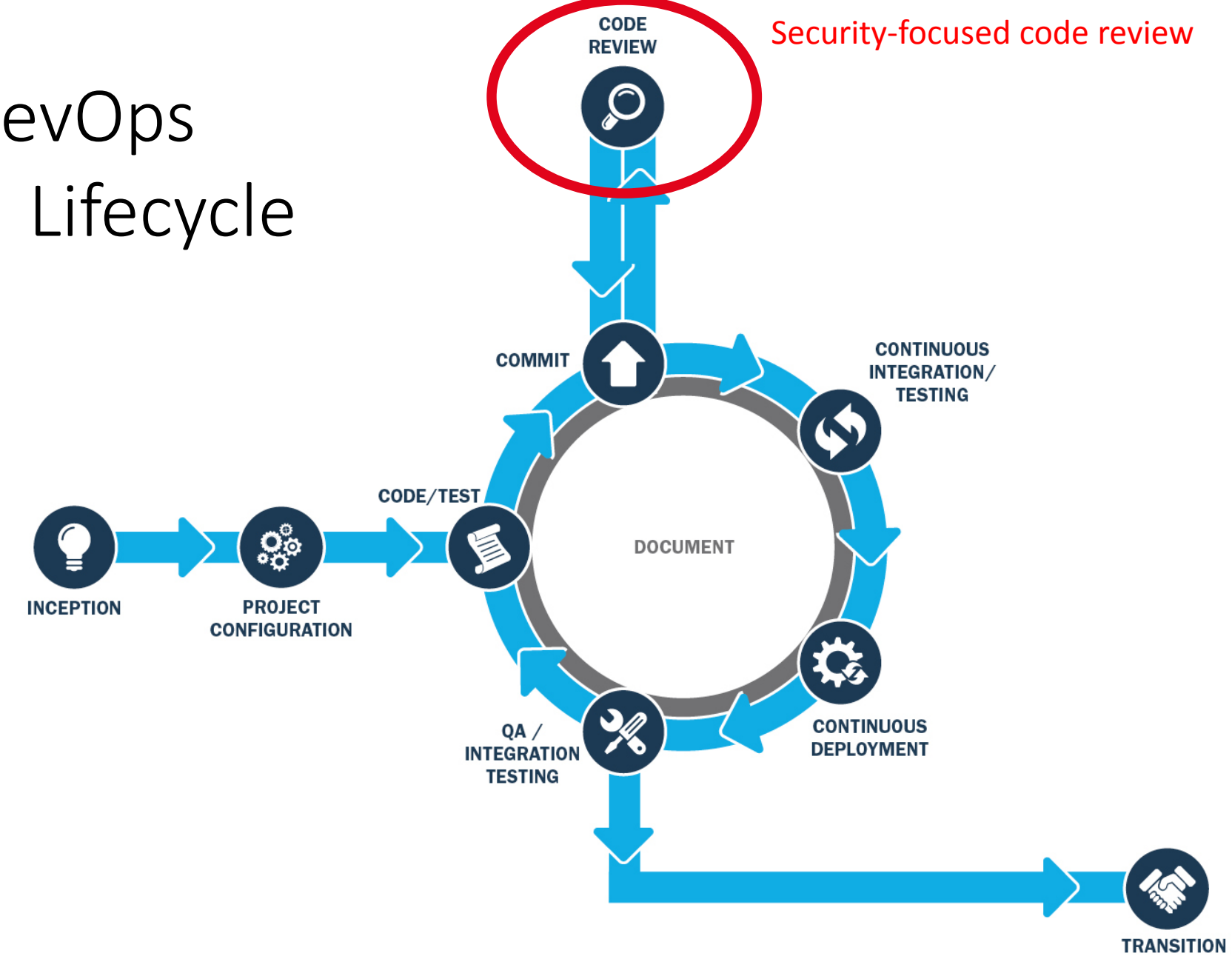
Threat Modeling,
Security as a quality attribute

DevOps Lifecycle

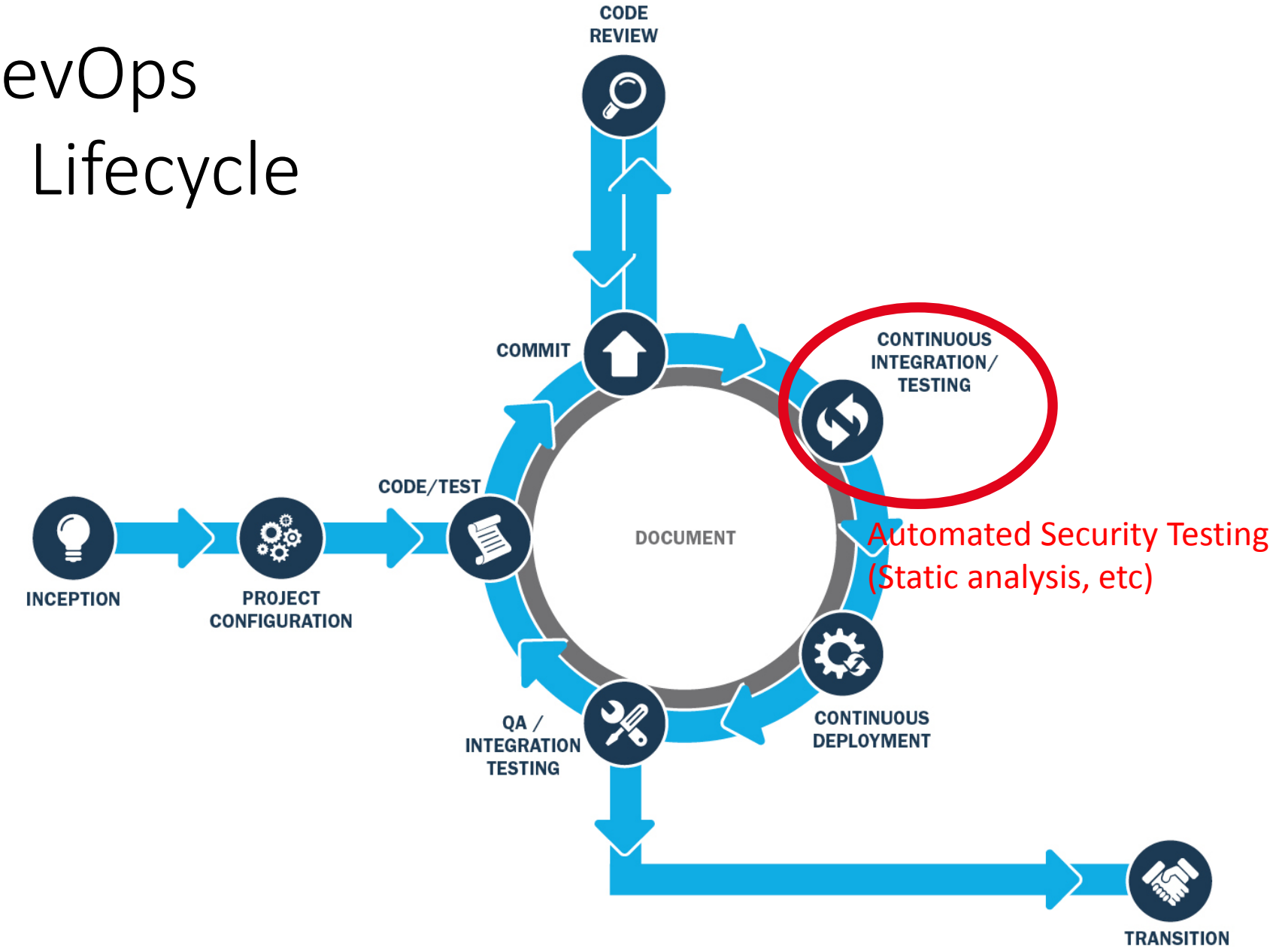


DevOps Lifecycle

Security-focused code review

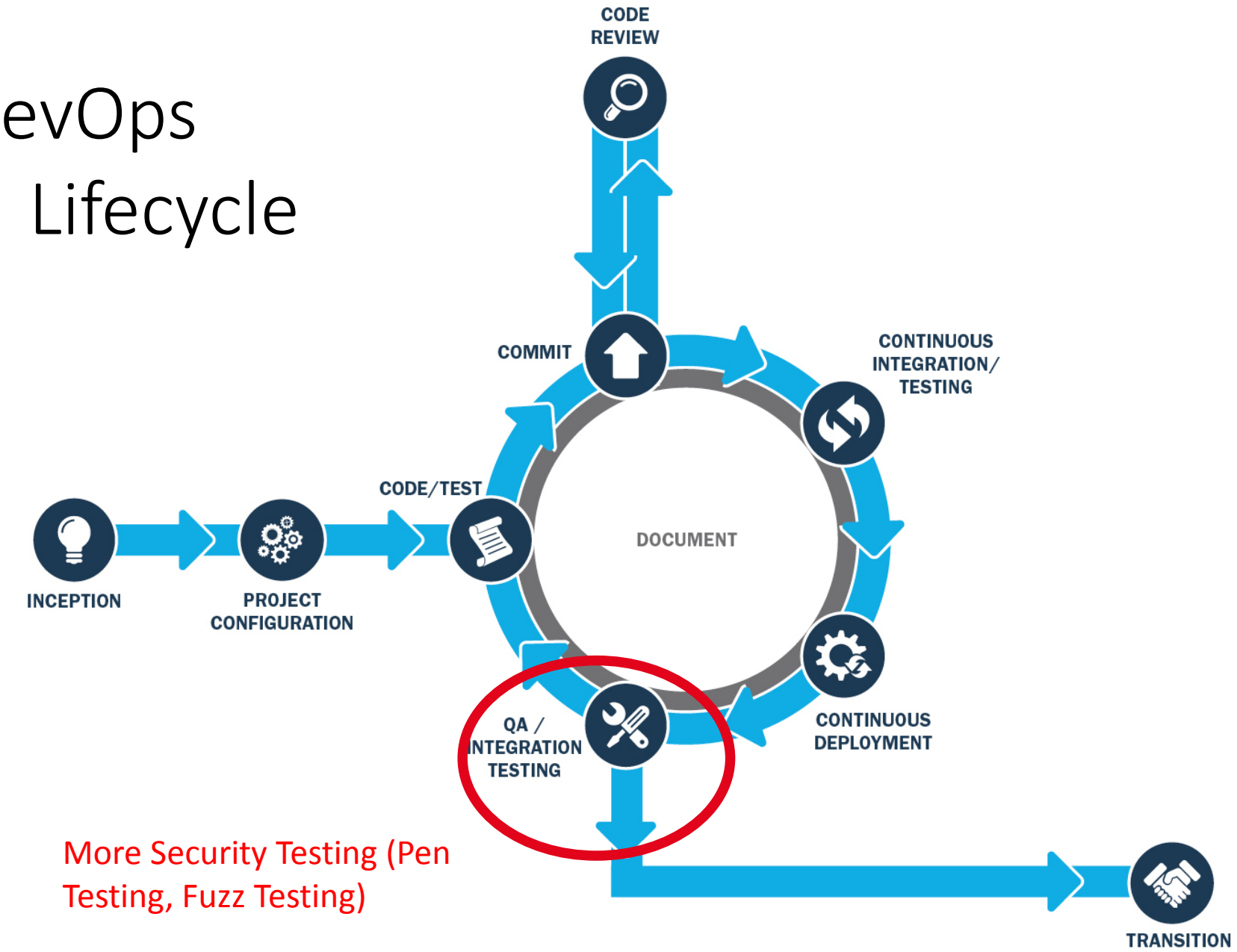


DevOps Lifecycle



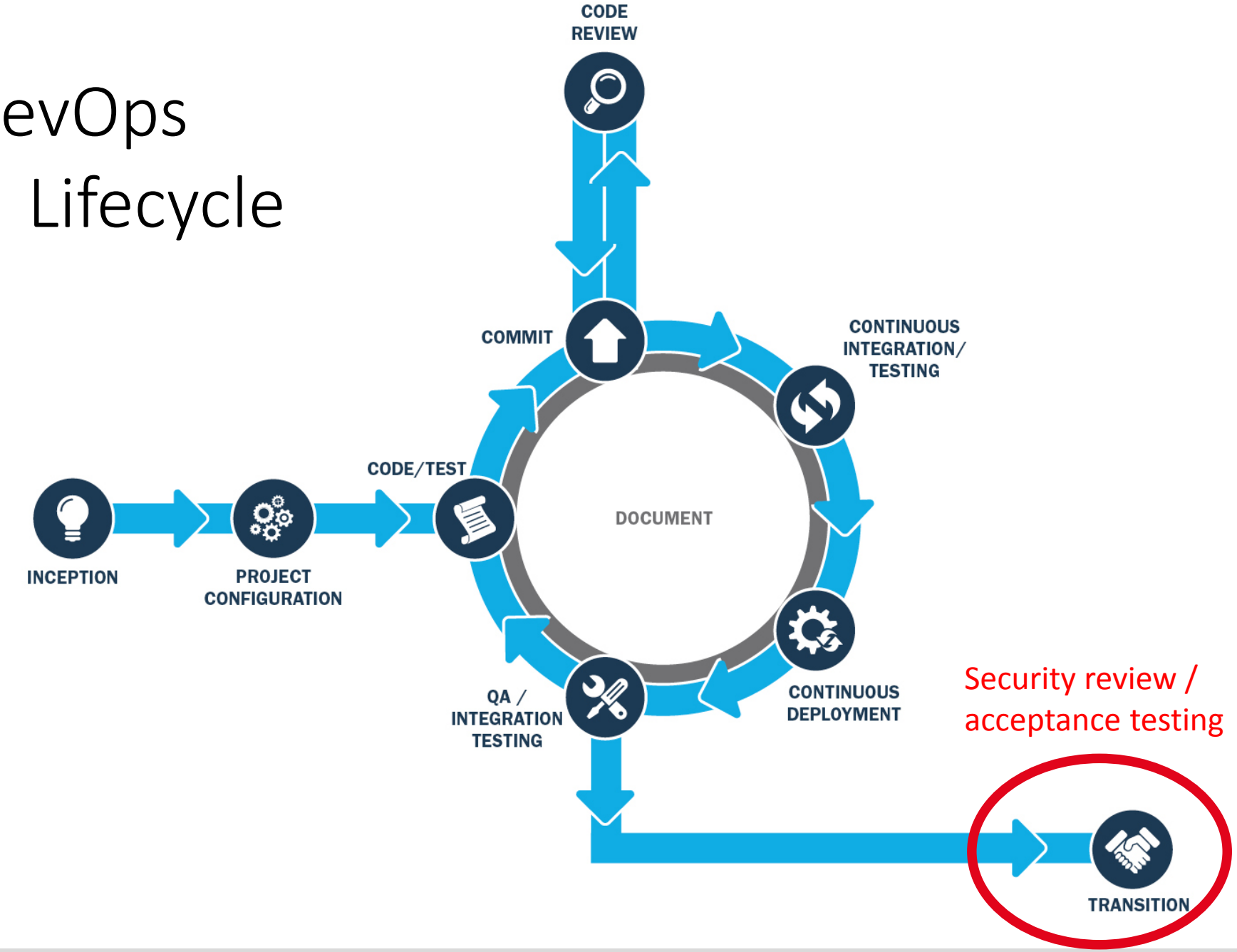
Automated Security Testing (Static analysis, etc)

DevOps Lifecycle

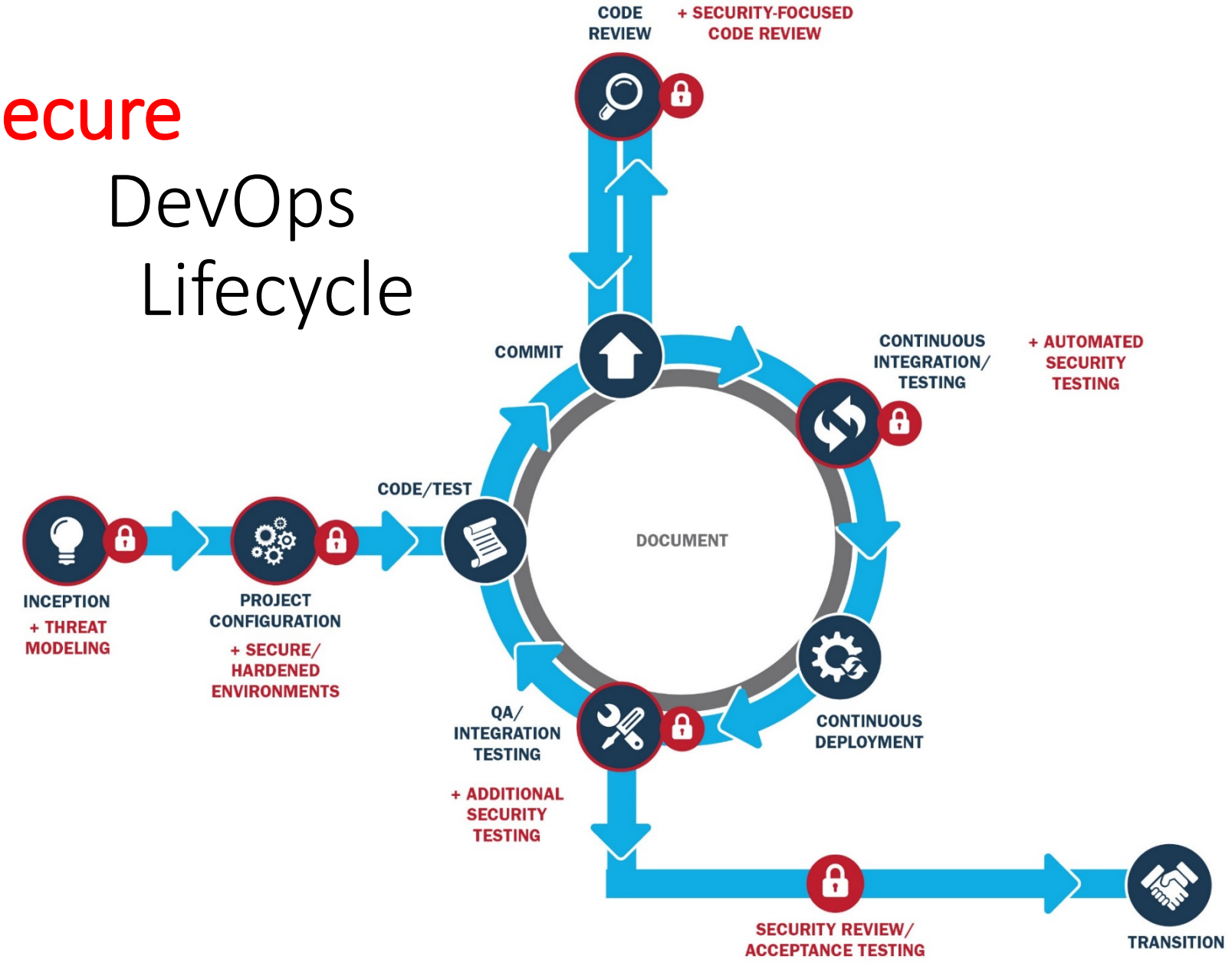


More Security Testing (Pen Testing, Fuzz Testing)

DevOps Lifecycle



Secure DevOps Lifecycle

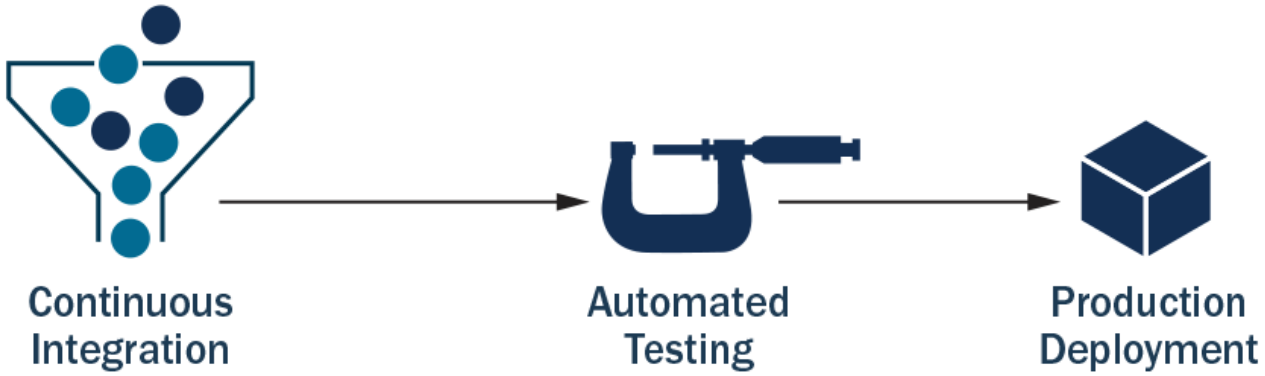


Security must be addressed without breaking the *rapid delivery*, *continuous feedback* model

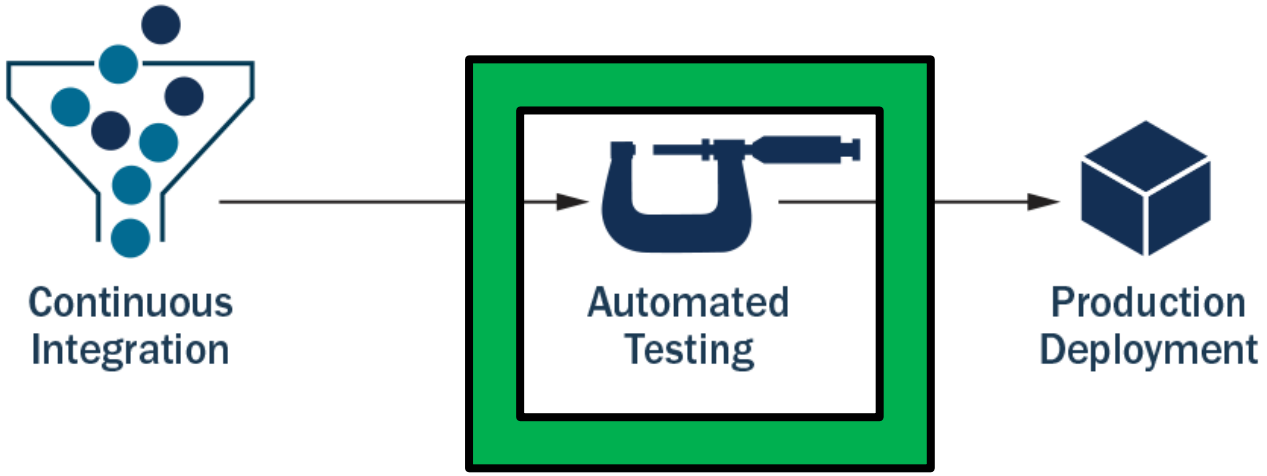
Secure DevOps

A typical scenario

Static Code Analysis

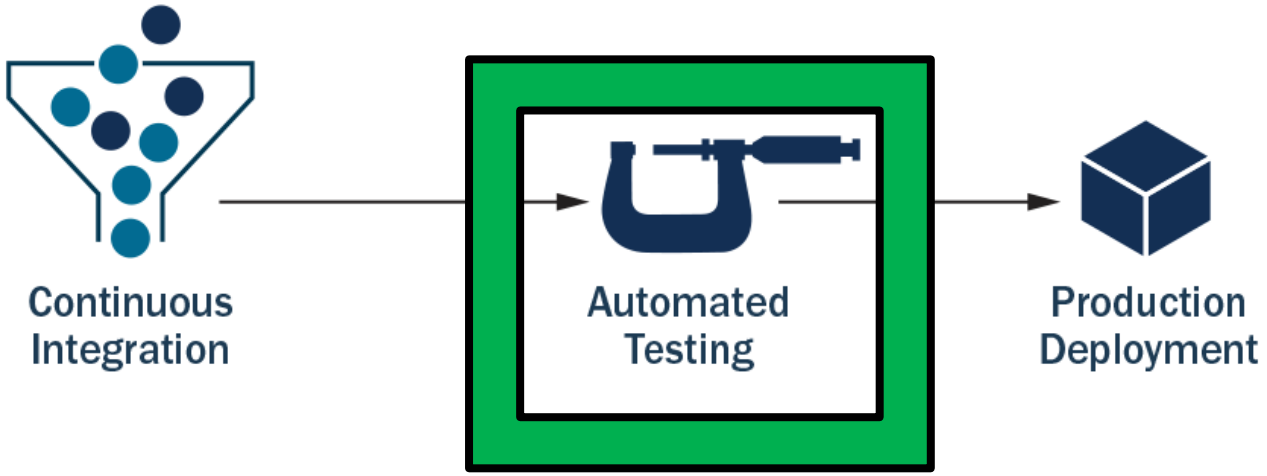


Static Code Analysis



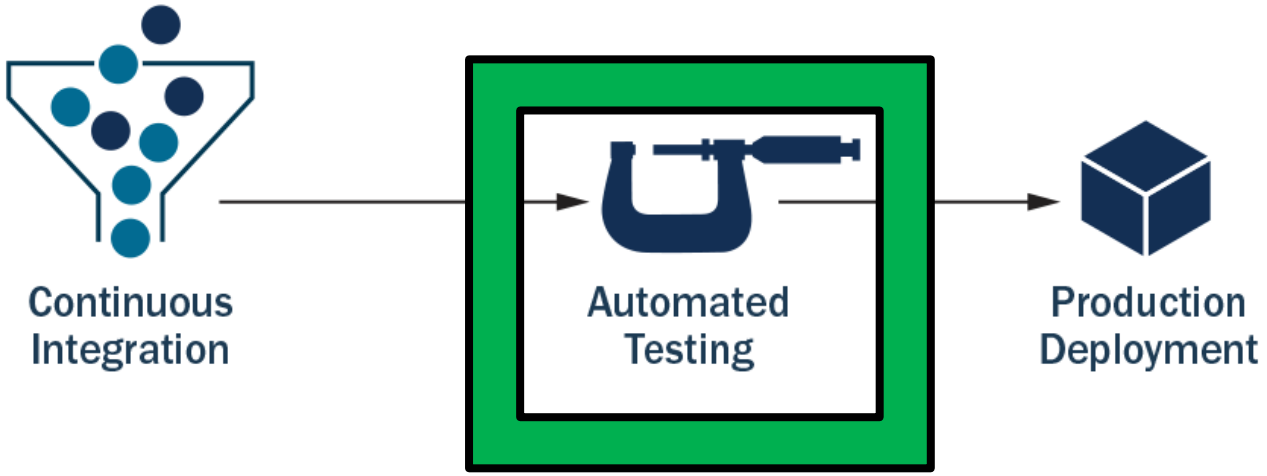
Tools Vary by Technology

Static Code Analysis



Regular Expressions

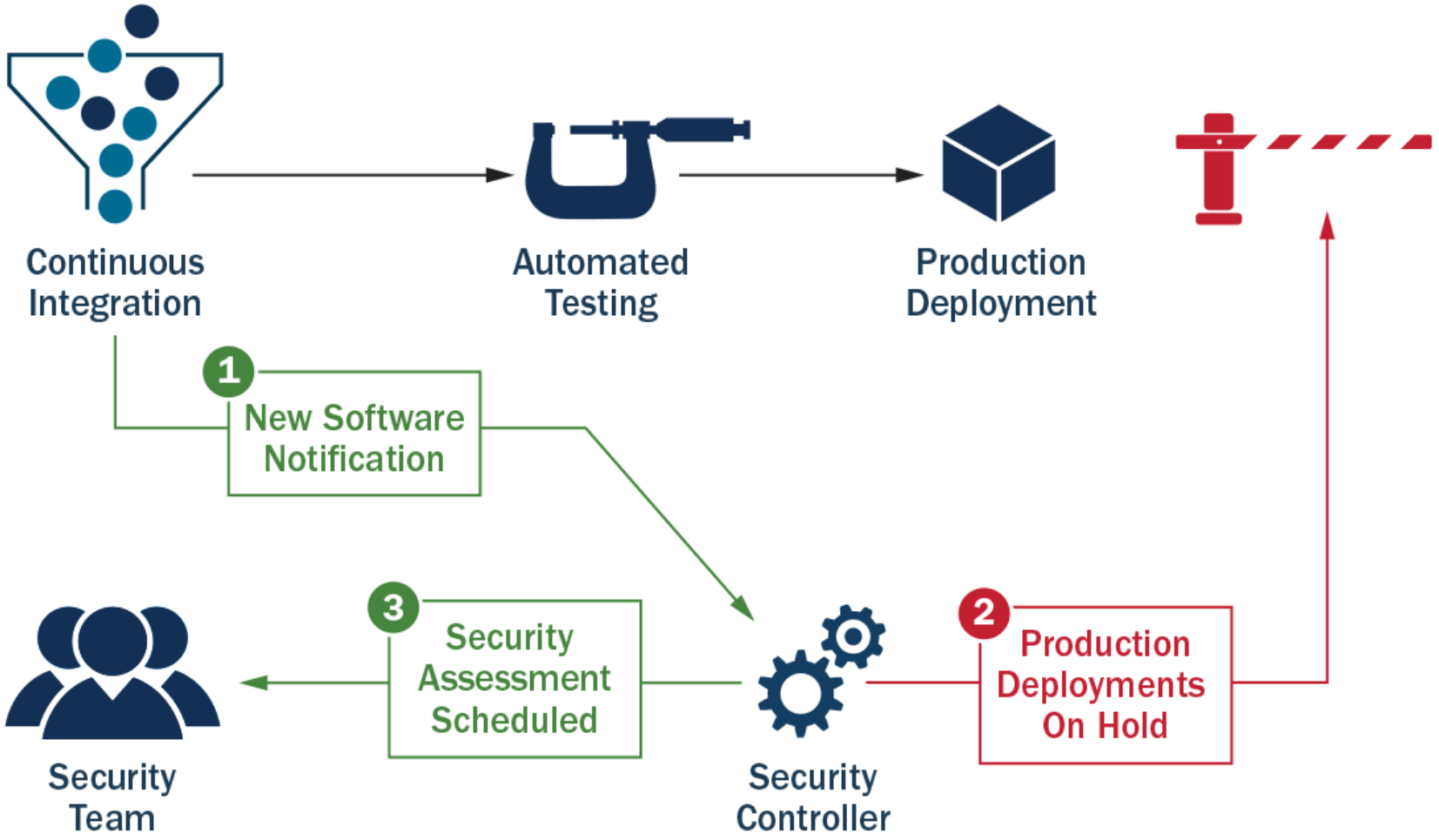
Static Code Analysis

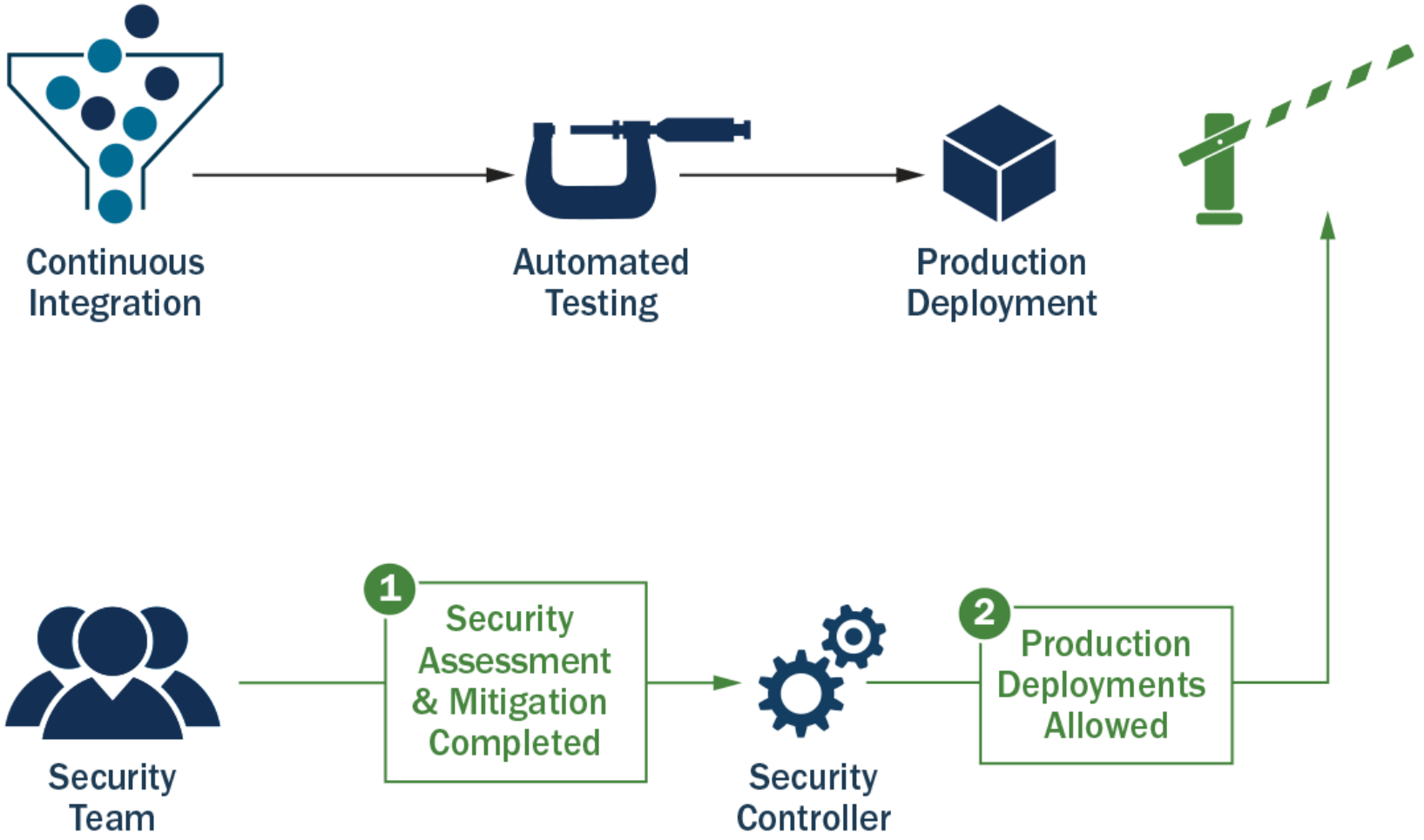


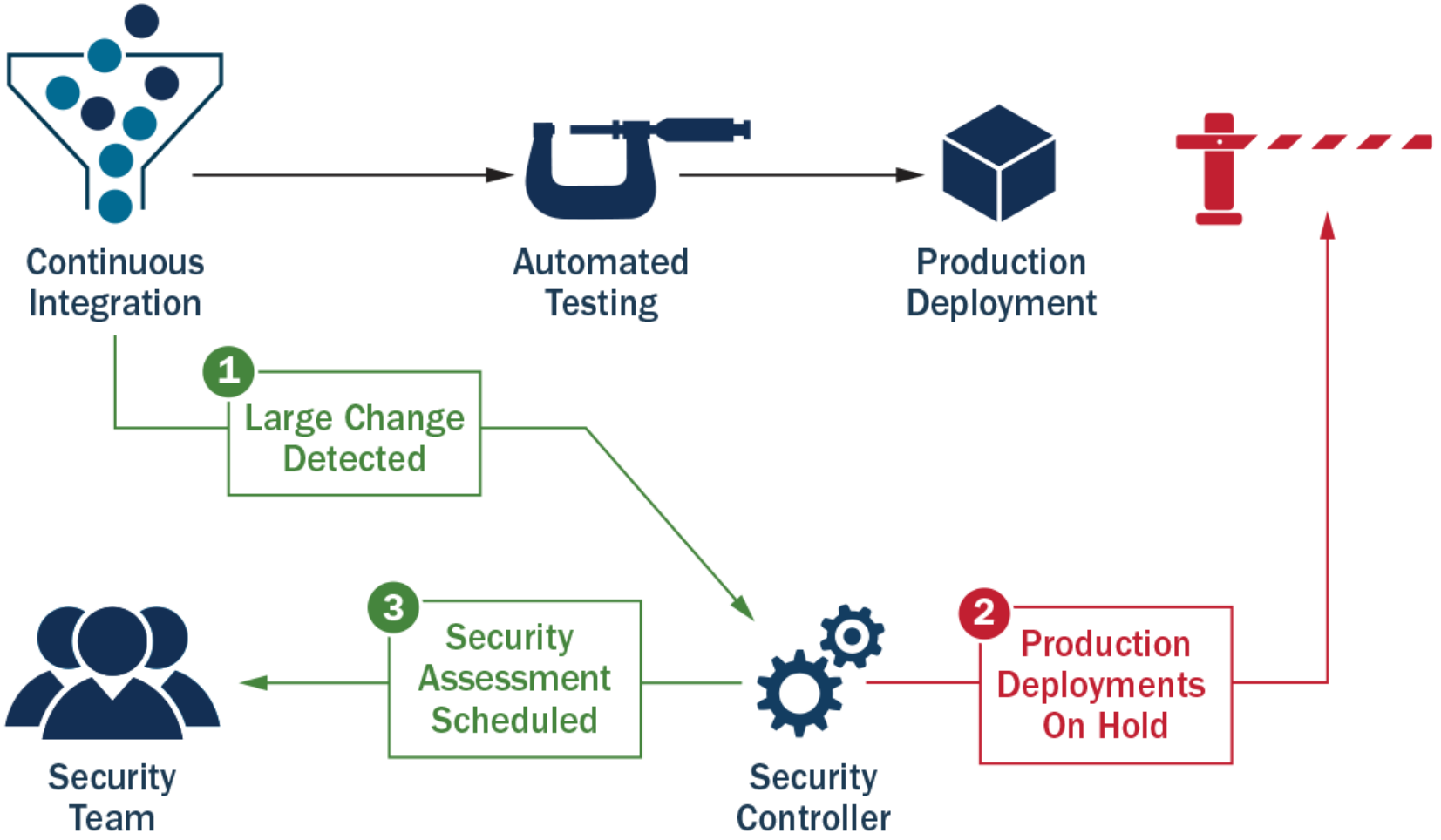
Wrappers

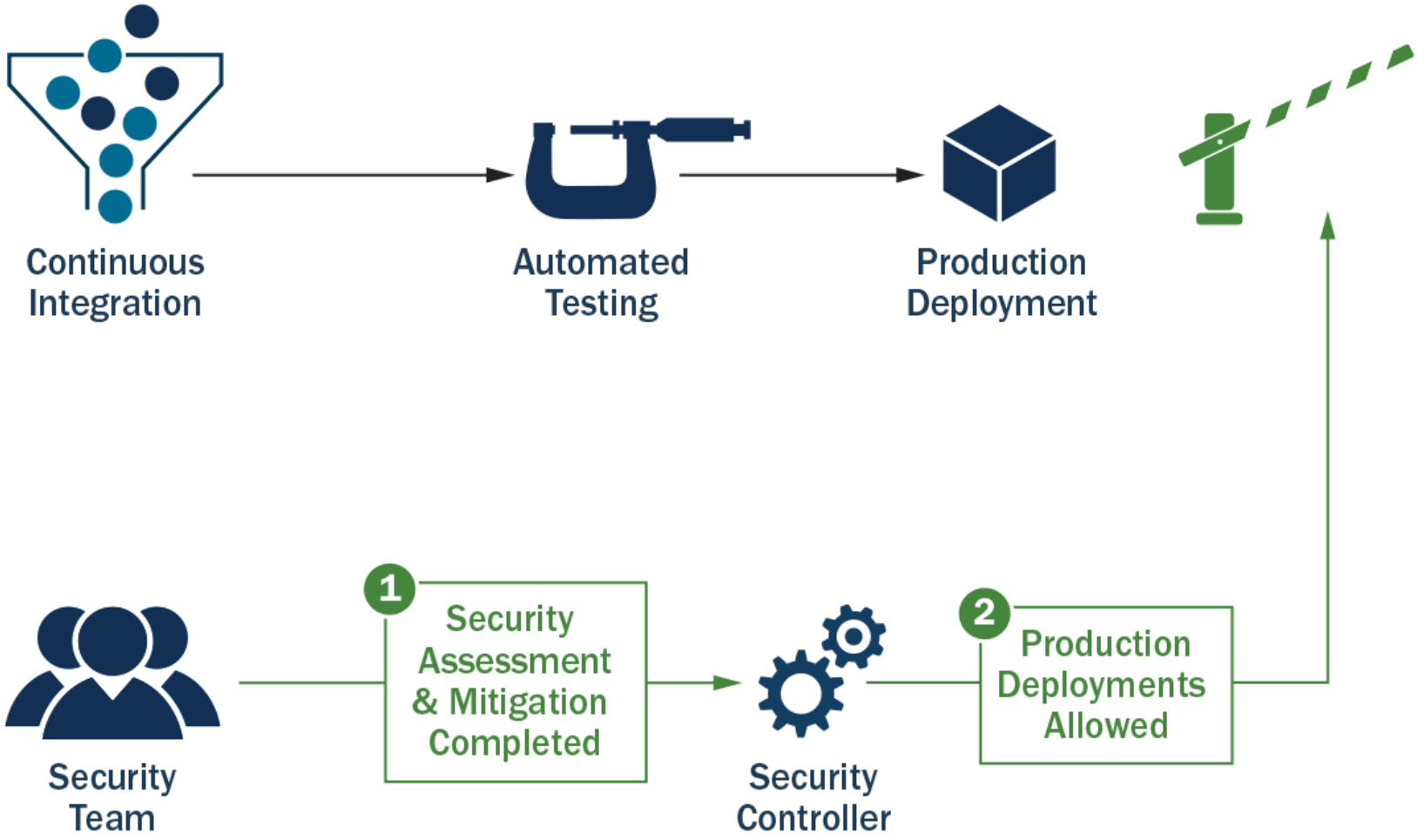
Manual Security Assessments

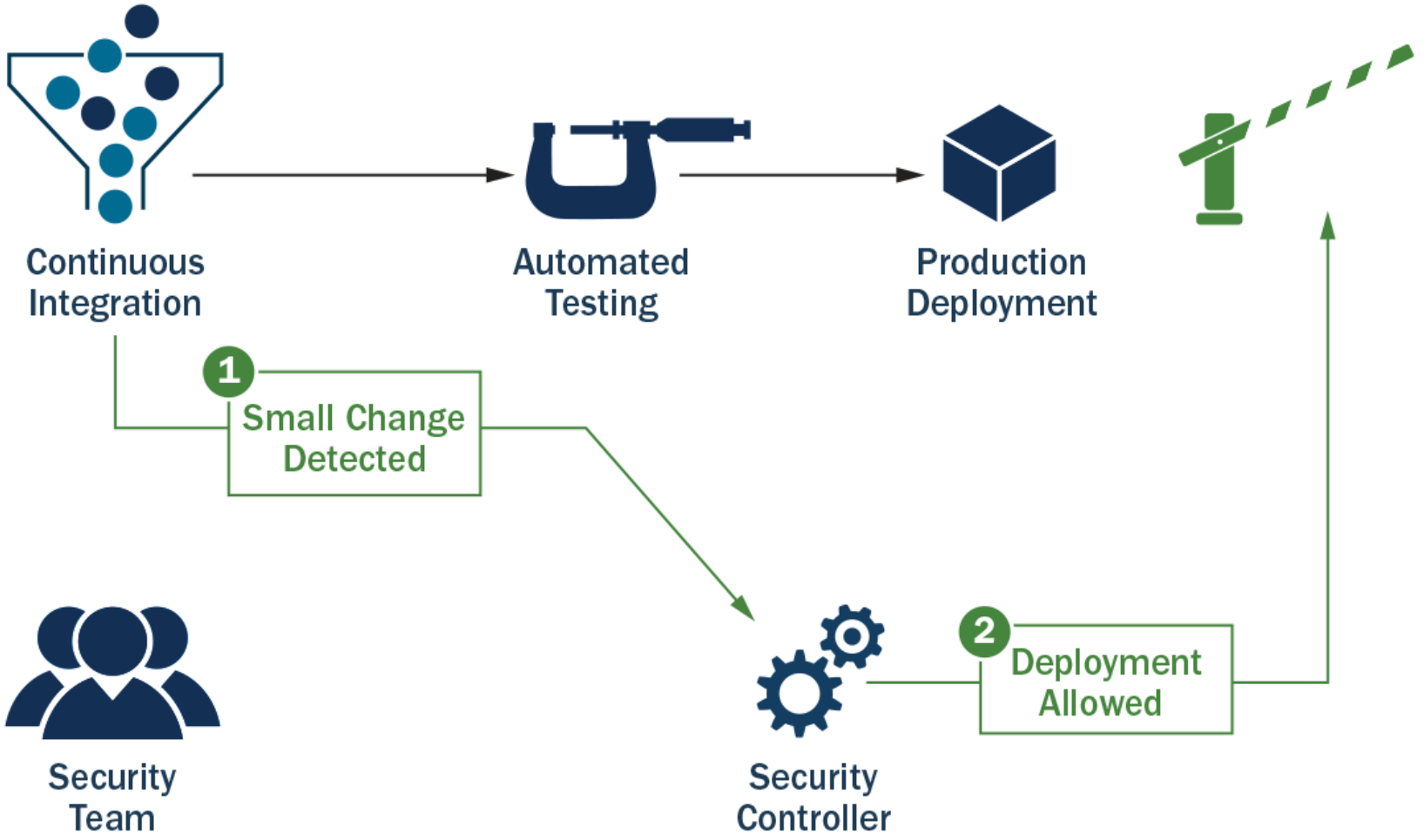
- Centralize information needed to conduct assessments
- Pick and choose your battles
- Integrate your tools as much as possible
- Capture outputs from tools in a central repository











More on SEI DevOps Blog

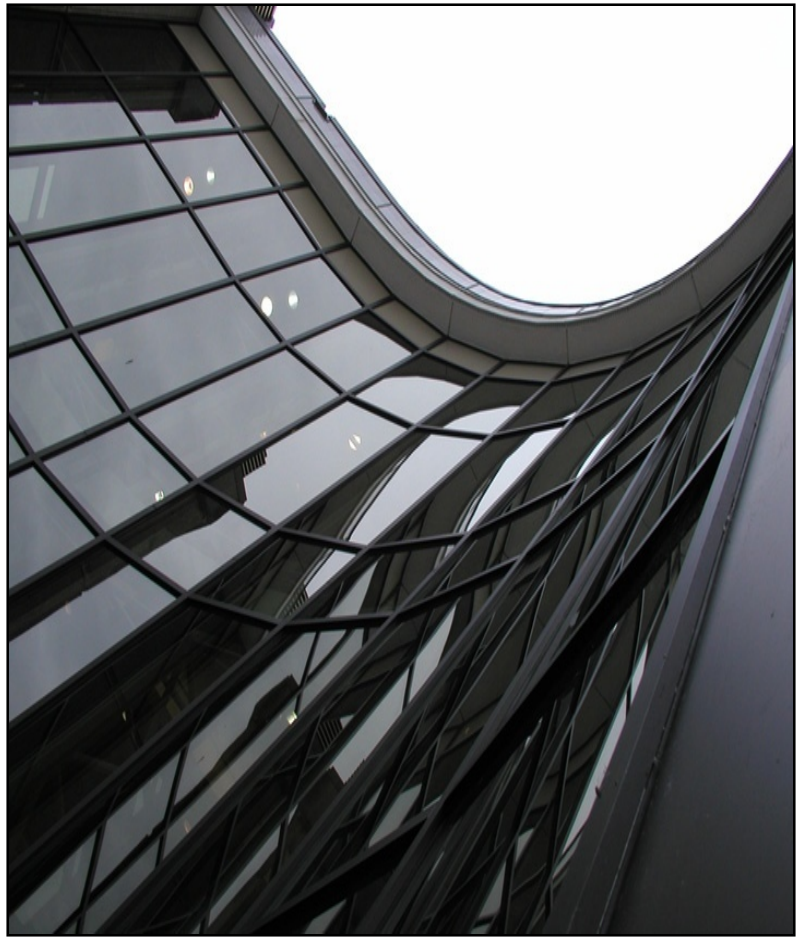
https://insights.sei.cmu.edu/devops

Contact Information

Hasan Yasar

hyasar@cmu.edu

https://www.linkedin.com/in/hasanyasar



Software Engineering Institute | Carnegie Mellon