RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **DSO-R01**

At What Point Does DevSecOps Become Too Risky for the Business?

Hasan Yasar

Technical Director
Software Engineering Institute
Carnegie Mellon University
@SecureLifecycle

Altaz Valani

Research Director
Security Compass

Agenda

- The Context of Business Risk in DevSecOps
- Managing the Risk Gap through Integrated Pipelines
- Demo

RSAConference2020

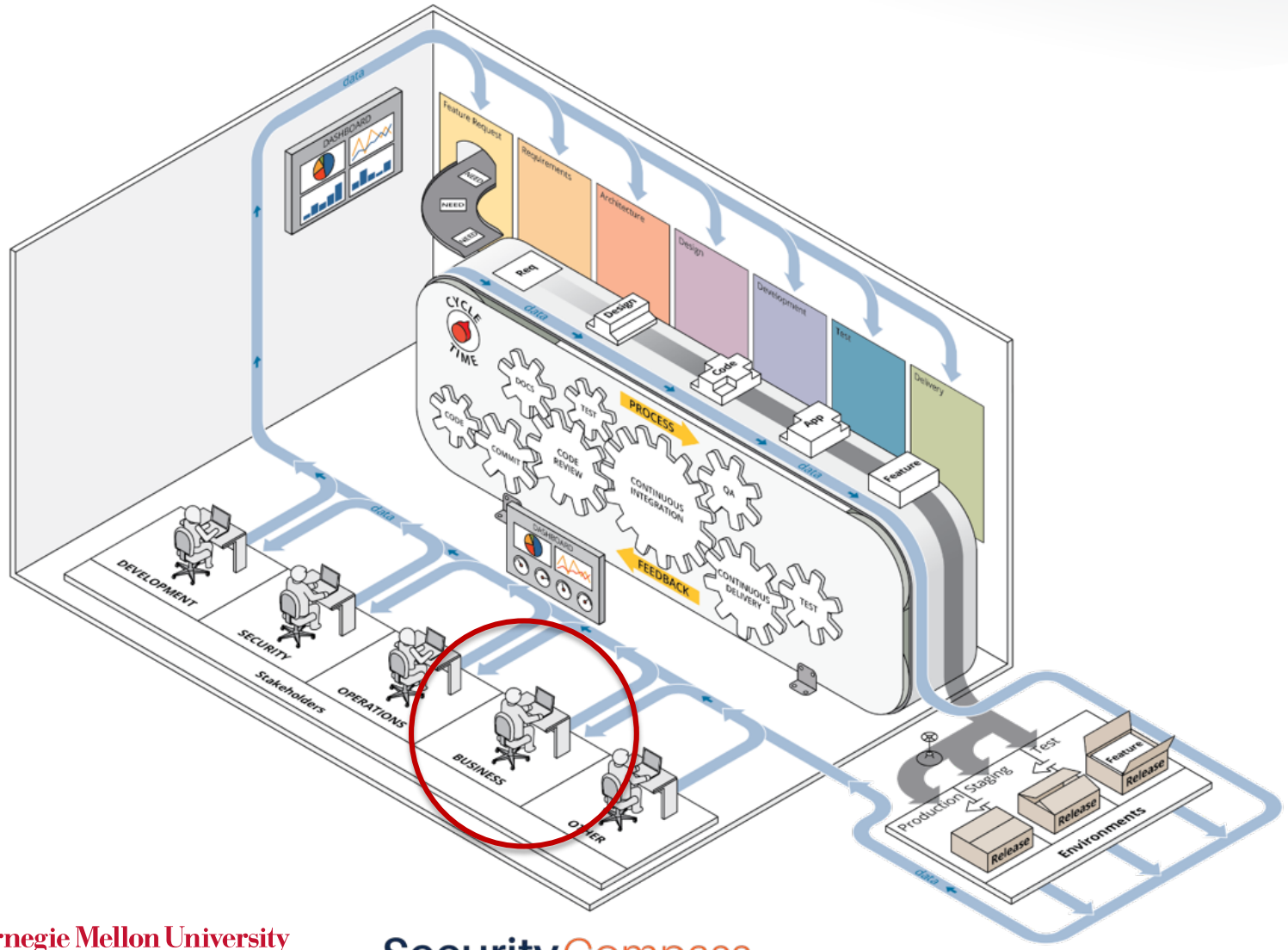
The Challenge of Managing Business Risk in DevSecOps

What the Business Wants

Realtime Risk Assessment Reporting against DevSecOps

- What is our compliance risk?
- Can we recover quickly in case of a breach?
- Where is DevSecOps a blocker to revenue?

Continuous Risk Management: Reference DevSecOps Factory

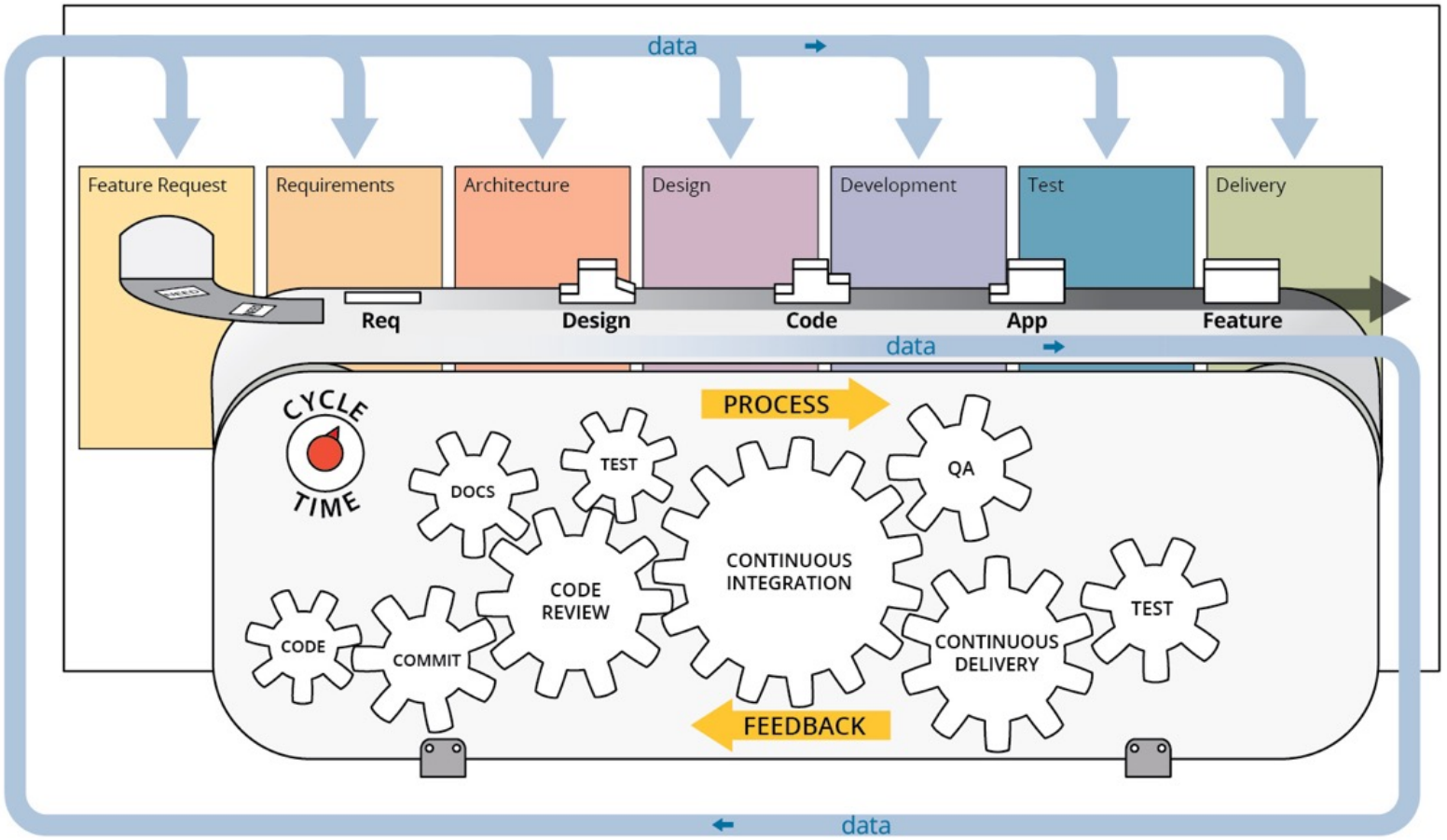


- Feature to deployment
- Iterative and incremental development
- Automation in every phase of the SDLC
- Continuous feedback
- Metrics and measurement
- Complete engagement with all stakeholders
- Transparency and traceability across the lifecycle

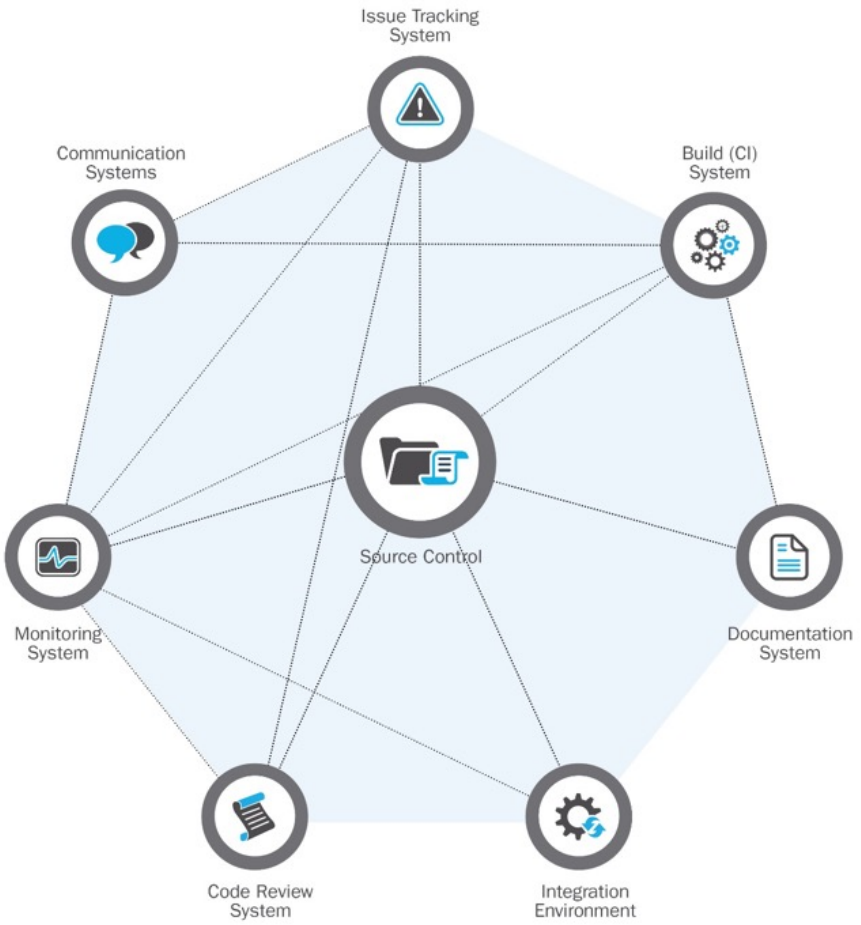
Poll the Audience

- DSO-R01
- Do you have a mature DevSecOps platform?
  - A. YES
  - B. NO
  - C. Partial
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=792005110

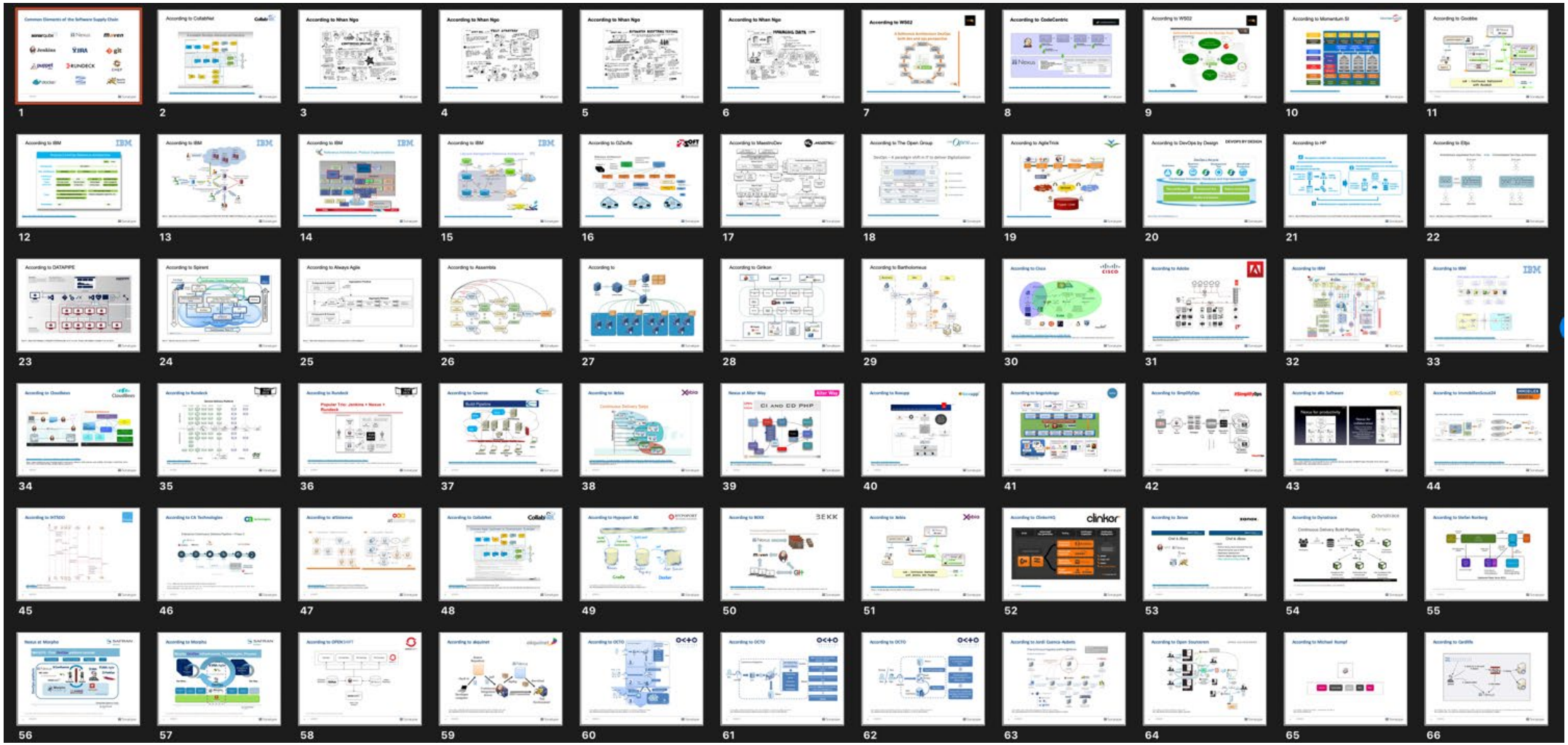
Continuous Risk Assessment: Reference DevSecOps Pipeline



Continuous Risk Assessment: Reference DevSecOps Architecture



Many Ways to Implement DevSecOps Pipeline



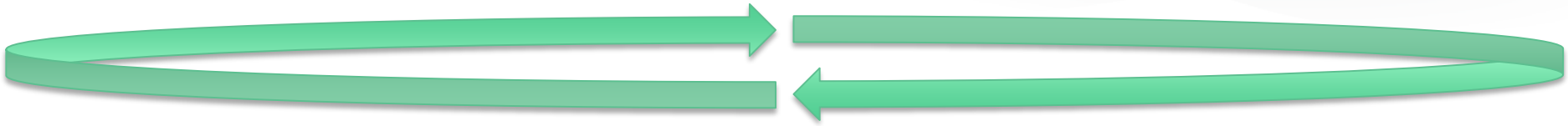
RSAConference2020

Managing the Risk Gap

Poll the Audience

- DSO-R01
- Do you follow organizational risk factors in your DevSecOps?
  - A. YES
  - B. NO
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=792005110

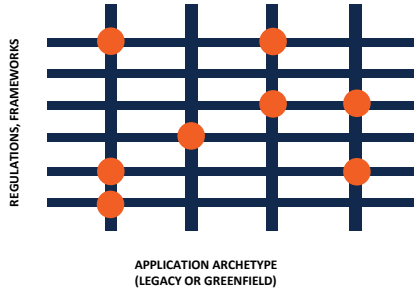
DevSecOps Means Integrating Business and DevOps Pipelines



Security Policy Pipeline

NIST IEEE ISO FFIEC

Policy to Execution Pipeline



DevOps Execution Pipeline

RSAConference2020

Demo

Poll the Audience

- DSO-R01
- Do you believe that we will have a more secure system with DevSecOps?
  - A. YES
  - B. NO
- https://rsa1-live.eventbase.com/polls?event=rsa2020&session=792005110

Now it is time to take an Action

- Immediate Action: Start tracking risk as a first order citizen
  - Inject security requirements based on business risk tolerance
  - Report on risk (requirements partially or not met at all)
  - Move to dual attestation (human testing and automated testing)

Now it is time to take an Action

- Over the next 90 days: Focus on the architecture
  - Integrate DevSecOps lifecycle with Business Risk Assessment through a Policy to Procedure layer
  - Map standards and frameworks to solution architecture archetypes for lightweight threat modeling in common use cases
  - Automate generation of audit reports that measure solution requirements against standards/regulations
  - Set go/no-go deployment policies based on business risk tolerance
  - Move toward consistent, quantitative risk assessment (OpenFAIR for example)

Any Questions?

Hasan Yasar

Technical Director,
hyasar@sei.cmu.edu
@securelifecycle

Altaz Valani

Research Director,
avalani@securitycompass.com

RSAConference2020

Notes/Backup