Securing your pipes with a TACO

The people and process of automating governance

Peter Maddison
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
Driving efficiency

1990 to 2020
Invest in technology capabilities

2020 and beyond
Drive immediate customer value
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 With Precision Without
- 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

Sources: McKinsey, Boston Consulting Group, 2020
Where to begin?
Introducing change

“This year, I resolve to stay away from unnecessary risks.”
“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
Bunch of pictures
Hitting a wall
GRC

Governance: Cost effectively govern the organization's risk landscape

Risk: Identifying and mitigating risks

Compliance: Documenting and reporting on how we address risk
Lost in translation
Is there a risk?
Let's start with the pipeline

1. Source Code Repository
2. Build
3. Dependency Management
4. Artifact Repository
5. Package
6. Non-production deploy
7. Production deploy
Running the pipe

1. Define work here
2. SCM
3. Quality tests
4. CI build
5. Artifacts
6. CI run 2
7. Organisational tests
8. Service state

Cycle time
Auditing the pipe

Tools

Logs

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

Work item number
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
Paved road

Photo by Jon Flobrant on Unsplash
Beyond roadmaps
Modeling

- Identify what happens in the pipe
- Secure the delivery process
- Validate the payload in the pipe
- Record execution and monitor

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

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

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

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

Ensure traceability exists
Validate access
Ensure issues are addressed
Strengthen team behaviour
Example

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Control</th>
<th>Artifact</th>
<th>Location</th>
<th>Control is passed</th>
<th>Control is failed</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that for a given request for change, we have a valid chain of custody allowing us to trace where issues occur</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ticket</td>
<td>Jira</td>
<td>Pull request contains a valid ticket number and</td>
<td>If PR doesn’t contain ticket number, build proceeds but only deploys to dev.</td>
<td>Team lead</td>
</tr>
</tbody>
</table>

Then link this to the tasks to create and the impediments to success
Visualize how much TACO
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
There’s more than pipelines

- Safety culture requires the ability to speak up.
- Speaking up requires we feel “safe”
- Psychological safety is critical

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

A real world example
DevOps
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

Automated Governance – John Willis
https://www.youtube.com/watch?v=j9eB0flTlY

Risk & Control is Dead, Long Live Risk & Control — Jon Smart
https://www.youtube.com/watch?v=XRMr9QjiUwI

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


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

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