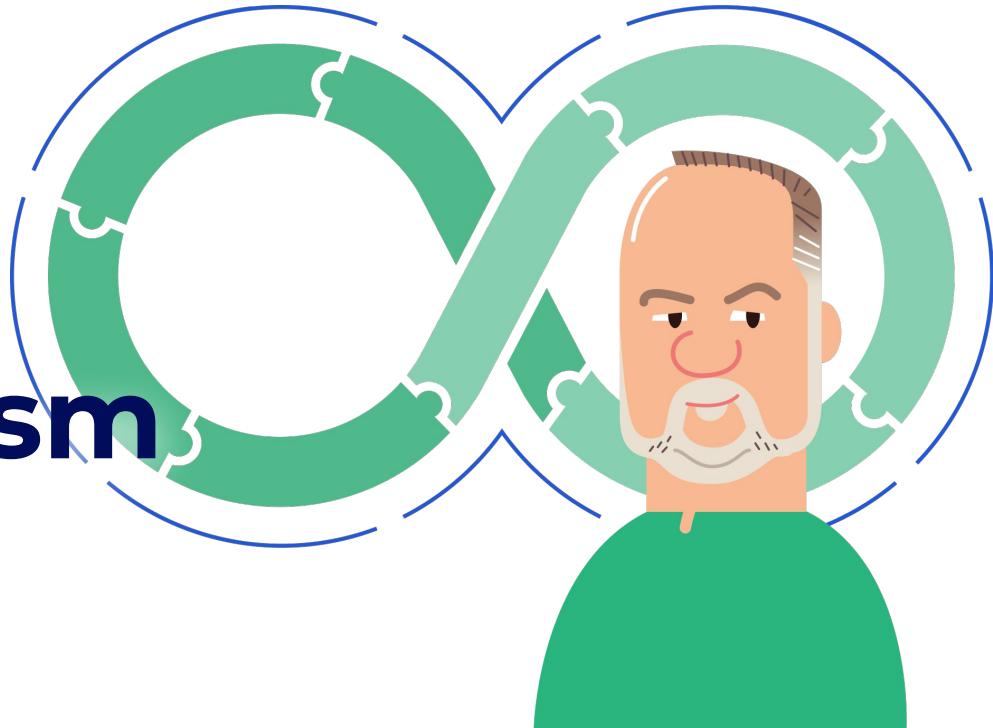


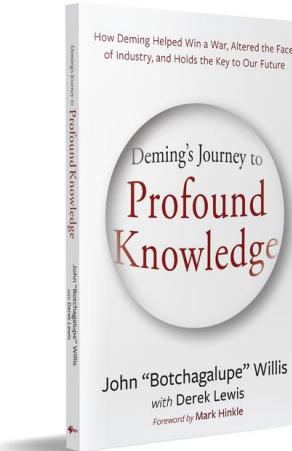
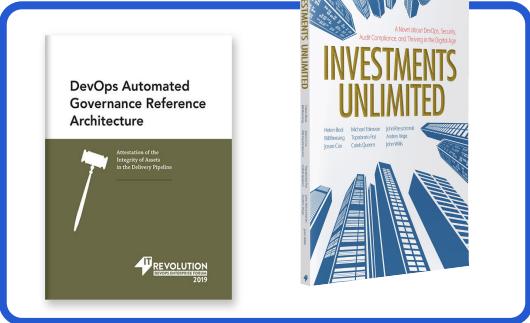
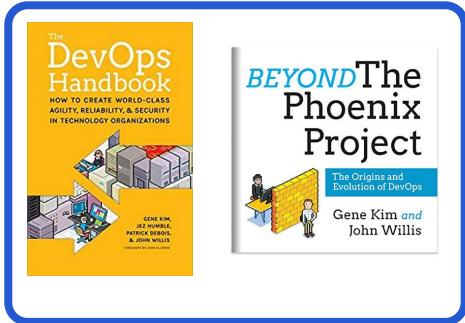


DevSecOps Operationalism

John Willis  @botchagalupe



@botchagalupe





Deliver to John
Auburn 36830

Books ▾

Search Amazon



EN ▾

All Amazon Health ▾ Prime Video Best Sellers Buy Again Health & Household Coupons Amazon Basics Amazon Home Pet Supplies Beauty & Personal Care

Books Kindle Rewards Advanced Search New Releases Best Sellers & More Amazon Book Clubs Children's Books Textbooks Textbook Rentals Best Books of the Month

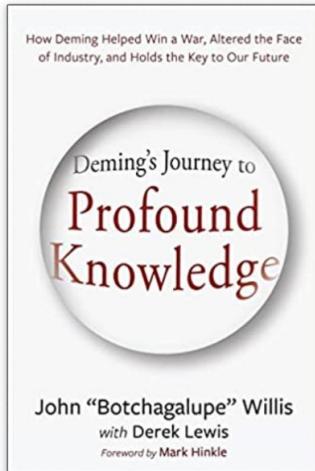


Are you a College Student?
Try Prime Student for 6 months for \$0.

Learn more+



Books > Biographies & Memoirs > Professionals & Academics



See this image

A thoroughly entertaining and educational look at Deming, a man whose insights are fundamental to modern software development. The book includes delightful stories of those around Deming who influenced his work and helped create the foundation for agile and DevOps"

Jim Whitehurst - President IBM, and CEO of RedHat

we work today, but also how we can continue to succeed in the future.

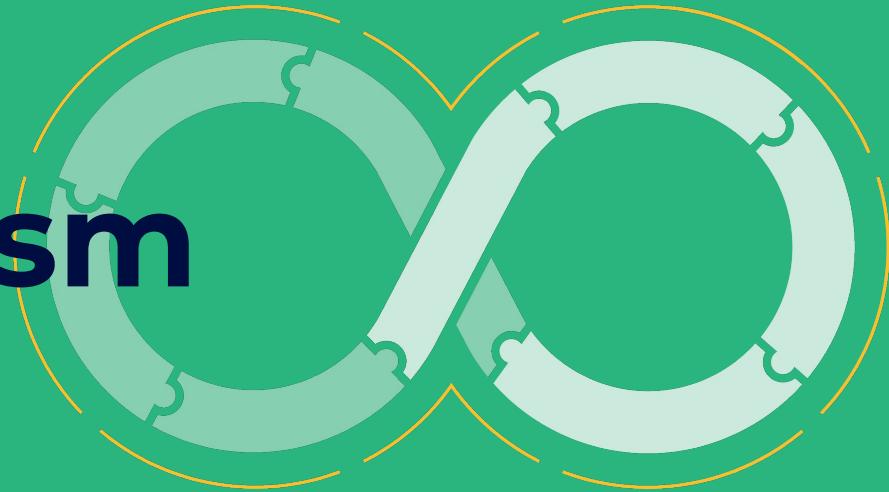
Part business history, part biography, part journey into deep business sense, bestselling author John Willis captures the full picture

John "Botchagalue" Willis is a best-selling author, speaker, and consultant. He has written several books on management and leadership, including "The Toyota Way to Leadership" and "The Toyota Way to Quality". He has also worked with companies like Toyota, GE, and IBM, and has spoken at numerous conferences and events around the world.

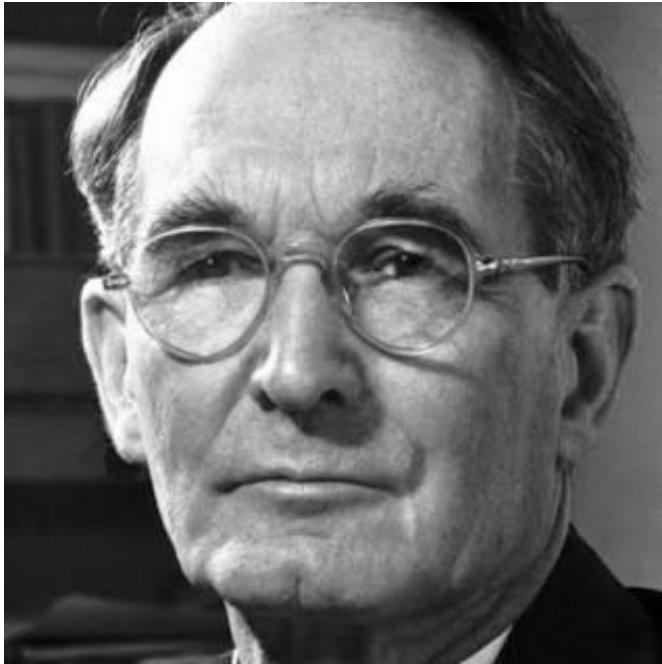
▼ Read more

Report incorrect product information.

Operationalism



Operationalism

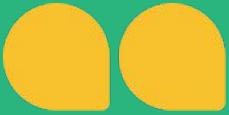


"We do not know the meaning of a concept unless we have a method of measurement for it."

The Logic of Modern Physics 1927
- Percy Williams Bridgman

Percy Williams Bridgman

- Harvard physics professor
- Won a Nobel prize for physics of high pressures
- Synthetic diamonds (gauges kept breaking)
- Albert Einstein's special theory of relativity, where measurements used in time and space were different than conventional means of measurement.
- Length, Square Footage, Light Years

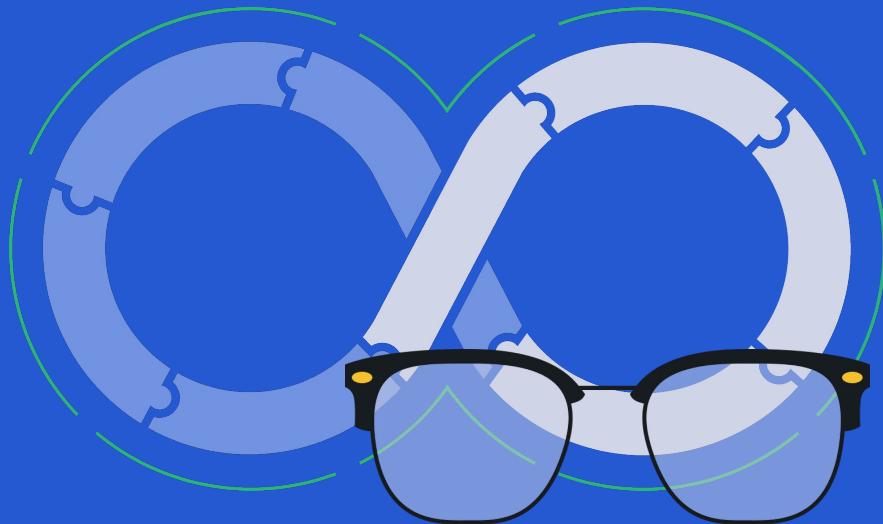


To find the length of an object, we have to perform certain physical operations. The concept of length is therefore fixed when the operations by which length is measured are fixed. The concept of length involves the set of operations by which length is determined.



Percy Williams Bridgman

Dr. Edwards Deming



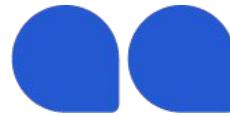
Deming's Influence

- Henri Fayol's 1916 General and Industrial Management
- Percy Bridgeman's 1927 The Logic of Modern Physics
- Clarence Irving Lewis' 1929, Mind and the World-Order
- Walter Shewhart's 1924 Statistical Process Control

Deming Management Philosophy

- Operational Definitions
- Analytical Statistics
- Fourteen Points for Management
- System of Profound Knowledge

Operational Definition



An operational definition is a procedure agreed upon for translation of a concept into measurement of some kind

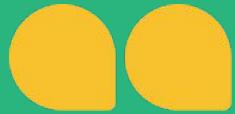


Count the Number of Horses, Elephants, and Pigs?



Count the Number People in a Restaurant?





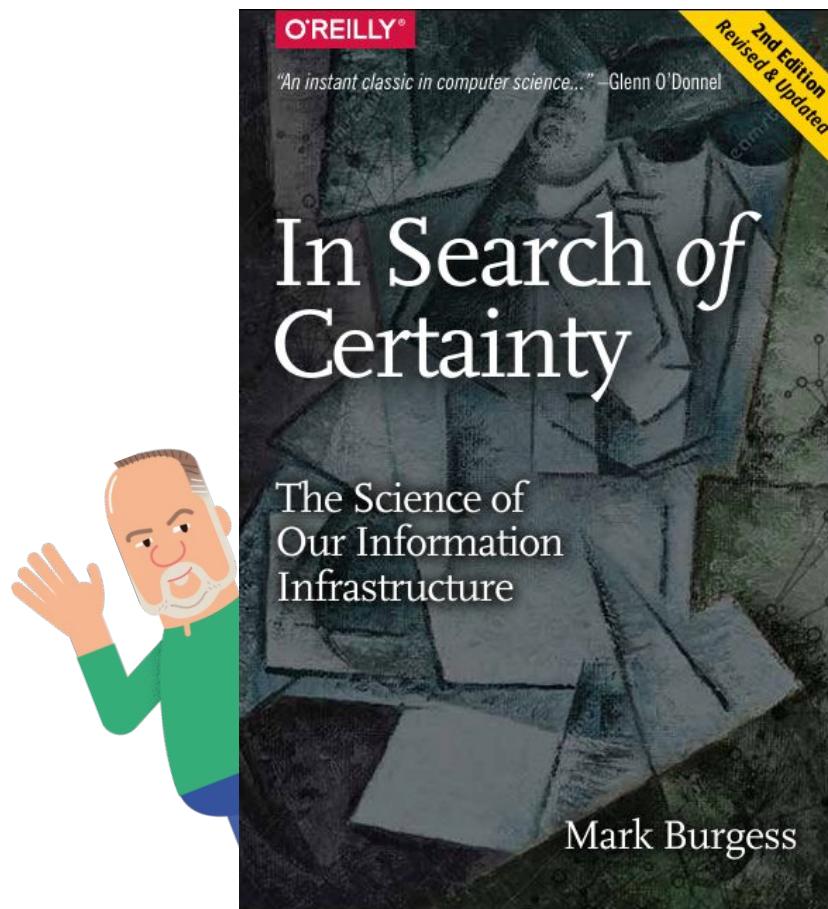
There is no true value of any characteristic, state, or condition that is defined in terms of measurement or observation



The New Economics
Deming, W. Edwards

In Complex Systems, Definitions Matter

- Time
- Root
- Zero
- Hermetic
- Service



What is Lead Time, or Time to Restore?

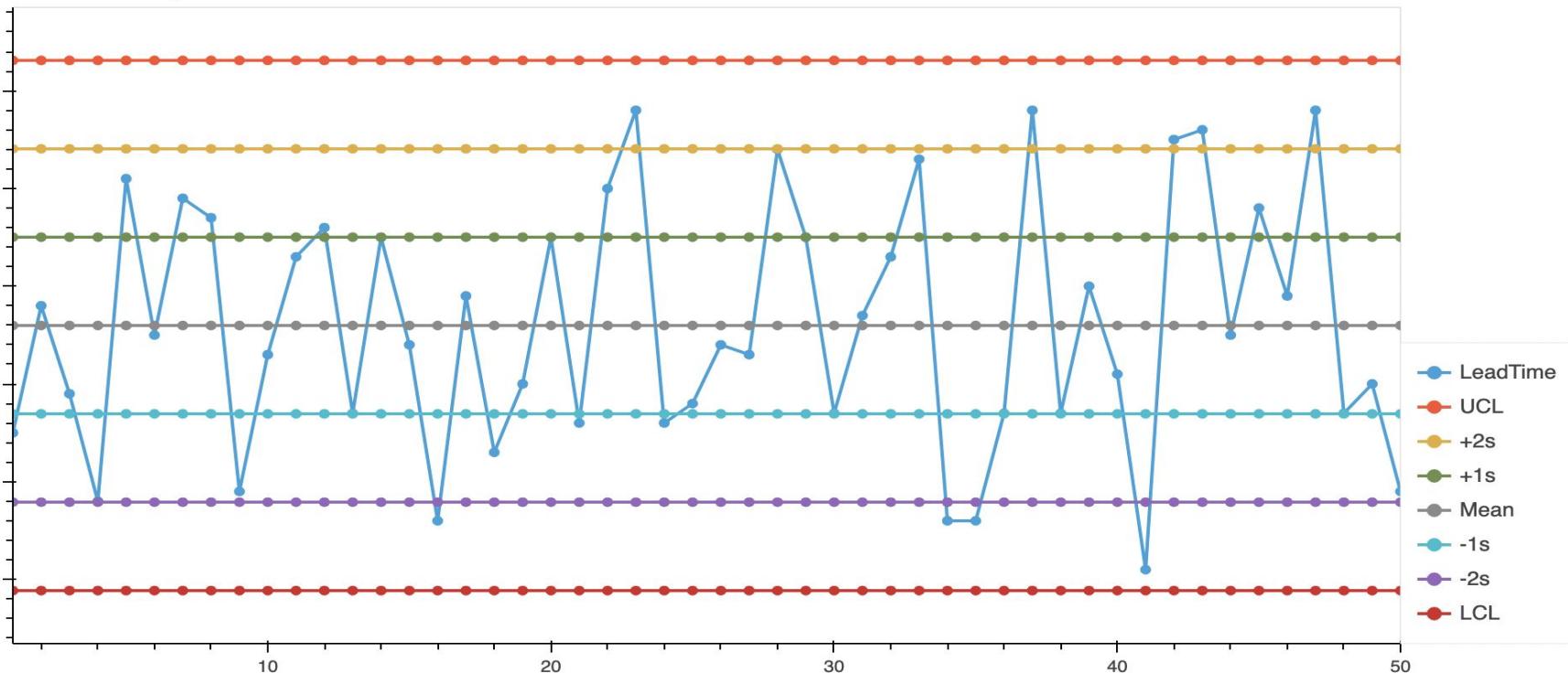
- **Criteria:** Why are we asking? What is good or bad, or standard? Are all the teams in an org aligned on the same operational definition? Industry?
- **Test:** What's the measurement? Delivery or deployment, branch, master branch or pull request? Dark launch, feature flag. Mean, mode, standard deviation?
- **Decision:** Did it meet the criteria? What action do we take? Are we continuously improving?

Dr. Donald Wheeler

- **Criteria:** A measurement system “is consistent if and only if repeated measurements of the same items result in a sequence of values that are homogeneous.”
- **Test:** An individuals control chart is used to determine if the values are homogeneous, i.e., in statistical control.
- **Decision:** The determination as to whether the test results show that the characteristic meets the criteria. The measurement process is inconsistent if there are points beyond the control limits or there are patterns present.

Analytical Statistics (Variation - No True Value)

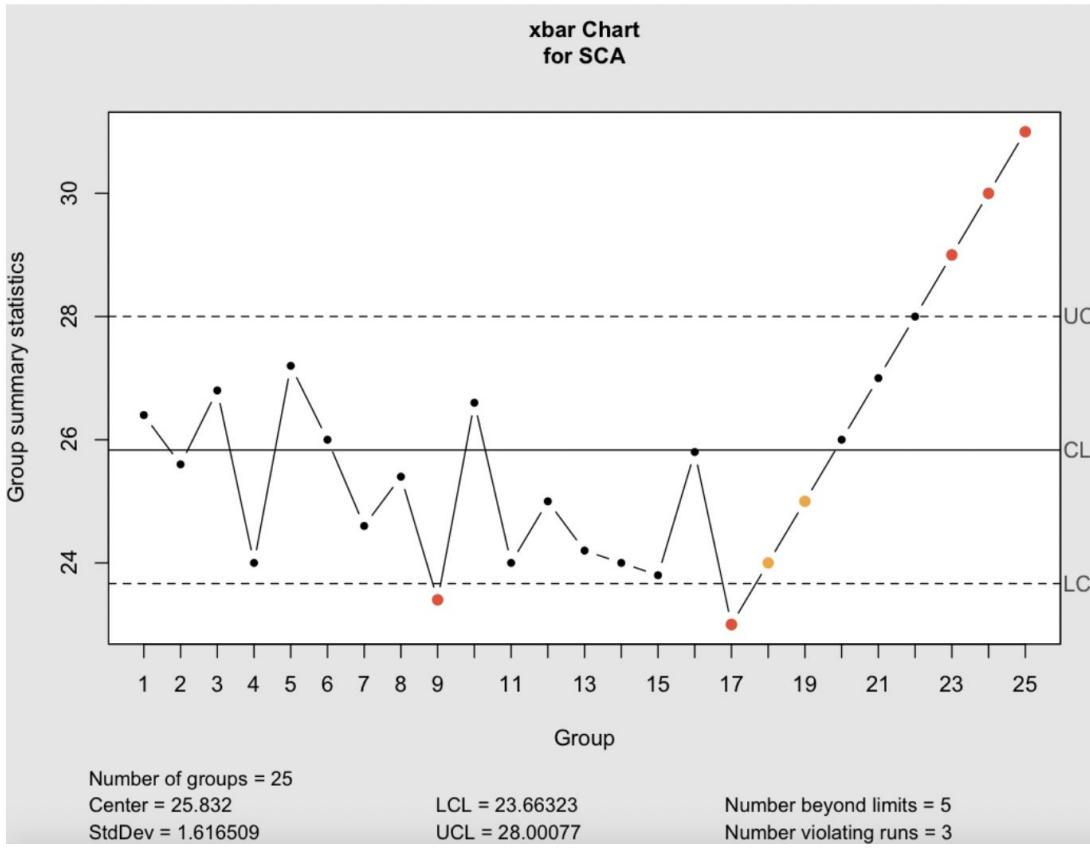
Lead Time by Service



Operationalization & Risk



Container Scan Vulnerability Fails



Complex Industry Risk Architectures



**SOC 2
TYPE II
CERTIFIED**



NIST
Security Guidelines
800-204



MITRE
ATT&CK™



FDA 21 CFR Part 11 Pharmaceutical Industry



General Principles of Software Validation; Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

This document supersedes the draft document, "General Principles of Software Validation, Version 1.1, dated June 9, 1997.



U.S. Department Of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Operationalization and FDA

- Specification
- Verification
- Validation

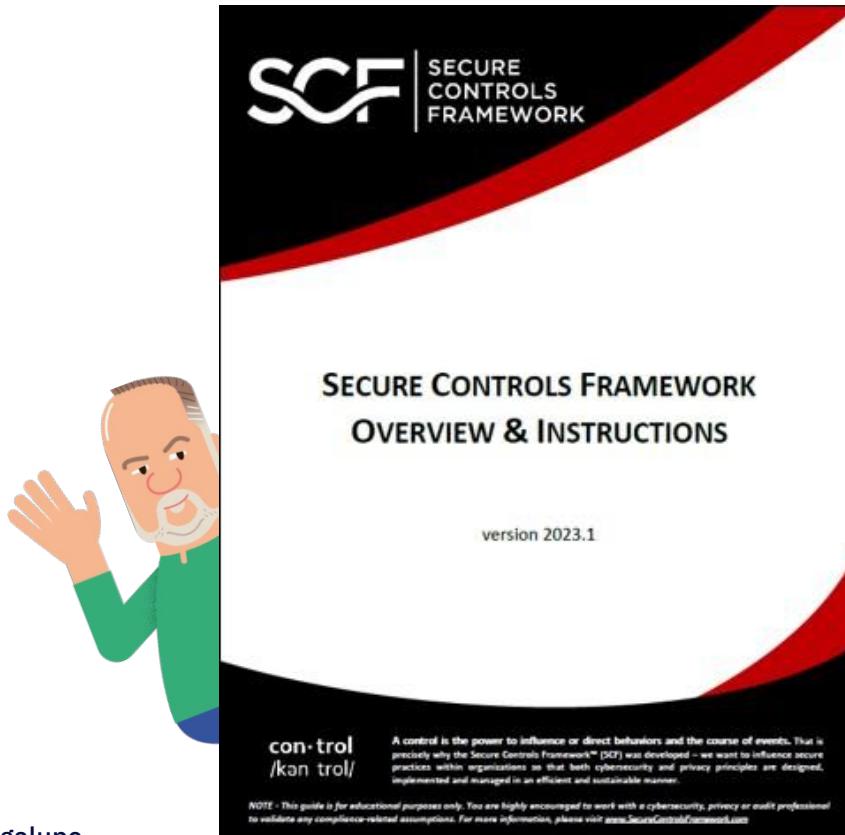
Operationalization and FDA

- Specification → Criteria
- Verification → Test
- Validation → Decision

Operationalization and FDA

- Specification → Criteria → Plan
- Verification → Test → Do
- Validation → Decision → Study/Act

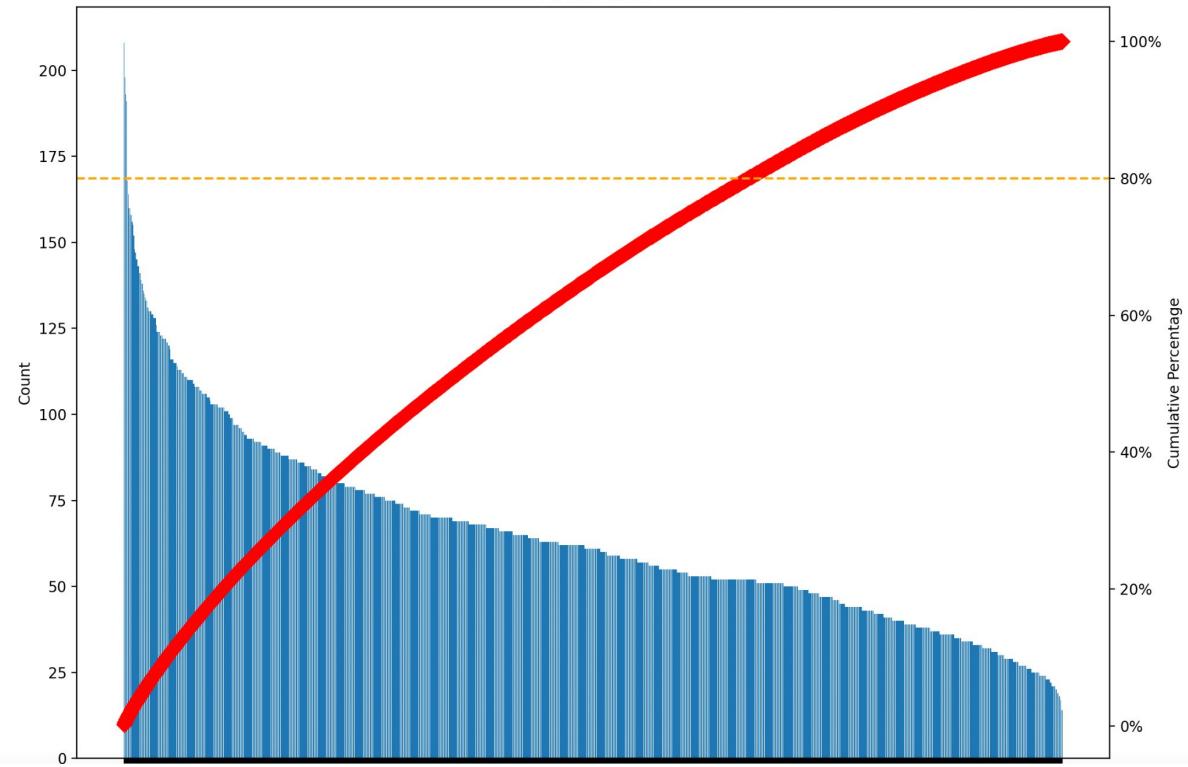
Secure Controls Framework



John Willis  @botchagalupe

Pareto - Secure Controls Framework (SCF)

1169 Risk Controls
285 Control Frameworks



Secure Controls Framework (SCF)

Sorted Risk Controls by Framework						
	Control	Count	Percentage	SCF Domain	Control Weight	Grouping
1	CPL-01	208	72.98%	Compliance	10	Identify
2	SEA-01	198	69.47%	Secure Engineering & Architecture	10	Protect
3	DCH-01	193	67.72%	Data Classification & Handling	10	Protect
4	CPL-02	191	67.02%	Compliance	10	Detect
5	IAC-01	168	58.95%	Identification & Authentication	10	Protect
6	RSK-01	164	57.54%	Risk Management	10	Identify
7	GOV-01	158	55.44%	Cybersecurity & Privacy Governance	10	Identify
8	TPM-01	156	54.74%	Third-Party Management	10	Identify
9	CPL-03	155	54.39%	Compliance	10	Detect
10	RSK-04	148	51.93%	Risk Management	10	Identify
11	IRO-02	147	51.58%	Incident Response	10	Respond
12	NET-01	143	50.18%	Network Security	10	Protect
13	TDA-01	143	50.18%	Technology Development & Acquisition	10	Protect
14	VPM-05	141	49.47%	Vulnerability & Patch Management	10	Protect
15	HRS-01	139	48.77%	Human Resources Security	10	Protect
16	-PES 3	138	48.42%	Physical & Environmental Security	10	Protect
17	MON-01	136	47.72%	Continuous Monitoring	10	Detect
18	TPM-05	135	47.37%	Third-Party Management	10	Identify
19	CFG-02	134	47.02%	Configuration Management	10	Protect
20	BCD-01	133	46.67%	Business Continuity & Disaster Recovery	10	Recover

Secure Controls Framework

GUIDELINE

[provides additional, recommended guidance]

PROCEDURE

[establishes proper steps to take]

STANDARD

[assigns quantifiable requirements]

CONTROL OBJECTIVE

[identifies desired conditions to be met]

POLICY

[sets high-level expectations]



SCF as Code

- Standards/Guidelines → Criteria
- Procedures → Test
- Control Objectives/Policy → Decision

NIST Documentation as Zero Day



NIST Special Publication 800-204C

Implementation of DevSecOps for a Microservices-based Application with Service Mesh

Ramaswamy Chandramouli

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-204C>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



1

2

3

4

5

6

7

8

9

10

11

12

13

NIST Special Publication
NIST SP 800-207A.ipd

A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments

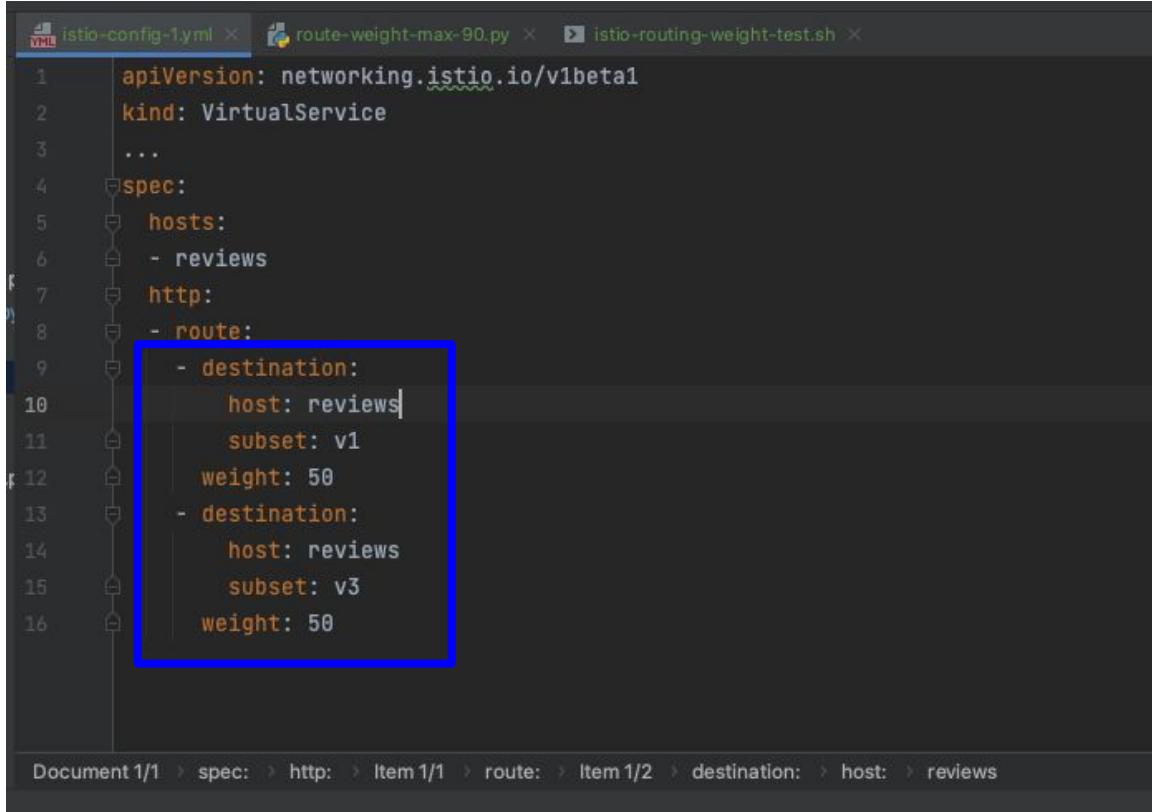
Initial Public Draft

Ramaswamy Chandramouli
Zack Butcher

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.800-207A.ipd>

NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

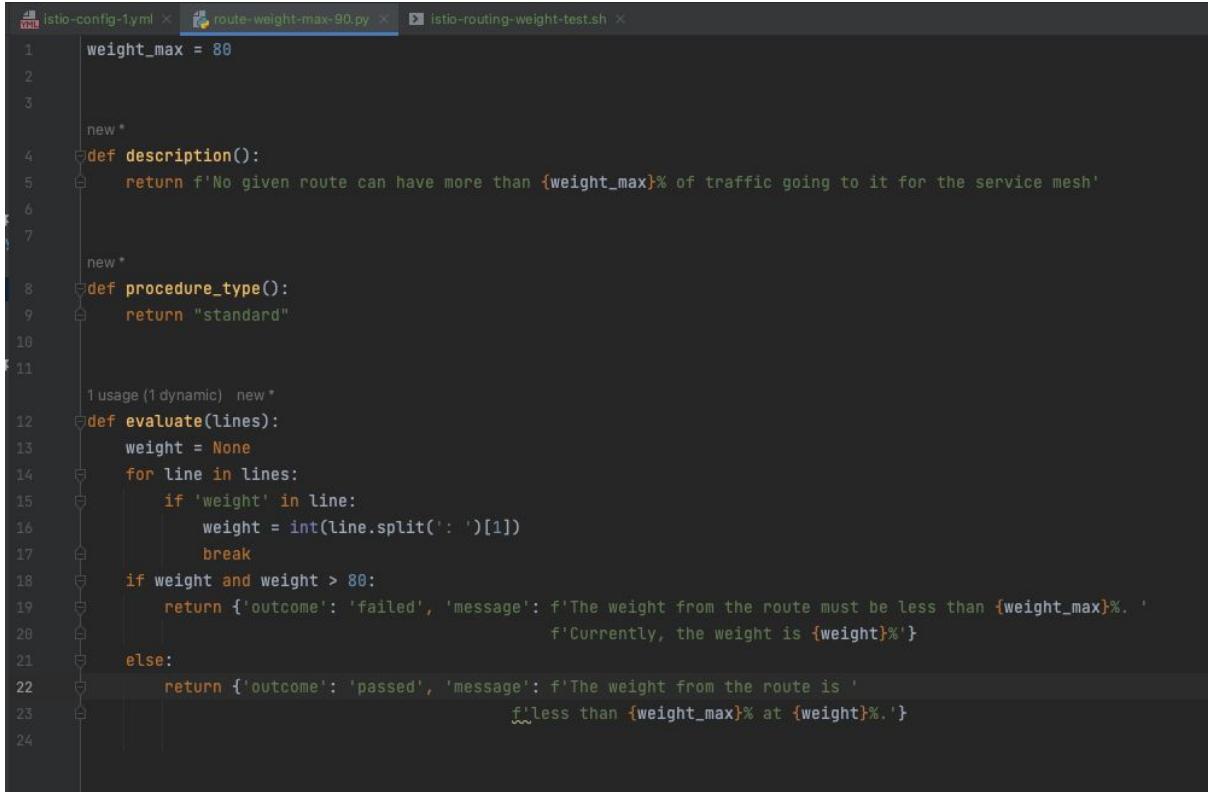
ISTIO Traffic Shaping (Standard/Criteria)



```
YAML istio-config-1.yaml × route-weight-max-90.py × istio-routing-weight-test.sh ×
1  apiVersion: networking.istio.io/v1beta1
2  kind: VirtualService
3  ...
4  spec:
5    hosts:
6      - reviews
7      http:
8        - route:
9          - destination:
10            host: reviews
11            subset: v1
12            weight: 50
13          - destination:
14            host: reviews
15            subset: v3
16            weight: 50
Document 1/1 > spec: > http: > Item 1/1 > route: > Item 1/2 > destination: > host: > reviews
```

The screenshot shows a code editor with three tabs: 'istio-config-1.yaml' (selected), 'route-weight-max-90.py', and 'istio-routing-weight-test.sh'. The YAML file contains a 'VirtualService' configuration. A blue box highlights the 'route' section under the 'http' block, which defines two routes to the 'reviews' host. Each route has a 'subset' (v1 or v3) and a 'weight' (50). The 'subset' field is highlighted in orange.

ISTIO Traffic Management (Control/Test)



```
istio-config-1.yml × route-weight-max-90.py × istio-routing-weight-test.sh ×
1 weight_max = 80
2
3
4     new *
5     def description():
6         return f'No given route can have more than {weight_max}% of traffic going to it for the service mesh'
7
8     new *
9     def procedure_type():
10        return "standard"
11
12    1 usage (1 dynamic)  new *
13    def evaluate(lines):
14        weight = None
15        for line in lines:
16            if 'weight' in line:
17                weight = int(line.split(':')[1][1])
18                break
19        if weight and weight > 80:
20            return {'outcome': 'failed', 'message': f'The weight from the route must be less than {weight_max}%. '
21                                            f'Currently, the weight is {weight}%'}
22        else:
23            return {'outcome': 'passed', 'message': f'The weight from the route is '
24                                            f'less than {weight_max}% at {weight}%. '}
```

ISTIO Traffic Management (Policy/Decision)

```
Target File: istio-config-1.yml
```

```
-----  
Total: 1  
Exec: 1  
Pass: 1  
Fail: 0  
-----
```

```
Standards
```

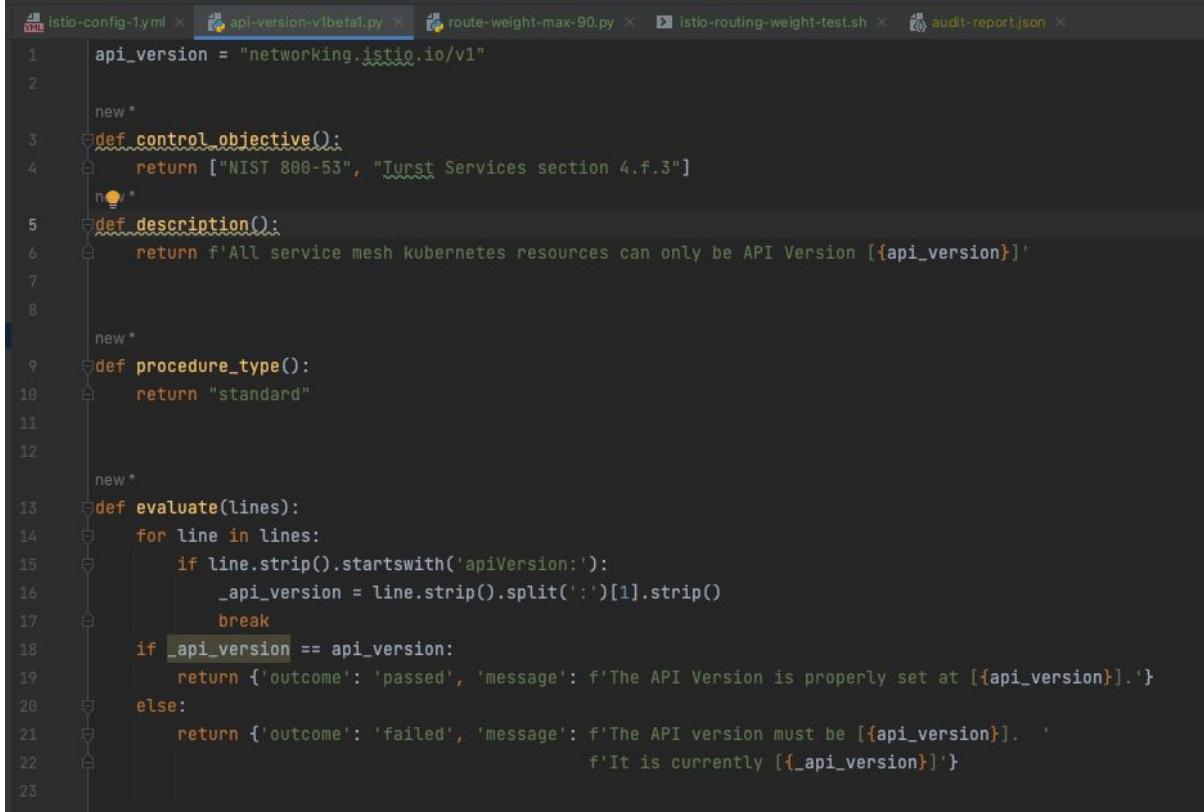
```
Outcome Message
```

```
No given route can have more than 80% of traffic going to it for the service mesh pass The weight from the route is less than 80% at 50%.
```

```
Guidelines
```

```
Outcome Message
```

ISTIO Traffic Management (API Version)



```
istio-config-1.yml × api-version-v1beta1.py × route-weight-max-90.py × istio-routing-weight-test.sh × audit-report.json ×
1     api_version = "networking.istio.io/v1"
2
3     new*
4         def control_objective():
5             return ["NIST 800-53", "Tiered Services section 4.f.3"]
6             n*/*
7         def description():
8             return f'All service mesh kubernetes resources can only be API Version [{api_version}]'
9
10        new*
11            def procedure_type():
12                return "standard"
13
14        new*
15            def evaluate(lines):
16                for line in lines:
17                    if line.strip().startswith('apiVersion:'):
18                        _api_version = line.strip().split(':')[1].strip()
19                        break
20                if _api_version == api_version:
21                    return {'outcome': 'passed', 'message': f'The API Version is properly set at [{api_version}].'}
22                else:
23                    return {'outcome': 'failed', 'message': f'The API version must be [{api_version}]. '
24                                         f'It is currently [{_api_version}]'}
```

ISTIO Traffic Management (Policy/Decision)

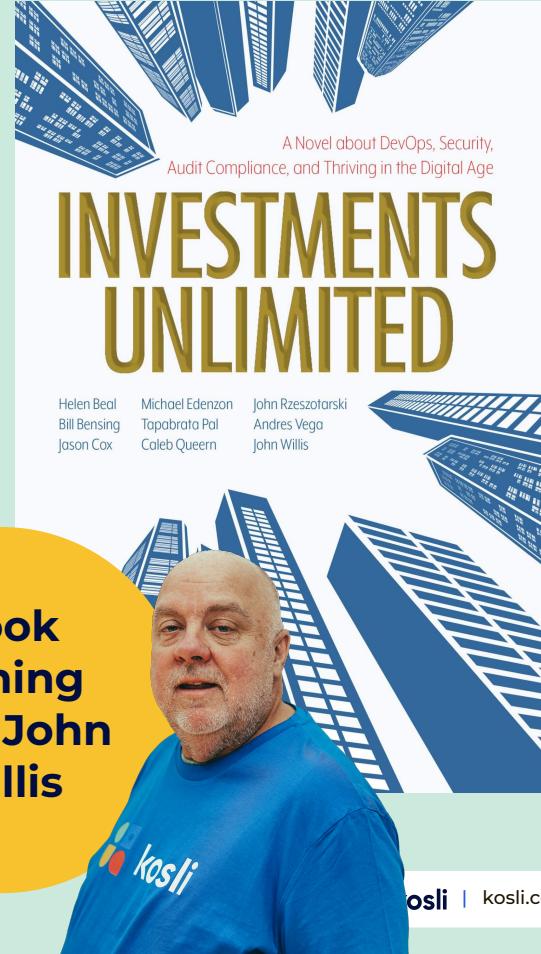
```
--  
Target File: istio-config-1.yml  
-----  
Total: 2  
Exec: 2  
Pass: 1  
Fail: 1  
-----  
  
Standards          Outcome    Message  
-----  
All service mesh kubernetes resources can only be API Version [networking.istio.io/v1]  fail  The API version must be [networking.istio.io/v1].  It is currently [networking.istio.io/v1beta1]  
No given route can have more than 80% of traffic going to it for the service mesh  pass  The weight from the route is less than 80% at 50%.  
  
Guidelines          Outcome    Message  
-----
```

**Grab a FREE copy
of Investments
Unlimited at the
Kosli stand**

**(Book signing after the
Lightning Talks 5:45pm)**

John Willis  @botchagalupe

**Book
signing
with John
Willis**



 kosli | kosli.com

Download a **FREE** White paper

SLSA 4 - 18 Controls
DAG - 51 Controls

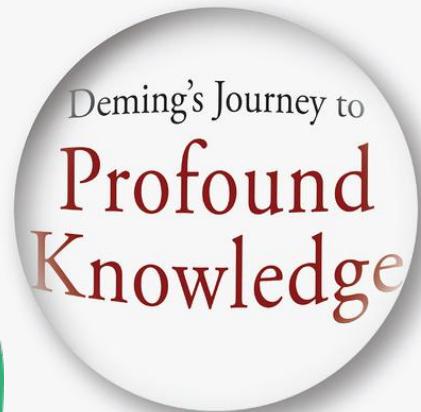


Find out more at...

- profound-deming.com
- linkedin.com/in/johnwillisatlanta/
- @botchagalupe
- john.willis@kosli.com
- DevOps and Operationalism
 - <https://bit.ly/3ymHVmp>
- Enumerated and Analytical Statistics
 - <https://bit.ly/3ZRH4WI>



How Deming Helped Win a War, Altered the Face of Industry, and Holds the Key to Our Future



John "Botchagalupe" Willis
with Derek Lewis
Foreword by Mark Hinkle