ACHIEVING CONTINUOUS ATO

SecurityCompass

Carnegie Mellon University
Software Engineering Institute

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.

DM20-1137

AGENDA

1. Current challenges with ATO
2. Aiming for Continuous ATO
3. Governance of Continuous ATO
4. Systems to enable Continuous ATO
5. Q&A

ATO: Authority to Operate

What is an ATO?

- An ATO is **Authority to Operate**
  - Authorizes the system to be placed on a production network
  - Interface with other components within the DoD
  - Authorizes access by end users to leverage these resources to execute mission
- Key staff in the ATO process
  - AO (Authorizing Official)
  - ISSO (Information System Security Officer)
  - Security assessor

- An AO makes a risk-based decision(**RMF NIST 800-37**) to grant an ATO for use of the system
- The decision has to be formalized in an ATO letter
  - An ATO letter must explicitly state the AO's acceptance of:
    - Use of the system at the Agency at the determined FIPS 199 impact level
    - All leveraged external services supporting the system
    - Any exceptions or exclusions of the Chief Security Officer (CSO) for use at the Agency

Why matters?

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.				

Current state of ATO (DoD Case Study)

- Authorizing application done just before operating the systems and average time to get approval ~6months
- Program Manger (PM) is graded against the system's KPP and their compliance with all regulations, along with cost and schedule parameters.
- PM makes trades between cost, schedule, quality, and functionality. With each trade residual risks occur.
- Someone must accept ALL residual risk associated with the system before placing it into operations.
- The Authorizing Official (AO) is responsible to accepting information security risks, which is done through the RMF process.
- An ATO is usually good for 3 years, but assumes no major changes to the system's cybersecurity posture will be made during that time.
- When changes do occur the AO may require a reassessment and reauthorization, which impacts the PM's cost and schedule and is contrary to being Agile.

Source: Timothy A. Chick. "Maintaining Your Authority to Operate (ATO) While Being Agile: Achieving Continuous Reauthorization with DevOps", 2018.

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

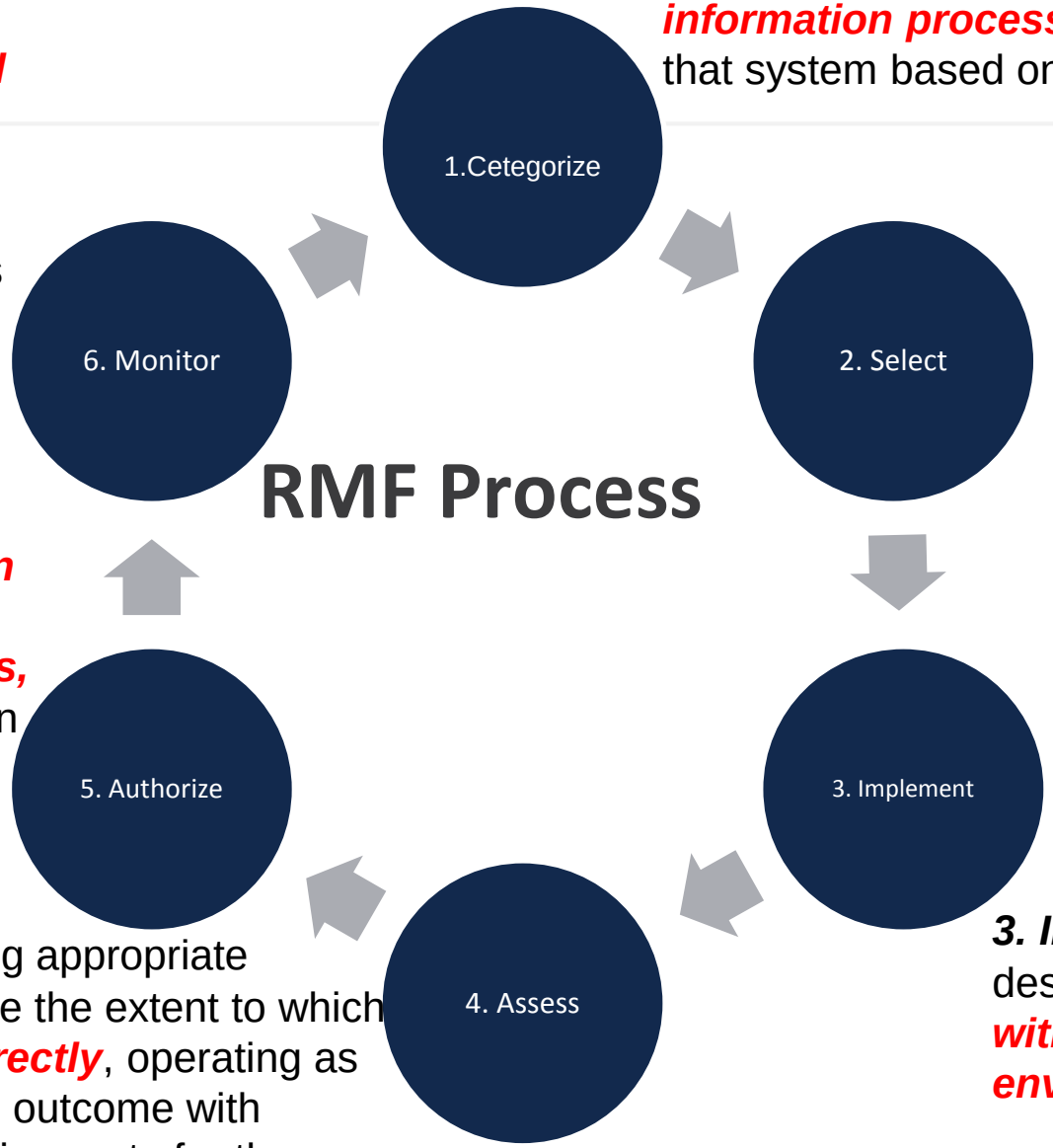
2. Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an ***organizational assessment of risk and local conditions***.

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

Continuous ATO(cATO) is the Goal

cATO authorizes the platform, process, and the team that produces the product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the Authorizing Official (AO)

cATO and DevSecOps

DevSecOps			
Continuous Authorization			
Security Control Assessment	**Security Status Monitoring**	**Security Status Reporting**	**Risk Tolerance Monitoring**
• Manual risk assessment of sprint backlog • DevSecOps automated tool sprint assessments STIG (Compliance as Code), SAST, DAST, & pen testing • Ops Incident analysis with feedback to DevSec • DevSec review of assessment findings	• Review security status: Tier II & III SIEM event log monitoring, control compliance/effectiveness, Analysis of cyber metrics and risk score • Review risk tolerance threshold monitoring: Review of change request impact analysis, Review of cyber findings, Review of threat landscape • Manual review of app security designs • Impact of risk to mission • Development of course of actions • Automated compliance checking and reporting	• Ongoing risk score/posture • Tolerance threshold trend data • Backlog list of security stories • Cybersecurity metrics: non-compliance, vulnerabilities, incidents, Sec issues on backlog • Change in threat	• Provide tolerance guidance • Assess based on time/event trigger • People certified for maintaining cATO • Process certified & accredited • Approve entry to continuous authorization

Continuous Risk Authorization with monitoring (NIST 800-137)

Continuous Monitoring

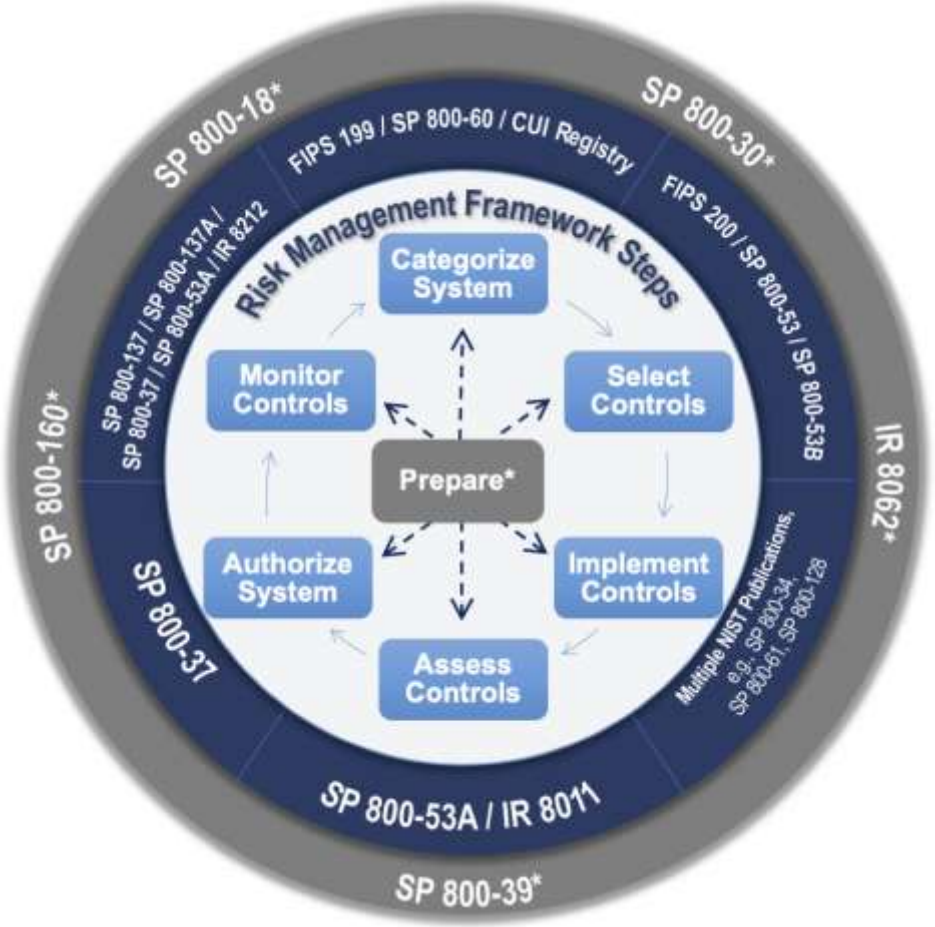
- Maps to risk tolerance
- Adapts to ongoing needs
- Actively involves management

Desired future state of Continuous ATO

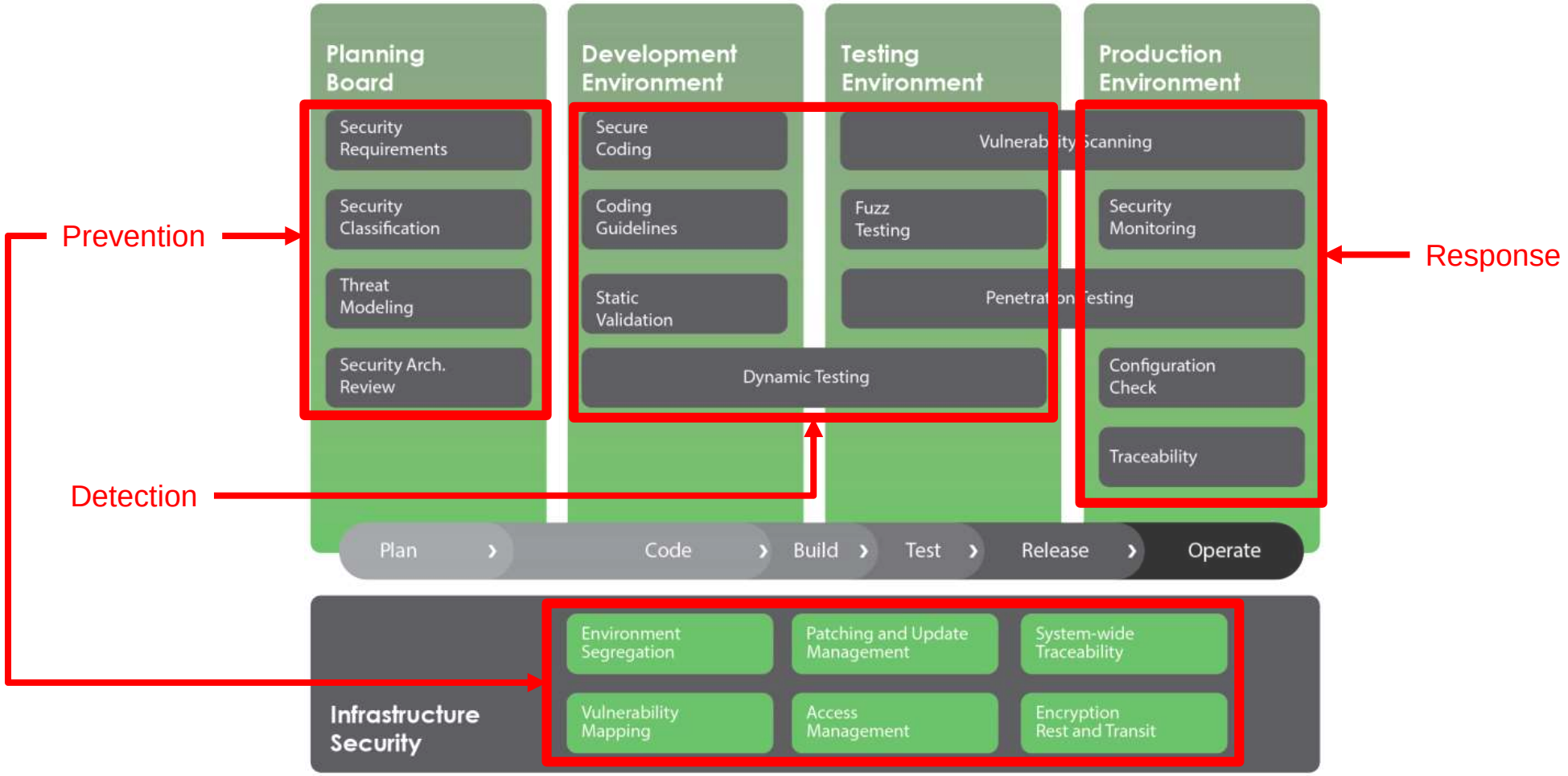
- Commoditize components and introduce containerization
- Address technical dept in legacy application
- Migrate to modular architecture (Microservices, MOSA)
- Improve development and deployment tools
- Integrate deployment pipeline from inception to operation
- Operationalize SRE on infrastructure team
- Develop contracts SLAs and SLOs
- Introduce Audit vs Gate keeper

- Codify CI/CD tools, creating DevSecOps Pipeline for Continuous Authorization
- Automation and Immutable Environments:
- Source controlling Infrastructure-as- Code(IaC)
- Pipeline release supporting a live DoD system
- DevSecOps enabled Data Science workflows and deployments
- Introduce New Governance approach based on DevSecOps
- Select small discreet parts of the enterprise as projects for DevSecOps enablement

Risk perspective



Security Best Practices



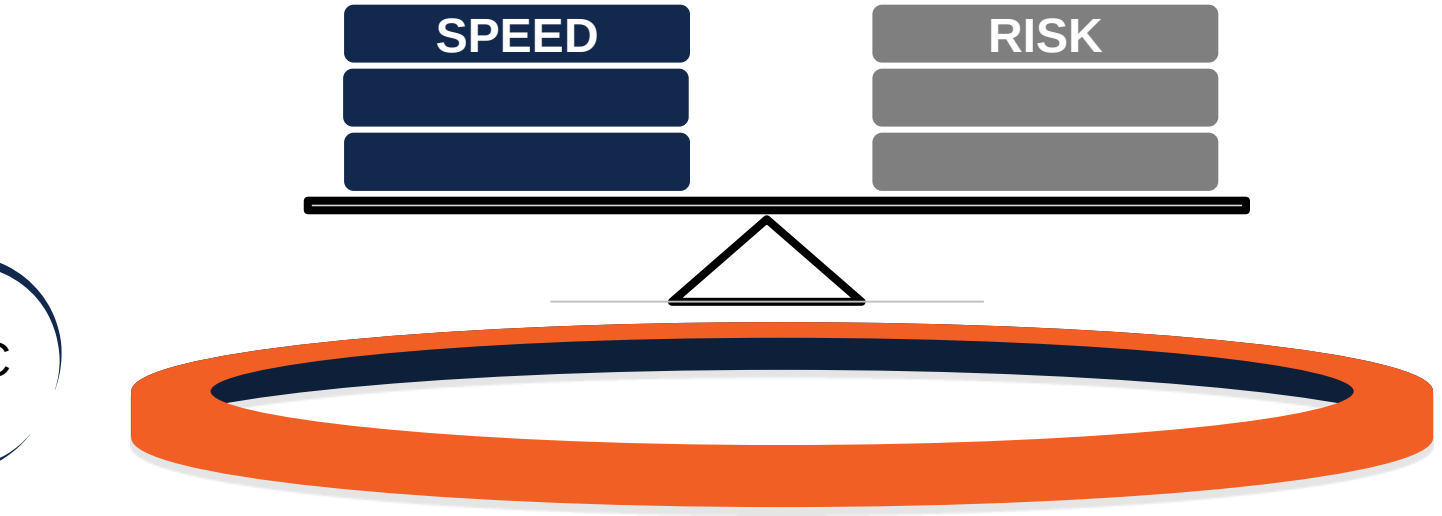
Source: Ahmed. "DevSecOps: Enabling Security by Design in Rapid Software Development", 2019.

The Risk Assessment Process

1	2	3	4	5	6	7
ELICIT VIEWS FROM STAKEHOLDERS	**IDENTIFY RISK**	**DETERMINE SOURCES, CAUSES AND DRIVERS OF RISK**	**ANALYZE CONTROLS**	**UNDERSTAND CONSEQUENCES AND LIKELIHOOD**	**SELECT BETWEEN OPTIONS**	**RECORD AND REPORT**
• Brainstorming • Delphi technique • Interview • Survey	• Checklist • Taxonomy • Classification • Scenario	• Ishikawa	• Bow Tie Analysis	• Business Impact Analysis • Privacy Impact Analysis	• Cost/Benefit Analysis	• Risk Register

Source: ISO. "ISO 31010: Risk Management – Risk assessment techniques", 2019.

Achieving Continuous ATO



STANDARDS

PLC

- Policy management
- Compliance and Audit

SDLC

- Security Requirements
- Threat Modeling
- Security Architecture
- Secure Coding
- Static Analysis

DEV

QMLC

- Dynamic Analysis
- Fuzz Testing
- Penetration Testing

TEST

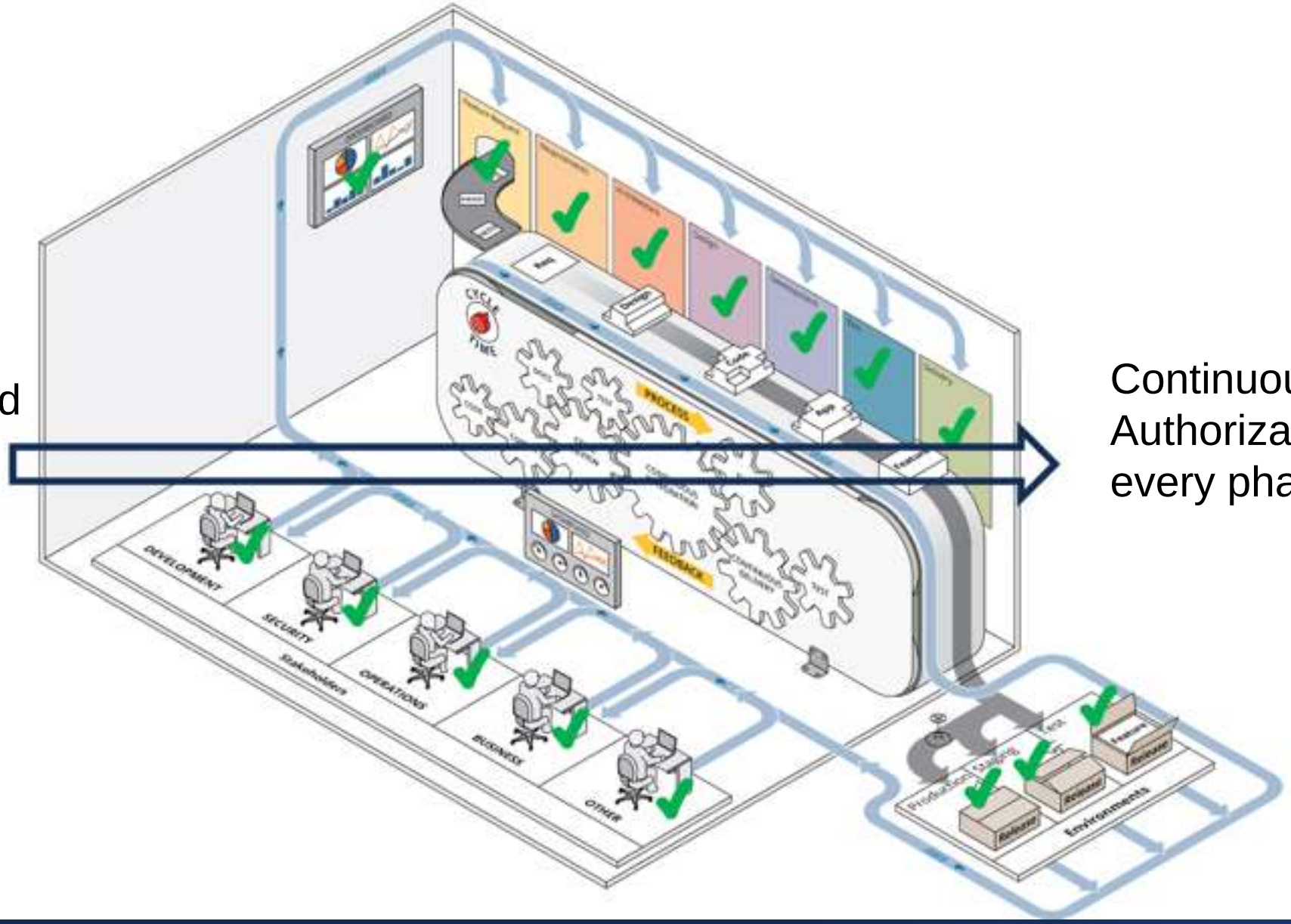
SMLC

OPS

- Container Security
- SecOps

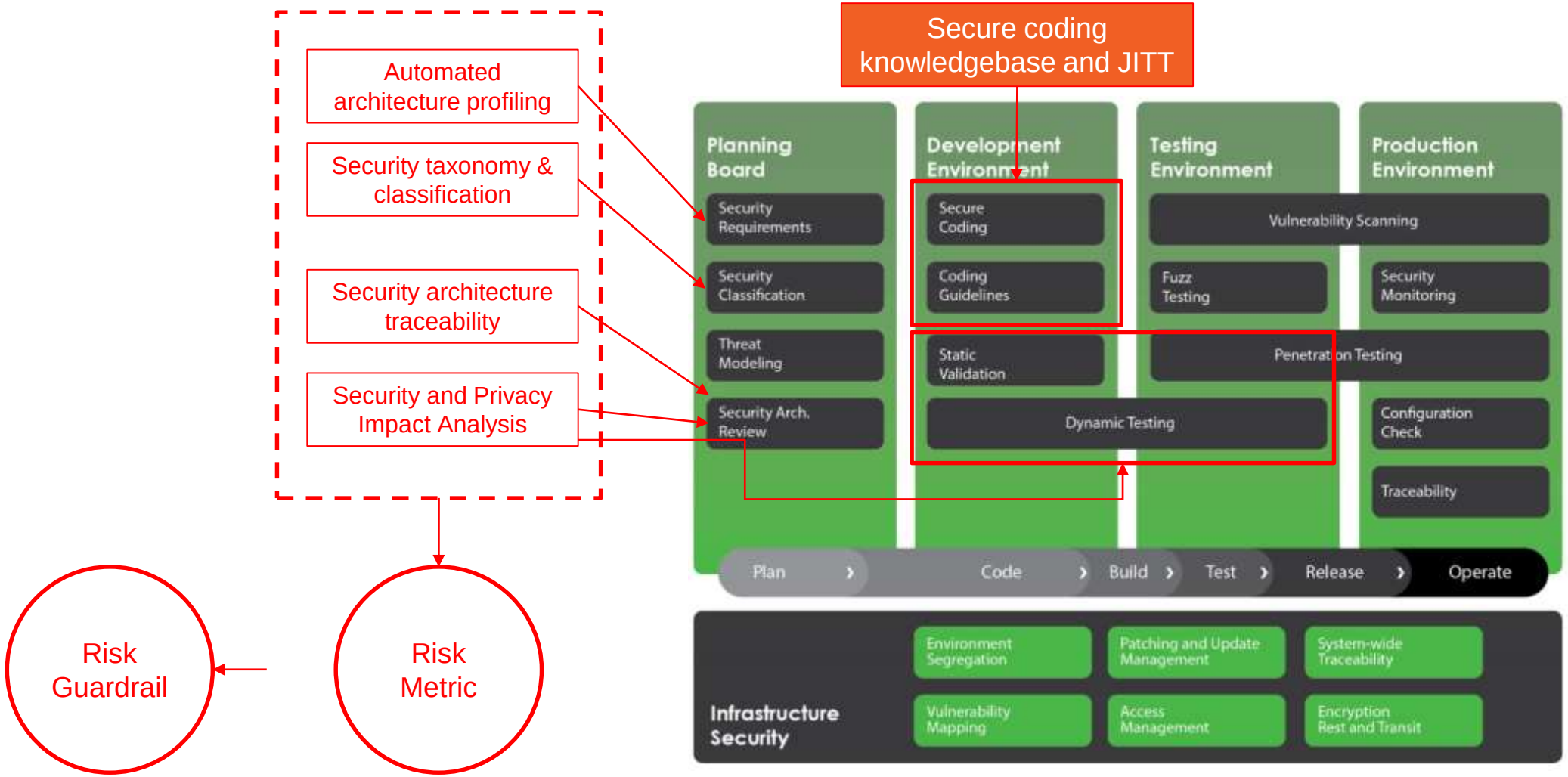
DevOps with Security(DevSecOps) for cATO

Security from inception to deployment and improvement with every delivery



Continuous Authorization on every phases

Combining Speed and Risk



Governance

	SPEED TO MARKET METRICS
SECURITY AUTOMATION	• Time to delivery • # high severity bugs found in production
THREAT MODELING	• # of unmitigated high severity attacks
COMPLIANCE AND REGULATORY	• # of unmitigated high severity clauses
SECURE DEVELOPMENT	• Code scan results
SECURITY OPERATIONS	• # of security incidents in production

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

Next steps

- Document your current and future state ATO architecture
- Identify business capabilities and value streams to fill the gap
- Create tooling architecture to support new business capabilities

THANK YOU

SecurityCompass

Carnegie Mellon University
Software Engineering Institute