We're Sorry, Love DevOps

Bill Bensing | Co-author | Investments Unlimited

The Beyonce Rule
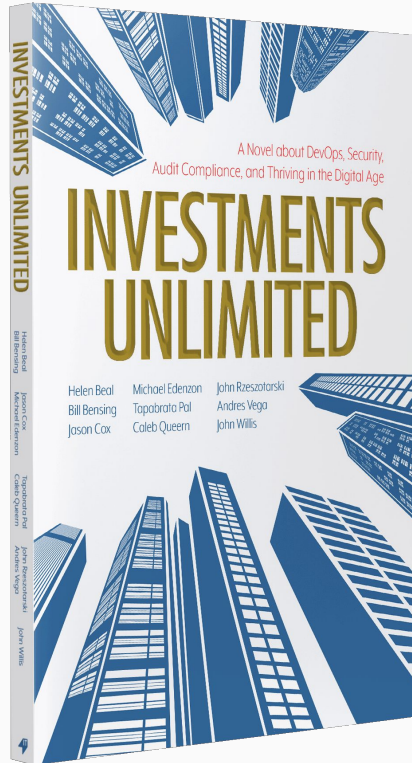
If You Like It , Then You Should Tweet On It

@BillBensing

"CI/CD was yesterday. We need a word to describe the next phase of DevOps. Modern Governance reminds us that software delivery must include everyone. It should be autonomous, at an industrial scale."

Bill Bensing
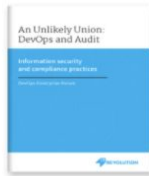@Bill_Bensing | www.billbensing.com

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

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

Pre Order Now!

AN UNLIKELY UNION: DEVOPS AND AUDIT
October 1, 2015

2015   2018   2019

DEVOPS AUTOMATED GOVERNANCE REFERENCE ARCHITECTURE
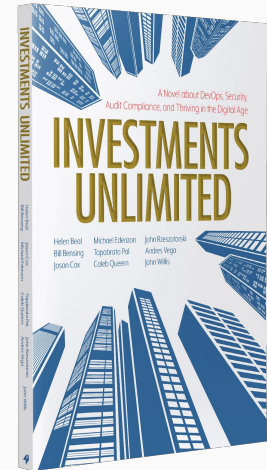September 17, 2019

DEAR AUDITOR
August 27, 2018

Agenda

What We Will Cover

3x Aspects of Modern Governance
- The Full Experience
- Object, Not Subjective
- Black, Green, Red

1 Unpopular Opinion, Maybe?

What is **Modern Governance**?

Modern **Governance** is thinking differently...

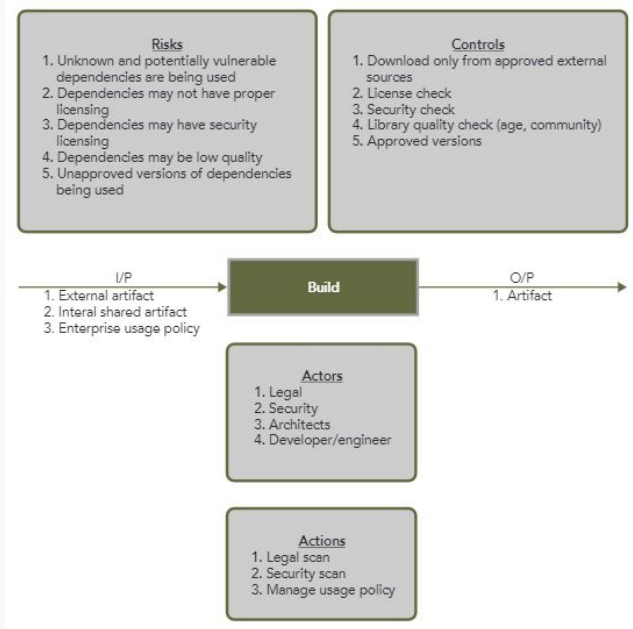Move from **implicit** security & compliance models…

To **explicit** security & compliance models

The Full Experience

Key Aspect #1

Beyond Dev & Ops, Everyone Must Be included

#1 - The Full Experience

Risks
1. Unknown and potentially vulnerable dependencies are being used
2. Dependencies may not have proper licensing
3. Dependencies may have security licensing
4. Dependencies may be low quality
5. Unapproved versions of dependencies being used

Controls
1. Download only from approved external sources
2. License check
3. Security check
4. Library quality check (age, community)
5. Approved versions

I/P
1. External artifact
2. Interal shared artifact
3. Enterprise usage policy

Build

O/P
1. Artifact

Actors
1. Legal
2. Security
3. Architects
4. Developer/engineer

Actions
1. Legal scan
2. Security scan
3. Manage usage policy

What Are Your IORCAAs?

- Input
- Output
- Risk
- Controls
- Actors
- Actions

#1 - The Full Experience

Two Types of Toil

Audit

Delivery

Objective
Not Subjective

Key Aspect #2

Governance Contract,
Automate Execution

#2 - Objective, Not Subjective

Creating a Governance Contract is Key to Externalized Policy
Evidence & Attestation - How to Codify Policy, Security, & Compliance

```
----------------------------------------
 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:    {}
```

#2 - Objective, Not Subjective
Externalize Governance - Audit Against Governance Contract
Policy Enforcement Point - How to Codify Policy, Security, & Compliance

```
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
```

```
▼ 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:         {}
```

Black, Red, Green

Key Aspect #3

Observability
What's Good,
What's Bad,
What's Unknown?

#3 - Red, Green, Black

Green

#3 - Red, Green, Black

Red

Black

Black -> **Red** -> **Green**

Want An Opinion?

Maybe Unpopular?

Repurpose You CAB

Repurpose Your CAB

Make It Work For You, Not Against You

Convert Change Approval Board Into **The Modern Governance Platform Team**

Repurpose Your Cab
Automated Governance
An On-Road For Modern Governance

On Road

- Automate Governance
- Investment to automate happens upfront
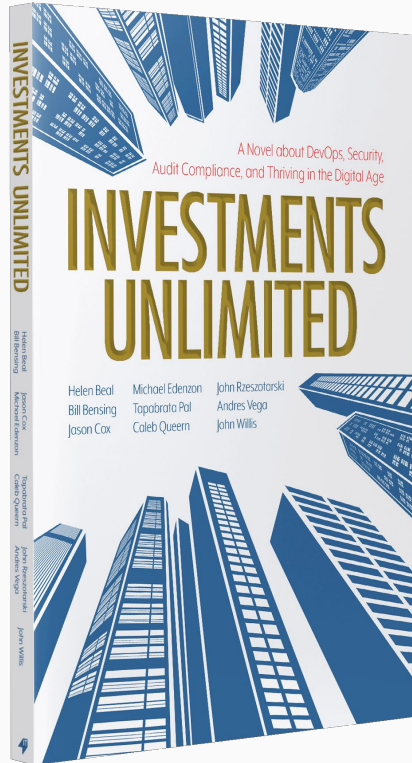- Canonical Implementations (80/20)

Off Road

- Manual Evaluation
- Costs incurred for each CAB session
- Appropriate for some situations

No Matter The Road Traveled…

Apply The Same Governance

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

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