Bank on Open Source for DevOps Success

Tapabrata “Topo” Pal

Sr. Director &
Sr. Distinguished Engineer

tapabrata.pal@capitalone.com
@TopoPal

- Developer
- DevOps Evangelist
- Member, Open Source Steering Committee
- Creator and core contributor of Hygieia DevOps Dashboard

Jamie Specter

Counsel

jamie.specter@capitalone.com

- Counsel, IP and Technology Legal
- Specializes on Open Source, IP, Information Governance
- Active participant in Women In Tech network

Capital One

Capital One

- Millions of accounts
- One of the largest Digital Banks
- #1 Information Week's Elite 100
- ~ 25 years old

Different DNA

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

Capital One

About 6 years ago

- Mostly out-sourced
- 100% Waterfall
- Manual Processes
- Slow
- Only Commercial Software
- Say No to Open Source

6 Year Journey

Mostly Out-Sourced → Mostly In-Sourced

Vertical Silos → Product Team

Dev, Ops, QA, RM → Engineers

Capital One

- DOES 2014

  Building out Automation steps

- DOES 2015

  Scaling DevOps, Open Source, Cloud, Innovation

- DOES 2016

  Measure, Improve, Mature

- DOES 2017

  Better Governance via Continuous Delivery

Capital One

Open Source

Over the last two decades, open source software has become widely adopted. In our survey, 58 percent of respondents agreed that their team made extensive use of open source components, libraries, and platforms, with over 50 percent agreeing that their team planned to expand use of open source software.

Elite performers are 1.75 times more likely to make extensive use of open source components, libraries, and platforms than low performers, and 1.5 times more likely to plan to expand their use of open source software.

About 6 years ago

- Mostly out-sourced
- 100% Waterfall
- Manual Processes
- Slow
- Only Commercial Software
- Say No to Open Source

Say NO to Open Source

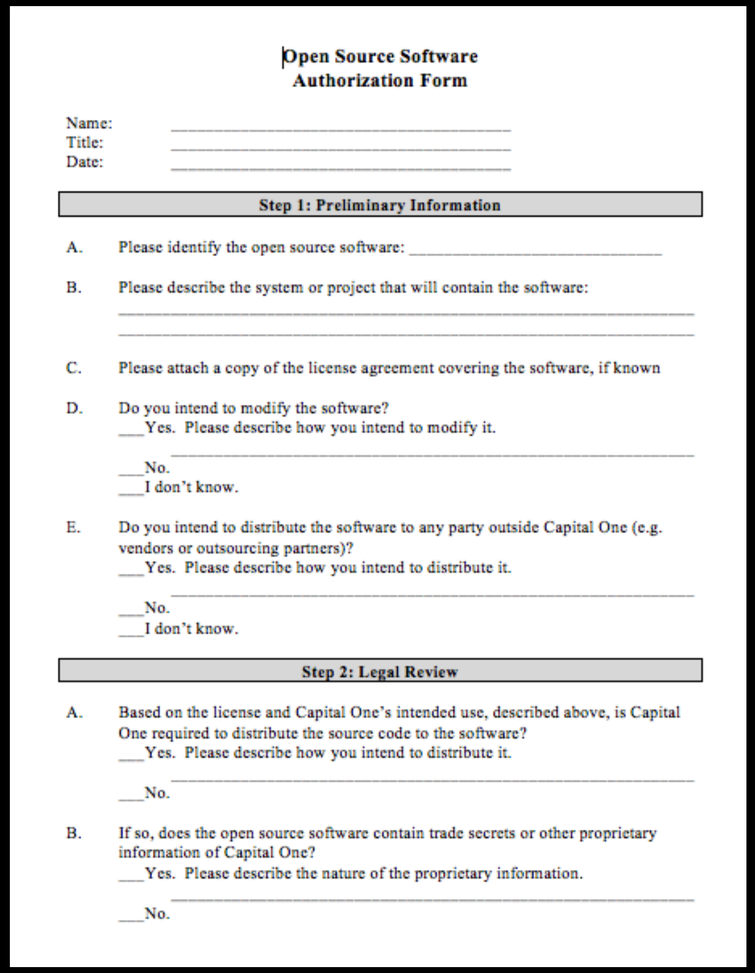
Use these instead:

2012 - Our First attempt at CI

Commercial SCM → Subversion

- Free tool?
- What if it breaks?
- Give our IP away?
- Someone stealing our code?

Open Source Approval Form



Open Source Software
Authorization Form

Name: _____
Title: _____
Date: _____

Step 1: Preliminary Information

A. Please identify the open source software: _____

B. Please describe the system or project that will contain the software:
_____
_____

C. Please attach a copy of the license agreement covering the software, if known

D. Do you intend to modify the software?
___Yes. Please describe how you intend to modify it.
_____
___No.
___I don't know.

E. Do you intend to distribute the software to any party outside Capital One (e.g. vendors or outsourcing partners)?
___Yes. Please describe how you intend to distribute it.
_____
___No.
___I don't know.

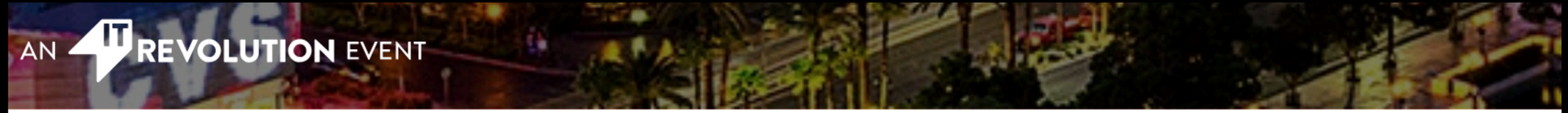
Step 2: Legal Review

A. Based on the license and Capital One's intended use, described above, is Capital One required to distribute the source code to the software?
___Yes. Please describe how you intend to distribute it.
_____
___No.

B. If so, does the open source software contain trade secrets or other proprietary information of Capital One?
___Yes. Please describe the nature of the proprietary information.
_____
___No.

@TopoPal

Capital One®



WHAT IS DEVOPS ENTERPRISE SUMMIT?

"give leaders the tools and practices they need to develop and deploy software faster and to win in the marketplace."

You take great care in writing code for your company

You do extensive due diligence in procuring commercial software

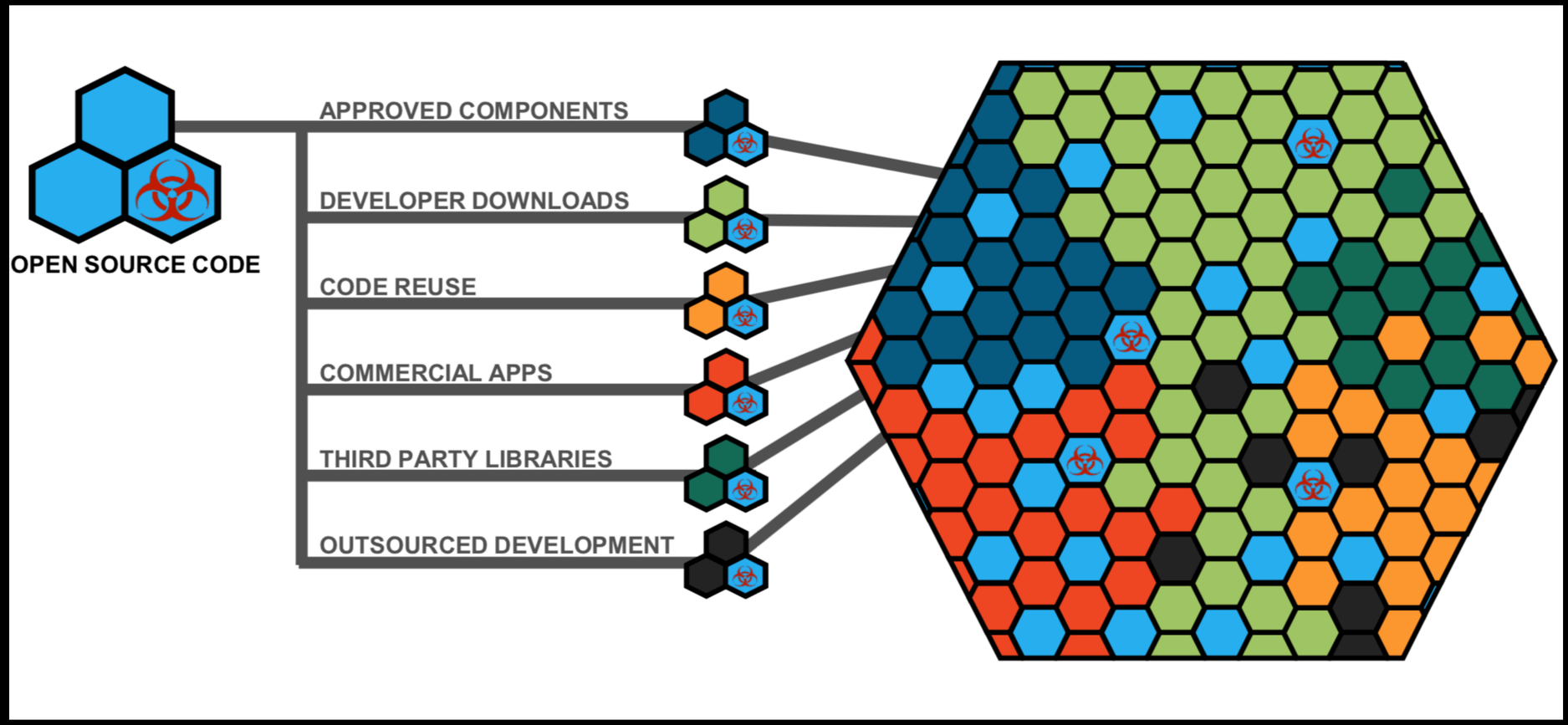
Why wouldn’t you treat Open Source you use with same care?

I bet you are using Open Source

96% applications contain Open Source

57% code base is Open Source

I bet you are using Open Source



https://www.slideshare.net/denimgroup/create-a-unified-view-of-your-application-security-program-black-duck-hub-and-threadfix

Capital One

Open Source is free as in "No Monetary Cost" and free as in "freedom".

But also… free as in puppy!

https://www.pexels.com/

Capital One

Risks: Security

2017: Over 4800 component vulnerabilities reported - 10% increase

2018: 134% increase in reported vulnerabilities per code base

Over 1500 days before fix

78% code base with at least one vulnerability

Average 64 vulnerabilities per code base

On an average, audit findings were disclosed nearly 6 years ago

- Developers are first line of defense
- Vulnerability can be found anytime
- Breaches will continue to increase
- Continuous Detection and Remediation

Remediation: Remove, Replace or Upgrade

Risks: License

85% code bases have license conflicts or unknown license

20% have copy left licenses

8% have weak copy left license

Over 2000 known open source licenses

- License = Permission and Rules
- Permissive vs Copy Left
- Respect developer rights - provide attribution
- Apply same source code license
- Make source code available
- Using AS-IS

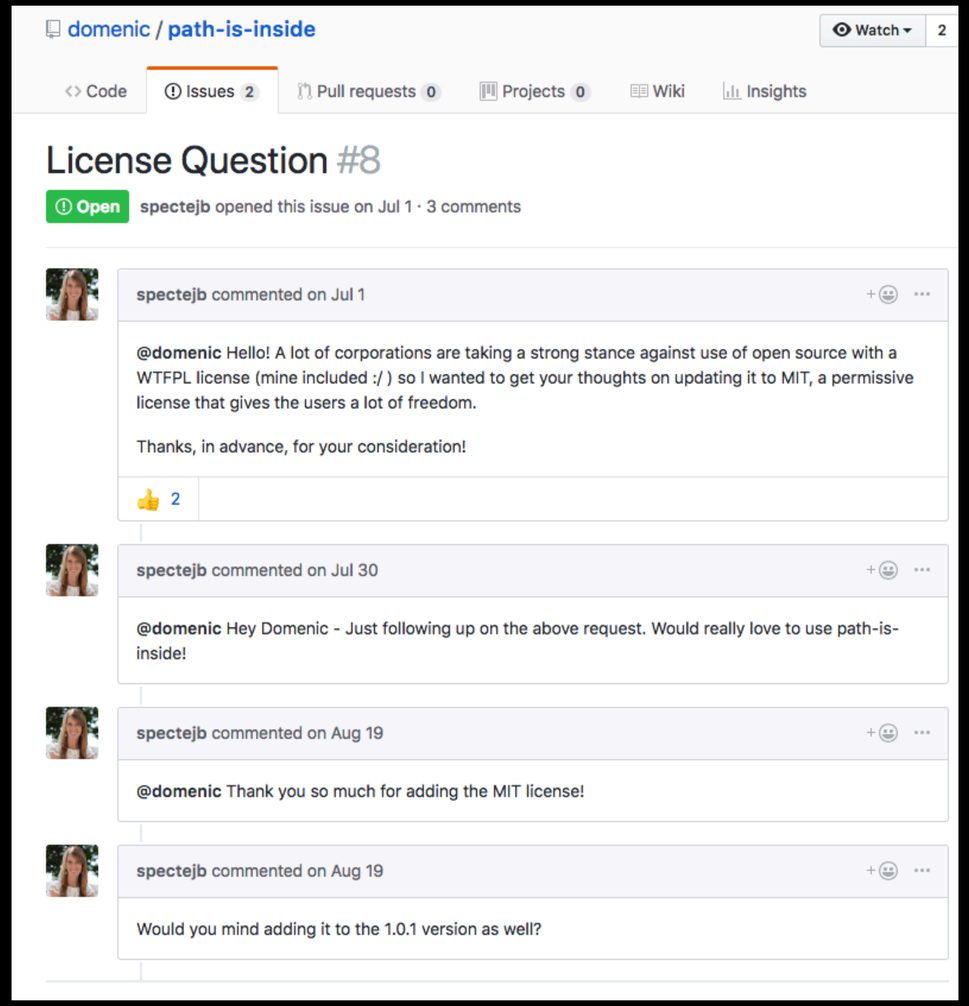
Remediation: Remove, Rewrite, Request change

Request Change!

@TopoPal

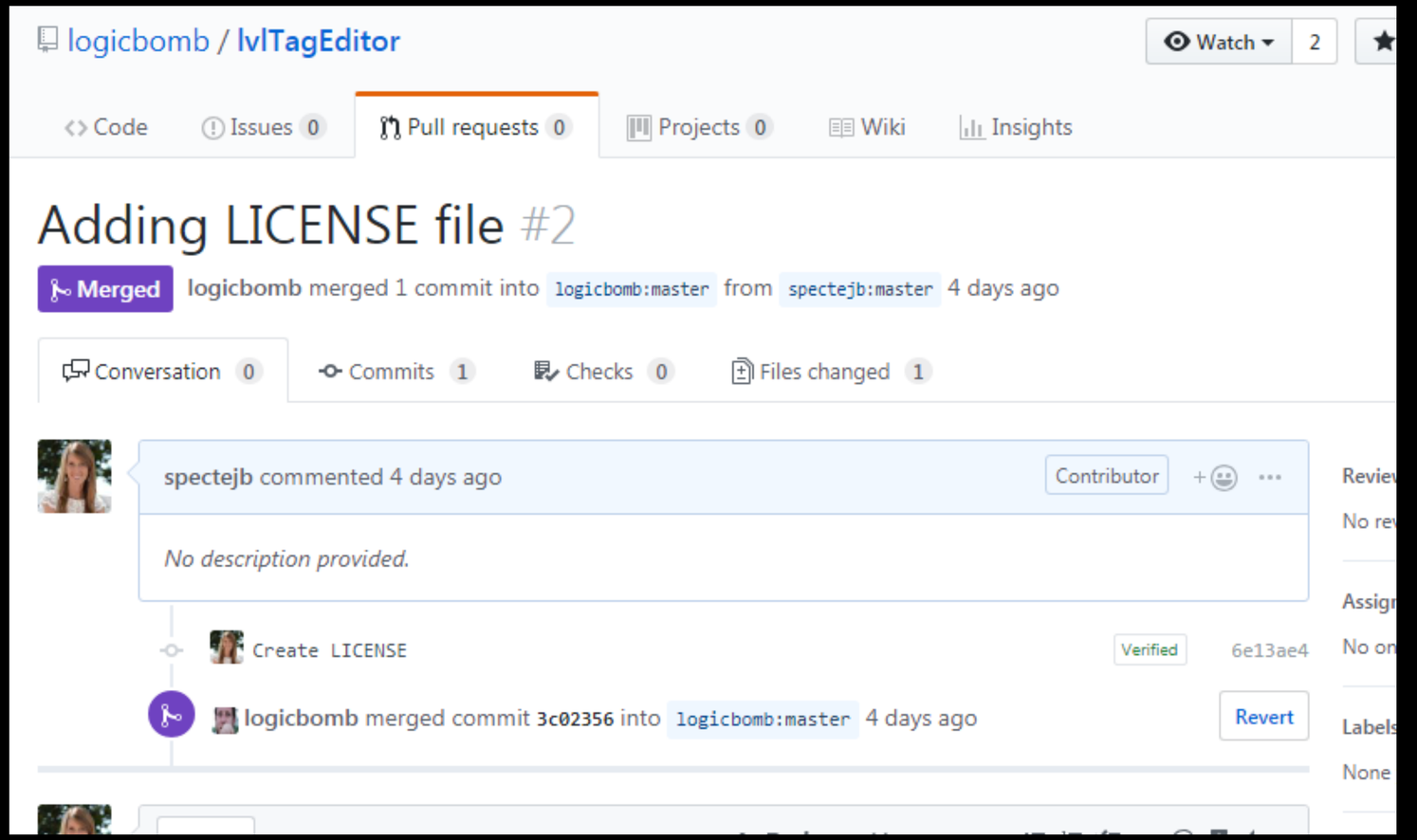
Capital One

Request Change!



Capital One

Request Change!



Capital One

Worst case scenarios

Trade Secret Disclosure

Required to give away proprietary source code

Security Threats + Potential Fines

Think “Heartbleed” (500,000 servers) and “Equifax” (148M+ people)

Devaluation of Patent Portfolio

Open source licenses include patent grants providing free licenses

Reputation Risks

Can impact sales and talent acquisition

M&A Impact

Negatively impact the value of your company or could prevent the deal completely

IP Infringement

Monetary damages and losing right to use open source software

@TopoPal

Capital One

JACQUELINE SCOTT CORLEY United States Magistrate Judge

ORDER RE: DEFENDANT'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Re: Dkt. No. 44

Plaintiff Artifex Software, Inc. brings breach of contract and copyright infringement claims against Defendant Hancom, Inc. arising out of Hancom's alleged breach of an open source software agreement. Hancom's motion for partial summary judgment on Plaintiff's breach of contract claim is now pending before the Court.[1] (Dkt. No. 44.) Having considered the parties' briefs and having had the benefit of oral argument on August 17, 2017, the Court DENIES Defendant's motion. Defendant has not established as a matter of law that it is entitled to judgment in its favor as to the relief available to Plaintiff on the breach of contract claim. // // //

Best Practices

- **Identify**:
  - Maintain Open Source inventory
- Analyze:
  - Track Open Source vulnerability
  - Track license terms
  - Report out findings
  - Prioritize by risk
- **Remediate**
- **Continuous Monitoring/Audit**

Mitigate with a Governance Strategy

- Open Source Policy
- Continuous Audit
- Governance - Technical, Legal, Security and Business
- Education and Training

Free resources:

https://opensource.google.com/docs/

https://todogroup.org/guides/

DevOps to Help

- Automation
- Shift-Left
- Frequent release
- Smaller batch size
- Collaboration & Transparency

You cannot do it alone

- Engineers
- Legal
- Security
- Risk office
- Anyone else you need

Capital One

Just using Open Source is not Enough!

Should Capital One contribute to Open Source Community?

Posted by Tapabrata "Topo" Pal in Enterprise Continuous Integration and Deployment on May 16, 2013 10:44:41 AM

@TopoPal

Capital One

Should Capital One Contribute to Open Source?

- It's against our policy.
- Why should we give our IP away?
- What are the legal implications?
- Who will use our software?
- What? Are we going to write another payment framework?
- What if we get a bad reputation?

Our Open Source Contributions

- 4 years
- ~ 90 developers
- 193 projects
- Examples: Angular, Ansible, Hadoop, Log4j, Spark, Chef, Commons, Consul, Fedora, FF4J, H2O, Jenkins, Kafka, Ngnix, Spring, Terraform, TensorFlow, Kubernetes

Our Open Source Projects

- 3 years
- 31 projects
- Most popular: Hygieia, Cloud Custodian

https://developer.capitalone.com/open-source/

Open Source

We're an open source first organization – actively using, contributing to, and managing open source software projects. Want to learn more about using, producing, and contributing to Open Source projects? We've put together a lot of Open Source information for you here.

Check out our GitHub page

Featured Projects

Cloud Custodian

Manage your AWS fleet with our Cloud Custodian rules engine. Cloud Custodian lets you define policies for a well-managed cloud infrastructure that's both secure and cost-optimized. It replaces many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

Learn more | View on GitHub

Hygieia

It's more than just Dev and Ops. If you are incorporating CI/CD into your organization's deployment process, keeping an eye on the overall health of your delivery pipeline is essential. Hygieia provides a nearly real-time, consolidated view of the health of entire delivery pipeline from build to test to deploy.

Learn more | View on GitHub

Projects by Category

Big Data ›

Tools to help manage and process complex data.

DevOps ›

Projects for developers and operations to work better together.

Dev Tools ›

Tools to help you work more efficiently and deliver higher quality solutions.

Framework ›

Streamlining processes within your existing framework.

Reference Apps ›

See how our APIs are being used in the real world

Top 5 reasons we use Open Source

- Culture of Collaboration
- Innovation and speed to market
- Quality
- Open Standards, Extensible
- Engineering Skills

Business Benefit

“Using Open Source software gives us numerous advantages from a business perspective. Open Source gives us the ability to re-use what already exist and work well, with full flexibility to customize and/or contribute back what we need for our business. It also means that we are inherently building with technology that a broader community is investing in, dramatically reducing the likelihood that we are relying on end of life tech as well as making us more permeable to the larger talent ecosystem."

John Schmidt, Product Manager

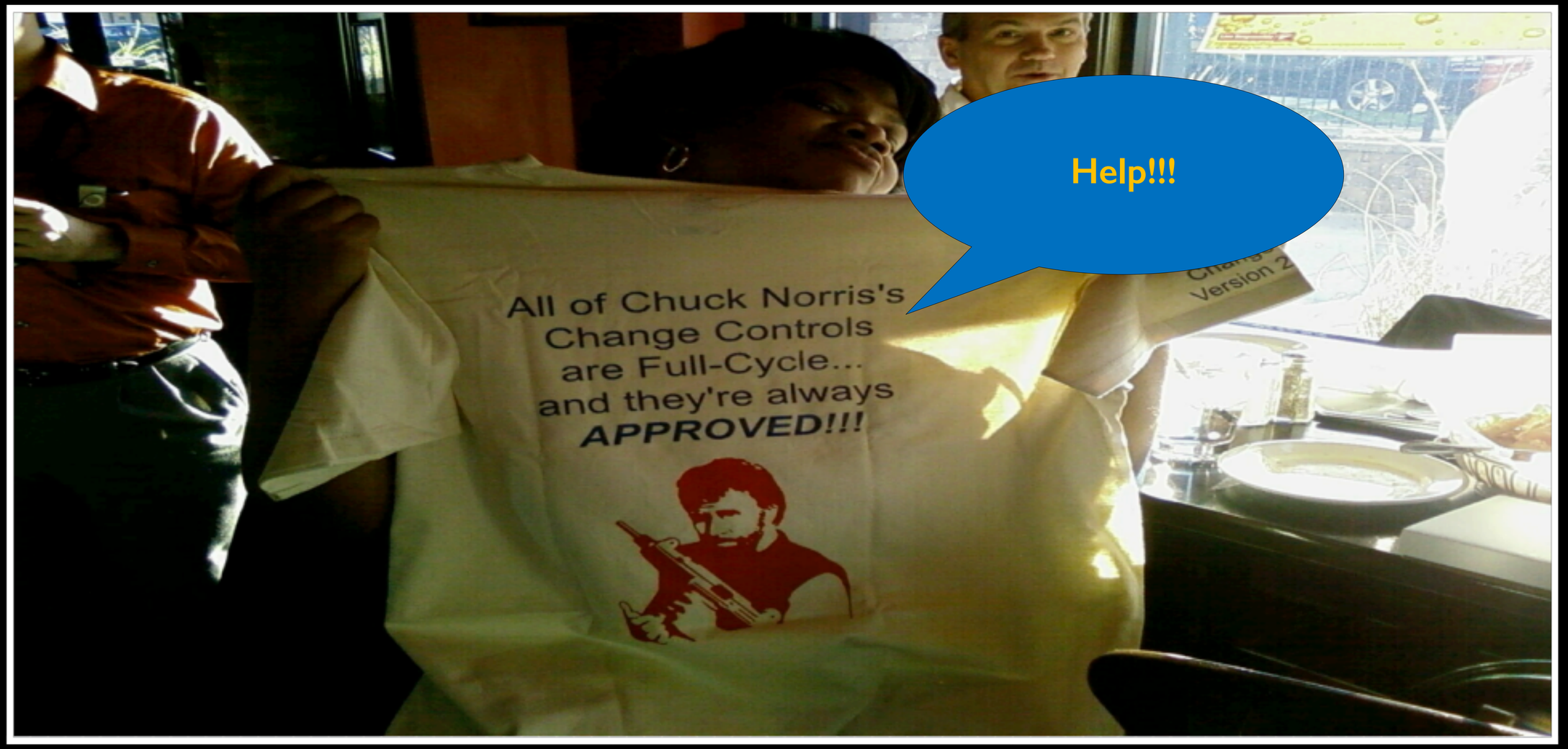
Approval process: Create good engineering experience

- Make it easy
- Streamline
- Automate
- Collaborate
- Engineering Experience

Capital One

#DevOpsHashtags

#YBYO
#YBYS
#MVC
#GTGF
#JFDI


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