We're Sorry. Love, DevOps

Dear Security, Compliance, and Audit

Bill Bensing

Beyonce Rule

If You Like It, Then You Should Tweet On It

@BillBensing

"CI/CD is what we did yesterday. Like usual, we need a word to describe the next phase of something, and CI/CD 2.0 is so 'mehhh.' Modern Governance reminds us that software delivery goes beyond development and operations. It includes everyone,and should be autonomous, at an industrial scale."

Bill Bensing
Red Hat - Managing Architect - Software Factory

Bottom Line Up Front

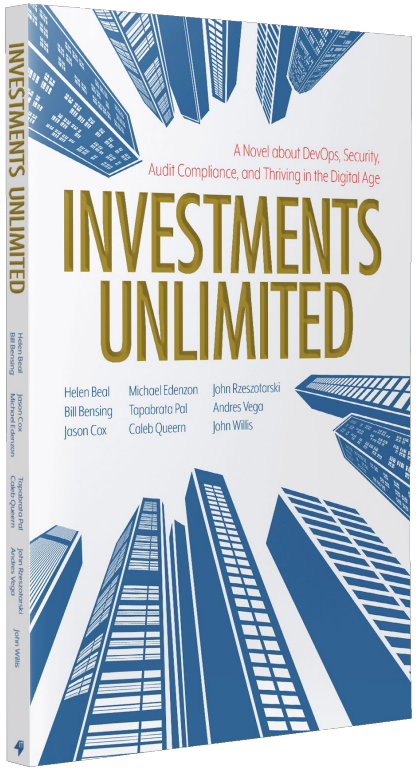
People Should Not Execute

The Governance Process

Machines Must Execute

The Governance Process

People Design, Develop, & Codify The Governance Process

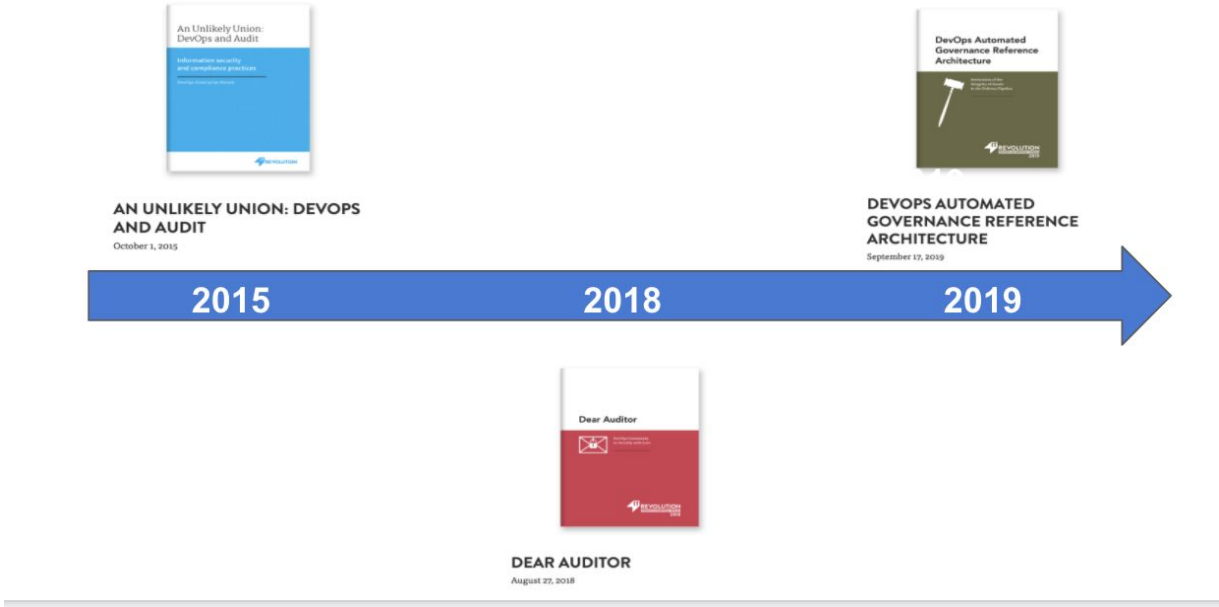


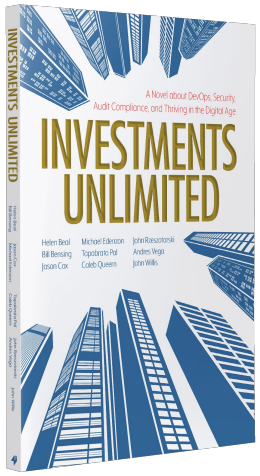
Investments Unlimited

A Novel About DevOps, Security, Audit Compliance, and Thriving in the Digital Age

By Helen Beal, Bill Bensing, Jason Cox, Michael Edenzon, Dr. Tapabrata "Topo" Pal, Caleb Queern, John Rzeszotarski, Andres Vega, and John Willis

https://itrevolution.com/investments-unlimited-book


An Unlikely Union: DevOps and Audit
Information security and compliance practices
AN UNLIKELY UNION: DEVOPS AND AUDIT
October 1, 2015
DevOps Automated Governance Reference Architecture
DEVOPS AUTOMATED GOVERNANCE REFERENCE ARCHITECTURE
September 17, 2019
2015
2018
2019
Dear Auditor
DEAR AUDITOR
August 27, 2018


INVESTMENTS UNLIMITED
A Novel about DevOps, Security, Audit Compliance, and Thriving in the Digital Age
INVESTMENTS UNLIMITED

Dear Auditor,

a love letter to auditors from devops,
where we promise to make life better

With all this growth, we made a mistake, we forgot to bring you along for the ride. That is totally our bad, but we want to make it right. We want to make some new commitments.

- We will bring you along
- We will be fully transparent about our development process
- We do realize that we own the risks
- We will maintain an open channel of discussion to demonstrate to you how we manage risks with our modern development practices

Please don't misinterpret that we are backing down from speed and providing value, but we are really excited to move forward, together.

XOXO,

The DevOps Community

From the Team

Created by Ben Grinnell, James Wickett, Jennifer Brady, Rob Stroud, Sam Guckenheimer, Scott Nasello, Tapabrata Pal

Source: https://www.dearauditor.org

Quickly, Some Epistemology

Governance Refers To Security, Compliance, and Audit.

Let Me Tell You What I'm Going To Tell You

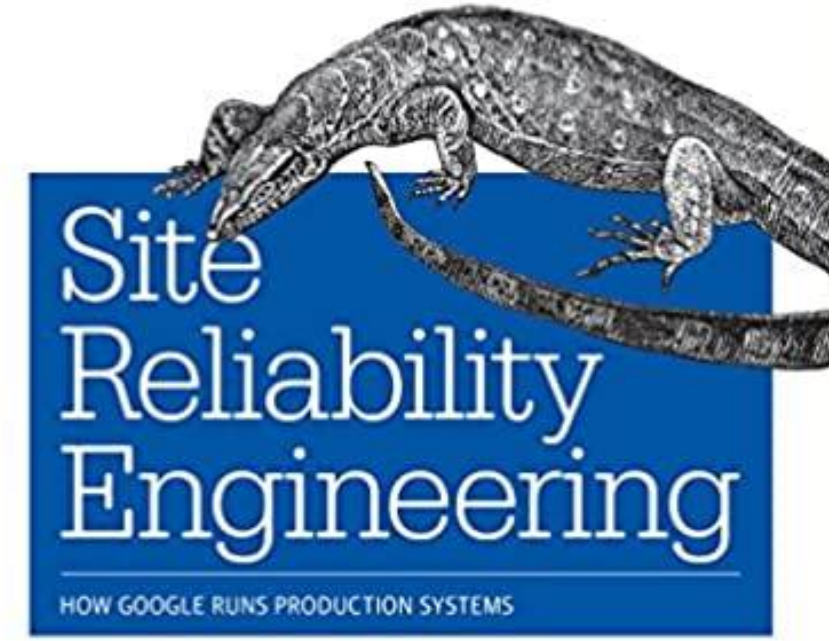
Governance Is The Current Bottleneck For Software Delivery

We Must Modernize Governance Capabilities

Modernizing Governance Is Automating The Governance Process

But...

It's More Than Just Automation, It's Autonomous



"For SRE, automation is a force multiplier, not a panacea. Of course, just multiplying force does not naturally change the accuracy of where that force is applied: doing automation thoughtlessly can create as many problems as it solves. Therefore, while we believe that software-based automation is superior to manual operation in most circumstances, better than either option is a higher-level system design requiring neither of them—an **autonomous** system. Or to put it another way, the value of automation comes from both what it does and its judicious application."

—

Site Reliability Engineer, Google
Chapter 7 - The Evolution of Automation at Google

Source: https://sre.google/sre-book/eliminating-toil/

Modern Governance Is A Higher-Level Governance System Design

Modern Governance is Autonomous Governance

We Must Resolve The Impedance Mismatches When Autonomizing Governance

Resolving Impedance Mismatch - Technology Adoption

"Beyond The Goal" - Dr. Eliyahu Goldratt

1

Its Power

Achieve speed-to-market & highest trust simultaneously.

2

Diminished Limitations

Ineffective manual processes which decrease time-to-market

3

Old Rules

Domain-specific people manually verify all aspects of trust: Security, Compliance, & more...

4

New Rules

Domain-specific people define & codify trust, automation validates.

Agenda

The Problem

How To Solve

A Solution, with Demo

A Recommendation

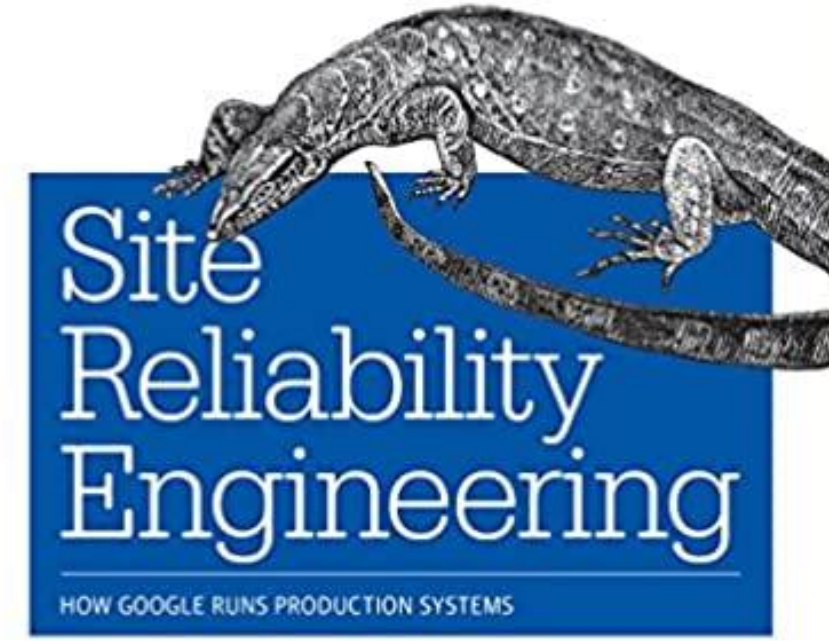
The Problem

In Most Organizations, Governance is...

Security
Compliance
+ Audit

Toil

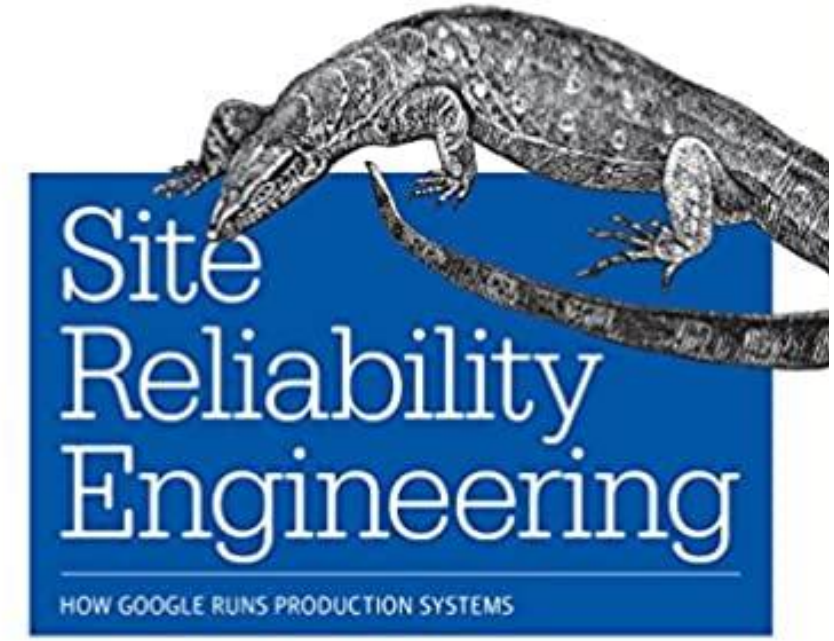
What Is This Toil?



"Toil is the kind of work tied to running a production service that tends to be manual, repetitive, automatable, tactical, devoid of enduring value, and that scales linearly as a service grows."

Vivek Rau
Site Reliability Engineer, Google

Source: https://sre.google/sre-book/eliminating-toil/



"If a human operator needs to touch your system during normal operations, you have a bug. The definition of normal changes as your systems grow."

Carla Geisser
Site Reliability Engineer, Google

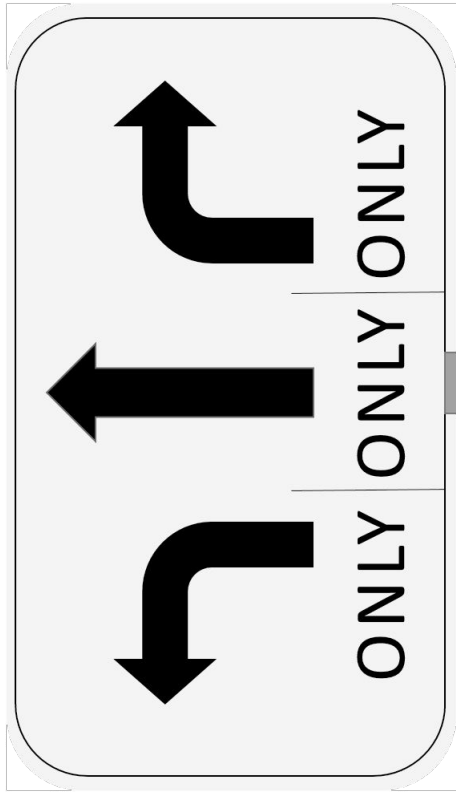
Source: https://sre.google/sre-book/eliminating-toil/

Governance Toil

Delivery Toil

Governance Toil

Humans Turning Cranks Of The Governance Process

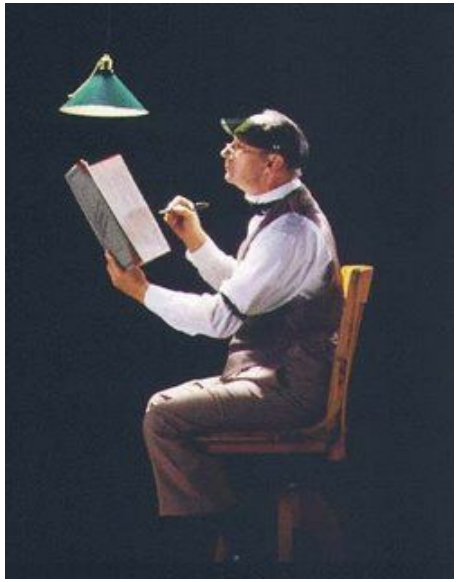


Delivery Toil

Outcomes Caused By Ambiguity of Governance Process

Because of this toil...

What is Meant To Mitigate Risks Actually Increases Risk!



I Have The Numbers

To Prove It

The Risk of Your Governance Process Implementation

Governance Creating Risk, Not Mitigating It

Work in Process

8 hrs.

98% Success Rate

40 hrs.

90% Success Rate

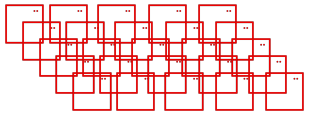
A More Relatable Example

Why Can't Governance Take Just Second?!

Work in Process

16 hrs.

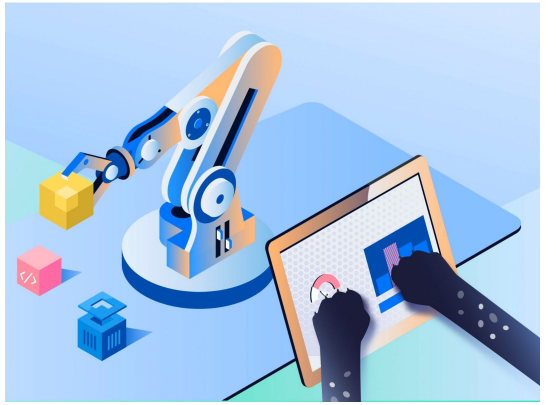
98% Success Rate



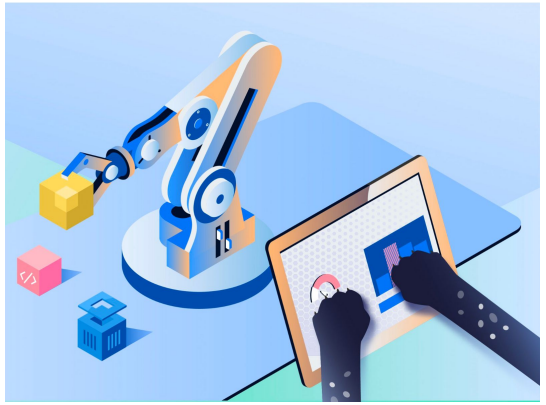
400 hrs.

60% Success Rate

How To Solve



Automate That Stuff!



~~Automate~~ Autonomize

That Stuff!

How Do We

Autonomize Governance?

Five Guiding Principles

1. **Collaboration** Across All Parties: Software Engineers, Systems Operators, Security, Compliance, Auditors.
2. Develop **Enabling Constraints**
3. Require **Explicit Evidence**
4. Treat Governance Execution as **Zero-Trust**
5. Implementation Must Operate **Ephemeral**, With **Idempotence,** And **Immutably**

Key Architectural Themes

Applying Modern Governance

1. **Externalize Policy Execution** - Policy evaluation must be extracted from any individual tool
2. **Trusted Agent** - Collect Evidence, Attest, Enforce Policy
3. **Observibility** - More important to know what is not/cannot be validated, as opposed to what is passing & failing
4. **Convergence** - Distill processes, tools, policies, and procedures to a few standardized reusable cross-cutting concerns

We Need To Think Differently

Autonomizing Requires Moving From Subjective to Continuous Verification

	Subjective	Objective	Verifiable
Risk	Change Management	Attestations and Control	Continious Verification

To Achieve Continuous Verification

We Must Autonomize The Human Controlled Gates

The Control Gates To Autonomize

Continuous Verification For All Go/No-Go Decision Points

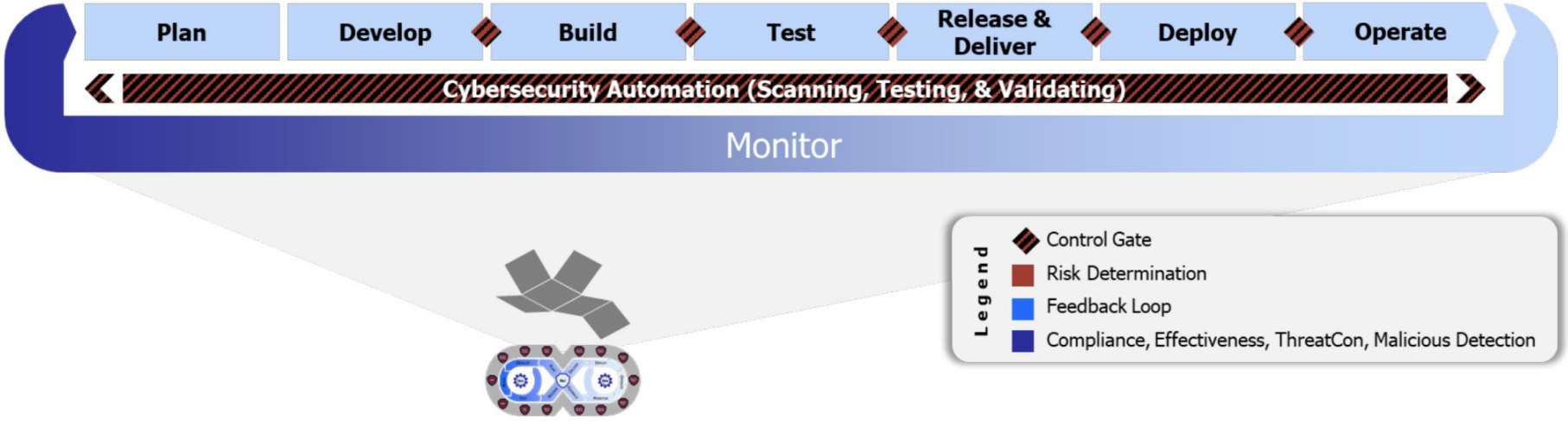


Figure 6 DevSecOps Lifecycle Phases, Continuous Feedback Loops, & Control Gates

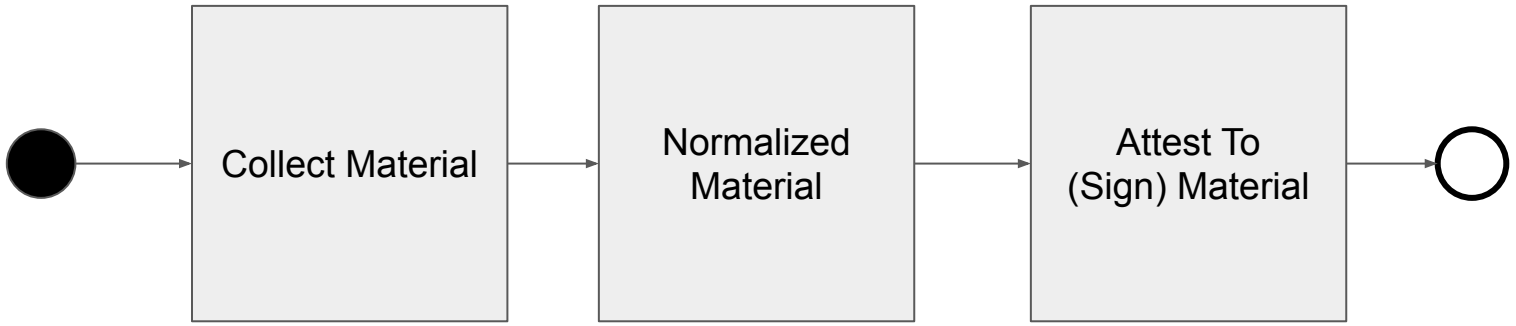
Source: https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Strategy-Guide.pdf (Pg. 19)

How Do We Autonomize Human Control Gates?

Some Quick Definitions

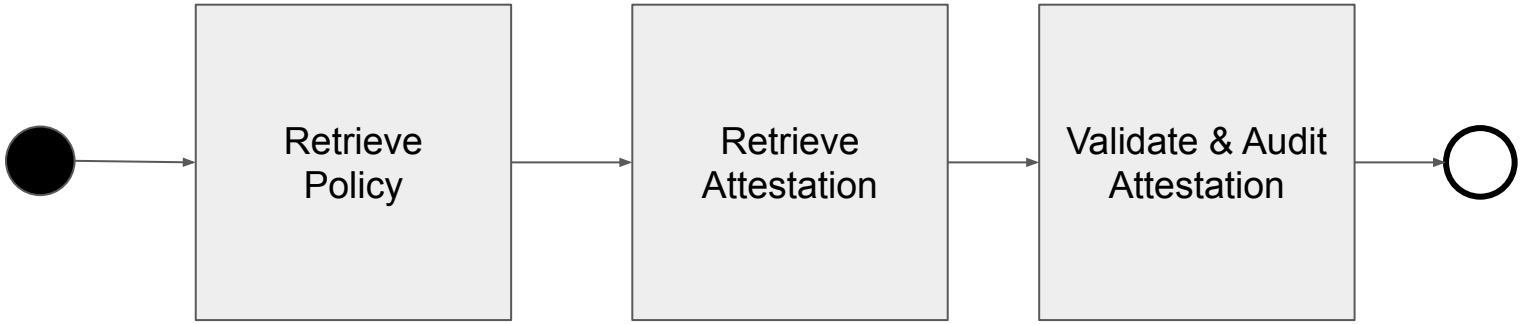
- **Evidence** - Structured/Unstructured data collected from a tool/service that performs some task against a software artifact
- **Attestation** - Summarized and signed evidence
- **Policy** - Data which describes the outcomes expected from a review of the evidence
- **Audit** - A pass/fail comparison of an attestation with a corresponding policy

Autonomize Control Gate Activity



Evidence & Attestation Procedure

Policy Enforcement Point Procedure



To Do This Properly,

We Need A New Concept

We Need A

Governance Contract

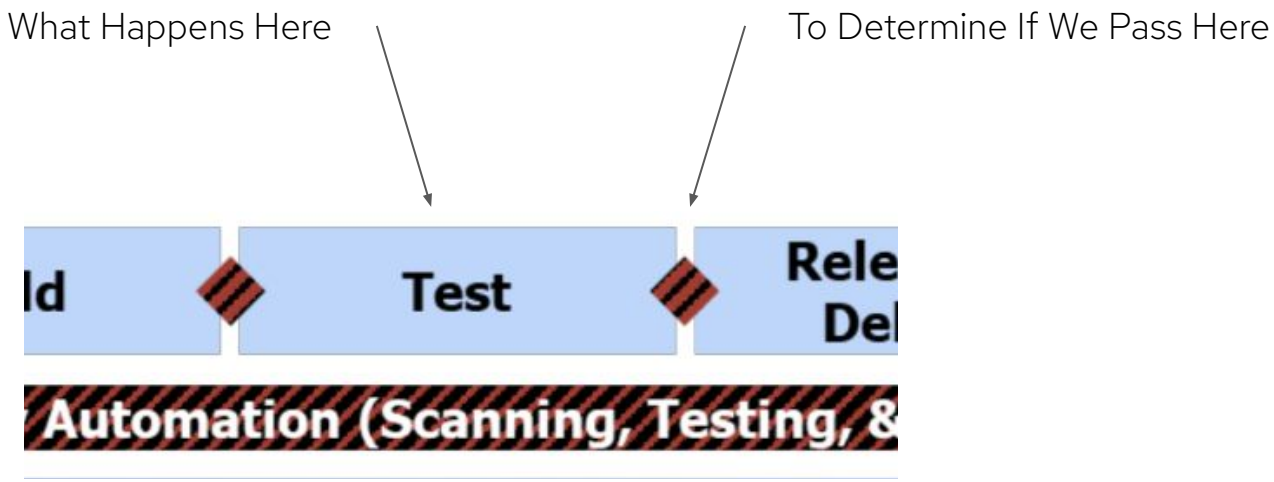
What Is a Governance Contract?

A Governance Contract Defines The Semantics & Syntax of Our Governance Primitives

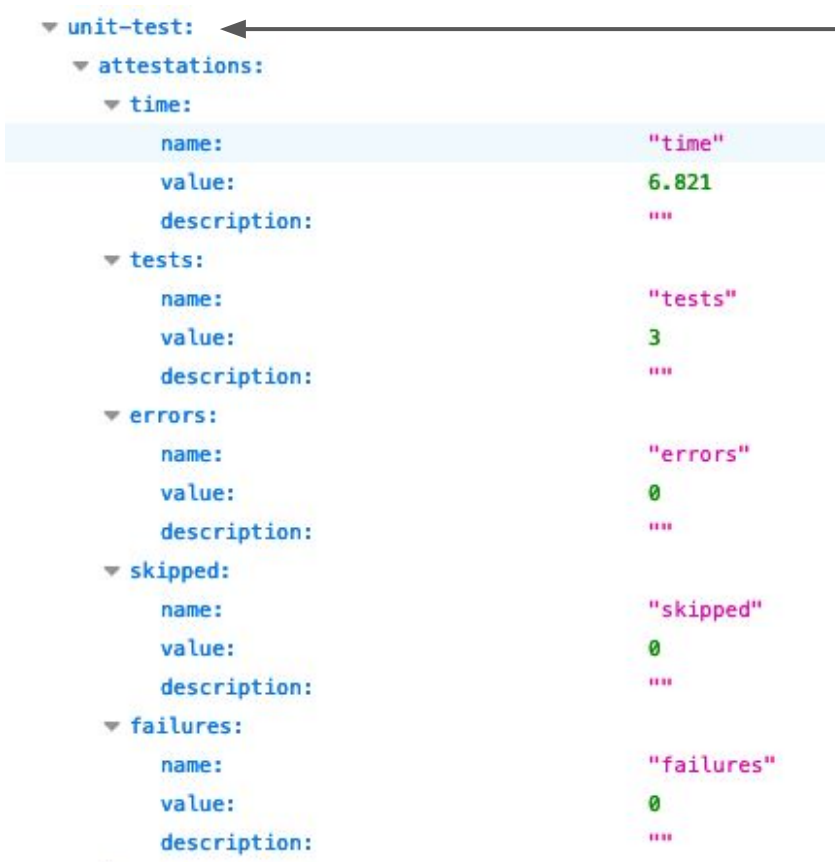
It's How We Codify Our Governance Specifications

The Governance Contract Describes

In A Way That Is Technology & Tool Agnostic

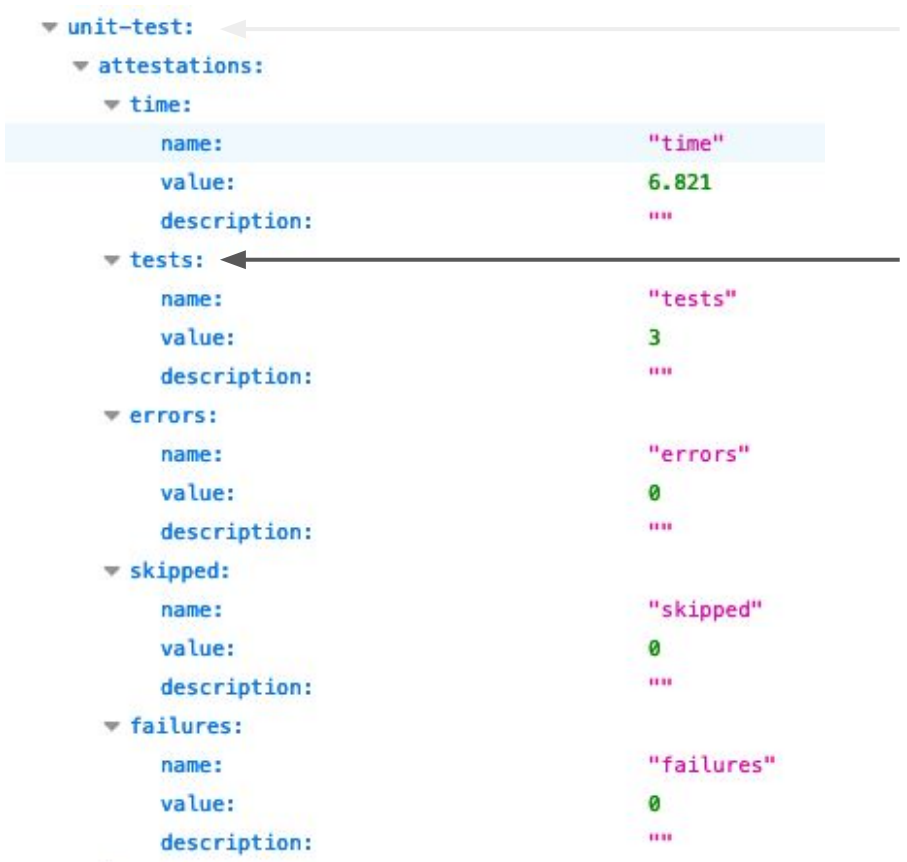


For **All Gates**, Not Just Testing



Governance Procedure

The control gate required by the governance process.



Governance Procedure

Procedure Element

A specific output of the procedure which is measured for compliance to a policy.

Governance Procedure

Procedure Element

Procedure Element Value

The value which is evaluated during an audit against a policy.

How Is a Governance Contract Created?

Governance Contract is Serialized Evidence

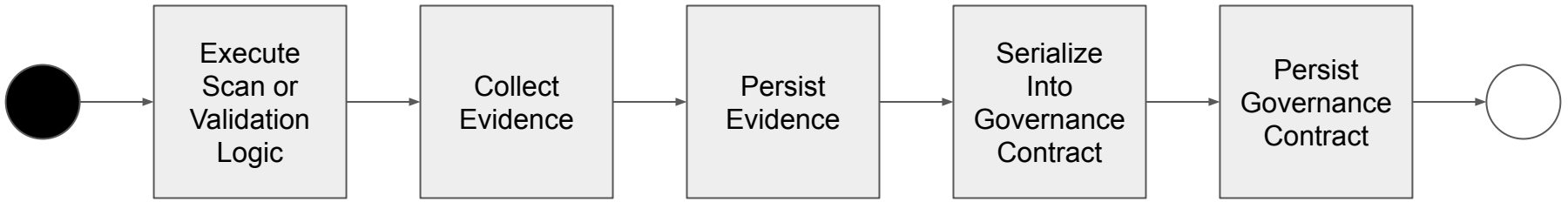
First Step To Externalizing Policy Execution

```
-------------------------------------------------------
 T E S T S
-------------------------------------------------------
Running org.acme.rest.json.[1mFruitResourceTest[m
[1;32mTests run: [0;1;32m2[m, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 6.81 s
Running org.acme.rest.json.[1mLegumeResourceTest[m
[1;32mTests run: [0;1;32m1[m, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 0.011 s

Results:

[1;32mTests run: 3, Failures: 0, Errors: 0, Skipped: 0[m
```


```
unit-test:
  attestations:
    time:
      name:        "time"
      value:       6.821
      description: ""
    tests:
      name:        "tests"
      value:       3
      description: ""
    errors:
      name:        "errors"
      value:       0
      description: ""
    skipped:
      name:        "skipped"
      value:       0
      description: ""
    failures:
      name:        "failures"
      value:       0
      description: ""
package:
  attestations:    {}
```

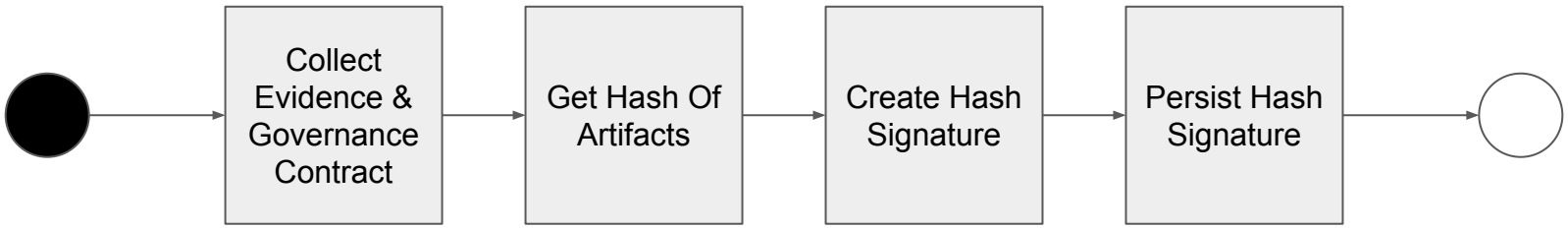
Evidence Collection & Serialization

Happens for Each And Every Scan or Validation



Attestation

At The End Of Either Each, Or A Group Of, Scans Or Validations



How Is A Governance Contract Evaluated Against A Policy?

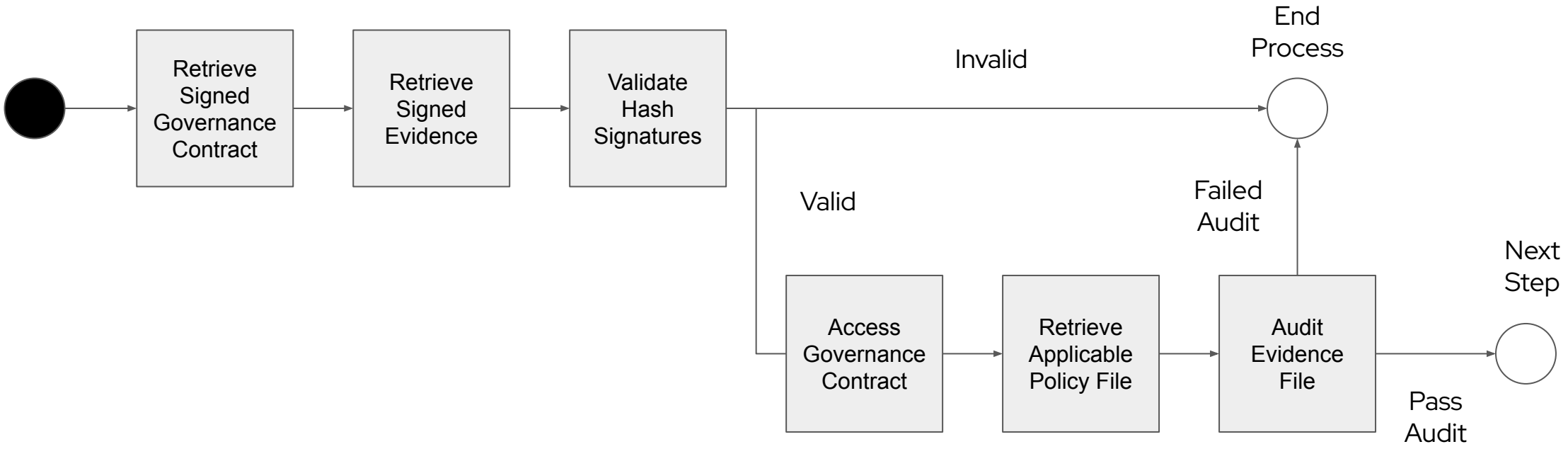
Apply Policy as Code To Governance Contract

Second Step To Externalizing Policy Execution

```
unitTestPass {
    input.workflow.unitTest.attestations.testQuantity == input.workflow.unitTest.attestations.passQuantity
}

codeCoveragePass  {
    input.workflow.staticCodeAnalysis.attestations.codeCoverage >= 80
}

complexityPass {
    input.workflow.staticCodeAnalysis.attestations.cyclomaticComplexity < 40
}

staticCodeAnalysisPass {
    codeCoveragePass
    complexityPass
}

passAll {
        unitTestPass
        staticCodeAnalysisPass
}
```

Policy Enforcement Point (Audit)

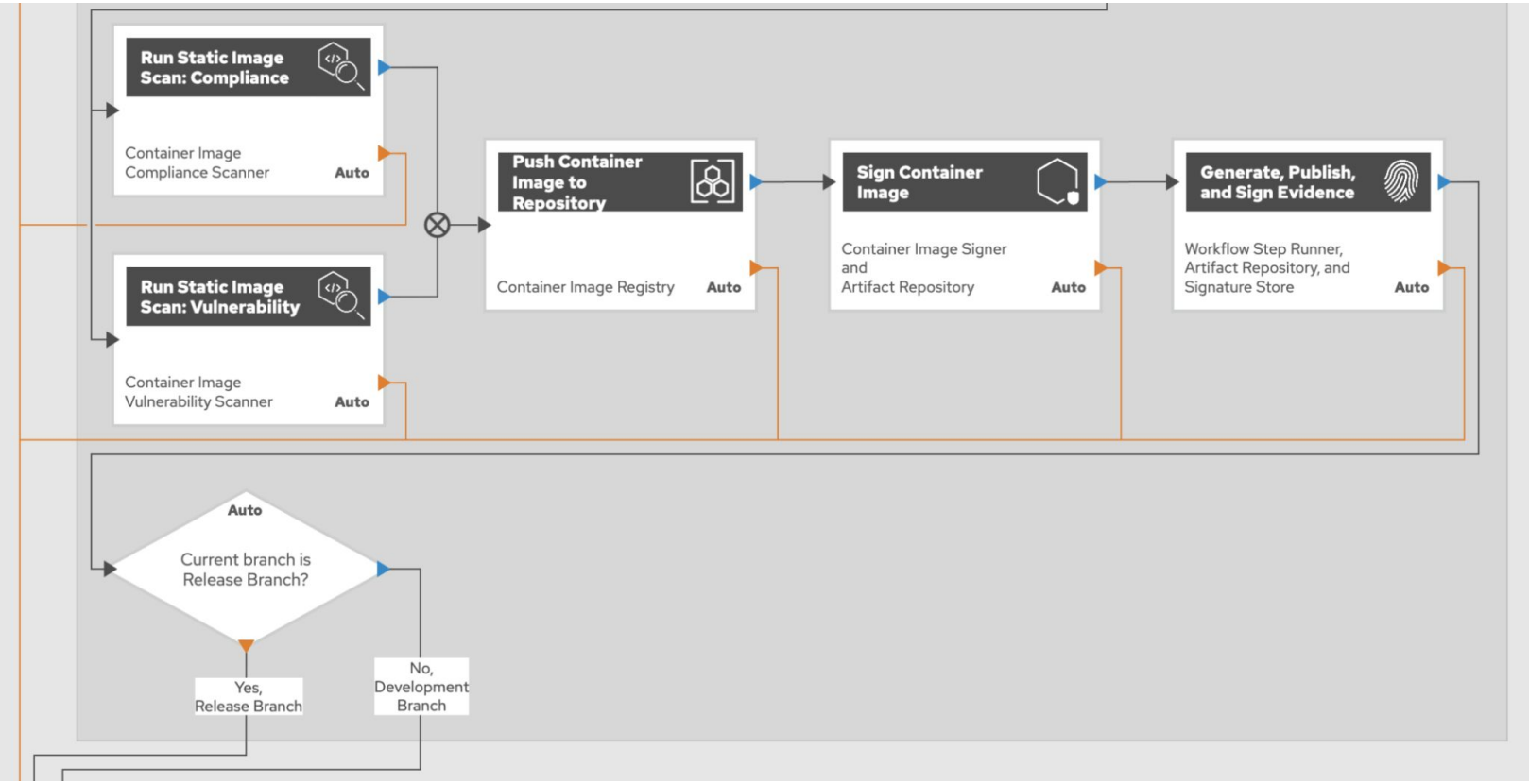
At The Beginning



What Does This Look Like When Applied to Software Delivery?

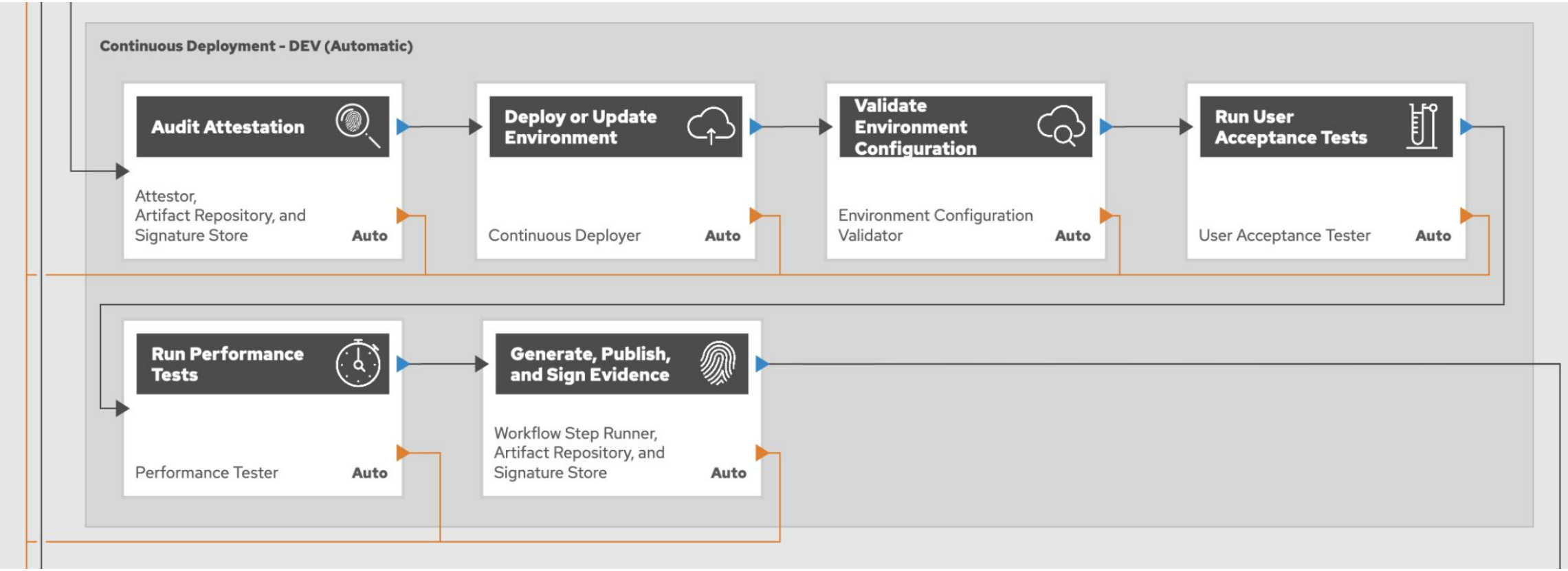
Continuous Integration as Evidence

Collection & Attestation of Continuous Integration



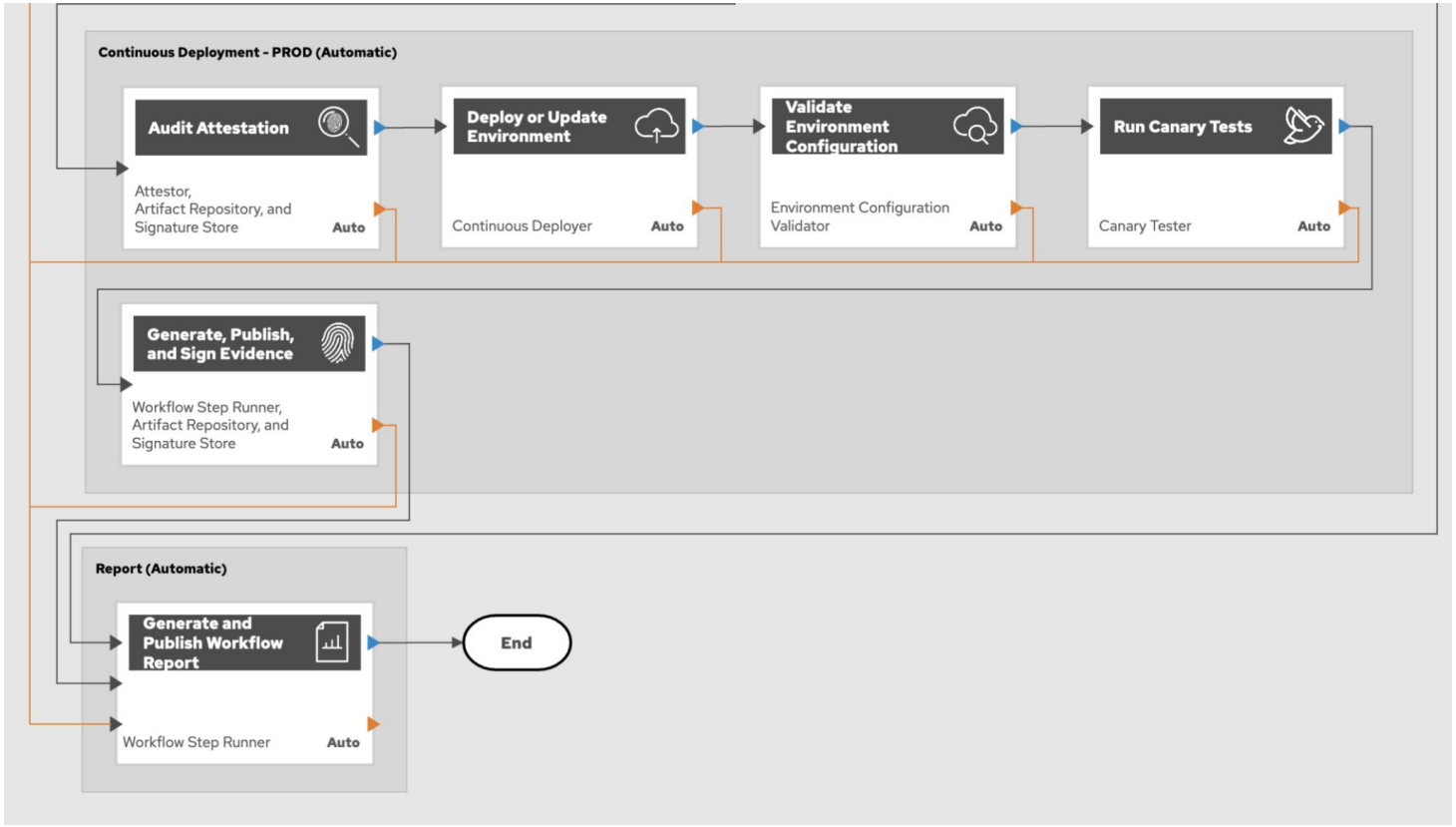
Validateable Continuous Deployment

Audits Are Autonomous Pre-Conditions of Continuous Deployment



100% Autonomous - Commit to Production

Autonomous Governance = Compliance as Code + Policy as Code



Autonomize Gates

Includes, But Not Limited Too

- Code Review Validation
- Unit Testing
- Static Code Analysis
- Dynamic Code Analysis
- Vulnerability Testing
- Compliance Validation
- Software Bill of Material (SBOM)
- Security Technical Implementation Guide (STIG)
- Use Acceptance Testing

A Solution

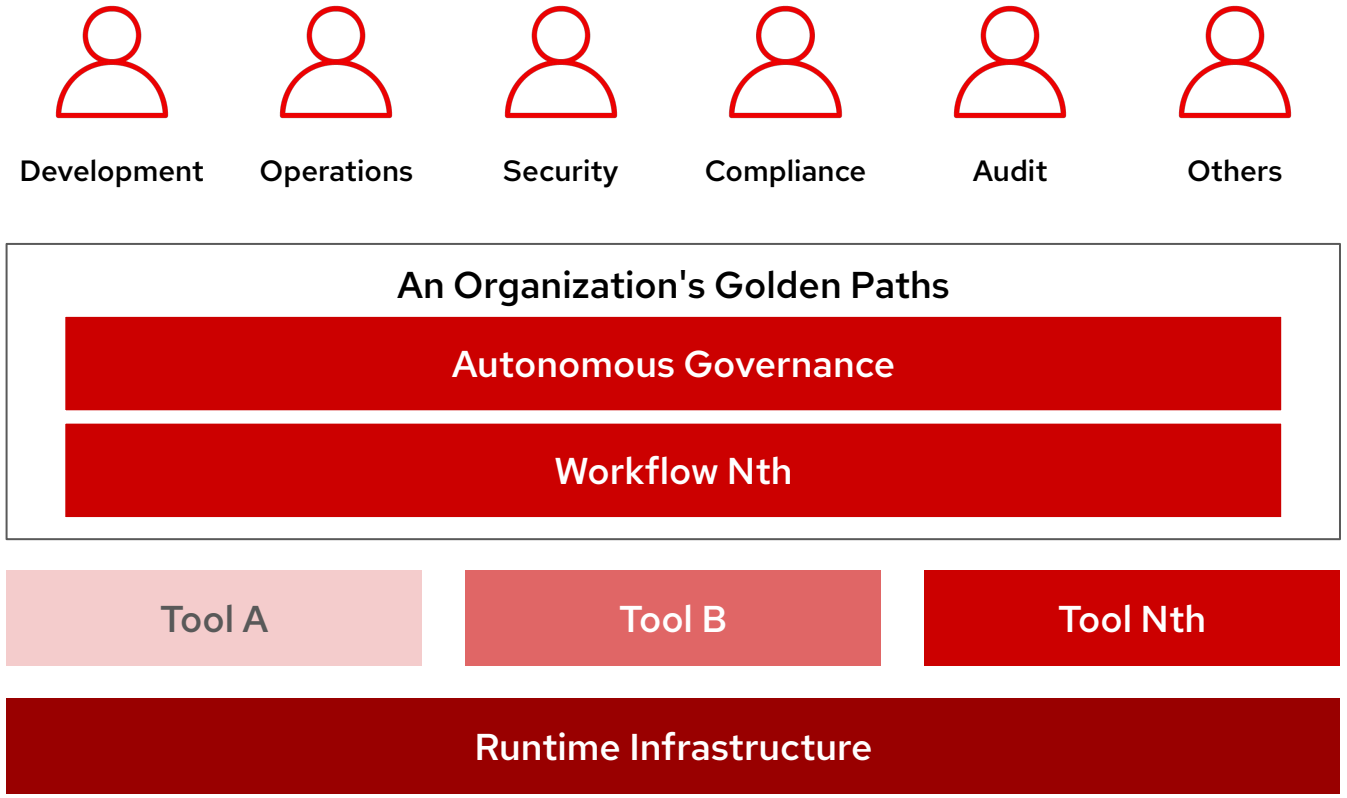
Ploigos

Source: https://github.com/ploigos

Ploigos - Step Runner

Making The Complex Manageable, Scalable, And Repeatable

A technology-agnostic canonical implementation of SDLC tooling, with default workflow implementations, that allows anyone to layer in current, and future unknown concerns, which are independent of SDLC tool execution.



Golden Paths with Ploigos

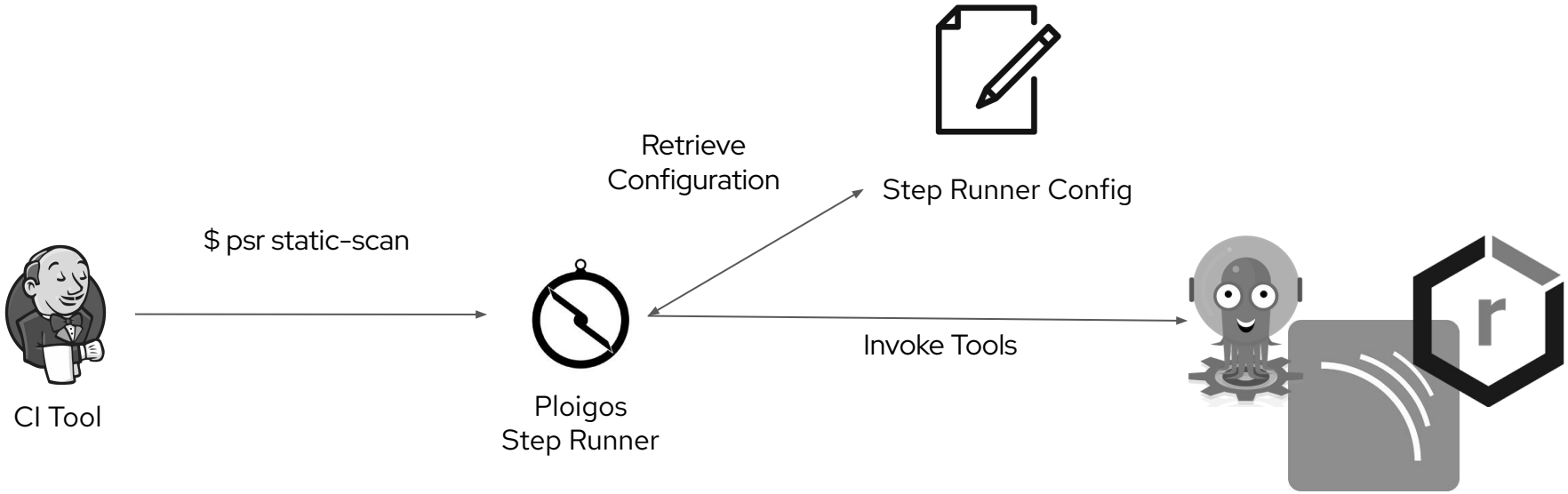
Solve software delivery with a software engineering approach.

Creating Golden Paths which are paved on-roads for an organization.

Truly mitigate risk and reduce total cost of ownership.

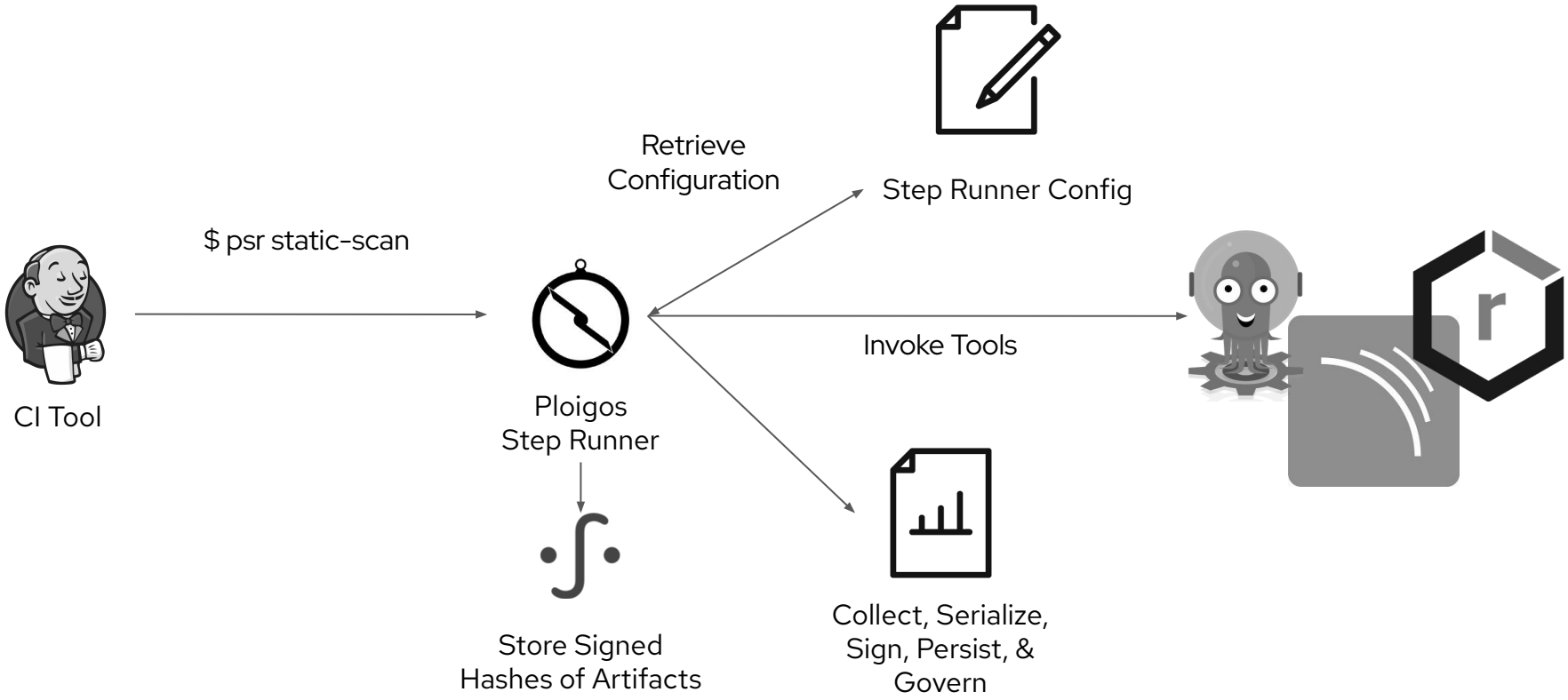
Ploigos Step Runner

Agnostic Implementation Of Tools



Ploigos Step Runner

Autonomous Governance




Do we get to mess with him now?
No. We wait until the worst possible moment.
AutoGov Demo
Rosdbb 2018

A Recommendation

Repurpose your Change Approval Board

Convert Your Change Approval Board Into A Modern Governance Platform Team

Paved Paths as Internal Products

The Modern Governance Platform Team

On Road

- Automate Governance
- Investment To Automate Occurs Upfront
- Canonical Implementations (80/20)

Off Road

- Manual Evaluation
- Costs Incurred For Each CAB session
- Appropriate For Some Situations

Not Matter Road Traveled

Apply The Same Governance

Modernize Your Governance With Autonomous Governance

No Questions
Just Conversations

Bill Bensing
Managing Architect - Red Hat

linkedin.com/in/billbensing

twitter.com/BillBensing