DevOps is the key for Continuous Security: RMF, ATO and beyond

Hasan Yasar

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1001

DevOps is the key for Continuous Security: RMF, ATO and beyond

DevOps

DevOps and How it started

DevOps is a set of principles and practices emphasizing collaboration and communication between software development teams and IT operations staff along with acquirers, suppliers and other stakeholders in the life cycle of a software system [1]

- Patrick Debois “Agile infrastructure and operations: how infra-gile are you?”, Agile 2008 Conference
- John Allspaw “ 10+Deploys per Day: Dev and Ops Cooperation”, Velocity 2009
- DevOpsDays, October 30th 2009, #DevOps term born

[1] IEEE P2675 DevOps Standard for Building Reliable and Secure Systems Including Application Build, Package and Deployment

DevOps has four Fundamental Principles

- **Collaboration:** between all stakeholders in the project team

- **Infrastructure as Code(IaC):** all assets are versioned, scripted, and shared where possible

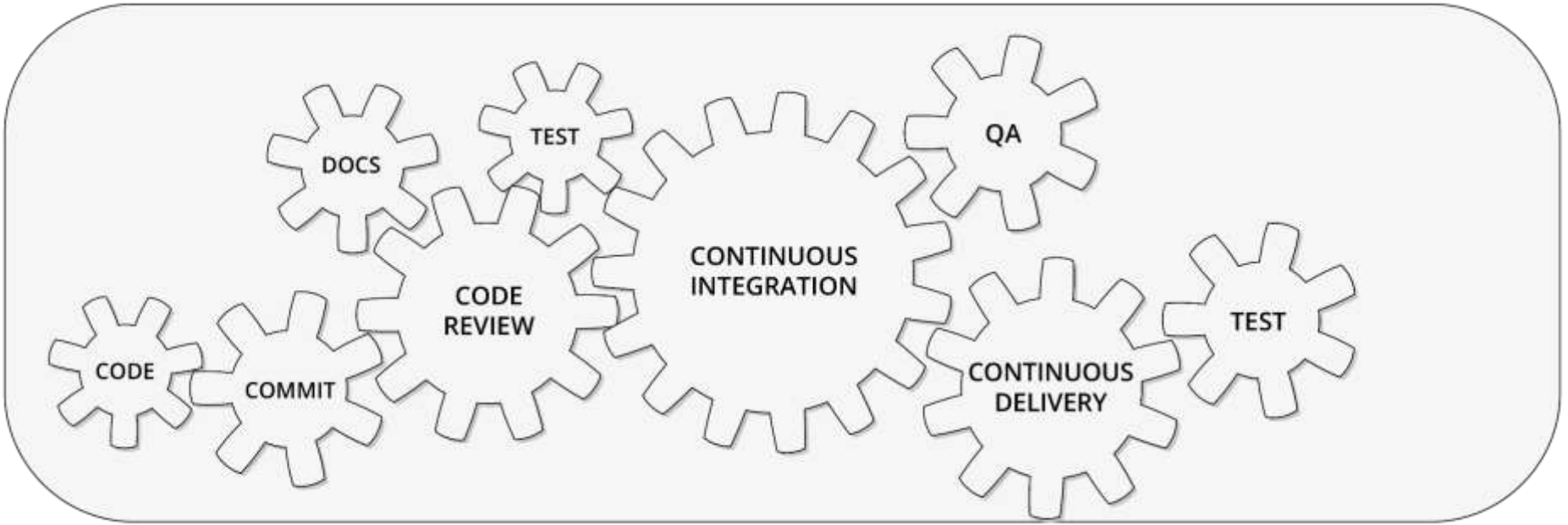
- **Automation:** deployment, testing, provisioning, any manual or human-error-prone process

- **Monitoring:** any metric in the development or operational spaces that can inform priorities, direction, and policy

Key Benefits of DevOps

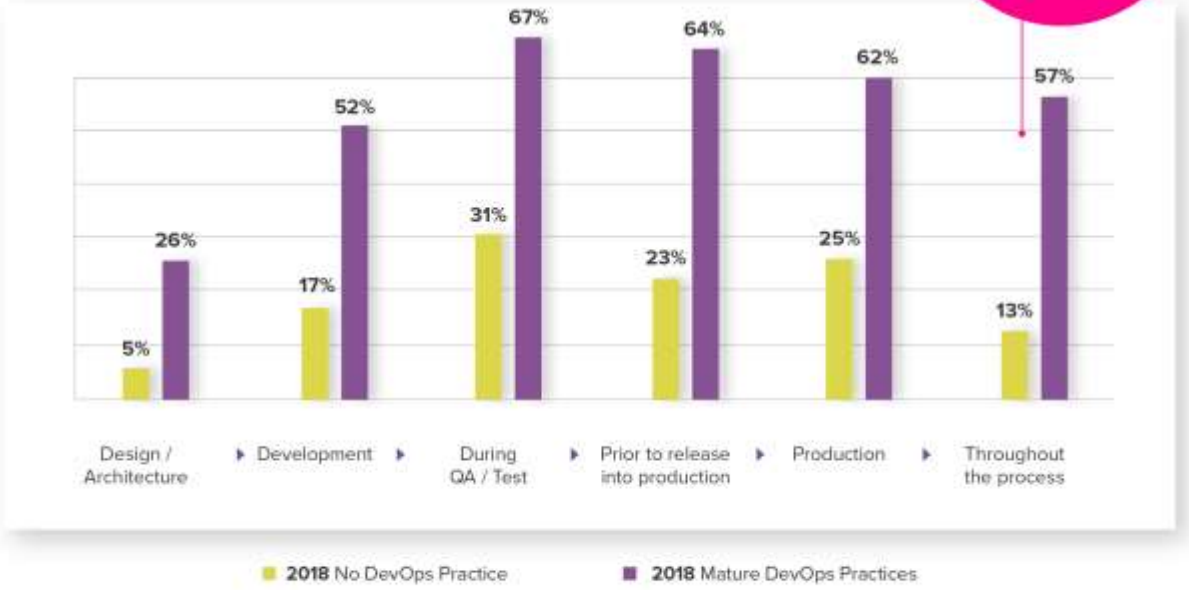
- Reduce ***errors*** during ***deployment***
- Reduce time to ***deploy*** and ***resolve*** discovered errors
- ***Repeatable*** of each steps
- ***Continuous availability*** of pipeline and application
- Increase ***Innovation*** time
- Responsiveness to ***business needs***
- Constant ***communication*** and ***collaboration*** platform
- ***Traceability*** and ***visibility*** throughout application lifecycle
- Increase software ***stability*** and ***quality***
- Ability of ***continuous feedback***

Security requires Automation with IaC, CI, CD



At what point in the development process does your organization perform automated application security analysis?

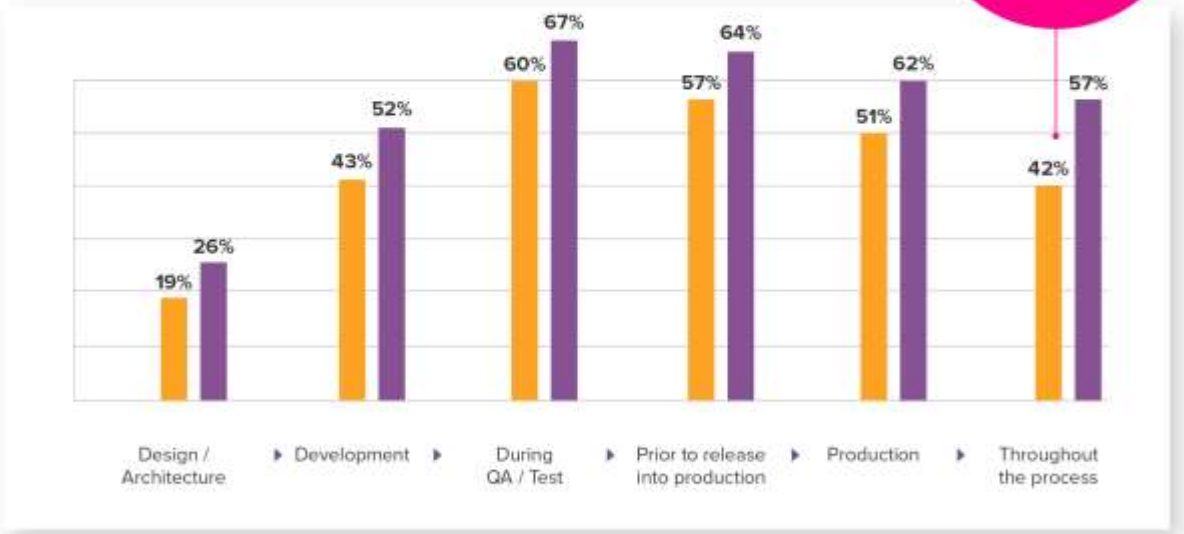
Mature DevOps practices are 338% more likely to integrate automated security.



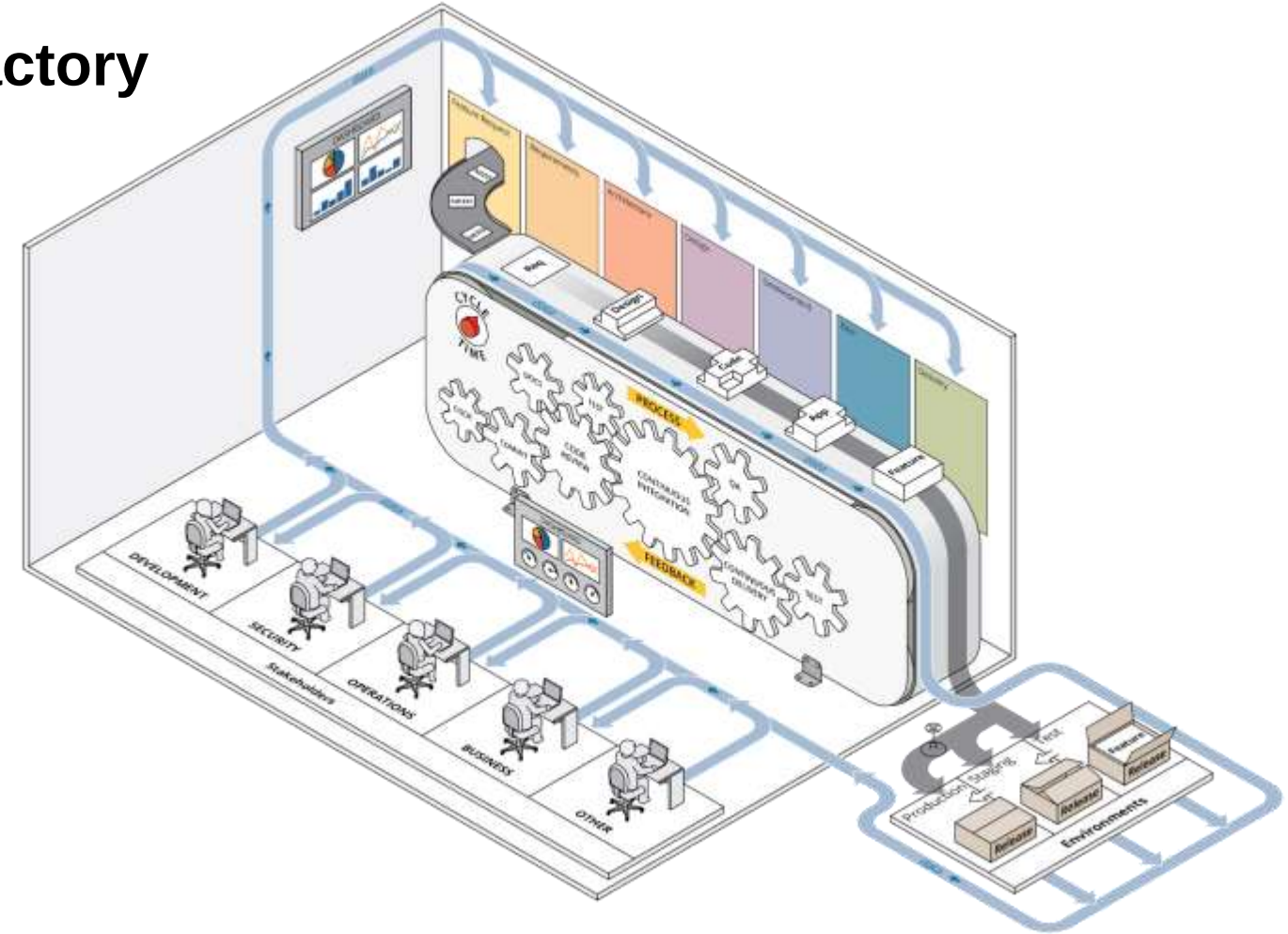
DevSecOps Community Survey 2018 7

At what point in the development process does your organization perform automated application security analysis?

Mature DevOps practices ramped their investment in automated security by 15%.



The DevOps Factory



DevOps is the key for Continuous Security: RMF, ATO and beyond

RMF, ATO &Compliances requirements

What is Risk Management Framework (RMF)?

- Information security framework for the entire federal government that replaces legacy Certification and Accreditation (C&A) Processes applied to information systems
- RMF is a key component of an organization’s information security program used in the overall management of organizational risk
- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", transforms the traditional Certification and Accreditation(C&A) process into the six-step Risk Management Framework (RMF).
- The Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle

1. *Categorize* the information system and the ***information processed, stored, and transmitted*** by that system based on an impact analysis

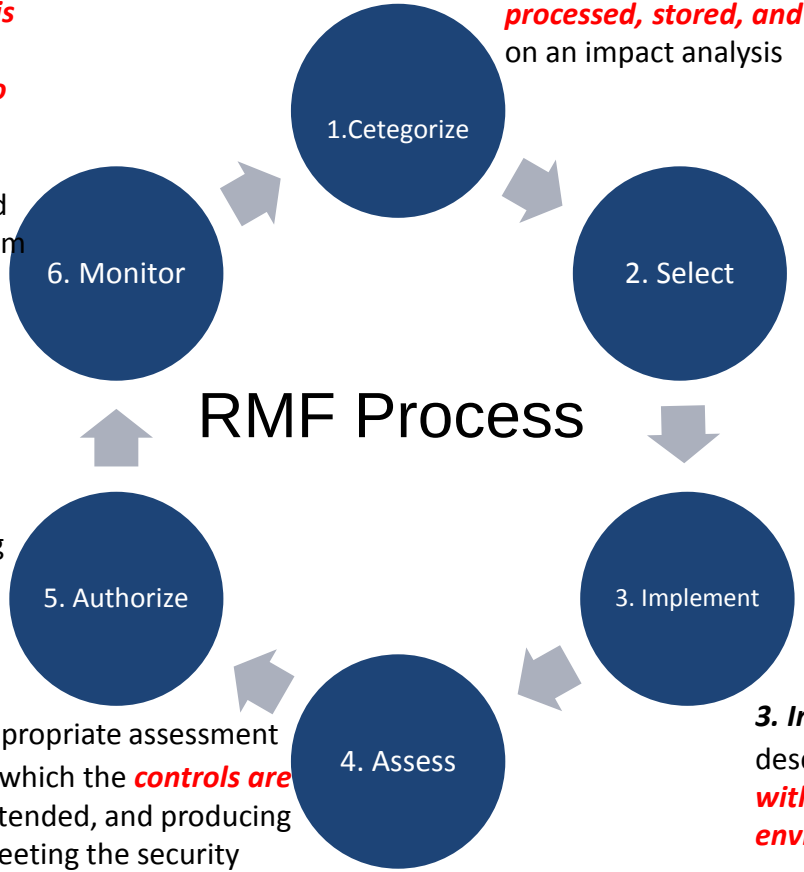
2. *Select* an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an ***organizational assessment of risk and local conditions***.

3. *Implement* the security controls and describe how ***the controls are employed within the information system and its environment of operation***.

4. *Assess* the security controls using appropriate assessment procedures to determine the extent to which the ***controls are implemented correctly***, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system

5. *Authorize* information system operation based on a ***determination*** of ***the risk to organizational operations and assets, individuals, other organizations***, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

6. *Monitor* the security controls in the information system on an ***ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation***, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.



RMF characteristics – NIST 800-37

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust ***continuous monitoring processes***;
- Encourages the use of ***automation*** to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security into the enterprise architecture and ***system development life cycle***;
- Provides emphasis on the selection, implementation, assessment, and ***monitoring*** of security controls, and the authorization of information systems;
- Links risk management processes at ***the information system level*** to risk management processes at the ***organization level*** through a risk executive (function); and
- Establishes ***responsibility*** and ***accountability*** for security controls deployed within organizational information systems and inherited by those systems

Next , Authorization to Operate(ATO)

A typical security controls are about **924** for a selected systems and all are in Excel format;

Control Number	Family	Control Title	Control Text	Confidentiality	Integrity	Availability	Supplemental Guidance
		TOOLS					
SI-4 (10)	SI	INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS	The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information system monitoring tools].	High Moderate	High Moderate	High Moderate	Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and for having insight into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for others, mission-assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.
SI-4 (11)	SI	INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to discover anomalies.	High Moderate Low	High Moderate Low	High Moderate Low	Supplemental Guidance: Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.
SI-4 (12)	SI	INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined activities that trigger alerts].	High Moderate Low	High Moderate Low	High Moderate Low	Supplemental Guidance: This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by information systems in SI-4 (5), which tend to focus on information sources internal to the systems (e.g., audit records), the sources of information for this enhancement can include other entities as well (e.g., suspicious activity reports, reports on potential insider threats). Related controls: AC-18, IA-3.
SI-4 (13)	SI	INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS	The organization: (a) Analyzes communications traffic/event patterns for the information system; (b) Develops profiles representing common traffic patterns and/or events; and (c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.				

Compliance, Legal Requirements

- There are many compliances and legal requirements
  - **GDPR**: General Data Protection Regulation
  - **FISMA** :Federal Information Security Management
  - **SOX** : Sarbanes–Oxley
  - **HIPAA** : Health Insurance Portability and Accountability
  - **PCI DSS**: Payment Card Industry Data Security Standard
  - **NIST** :National Institute of Standards and Technology,
  - And many more..
- All requires
  - Reporting,
  - Auditing
  - Traceability
- Volkswagen emission case: SW Engineer 40 months in prison, VW $20Billion in fines

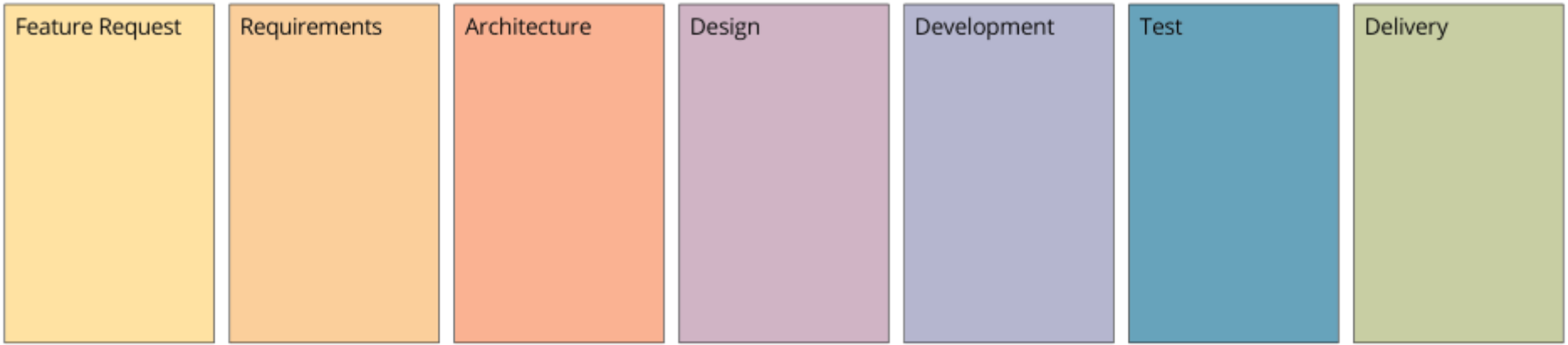
https://www.nytimes.com/2017/08/25/business/volkswagen-engineer-prison-diesel-cheating.html

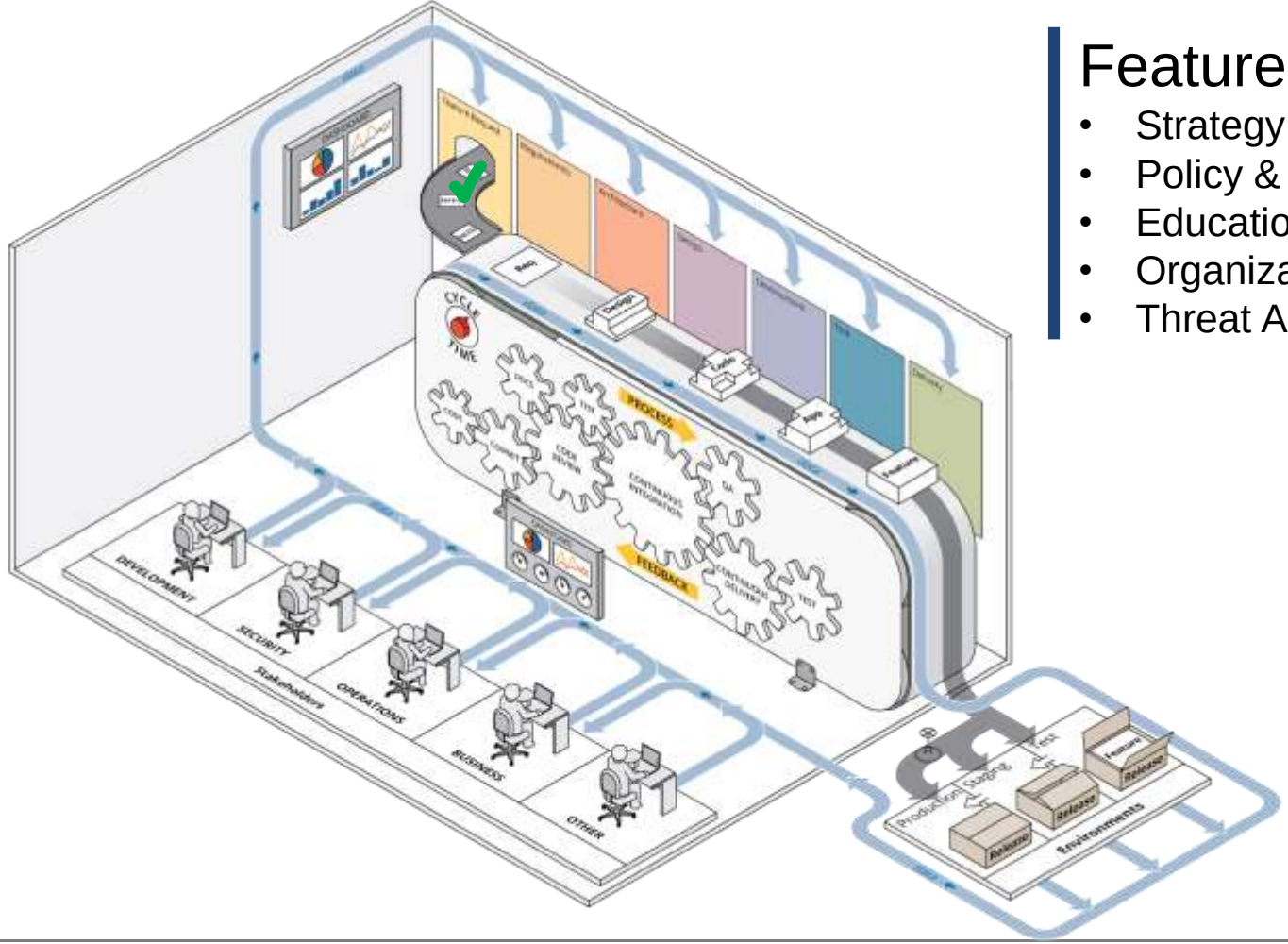
DevOps is the key for Continuous Security: RMF, ATO and beyond

With Secure DevOps

Secure DevOps is a model on integrating the software development and operational process considering security activities: requirements, design, coding, testing ….

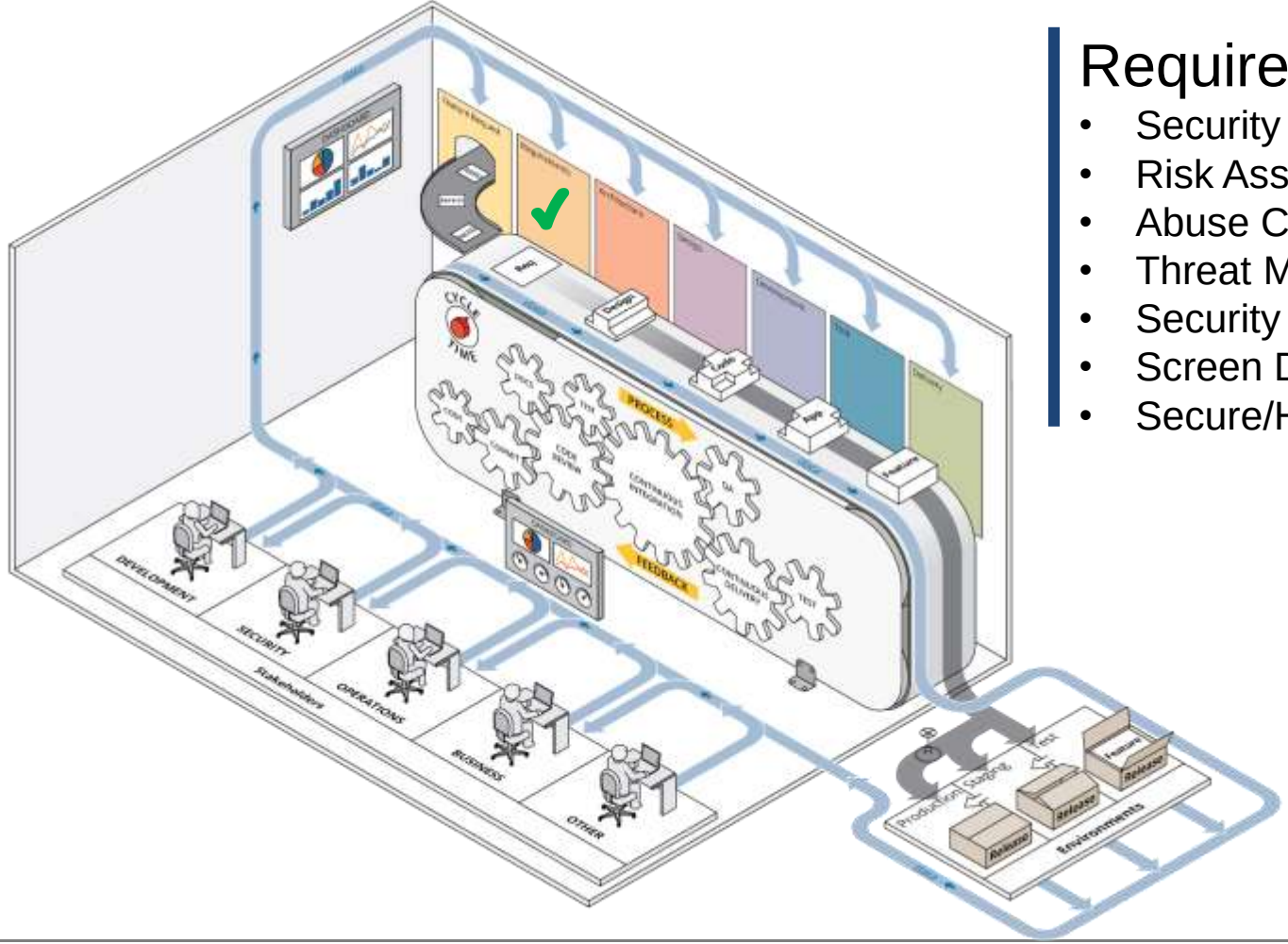
DevOps Phases – *on each iteration/sprint*





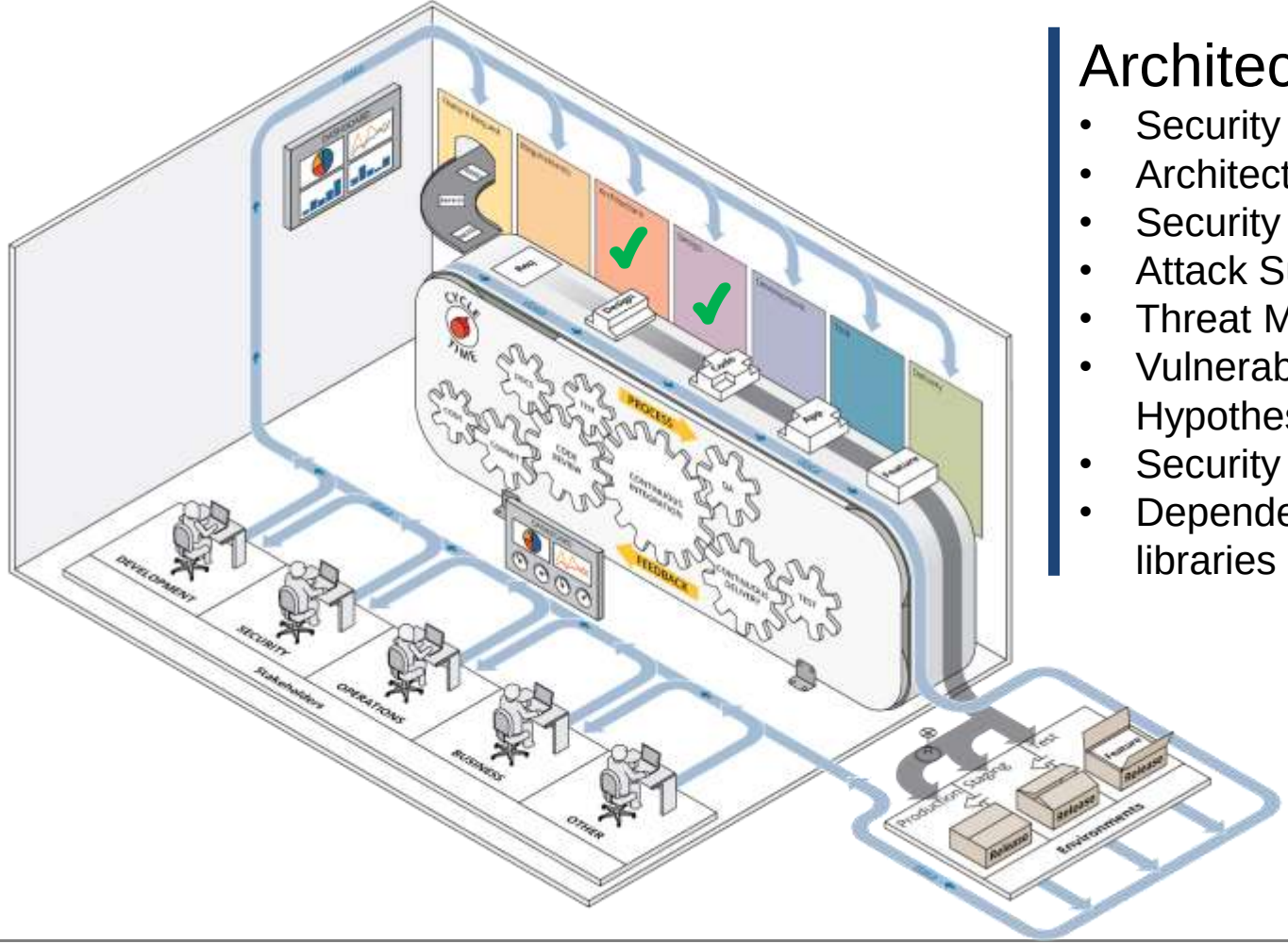
Feature Request

- Strategy & Metrics
- Policy & Governance
- Education & Security Guidance
- Organizational Risk Factors
- Threat Assessment



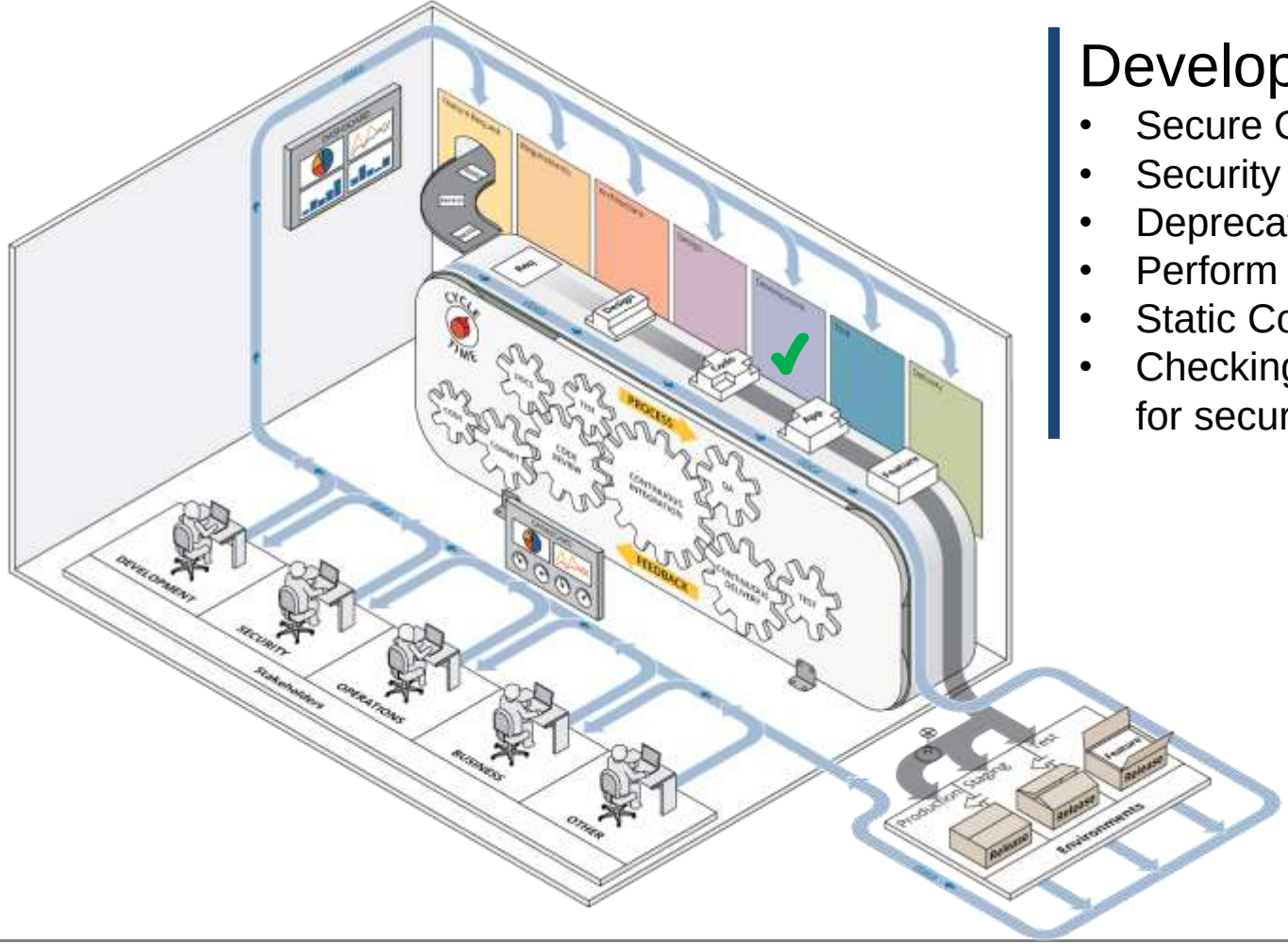
Requirements

- Security Requirements (SFR/SAR)
- Risk Assessment
- Abuse Case Development
- Threat Modelling
- Security Stories
- Screen Development Tools
- Secure/Hardened Environments



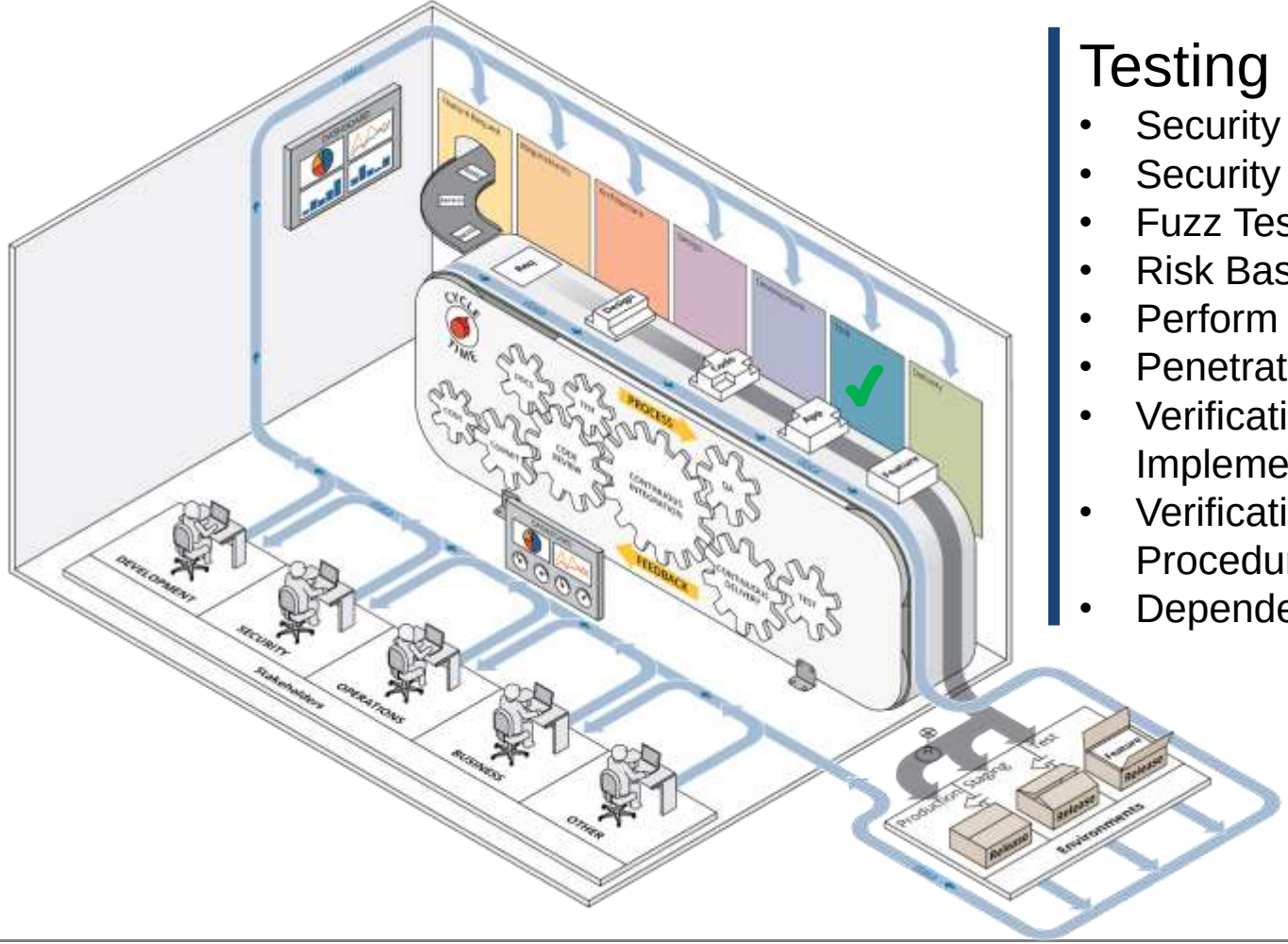
Architecture & Design

- Security Architecture
- Architectural Risk Analysis
- Security Design Requirements
- Attack Surface Analysis
- Threat Modelling
- Vulnerability Analysis and Flow Hypothesis
- Security Design Review
- Dependencies List, Open-source libraries



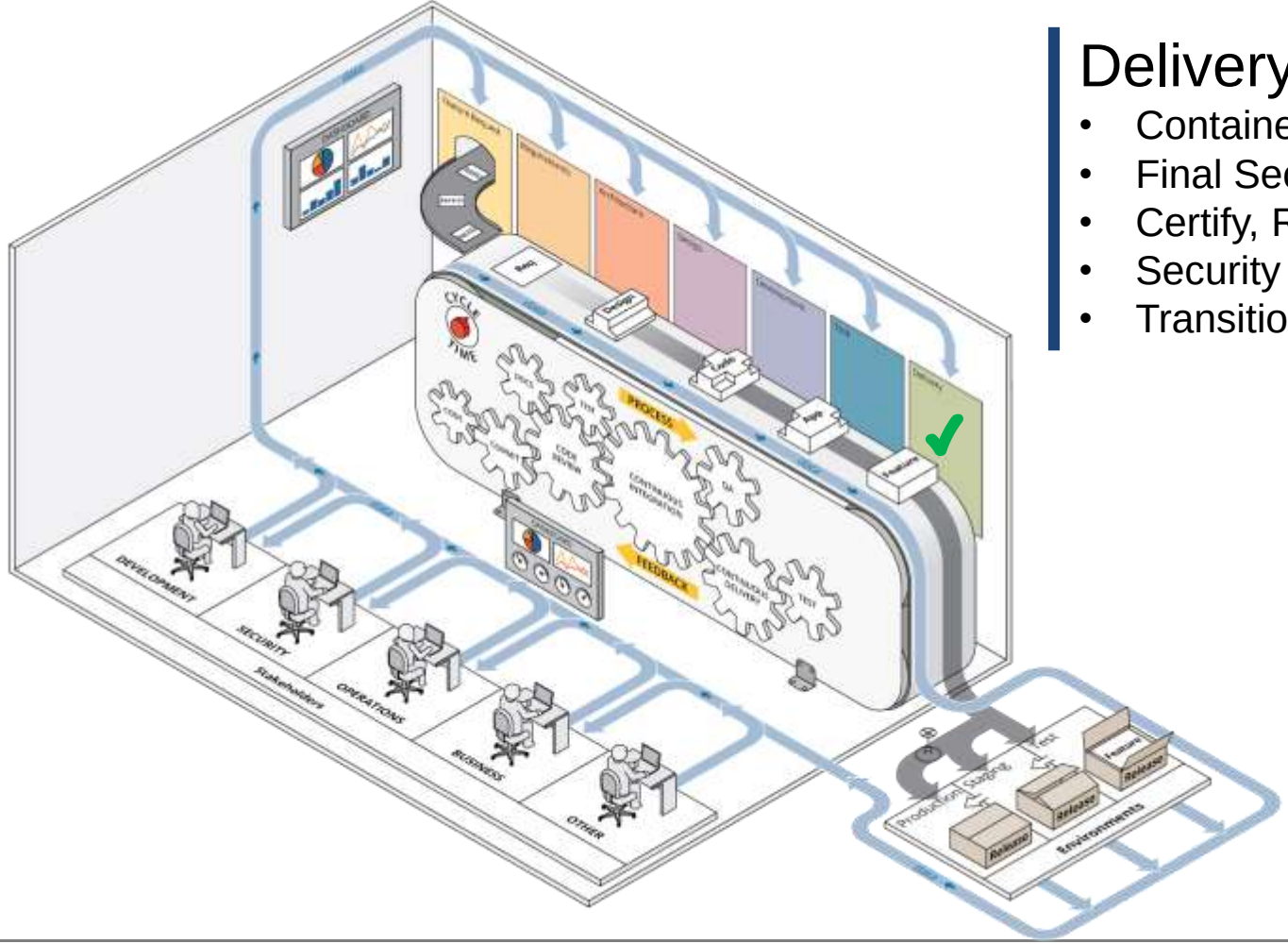
Development

- Secure Coding Practices
- Security Focused Code Review
- Deprecate Unsafe Functions
- Perform Security Unit Testing
- Static Code Analysis
- Checking of process and procedures for secure coding & traceability



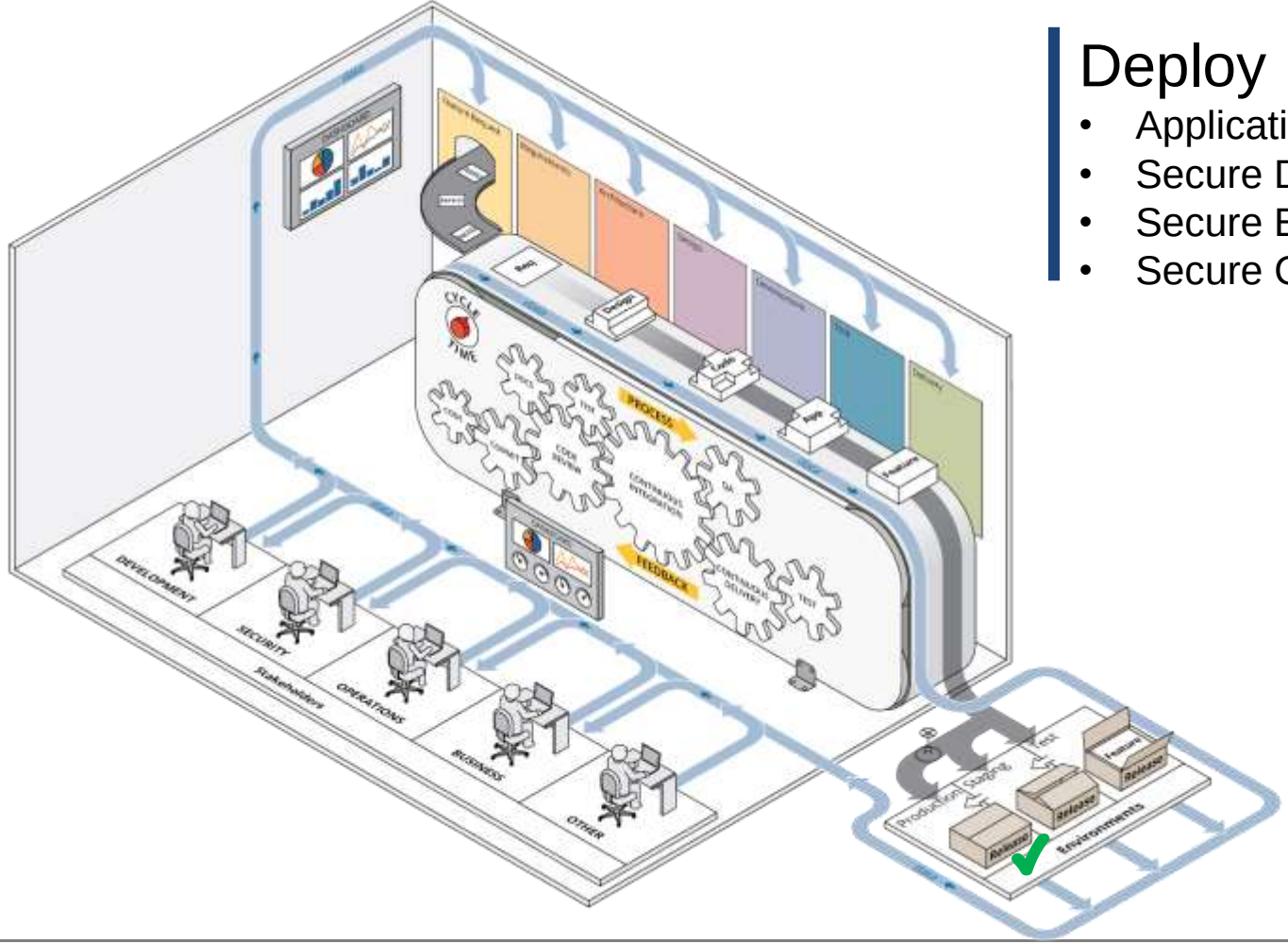
Testing

- Security Test Planning
- Security Testing
- Fuzz Testing
- Risk Based Security Testing
- Perform Dynamic Analysis
- Penetration Testing
- Verification of Security Implementation
- Verification of Process and Procedures
- Dependency Monitoring



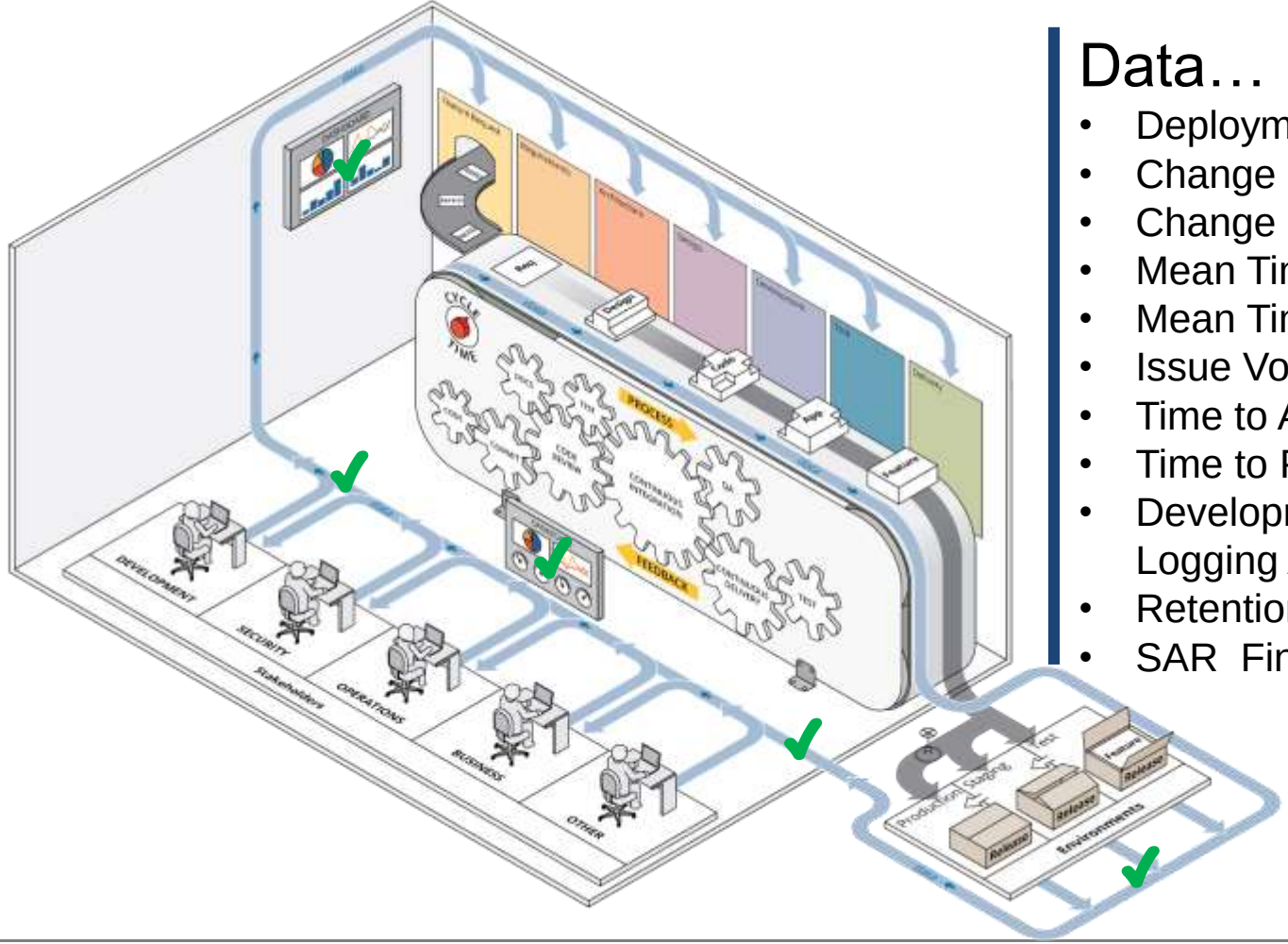
Delivery

- Container Security
- Final Security Review
- Certify, Release and Archive
- Security Acceptance Testing
- Transition Incident Response Plan



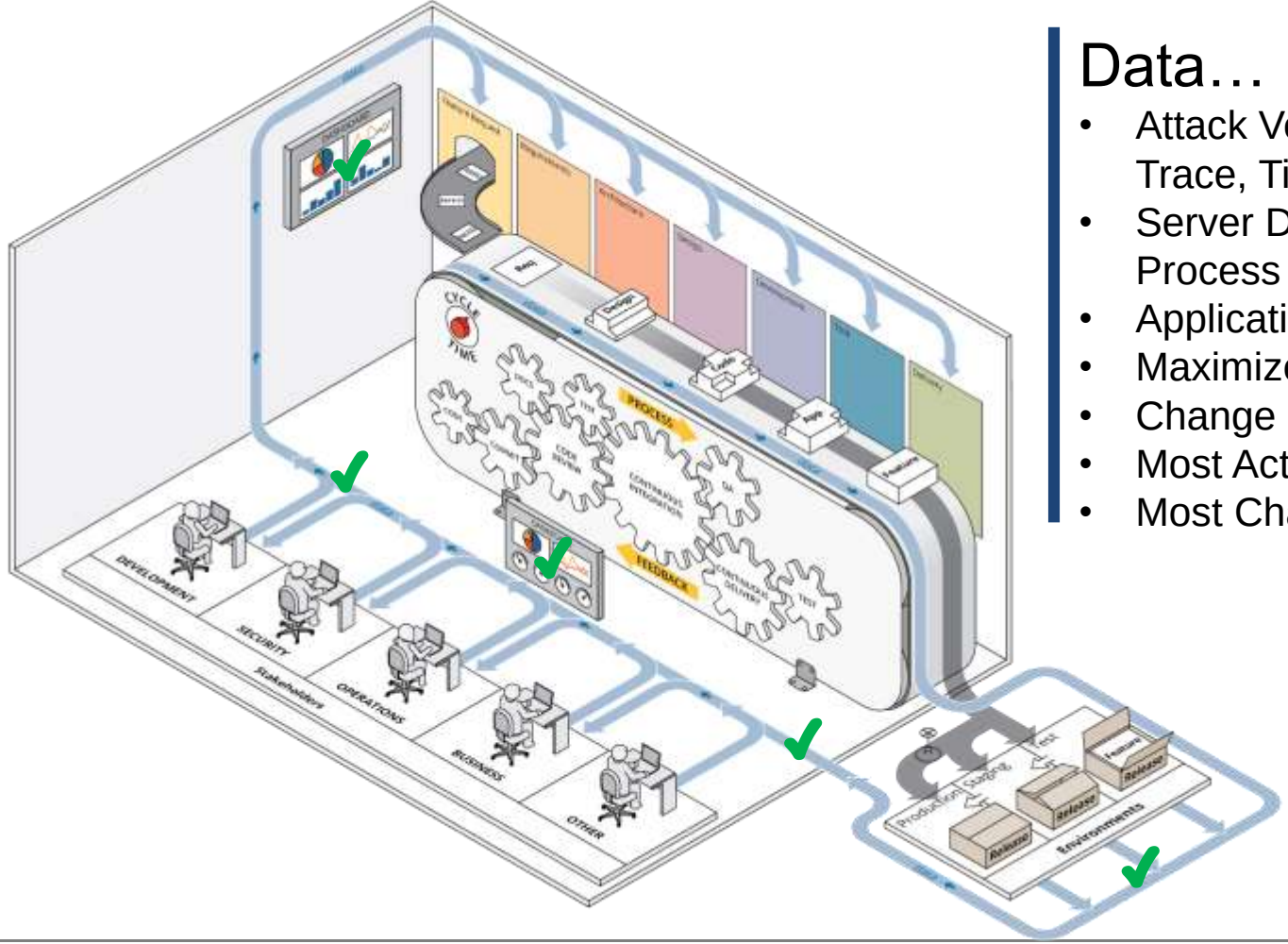
Deploy

- Application Security Monitoring
- Secure Deployment Process
- Secure Environment
- Secure Operational Enablement



Data…

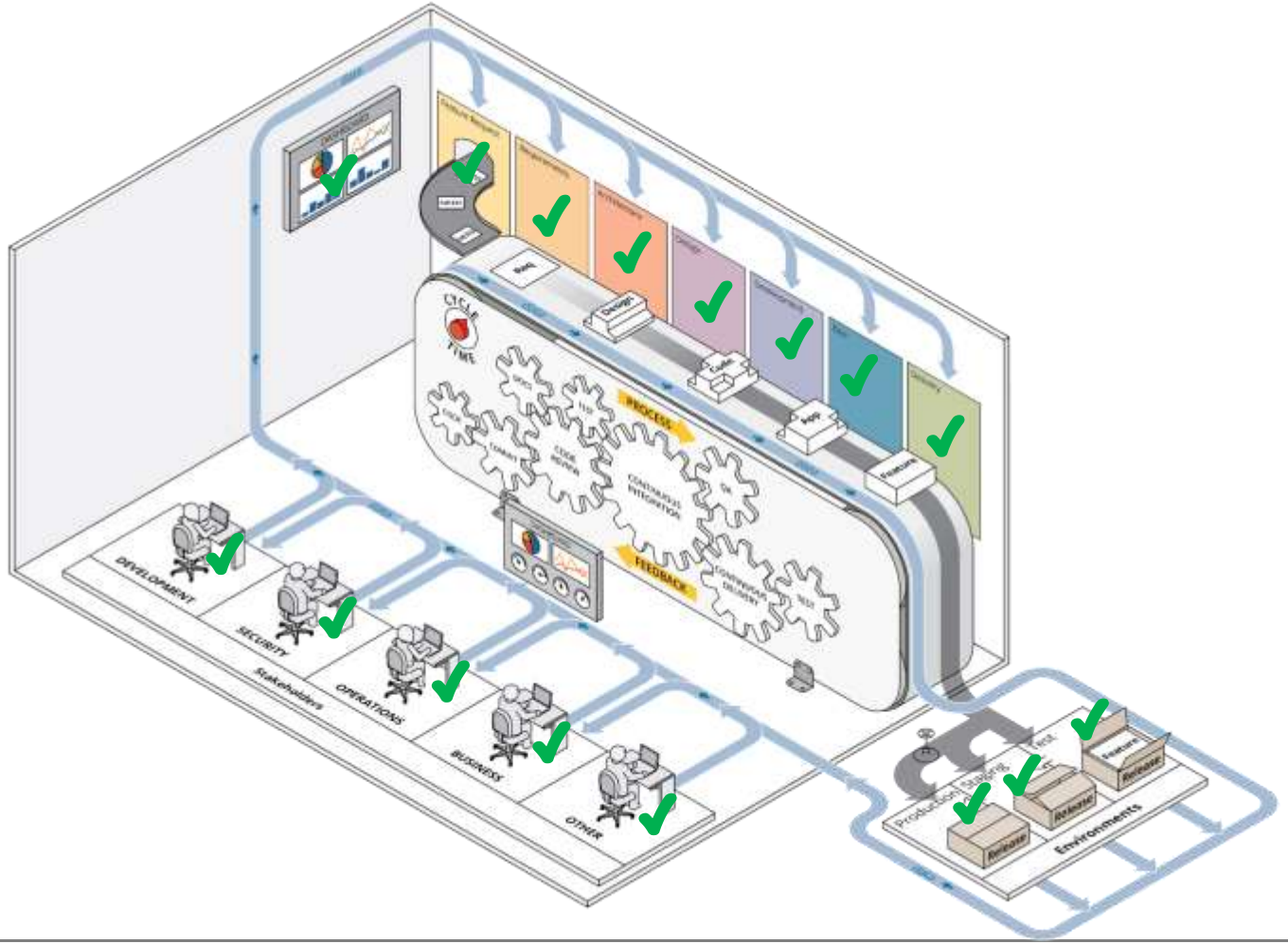
- Deployment Frequency
- Change Lead Time and Volume
- Change Failure Rate
- Mean Time To Recovery (MTTR)
- Mean Time to Detection (MTTD)
- Issue Volume and Resolution Time
- Time to Approval
- Time to Patch Vulnerabilities
- Development and Application Logging Availability
- Retention Control Compliance
- SAR Findings



Data…

- Attack Vector Details (IP, Stack Trace, Time, Rate of Attack, etc)
- Server Disk Space, Load and Process Monitoring
- Application Performance
- Maximize Monitoring
- Change in Size to Code Base
- Most Active Code Contributors
- Most Changed Code Areas

Think Security from Inception to Deploy and improve every delivery



For more information…

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

Webinar : https://www.sei.cmu.edu/publications/webinars/index.cfm

Podcast : https://www.sei.cmu.edu/publications/podcasts/index.cfm

SLS team GitHub Projects

- Once Click DevOps deployment
  https://github.com/SLS-ALL/devops-microcosm
- Sample app with DevOps Process
  https://github.com/SLS-ALL/flask_api_sample
  - Tagged checkpoints
    - v0.1.0: base Flask project
    - v0.2.0: Vagrant development configuration
    - v0.3.0: Test environment and Fabric deployment
    - v0.4.0: Upstart services, external configuration files
    - v0.5.0: Production environment
- On YouTube:
  https://www.youtube.com/watch?v=5nQlJ-FWA5A

Any Questions?

Hasan Yasar

Technical Manager,
Secure Lifecycle Solutions
hyasar@sei.cmu.edu
@securelifecycle