RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **DSO-R09**

How to GRC Your DevOps

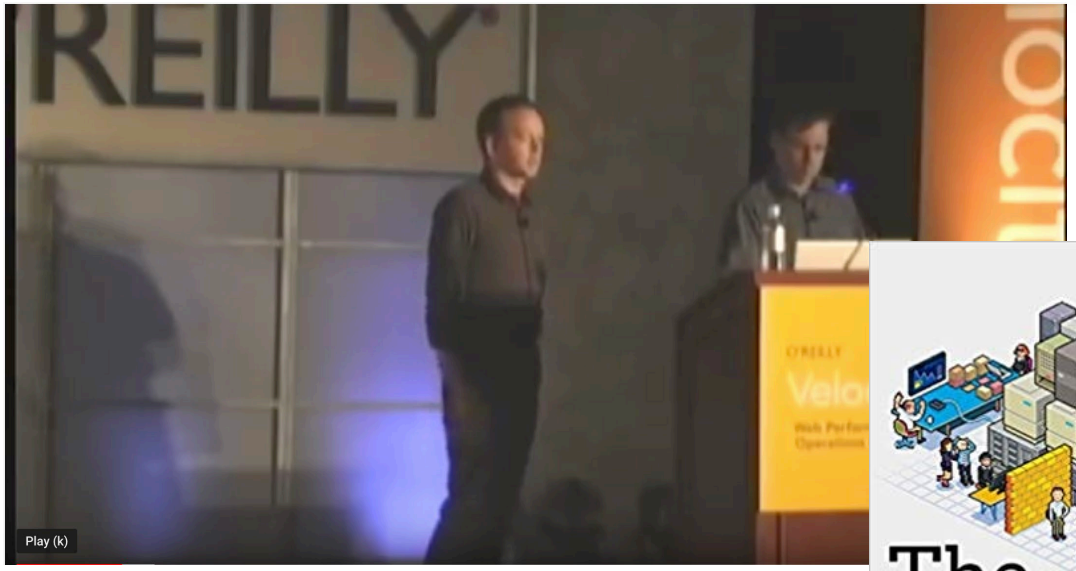
Susan Allspaw Pomeroy

Technology Compliance Manager
Fastly, Inc.
@sueallspaw

A Story

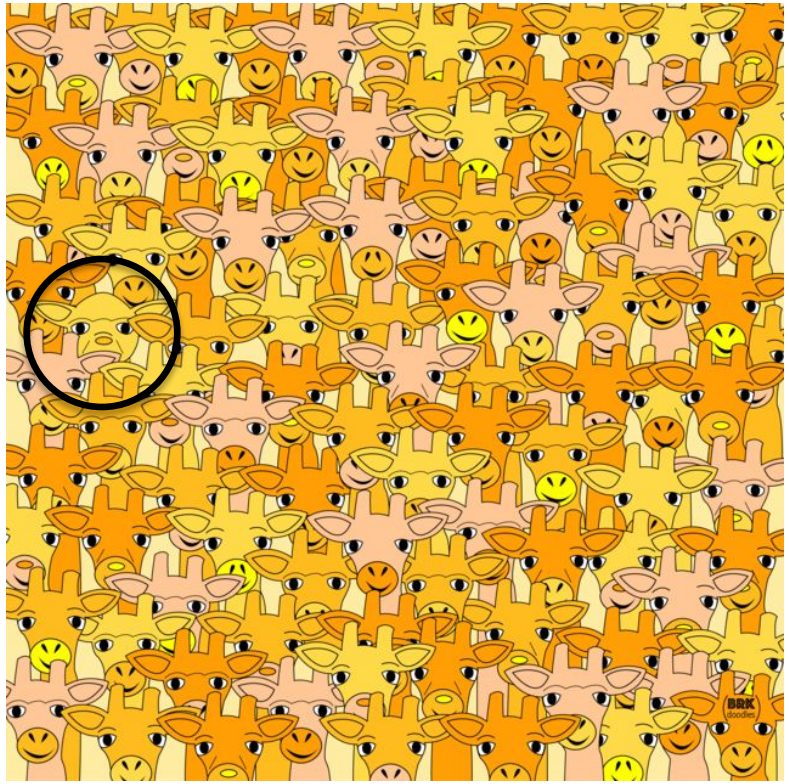

CHANGE CONTROL
REQUIRES MANAGER APPROVAL!
PEER REVIEW
AND AUTOMATED TESTS

A Brief History of DevOps Part 1



DEVOPS DAYS

DEV SEC OPS DAYS



Where's GRC?

James Wickett Retweeted

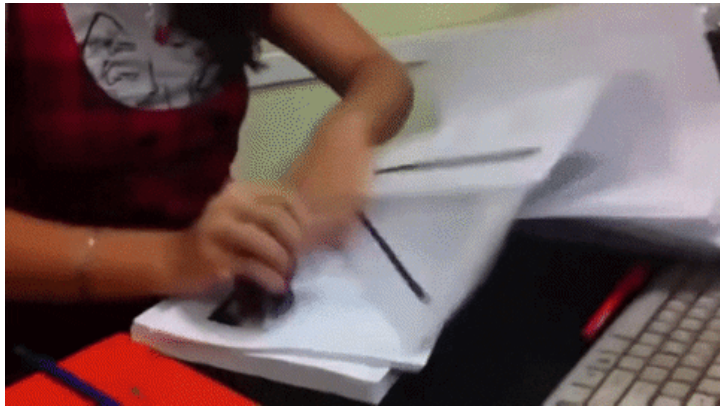
James Wickett
@wickett

How do we get GRC (Governance, Risk, and Compliance) folks involved with DevOps (or DevSecOps) movement? Is this an unachievable thing or is it possible? Looking for who is having success at it and how. Would also love advice on books, tools, or other.

2:08 PM · Sep 17, 2019 · Twitter Web App

What we think we do

What engineers think we do



What I'm here to tell you today

- DevOps and GRC collaboration makes audits smoother and engineers happier
- Traditional views of controls can (and should) change
- Calibration of how things work is the foundation of DevOps and GRC collaboration

A note on terminology

- Auditor, IA, GRC, compliance
- Software Engineer, Ops Eng, SRE
- Security team

Compliance Frameworks

(they're good for you)

Security Frameworks Are Your Friends*

- FLEXIBLE to your business
- Enable engineering teams
- Utilize basic security tenets you want to do anyway

*Not always

Security Frameworks Are Awful*

- Have the capability to create business slowdowns
- Can be interpreted as RIGID
- Make paperwork

*Not always, either

What we want (auditor version)

- Effective security controls
- Evidence of security controls
- Repeatable processes

What we want (engineer version)

- Stable systems
- Ability to improve/respond to unstable systems quickly
- Common systems understanding
- Visibility into our systems

What we want (security version)

- Well-tested code
- Visibility to unusual activity
- Rule-following

The Difference?

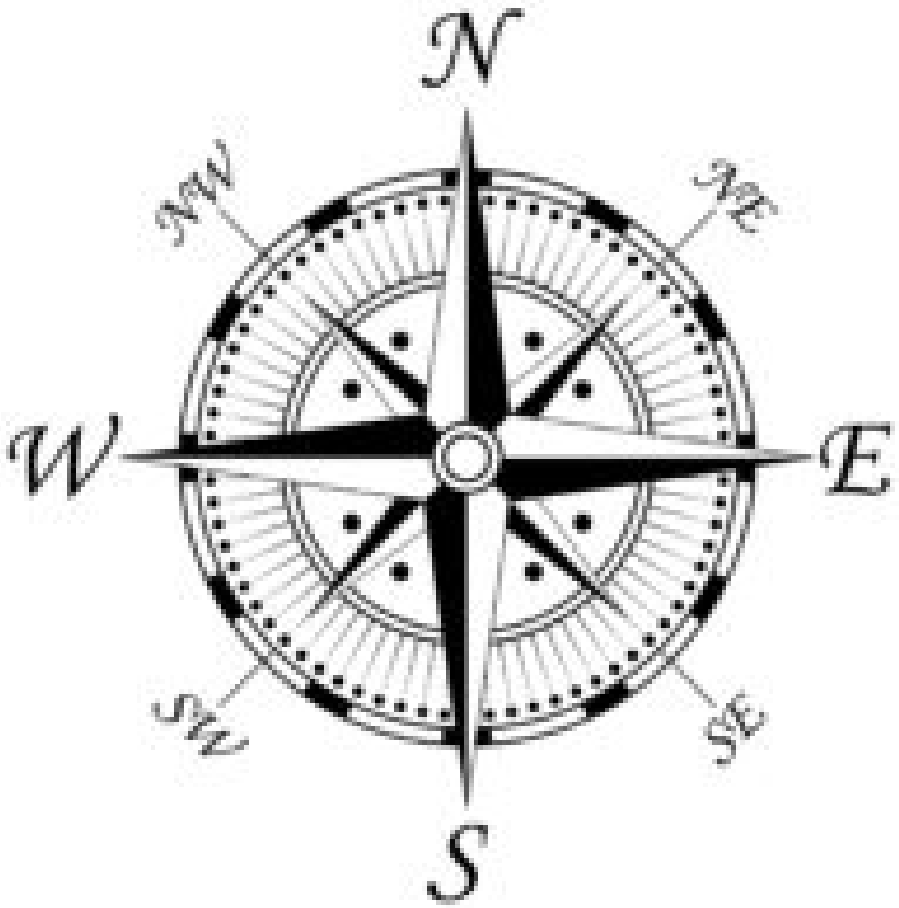
Things we all want:

- Resiliency
- Visibility/Response
- Quality

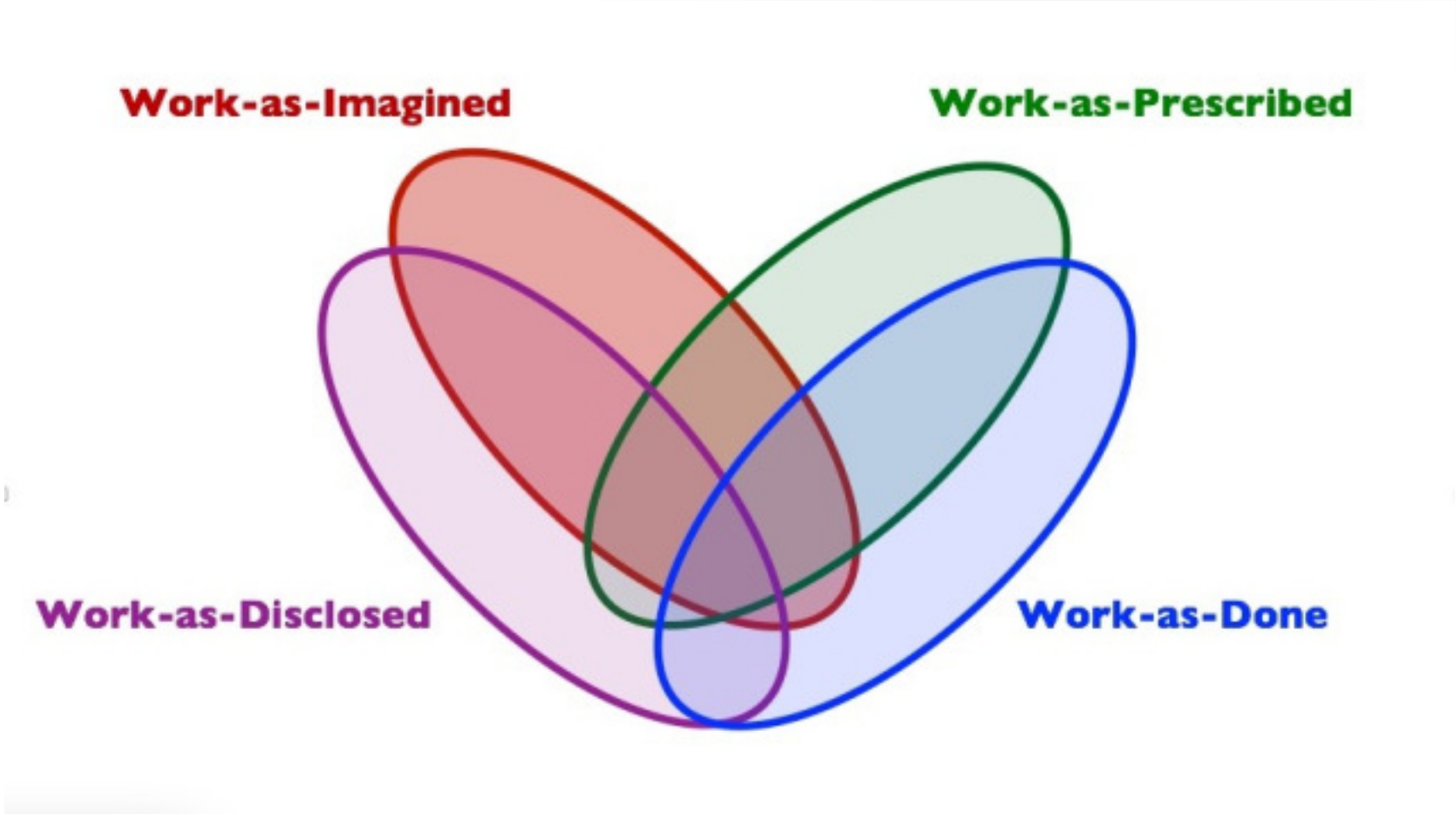
How we want it:

- Auditable/not auditable
- Fast/Methodical
- Perfect/Good enough

To Make Our Jobs Easier

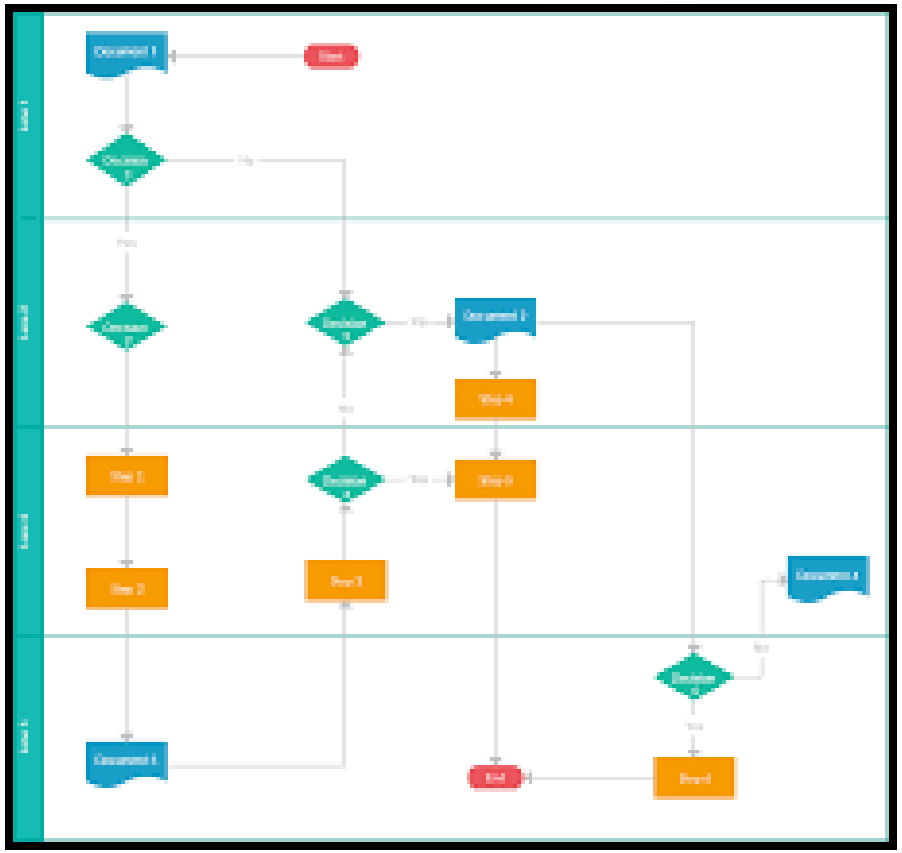

N
NW
NE
W
E
SW
SE
S

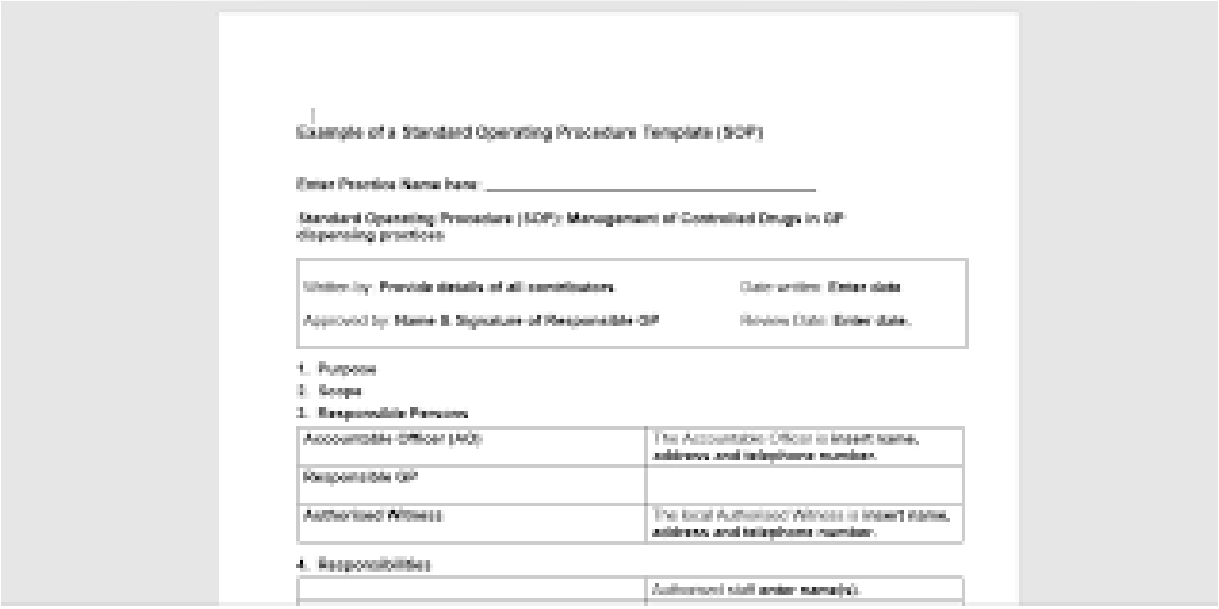
Mental models of how things work



https://safetydifferently.com/the-varieties-of-human-work/

Work-as-Imagined





Example of a Standard Operating Procedure Template (SOP)

Enter Practice Name here: _____

Standard Operating Procedure (SOP): Management of Controlled Drugs in GP dispensing practices

Written by: Provide details of all contributors	Date written: Enter date
Approved by: Name & Signature of Responsible GP	Review Date: Enter date.

1. Purpose
2. Scope
3. Responsible Persons

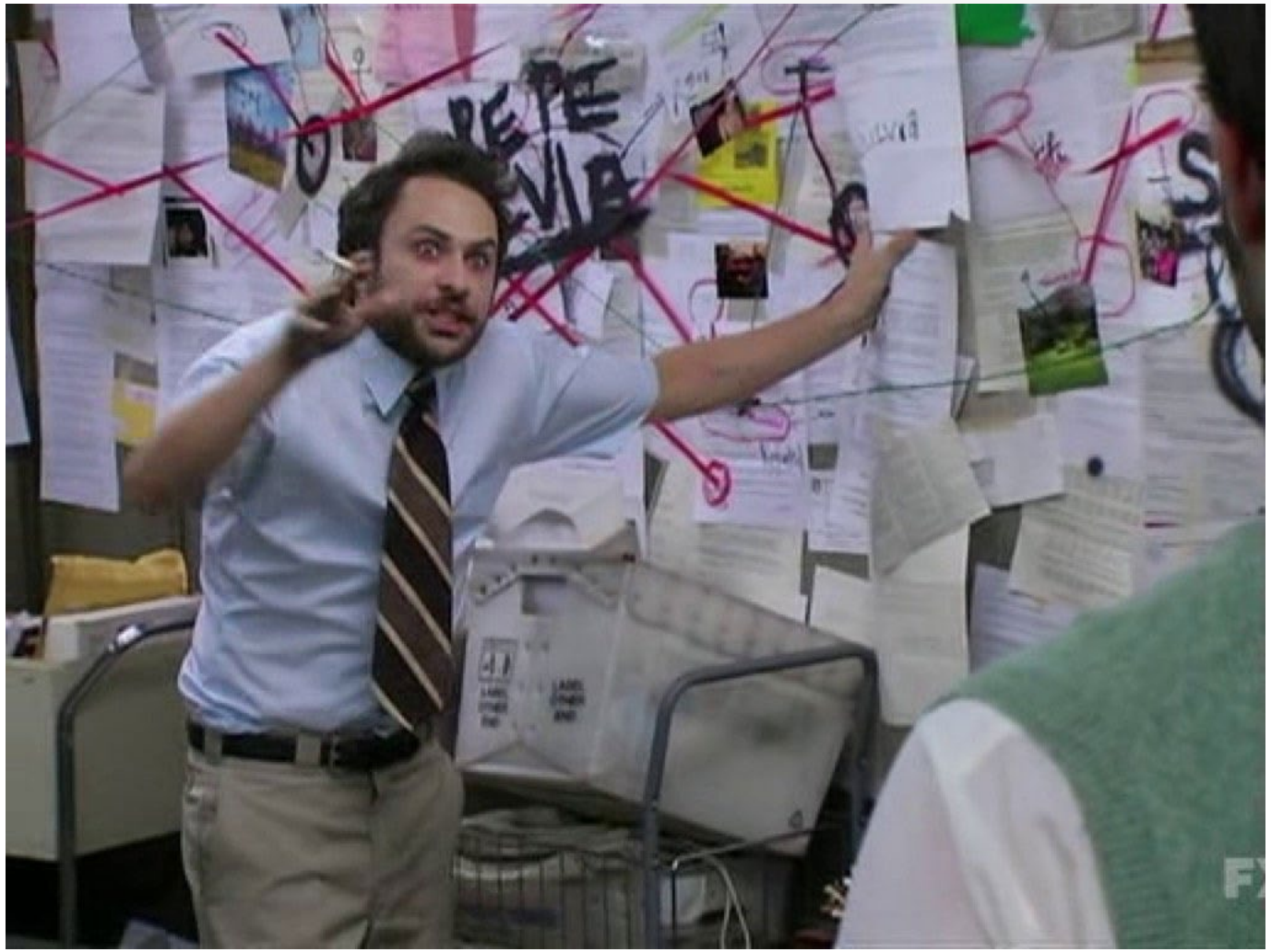
Accountable Officer (AO)	The Accountable Officer is insert name, address and telephone number.
Responsible GP	
Authorised Witness	The local Authorised Witness is insert name, address and telephone number.

4. Responsibilities

	Authorised staff under name(s).

Mental models of how things work

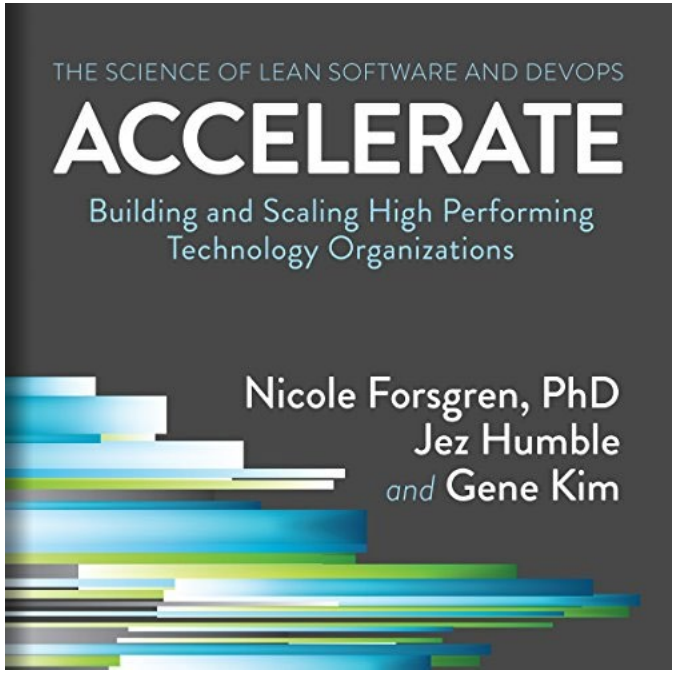
Work-as-Done

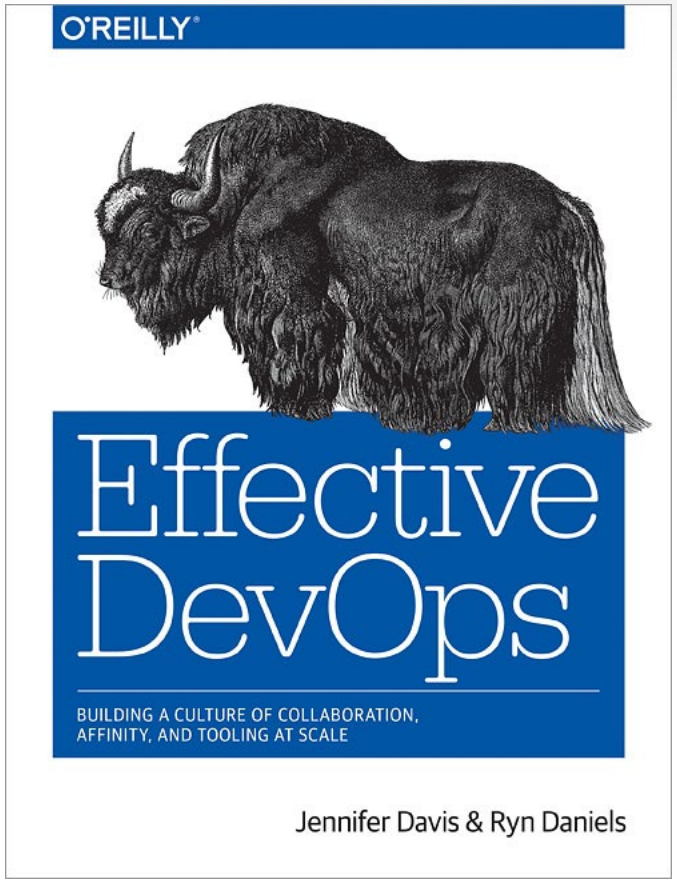


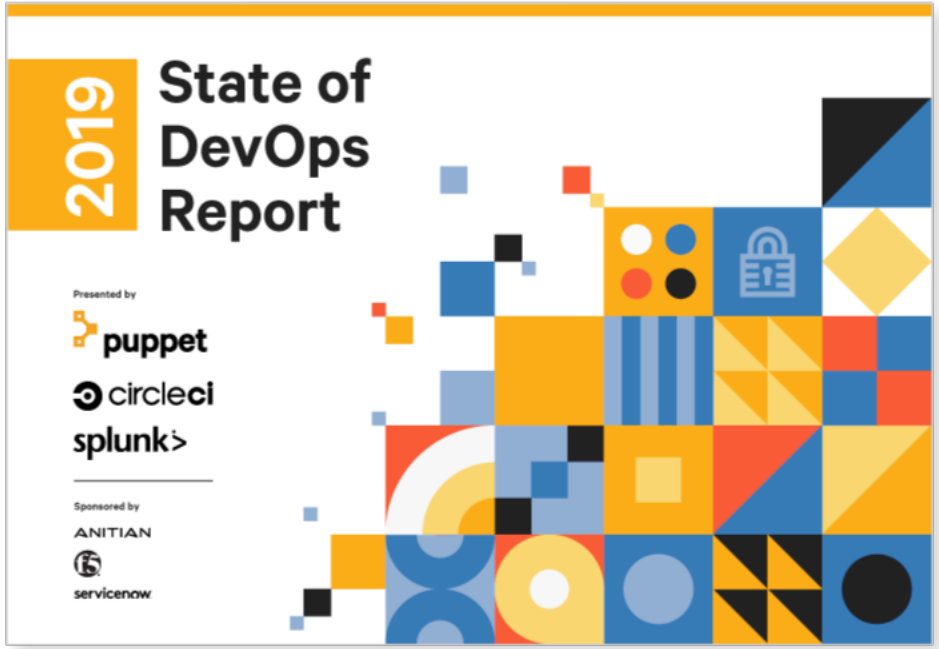
"Procedures are an investment in safety—but not always. Procedures are thought to be required to achieve safe practice—yet they are not always necessary, nor likely ever sufficient for creating safety."

--Sidney Dekker

A Brief History of DevOps Part 2







GRC evolution

- SAS70>>SSAE-16>>SSAE-18
- HIPAA/HITECH/HITRUST
- SOX
- FISMA/FEDRAMP

What is the risk you're trying to mitigate?

What are your goals for this process/control?

Reasonable Assurance

Timely Detection

The best security tool


Jessica DeVita
@UberGeekGirl
"the safest aircraft never flies, the safest anesthesia is never given... All operators in risky domains must find and adjust the balance between acute "faster-better-cheaper" goals... and chronic goals such as safety"
Morel, et al., 2008 ncbi.nlm.nih.gov/pubmed/18354967
3:45 PM · Jan 5, 2020 · Twitter Web App

Study: Separation of Duties

Separation of Duties

What it is:

According to NIST, “Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.”

(the problem with) Separation of Duties

(the problem with) Separation of Duties

- Has always been assumed to require multiple humans as primary operators of functions
- To security/compliance, separation of duties is a good thing.
- To engineering, it's a slow-down, and a risk to system resiliency.

(the problem with) Separation of Duties

In an outage, I have to be able to fix the system without a whole lot of people. I have to be fast.

If we can't move quickly, we can't beat our competition to solve that customer problem.

We have to have separate people develop and deploy. Regs say so.

If we get a finding, we'll lose the trust of our customers. But if the systems are down, we lose it, too.

(the problem with) Separation of Duties

- Malicious compliance
- Check box compliance

higher business risk

Separation of Duties

What’s the risk you’re trying to mitigate?

Separation of Duties (trust)

How can we be ok with engineers deploying their own code?

- Trust that engineers use their expertise to adapt (there are controls for this!)
- Create a safe, transparent environment (psychological safety is imperative)

Separation of Duties

Separation of Duties (verify)

- Transparency (logs, evidence, artifacts) and visibility (smart notification/review)
- Tools and People
  - Utilize CI/CD pipeline for deployments (and have logs!)
  - People (and tools) for code review
  - Security review on anomalies

Other Controls

Change Management

- Automated testing/deployment
- Automated configuration management
- Enforced peer review
- Break-glass solutions

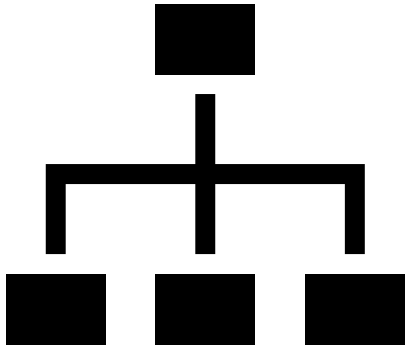
Other Controls

Access Management

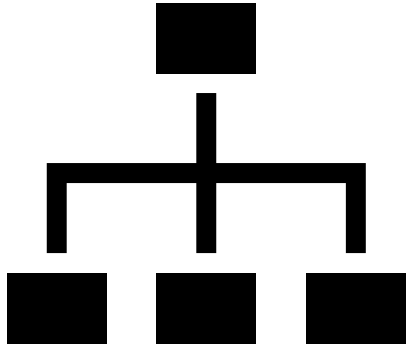
- Pre-approvals on standard access based on role
- Access changes following change management
- Single sign-on and 2FA
- Automated access termination

Communication

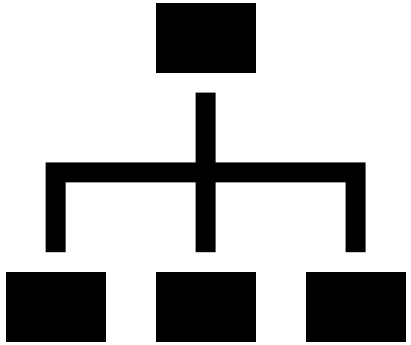
Communication



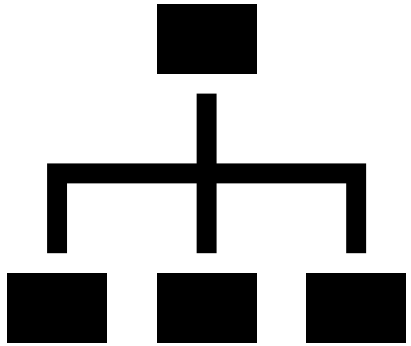
Compliance/IA



Eng/Ops/Internal Tools



Security



Eng/Development

(the challenges with) Communication

- Information is shared… among managers
- Work for audits is requested without context
- “I don’t have time to meet with (Compliance/Engineering)!”

Communication

- Make friends with your compliance/IA teams
  - Invite compliance to product meetings, engineering planning meetings, Engineering all hands, etc. (Auditors: GO TO MEETINGS!)
- Establish common ground
  - What do engineers know about your security controls/frameworks?
  - What do auditors know about the systems/eng processes?
  - What will make their jobs easier?
- Establish workable internal checks
  - Recurring monthly/quarterly ticket generation

Communication

- Have an Infrastructure product manager? Invite them to audit planning meetings.
  - (don't have an Infrastructure PM? Watch this talk and get one!)
- Share your controls matrix with Engineering. Publicize it.
- Ask to go to product meetings.
- Eng: Make communication with Compliance part of your performance review/goals.

What Now?

Apply What You Have Learned

Next Week:

- Set up a tea/virtual tea meeting with your counterparts (IA/Compliance, meet up with at least one Engineering manager)
- Share your controls matrix with Engineering. Invite questions.

Apply What You Have Learned

Next Month:

- Whiteboard the deployment process with engineers who manage deployment tools.
- Revisit your change management, access management, SoD controls to see if they need to change.

People’s ability to adapt to adverse situations are your greatest security control.

References

"Failure to adapt or adaptations that fail: contrasting models on procedures and safety" Sidney Dekker

"DevOps and Product Management Together at last and kicking butt," James Heimbuck

"10+ Deploys per Day" (John Allspaw and Paul Hammond)

"Malicious Compliance," Sidney Dekker, Hindsight 25

"Can We Ever Imagine How Work is Done?" Erik Hollnagel, Hindsight 25

References

"The Varieties of Human Work" Steve Shorrock

"Articulating the differences between safety and resilience: the decision-making process of professional sea-fishing skippers." Morel, et. al.