Policy as Code 2.0

Doing It The Right Way

I Need Your Help

Can I shoulder surf & research how you do “Policy”?

I Can Help You

Share these ideas with your company.

The Beyonce Rule

“If you like it then you should tweet on it.”

@BillBensing

The Beyonce Rule

"If you like it then you should ~~tweet on~~ LinkedIn it."

@BillBensing

The Bottom Line Up Front

Policy as Code

An unfortunate & misleading colloquialism

In Common?

What to to following words have in common?

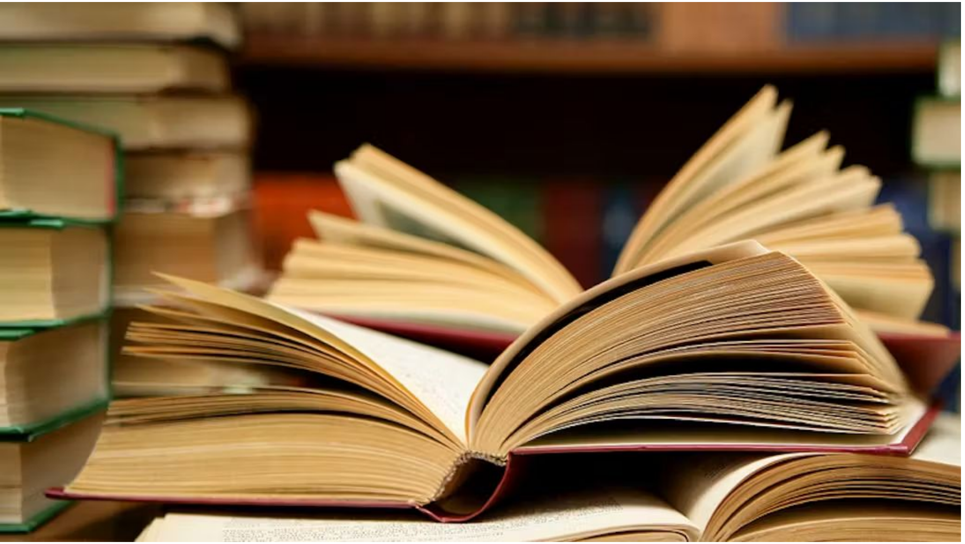
- Text
- Friend
- Viral
- Cloud
- Stream

In Common?

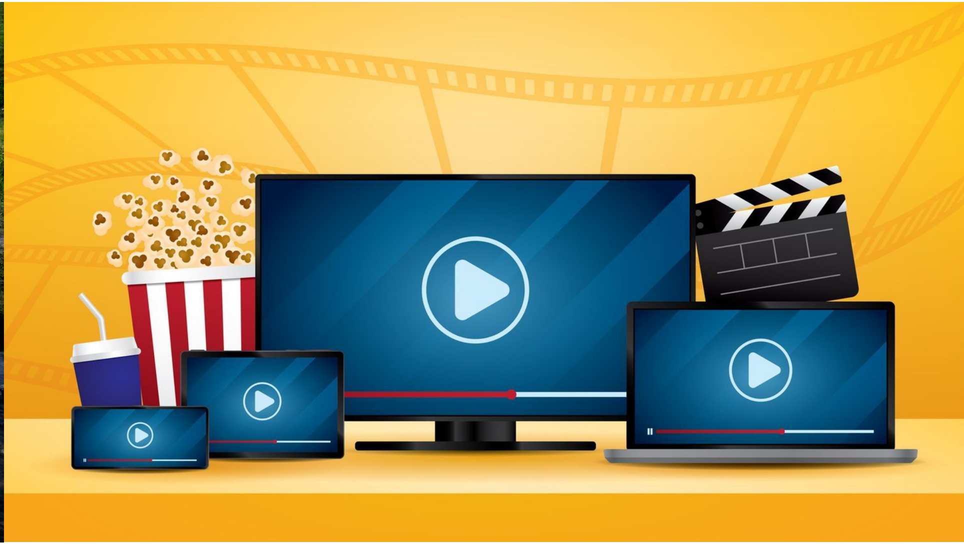
They all mean something different today than they meant 20 years ago

- ➔ Text
- ➔ Friend
- ➔ Viral
- ➔ Cloud
- ➔ Stream

Text

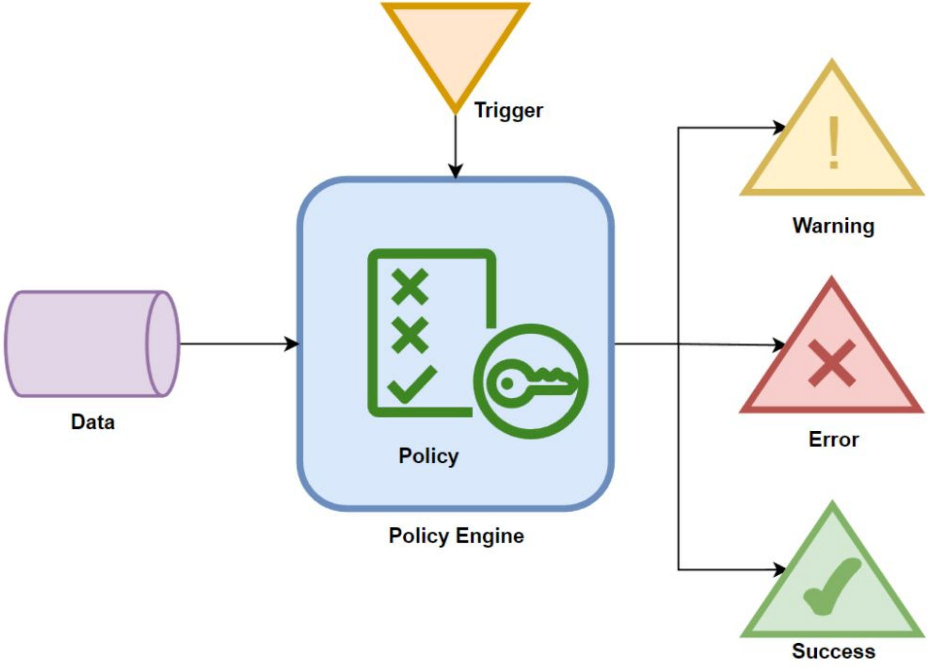


Streams



Bad Policy

No clear & direct link between high-level intentions and low-level activities.

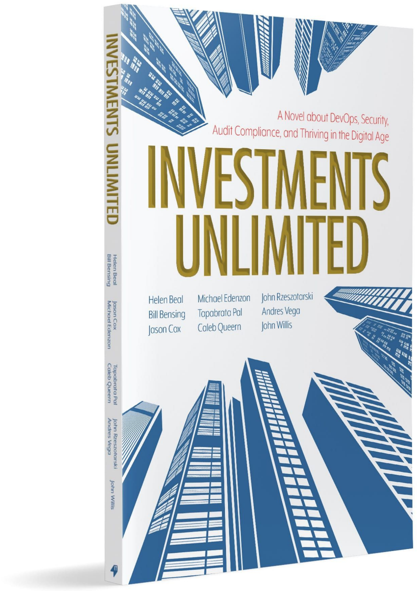


Good Policy

Irrefutable clear & direct link between high-level intent and lower-level activities.

The BLUF

- ➔ Policy as Code is misleading.
- ➔ You cannot codify Policy.
- ➔ Codify the “Am I doing what I’m supposed to do?” is the goal.



The Agenda

Policy as Code 2.0 - Strategy

- The Problem Diagnosis
- Guiding Principles
- Coherent Actions

What Is Policy?

A - Is This Policy?

As Chief Information Officer, I wish to express our organization's steadfast commitment to the privacy and availability of customer data. Our customers entrust us with invaluable information, and it is our ethical and operational obligation to safeguard this data diligently.

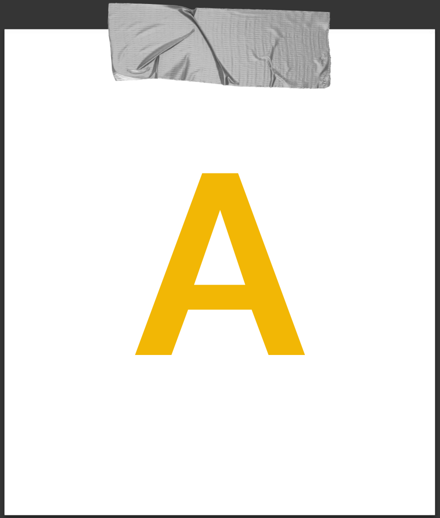
On Data Privacy:
We are committed to implementing the strongest measures to protect customer data from unauthorized access, disclosure, or alteration. We will adhere to all applicable laws, regulations, and industry standards to ensure the highest level of data privacy.

On Data Availability:
We will maintain a secure and reliable infrastructure that allows customers to access their data when they need it, without compromising its safety.

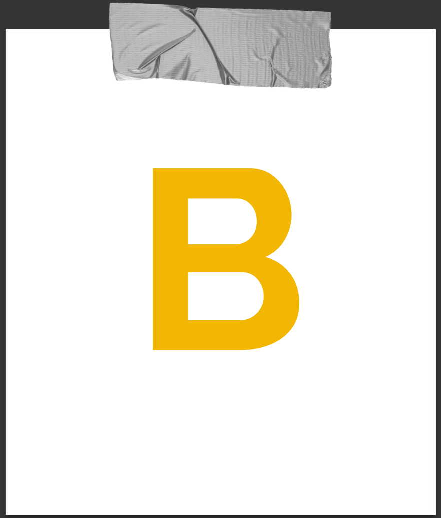
B - Is This Policy?

```
deny[reason] {
    input.spec.resourceAttributes.namespace == "kube-system"
    reason := "OPA: denied access to namespace kube-system"
    }
deny[reason] {
    input.spec.resourceAttributes.namespace == "opa"
    required_groups := {"system:authenticated", "devops"}
    provided_groups := {group | group := input.spec[groups][_]}
    count(required_groups & provided_groups) != count(required_groups)
    reason := sprintf("OPA: provided groups (%v) does not include all required groups: (%v)", [
        concat(", ", provided_groups),
        concat(", ", required_groups),
    ])
}
decision = {...
```

Which One Is A Policy?



A



B

Well…What Is Policy?

Secure Controls Framework

The Secure Controls Framework™ (SCF) focuses on internal controls. These are the cybersecurity & data privacy-related policies, standards, procedures, technologies and associated processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected. The concept is to address the broader People, Processes, Technology and Data (PPTD) that are what controls fundamentally exists to govern.

Why SCF?

Domain Driven Design

So…What is a Policy

Policies...

Are established by the organization’s corporate leadership and establishes “management’s intent” for cybersecurity and data protection requirements that are necessary to support the organization’s overall strategy and mission.

SCF - Integrated Controls Management - Pg. 12

Management's Intent?

A

B

A - Management's Intent

As Chief Information Officer, I wish to express our organization's steadfast commitment to the privacy and availability of customer data. Our customers entrust us with invaluable information, and it is our ethical and operational obligation to safeguard this data diligently.

On Data Privacy:
We are committed to implementing the strongest measures to protect customer data from unauthorized access, disclosure, or alteration. We will adhere to all applicable laws, regulations, and industry standards to ensure the highest level of data privacy.

On Data Availability:
We will maintain a secure and reliable infrastructure that allows customers to access their data when they need it, without compromising its safety.

What’s Wrong with B?

B - Low Level

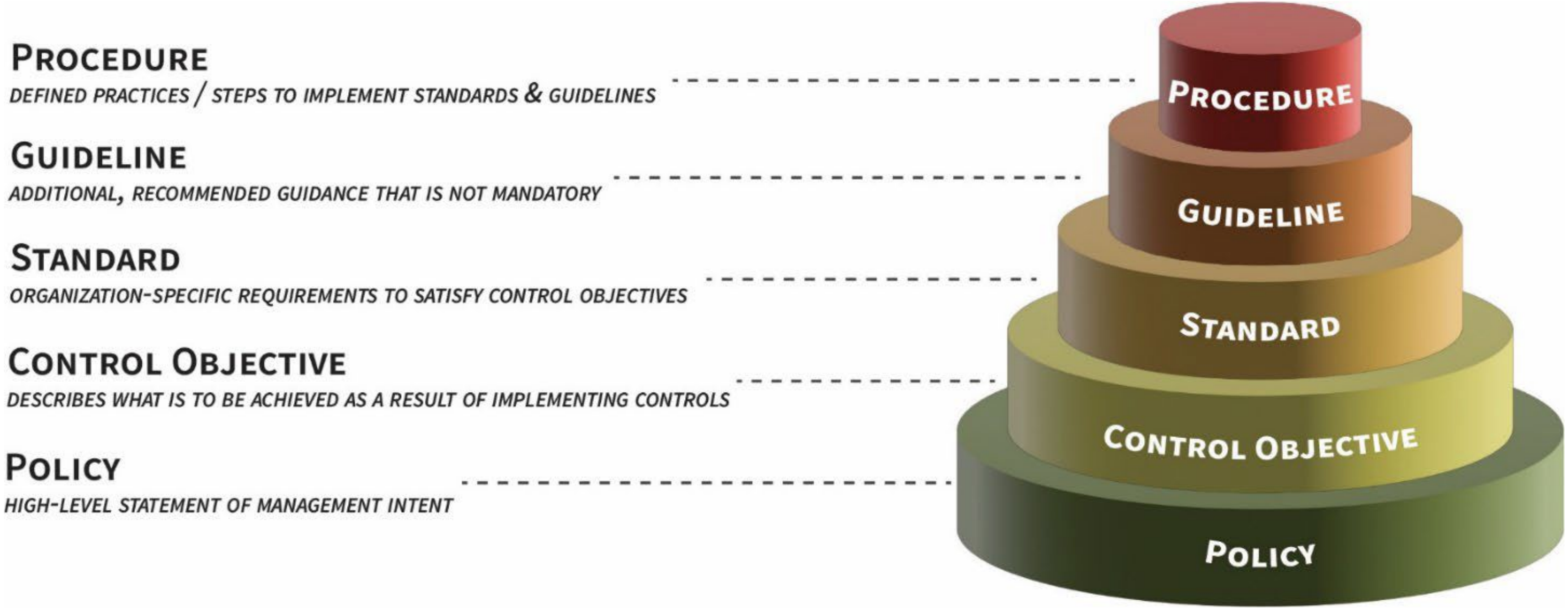
```
deny[reason] {
    input.spec.resourceAttributes.namespace == "kube-system"
    reason := "OPA: denied access to namespace kube-system"
    }
deny[reason] {
    input.spec.resourceAttributes.namespace == "opa"
    required_groups := {"system:authenticated", "devops"}
    provided_groups := {group | group := input.spec[groups][_]}
    count(required_groups & provided_groups) != count(required_groups)
    reason := sprintf("OPA: provided groups (%v) does not include all required groups: (%v)", [
        concat(", ", provided_groups),
        concat(", ", required_groups),
    ])
}
decision = {...
```

Procedure

Establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives;

SCF - Integrated Controls Management - Pg. 12

The Layer Cake



PROCEDURE
DEFINED PRACTICES / STEPS TO IMPLEMENT STANDARDS & GUIDELINES

GUIDELINE
ADDITIONAL, RECOMMENDED GUIDANCE THAT IS NOT MANDATORY

STANDARD
ORGANIZATION-SPECIFIC REQUIREMENTS TO SATISFY CONTROL OBJECTIVES

CONTROL OBJECTIVE
DESCRIBES WHAT IS TO BE ACHIEVED AS A RESULT OF IMPLEMENTING CONTROLS

POLICY
HIGH-LEVEL STATEMENT OF MANAGEMENT INTENT

SCF - Integrated Controls Management - Pg. 12

The Diagnosis

- Ties between high & low level are the “policy” issue
- Policy is high-level
- Policy as code is low-level
- You cannot codify Policy
- You can codify Procedures
- Policy as Code are Procedures with lipstick
- Policy as code fails to connect high to low level

How Do We Cure This?

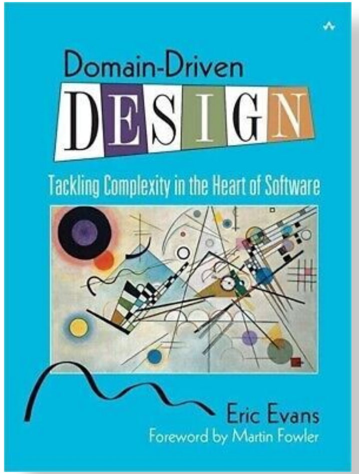
3 Guiding Principles

- → Domain Driven Design
- → Control-Centric View
- → Irrefutable Link between high & low

Domain Driven Design

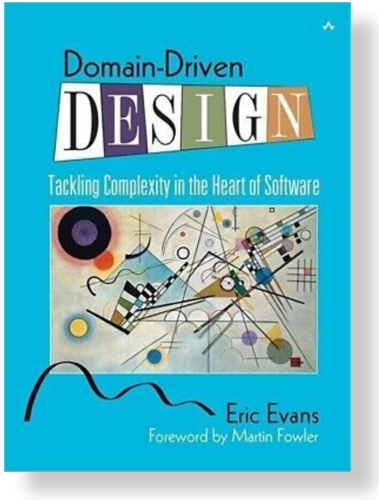
Domain Driven Design

A software design approach, focusing on modeling software to match a domain according to input from that domain experts.


Domain-Driven
DESIGN
Tackling Complexity in the Heart of Software
Eric Evans
Foreword by Martin Fowler

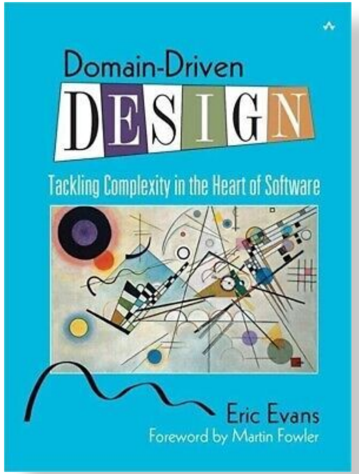
Domain Driven Design

Software designed around how
domain experts think, talks, and act.


Domain-Driven
DESIGN
Tackling Complexity in the Heart of Software
Eric Evans
Foreword by Martin Fowler

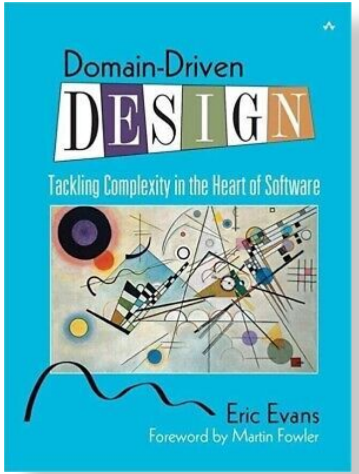
Ubiquitous Language

Ubiquitous Language is modeled…
where the terms and concepts of the business domain are identified, and there should be no ambiguity.


Domain-Driven
DESIGN
Tackling Complexity in the Heart of Software
Eric Evans
Foreword by Martin Fowler

Ubiquitous Language

This is not developers making up words, or generating colloquialisms to described what they think that domain think, how the expert talks, and the actions.


Domain-Driven
DESIGN
Tackling Complexity in the Heart of Software
Eric Evans
Foreword by Martin Fowler

What Is The Domain?

Integrated Controls Management

The premise of Integrated Controls Management (ICM) is that controls are central to cybersecurity and privacy operations, as well as the overall business rhythm of an organization.

It’s a holistic, technology-agnostic approach to cybersecurity and data protection controls to identify, implement and manage secure and compliant practices, covering an organization’s people, processes, technology and data, regardless of how or where data is stored, processed and/or transmitted.

Integrated Controls Management

The premise of Integrated Controls Management (ICM) is that controls are central to cybersecurity and privacy operations, as well as the overall business rhythm of an organization.

It's a holistic, technology-agnostic approach to cybersecurity and data protection controls to identify, implement and manage secure and compliant practices, covering an organization's people, processes, technology and data, regardless of how or where data is stored, processed and/or transmitted.

Integrated Controls Management

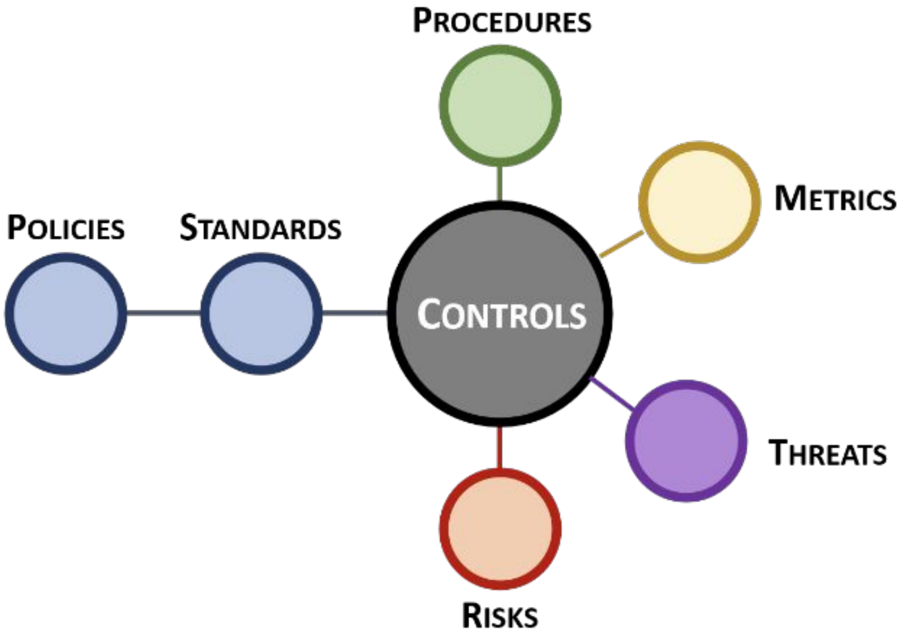
ICM takes a different approach from the traditional definition of Governance, Risk Management and Compliance (GRC) and/or Integrated Risk Management (IRM), since ICM is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization’s cybersecurity and privacy operations.

Integrated Controls Management

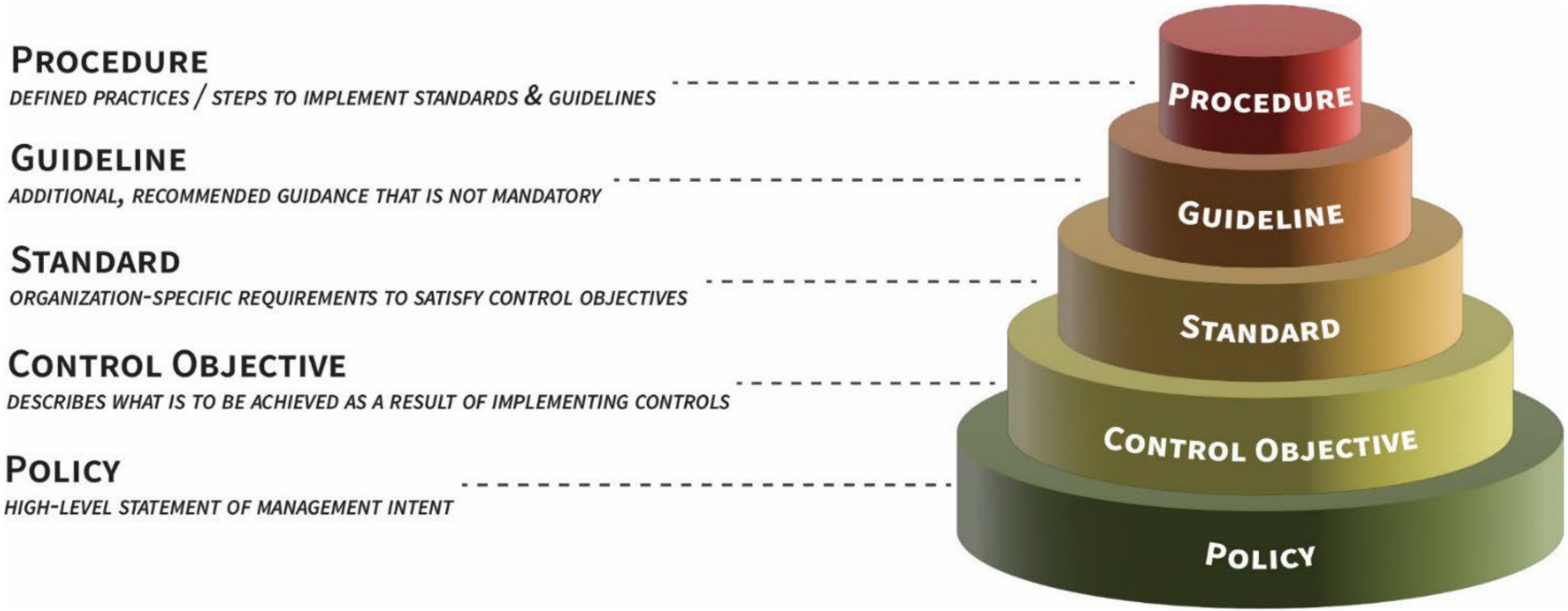
ICM takes a different approach from the traditional definition of Governance, Risk Management and Compliance (GRC) and/or Integrated Risk Management (IRM), since ICM is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization’s cybersecurity and privacy operations.

Control-Centric View Point

Control Centric View Point



The Ubiquitous Language



PROCEDURE
DEFINED PRACTICES / STEPS TO IMPLEMENT STANDARDS & GUIDELINES

GUIDELINE
ADDITIONAL, RECOMMENDED GUIDANCE THAT IS NOT MANDATORY

STANDARD
ORGANIZATION-SPECIFIC REQUIREMENTS TO SATISFY CONTROL OBJECTIVES

CONTROL OBJECTIVE
DESCRIBES WHAT IS TO BE ACHIEVED AS A RESULT OF IMPLEMENTING CONTROLS

POLICY
HIGH-LEVEL STATEMENT OF MANAGEMENT INTENT

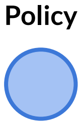
SCF - Integrated Controls Management - Pg. 12

Example Time

Policy

Our commitment to delivering high-quality, error-free products and services to our customers is paramount. To further this commitment and safeguard our reputation, we are instating a Dual Review Policy regarding all changes that directly impact our customers.

Policy Objective:
Ensure that all changes in products, services, or communications that are customer-facing undergo a thorough review by at least two qualified individuals before implementation or dissemination to ensure accuracy, consistency, and quality.



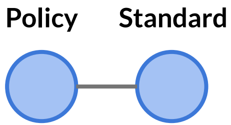
Policy

Standard

For all production deployments, the following must happen:

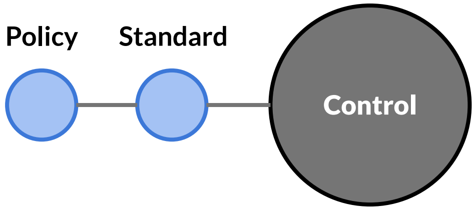
➔ An Engineer in Test must sign off that current testing sufficiently covers feature and functionality

➔ The product own with P&L responsibility must sign off on the change



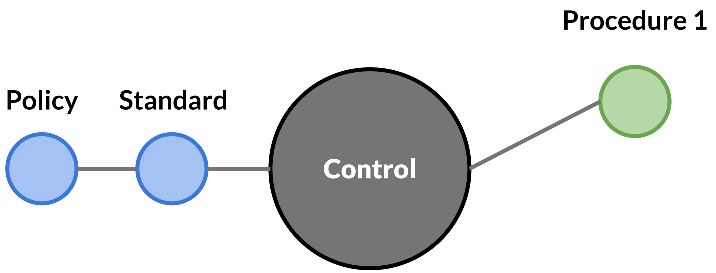
Control

The production deployment server must allow or prevent the change from going to production if the constraints of the standard are not met by the defined procedures.



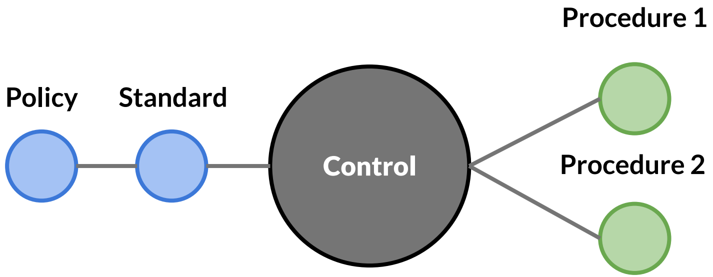
Procedure - (1) Engineer in Test

1. Look at the reviewers on the pull-request
2. At least one must be categorized as an Engineer In Test in the HR System
3. The Engineer in Test must approve the pull-request



Procedure - (2) - P&L Owner

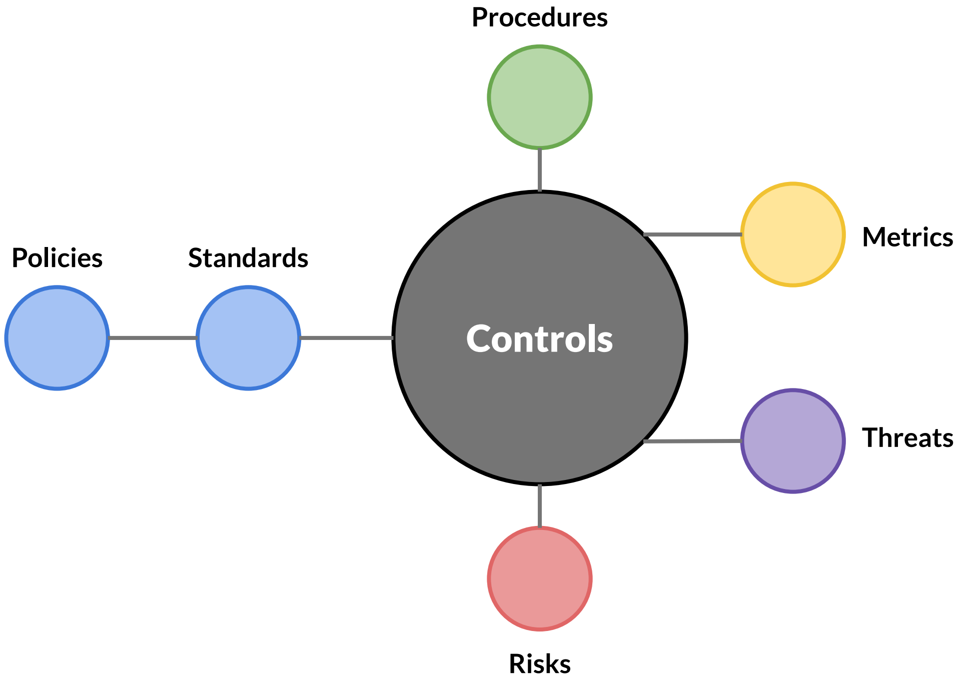
1. Find the owner of the system in the prod-mgt. system
2. Find the commit of the change in the prod-mgt. system
3. Validate the owner of the system has approved the commit in the prod-mgt. system .



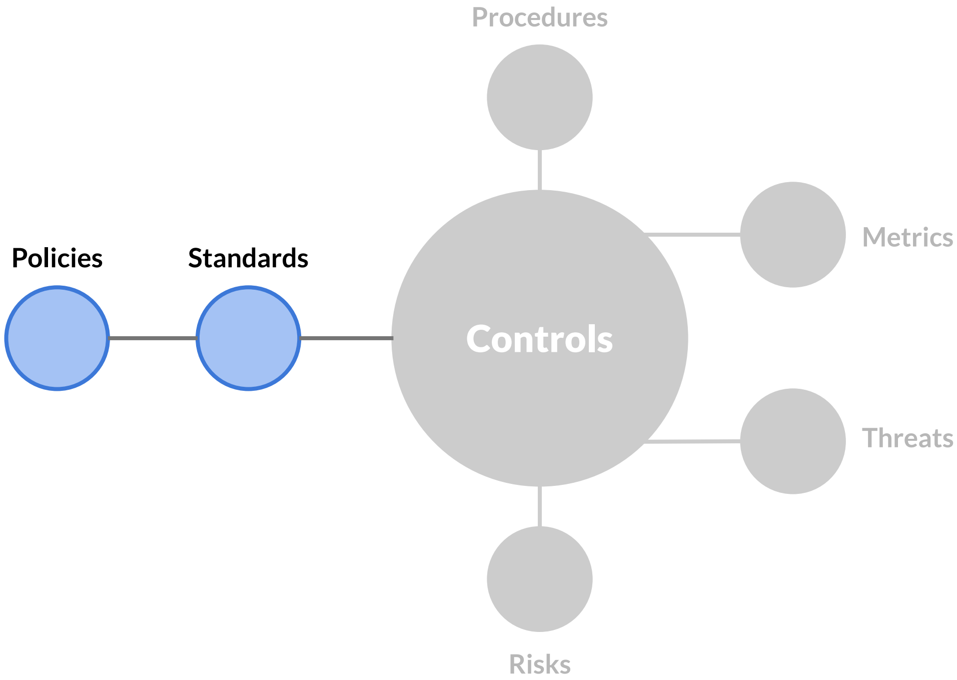
SCF - Integrated Controls Management - Pg. 12

ICM, Roles & Responsibilities

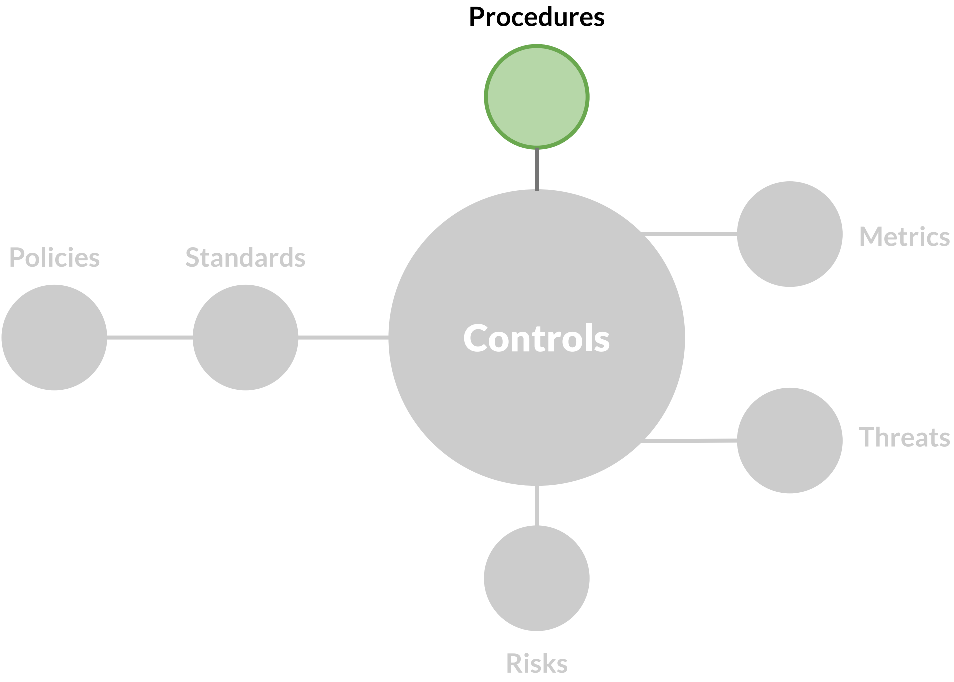
Control Centric Viewpoint



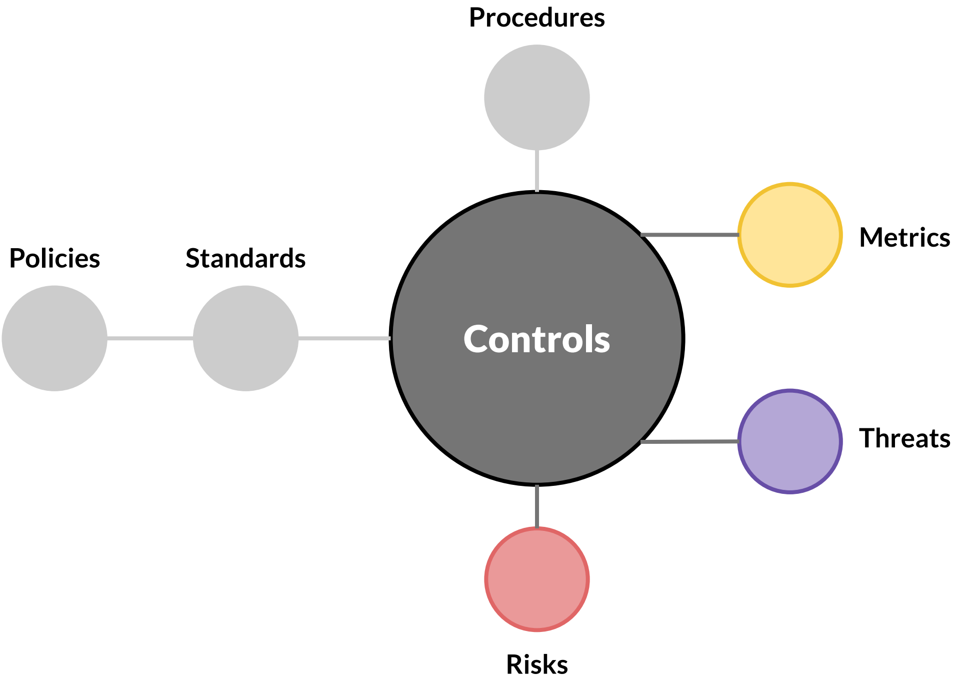
Management


Procedures
Policies
Standards
Controls
Metrics
Threats
Risks

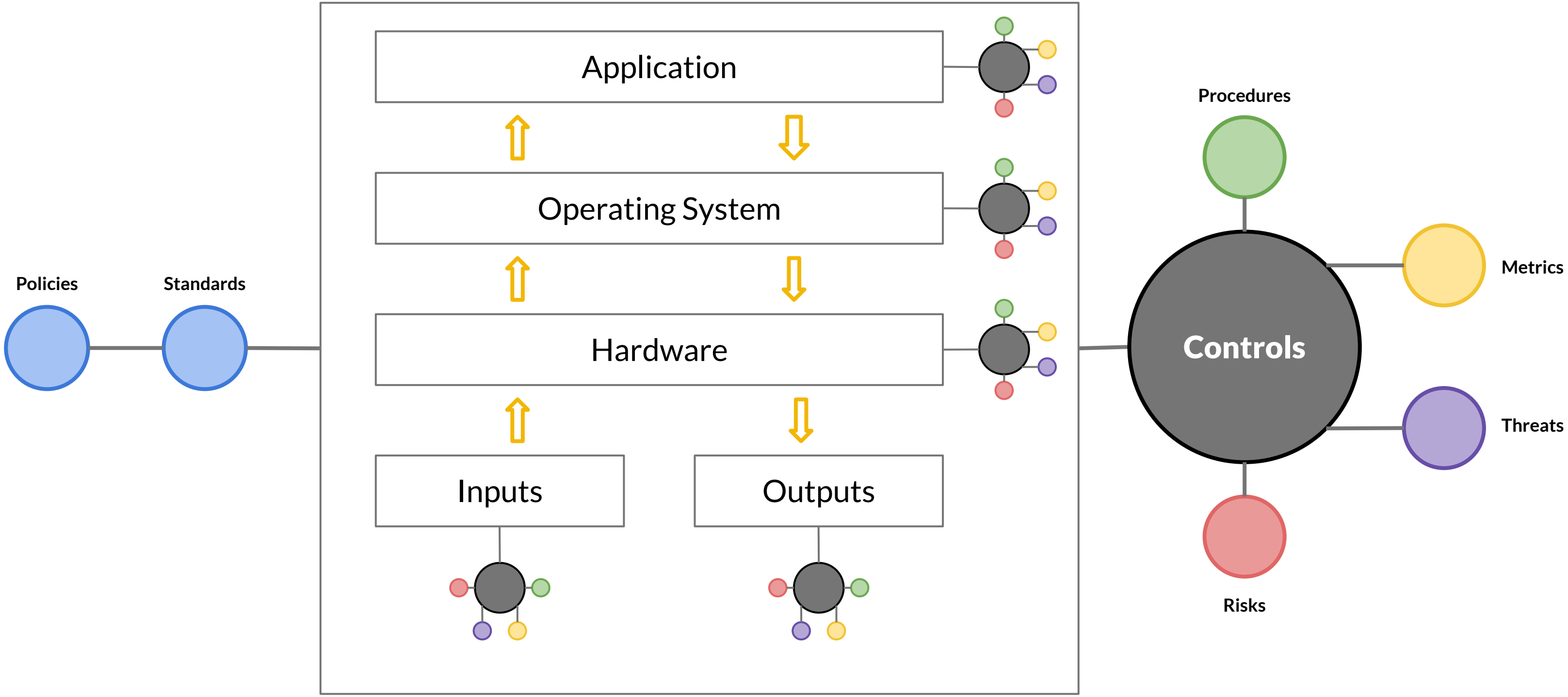
Boots on Ground



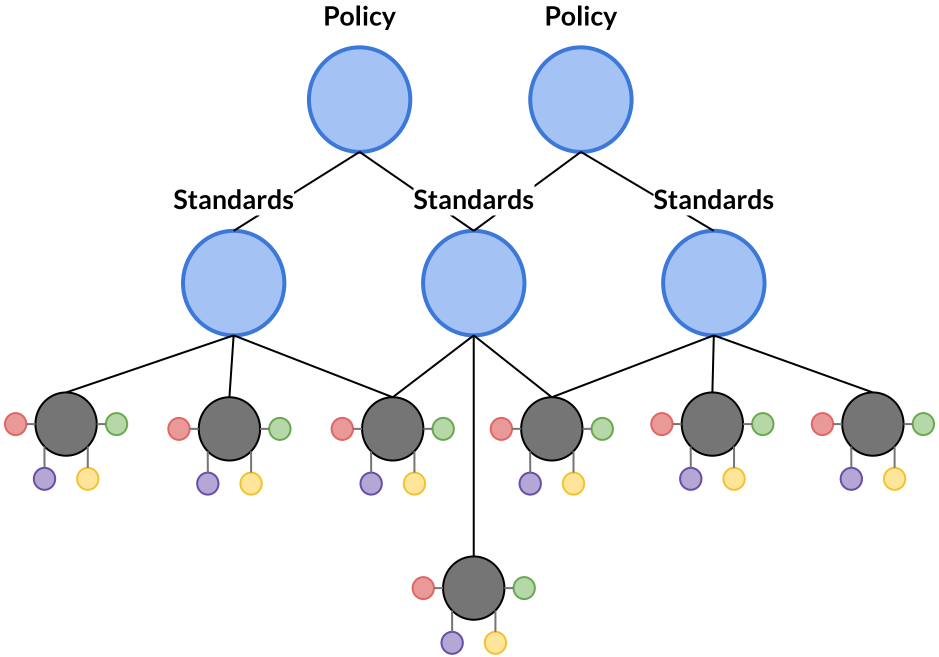
Collaboration



Control Compositions



Governance Graph



Governance Graph

- Policy can have more than one Standard
- Standard can have more than one Control
- Control can be validated by more than one Procedure

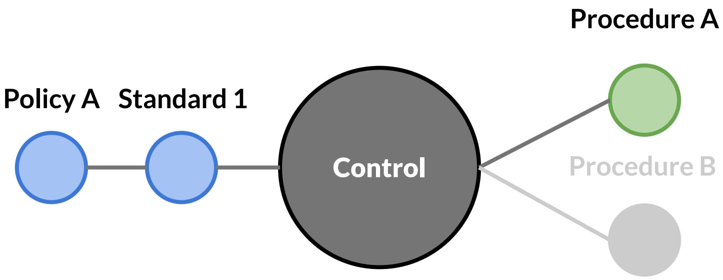
SCF - Integrated Controls Management - Pg. 12

Governance Graph - Depth ?s

A depth-based question might seek to understand the relationships or details through multiple levels of the structure.

Governance Graph - Depth ?s

"How does Procedure A validate the effectiveness of its associated Control, and how does this, in turn, ensure adherence to the overarching Standard and Policy?"



SCF - Integrated Controls Management - Pg. 12

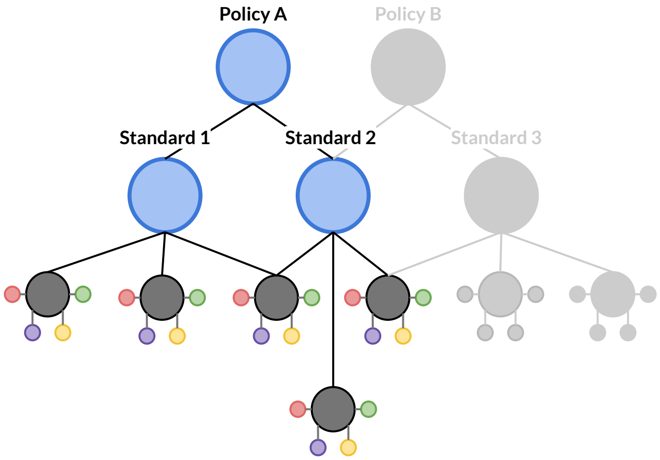
Governance Graph - Breadth ?s

A breadth-based question might seek to understand the relationships or comparisons across a single level of the governance graph.

SCF - Integrated Controls Management - Pg. 12

Governance Graph - Breadth ?s

"How do different Standards under a single Policy ensure compliance with that Policy?"



Governance Graph - High to Low

As Chief Information Officer, I wish to express our organization's steadfast commitment to the privacy and availability of customer data. Our customers entrust us with invaluable information, and it is our ethical and operational obligation to safeguard this data diligently.

On Data Privacy:
We are committed to implementing the strongest measures to protect customer data from unauthorized access, disclosure, or alteration. We will adhere to all applicable laws, regulations, and industry…

```
deny[reason] {
        input.spec.resourceAttributes.namespace
== "kube-system"
        reason := "OPA: denied access to
namespace kube-system"
        }
deny[reason] {
        input.spec.resourceAttributes.namespace
== "opa"
        required_groups :=
{"system:authenticated", "devops"}
        provided_groups := {group | group :=
input.spec[groups][_]}
        count(required_groups &
provided_groups) != count(required_groups)
        reason := sprintf("OPA: provided groups…
```

Conclusion

Policy as Code

An unfortunate & misleading colloquialism

Code Procedures, Not Policy

Code written for the proper domain concept

Centralize on Controls

Ask yourself, what procedures to create to test control?

Governance Graph

Irrefutable connection between high-level intent (policy) and low-level activity (procedures).

Bill Bensing - LinkedIn

GOVERNANCE ENGINEERING
GE
GOVENG.IO