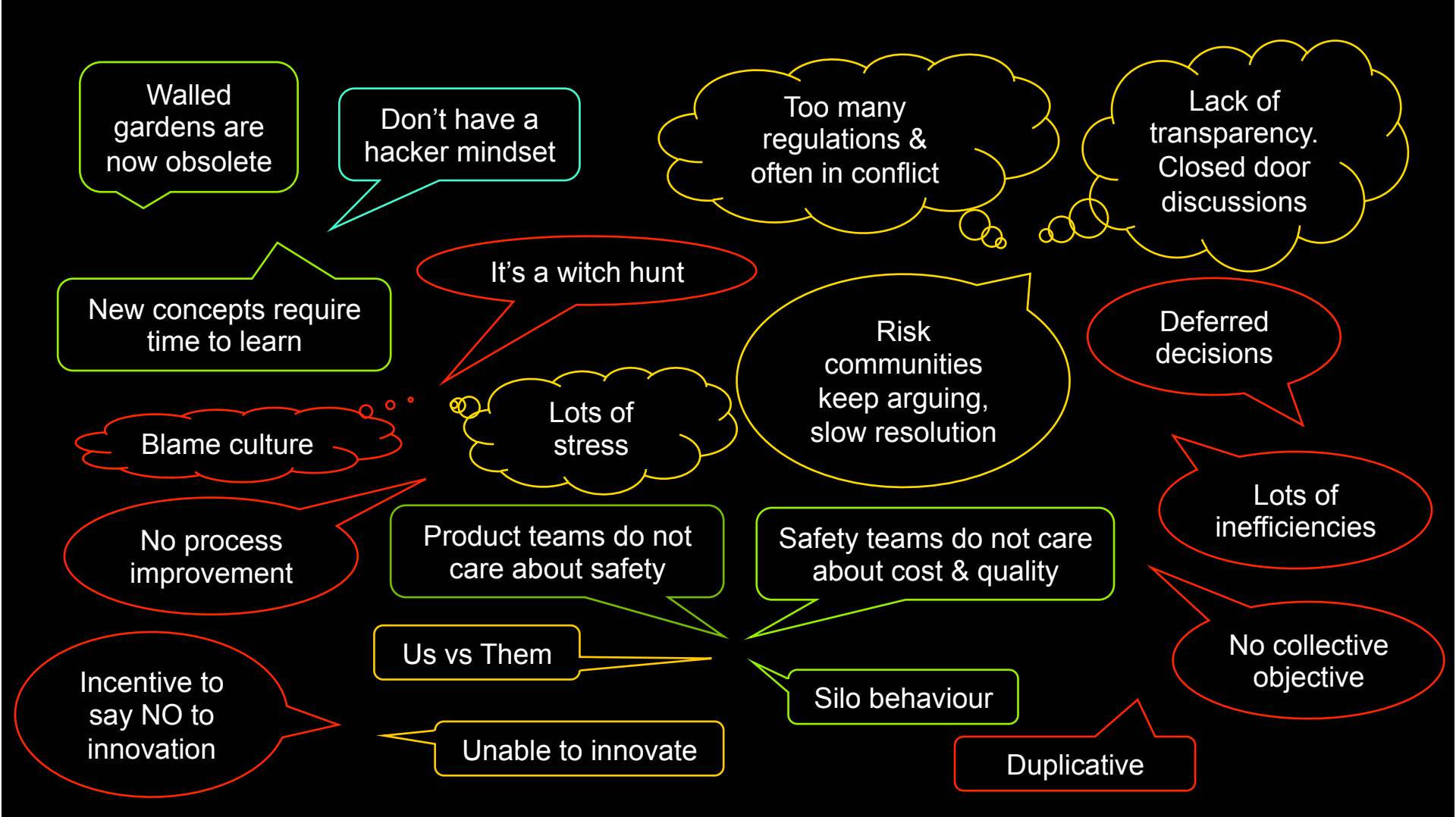
Risk & Control is Dead
Long live Risk & Control!

Quotes


Walled gardens are now obsolete
Don't have a hacker mindset
Too many regulations & often in conflict
Lack of transparency. Closed door discussions
New concepts require time to learn
It's a witch hunt
Risk communities keep arguing, slow resolution
Deferred decisions
Blame culture
Lots of stress
Lots of inefficiencies
No process improvement
Product teams do not care about safety
Safety teams do not care about cost & quality
Us vs Them
No collective objective
Incentive to say NO to innovation
Silo behaviour
Unable to innovate
Duplicative

BBC Home More

NEWS

Business

British Airways faces record £183m fine for data breach

8 July 2019

BBC Home More

NEWS

Technology

UK watchdog plans to fine Marriott £99m

9 July 2019

BBC Home More

NEWS

Technology

Equifax to pay up to $700m to settle data breach

22 July 2019

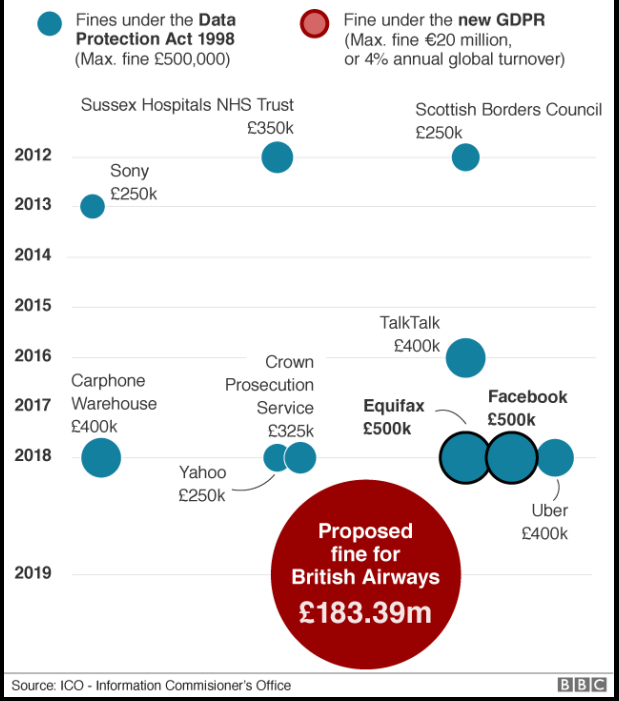
BBC NEWS

Capital One data breach: Arrest after details of 106m people stolen

30 July 2019 US & Canada

Biggest fines for data breaches

Fines over £250,000



Source: ICO - Information Commisioner's Office BBC

NotPetya
$10,000,000,000*

$870m Merck
$400m FedEx
$300m Maersk
4 hospitals
6 power companies
2 airports
22 banks
300 companies

*source: White House

What are you optimising for?

Antipattern 1
Lack of safety within safety

Head of Regulatory Compliance
Gobal Enterprise, 2019

“It’s a witch hunt, there’s always someone to blame. ISO9000 says treat exceptions as learning experiences, it doesn’t happen”

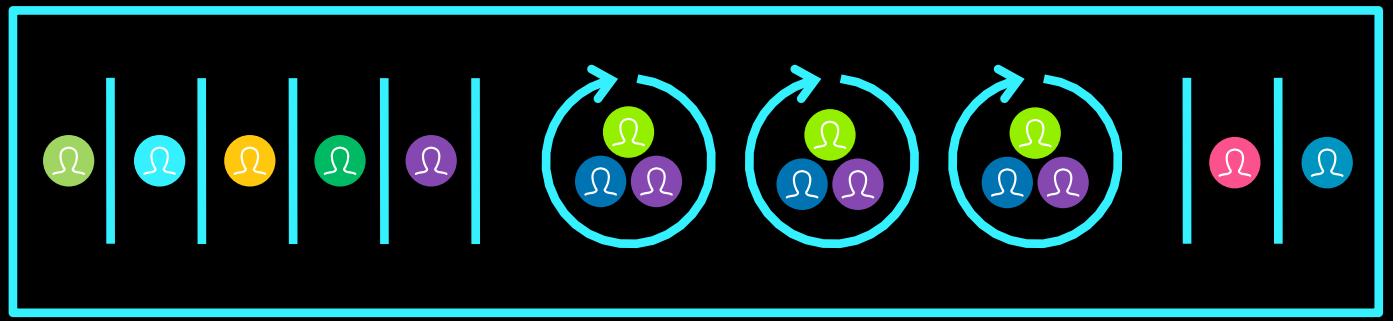
Professor Sidney Dekker
DevOps Enterprise Summit 2017

“Inverse correlation between number of incidents reported, honesty, and things actually going wrong”

Is your Risk & Control culture keeping your organisation safe?

Safe to learn?
Bad news buried?
Safety within safety?

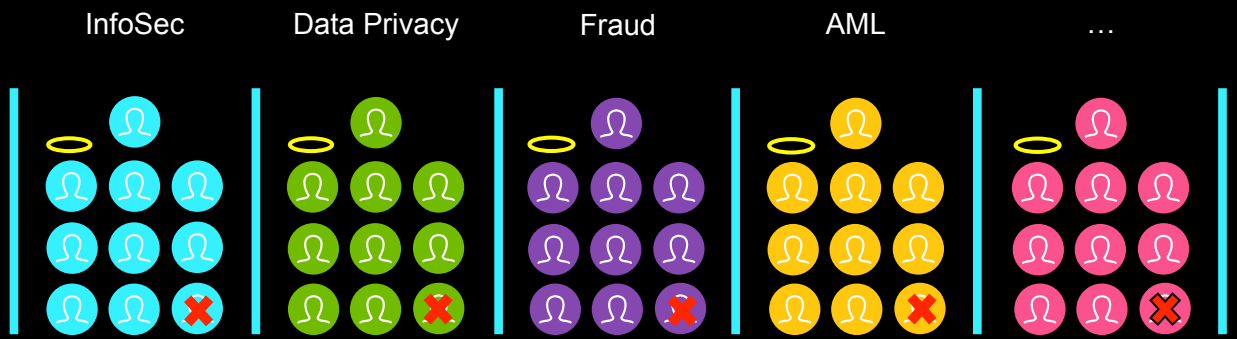
Antipattern 2
Role Silos



Solution pre-determined (BUFD)
Risks pre-determined (BUFR)
At point least is known
Handoffs
Time slicing & context switching

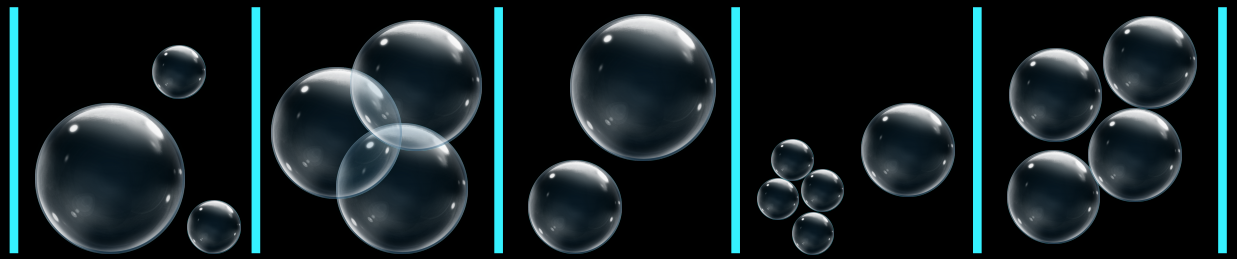
First learning
Risk back-loaded
Unplanned work
Big Bang

What are you optimising for?



What are you optimising for?

The Bubble Effect



What are you optimising for?

Antipattern 3
Fixed Mindset to Risk


#MaximumPossibleCompliance (#MPC)

“You need a perimeter to keep criminals out, and you need to think wider.

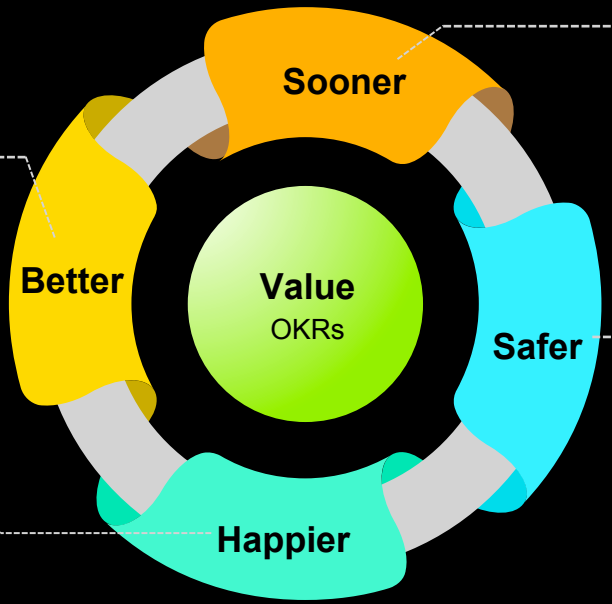
You have to assume that the increasing number of state-level attacks are all going to be 100% successful.”

Adam Banks, CIO, Maersk

Patterns

What do you *want* to optimise for?

Better Value Sooner Safer Happier



Sooner
Lead Time,
Throughput,
Flow Efficiency

Better
Quality

Safer
Intelligent Control,
Agile not Fragile

Happier
Colleagues, Customers,
Citizens and Climate

People ➡ Process ➡ Tooling

Pattern 1
People: Psychological Safety

Professor Sidney Dekker, DOES 2017

Factors in things that go wrong

Human errors

Guidelines not followed

Communication failures

Miscalculations

Procedural violations

Professor Sidney Dekker, DOES 2017

Factors in things that go right

Human errors

Guidelines not followed

Communication failures

Miscalculations

Procedural violations

Professor Sidney Dekker, DOES 2017

“The difference between things going wrong and things not going wrong,
is not in the absence of negatives,
it is in the presence of positives”

Ability to say stop

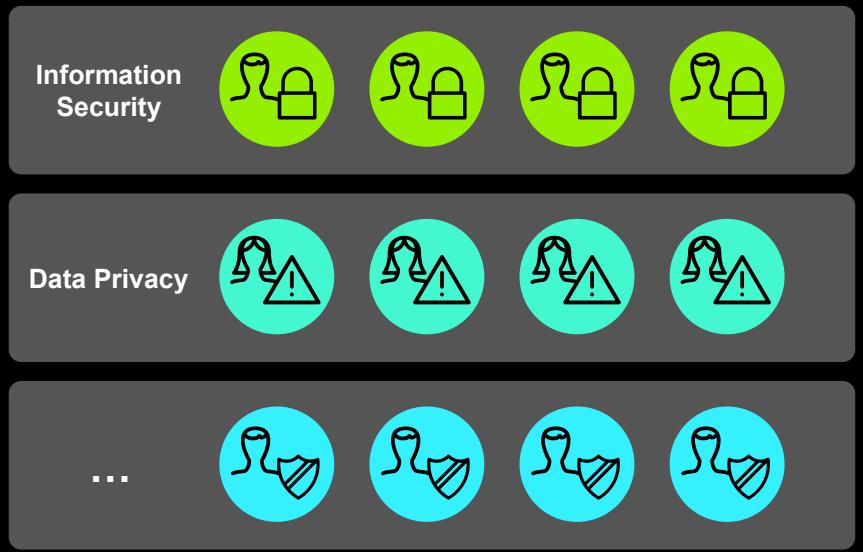
Past success not taken as a guarantee

Diversity of opinion, dissent

Keep discussion on risk alive

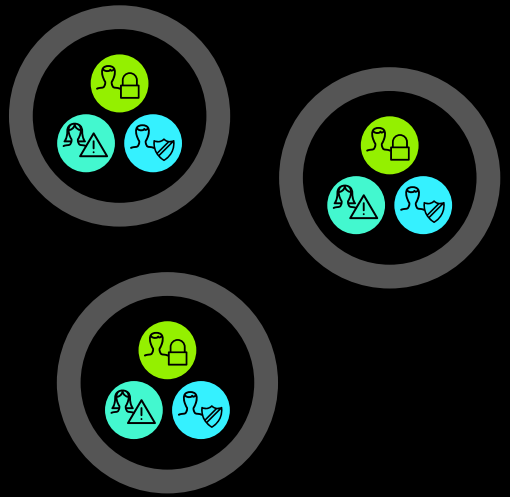
Pattern 2
People: Safety Teams

From Role Silos



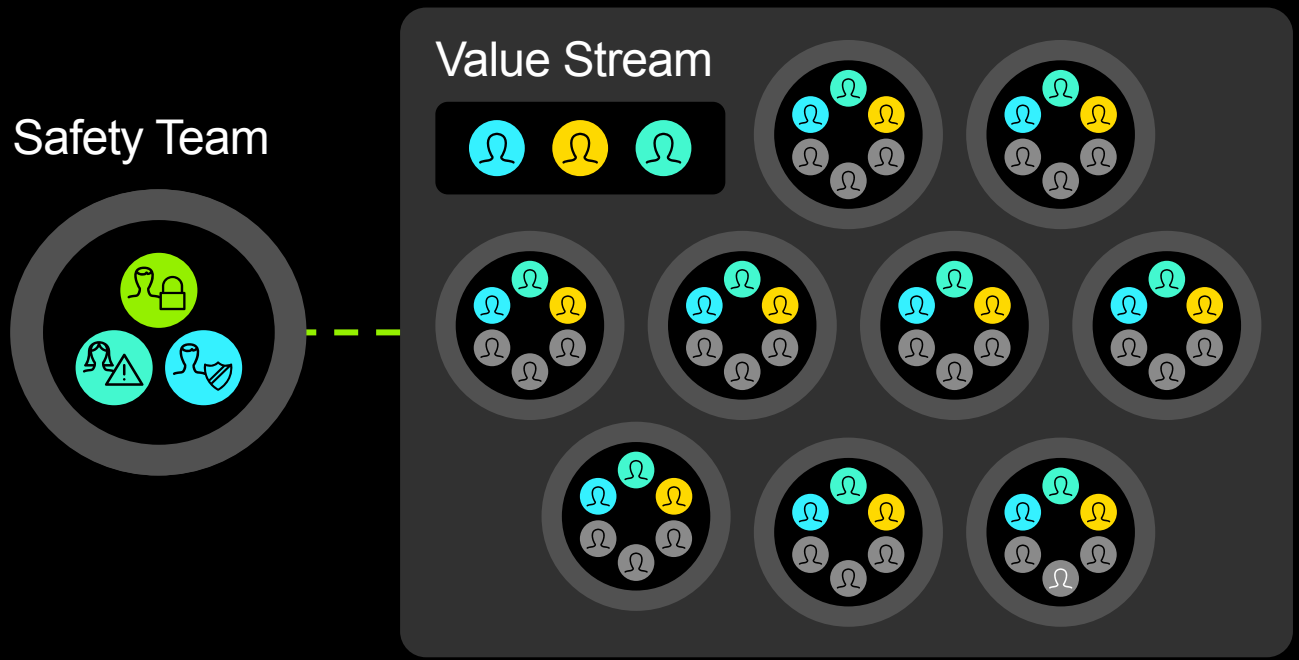
Siloed, temporal,
timesliced, context switching

To Safety Teams



Multidisciplinary, small, long-lived,
value stream aligned, safety teams

Pattern 3
People: Shared Purpose



Shared Purpose

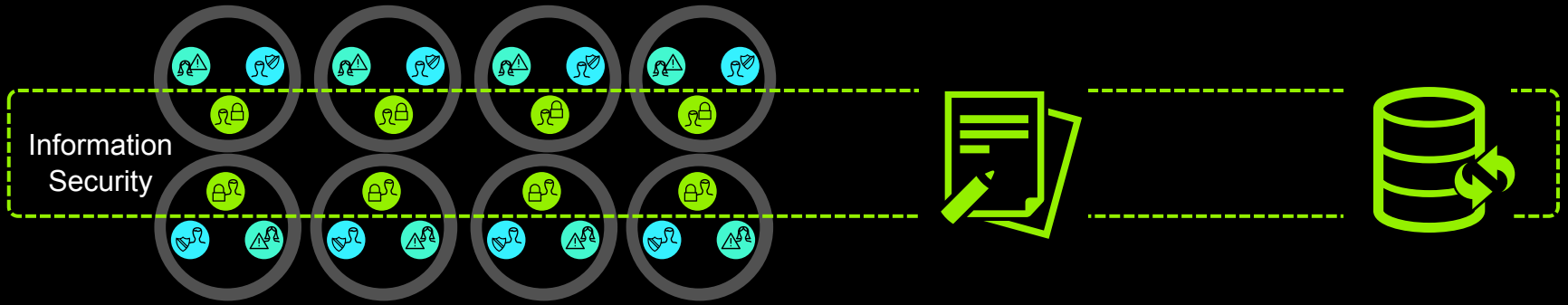
Shared Accountability

Customer aligned

Context sensitive

Optimised for learning

Safety Authorities



Mobilise Safety Teams
Servant Leadership
Community, Innovation
Foster a learning organisation

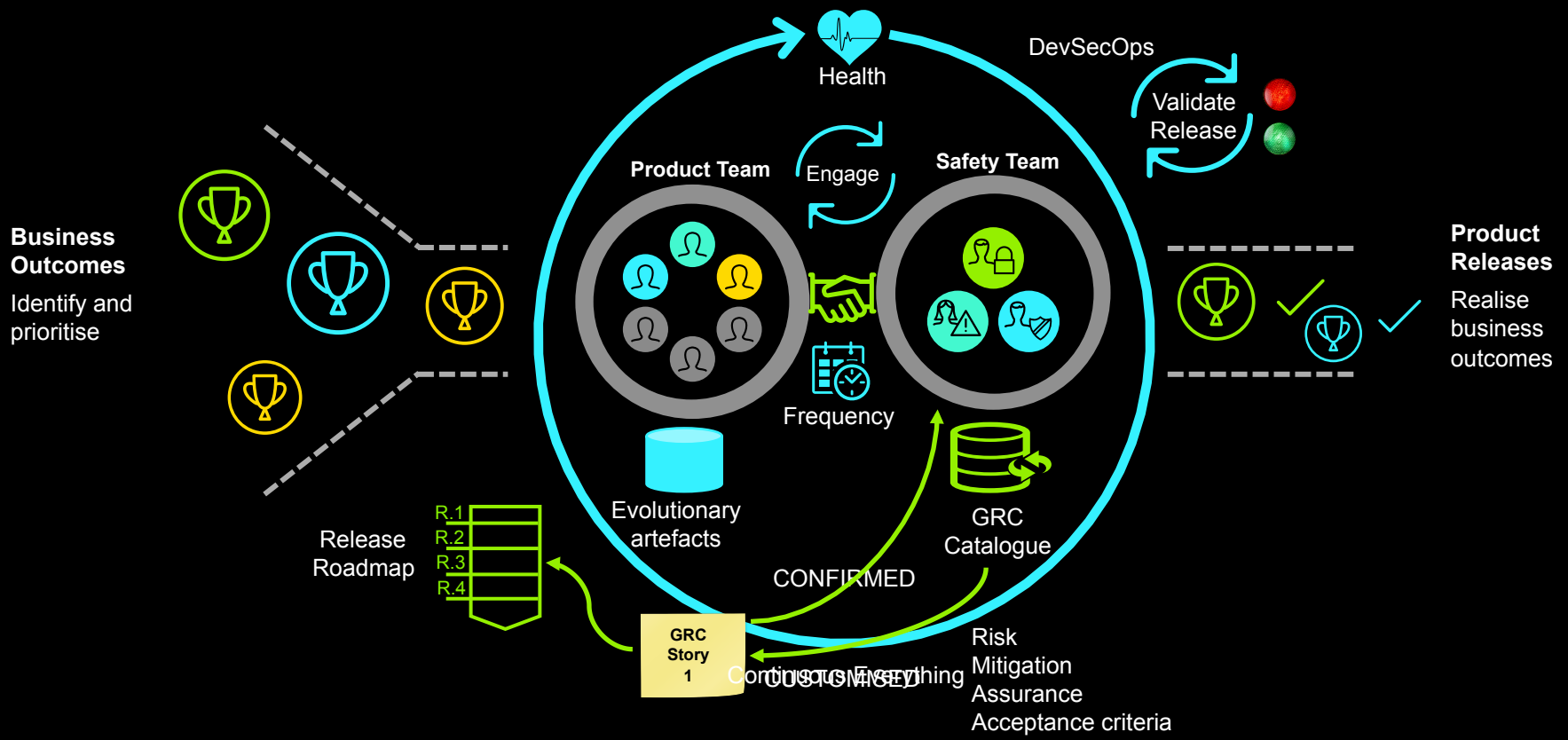
Policy & Standard
Risk Appetite

~~Specify solutions~~

GRC Catalogue

Pattern 4
Process: Intelligent Control

Intelligent Control



<Risk Story template here>

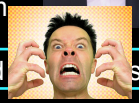
True Story

Research Team

We have a great opportunity for machine learning and want to import a 90TB dataset from a 3rd party vendor

We will be disrupted! We can't compete!

Product Team



Our data and [illegible]s in the cloud

Can we import from vendor's cloud account to our own?

Err… that's nuts. How about we press the button "Big Data Xfer" on our cloud control panel?

OK… how about we just do the scans ourselves in the cloud?

Hmm. This is ASCII data. How about we get to the whiteboard and work out an alternative set of mitigations?

Options 1..2..3..4..?

Great. We can code this in 2 weeks

….

We're done, please can you validate?

Safety Team

Engage

The standard says use an approved method:
- encrypted physical disk (x90 disks)
- secure download to on-prem (3 months)

That button has not yet been security verified. Everyone is too busy. It will be at least 6 months

Our approved method for malware scanning is not available on the cloud

OK. Our risk appetite requires us to ensure there is no malware in imports but perhaps we can find a new way to do this

Option 3 is best. Using massively parallel lambda scanning in an 'airlock' account we can verify 90TB in minutes not months

Risk Story

We have raised a risk story

Confirm

Agreed this meets the pattern

Stop. No innovation. Fixed mindset.

We are the dream team !

Safety Differently

Curiosity	over	Control
Participation	over	Prescription
Involvement	over	Instructions
Diversity	over	Deference

Intelligent Control enablers

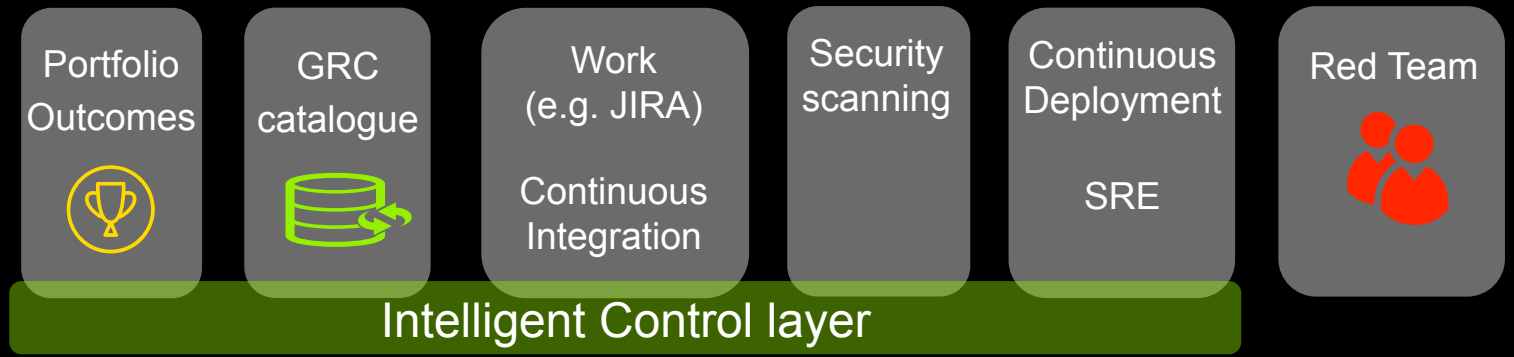
- Psychological safety within safety
- Standards set risk appetite
- Shared purpose & technical excellence
- Emergent mitigation & continual improvement

Source: Sidney Dekker, 2018
www.safetydifferently.com
https://www.safetydifferently.com/i-am-not-a-policy-wonk/

Pattern 5
Tooling: Install Traceability

From DevSecOps To

Sec Dev Sec Ops Sec



6 Things To Get Started

- ✓ Start small, learn fast
- ✓ Engage leaders
- ✓ Invite first value stream and first safety team (Rule of One)
- ✓ People: Focus on effective conversations
- ✓ Process: small safe-to-learn experiments
- ✓ Tooling: minimal viable tooling to start

Learn Fast
Stay Safe
Together

Thank you

deloitte.co.uk/BVSSH

medium.com/sooner-safer-happier