Better Governance

Banking on Continuous Delivery

Tapabrata “Topo” Pal

Sr. Director &
Sr. Engineering Fellow

tapabrata.pal@capitalone.com
@TopoPal

- Developer
- DevOps Evangelist
- Product Manager of Shared Continuous Delivery Tools Platform
- Creator and core contributor of Hygieia DevOps Dashboard

Jennifer Brady

Director, Technology Governance

jennifer.brady@capitalone.com

- Former Audit Director
- Current IT Governance Director
- Responsible for both a control automation and data analytics team
- Work with Data Scientists, Data Engineers, and Developers

Capital One

Capital One

- Millions of accounts
- One of the largest Digital Banks
- #1 Information Week's Elite 100
- ~ 20 years old

Different DNA

- Build our own software
- Build on public cloud
- MicroServices
- Open Source
- Continuous Delivery


Capital One
by Capital One Services, LLC
149
Free to Enable
"Alexa, Open Capital One"


eno
from
CapitalOne

Capital One

https://github.com/capitalone

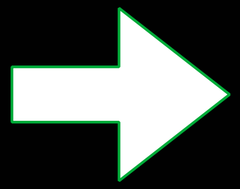
25 Projects

109 developers

12 teams

5 Year Journey

- Waterfall
- Manual Build
- Manual Deployment
- Manual Test
- Data Center
- Closed Source First



- Agile
- Automated Build
- Automated Deployment
- Automated Test
- Public Cloud
- Open Source First

Capital One

5 Year Journey

Mostly Out-Sourced	→	Mostly In-Sourced
Vertical Silos	→	Product Team
Dev, Ops, QA, RM	→	Engineers

- DOES 2014

  Building out Automation steps

- DOES 2015

  Scaling DevOps, Open Source, Cloud, Innovation

- DOES 2016

Measure, Improve, Mature

Capital One

2017 and beyond

- #SlayTheMonolith
- #NoFearRelease
- #YouBuildItYouOwnIt

#YouBuildItYouOwnIt

- YOU Coded It, YOU Build It
- YOU Built It, YOU Test It
- YOU Tested It, You Deploy It
- YOU Deployed It, YOU Own It

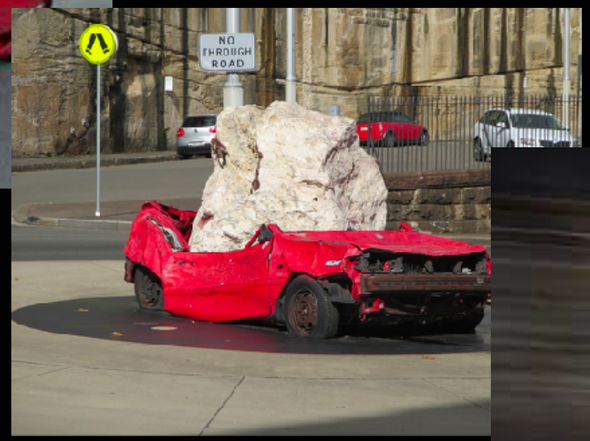
#NoFearRelease

- Fear of speed
- Fear of breakdown
- Fear of being out of control
- Fear of being non-compliant

We want this…

Capital One

And not this…



Safety in Continuous Delivery

Former Auditor's Perspective

Image Credit http://www.freepik.com
Designed by Freepik

And at Capital One…

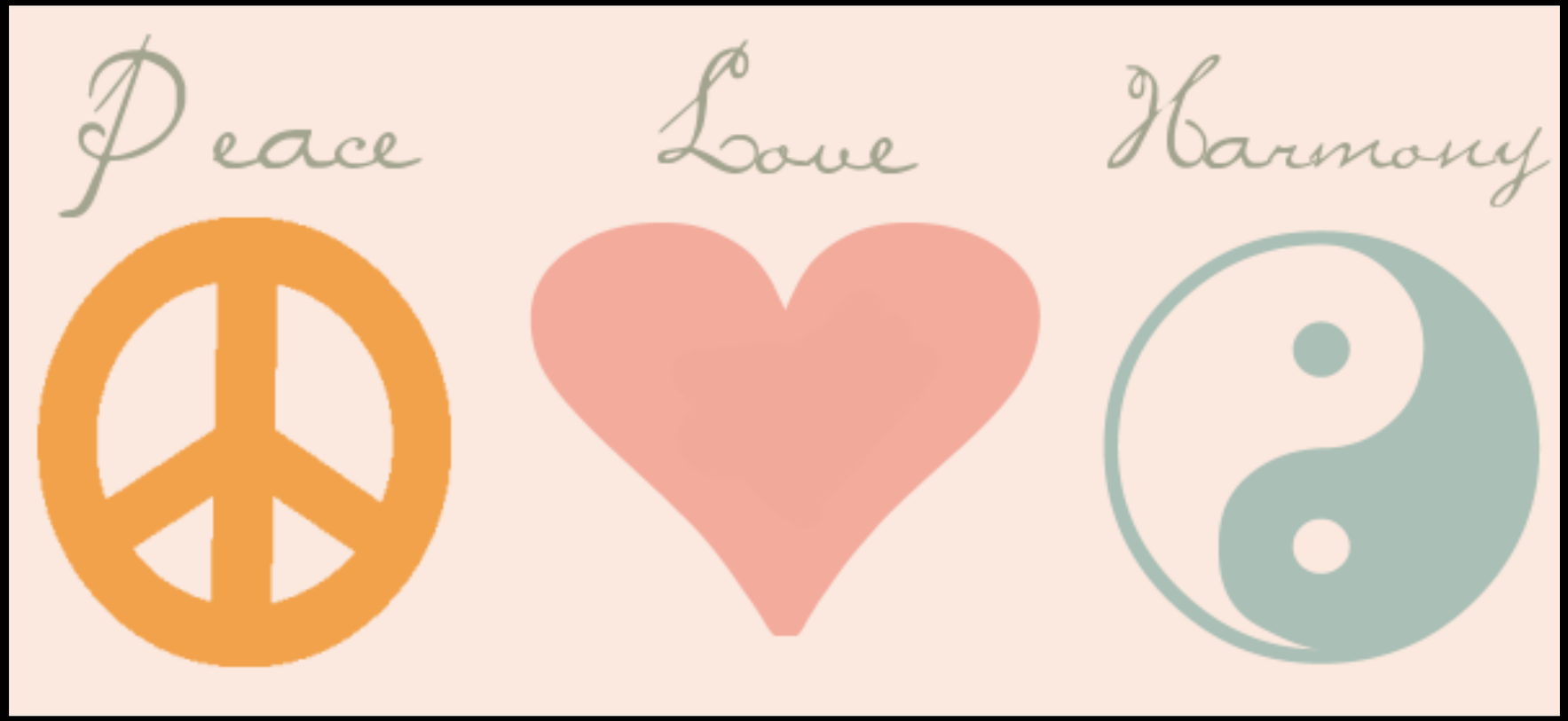


Image Credit: http://dkcoin8.com

Capital One

Compliance

~~Compliance~~

Governance

Compliance vs Governance

Compliance = Checking the box

Governance = Awareness of and active management of risk

Three Lines of Defense

- 1st Line : Who Owns the Risk
- 2nd Line: Sets Policy, Monitors the Risk
- 3rd Line: Independent Assurance

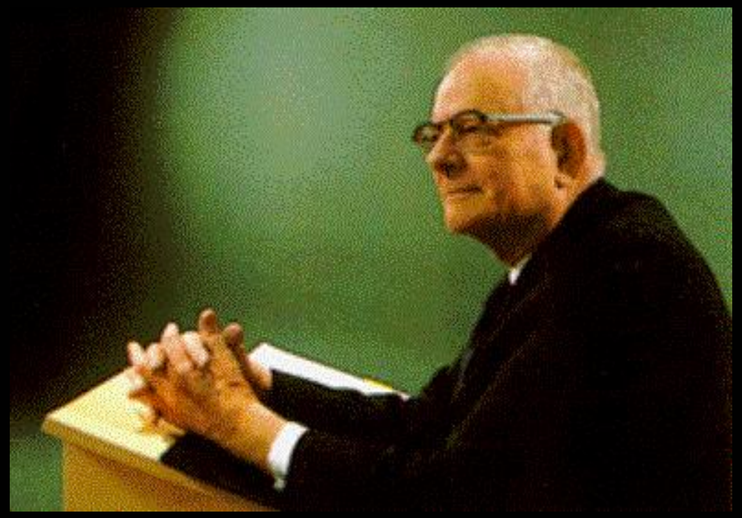
Capital One

What is the Developer's Role in Governance?

- Awareness
- Risk mitigation
- Follow control best practices

Why Controls?

- Controls are there to protect you and the company
- Provide assurance around financial reporting
- Provide comfort to investors



"Uncontrolled variation is the enemy of quality”

Capital One

Minimum Set of Controls

- Two Sets of Eyes
- Least Privilege
- Unauthorized Change Monitoring

Automation is easy, almost, such as…

- Build on every commit
- Static code analysis on every build
- Scanning for open source vulnerability
- Static security scan
- Automated tests
- ….

Biggest hurdle

Ensure that a single developer can not make changes to production bypassing all controls

Options

- Separate team managing pipeline
- Separate team just to perform production deployment
- Hire professional “button pushers”

Assumptions

- Enough “button pushers” available
- They cannot code
- Cannot train them to do anything else
- But, they should know if it is okay to push the button

Capital One

“the secrets of change is to focus all your energy not on fighting the old but on building the new”

Clean Room

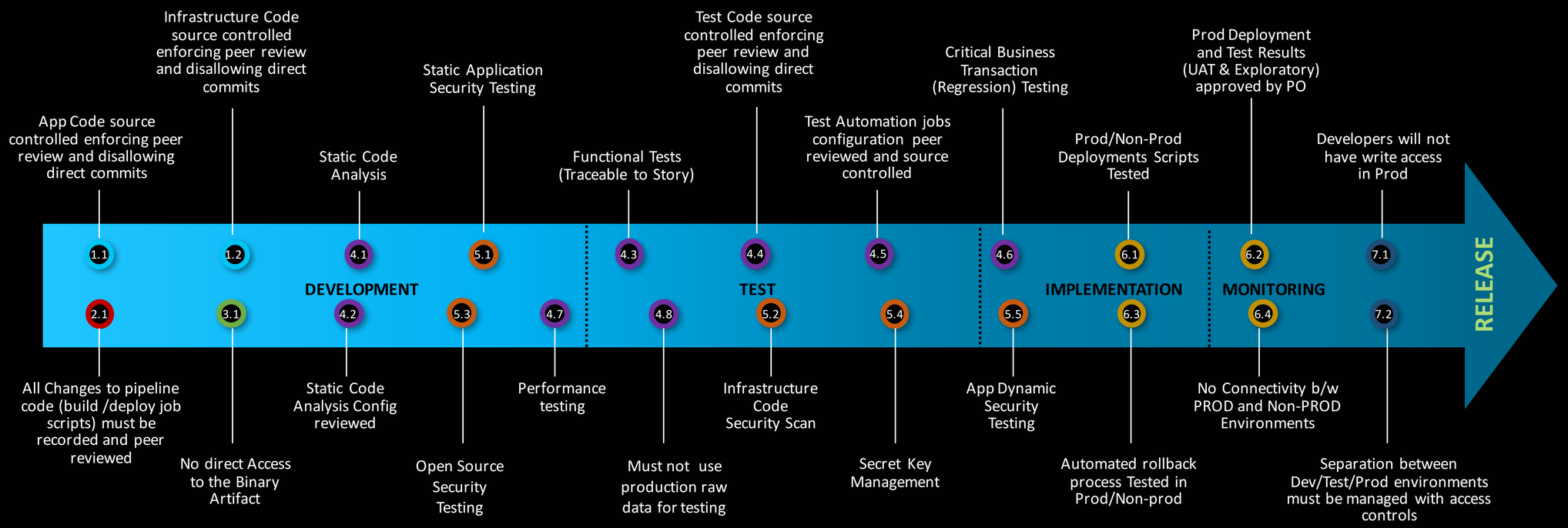
A clean room or cleanroom is an environment, typically used in manufacturing, including of pharmaceutical products or scientific research, as well as semiconductor engineering applications with a lower level of environmental pollution such as dusts, airborne microbes, aerosol particles and chemical vapors.

https://en.wikipedia.org/wiki/Cleanroom

Software Delivery Clean Room

- All product pipelines are identified and registered
- Everything is under source control
- Every change is peer-reviewed
- Production Changes occur only via code changes
- Nobody has access to production servers
- Every code change goes through various levels of testing and scanning
- Pipeline stops or alerts if things fail
- Evidences captured and evaluated at near real time
- Evidences are analyzed for discrepancies

Software Delivery Clean Room



1 Source Control

1.1 Application Code source controlled enforcing no direct commits to master/release without peer review

1.1 Infrastructure Code Source Controlled enforcing no direct commits to master/release without peer review

2 Build

2.1 All Changes to pipeline code (build /deploy job scripts) must be recorded and peer reviewed

3 Binary Repository and Application versioning

3.1 No direct access to the binary artifact

4.1 Build will be successful only if it passes static code analysis

4.2 Static Code analysis configuration is reviewed by the team and approved by PO

4.3 Every testable story must have corresponding test case/scenario/ step

4 Quality Checks

4.4 Test Code source controlled enforcing peer review and disallowing direct commits

4.5 Test Automation jobs configuration peer reviewed and source controlled

4.6 A core set of test cases that are considered critical (e.g regression testing) must meet the passing threshold defined by the team lead

4.7 Performance test results must meet the passing threshold defined by the team lead

4.8 Must not use production raw data for testing

5 Security Checks

5.1 Static Security scan/testing results are reviewed and approved by the PO or Tech lead for App Code

5.2 Security scan/testing results are reviewed and approved by the PO or Test lead for Infrastructure code

5.3 Open Source Security Testing (Build Artifact has ONLY approved libraries)

5.4 Secret key Management

5.5 App Dynamic Security Scan/testing results are reviewed and approved by the PO/Tech lead

6 Deployment

6.1 Prod/Non-prod Deployment scripts/configurations tested by the team

6.2 Prod Deployments and Test Results (UAT/Exploratory) must be approved by PO/Tech lead

6.3 Automated roll back process for production deployment must be tested in Prod and Non-prod

6.4 Must not have any connectivity or access between Prod and Non-Prod Environment

7 Support

7.1 Developers will not have write access in PROD

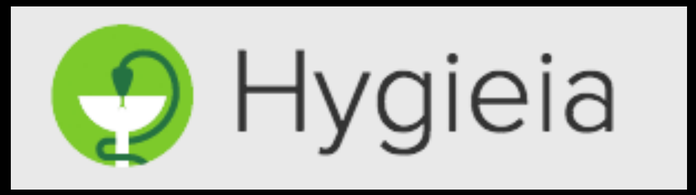
7.2 Separation between dev/test and prod environments enforced with access controls

Capital One

Result

	2016	2017
# Products deploying multiple times a day	~20	~300
Average #deployments per day	~1	~4
Max #deployments for a product in a single day	~30	~50

Automating Clean Room Monitoring



Audit API

https://github.com/capitalone/Hygieia/tree/master/api-audit

Capital One

Are you well managed if you are doing Continuous Delivery?

Are you well managed if you are **not** doing Continuous Delivery?


Thank You!
All of Chuck Norris's
Change Controls
are Full-Cycle...
and they're always
APPROVED!!!