Securing your pipes with a TACO

The people and process of automating governance

Peter Maddison

Talk map

Intro

Risk

Automating Governance

Why and how to make a TACO

Wrap Up and Q&A
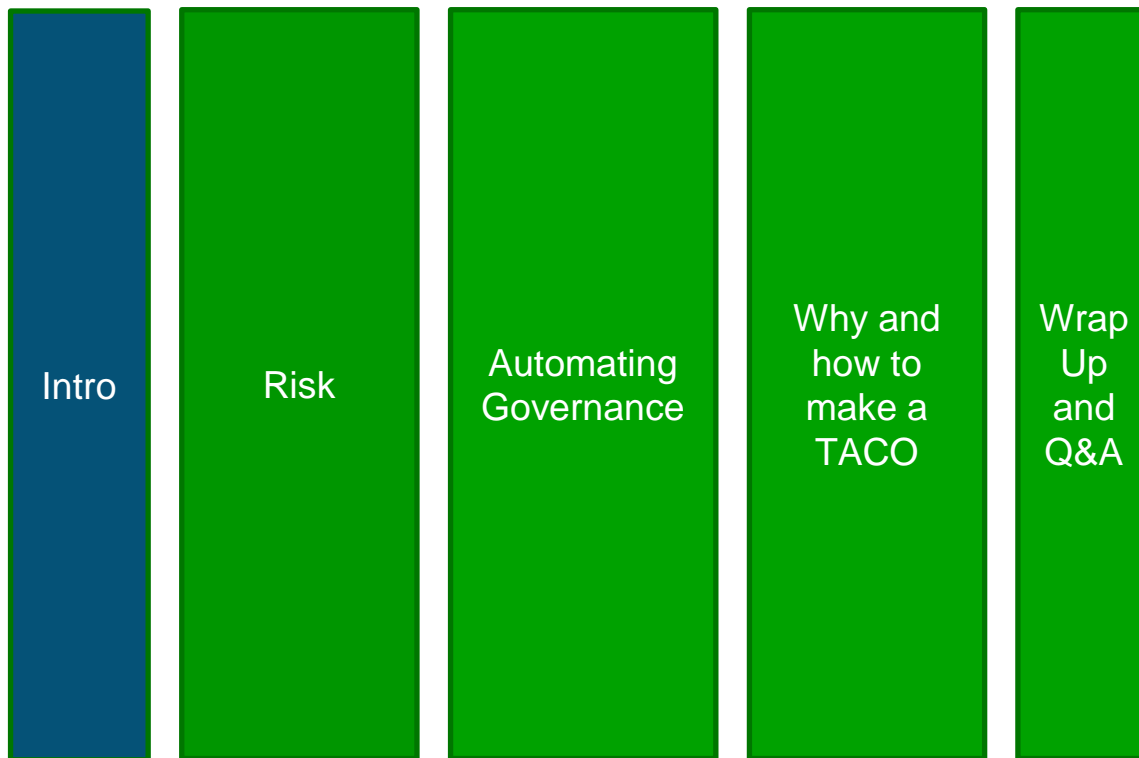
xodiac

Who am I?

Peter Maddison

Coach, consultant, founder...

✉ peter.maddison@xodiac.ca
🐦 @pgmaddison
in https://www.linkedin.com/in/peter-maddison/

xodiac

In our fast-paced world customers demand instant gratification

Moving towards value delivery
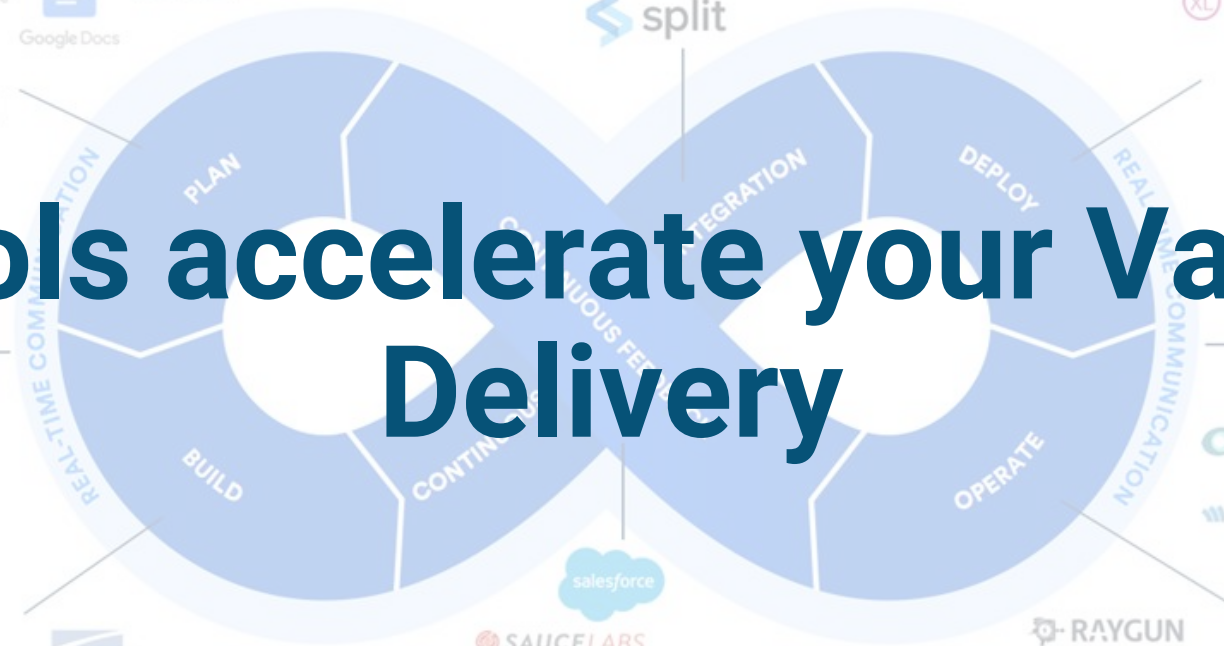
1990's and before

1990 to 2020

2020 and beyond

Driving efficiency

Invest in technology capabilities

Drive immediate customer value

xodiac

Tools accelerate your Value Delivery
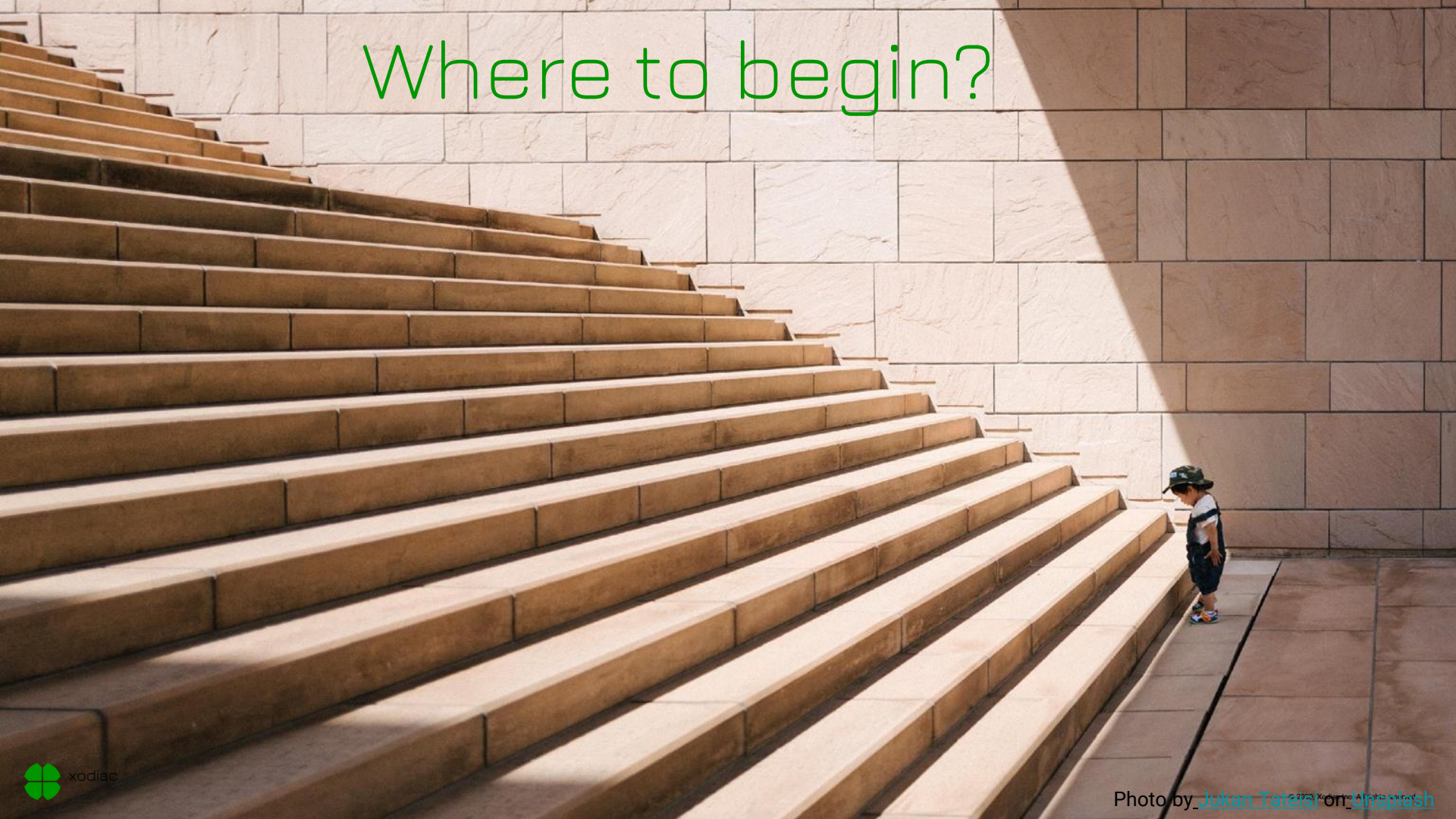
Efforts Fail From Lack of Clarity, Not Tools

- 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 Tooling
- Automation Without Value
- Ineffective Measures
- 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

xodiac

Sources: McKinsey, Boston Consulting Group, 2020

Where to begin?

Introducing change

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

xodiac

"*People, processes and tools working together to enable rapid and continuous delivery of value to customers.*"
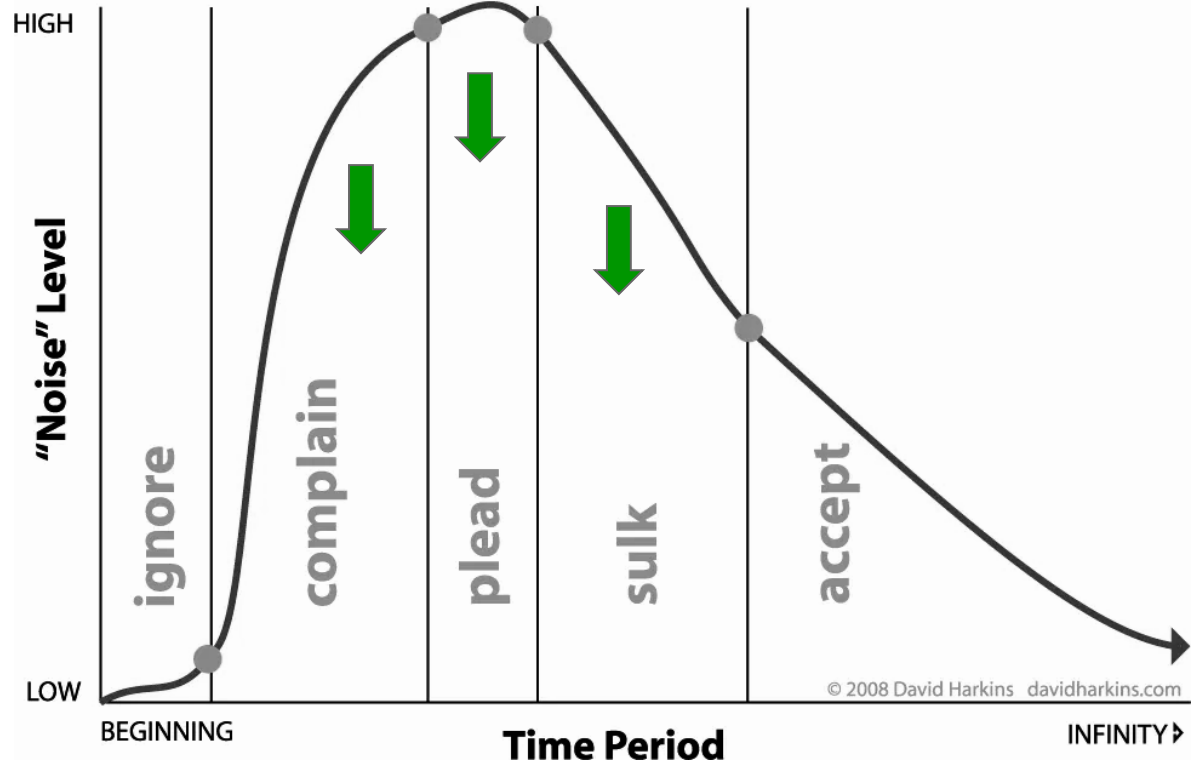
- A bunch of people

Introducing:

- New paradigms
- New ways of working
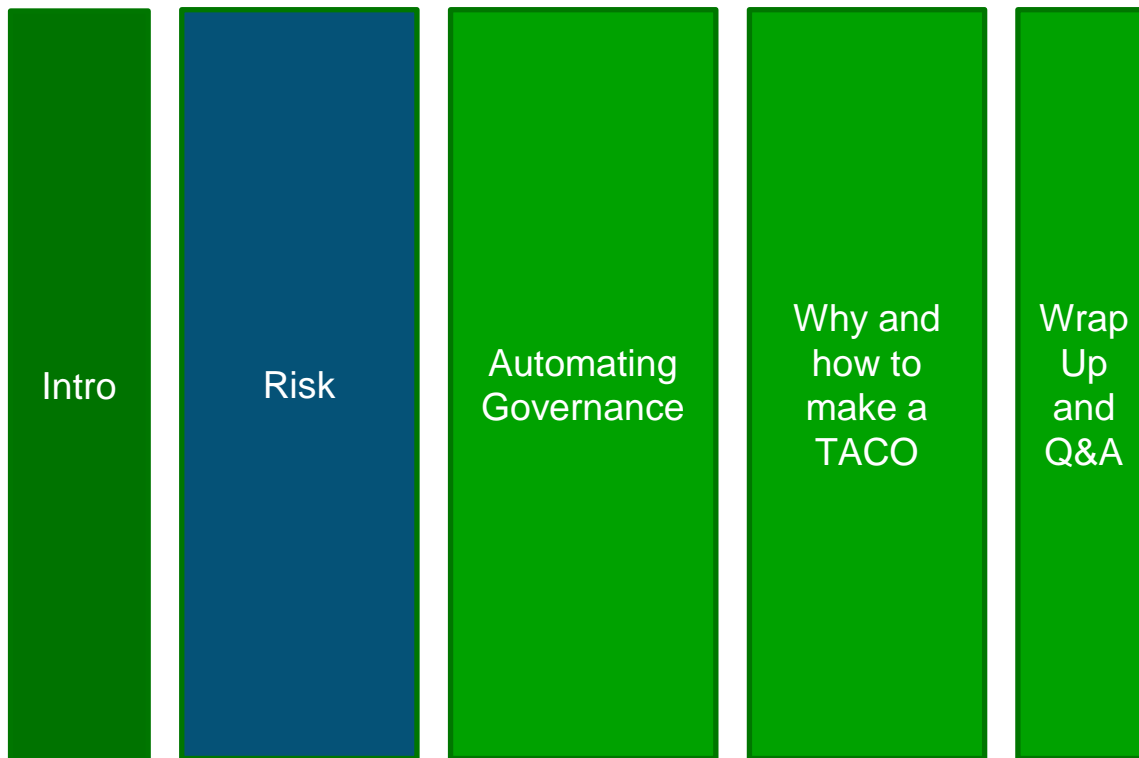- Necessary training

All while meeting any obligations to existing commitments

Change Adoption Curve
How humans react to change

HIGH

"Noise" Level

ignore   complain   plead   sulk   accept

LOW

BEGINNING

Time Period

INFINITY ▶

xodiac

Talk map

| Intro | Risk | Automating Governance | Why and how to make a TACO | Wrap Up and Q&A |

xodiac

Bunch of pictures

Hitting a wall

xodiac

GRC

Governance: Cost effectively govern the organizations risk landscape

Risk: Identifying and mitigating risks

Compliance: Documenting and reporting on how we address risk
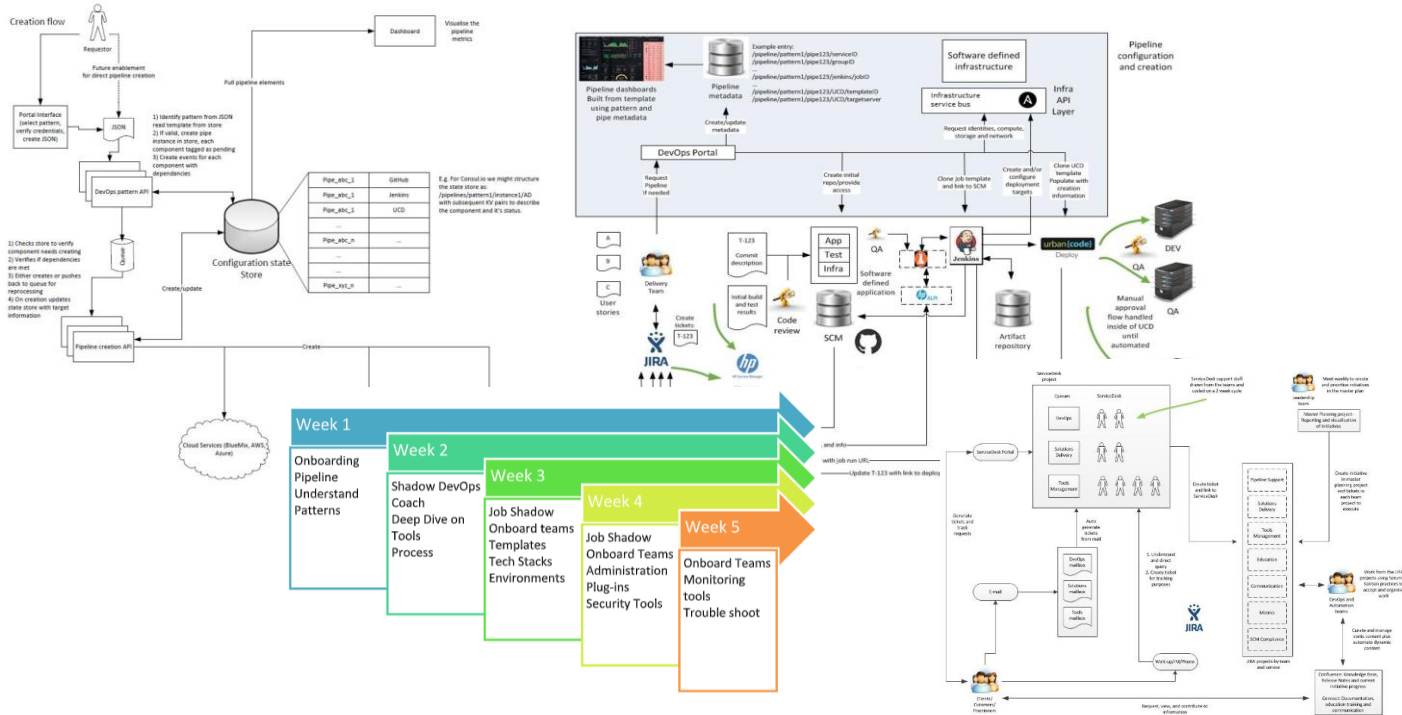
xodiac

Lost in translation

Developers
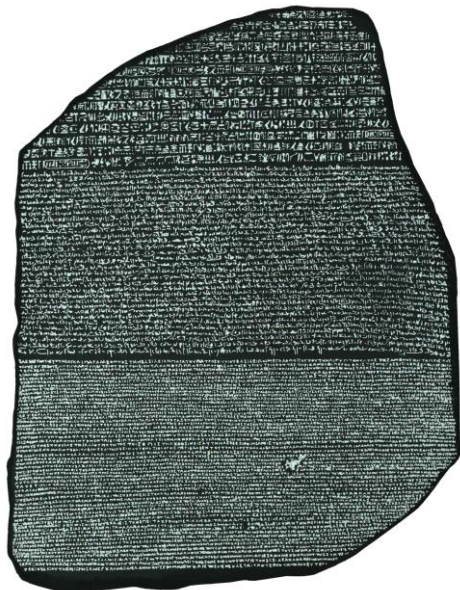
Compliance

Security

Testing

Operations

Architecture

Conversation

Talk map

Intro	Risk	Automating Governance	Why and how to make a TACO	Wrap Up and Q&A

xodiac

Is there a risk?

xodiac
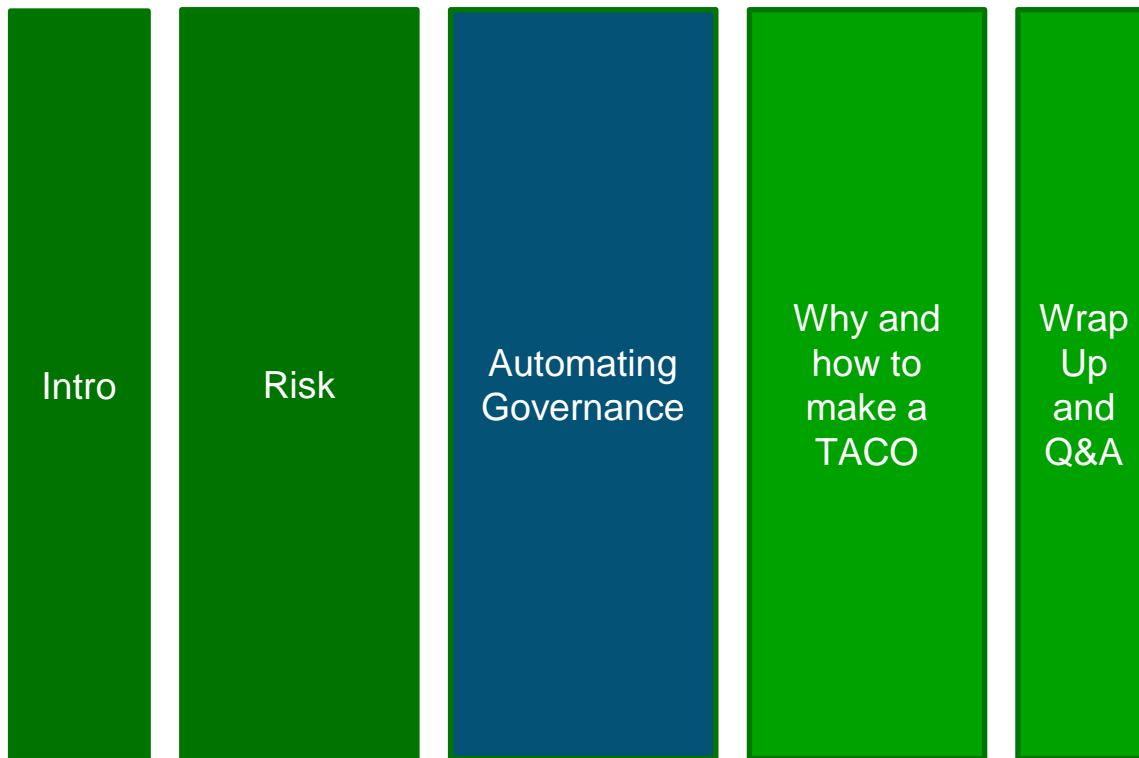
Let's start with the pipeline

Running the pipe
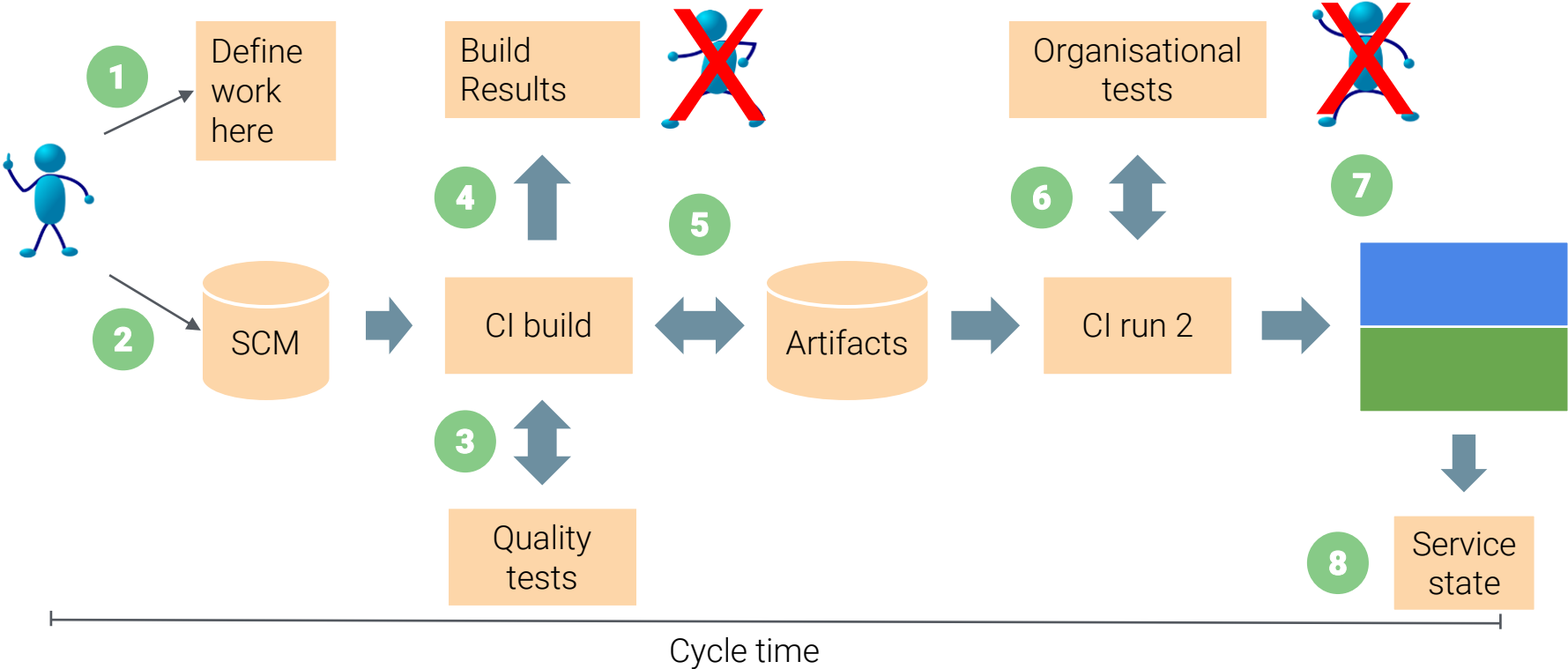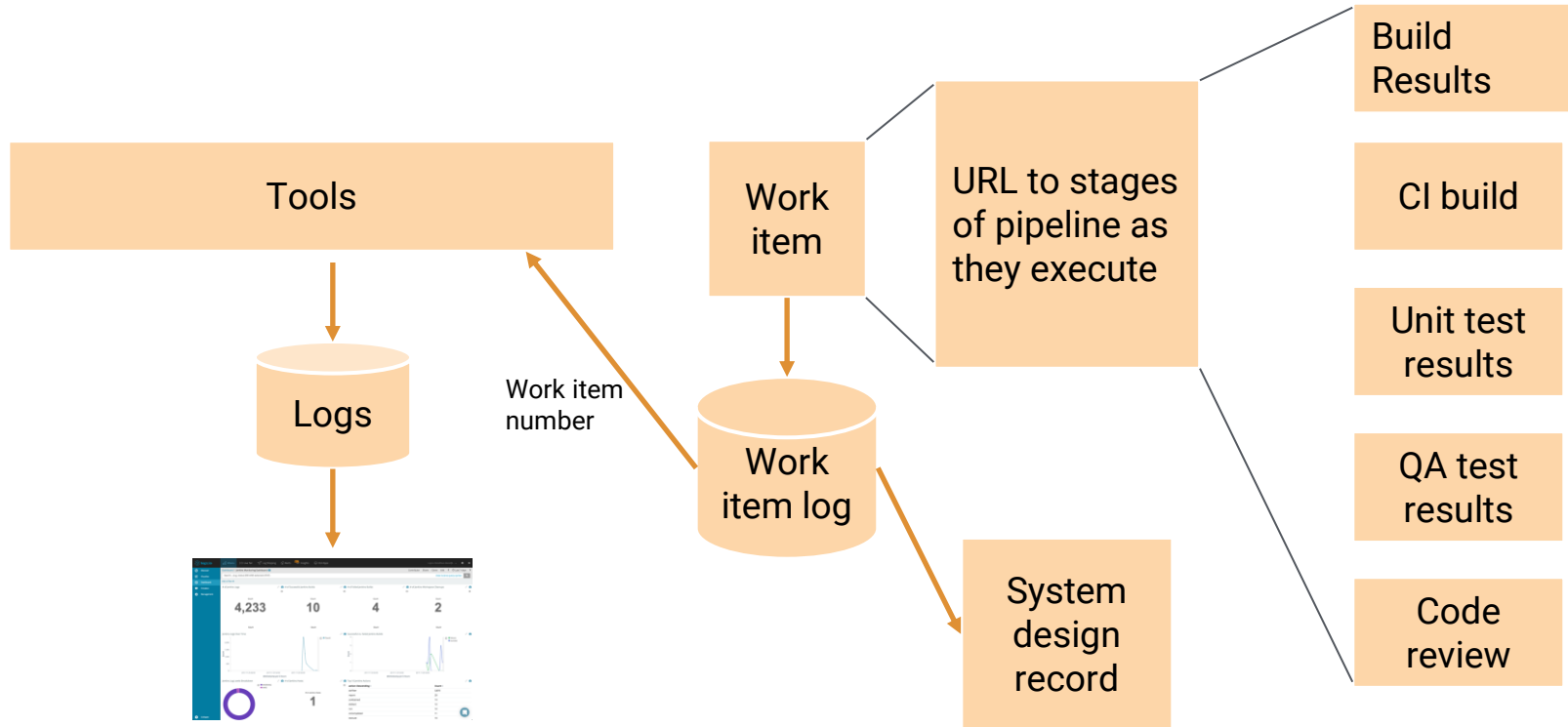
1 → Define work here

Build Results

Organisational tests

4 ↑

5

6 ↕

7

2 → SCM → **CI build** ↔ **Artifacts** → **CI run 2** →

3 ↕

Quality tests

8 Service state

Cycle time

Auditing the pipe

Tools

Logs

Work item number

Work item

Work item log

URL to stages of pipeline as they execute

System design record

Build Results

CI build

Unit test results

QA test results

Code review

Making it visible
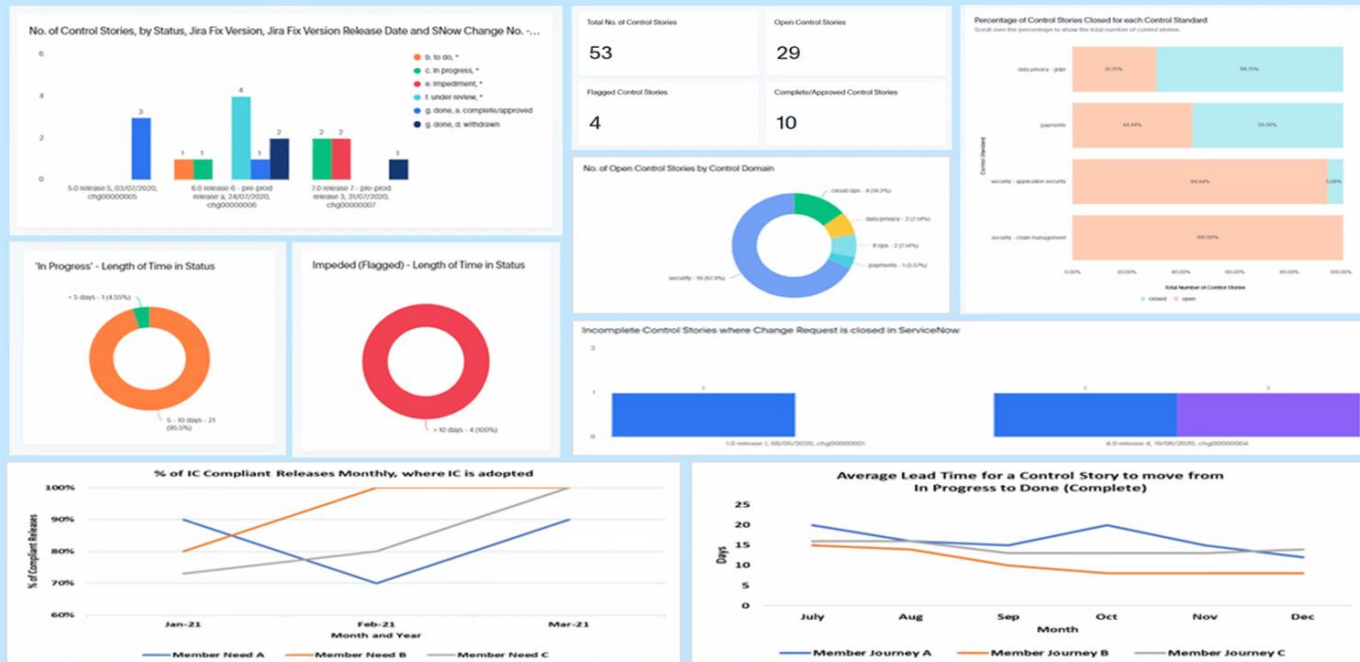
Automating Governance

- Not about keeping audit off your back

- Start small, get one team working and grow from there

- Engage leaders, focus on conversation, not tooling

xodiac

Talk map

Intro

Risk

Automating Governance

Why and how to make a TACO

Wrap Up and Q&A

xodiac

Paved road

xodiac
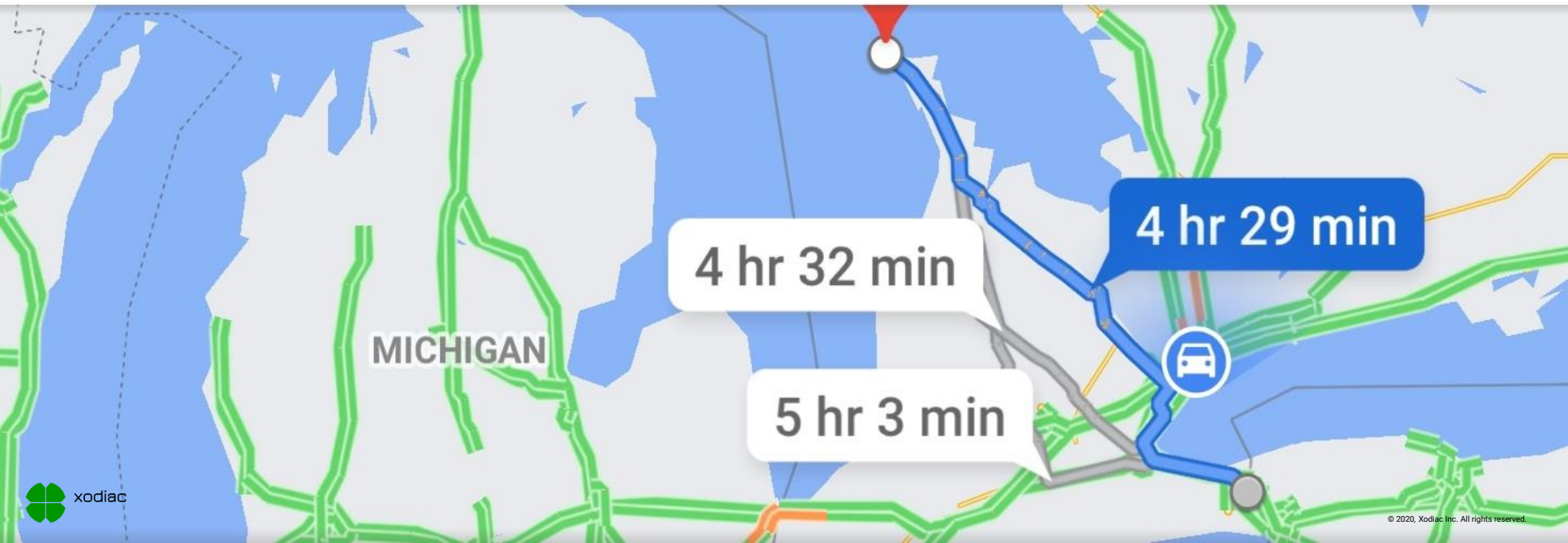
Beyond roadmaps

Modeling

Identify what happens in the pipe

Traceability

(1)
- Chain of custody
- Test results for all
- Deployed version is tracked
- Change is recorded

Ensure traceability exists

Secure the delivery process

Access

(2)
- Source code managed
- Creator tracked
- Build once, deploy many
- Pipelines only

Validate access

Validate the payload in the pipe

Compliance

(3)
- Peer review
- Scan the code
- Scan the artifact
- Manage the data

Ensure issues are addressed

Record execution and monitor

Operations

(4)
- Validate the target
- Validate quality
- Check it works
- Watch it live

Strengthen team behaviour

xodiac

TACO!

Traceability Access Compliance Operations

TACO

xodiac

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

xodiac

Visualize how much TACO

Access

30
25
20
15
10
5
0

Compliance

Operations

Traceability
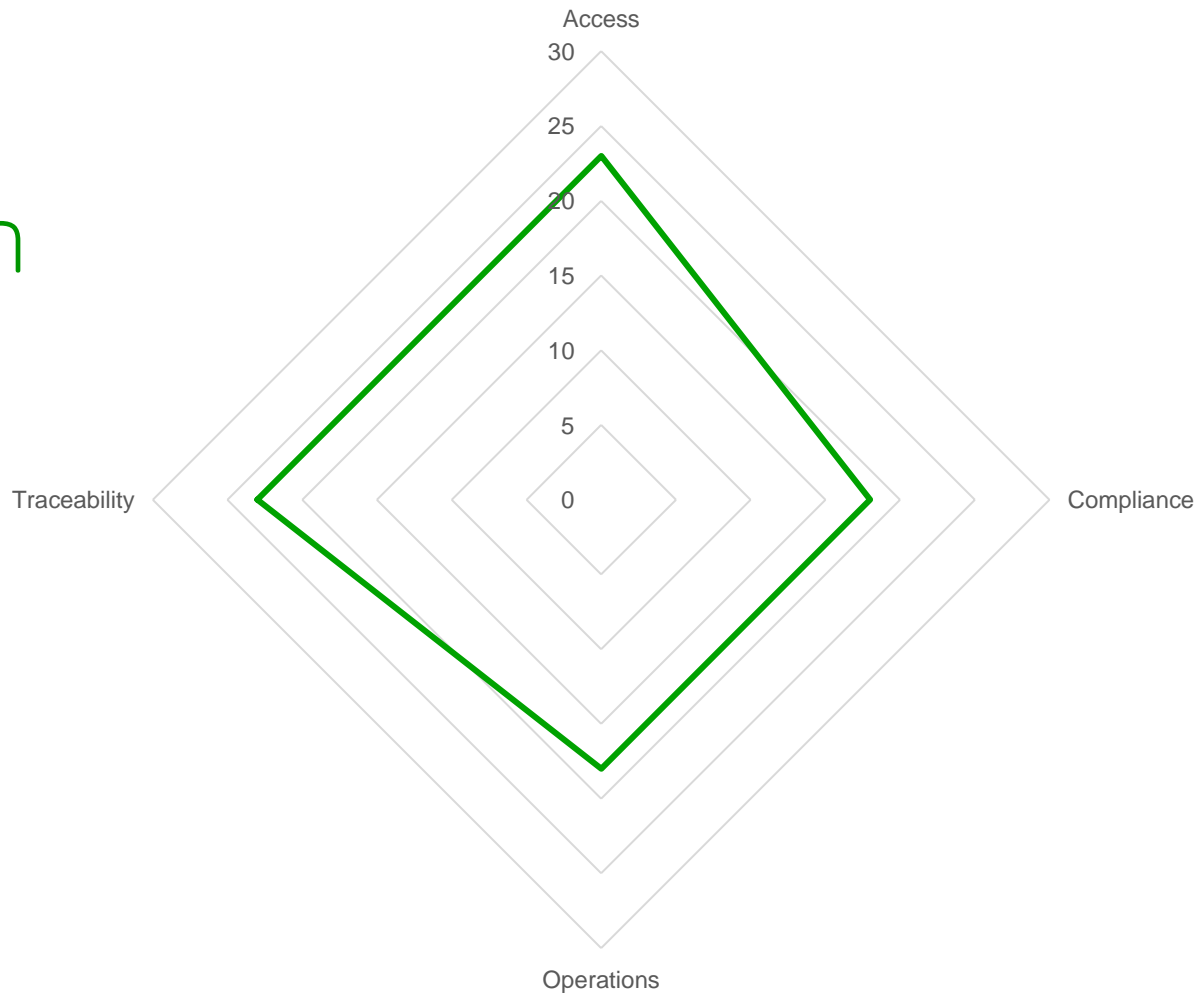
CapitalOne example

- 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

xodiac

There's more than pipelines

- Safety culture requires the ability to speak up.

- Speaking up requires we feel "safe"

- Psychological safety is critical

Accountability for Meeting Demanding Goals

	LOW	HIGH
HIGH (Psychological Safety)	**Comfort zone** Employees really enjoy working with one another but don't feel particularly challenged. Nor do they work very hard. Some family businesses and small consultancies fall into this quadrant.	**Learning zone** Here the focus is on collaboration and learning in the service of high-performance outcomes. The hospitals described in this article fall into this quadrant.
LOW (Psychological Safety)	**Apathy zone** Employees tend to be apathetic and spend their time jockeying for position. Typical organizations in this quadrant are large, top-heavy bureaucracies, where people fulfill their functions but the preferred modus operandi is to curry favor rather than to share ideas.	**Anxiety zone** Such firms are breeding grounds for anxiety. People fear to offer tentative ideas, try new things, or ask colleagues for help, even though they know great work requires all three. Some investment banks and high-powered consultancies fall into this quadrant.

Taken from: Amy Edmondson, The Fearless Organisation, p. 20

xodiac

A real world example

Intelligent Control – Delivering Safer Value

Building the Right Thing and Building It Right

Intelligent Control Enables…

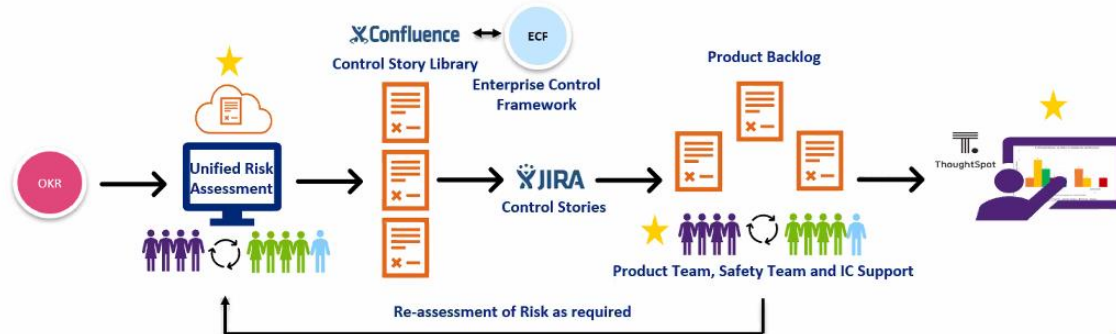| Consistent risk assessments | Minimum Viable Control | Minimum Viable Governance | Control automation | Continuous assurance | Full traceability | Increased flow |

Confluence ←→ **ECF**

Control Story Library

Enterprise Control Framework

Product Backlog

OKR → **Unified Risk Assessment** → **JIRA Control Stories** → ThoughtSpot

Product Team, Safety Team and IC Support

Re-assessment of Risk as required

DevOps

DevSecOps

RiskDevRiskOpsRisk

Talk map
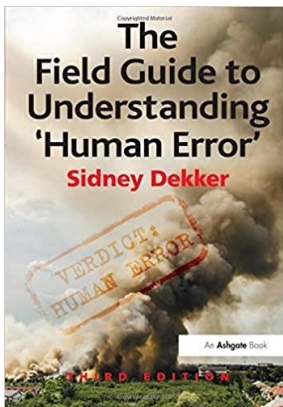
Intro

Risk

Automating Governance

Why and how to make a TACO
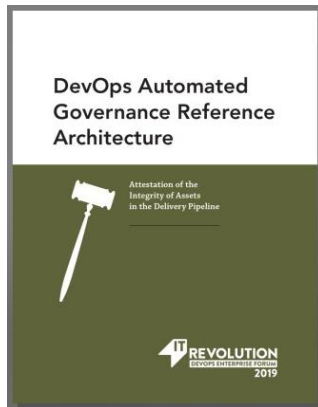
Wrap Up and Q&A

xodiac

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

- Albert Einstein

xodiac

References

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=_j9eB0flTtY

Risk & Control is Dead, Long Live Risk & Control — Jon Smart
https://www.youtube.com/watch?v=XRMf9QjUwlI

xodiac

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

Developers

Compliance

Security

Testing

Operations

Architecture

xodiac

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
@pgmaddison
https://www.linkedin.com/in/peter-maddison/