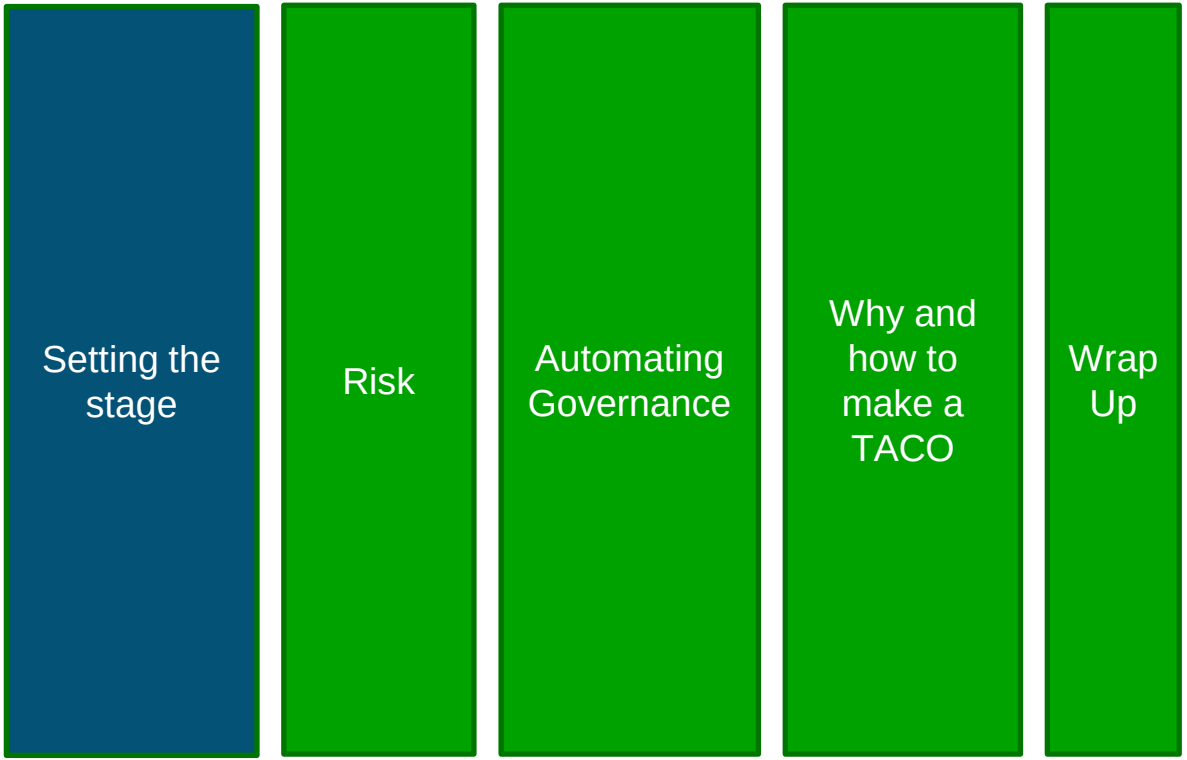
Automating Governance

Securing your pipes with a TACO

Peter Maddison

Talk map



xodiac

Who am I?

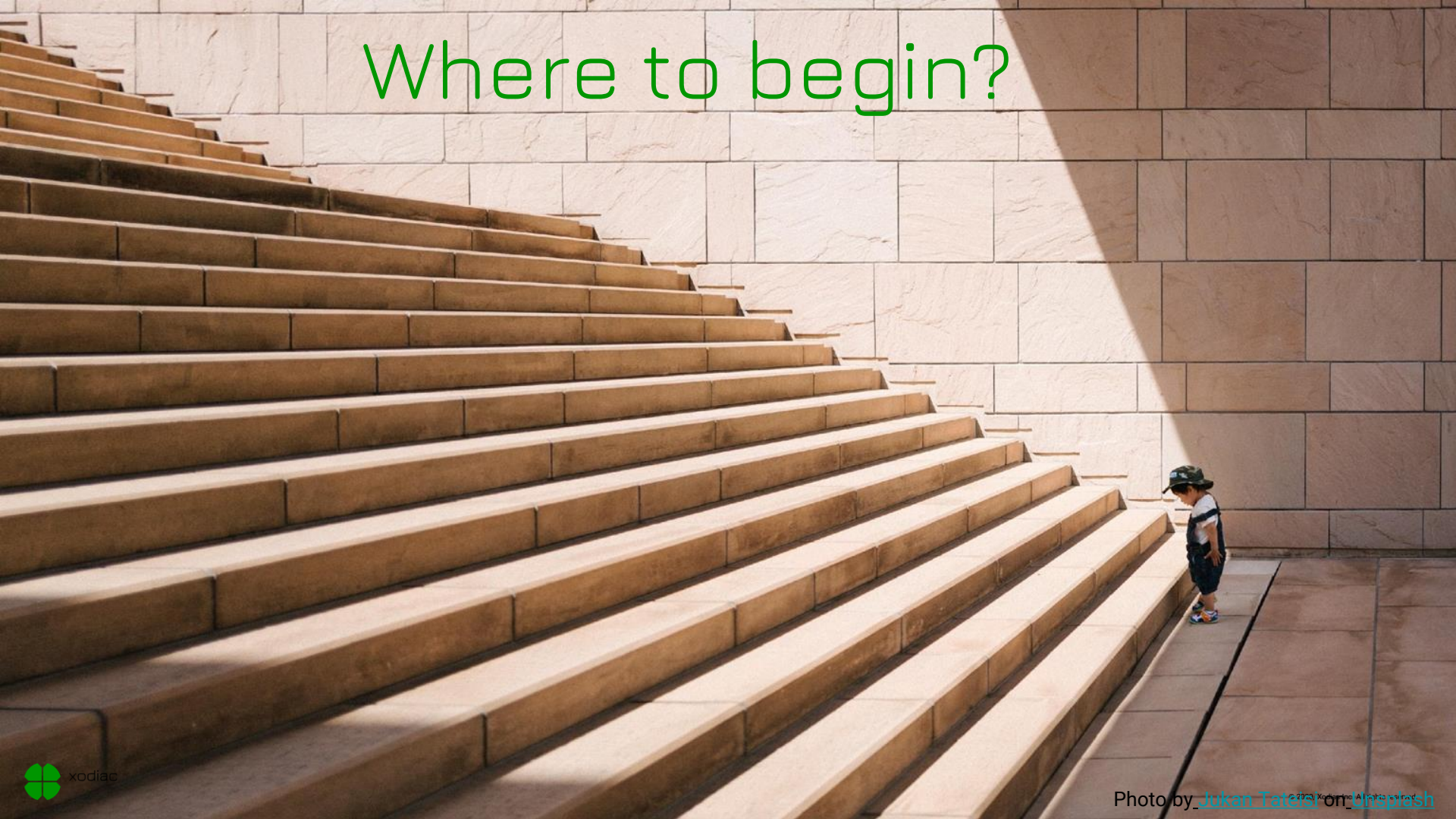
Peter Maddison

Coach, consultant, founder…

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

xodiac

Where to begin?



xodiac

Photo by Jukan Tateisi on Unsplash

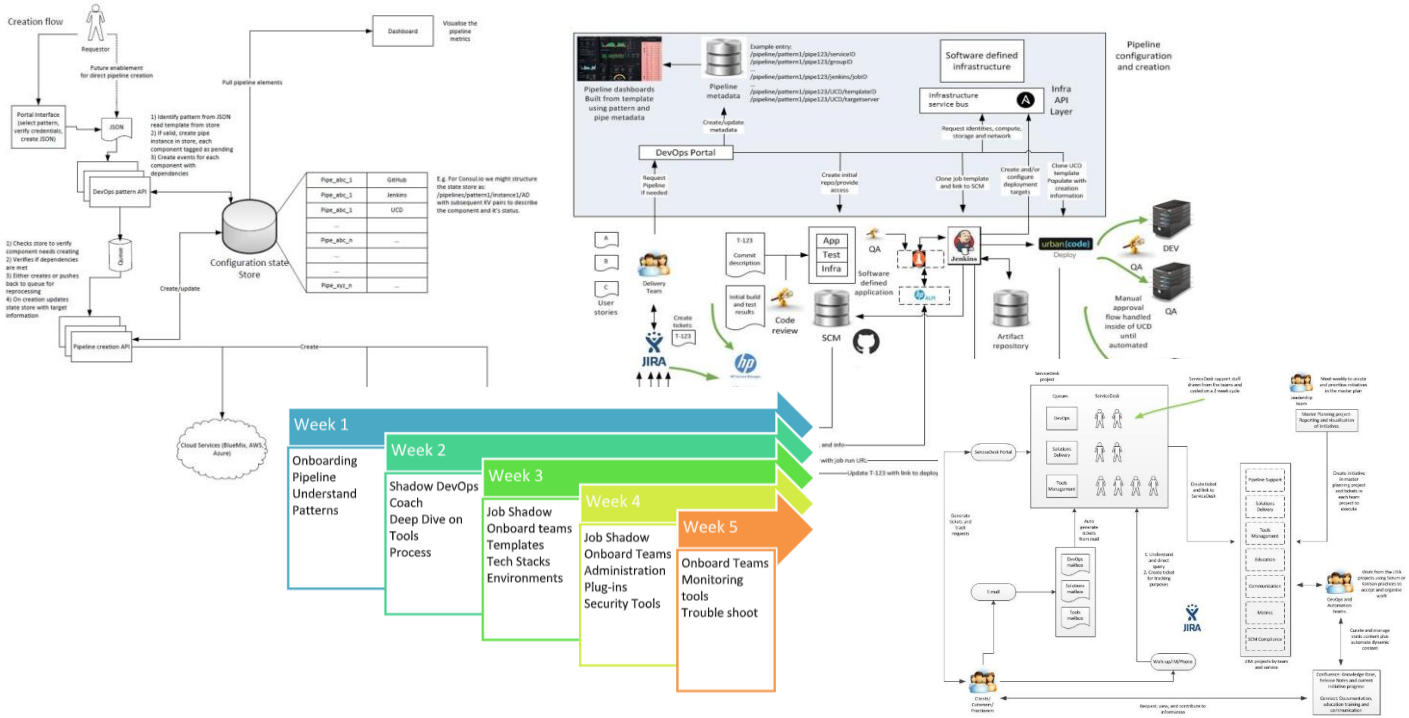
Introducing change

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

xodiac

xodiac

Bunch of pictures

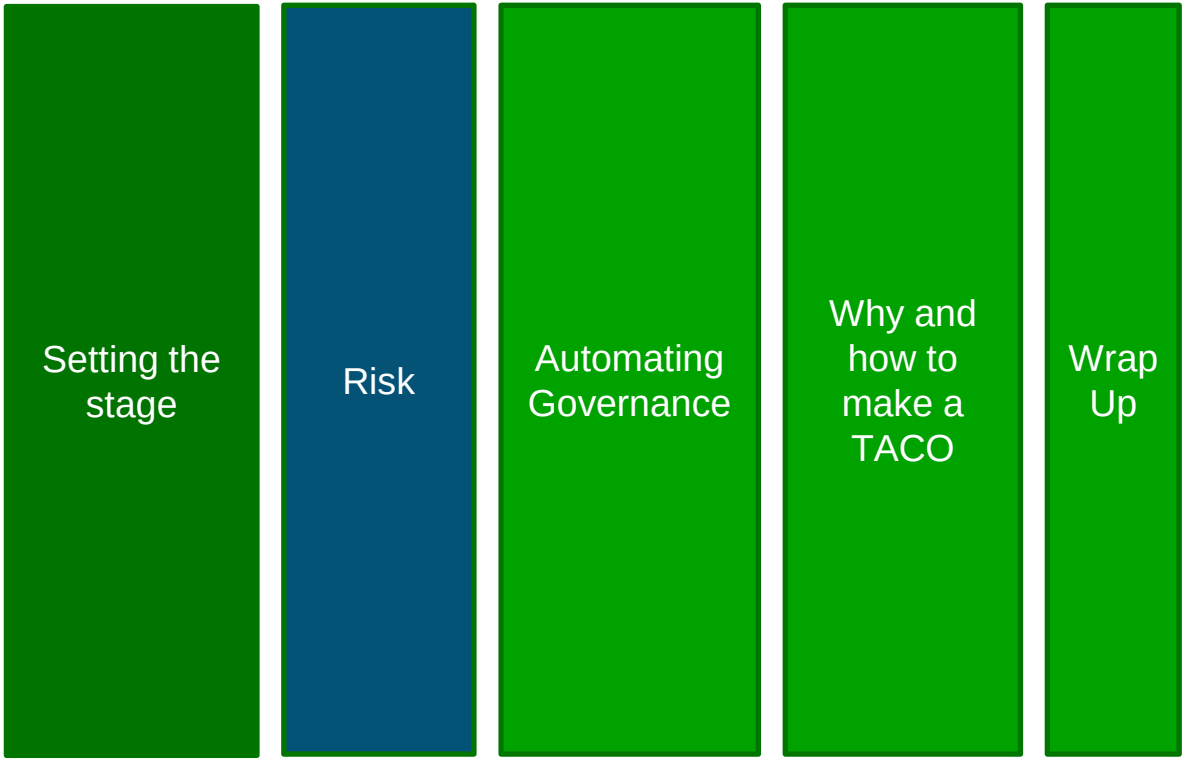


Hitting a wall

xodiac

Photo by Michael Longmire on Unsplash

Talk map



xodiac

GRC

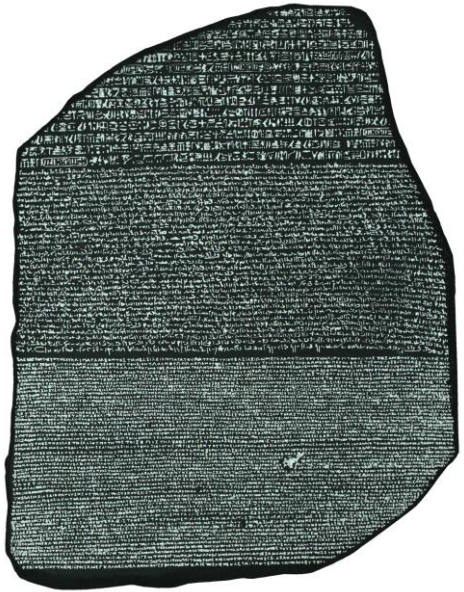
xodiac

Lost in translation

Developers

Security

Operations



Compliance

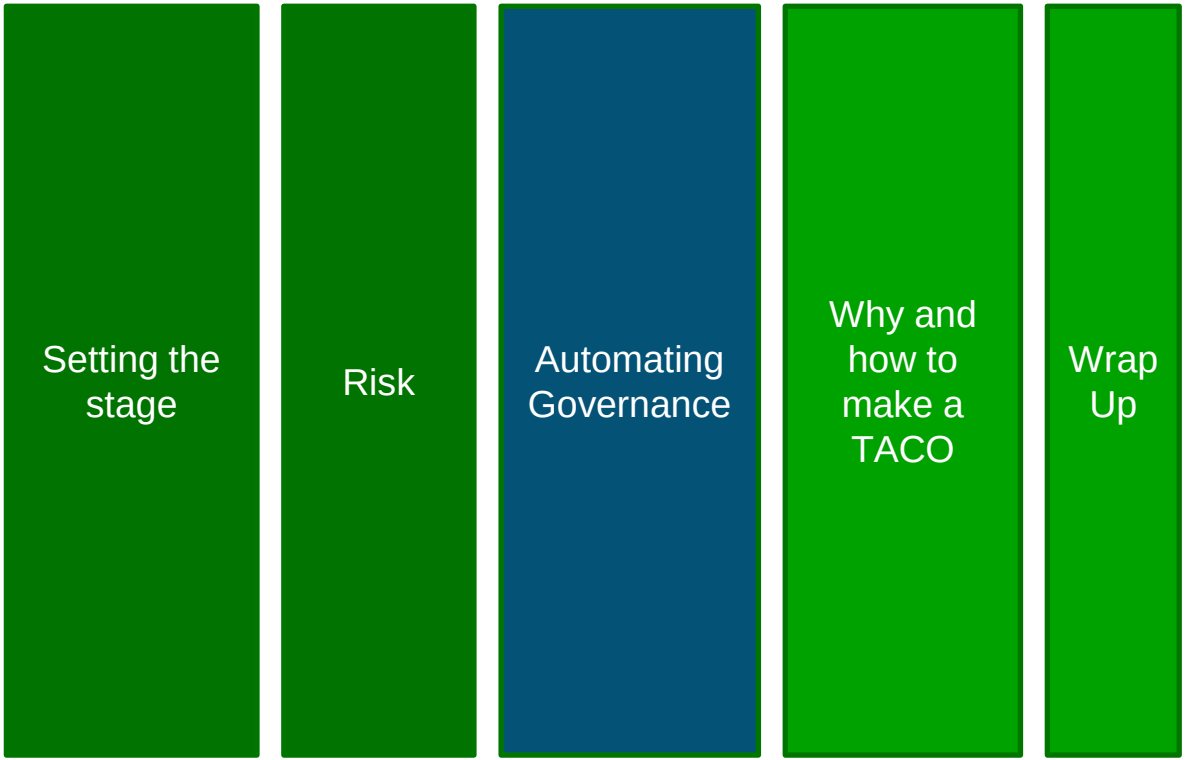
Testing

Architecture

xodiac


Conversation

Talk map



xodiac

Is there a risk?

xodiac

Photo by NordWood Themes on Unsplash

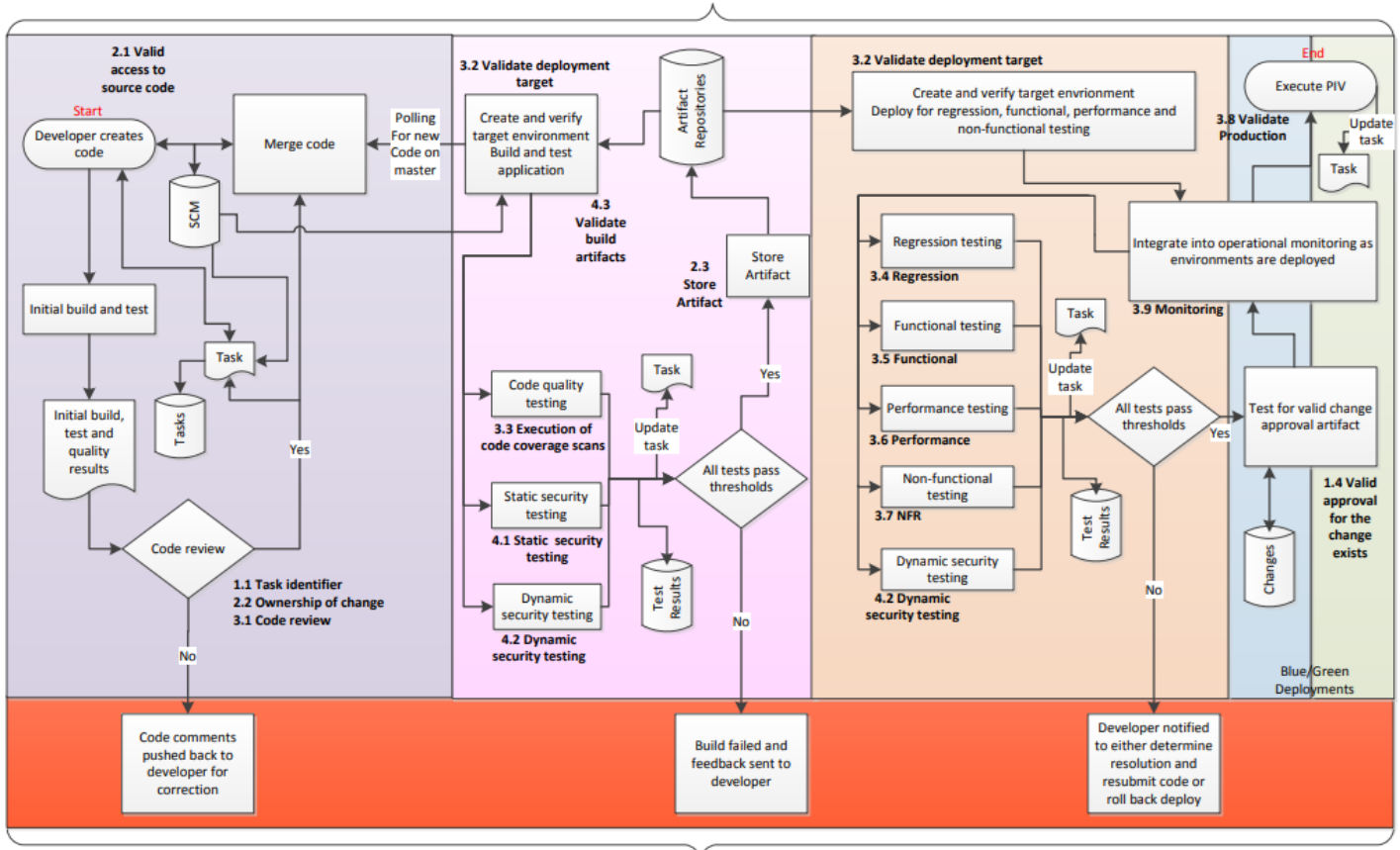
Collaboration

xodiac

Photo by John Schnobrich on Unsplash

Pipeline general case – Controls example

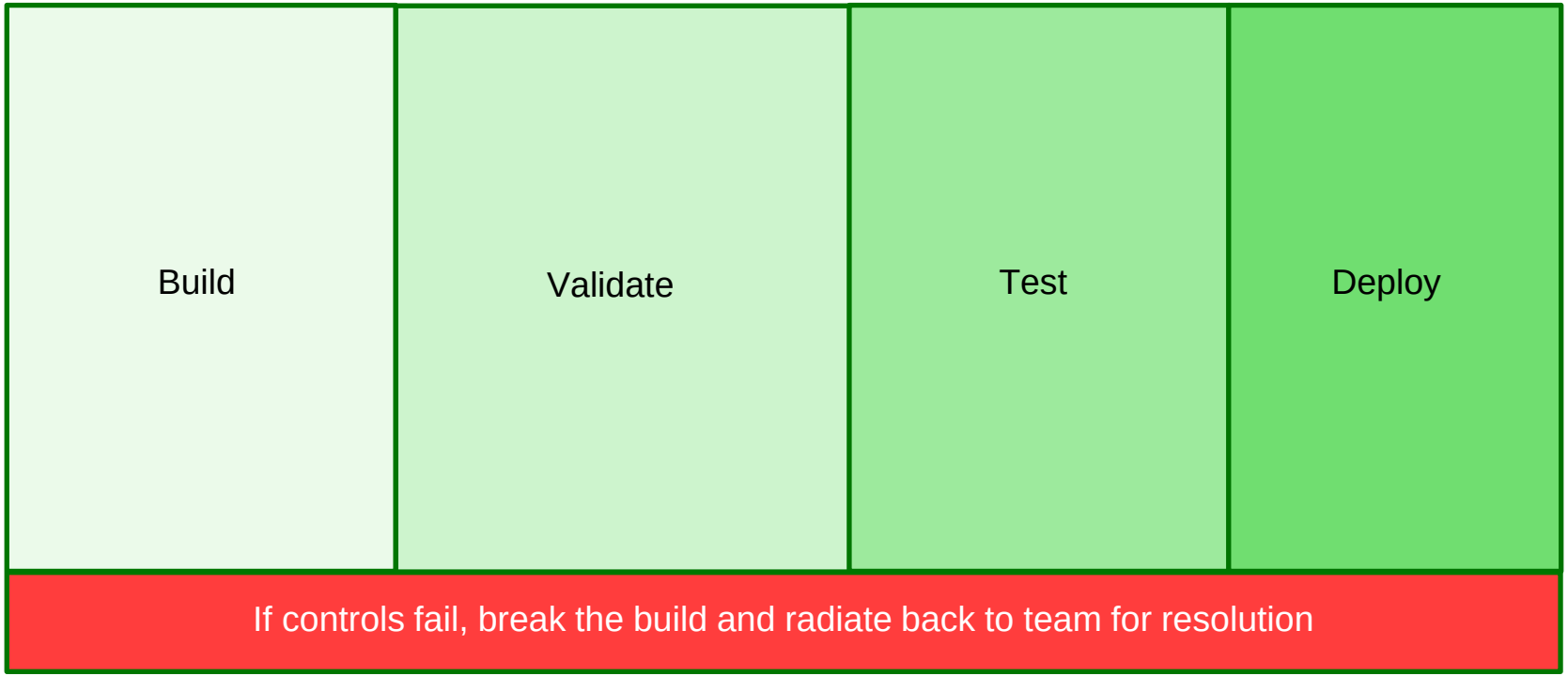
1.5, 2.5, 3.10 and 4.4
Verification that the automated gates put into place are functioning as expected



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

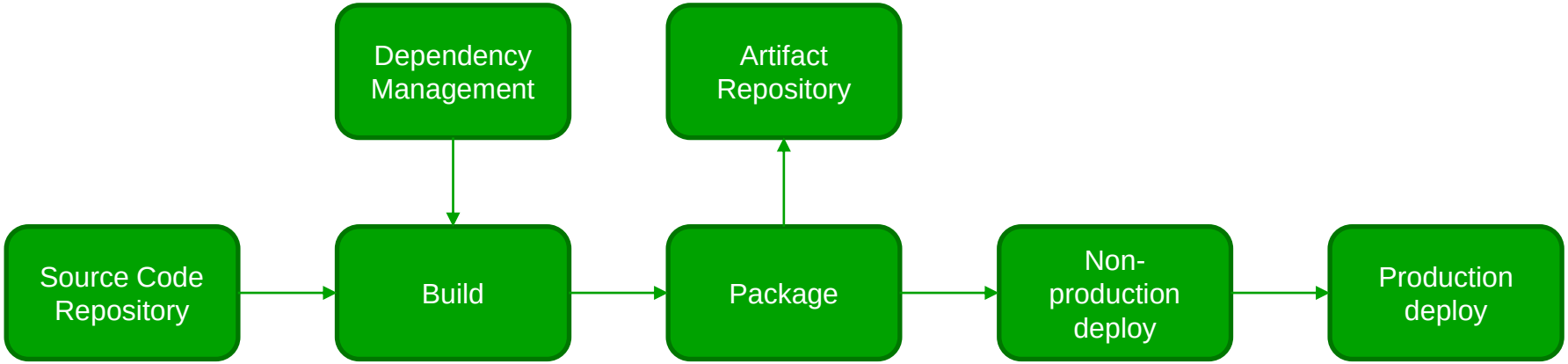
xodiac

Mapping the controls



xodiac

Pipeline



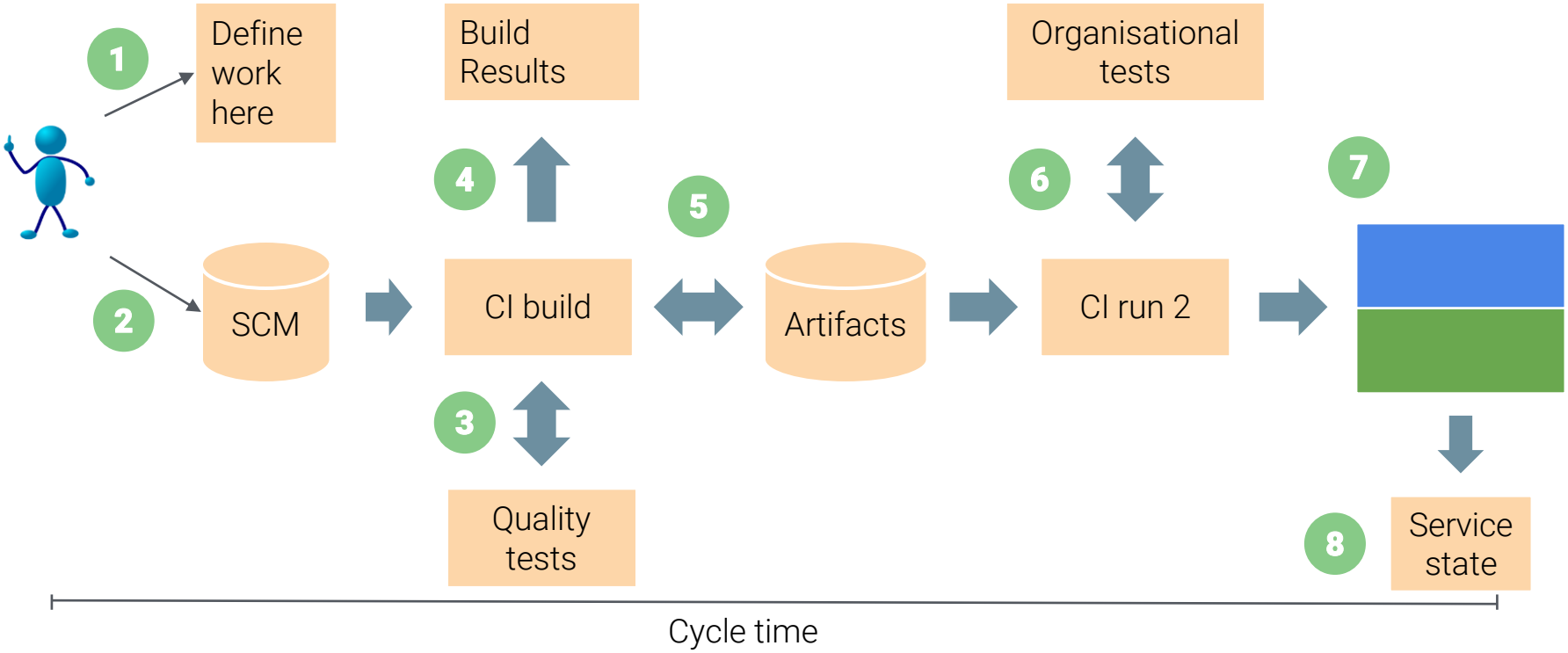
xodiac

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

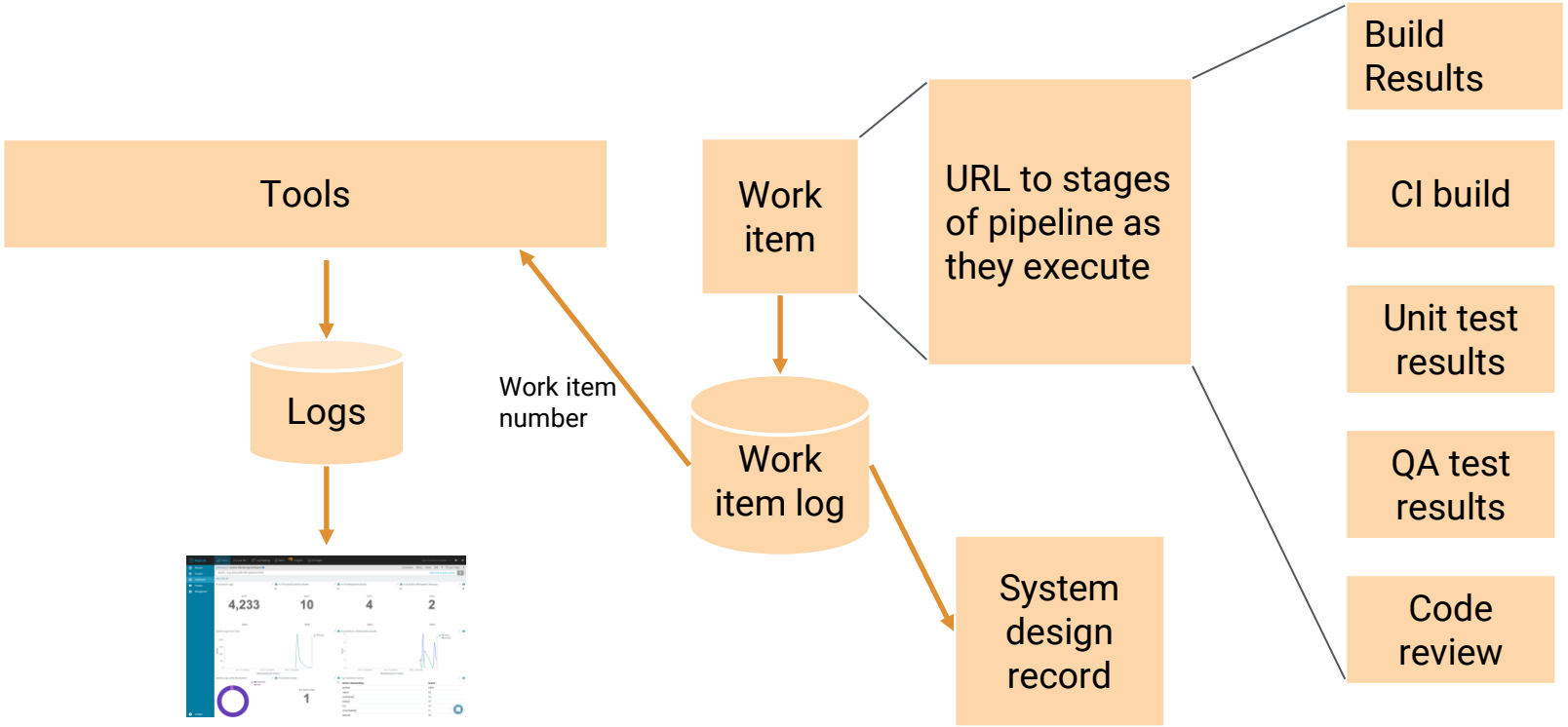
xodiac

Running the pipe



xodiac

Auditing the pipe



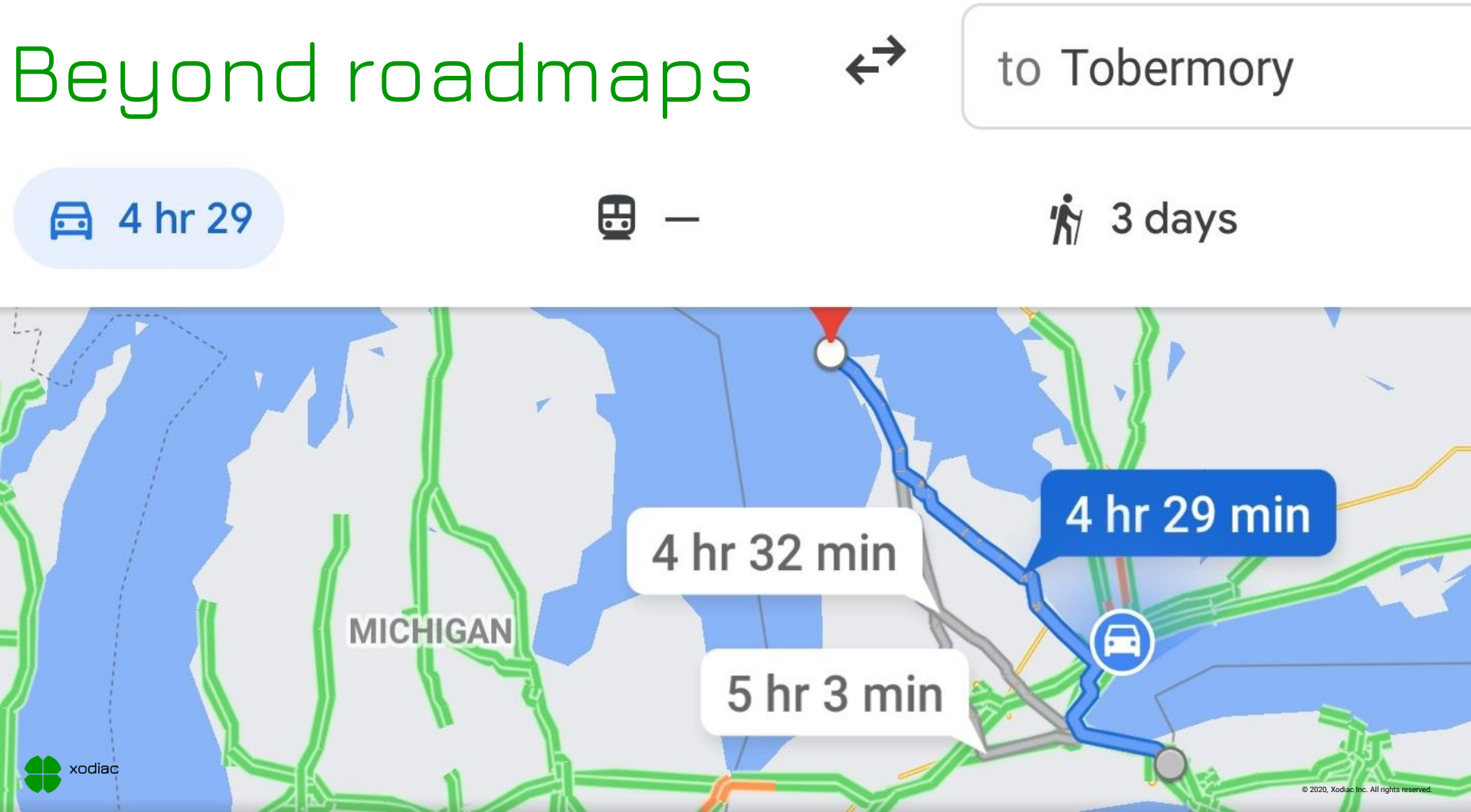
xodiac

Paved road

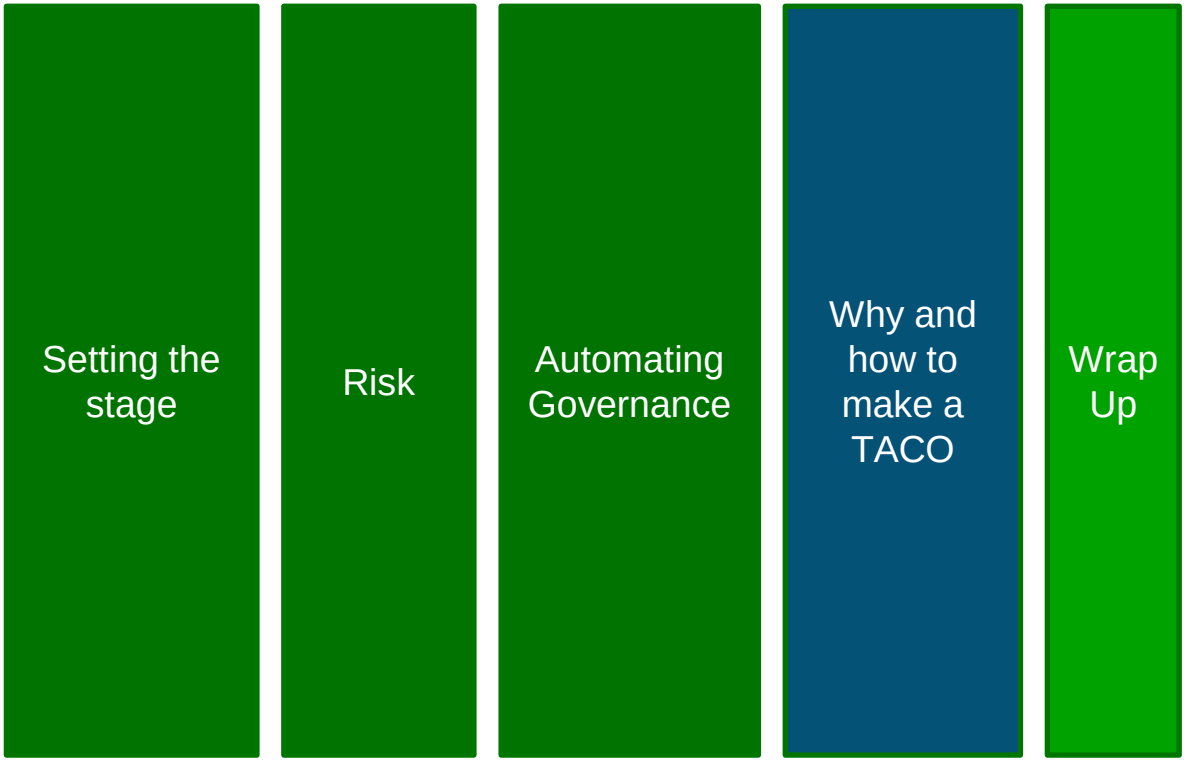
xodiac

Photo by Jon Flobrant on Unsplash

Beyond roadmaps



Talk map



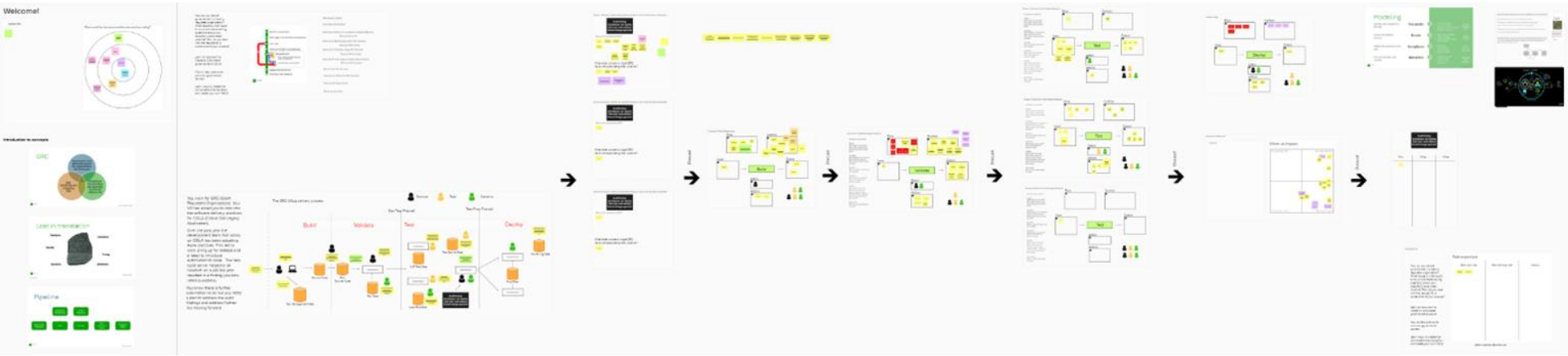
xodiac

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*

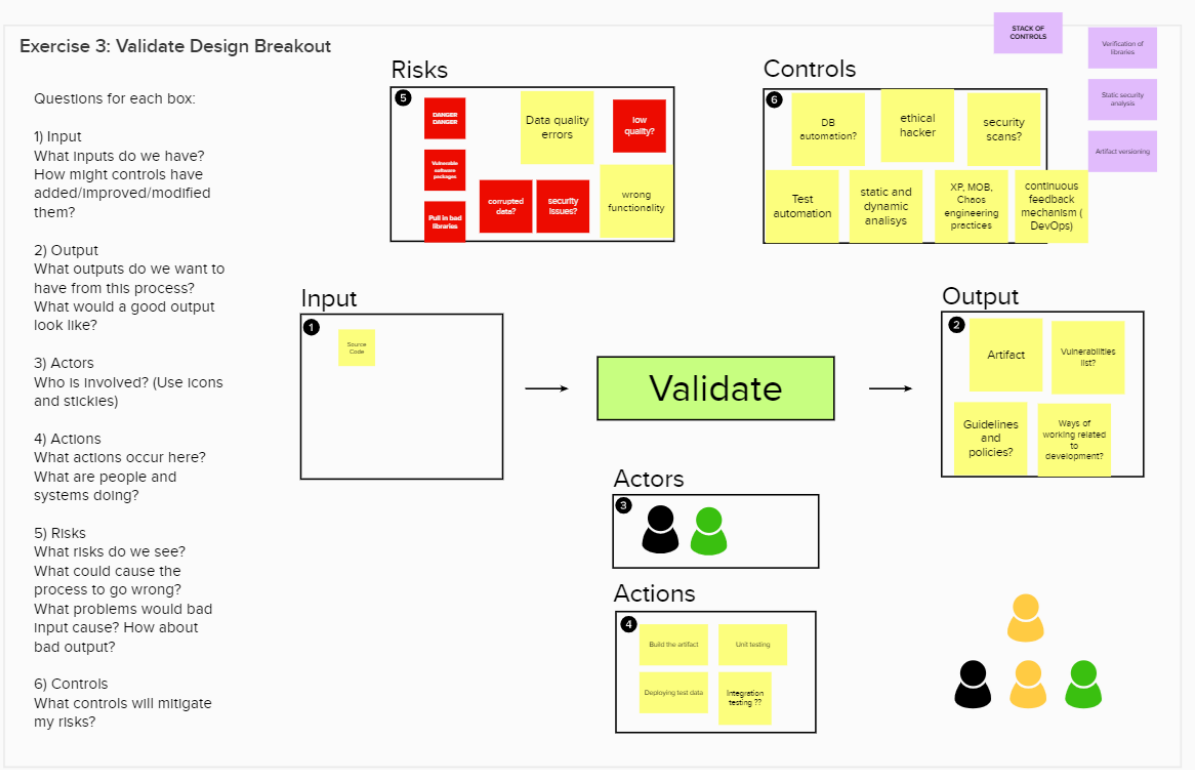
xodiac

Initial controls design



xodiac

Mapping the controls



xodiac

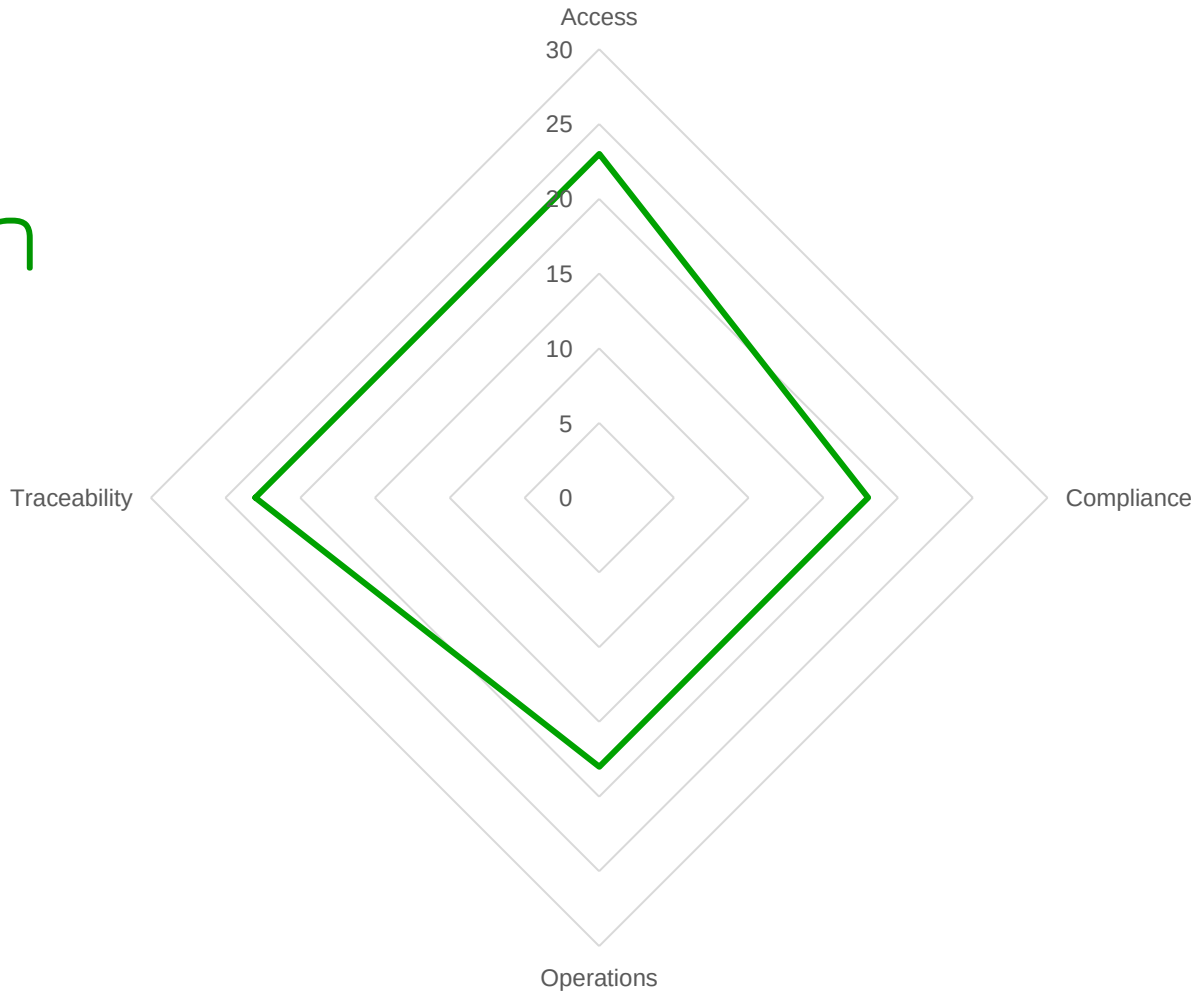
Example

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

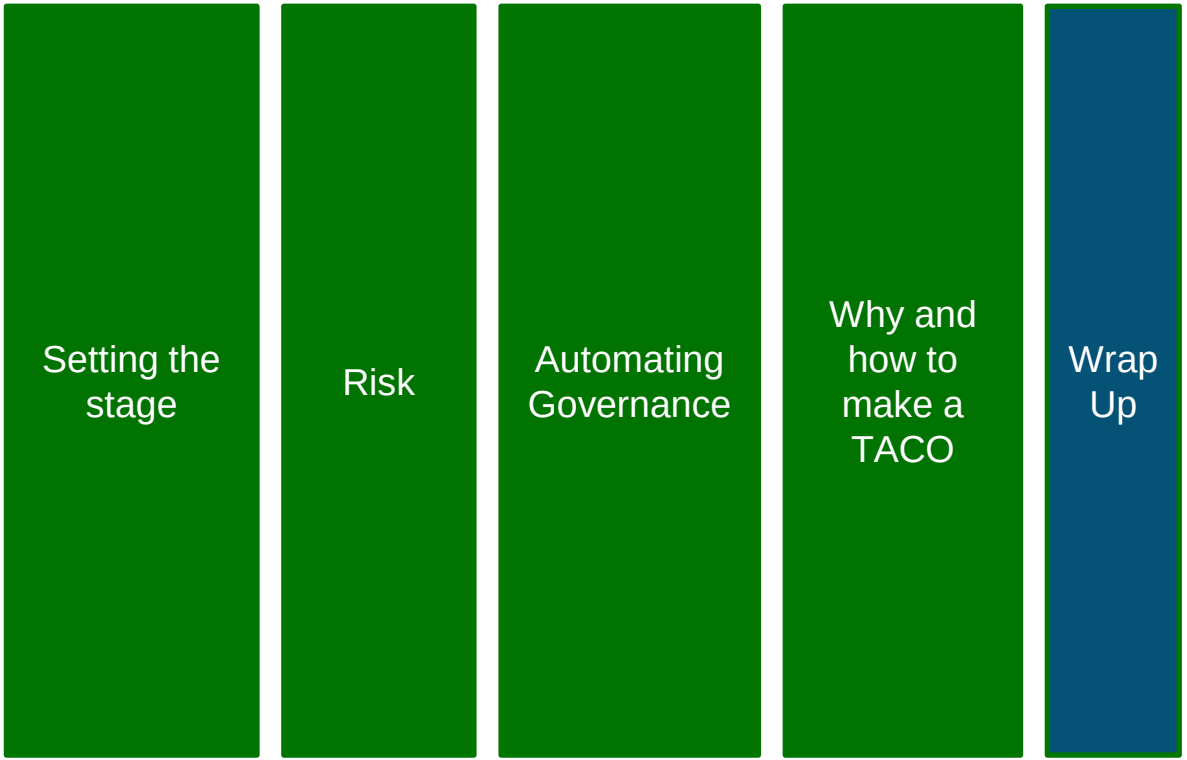


xodiac

TACO!

xodiac

Talk map



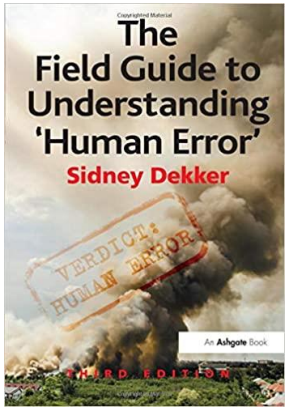
xodiac

Automating Governance

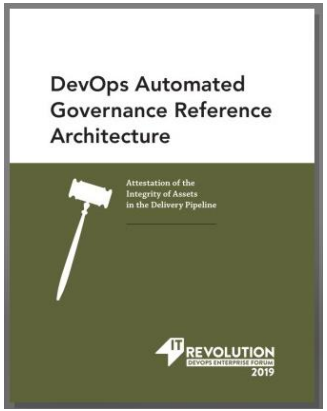
- Not about keeping audit off your back
- Start small, get one team working and grow from there
- Engage leaders, focus on conversation, not tooling

xodiac

References



https://www.amazon.ca/Field-Guide-Understanding-Human-Error-dp-1472439058/dp/1472439058/ref=dp_ob_title_bk



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

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

xodiac
making every team thrive

Feedback survey:

https://bit.ly/2KWP1pA

Thank you!

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

