

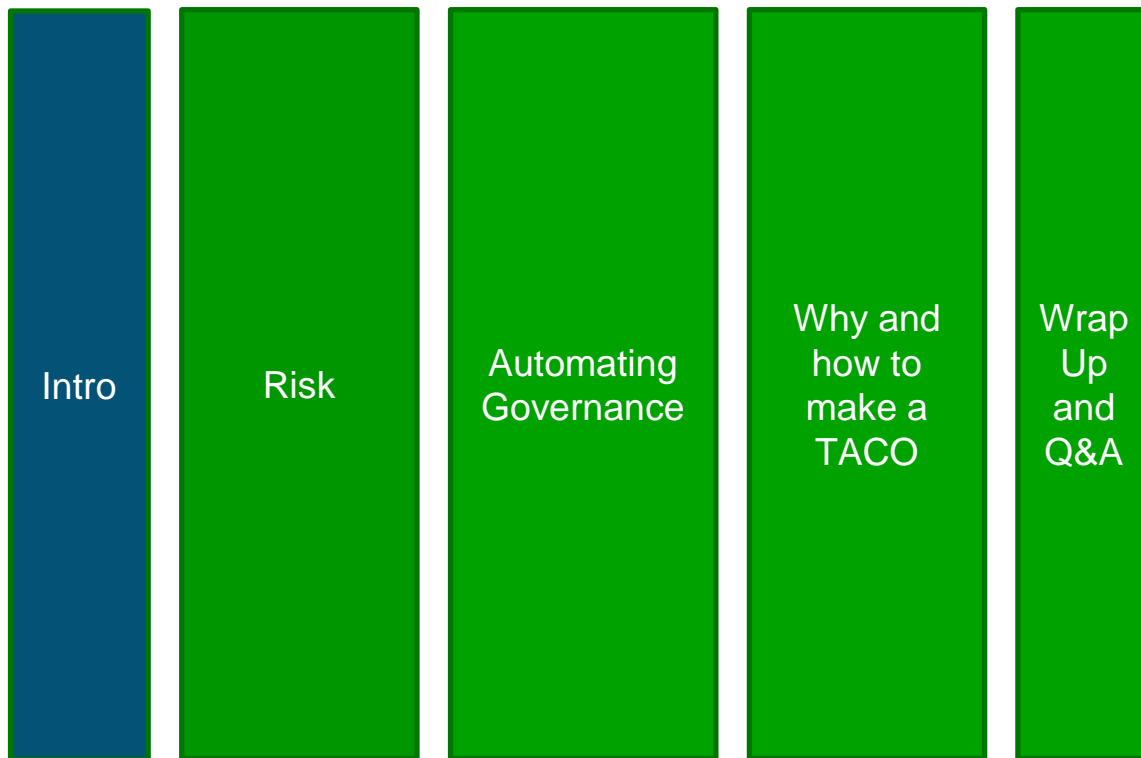


# Securing your pipes with a TACO

The people and process of automating governance

Peter Maddison

# Talk map



# Who am I?



Peter Maddison

Coach, consultant, founder...



peter.maddison@xodiac.ca



@pgmaddison



<https://www.linkedin.com/in/peter-maddison/>

In our fast-paced world  
customers demand instant  
gratification

# Moving towards value delivery

1990's and before



1990 to 2020



2020 and beyond



Driving  
efficiency

Invest in technology  
capabilities

Drive immediate  
customer value

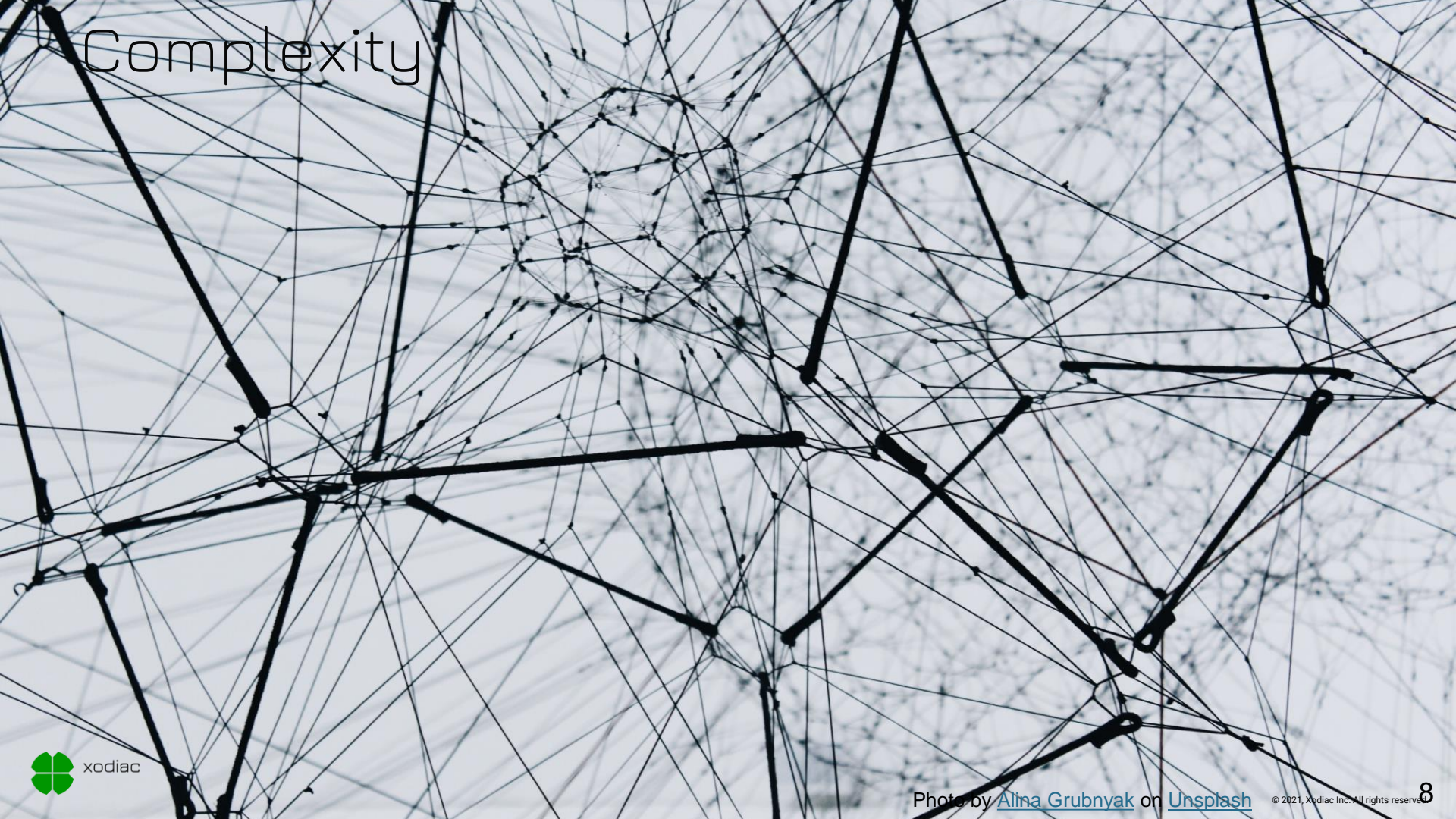


# Efforts Fail From Lack of Clarity, Not Tools

- Micromanagement
- Lack of Capability
- DevOps Team Silos
- Not Taking a Holistic Approach
- Doing Without Learning
- Lack of Shared Ownership
- Broken-Window Syndrome
- Fear of Failure
- Lack of Psychological Safety
- Lack of Valuable Measurement
- Lack of Vision
- Lack of Visibility
- Unspoken Disagreements
- Failure to Scale Pilots
- Unrealistic Expectations
- Overlooking Organizational Change
- Overemphasis on Velocity
- Automation Without Value
- Ineffective Measurement
- Ignoring Existing Process
- Ignoring Lean and Agile Principles
- Imbalanced Top-Down/Bottom-Up Approach
- Neglecting Stakeholders Beyond Dev / Ops
- Lack of Incentive and Governance Adaptation







# Complexity



xodiac



# Talk map

Intro

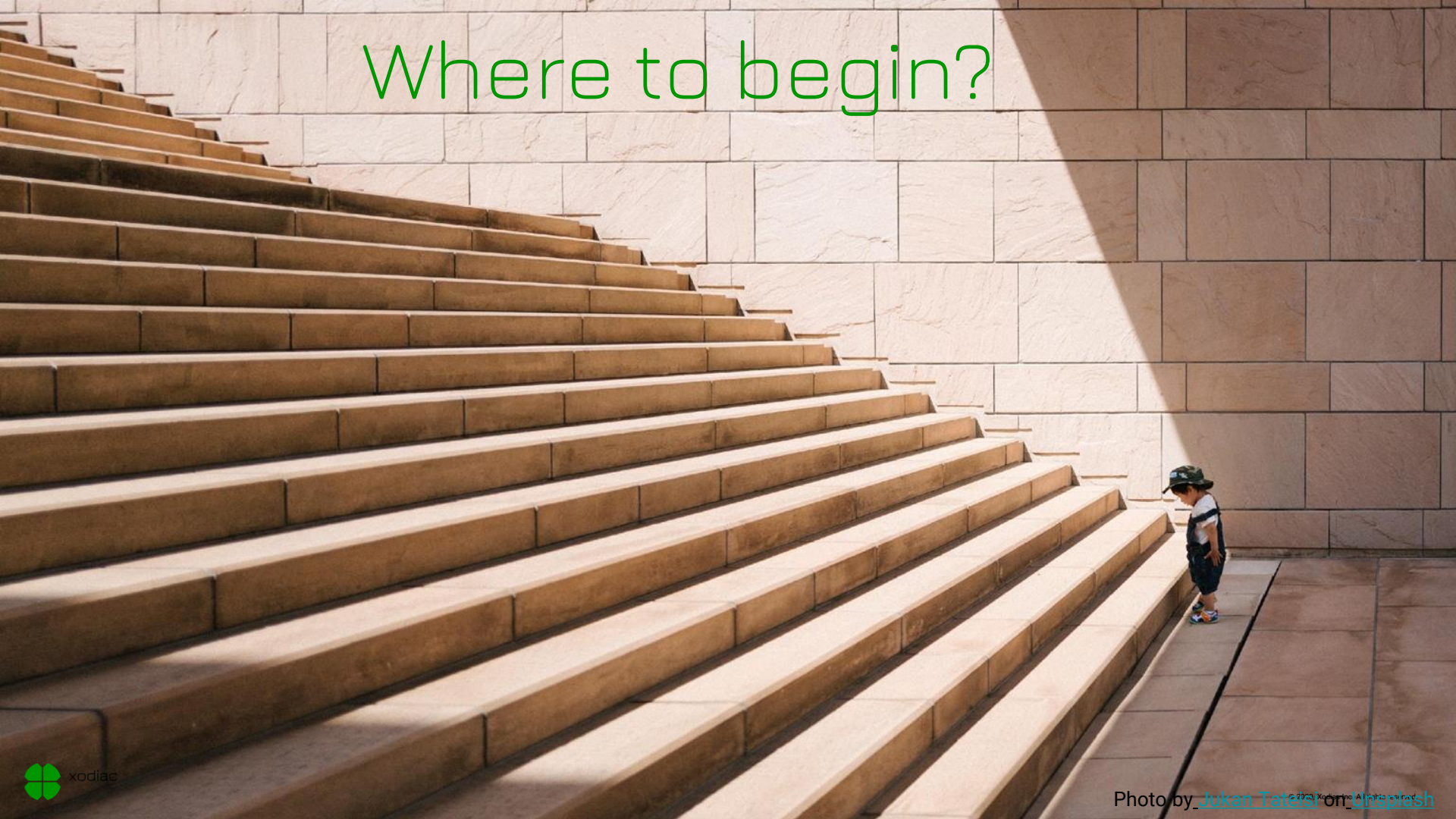
Risk

Automating  
Governance

Why and  
how to  
make a  
TACO

Wrap  
Up  
and  
Q&A

# Where to begin?



xodiac

Photo by [Jukan Tatal](#) on [Unsplash](#)

# Introducing change



“This year, I resolve to stay away from unnecessary risks.”

“<sup>?!?</sup> People, processes and tools working together to enable rapid and continuous delivery of value to customers.”

- A bunch of people



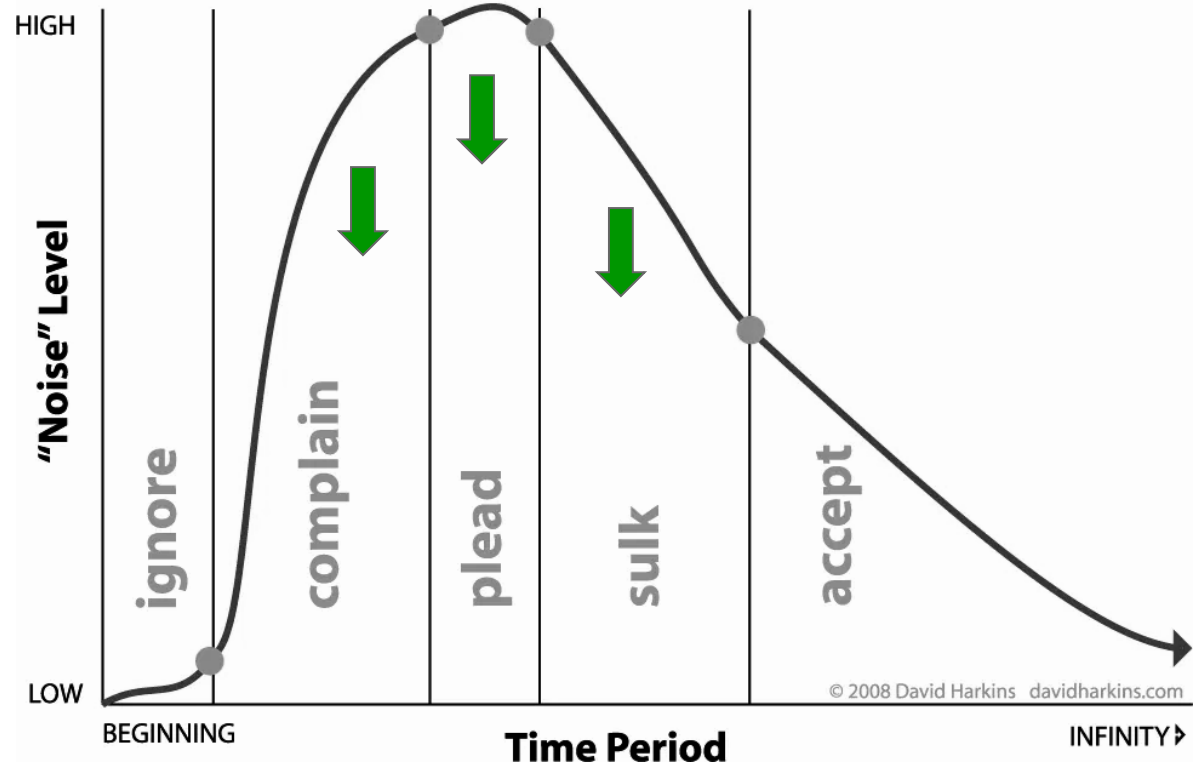
Introducing:

- New paradigms
- New ways of working
- Necessary training

All while meeting  
any obligations to  
existing  
commitments

## Change Adoption Curve

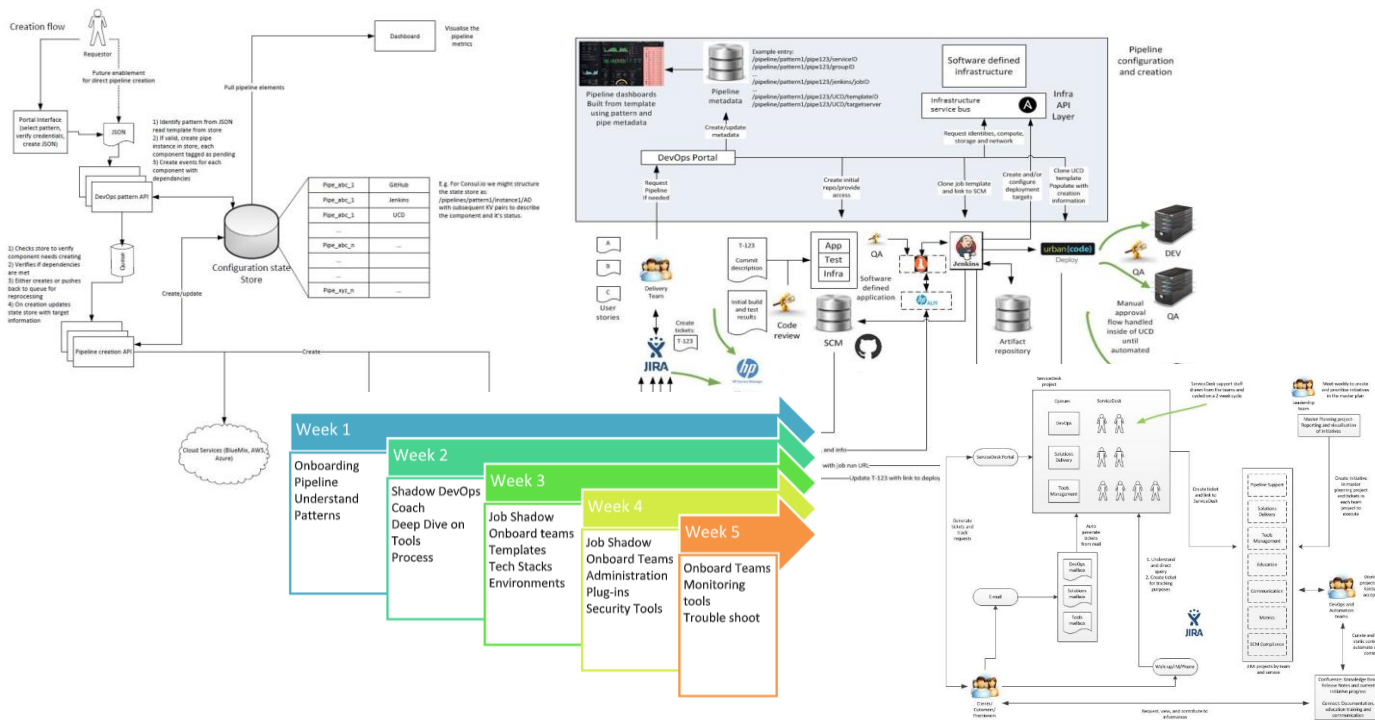
How humans react to change



xodiac



# Bunch of pictures



# Hitting a wall



# Lost in translation

**Developers**

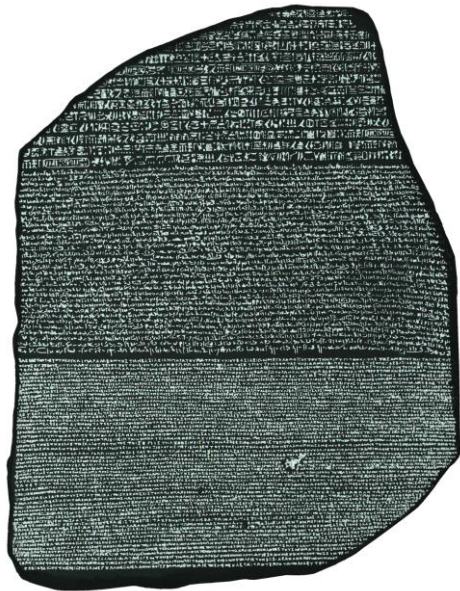
**Compliance**

**Security**

**Testing**

**Operations**

**Architecture**

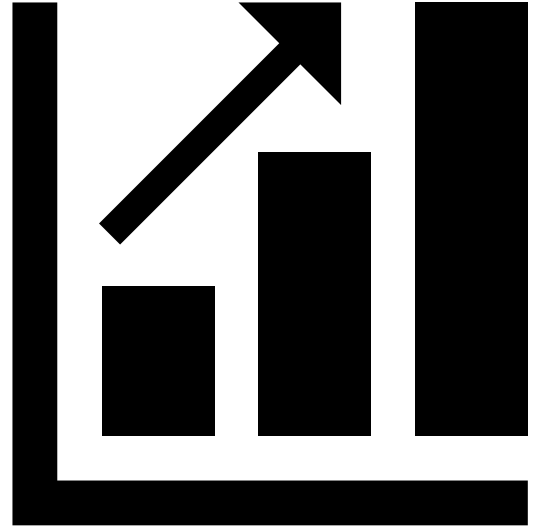




Creating alignment

# How will we measure?

- Incremental improvements
- Quantify risk
- Anomolies



# Talk map

Intro

Risk

Automating  
Governance

Why and  
how to  
make a  
TACO

Wrap  
Up  
and  
Q&A



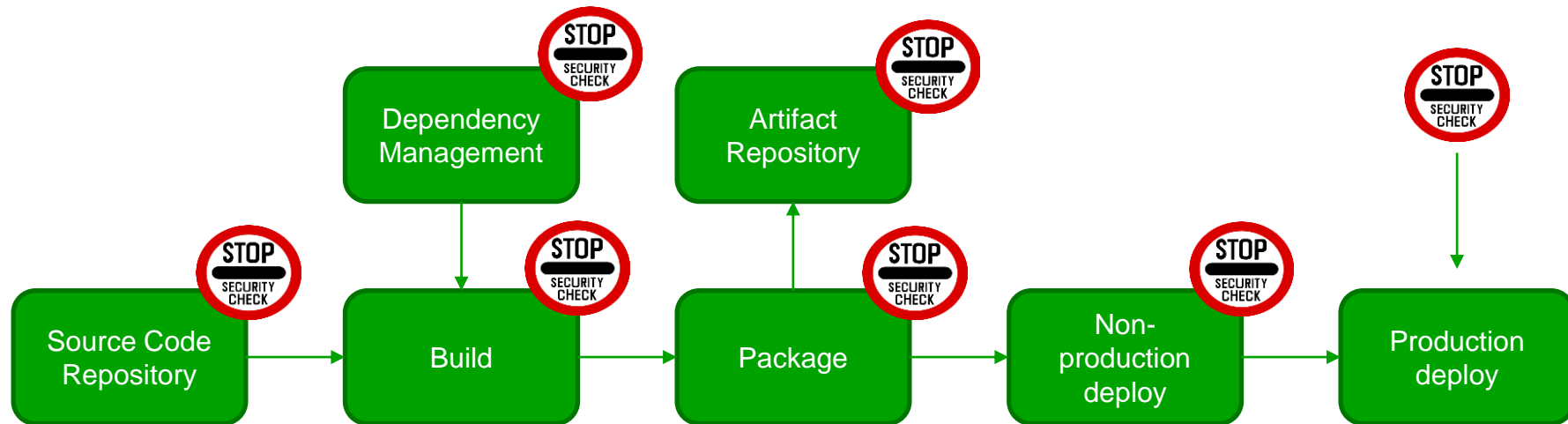
A close-up photograph of a person wearing a white chef's coat, holding a white smartphone in their left hand and pointing at the screen with their right index finger. The background is a plain, light-colored wall.

# Is there a risk?

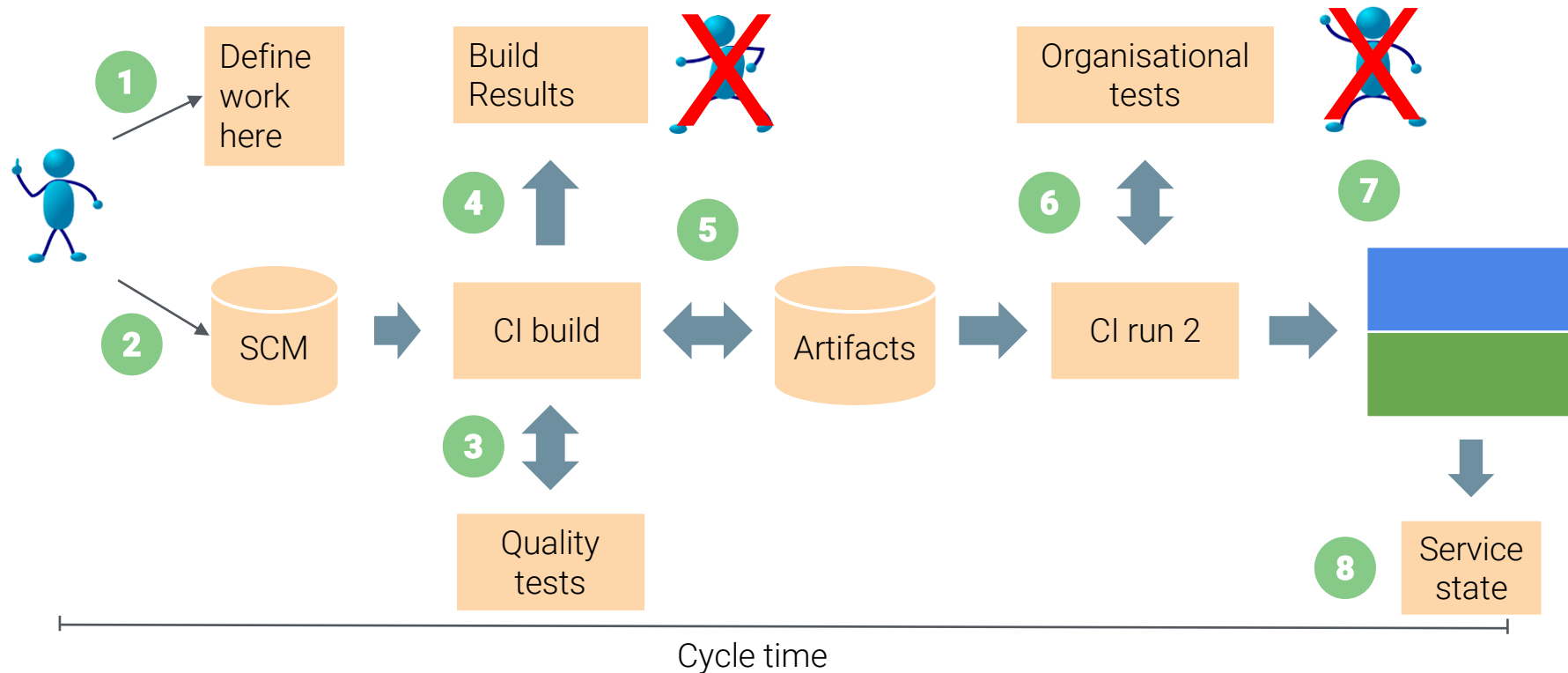


xodiac

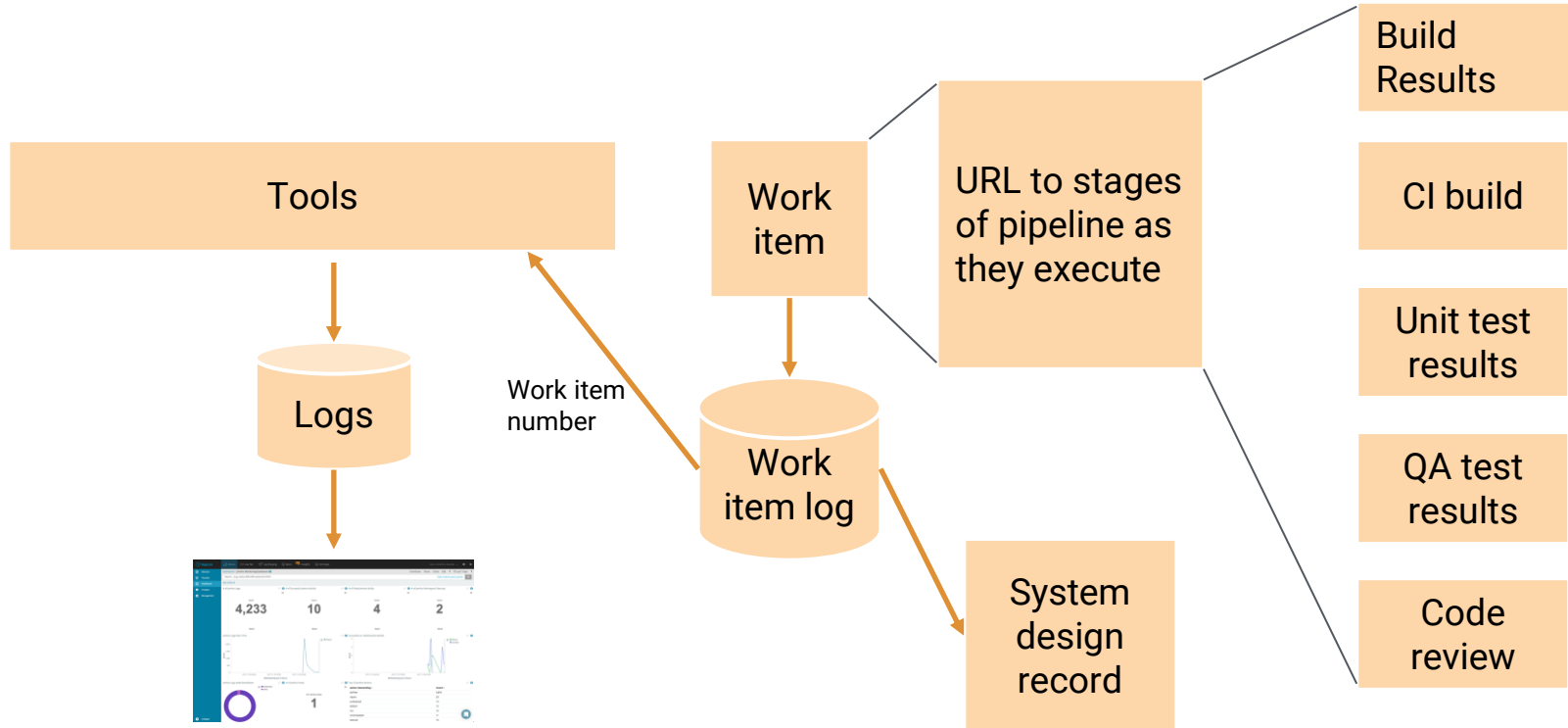
# Let's start with the pipeline



# Running the pipe



# Auditing the pipe



# Paved road



xodiac

Photo by Jon Flobrant on Unsplash

© 2020 xodiac. All rights reserved.



# Beyond roadmaps

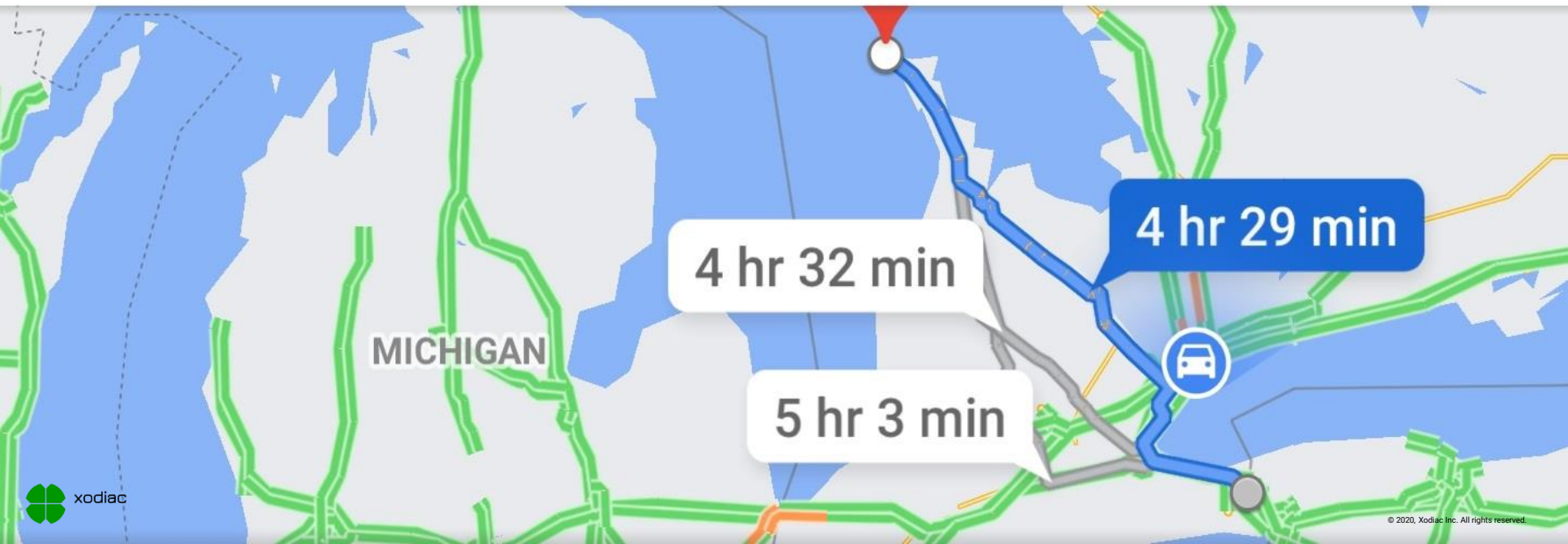


to Tobermory

 4 hr 29



 3 days





# Automating Governance

- Not about keeping audit off your back
- Start small, get one team working and grow from there
- Engage leaders, focus on conversation, not tooling

# Talk map

Intro

Risk

Automating  
Governance

Why and  
how to  
make a  
TACO

Wrap  
Up  
and  
Q&A

# Modeling

Identify what happens in the pipe

Secure the delivery process

Validate the payload in the pipe

Record execution and monitor

## Traceability

1

- Chain of custody
- Test results for all
- Deployed version is tracked
- Change is recorded

*Ensure traceability exists*

## Access

2

- Source code managed
- Creator tracked
- Build once, deploy many
- Pipelines only

*Validate access*

## Compliance

3

- Peer review
- Scan the code
- Scan the artifact
- Manage the data

*Ensure issues are addressed*

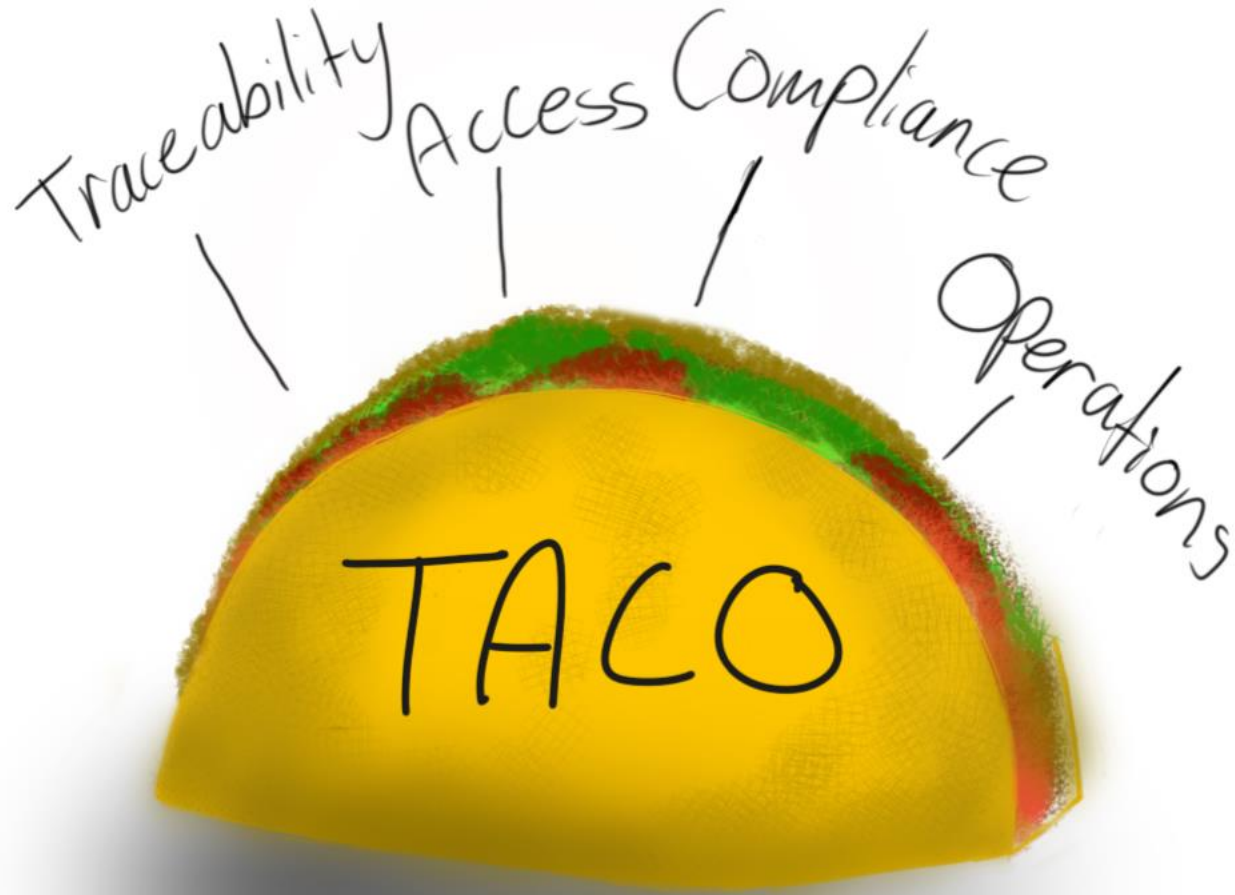
## Operations

4

- Validate the target
- Validate quality
- Check it works
- Watch it live

*Strengthen team behaviour*

# TACO!

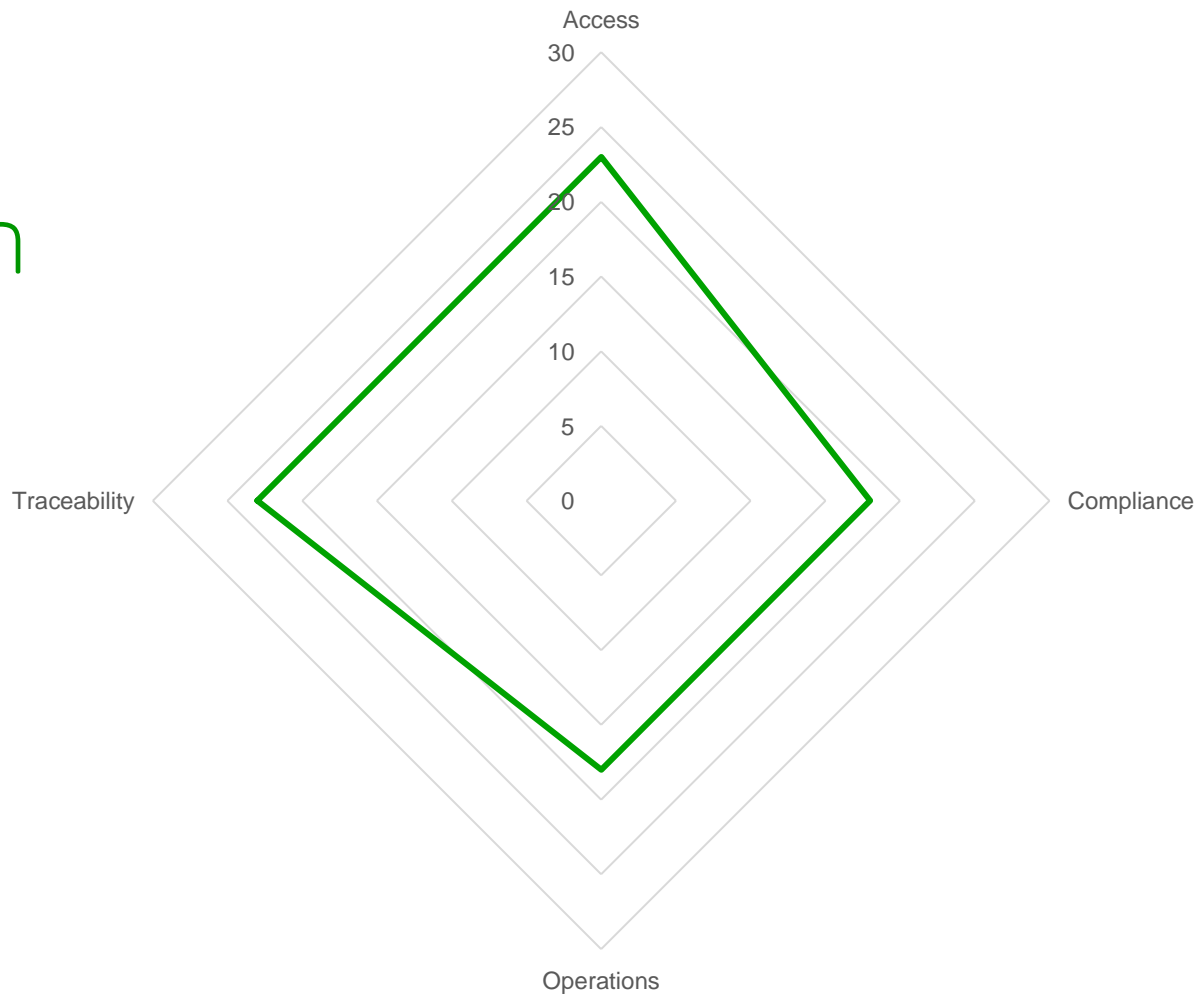


# Example

Purpose	Control	Artifact	Location	Control is passed	Control is failed	Owner
To ensure that for a given request for change, we have a valid chain of custody allowing us to trace where issues occur	All production deployments must have a ticket number. Developers must put the ticket number into the submitted pull request in order for the request to be pushed through to production. All ticket numbers since last production deploy must be included in the pull request.	Ticket	Jira	Pull request contains a valid ticket number and	If PR doesn't contain ticket number, build proceeds but only deploys to dev.	Team lead

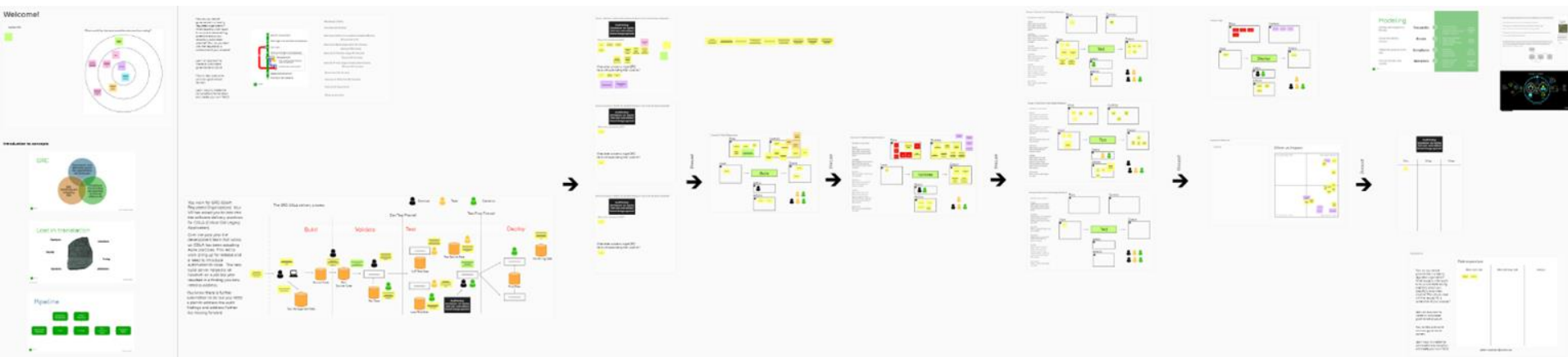
Then link this to the tasks to create and the impediments to success

# Visualize how much TACO





# Initial controls design



# Mapping the controls

## Exercise 3: Validate Design Breakout

Questions for each box:

1) Input

What inputs do we have?

How might controls have added/improved/modified them?

2) Output

What outputs do we want to have from this process?

What would a good output look like?

3) Actors

Who is involved? (Use icons and stickies)

4) Actions

What actions occur here?

What are people and systems doing?

5) Risks

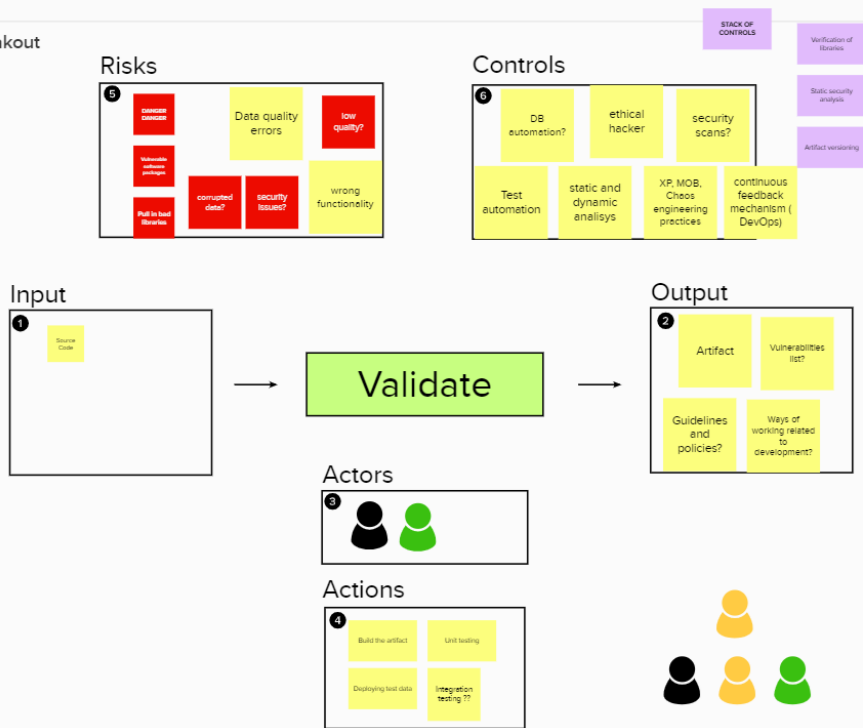
What risks do we see?

What could cause the process to go wrong?

What problems would bad input cause? How about bad output?

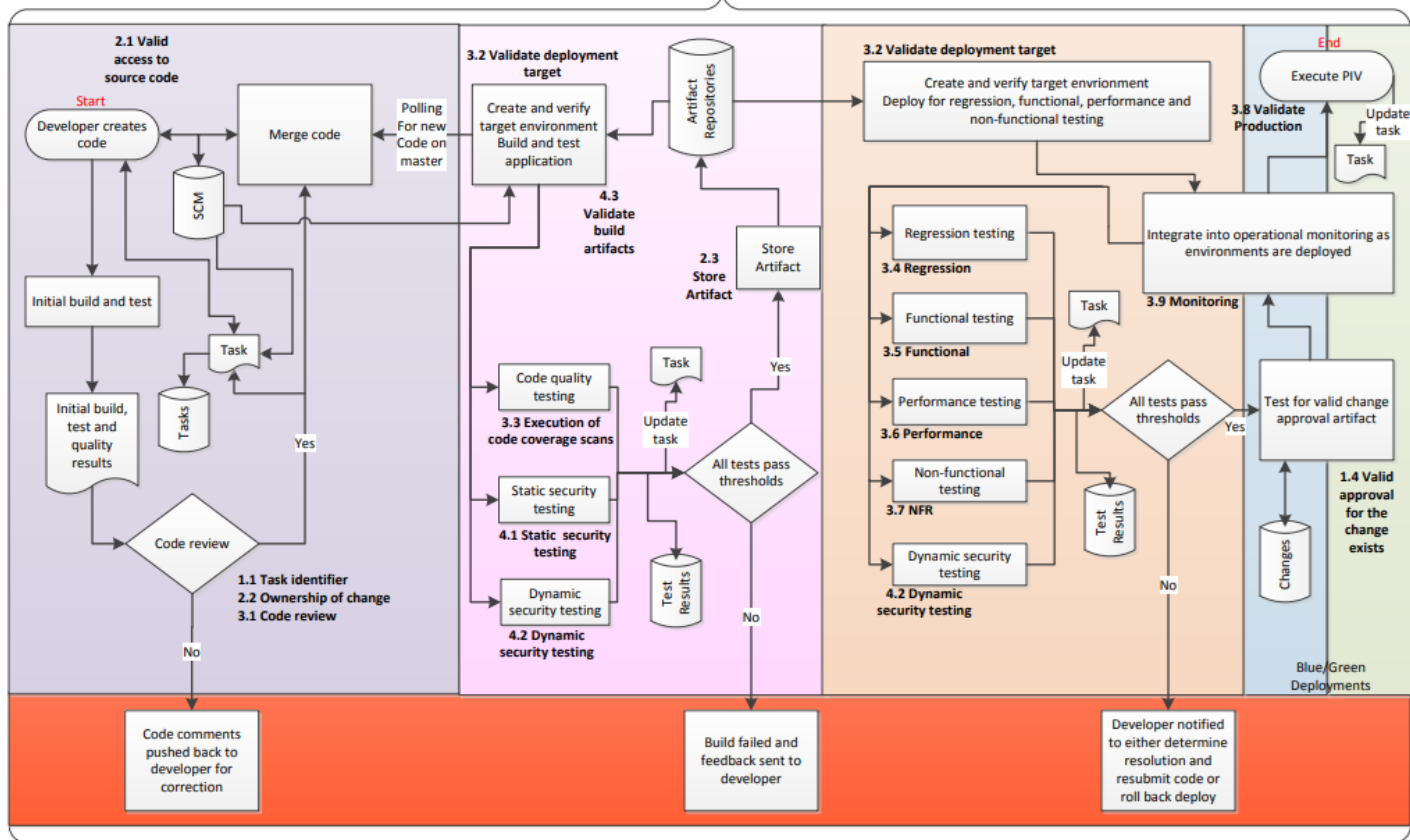
6) Controls

What controls will mitigate my risks?



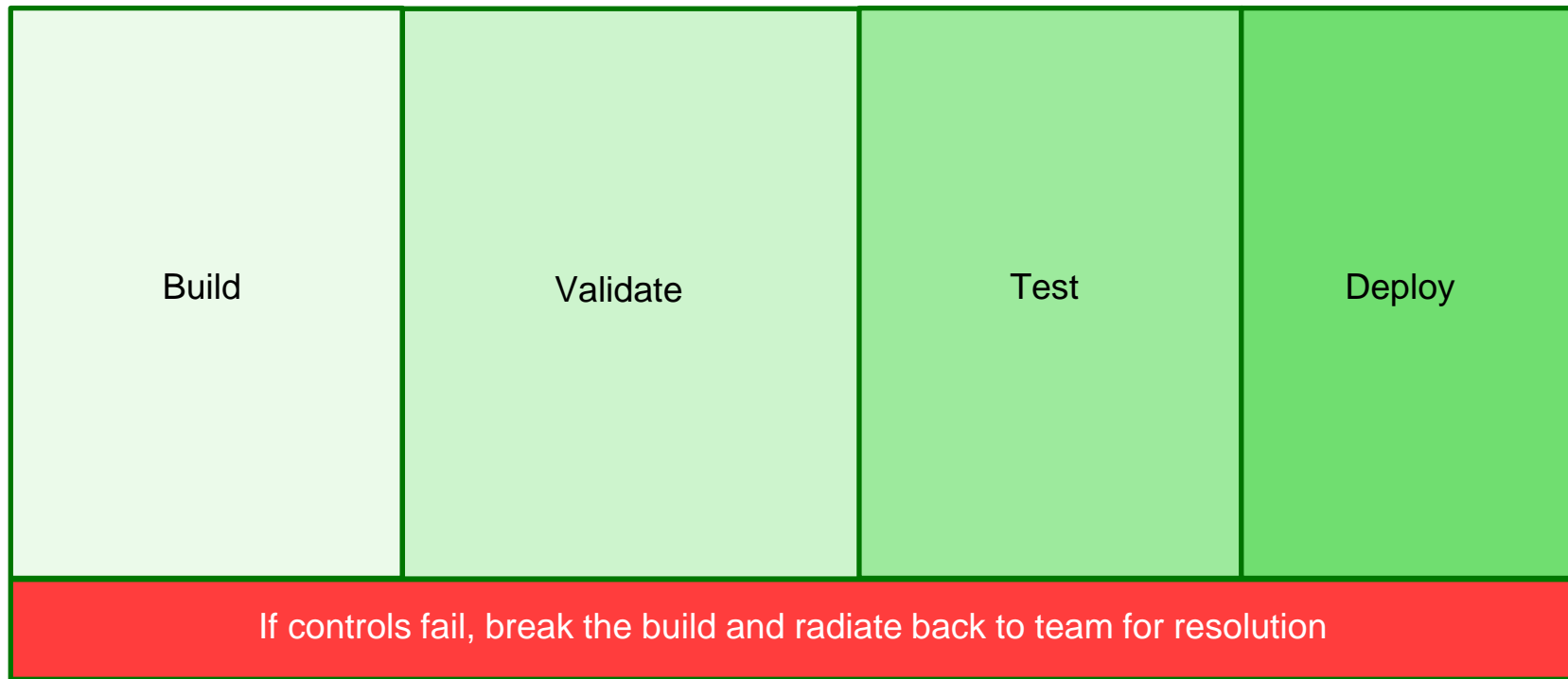
## Pipeline general case – Controls example

1.5, 2.5, 3.10 and 4.4  
Verification that the automated  
gates put into place are functioning  
as expected



1.2, 1.3, 2.4 and 3.9  
Traceability, access and monitoring including  
feedback loops

# Mapping the controls



# CapitalOne example

- Source code version control
- Optimum branching strategy
- Static analysis
- >80% code coverage
- Vulnerability scan
- Open source scan
- Artifact version control
- Auto provisioning
- Immutable servers
- Integration testing
- Performance testing
- Build deploy testing automated for every commit
- Automated rollback
- Automated change order
- Zero downtime release
- Feature toggle



# Another real world example

## Intelligent Control – Delivering Safer Value

### Building the Right Thing and Building It Right

#### Intelligent Control Enables...



Consistent risk assessments



Minimum Viable Control



Minimum Viable Governance



Control automation



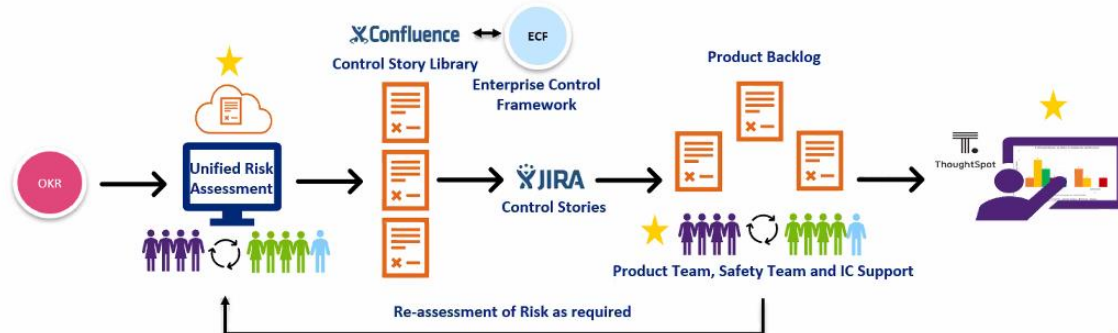
Continuous assurance



Full traceability



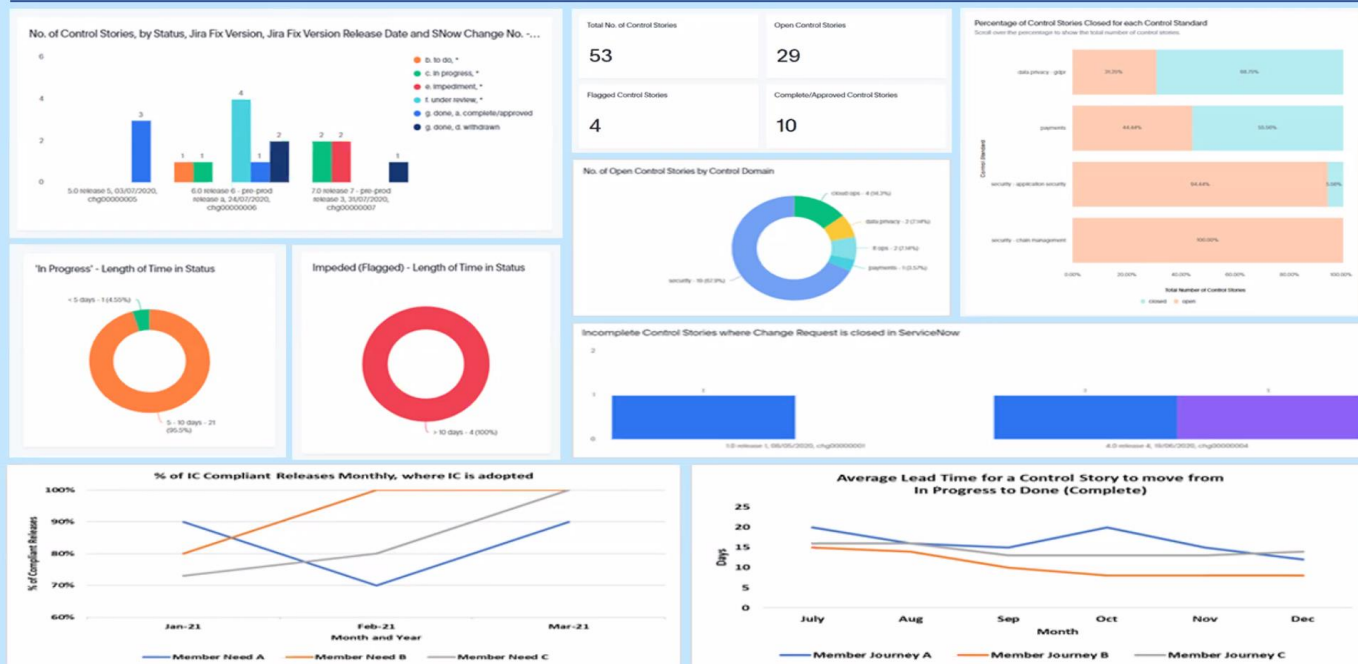
Increased flow



# Altogether now, measure

## Intelligent Control – Delivering Safer Value

Test Data only for Demonstration purposes



# DevOps

DevSecOps

RiskDevRiskOpsRisk

# Talk map

Intro

Risk

Automating  
Governance

Why and  
how to  
make a  
TACO

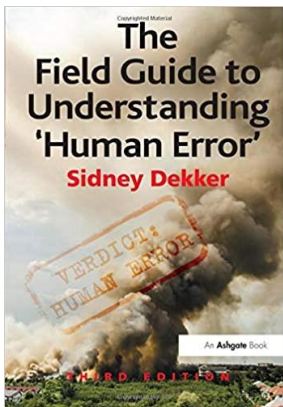
Wrap  
Up  
and  
Q&A



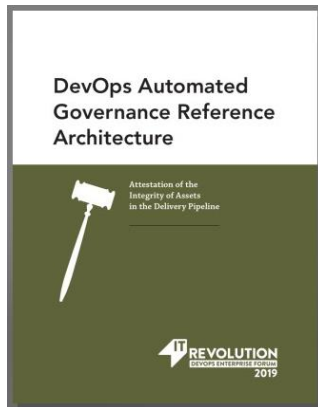
“We cannot solve our problems with the same thinking we used when we created them”

- Albert Einstein

# References



[https://www.goodreads.com/book/show/376964.Field\\_Guide\\_to\\_Understanding\\_Human\\_Error](https://www.goodreads.com/book/show/376964.Field_Guide_to_Understanding_Human_Error)



<https://itrevolution.com/forum-paper-downloads/>



<https://devopsinstitute.com/certifications/devsecops-foundation/>

CapitalOne Focusing on the DevOps Pipeline:  
<https://medium.com/capital-one-tech/focusing-on-the-devops-pipeline-topo-pal-833d15edf0bd>

Automated Governance – John Willis  
<https://www.youtube.com/watch?v=j9eB0fIttY>

Risk & Control is Dead, Long Live Risk & Control – Jon Smart  
<https://www.youtube.com/watch?v=XRMf9QjUwI>

# Let's review

- A way to create common understanding of a “good pipeline”
- Safety is about behaviour, not just tools.
- Ways to help automate software delivery compliance





xodiac  
making every team thrive

Feedback survey (only 1 question is required):

<https://forms.xodiac.ca/securing-your-pipes-with-a-TACO>

Thank you!



[peter.maddison@xodiac.ca](mailto:peter.maddison@xodiac.ca)

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

<https://www.linkedin.com/in/peter-maddison/>

