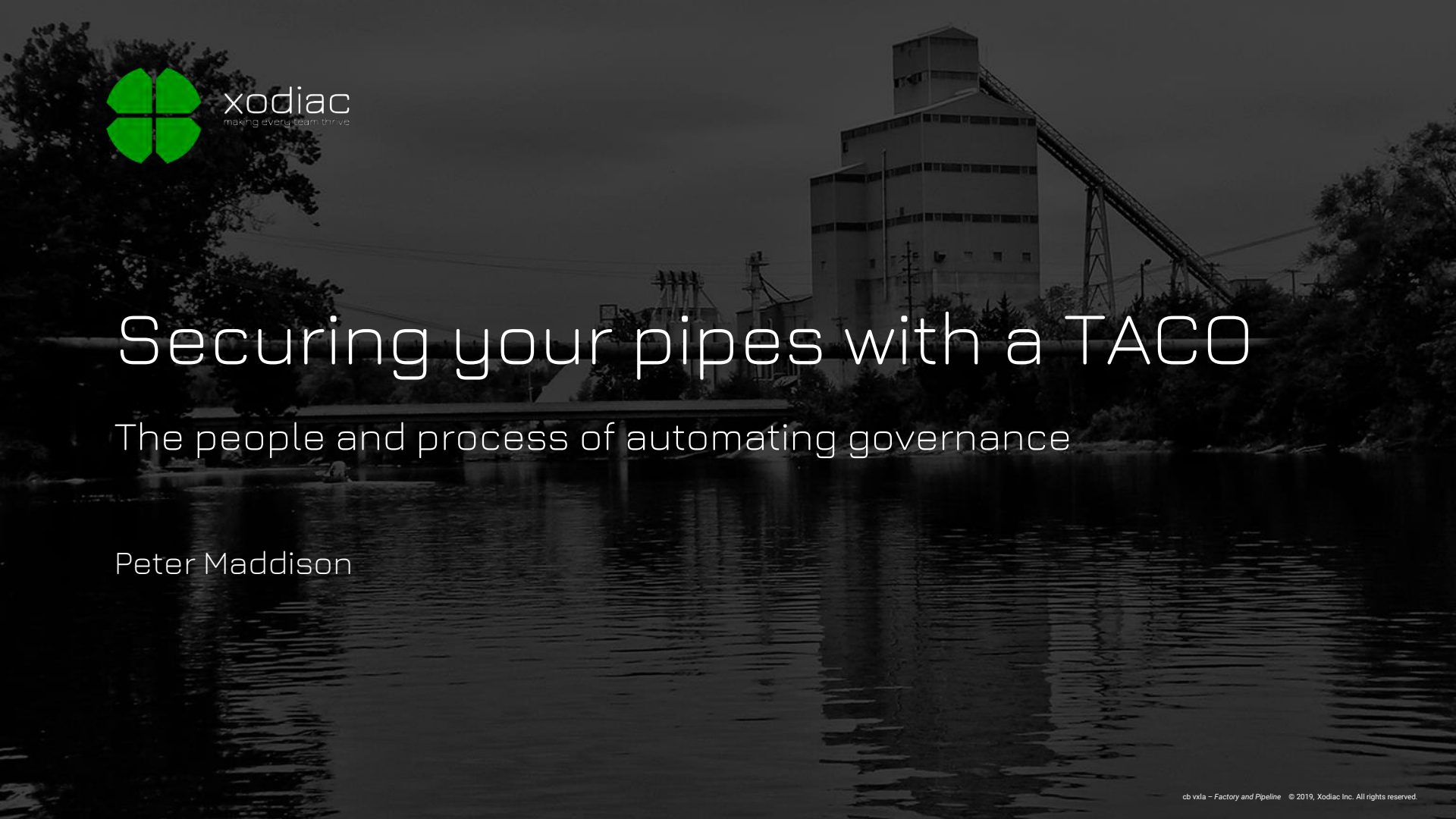
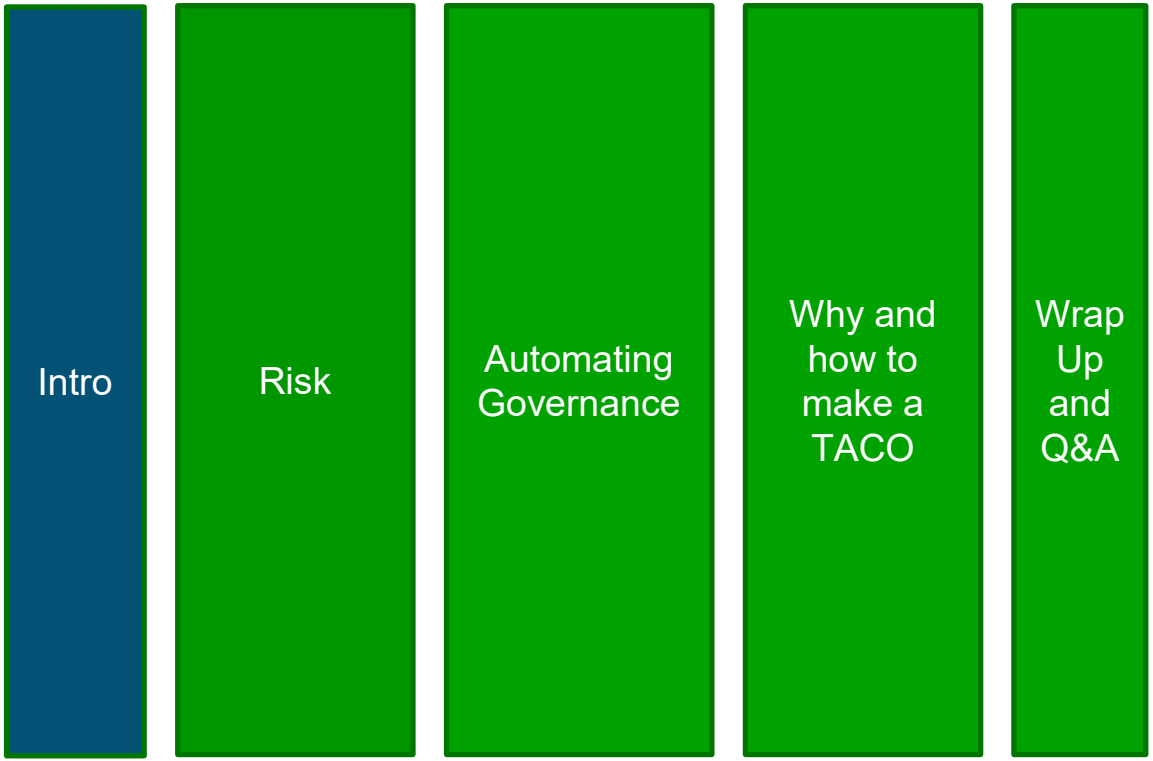


Securing your pipes with a TACO

The people and process of automating governance

Peter Maddison

Talk map



xodiac

Who am I?

Peter Maddison

Coach, consultant, founder…

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

xodiac

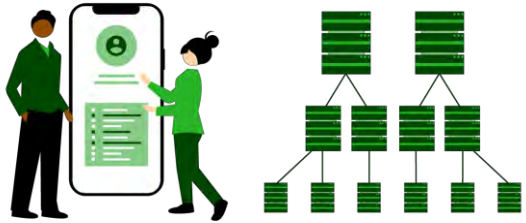
In our fast-paced world customers demand instant gratification

xodiac

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

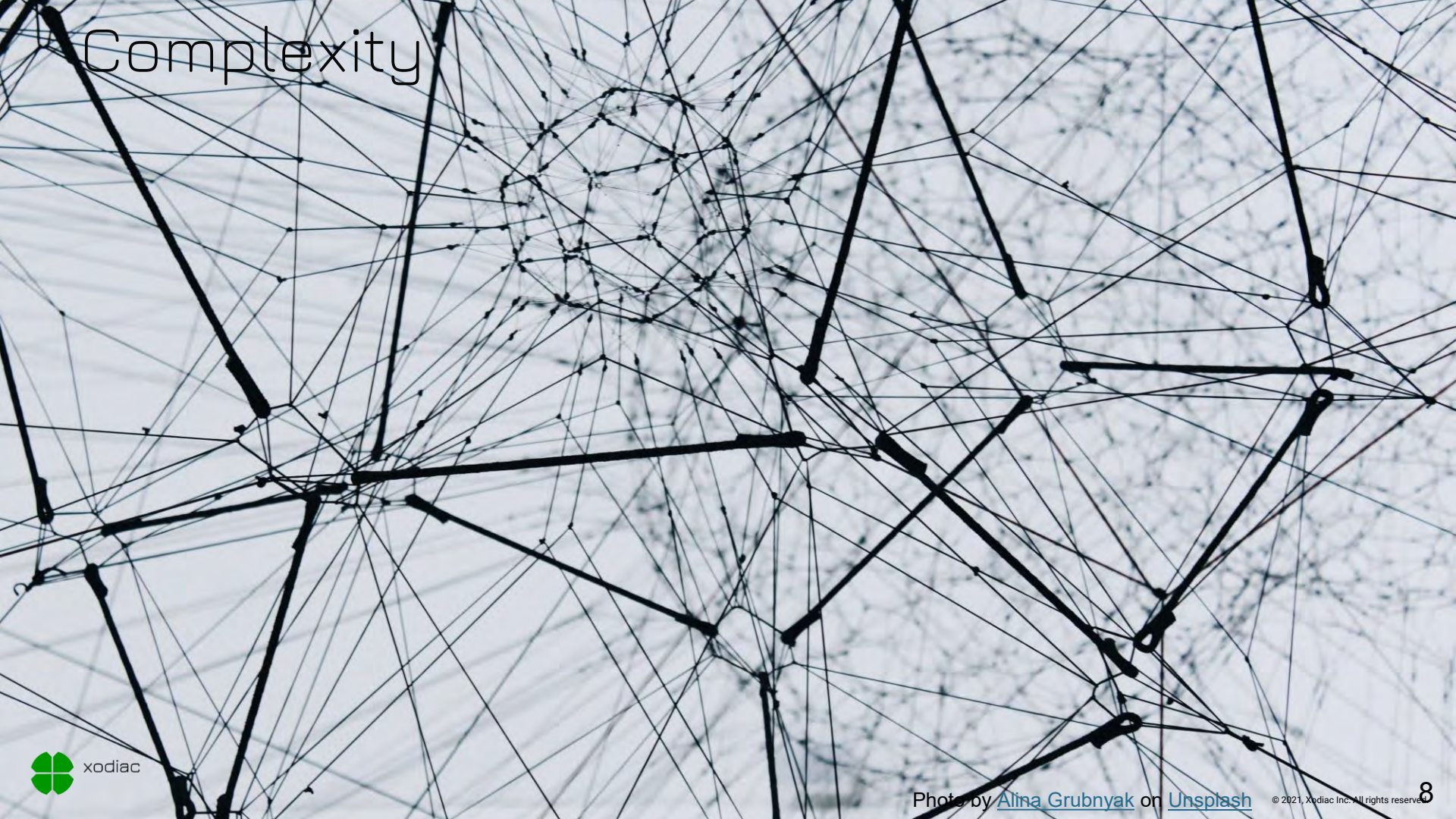
Efforts Fail From Lack of Clarity, Not Tools

- 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 Tools
- Automation Without Value
- Ineffective Metrics
- 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

Complexity



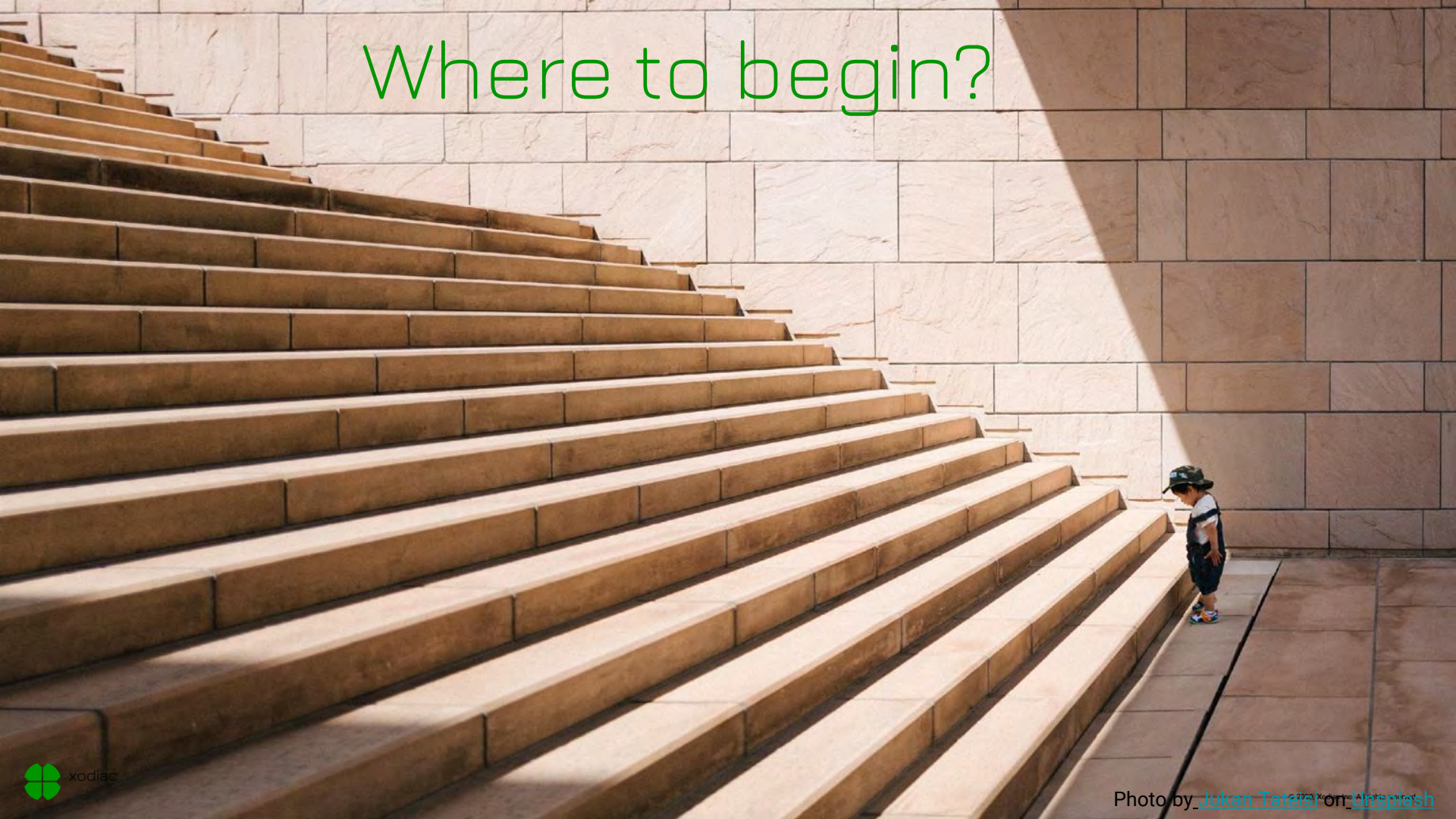
xodiac

Photo by Alina Grubnyak on Unsplash

Talk map

xodiac

Where to begin?



xodiac

Photo by Jukan Tateisi on Unsplash

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

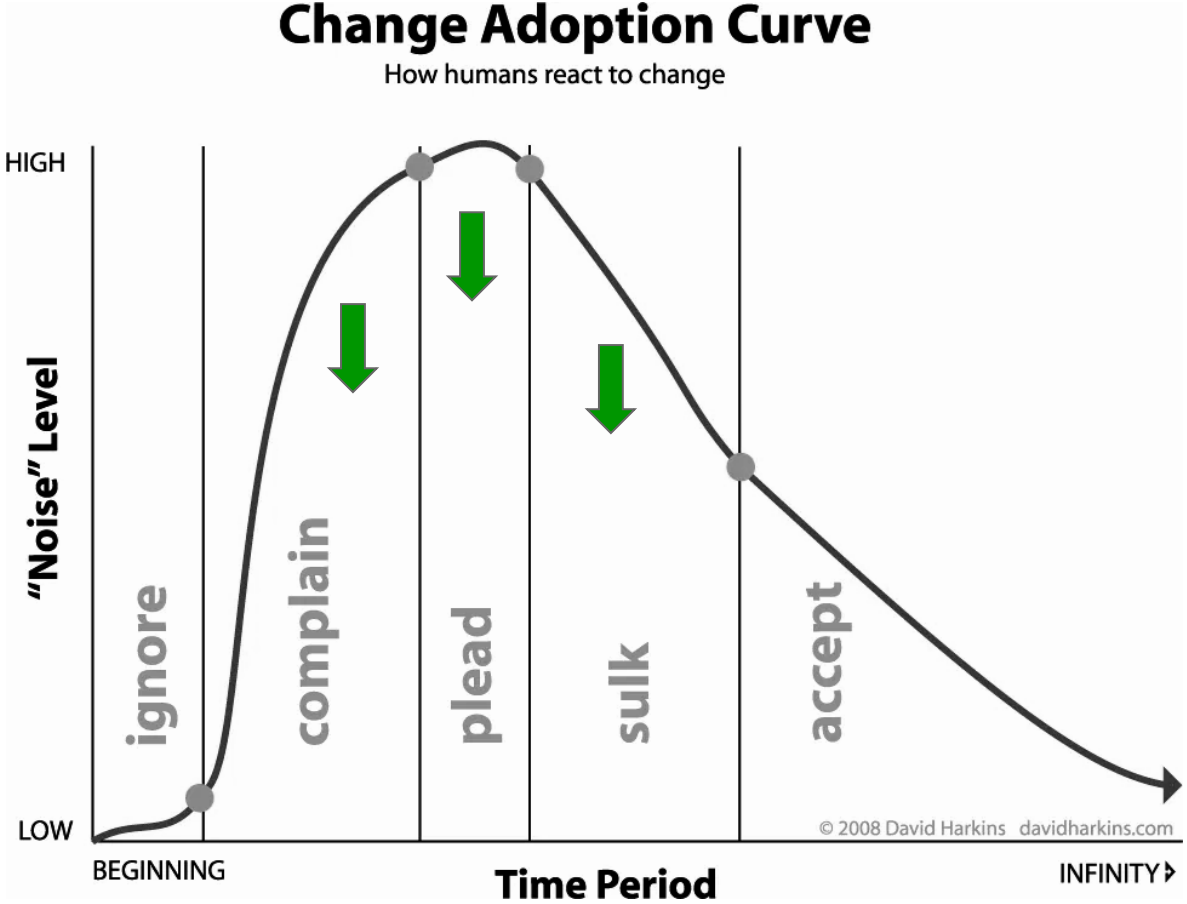
xodiac

xodiac

Introducing:

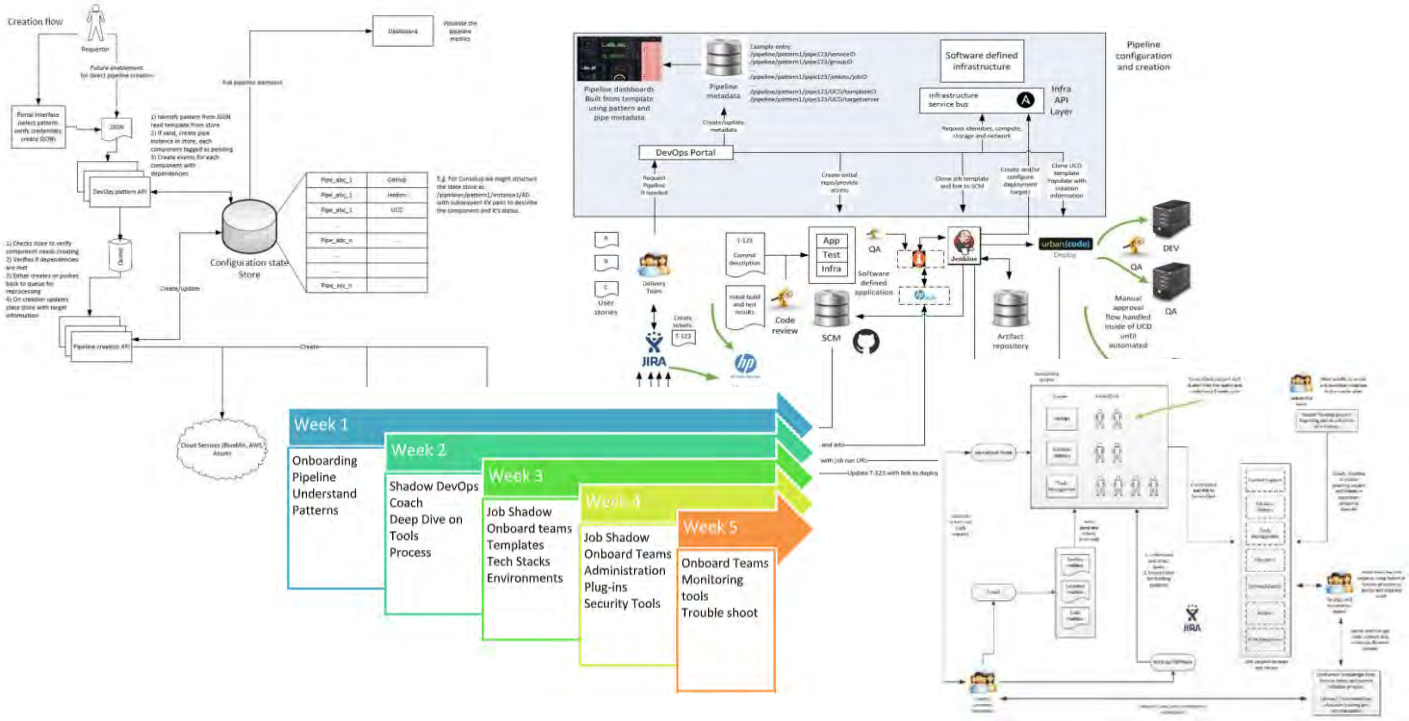
- New paradigms
- New ways of working
- Necessary training

All while meeting any obligations to existing commitments



xodiac

Bunch of pictures



xodiac

Hitting a wall

xodiac

Photo by Michael Longmire on Unsplash

Lost in translation

Developers

Security

Operations

Compliance

Testing

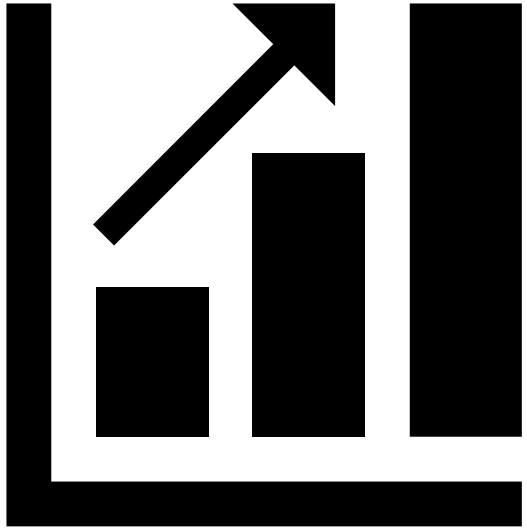
Architecture

xodiac

xodiac

How will we measure?

- Incremental improvements
- Quantify risk
- Anomolies



Talk map

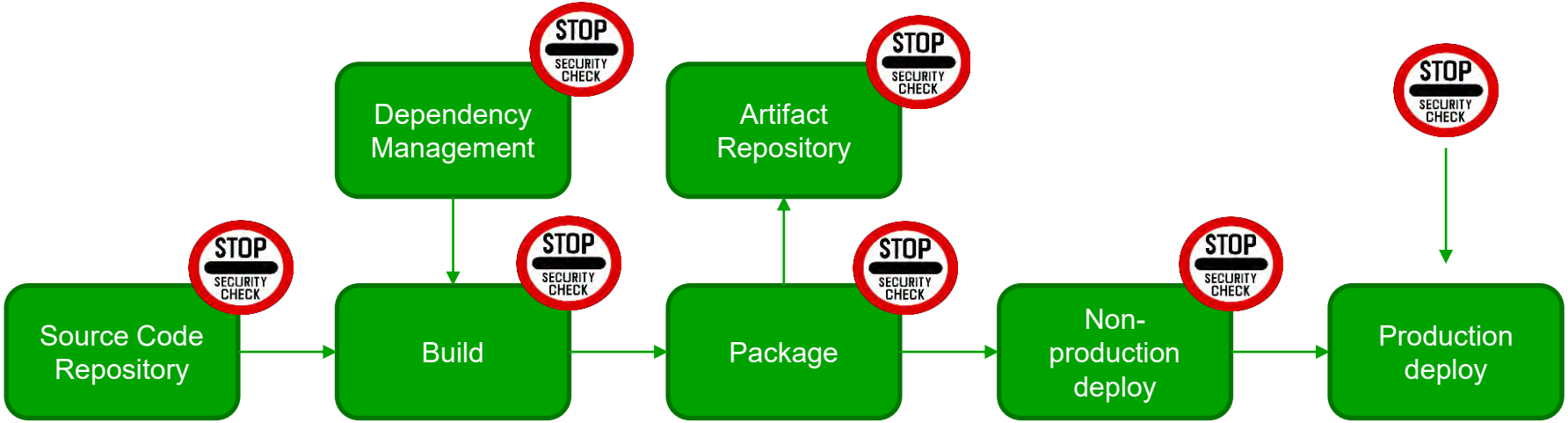
xodiac

Is there a risk?

xodiac

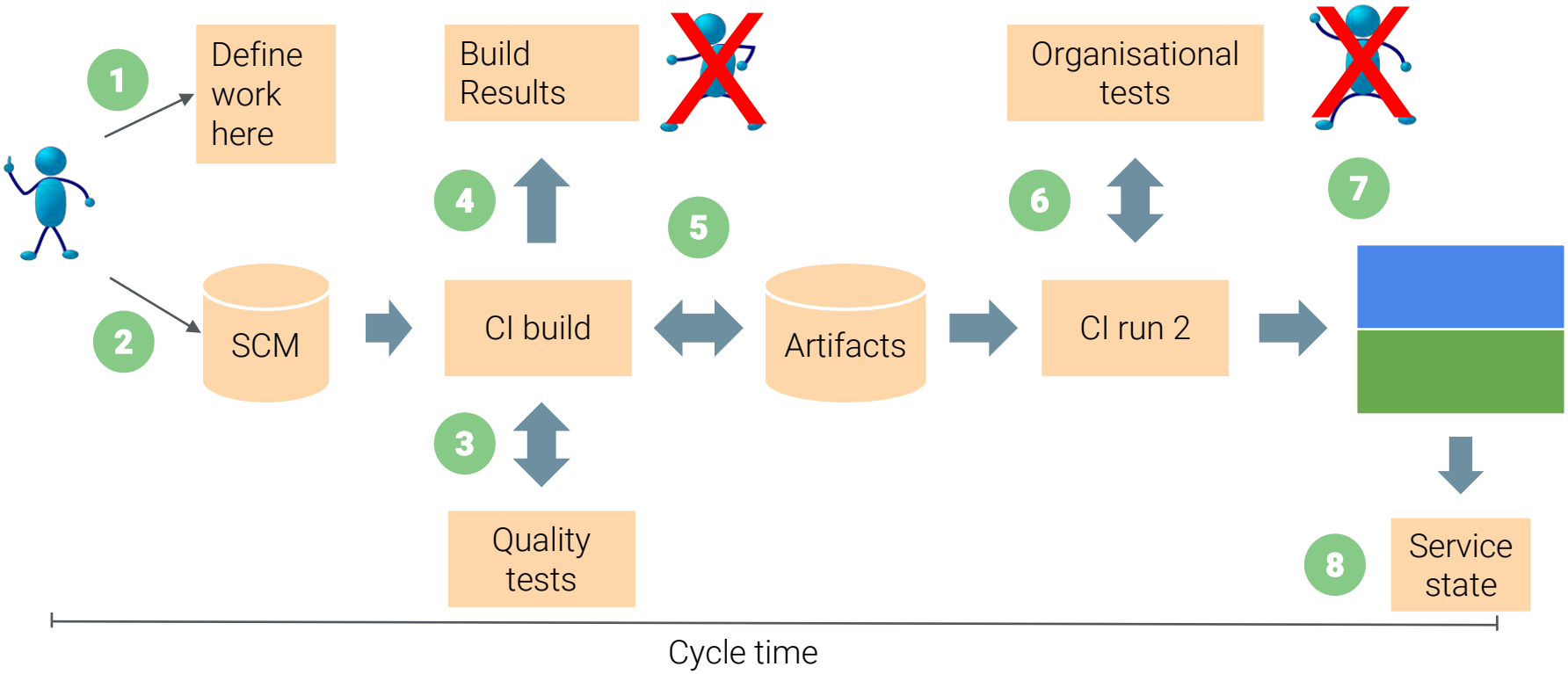
Photo by NordWood Themes on Unsplash

Let’s start with the pipeline



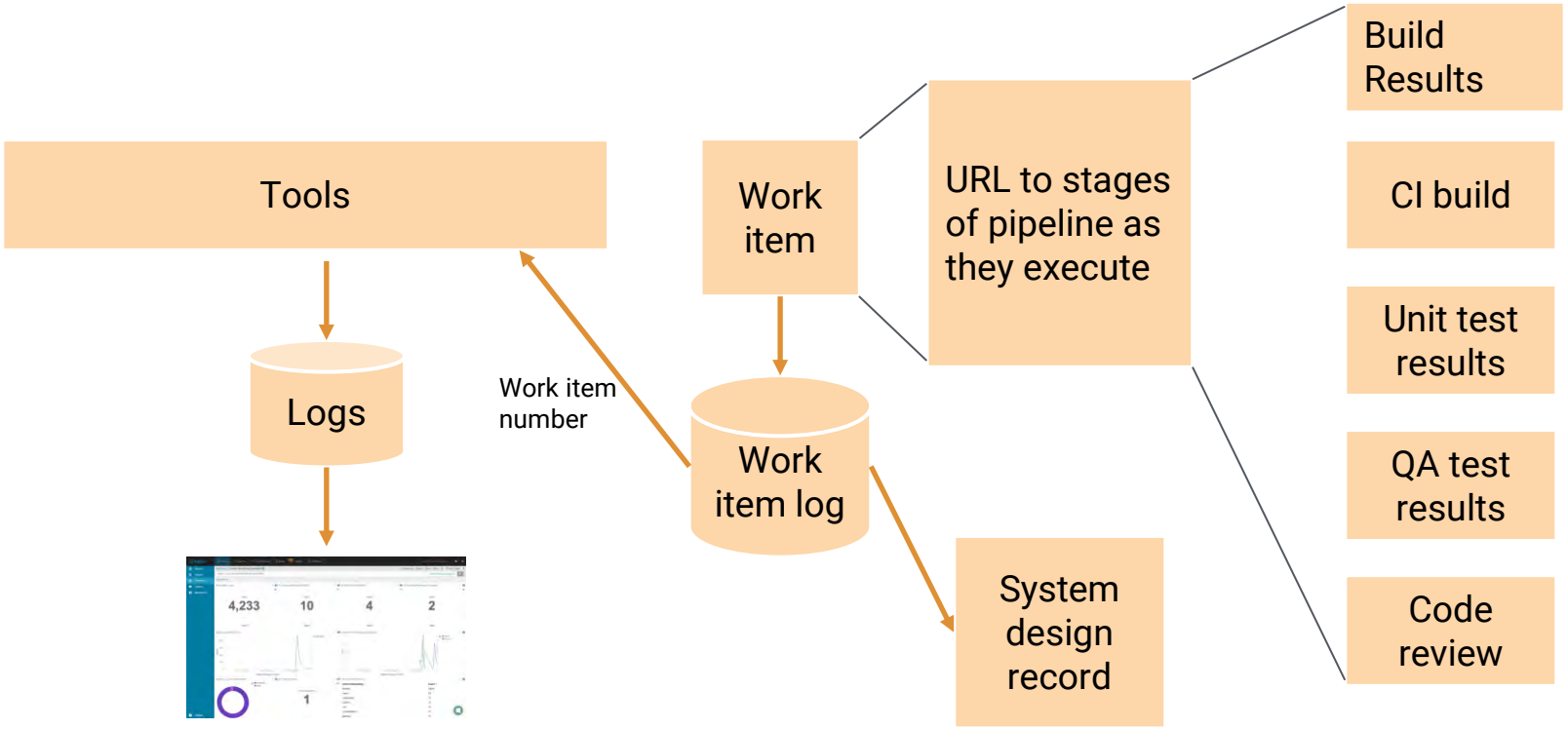
xodiac

Running the pipe



xodiac

Auditing the pipe



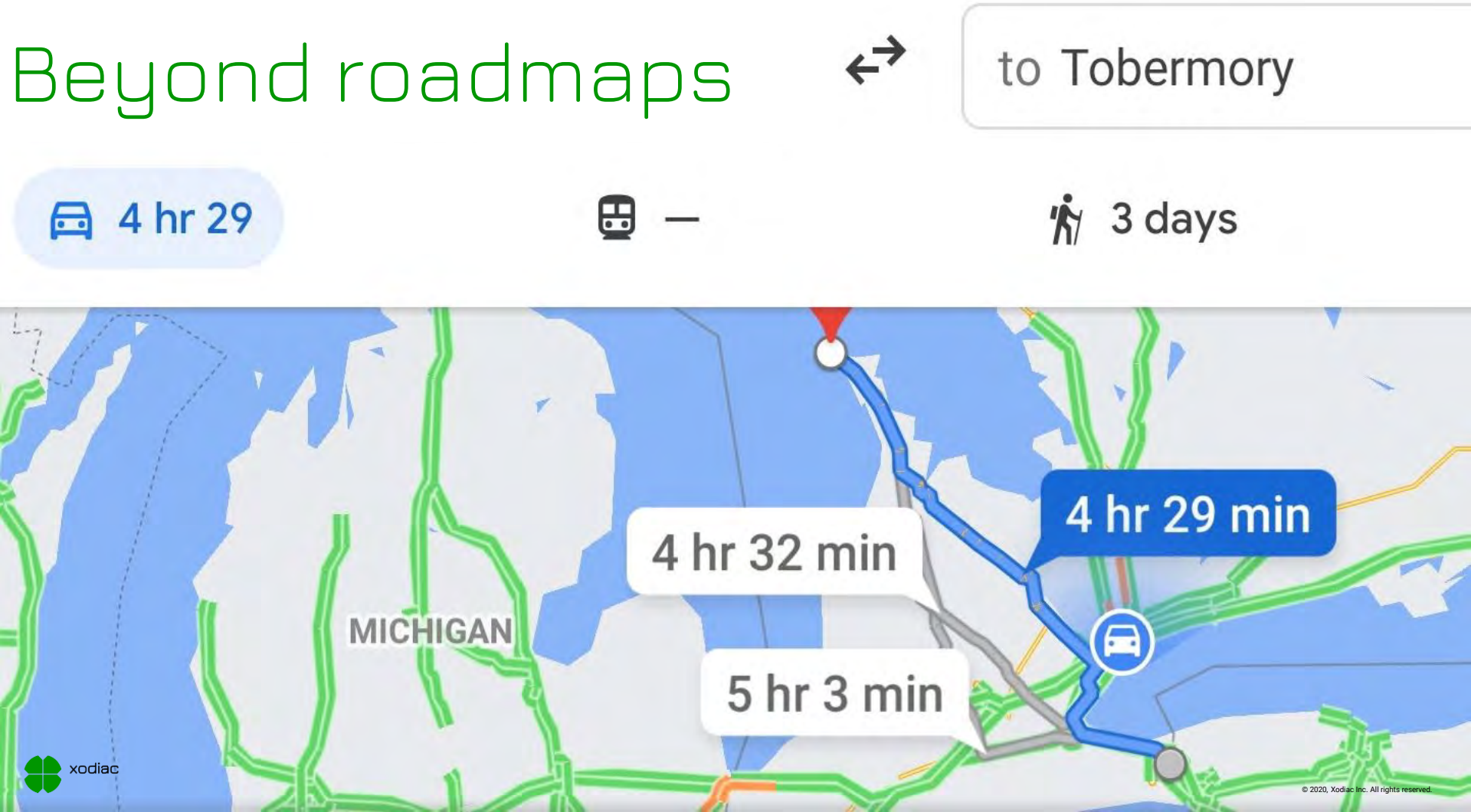
xodiac

Paved road

xodiac

Photo by Jon Flobrant on Unsplash

Beyond roadmaps



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

xodiac

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!

xodiac

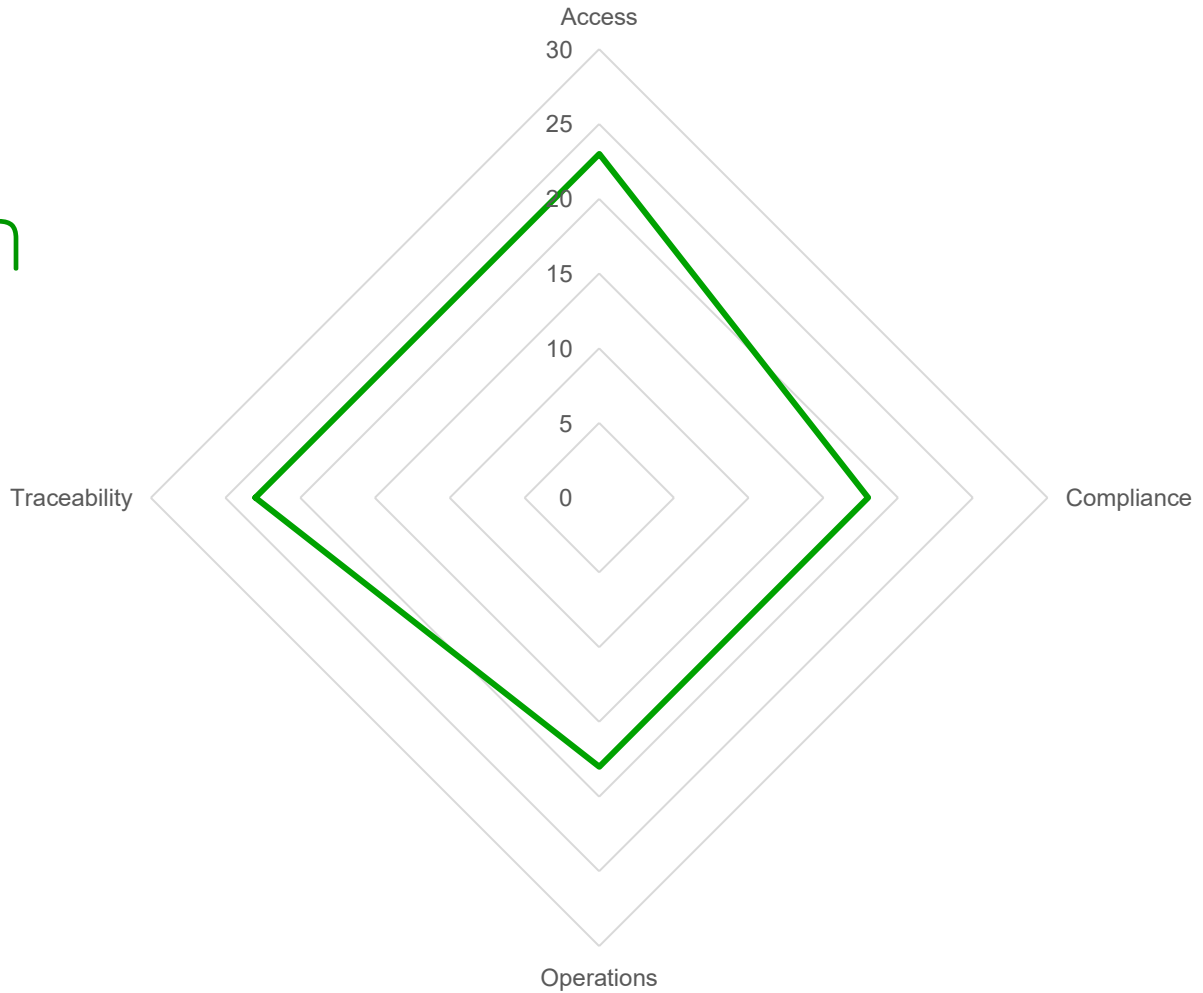
Example

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

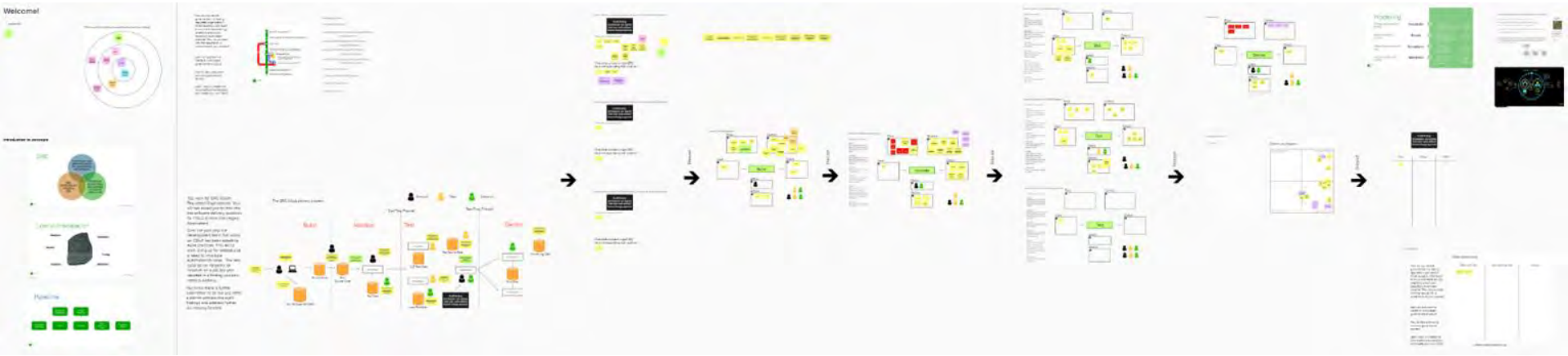
xodiac

Visualize how much TACO



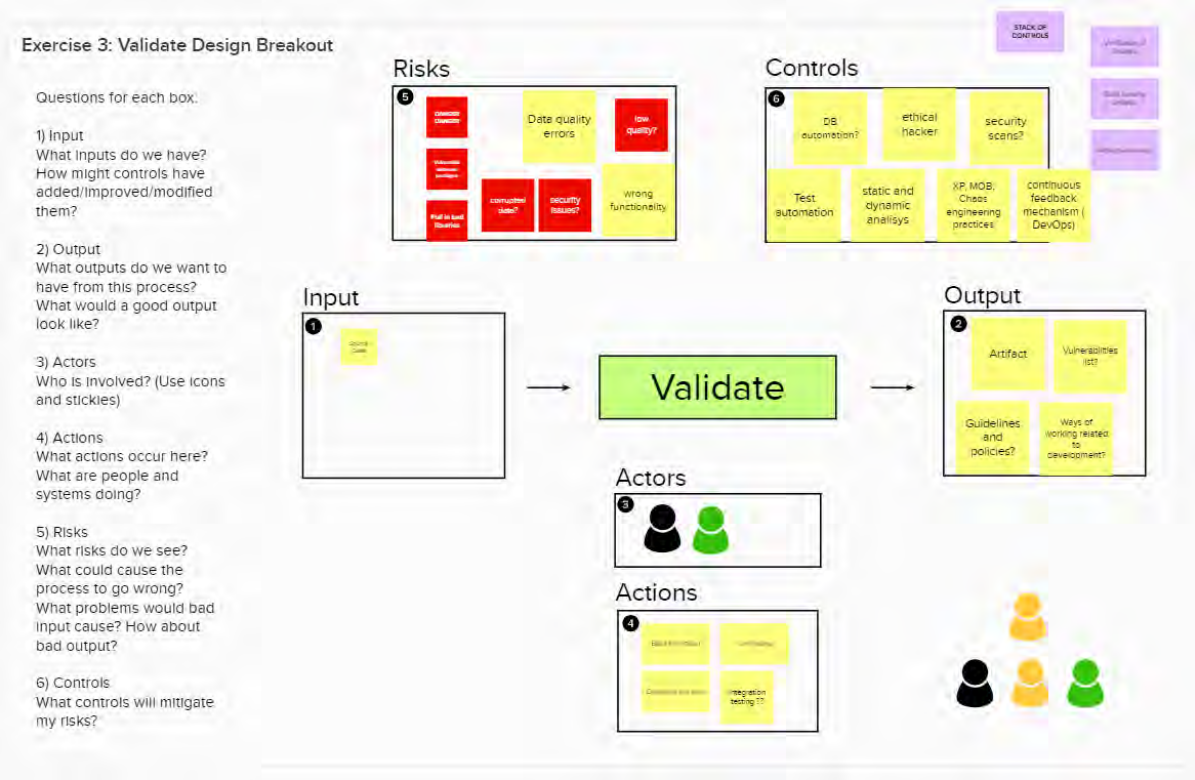
xodiac

Initial controls design



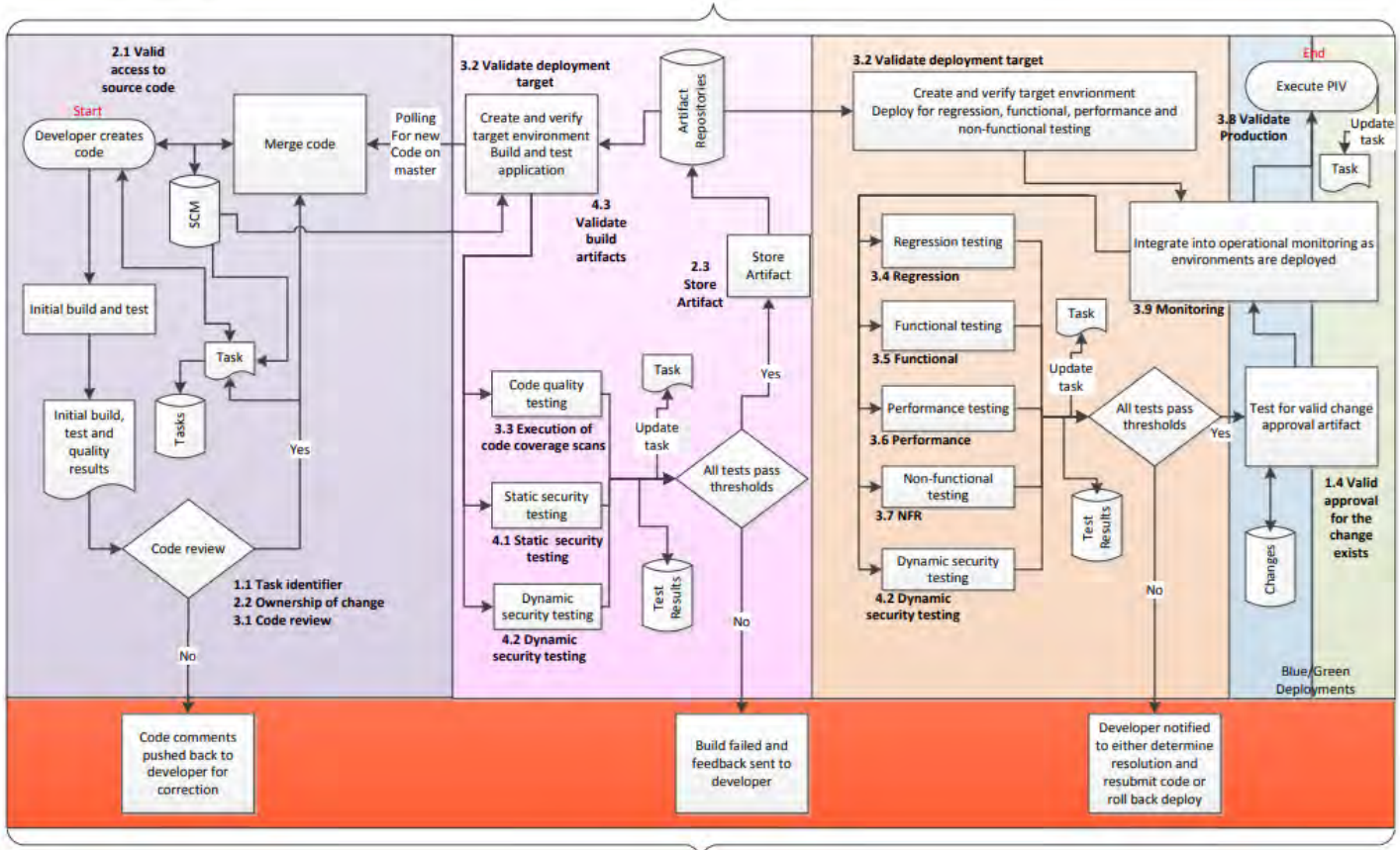
xodiac

Mapping the controls



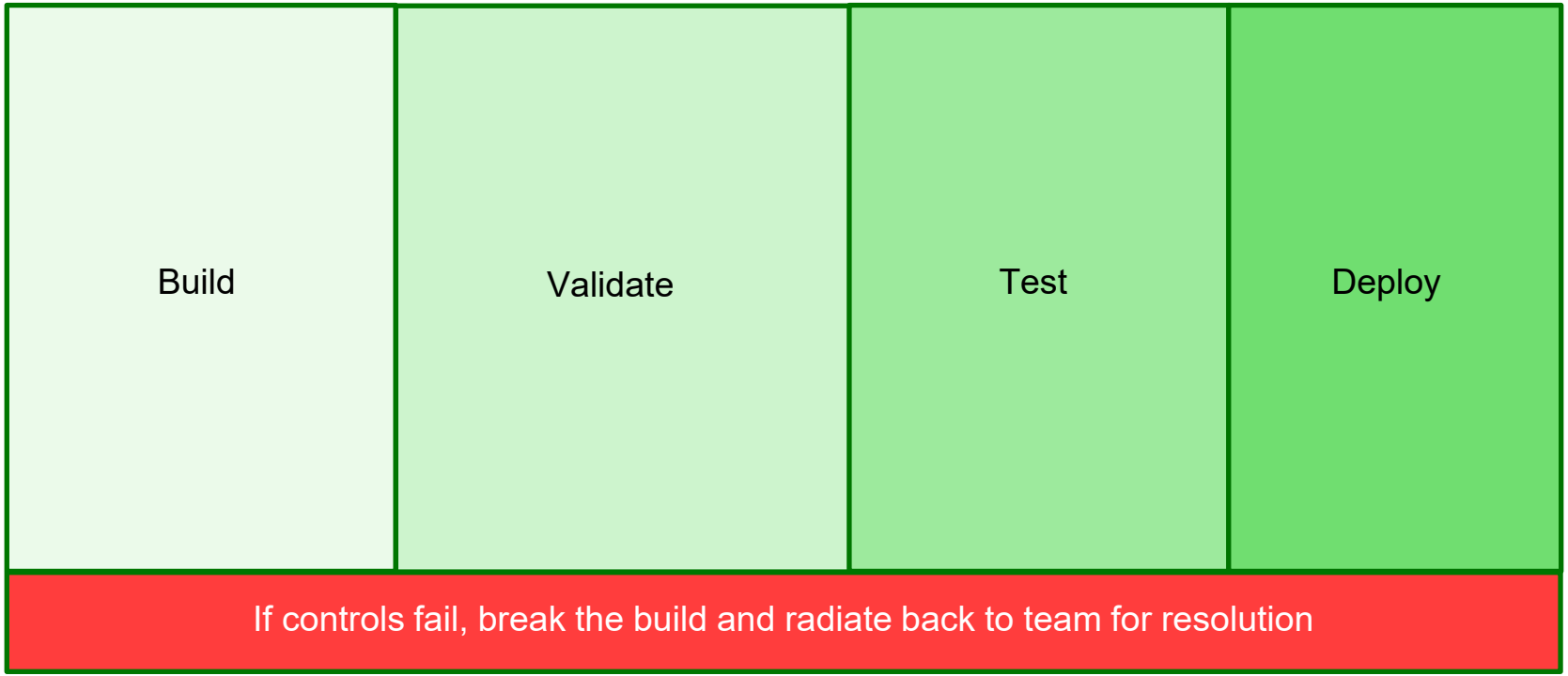
xodiac

Pipeline general case – Controls example



xodiac

Mapping the controls

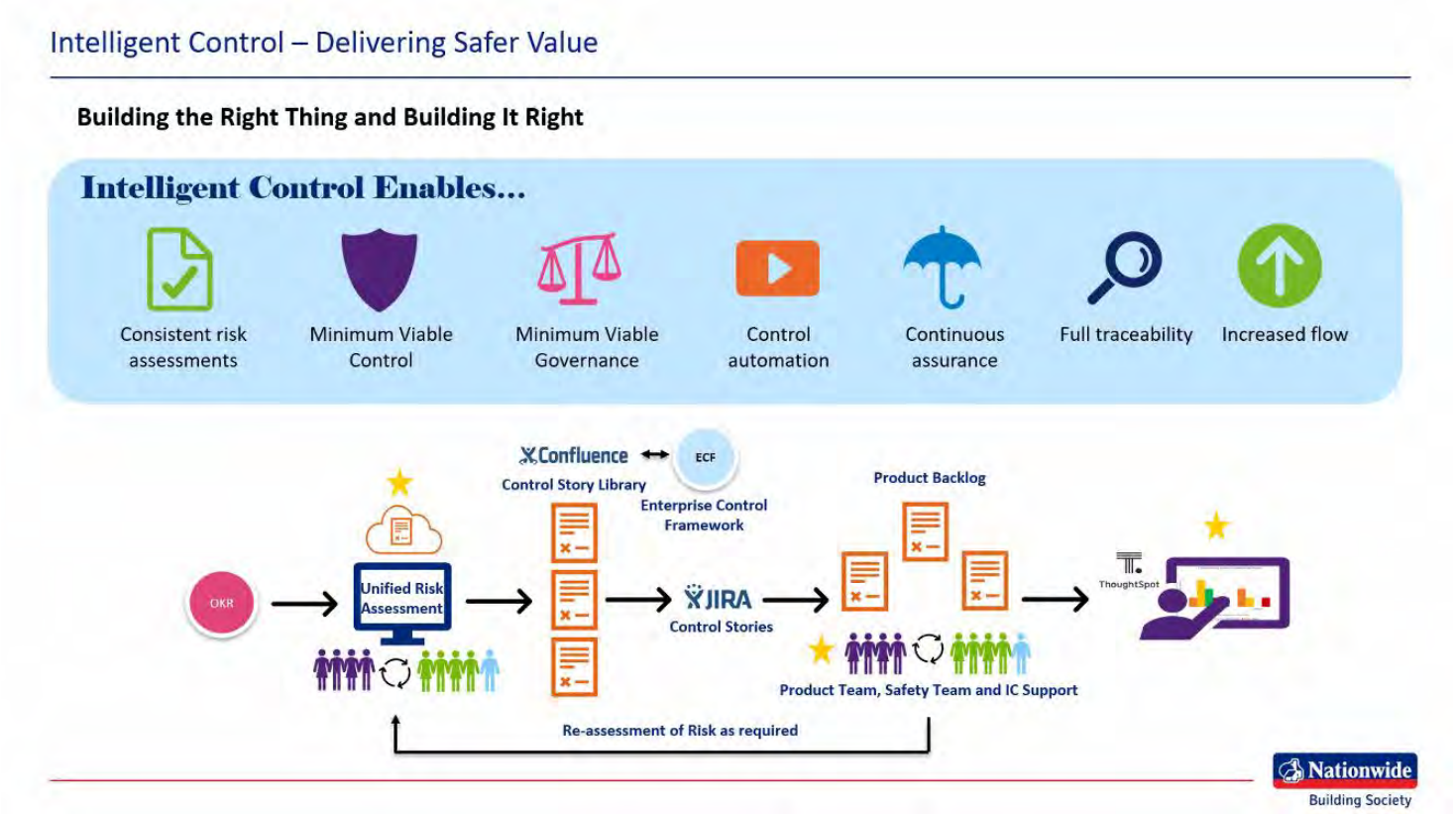


xodiac

CapitalOne example

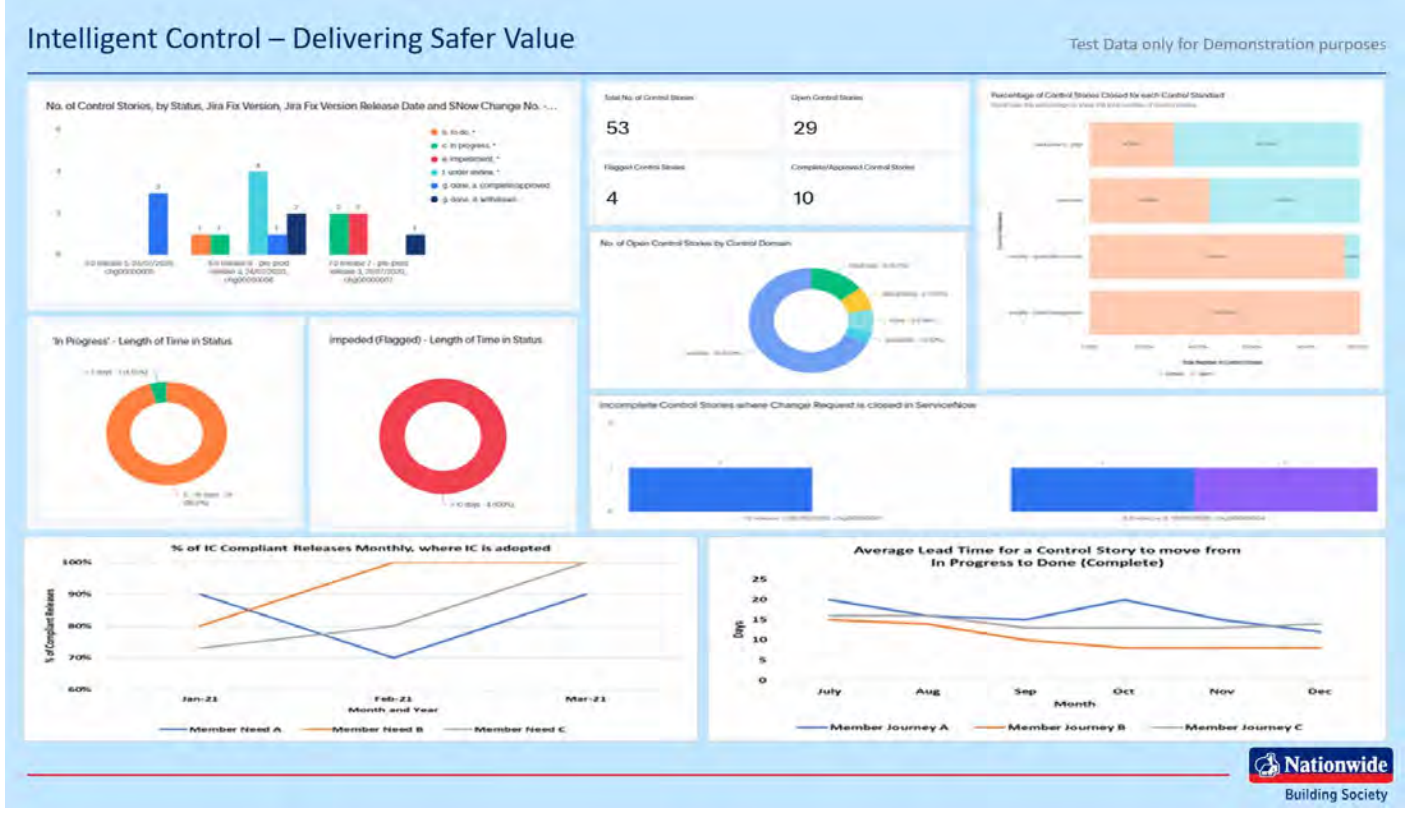
- Source code version control
- Optimum branching strategy
- Static analysis
- >80% code coverage
- Vulnerability scan
- Open source scan
- Artifact version control
- Auto provisioning
- Immutable servers
- Integration testing
- Performance testing
- Build deploy testing automated for every commit
-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

Another real world example



xodiac

Altogether now, measure



xodiac

DevOps

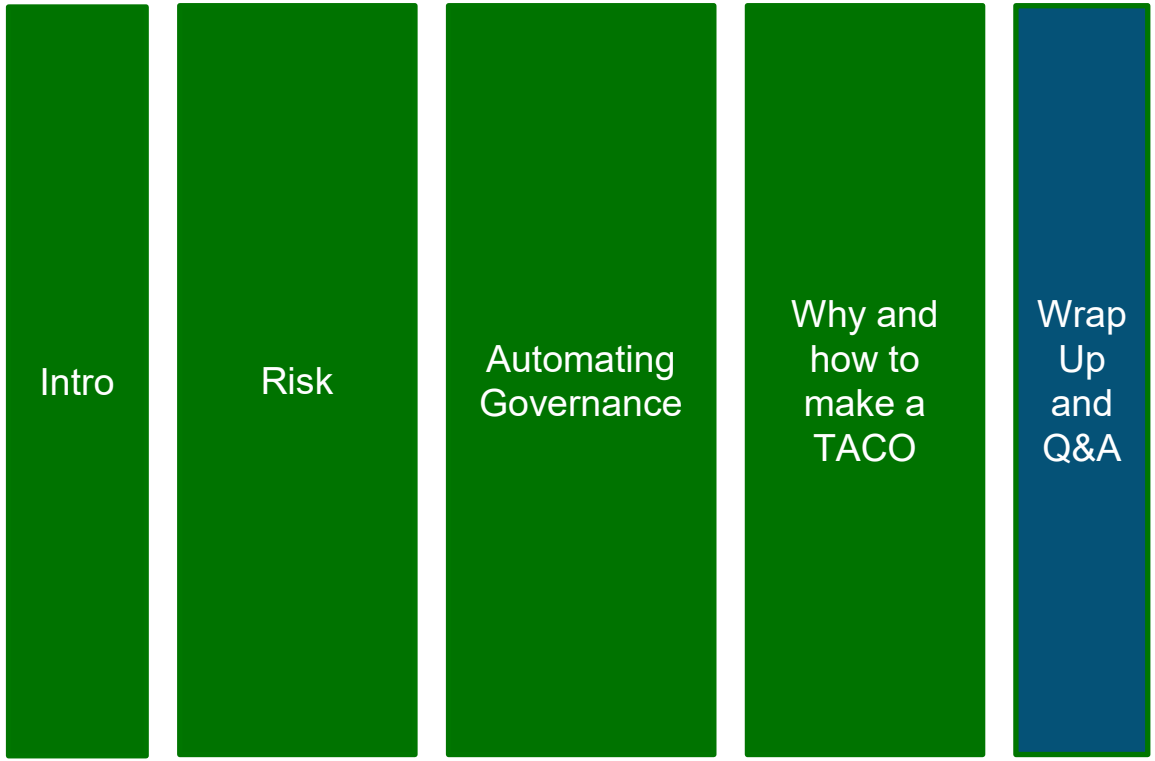
xodiac

DevSecOps

xodiac

RiskDevRiskOpsRisk

Talk map



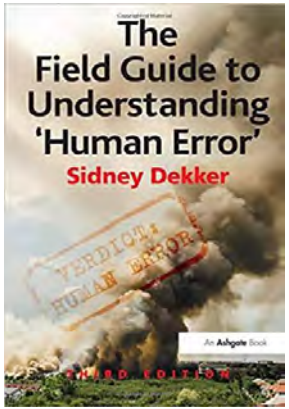
xodiac

> “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/

DevOps INSTITUTE
ADVANCING THE HUMANS OF DEVOPS

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

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

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/

