

Move Fast and (Don't) Break Things

How Quality Engineering Transforms Application Security

Alex Beaver
alexbeaver.com
[/in/alex-beaver](https://www.linkedin.com/in/alex-beaver)





MOVE FAST &
BREAK THINGS



BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS



BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS
BREAK THINGS

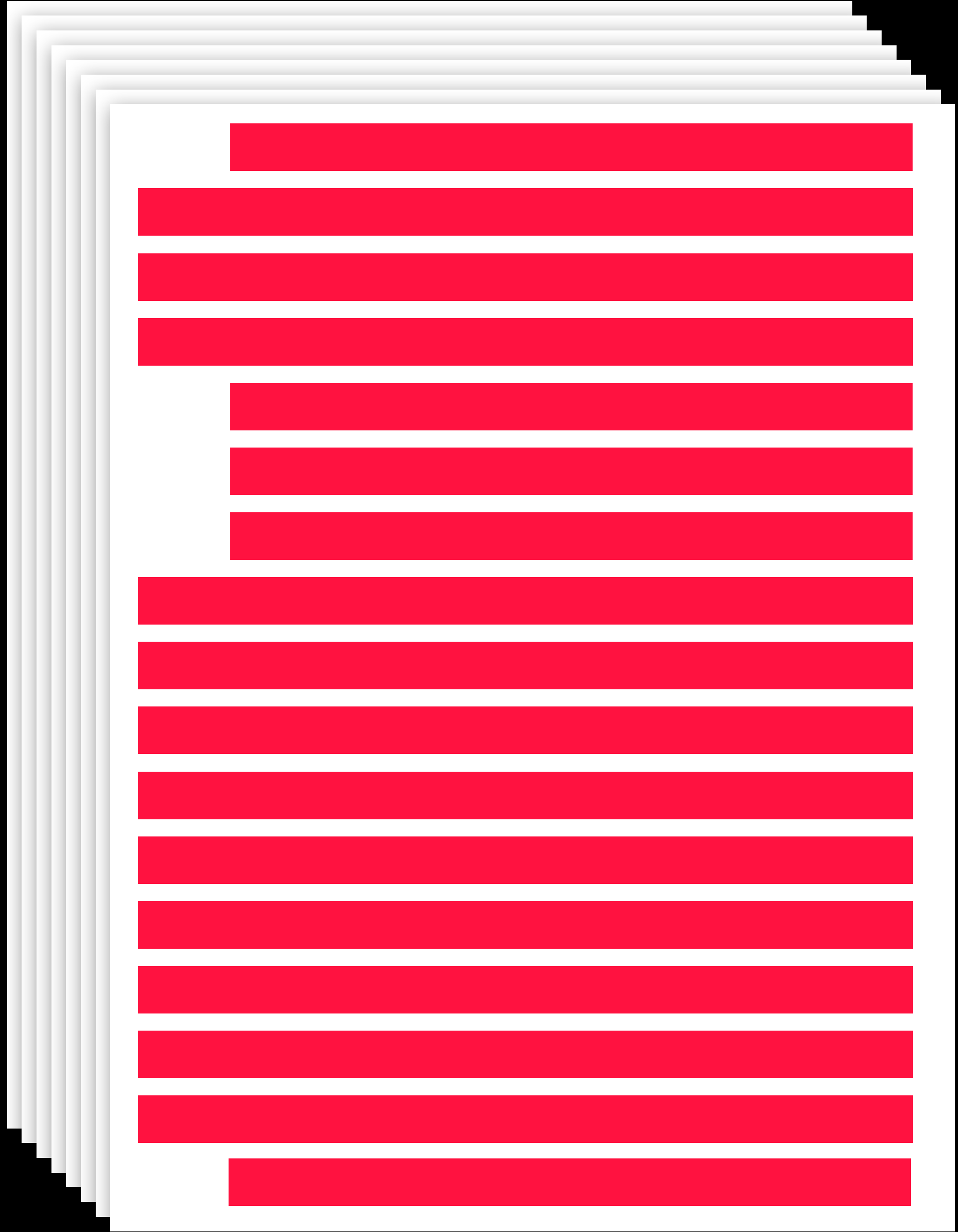


DO YOU HAVE TO
BREAK THINGS
TO MOVE FAST?

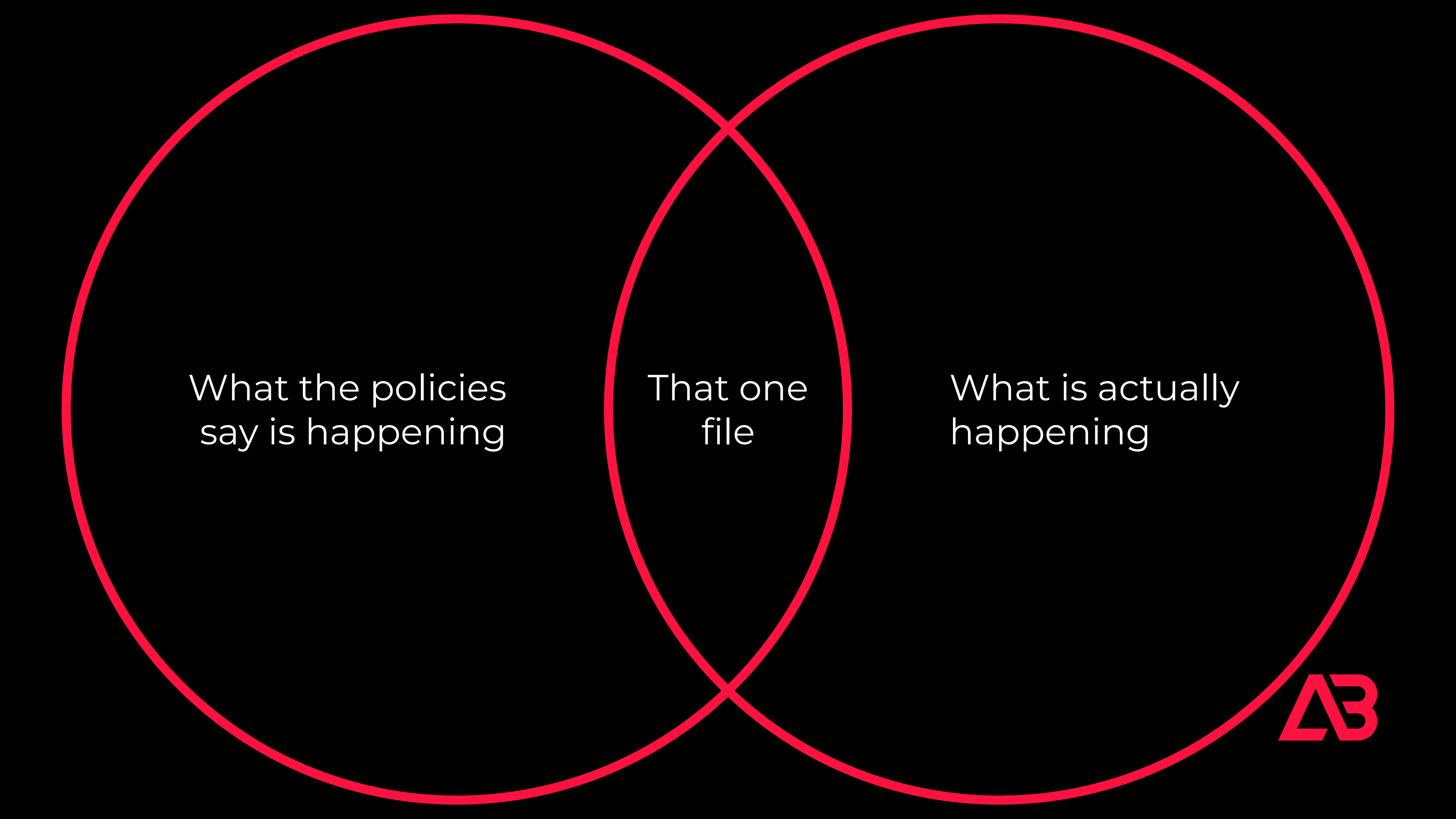


clean Number String Function Array Date RegEx
={};function F(e){var t=[e]={};return b.eac
t[1])===!1&&e.stopOnFalse){r=!1;break}n=!1,u&
?o=u.length:r&&(s=t,c(r))}return this},remove
nction(){return u=[1,this],disable:function()
re:function(){return p.fireWith(this,arguments
ending",r={state:function(){return n},always:
romise)?e.promise().done(n.resolve).fail(n.re
dd(function){n=s},t[1^e][2].disable,t[2][2].
=0,n=h.call(arguments),r=n.length,i=1!==r||e&
(r),l=Array(r);r>t;t++)n[t]&&b.isFunction(n[t
</table></table>a<input type
TagName("input")[0],r.style.cssText="top:1px

POLICIES
STANDARDS
BEST PRACTICES







What the policies
say is happening

That one
file

What is actually
happening





Investing in Quality Engineering
Delivers **Better Software Faster**



1

Invest with Intention

2

Engage with Engineering

3

Transform with Time



Y Q U A L I T Y C

Y Q U A L I T Y C

Y Q U A L I T Y C

Y Q U A L I T Y C

Y Q U A L I T Y C

Quality is Cultural

Y Q U A L I T Y C

UNDERSTAND
WHAT MATTERS
AND INVEST IN IT



UNDERSTAND
WHAT MATTERS
AND INVEST IN IT



WHAT MATTERS

DELIVERY

EFFICIENCY

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

RELIABILITY

PROFITABILITY



WHAT MATTERS

DELIVERY

EFFICIENCY

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

RELIABILITY

PROFITABILITY



WHAT MATTERS

RELIABILITY



Trusted
Control
Systems

Automation-Centric Design

Standard Workflows

Best Practices and Guidelines

Trusted Abstractions

FOSS Libraries



1

Invest with Intention

2

Engage with Engineering

3

Transform with Time



ADVERSARIES
DON'T CARE
ABOUT POLICIES





ITS SUPPORTS

T SUPPORTS

T SUPPORTS



Photo by National Cancer Institute on Unsplash

EVERYONE
MUST SPEAK UP



Early and Small Honest and Blameless

Major Concern

Stop and Redirect

Development Slowed / Future Risk

Slow and Triage

On Track

No Action Needed

The Red String

1

Invest with Intention

2

Engage with Engineering

3

Transform with Time

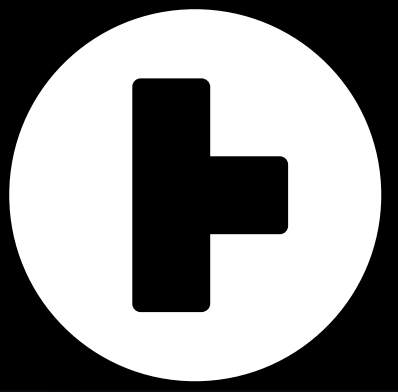
Change is Hard



Smaller Steps

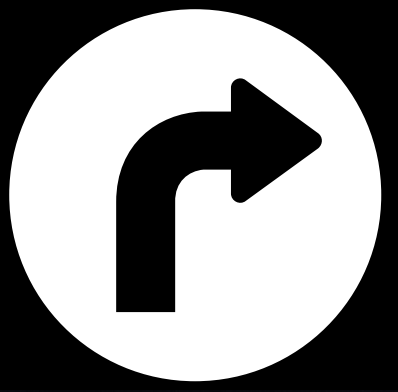
Shorter Focus





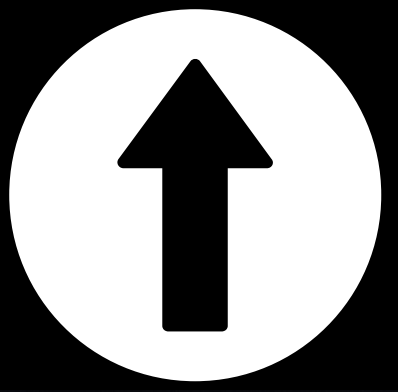
Analyze failure data





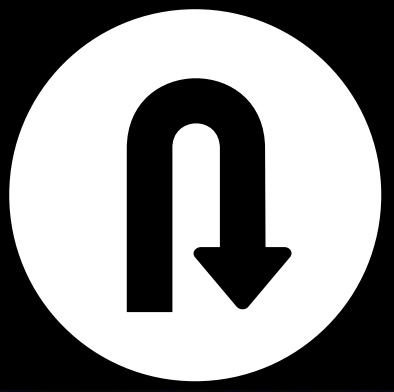
Develop workflow changes





Adopt workflow changes





Demonstrate impact and repeat



impact



1

Invest with Intention

Understand What Matters

Make Difficult Decisions

2

Engage with Engineering

Support Your Engineers

Everyone Speaks Up

3

Transform with Time

Take Smaller Steps

Lessen Intimidation



What we did

* Implementations should be based on your own organization's needs, so this is ***not*** advice

DO IT ONCE
RIGHT



Data Collection



TIME	COMPILE	ROOT CAUSE
0	Compile	Perform RCA
30		
60		
90		Fill Out Form
120		Relax
150		
180		
210		



Non-Compliance



NATURAL
ACCOUNTABLE POLICIES



NATURAL POLICIES

- ~90% of policies and procedures
- Integrate into existing workflows
- Noncompliance as a policy issue
- Examples
 - Development guidelines
 - Software architecture
 - Workflows



ACCOUNTABLE POLICIES

- ~10% of policies and procedures
- Situations where can't change
- Add verifications and separation of duties
- Preventative accountability
- Examples
 - Signing your name at the bottom of a form
 - Requiring two signatures
 - Requiring physical check-offs



Matches Lost due to Software Failures



0

Matches Lost due to Software Failures



0

Production Failures Caused by Software



For resources and my blog, visit

alexbeaver.com

Connect With Me

 [/in/alex-beaver](https://www.linkedin.com/in/alex-beaver)

 [@alexcbeaver](https://twitter.com/alexcbeaver)