DevOps In a Highly Regulated Environment

Aiming high like a 🦄 in skates

Marc Cluet (@lynxman)

Who am I?

Twitter @lynxman

Partner SE at Hashicorp

Previously DevOps instigator at Rackspace, Trainline, Canonical, ASOS, DevOpsGroup, Nationwide Building Society

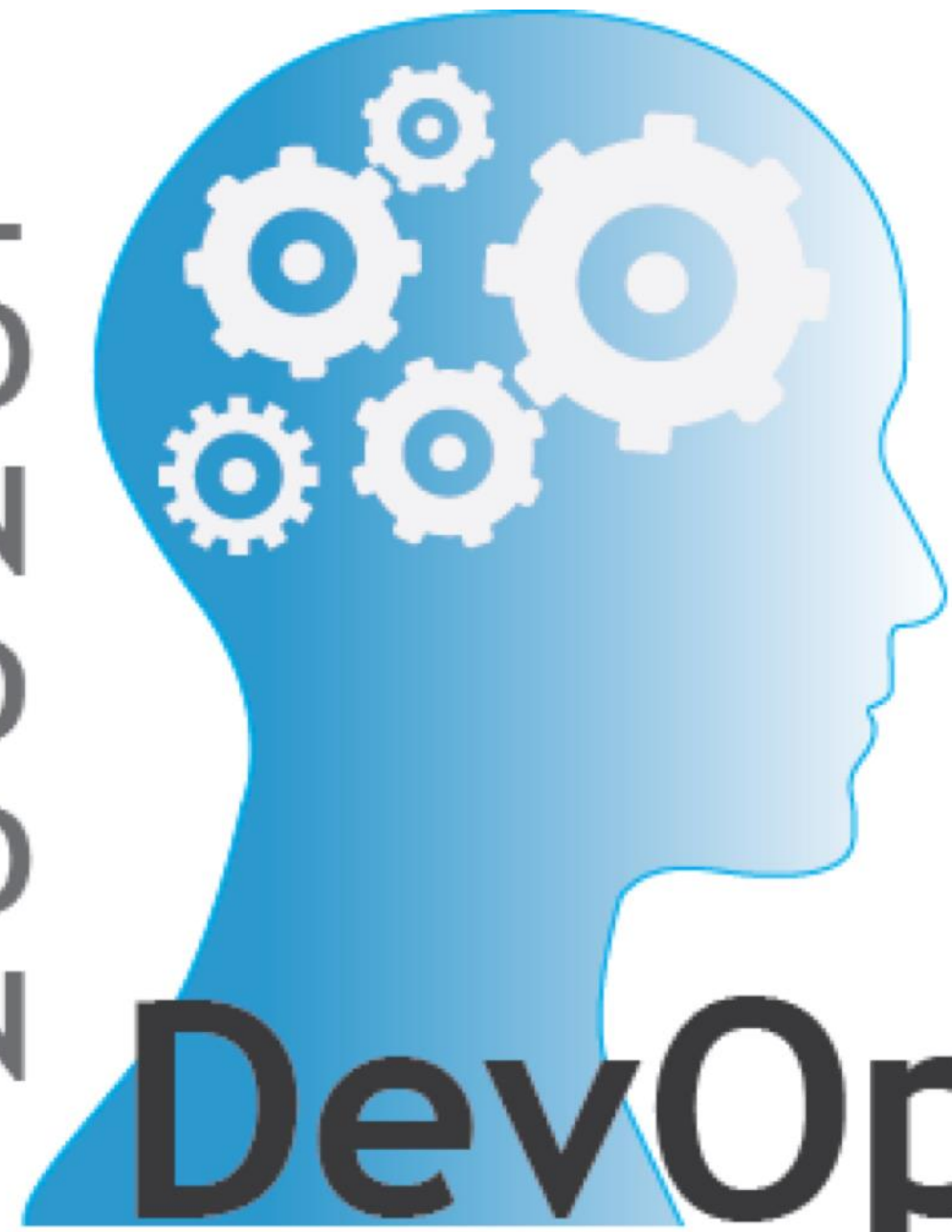Been DevOps'in for way too long… I need a coffee

Likes to swear a lot

UK

Dec 4th 2020

What is Nationwide

What is Nationwide

- Building Society started in 1846
- Largest building society in the world with over 15 million members
- Second biggest provider of household savings and mortgages in the UK
- Assets of over £200 billions

Which services Nationwide provide?

Mortgages

Savings

Current Accounts

Who regulates Nationwide?
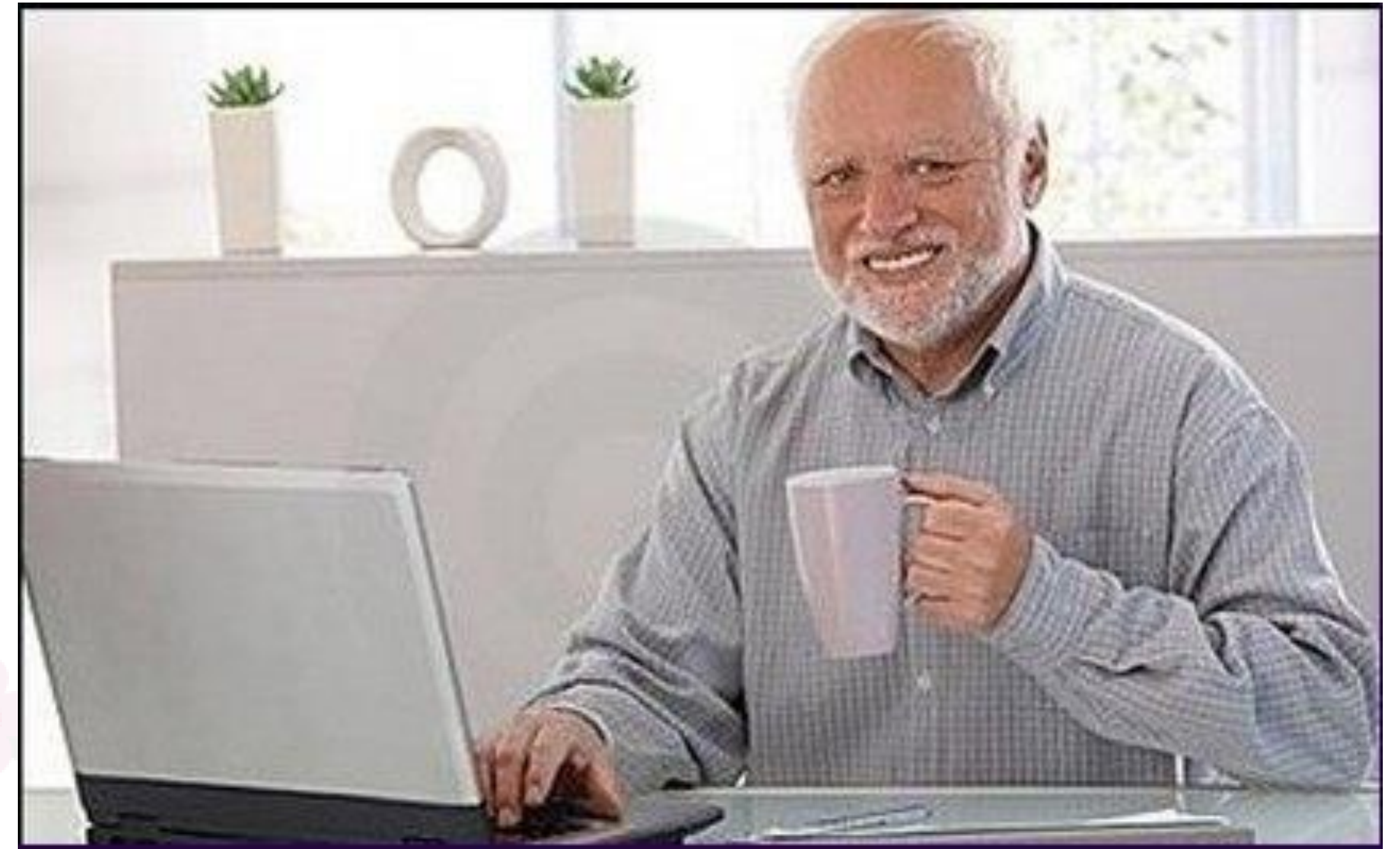
Infrastructure legacy

Infrastructure legacy

- Several data centres across the UK
- All kinds of hardware vital for everyday banking
  - Mainframes! Yes we have them!
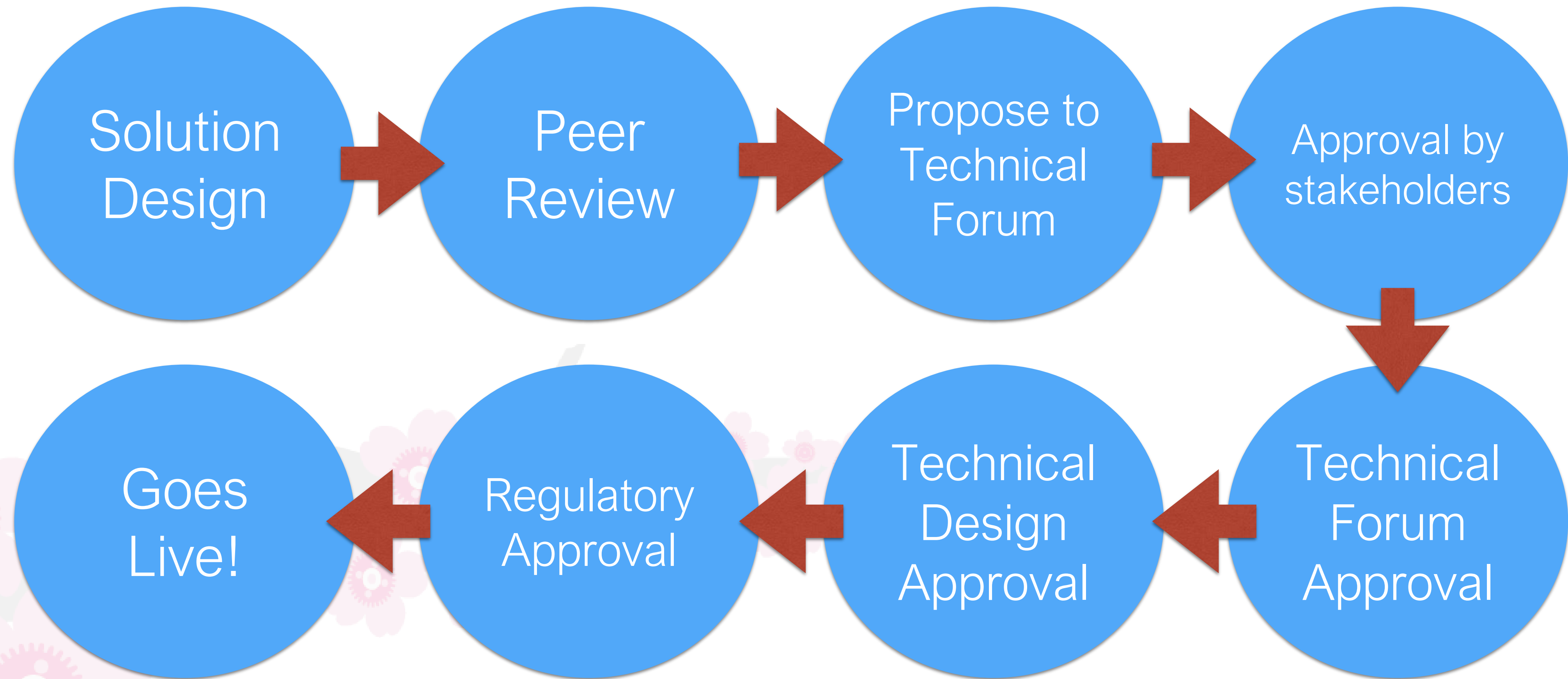 - Server state that has been operating for many years

Governance, Risk & Control

- All designs and software need to be based on evidence
- Evidence available for Governance, Risk & Control
  - Which includes the regulator as well
- Approval process crafted to ensure compliance
- All data tightly classified and controlled

Governance, Risk & Control

Launching full DevOps

Challenges

- Engineering not confident enough in Agile & DevOps
- Upskilling in new technologies necessary
- Need to maintain levels of controls for Risk & Governance
- Need to increase speed of innovation to succeed
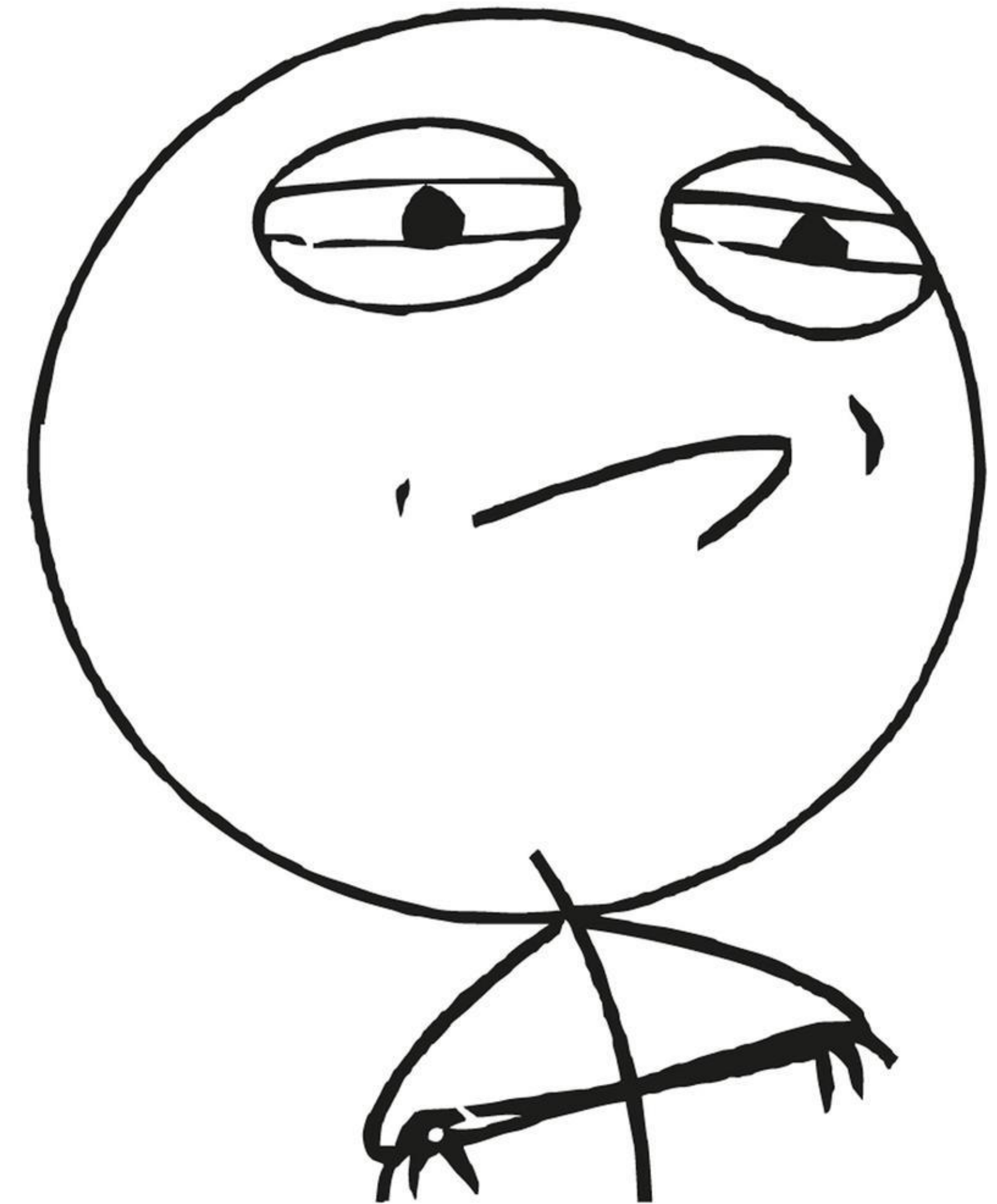
Going to the Cloud

- Cloud Computing is an option for reducing expense while staying competitive
- Helps modernise processes and thinking
- Increases robustness of applications
- Greater benefit for members
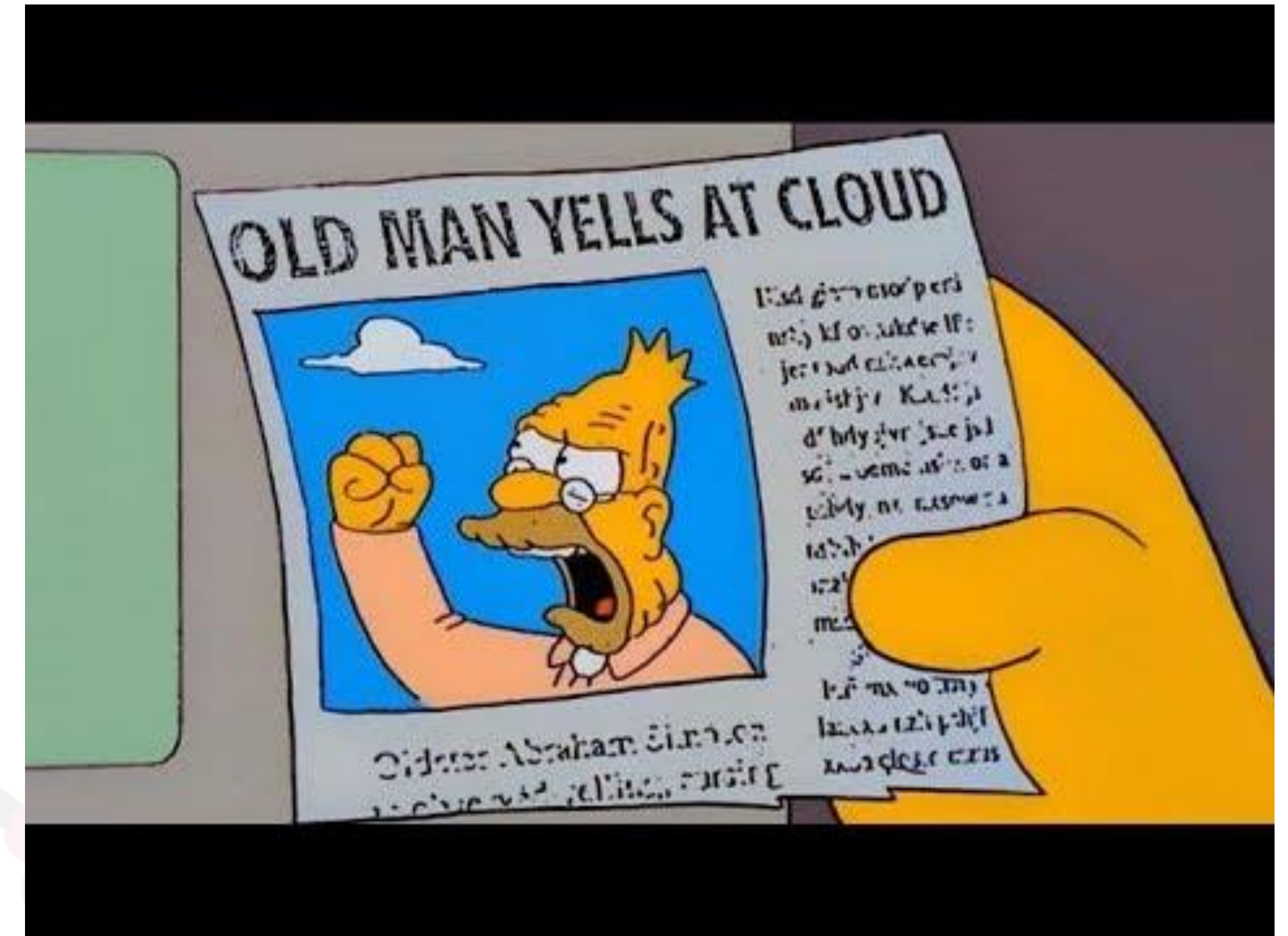
The rubber band theory

- People
- Process
- Tools

People

- First of all… instigate the culture!
- Created a Ways of Working group (WoW)
  - Representatives of all major areas
  - Discovering DevOps & Agile together
  - Experts come in to help accelerate

People

- Started playing with Scrum
  - Helps ease in into agile
- Some teams evolved to full kanban
- Space to experiment and evolve
- Scrum masters driving change through metrics

INTRODUCTION TO AGILE
CONCEPT OF AGILE ADOPTION IN SOFTWARE INDUSTRY

© www.SoftwareTestingHelp.com
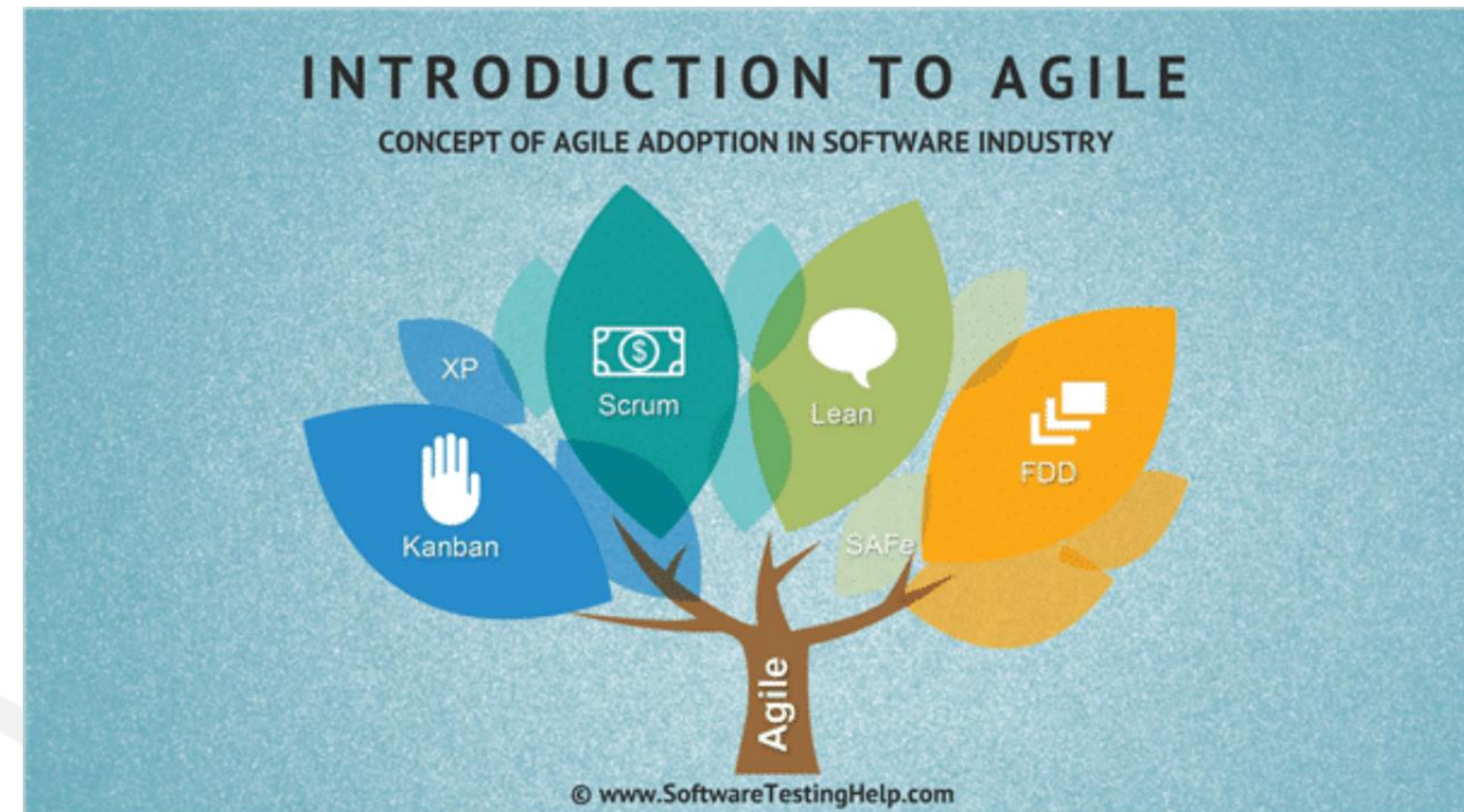
People

- Change through metrics
- Measure with industry standards
- Iterate and evolve
- Tie metrics to business results
- Based on DORA

People

- Created new Cloud Platform team
  - Accelerate first with NDAP
  - Evolve into CCoE

Process

- Agile governance
  - Controls are business requirement
  - Need to ensure we accelerate controls
- Continuous Governance
  - Controls as code
  - Governance as code
  - Policy as code

Process

Open Policy Agent

Sentinel

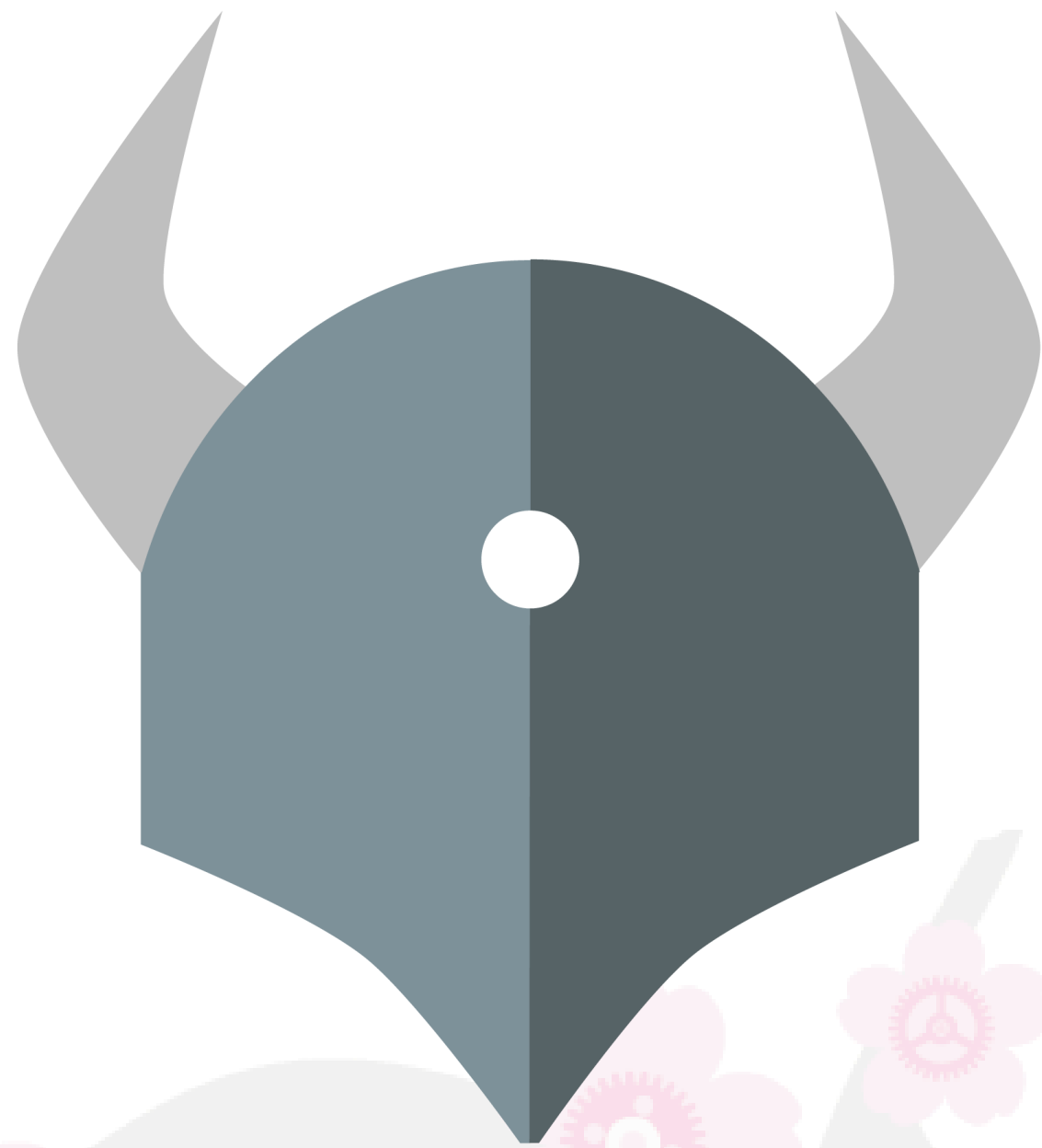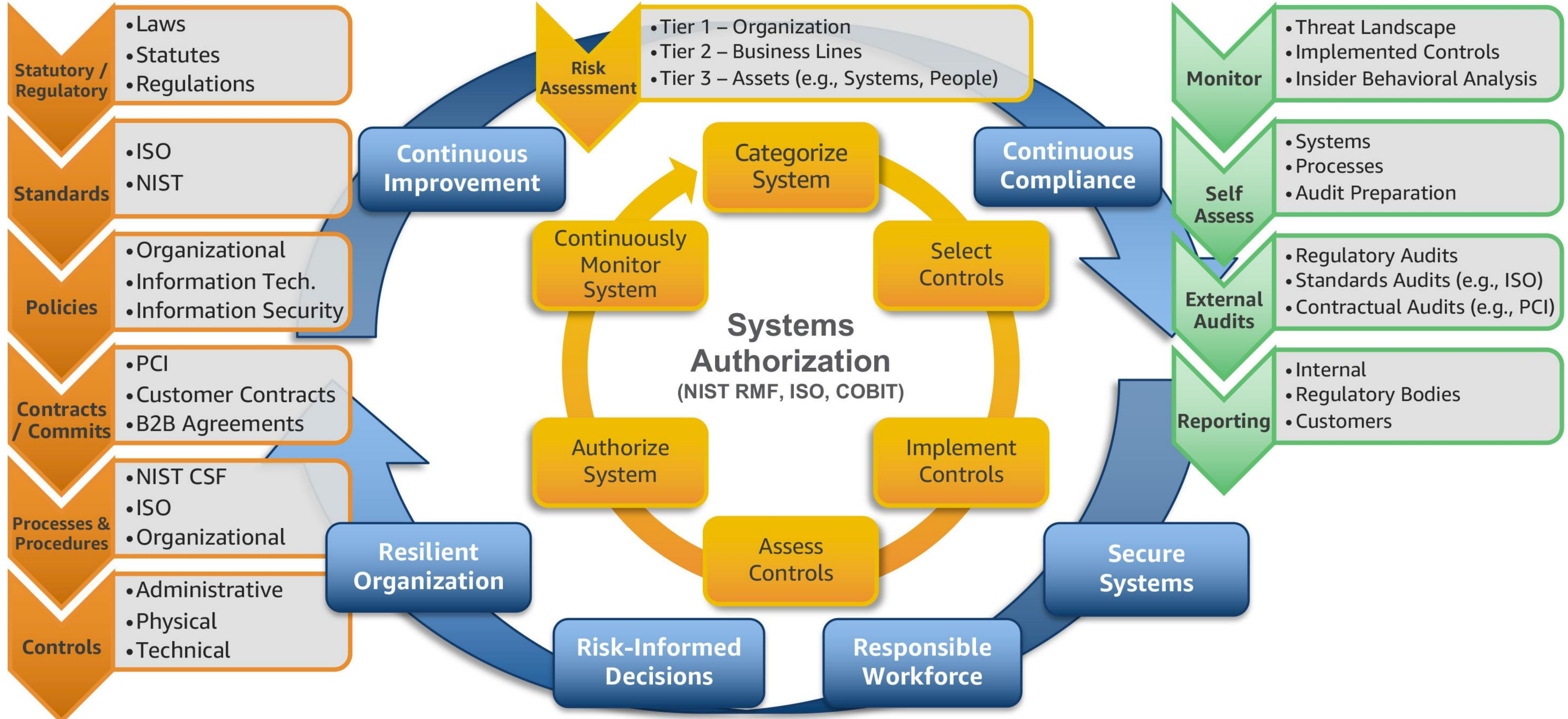# Governance | Risk | Compliance

Governance

Statutory / Regulatory	•Laws •Statutes •Regulations
Standards	•ISO •NIST
Policies	•Organizational •Information Tech. •Information Security
Contracts / Commits	•PCI •Customer Contracts •B2B Agreements
Processes & Procedures	•NIST CSF •ISO •Organizational
Controls	•Administrative •Physical •Technical

Risk

- Risk Assessment
  - •Tier 1 – Organization
  - •Tier 2 – Business Lines
  - •Tier 3 – Assets (e.g., Systems, People)

Systems Authorization (NIST RMF, ISO, COBIT)

- Categorize System
- Select Controls
- Implement Controls
- Assess Controls
- Authorize System
- Continuously Monitor System

- Continuous Improvement
- Continuous Compliance
- Resilient Organization
- Risk-Informed Decisions
- Responsible Workforce
- Secure Systems

Compliance

Monitor	•Threat Landscape •Implemented Controls •Insider Behavioral Analysis
Self Assess	•Systems •Processes •Audit Preparation
External Audits	•Regulatory Audits •Standards Audits (e.g., ISO) •Contractual Audits (e.g., PCI)
Reporting	•Internal •Regulatory Bodies •Customers

https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/

Process

- Shift left Security
  - Zero Trust security in the cloud
  - Code security checks in pipeline
  - Dependency checks in pipeline
  - External dependencies scanned

Process

- Platform security
  - Platform releases at intervals (AC)
  - Pentest of any new platform release required
  - Everybody required to jump to new platform version
  - Anything running for more than 3 months killed and refreshed

Tools

- Everything is a pipeline
  - All applications moving to CI
  - Evolve CI model based on feedback
- Deployment is also a pipeline
  - Working on CD solutions
  - CD solution needs to align to governance

Tools

- Everything is an API
  - Follow twelve-factor app
  - RESTful interfaces always secured
  - Short lived sessions for re-auth

Accelerate to ludicrous speed!

Mortgage Payment Holidays

- Financial plan against Coronavirus
  - 3 months mortgage payment holiday
  - Effective immediately
- Mortgage Payment Holidays unusual
  - Completely manual process
  - Very few per month

Team Assemble!

- Need automated solution for MPH
  - Agile teams organised
  - Continuous Governance, Risk & Control activated
  - Initial design & plan approved in 2 days
  - Mortgage teams works at full speed
  - Platform & Ops supporting

Ideation to released product

2 weeks!

Key takeaways

- It is possible to transform a big business into full Agile & DevOps
  - Like the Titanic, takes time to turn around
  - Need to focus on people first, then process and tools
- Use technology as a catalyst for change
  - Tech helps drive change, shouldn't be the only reason
  - Upskill your people for happiness and retention

We're hiring spiel

Questions?

Follow me on Twitter! Only 400 followers behind @devopsdom

I will thank you individually!

HUGS WILL BE GIVEN!!!

@lynxman