Automated Governance Changed What We Believe In

Michael Edenzon
Co-Founder, Fianu Labs

John Rzeszotarski
SVP Infrastructure, PNC

Disclaimer

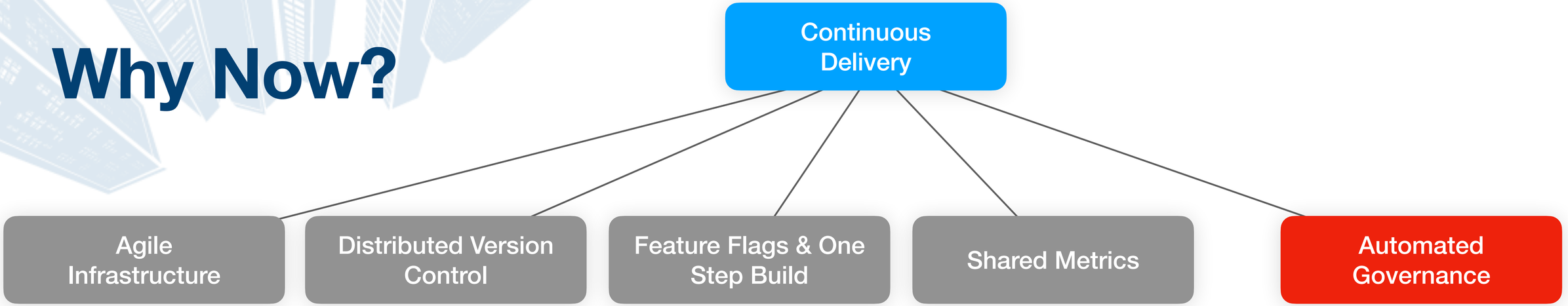
Law of Two Feet w/ Words and Things

- If people find themselves in situations where they are neither learning anything nor contributing, they are responsible for moving to another place using their two feet.

- Ask …. “Is this meeting about **words** or **things**?” If its words make sure you consider the law.

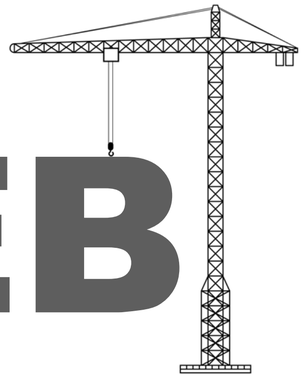
- Ideally meetings should end with “**Lets go do the things!**”

Why Now?



BUILDING the BIG

WEB



flickr NETFLIX aws Etsy Google

Remove Traditional Thinking of “Dev’s job to add new features and Ops’s job to keep the site stable and fast” - John Allspaw & Paul Hammond

Regulated Industries

Lower Risk of Change

“Lowering Risk of Change thru Tools & Culture”
- Also by John Allspaw & Paul Hammond

We Do This Already

Developers Have The Tools and We Have The Processes

Secure Coding Standards

Pipeline Integration

Change Record Creation

My tool has:

- Banking industry knowledge and competence sufficient to respond appropriately to the risks of material misstatement in the company's systems
- Meet any additional regulatory requirements that may be part of an audit
- Magic abilities to adopt to companies policies and procedures
- An ability to make toast

If You Build It
They Will Come

Vision

A Super Highway

Automated Governance Reference Architecture

IT Revolution, 2019

- Defined Stages of Metadata and Asset Collection
- Reference of Controls Required
- Fine Grained Access Controls for Metadata
- Implementation Reference Architectures

Our Beliefs

Belief #1

Developer Autonomy

Belief #2

Carrots Instead of Sticks

Belief #3

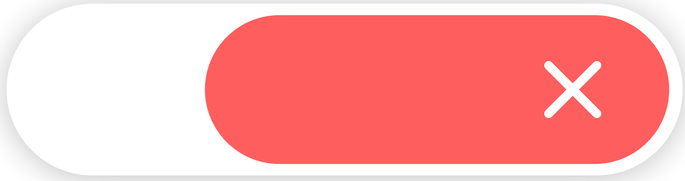
No Downward Pressure

Strategy

A simple, shared language.

PASS

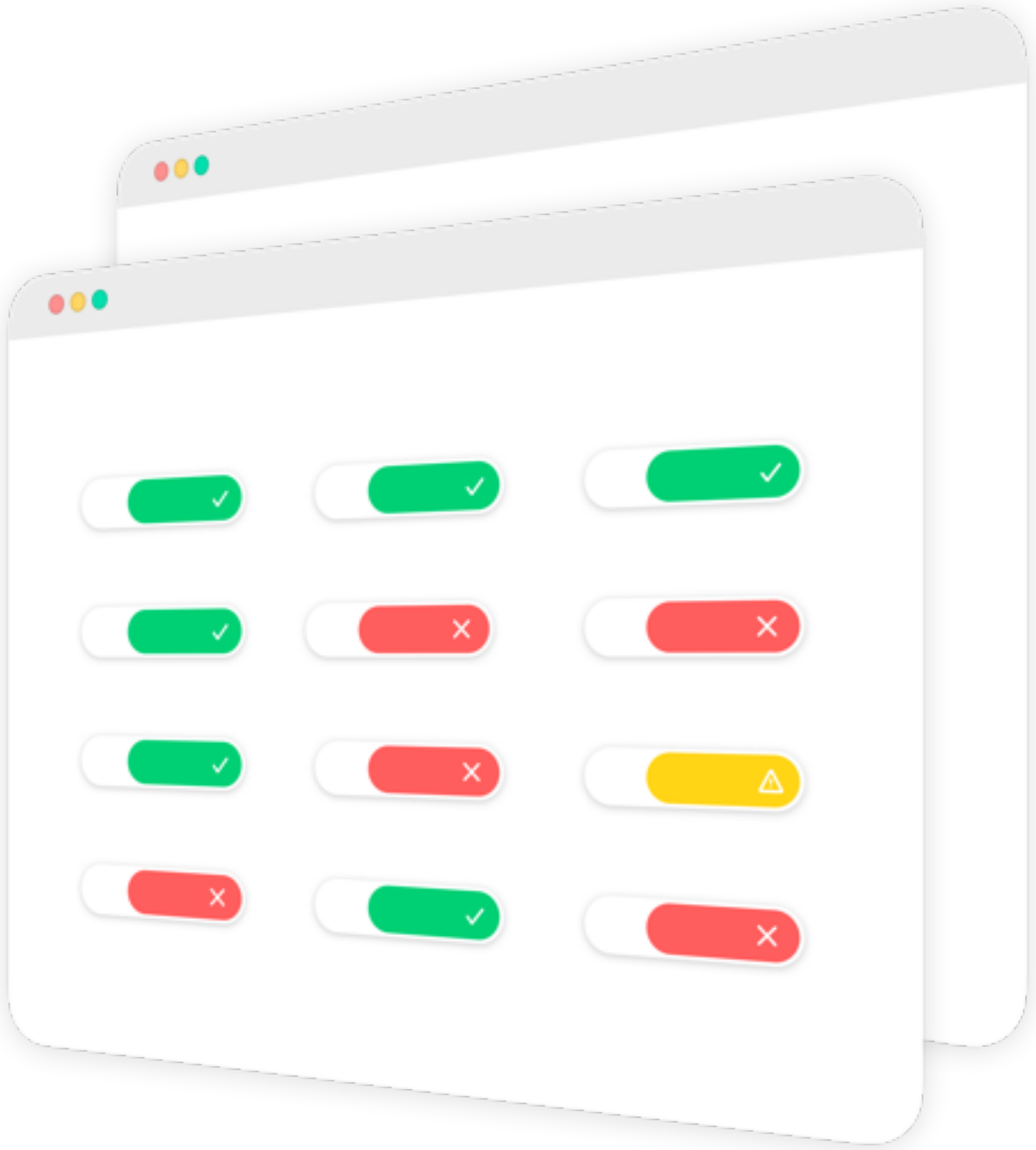
WARN (PASS)



FAIL

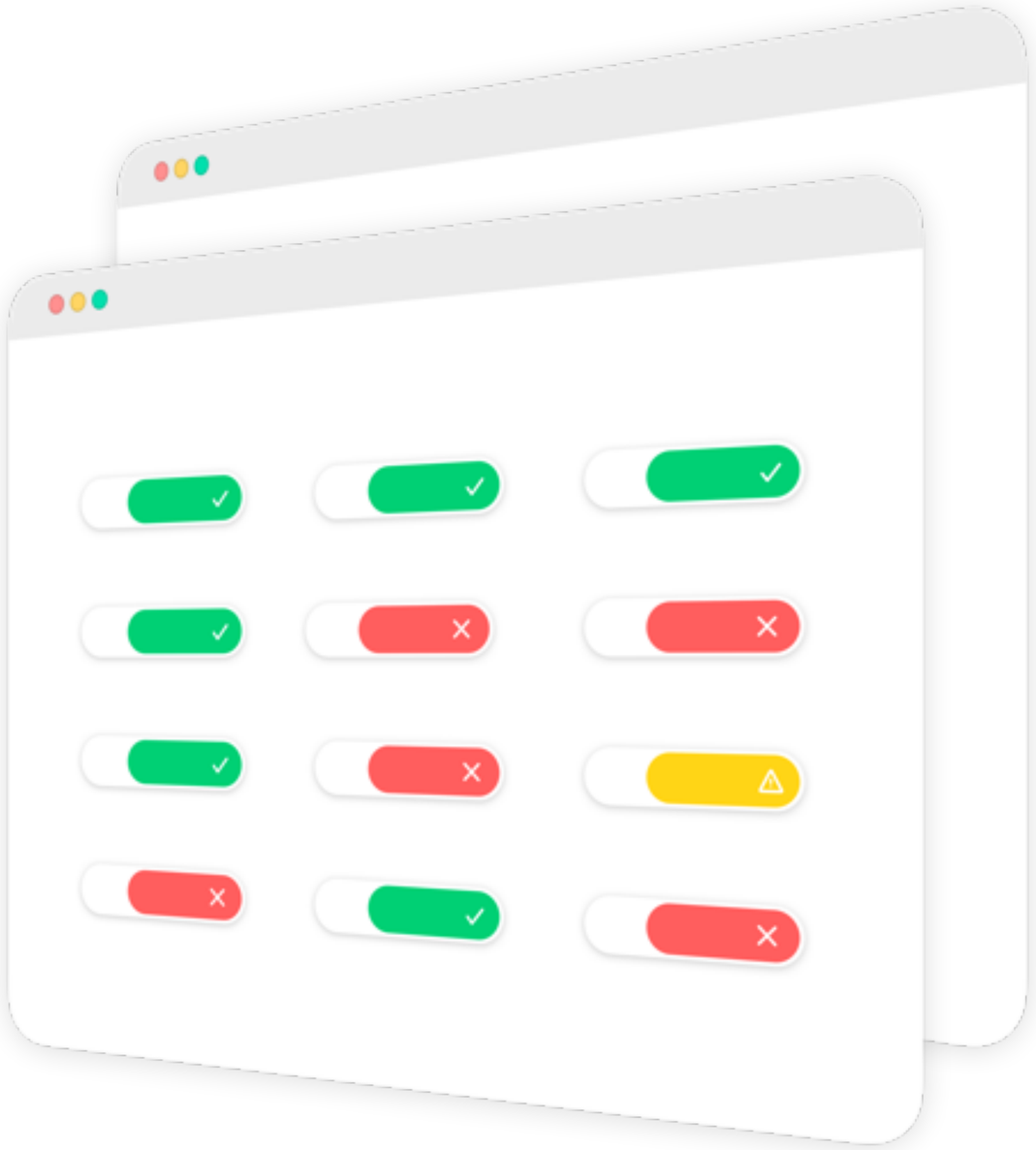
NOT FOUND (FAIL)

We Built It



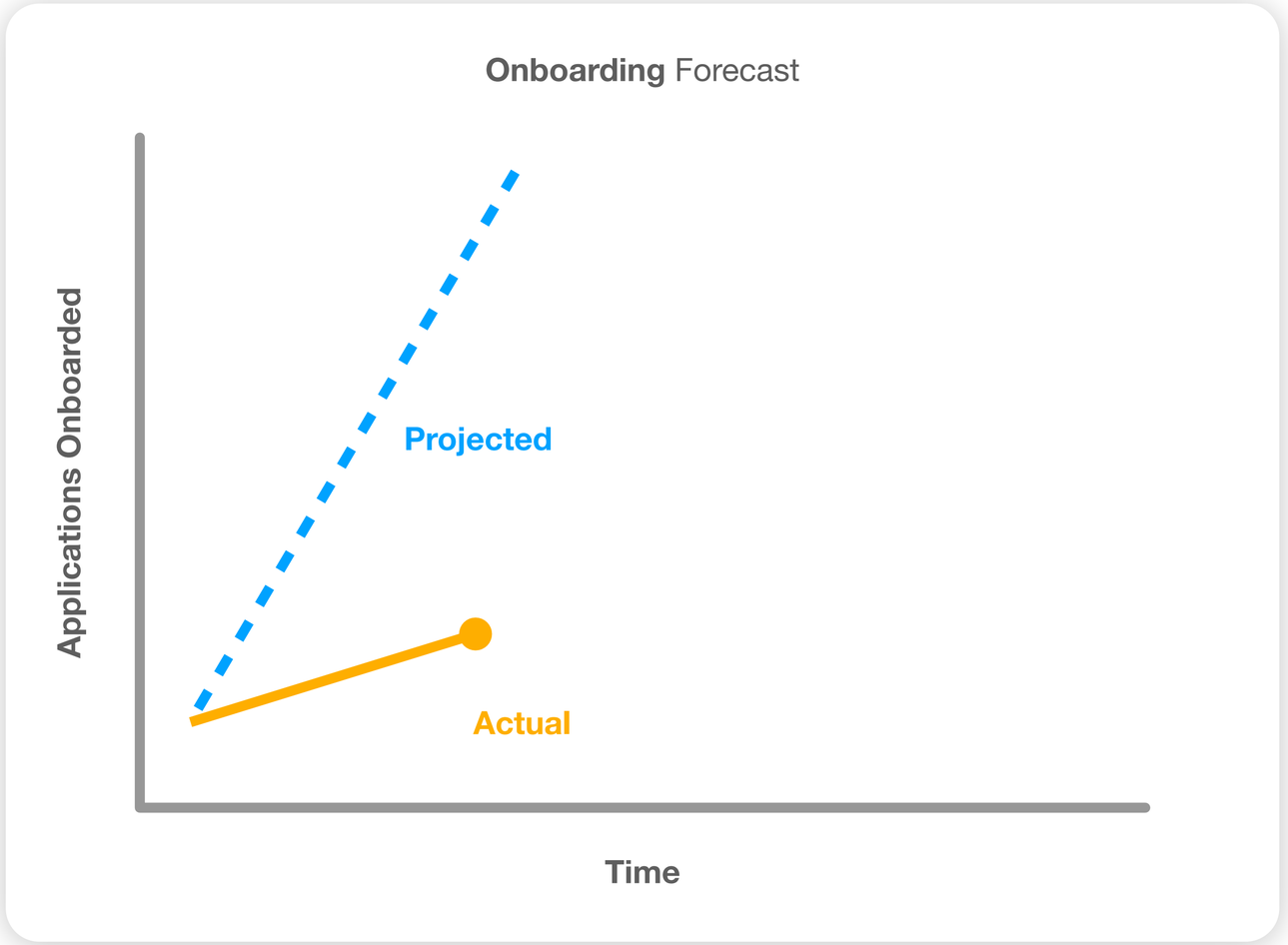
We Built It

But they didn’t come…



Onboarding Failed

You can’t onboard what you can’t see.

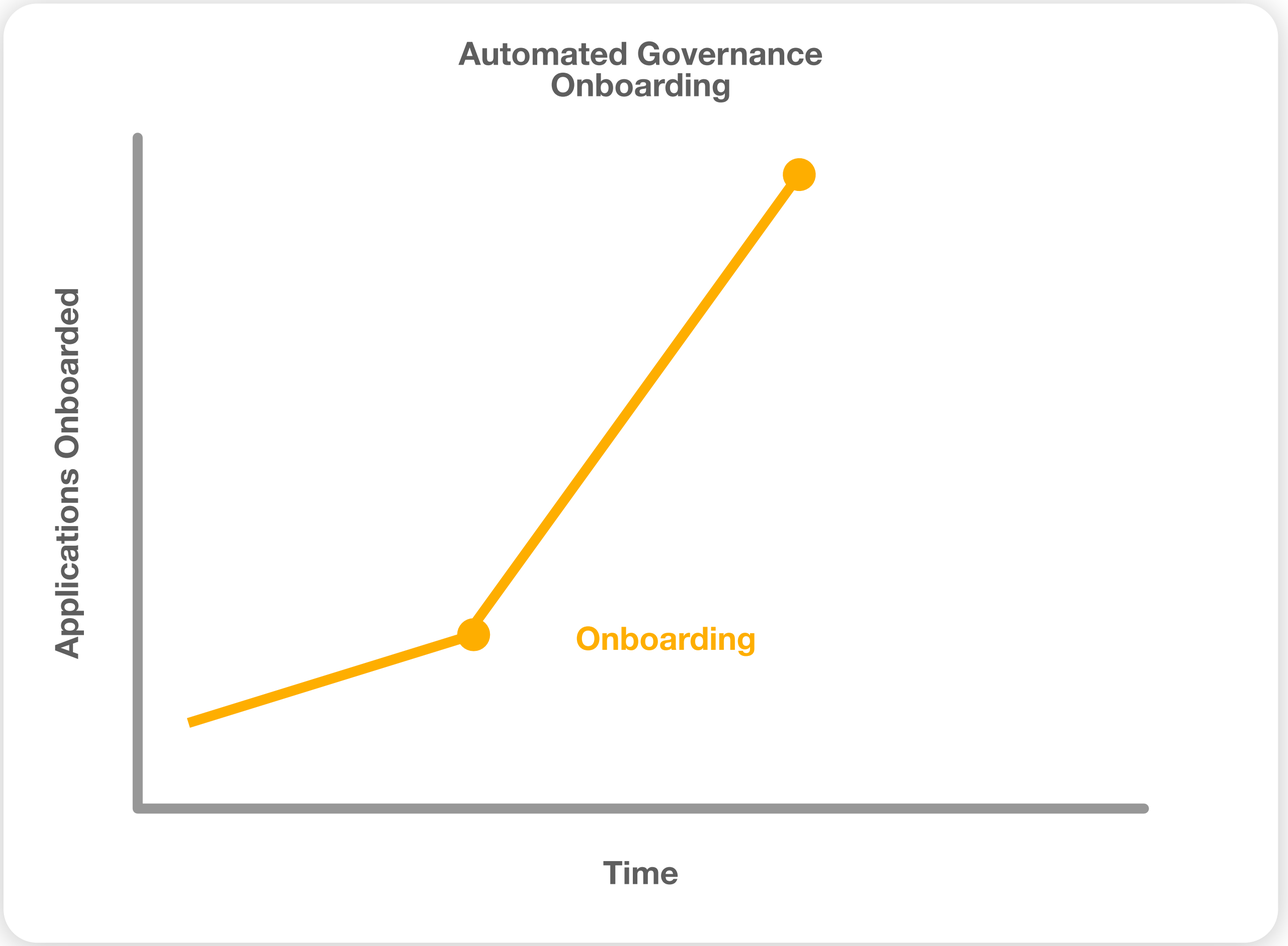


Choice #1

Autonomy or Standardization

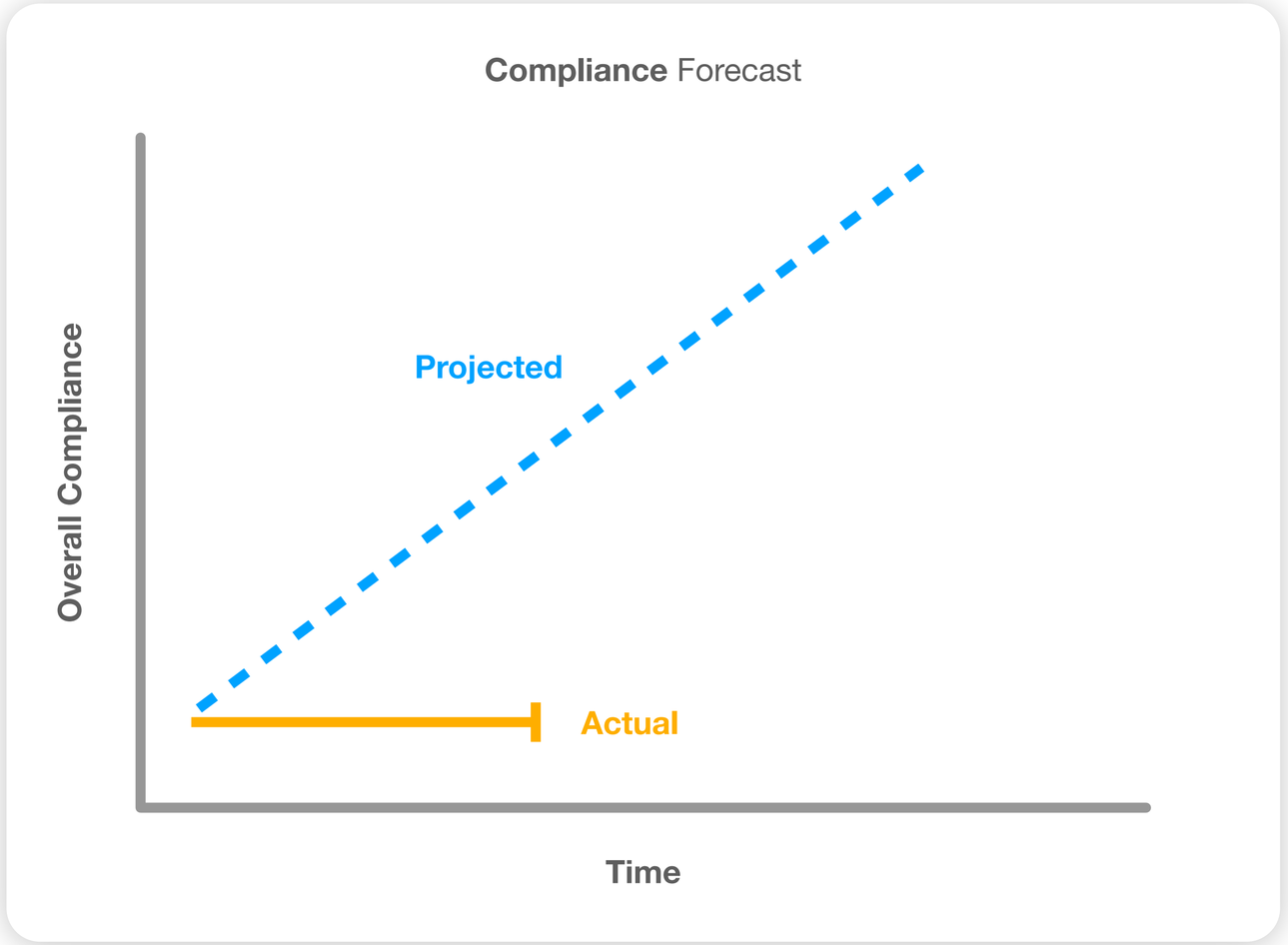
We Standardized

And onboarding took off



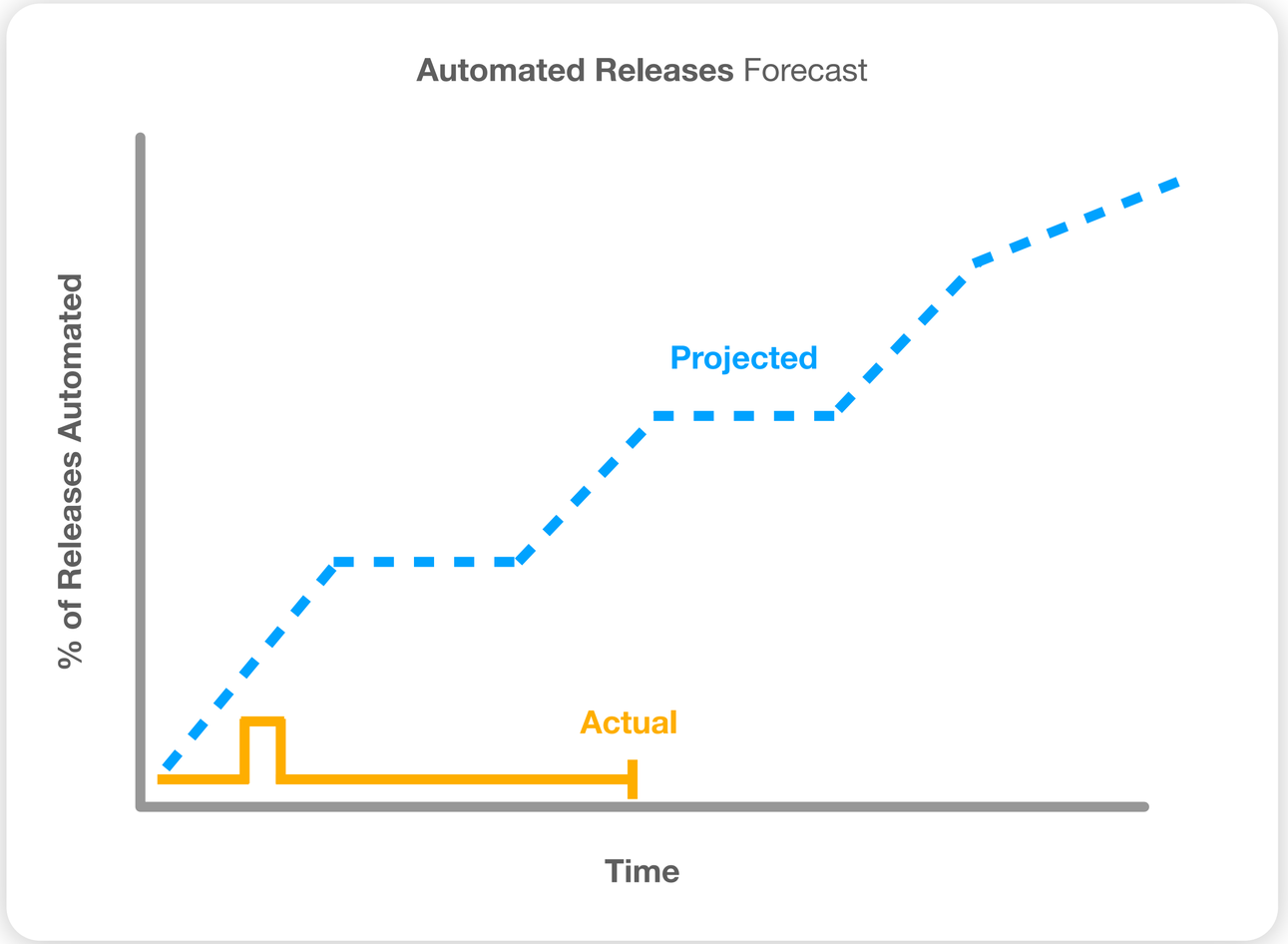
Then We Fell Flat

Compliance didn’t improve.



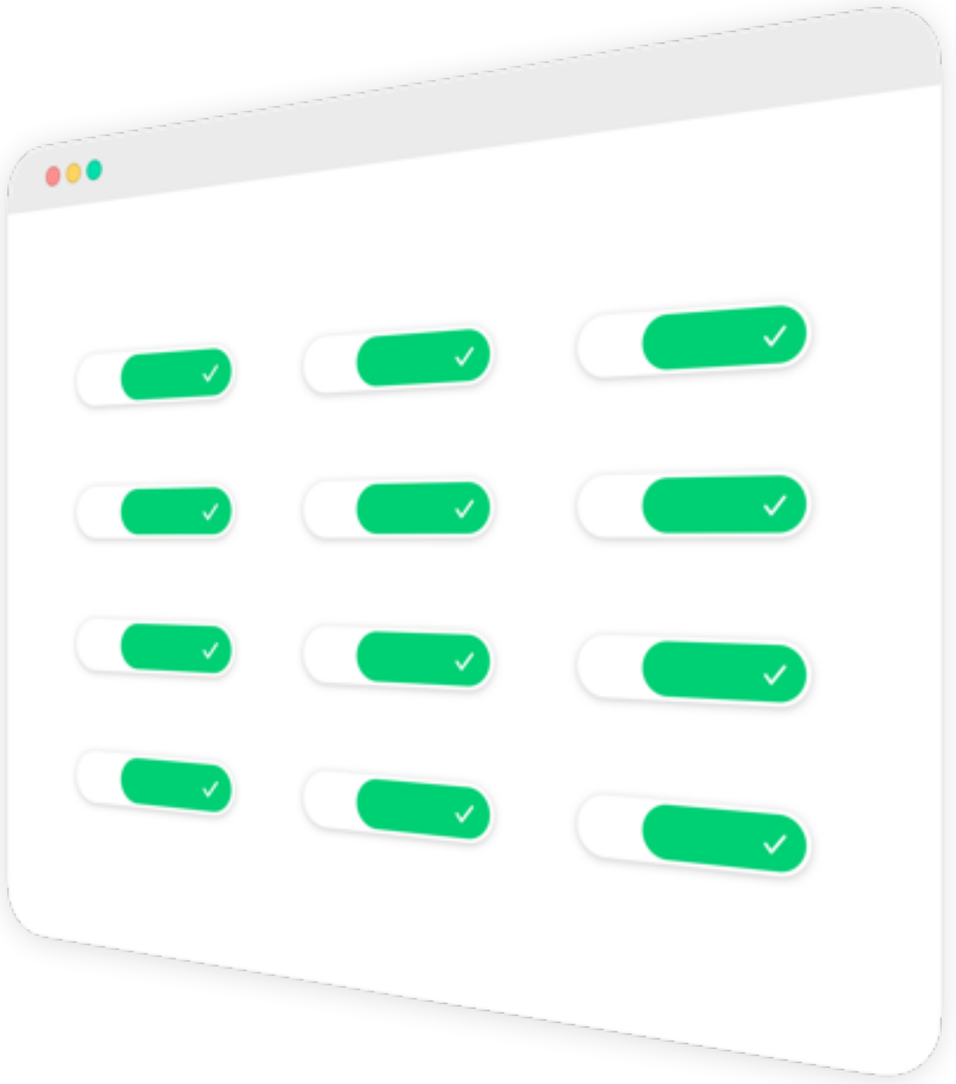
Then We Fell Flat

Automated releases flatlined.



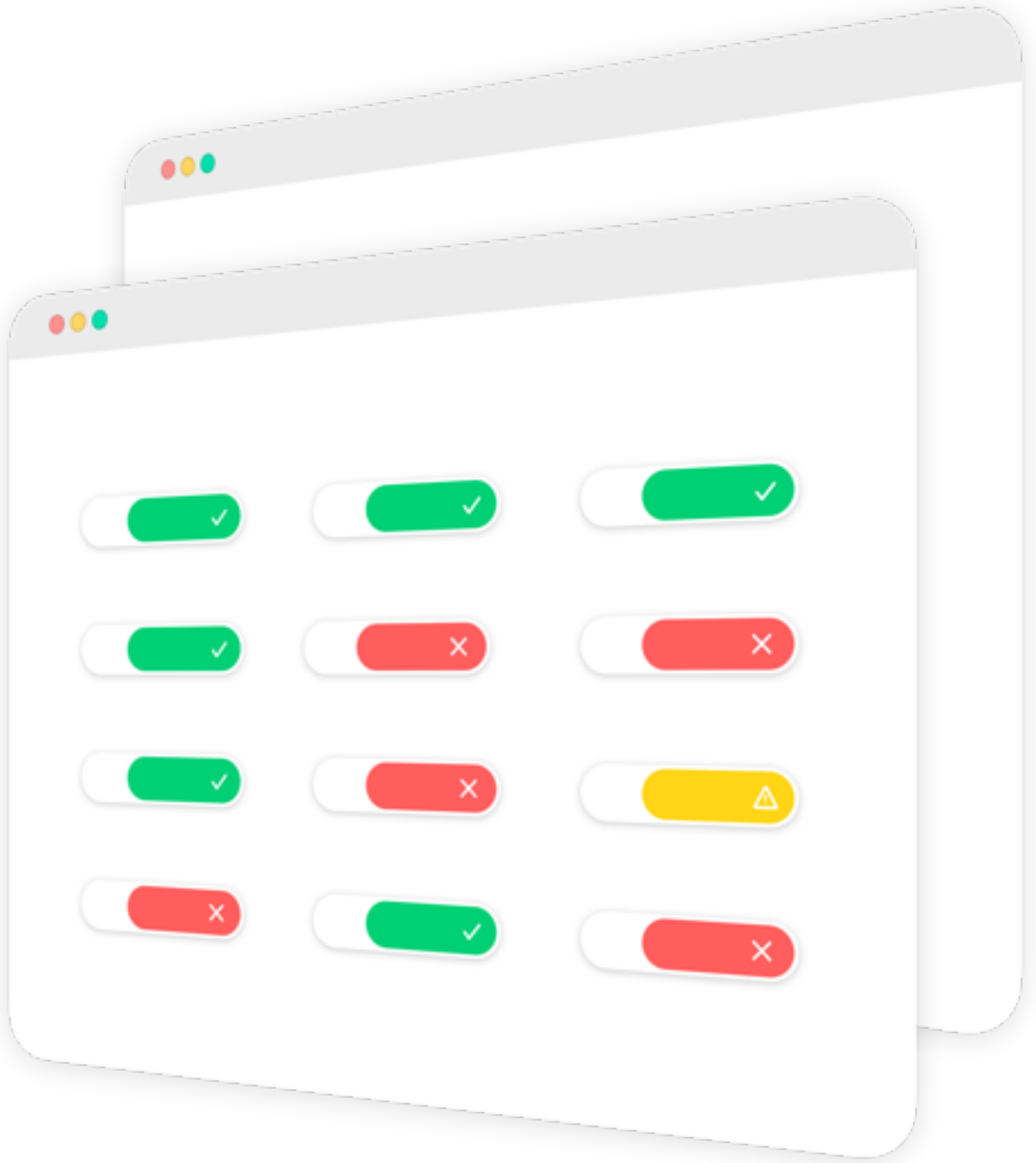
What We Sold

A superhighway, driven by compliance.



What They Saw

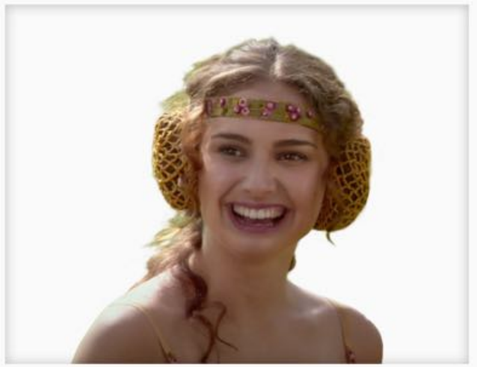
The reality of application compliance.



Teaching to Fish

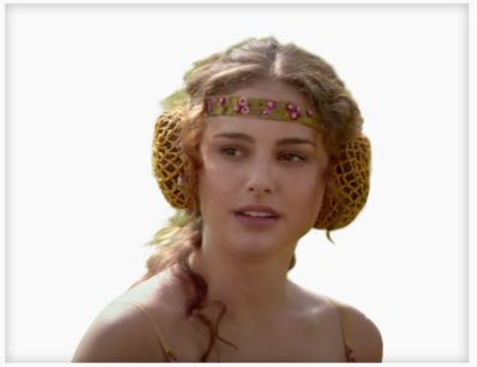
Developers must be responsible for the compliance of their applications.

Your compliance badges are over here.



Great! Let me know when they’re all green.

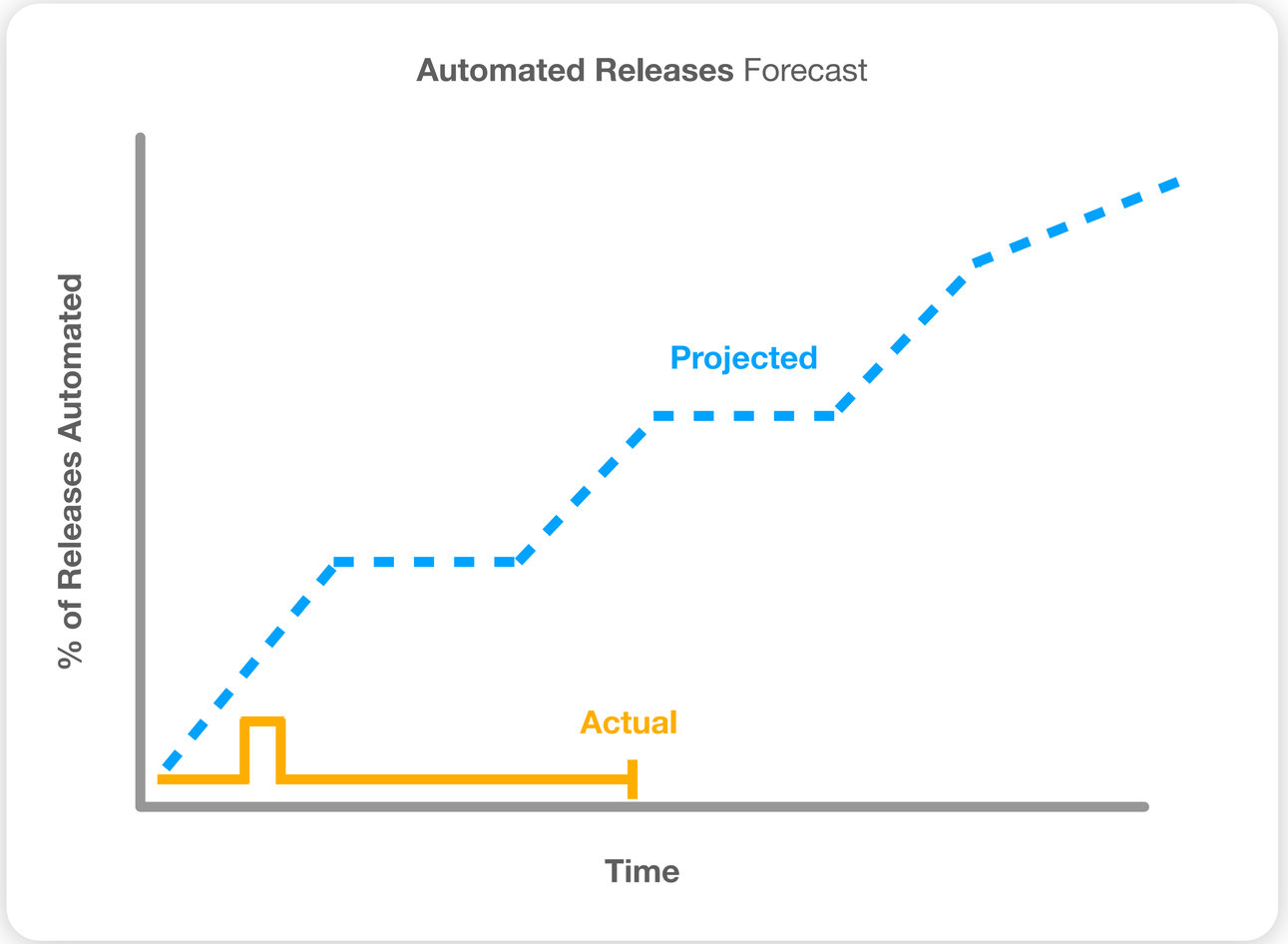
?



You’re going to make them green for me, right?

Our First Carrot Didn’t Work

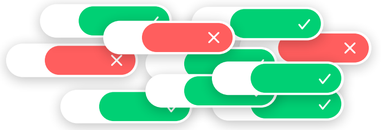
We had to try something different.



The Scorecard

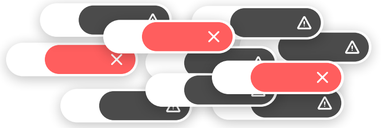
The Scorecard

= A

 = B

= C

= D

 = F

Choice #2

What should our data be used for?

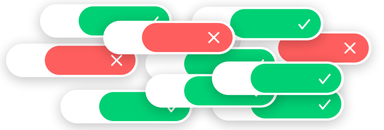
DON'T TALK TO ME UNTIL
YOUR SCORES ARE HIGHER

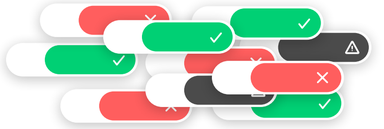
I GOTCHA RIGHT
WHERE I WANT YOU

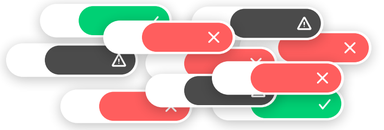
Abstraction

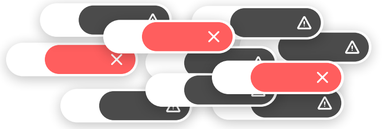
Provides directionally accurate insights, but insufficient detail for automated governance.

= A


= B

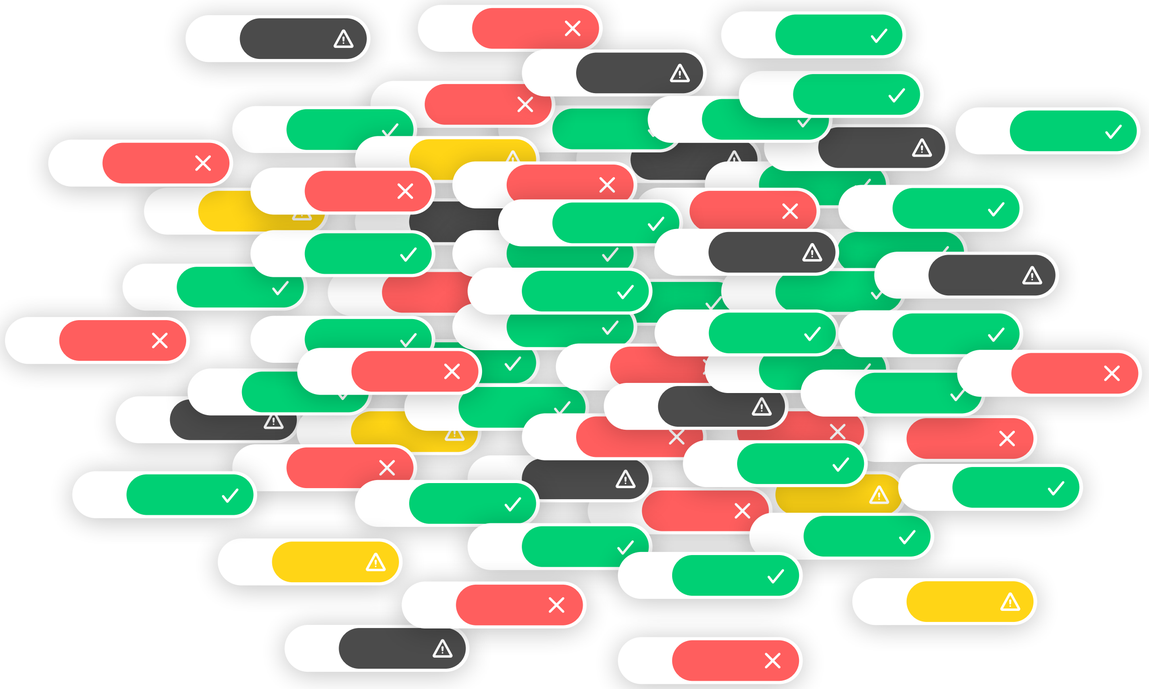

= C


= D


= F

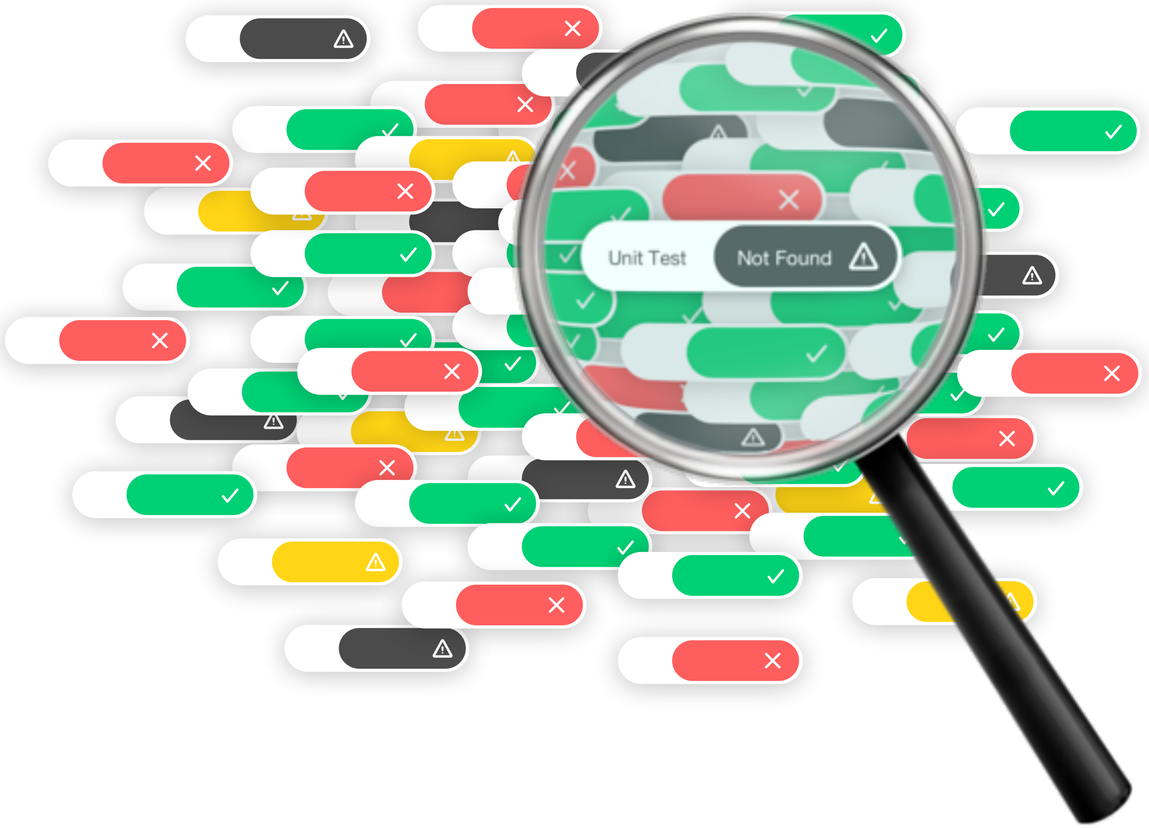
Details

With great power comes great responsibility.

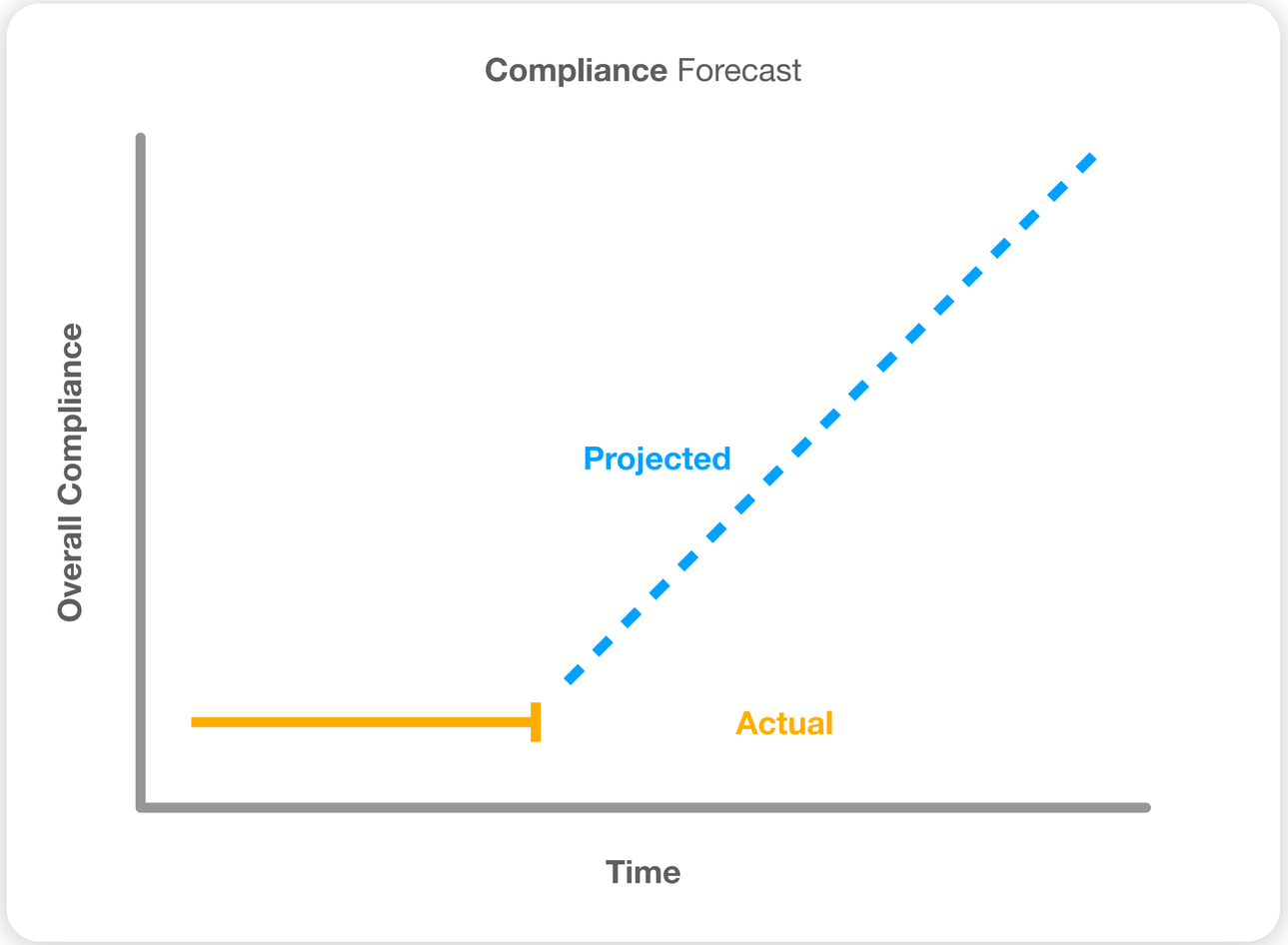


Details

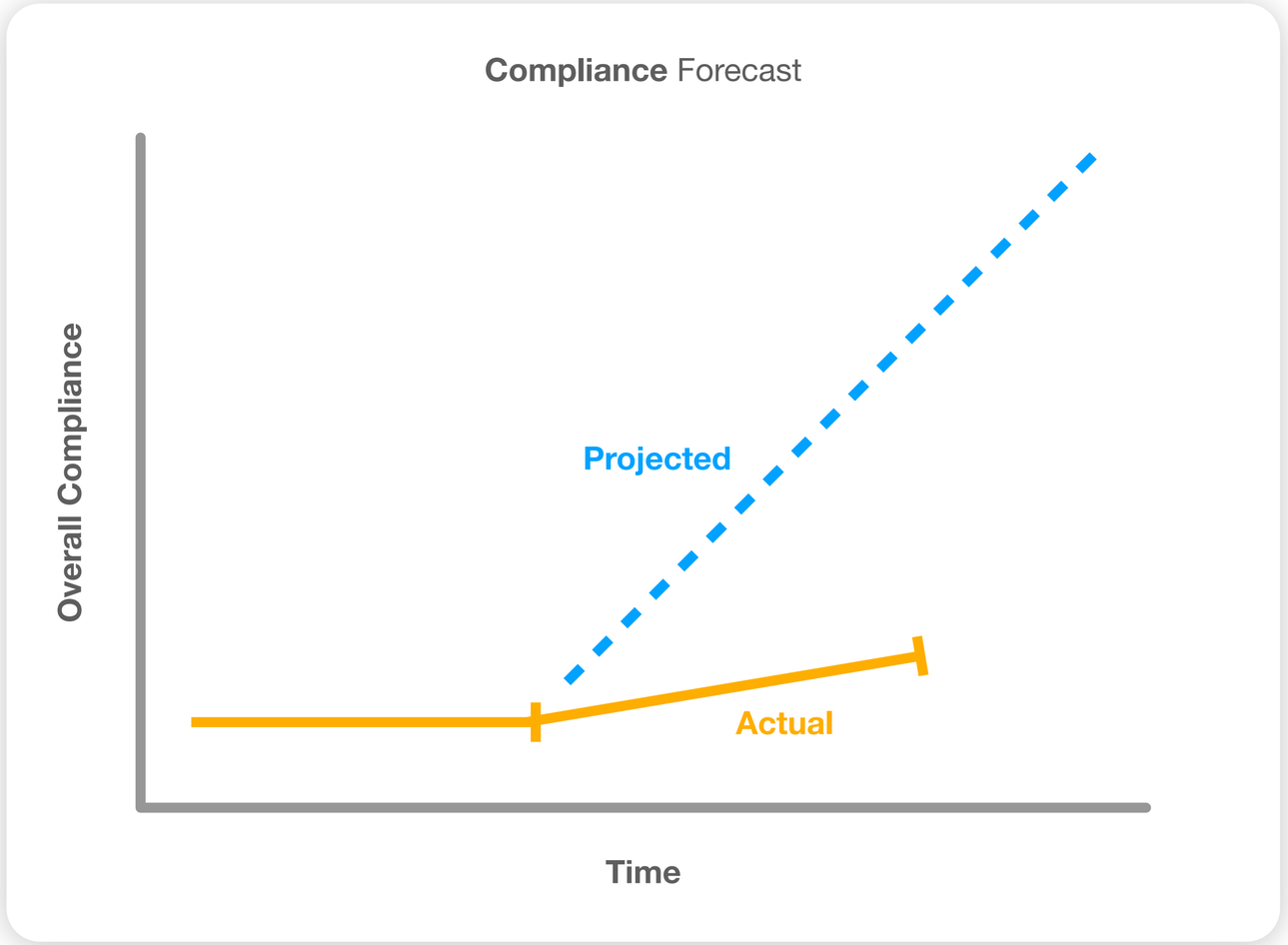
With great power comes great responsibility.



The Scorecard



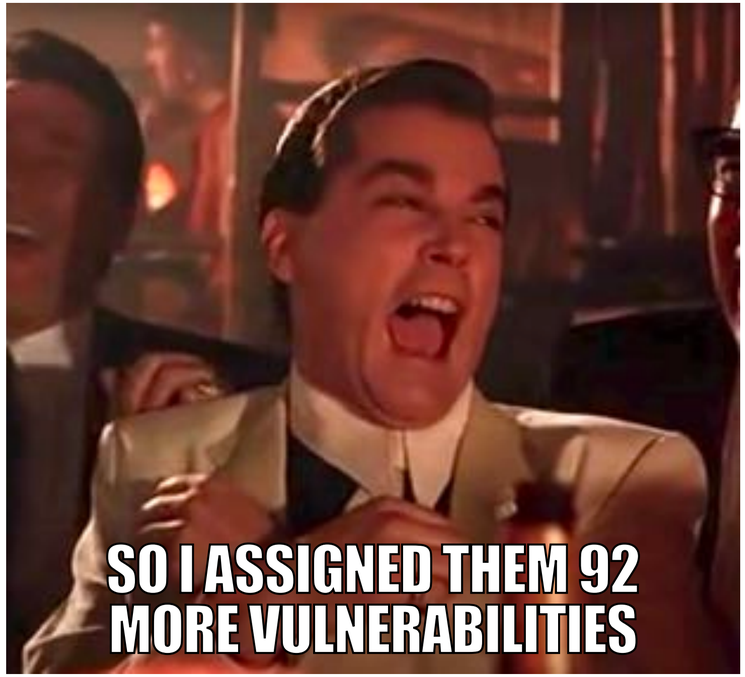
The Scorecard Didn’t Make a Difference



Downward Pressure

Choice #3

If you can use downward pressure, does that mean you should?

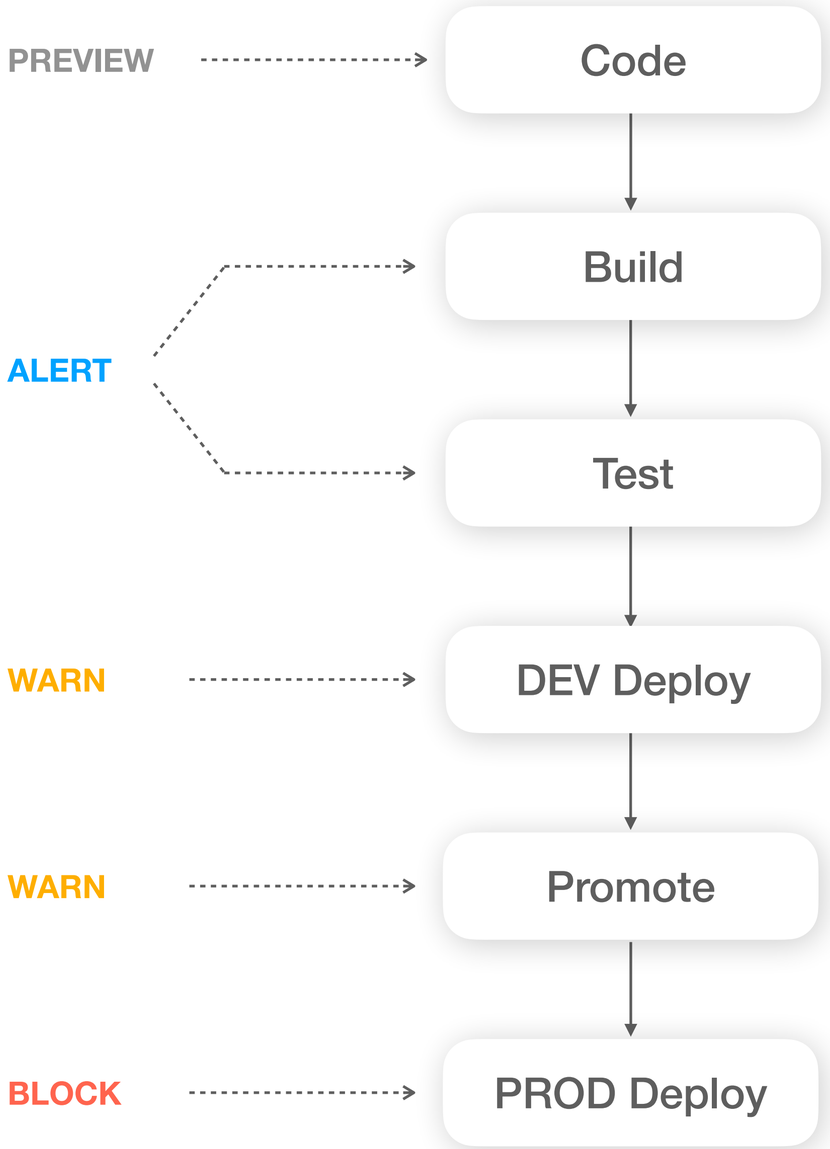


“Anything that puts downward pressure in your organization on honesty, openness, and learning is bad for business”

- Sidney Dekker

Automated Enforcement

How It Works



Game Theory

Governance, Risk, and Compliance

Automated Enforcement

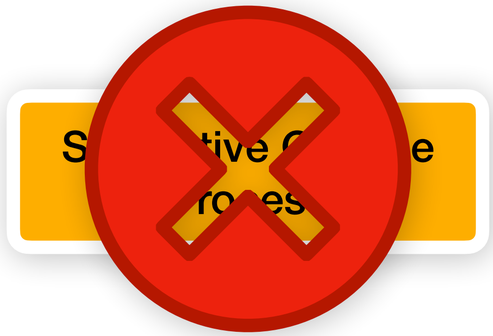
Optimal

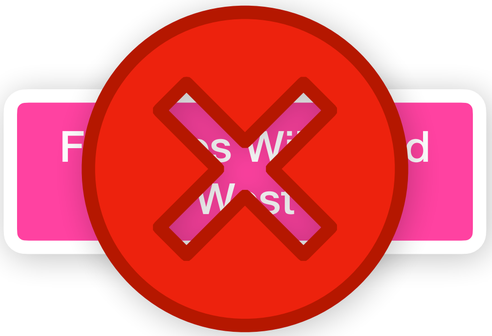
Not Optimal

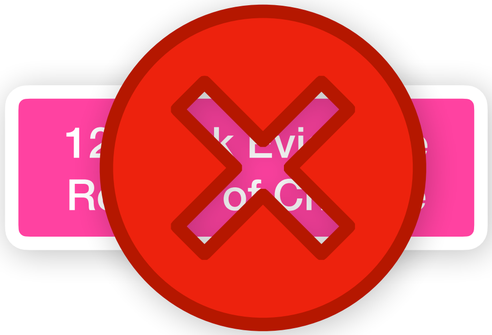
Optimal

Developers & Engineers

Not Optimal



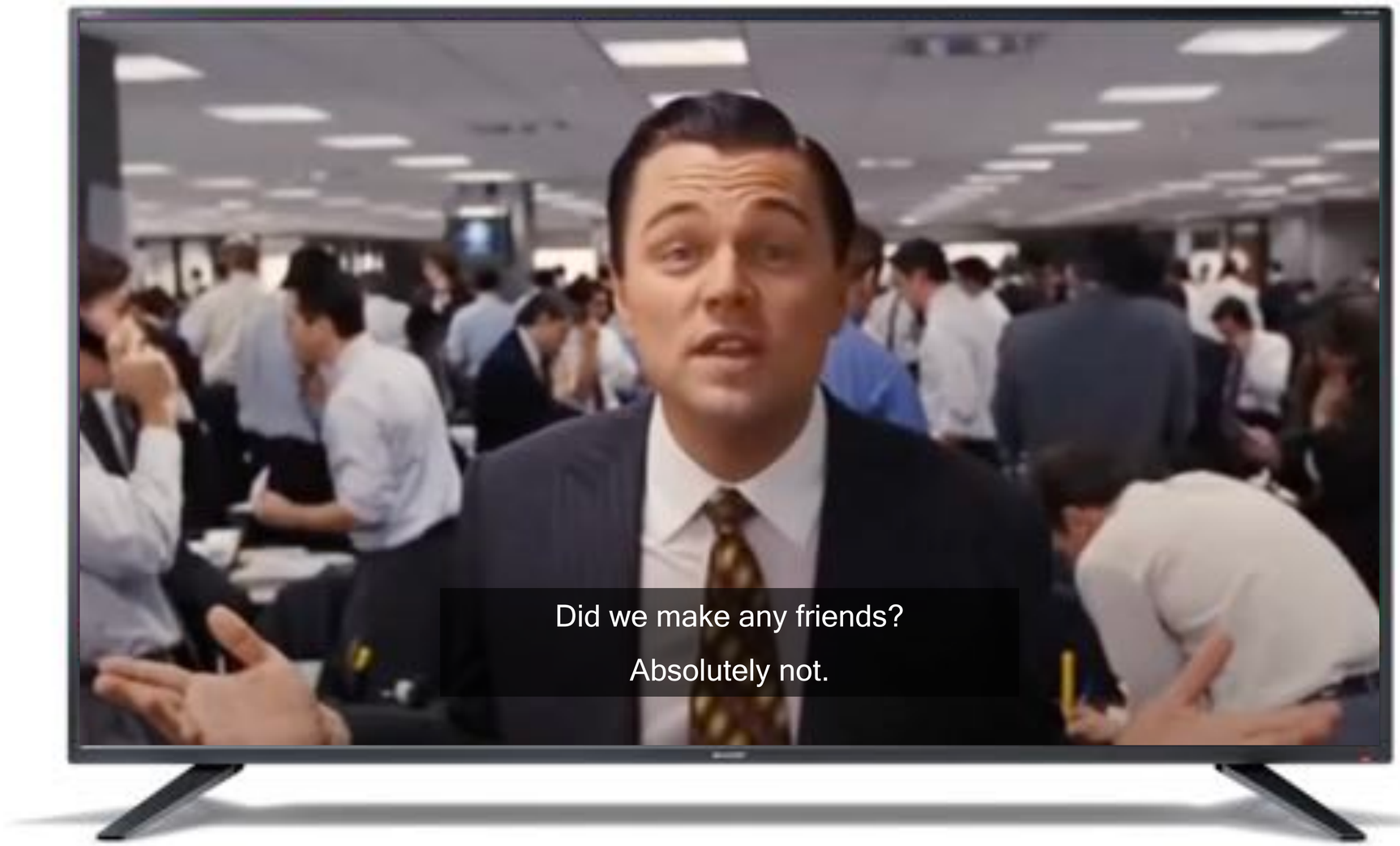




Automated Governance

Rollout

Easy Controls
Easy Controls
Medium Controls
Difficult Controls
Month 1
Month 2
Month 3
Month 4
Soft Enforcement
Hard Enforcement
End of Grace Period
Full Enforcement


Did we make any friends?
Absolutely not.

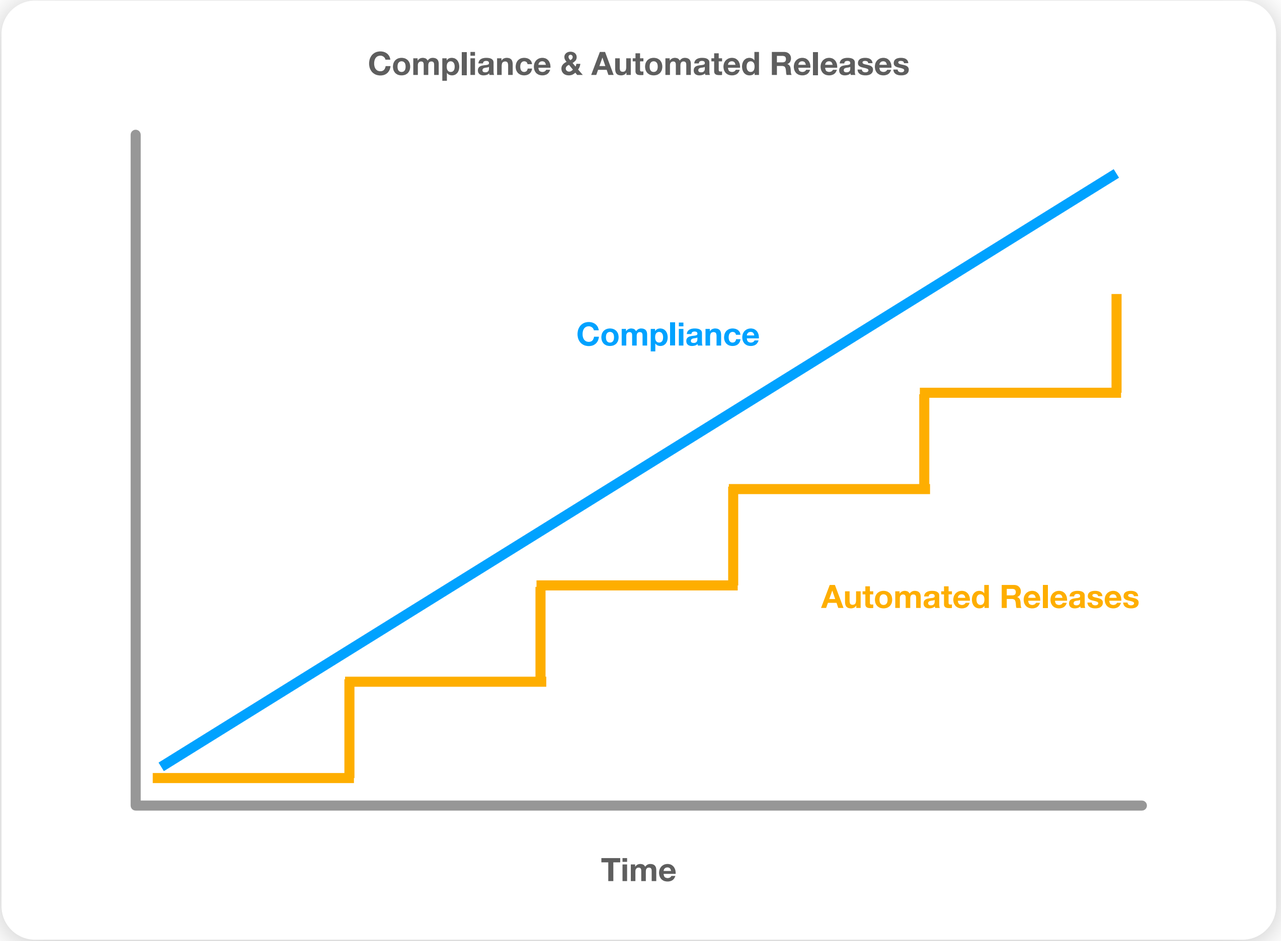
The Automated Enforcement Effect

Chat Room Engagement **5x** ↑

Office Hours Attendance **10x** ↑

Production Incidents Caused by Gates **Zero**

The Automated Enforcement Effect



What onboarding or adoption stories can you share?

Let’s go do the things!