Compliance Help for the Agile Enterprise

Dave Owczarek | Senior Manager, Adobe Systems, Inc.

Some compliance framework stuff

PCI DSS ❖ HIPAA ❖ SOC II

credit card information — medical information — operations management

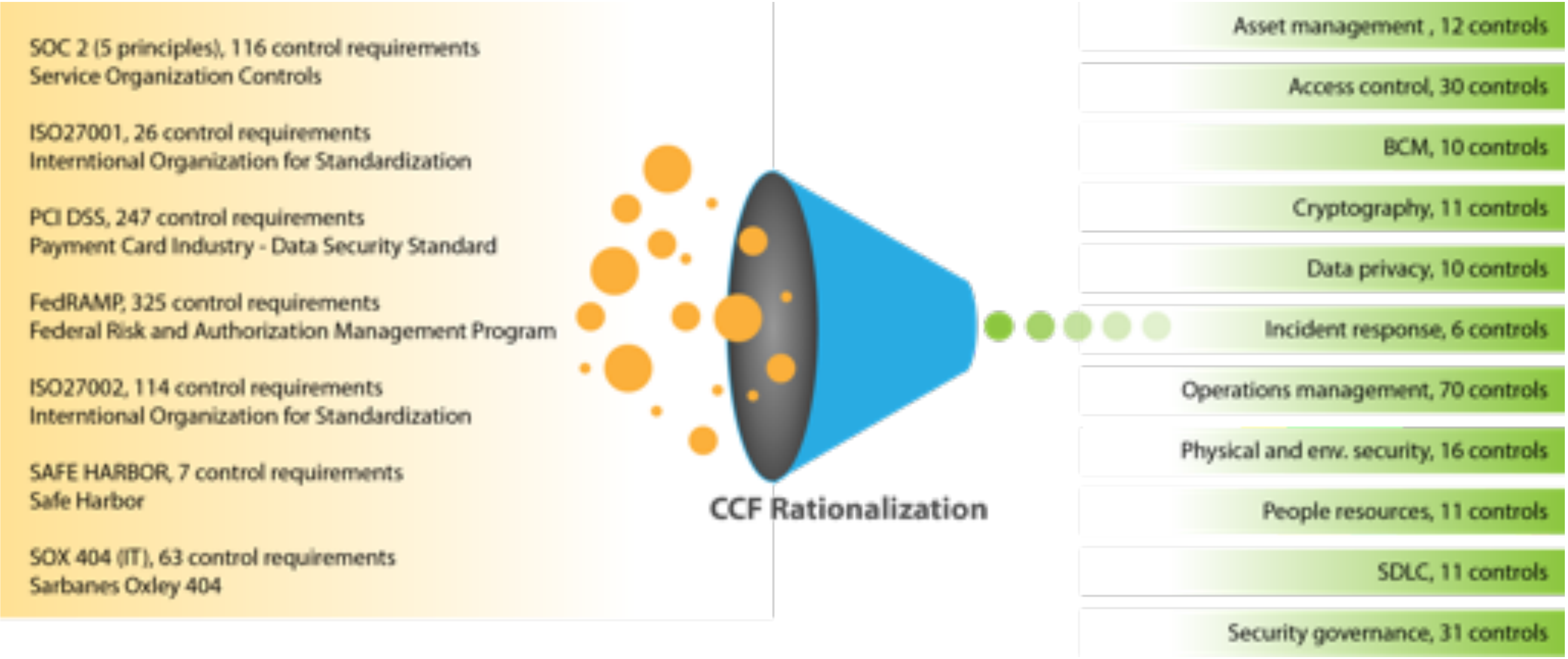
Precise Language

ePHI - protected health information

CHD - cardholder data

controls, processes, policies, standards

Unified compliance mapping – The Adobe Common Controls Framework (CCF)



SOC 2 (5 principles), 116 control requirements
Service Organization Controls

ISO27001, 26 control requirements
Interntional Organization for Standardization

PCI DSS, 247 control requirements
Payment Card Industry - Data Security Standard

FedRAMP, 325 control requirements
Federal Risk and Authorization Management Program

ISO27002, 114 control requirements
Interntional Organization for Standardization

SAFE HARBOR, 7 control requirements
Safe Harbor

SOX 404 (IT), 63 control requirements
Sarbanes Oxley 404

CCF Rationalization

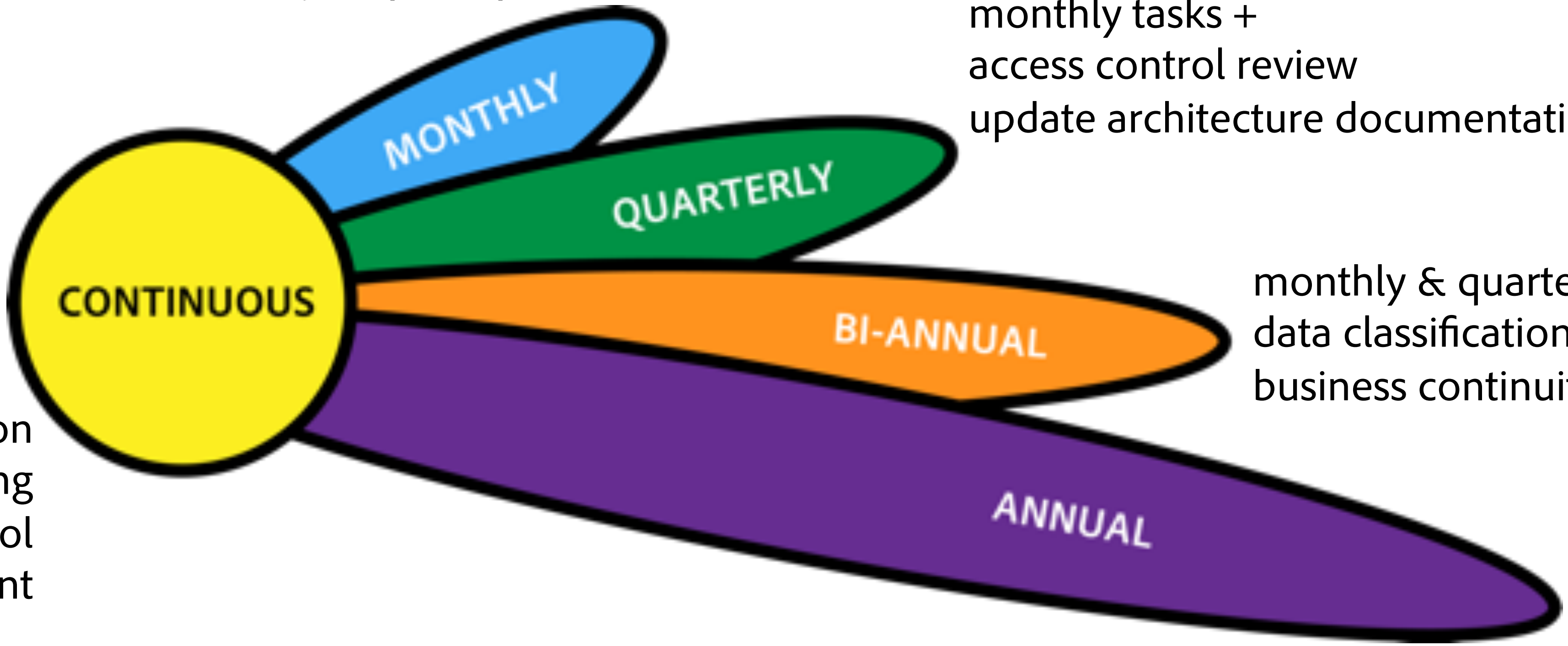
- Asset management , 12 controls
- Access control, 30 controls
- BCM, 10 controls
- Cryptography, 11 controls
- Data privacy, 10 controls
- Incident response, 6 controls
- Operations management, 70 controls
- Physical and env. security, 16 controls
- People resources, 11 controls
- SDLC, 11 controls
- Security governance, 31 controls

~1,000 controls in 10+ standards versus ~200 controls in 11 domains

What is continuous compliance?

monitoring review
firewall rule update
capacity analysis

monthly tasks +
access control review
update architecture documentation



monthly & quarterly tasks +
data classification review
business continuity plan review

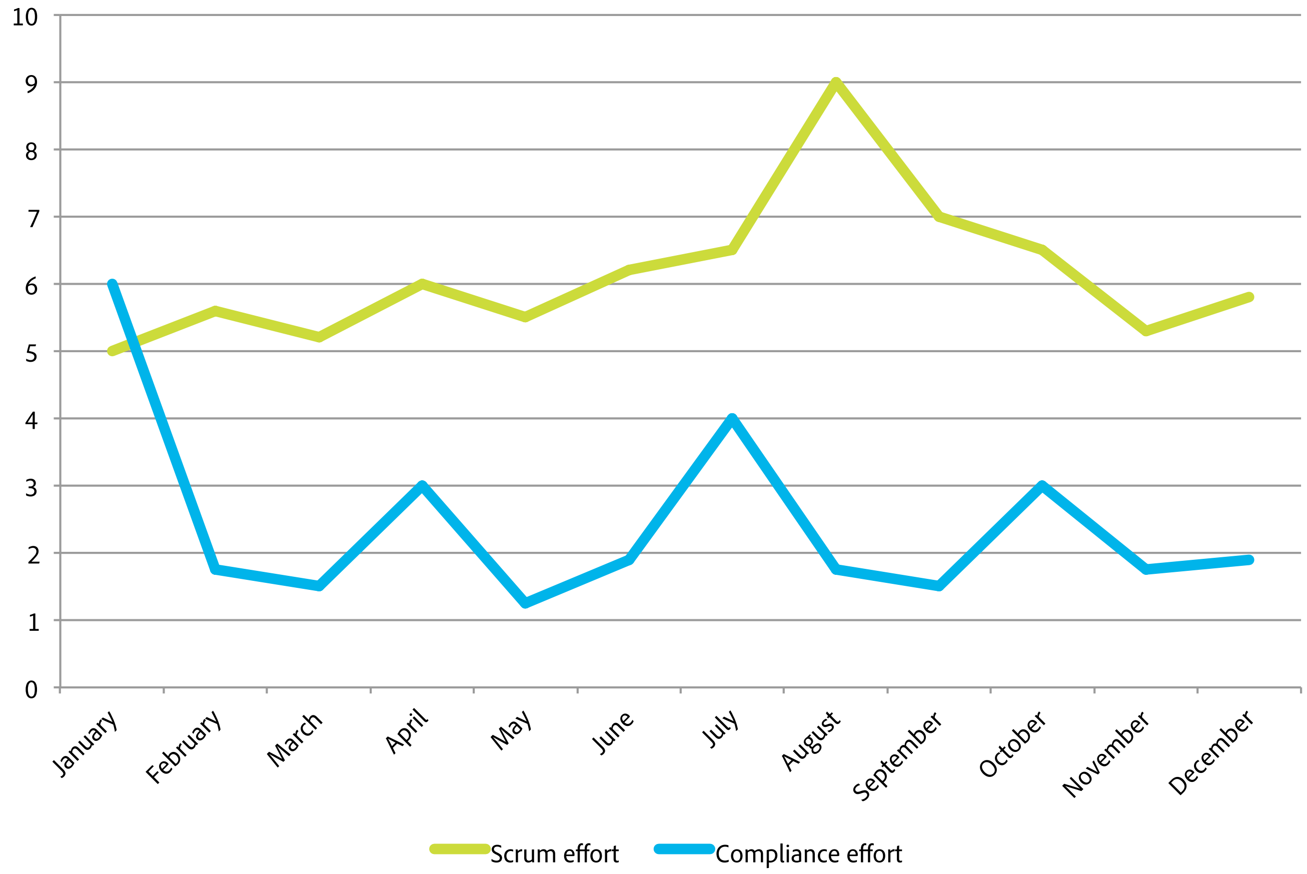
intrusion detection
file integrity monitoring
access control
session management

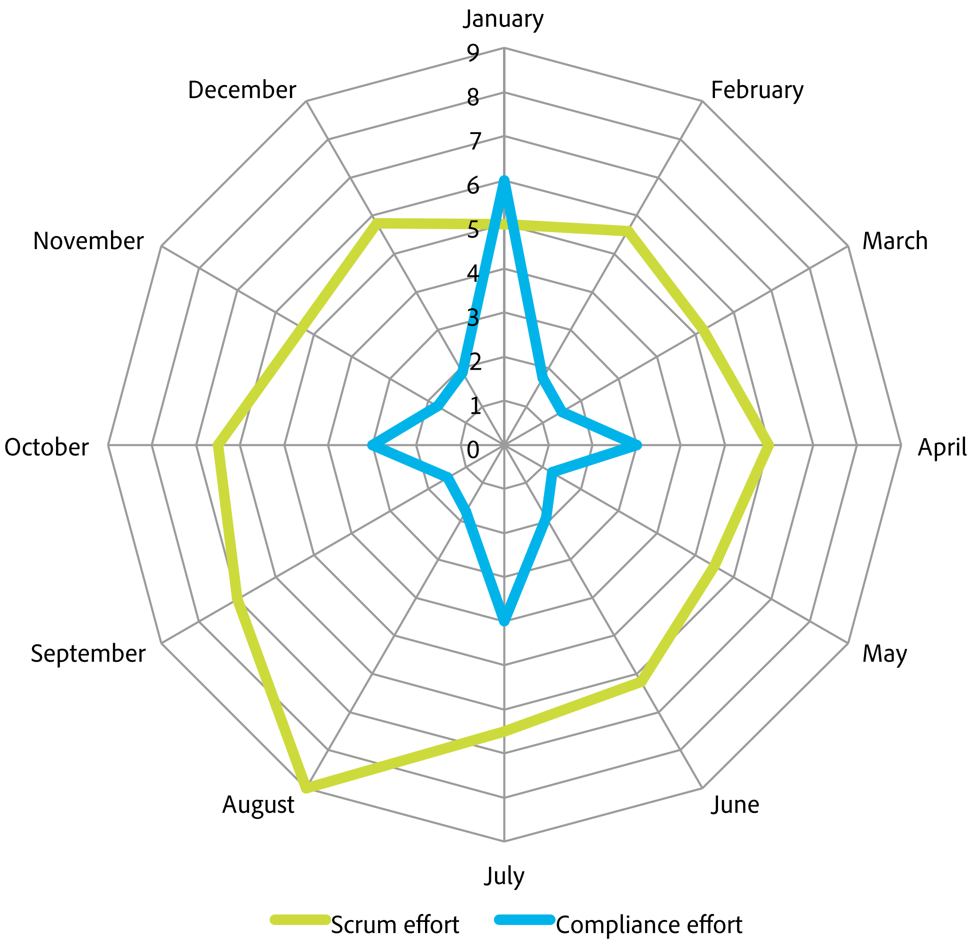
monthly, quarterly, bi-annual tasks +
disaster recovery drill
risk analysis
annual compliance audit

Continuous compliance harmonic cycles

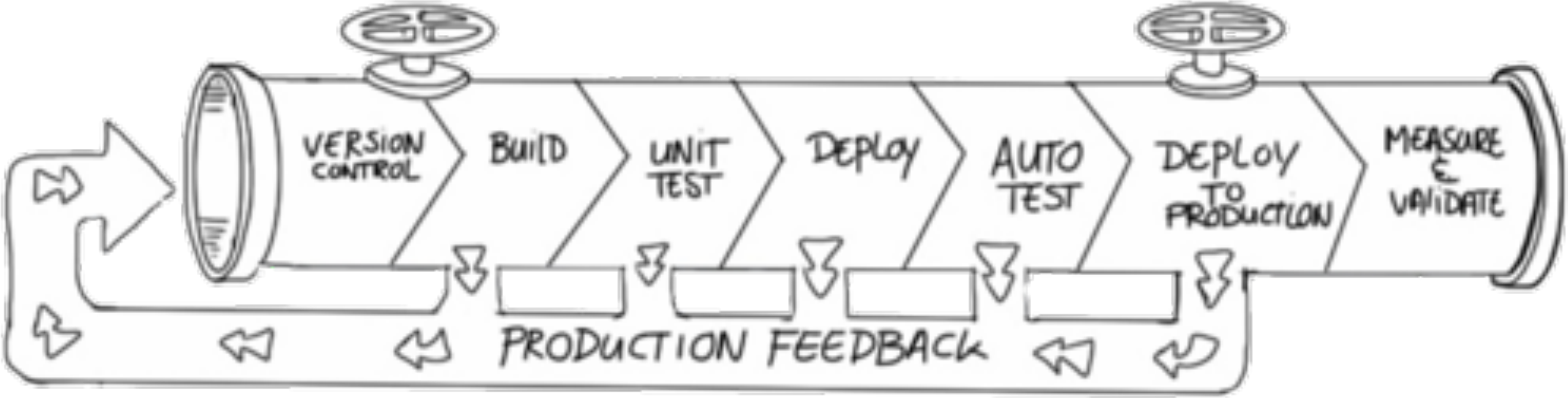
the continuous compliance chainsaw

Cyclical nature of work

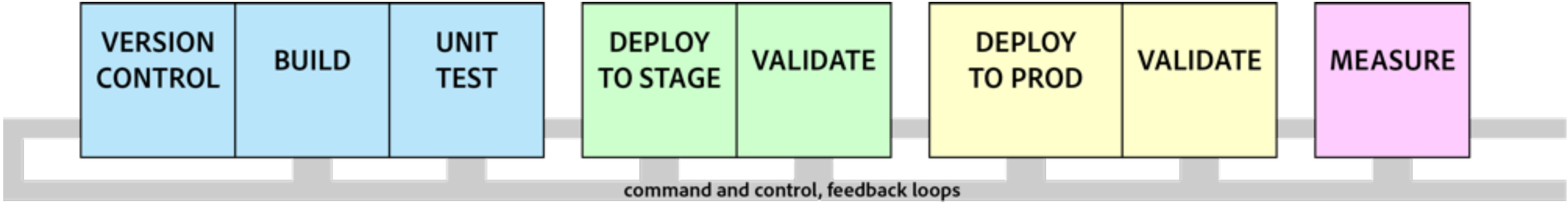




Docker continuous delivery pipeline

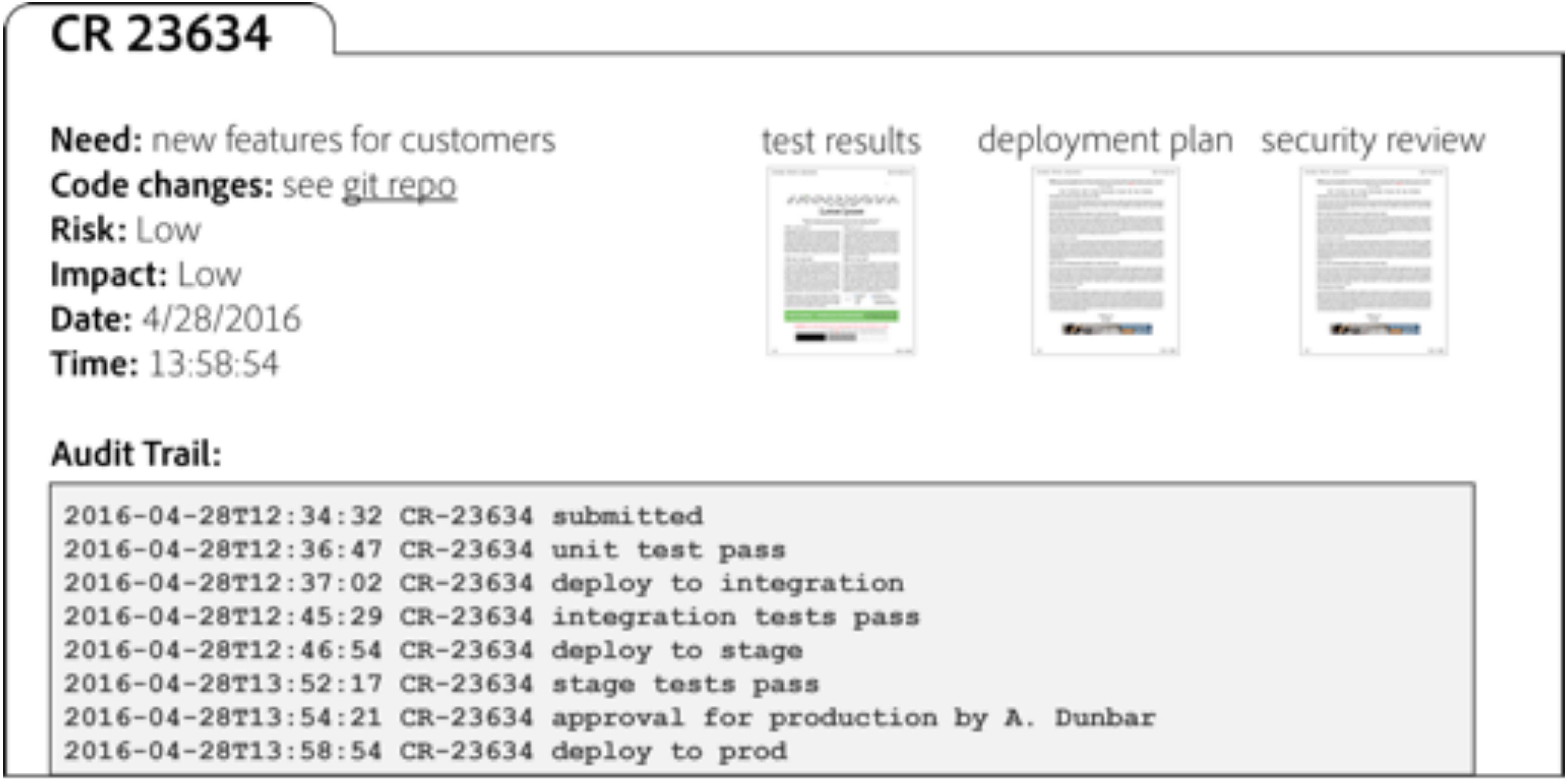


Baseline continuous pipeline



Four important compliance contexts

Change control – evidence-based design



CR 23634

Need: new features for customers

Code changes: see git repo

Risk: Low

Impact: Low

Date: 4/28/2016

Time: 13:58:54

test results

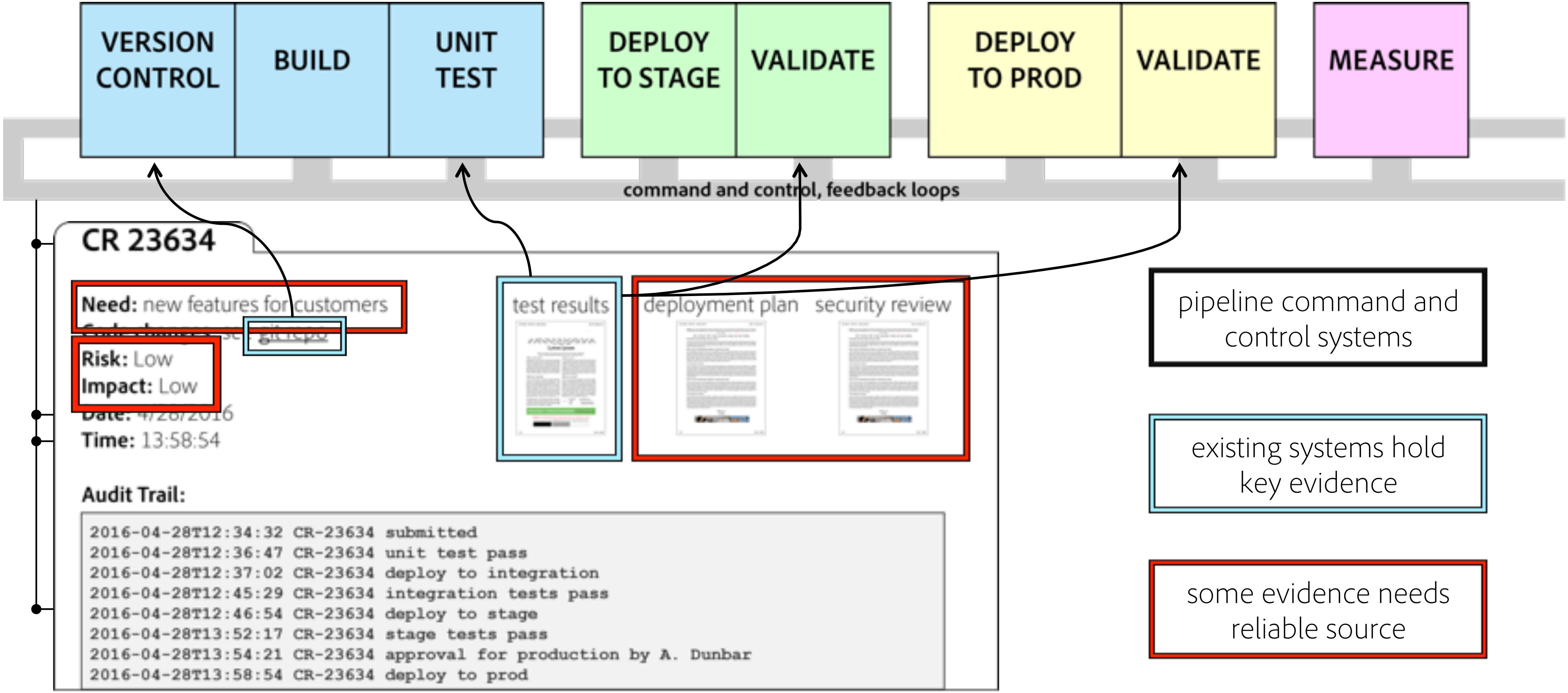
deployment plan

security review

Audit Trail:

```
2016-04-28T12:34:32 CR-23634 submitted
2016-04-28T12:36:47 CR-23634 unit test pass
2016-04-28T12:37:02 CR-23634 deploy to integration
2016-04-28T12:45:29 CR-23634 integration tests pass
2016-04-28T12:46:54 CR-23634 deploy to stage
2016-04-28T13:52:17 CR-23634 stage tests pass
2016-04-28T13:54:21 CR-23634 approval for production by A. Dunbar
2016-04-28T13:58:54 CR-23634 deploy to prod
```

Mapping evidence to the pipeline



CR 23634

Need: new features for customers

Code changes: see git repo

Risk: Low

Impact: Low

Date: 4/28/2016

Time: 13:58:54

Audit Trail:

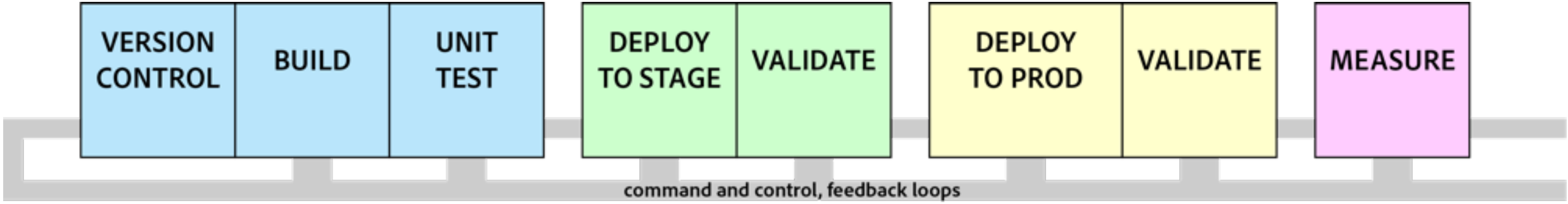
```
2016-04-28T12:34:32 CR-23634 submitted
2016-04-28T12:36:47 CR-23634 unit test pass
2016-04-28T12:37:02 CR-23634 deploy to integration
2016-04-28T12:45:29 CR-23634 integration tests pass
2016-04-28T12:46:54 CR-23634 deploy to stage
2016-04-28T13:52:17 CR-23634 stage tests pass
2016-04-28T13:54:21 CR-23634 approval for production by A. Dunbar
2016-04-28T13:58:54 CR-23634 deploy to prod
```

pipeline command and control systems

existing systems hold key evidence

some evidence needs reliable source

Change control – approval automation example



VERSION CONTROL | BUILD | UNIT TEST | DEPLOY TO STAGE | VALIDATE | DEPLOY TO PROD | VALIDATE | MEASURE

command and control, feedback loops

Change Classification Standard

Risk

Low - Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
Medium - incididunt ut labore et dolore magna aliqua. Ut enim ad minim
High - veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea

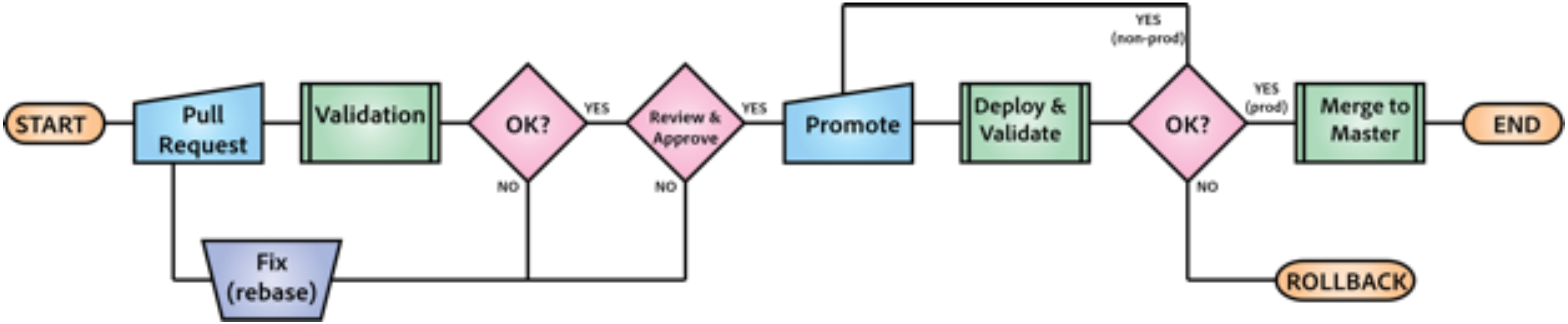
Impact

Low - Lorem ipsum dolor sit

Approval Criteria

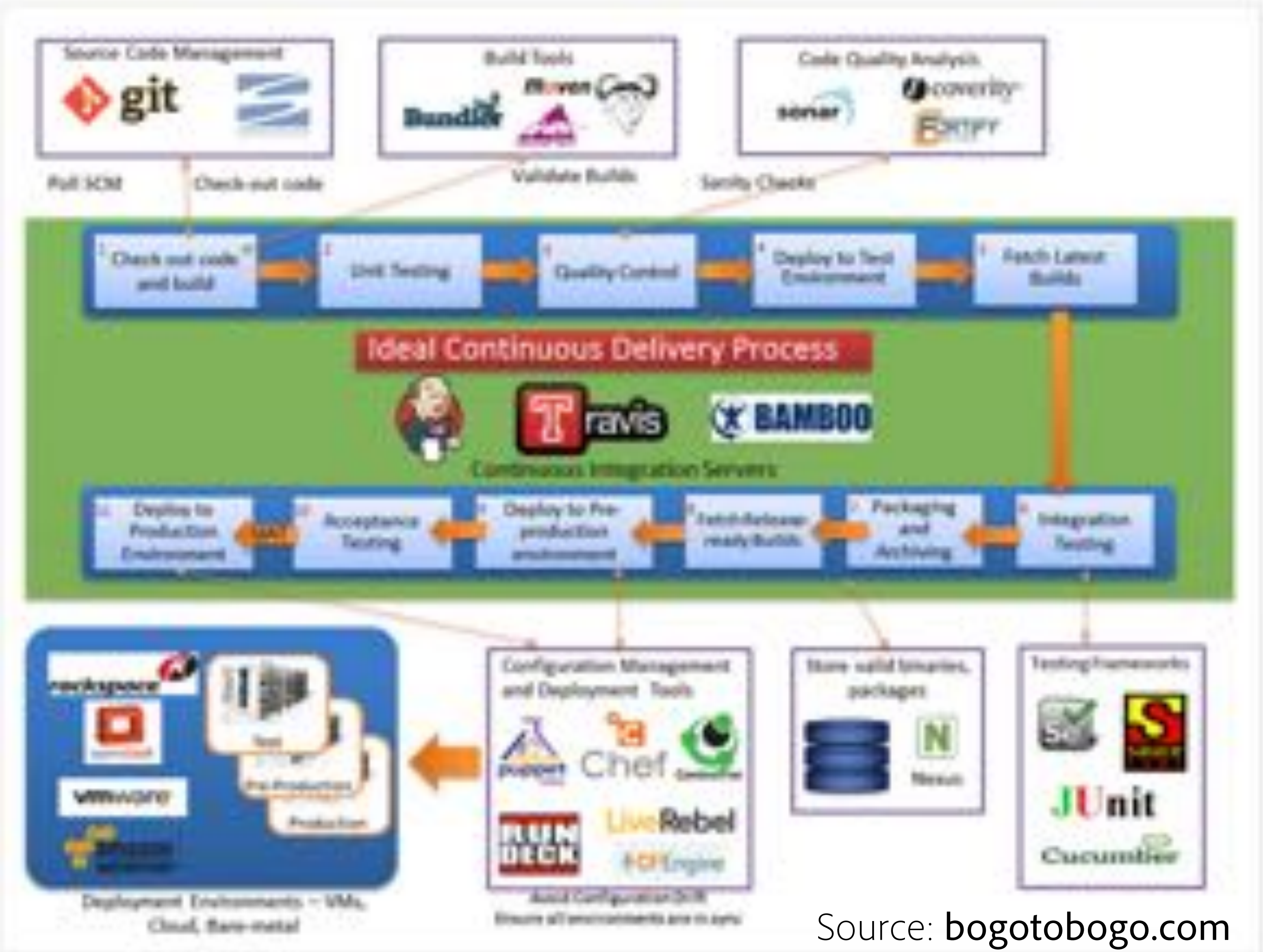
- ❑ Passed all prior gates/tests before production approval
- ❑ Low risk change
- ❑ No or low impact
- ❑ Peer review completed
- ❑ Stage validation passes
- ❑ Security review passes
- ❑ Final approval from named individual

Continuous Pipeline Change Process Diagram



Infrastructure compliance

- ❑ Access control
- ❑ Third party code
- ❑ Data governance



Source: **bogotobogo.com**

The three hard truths of continuous compliance

Completing the implementation is just the start – you aren’t done

You may not be solving the problems you want to solve

Compliance work is not optional

Thank you for attending!

dowczare@adobe.com ❖ @devopsmuse

Adobe. Transforming Digital Experiences for 30 Years.