Trust teams but verify: Compliance as code done right

Effy Elden

Effy Elden

(consultus technologus)

"We have listened to the wisdom in an old Russian maxim… the maxim is '**Doveryay, no proveryay**', '**Trust, but verify**'."

President Ronald Reagan

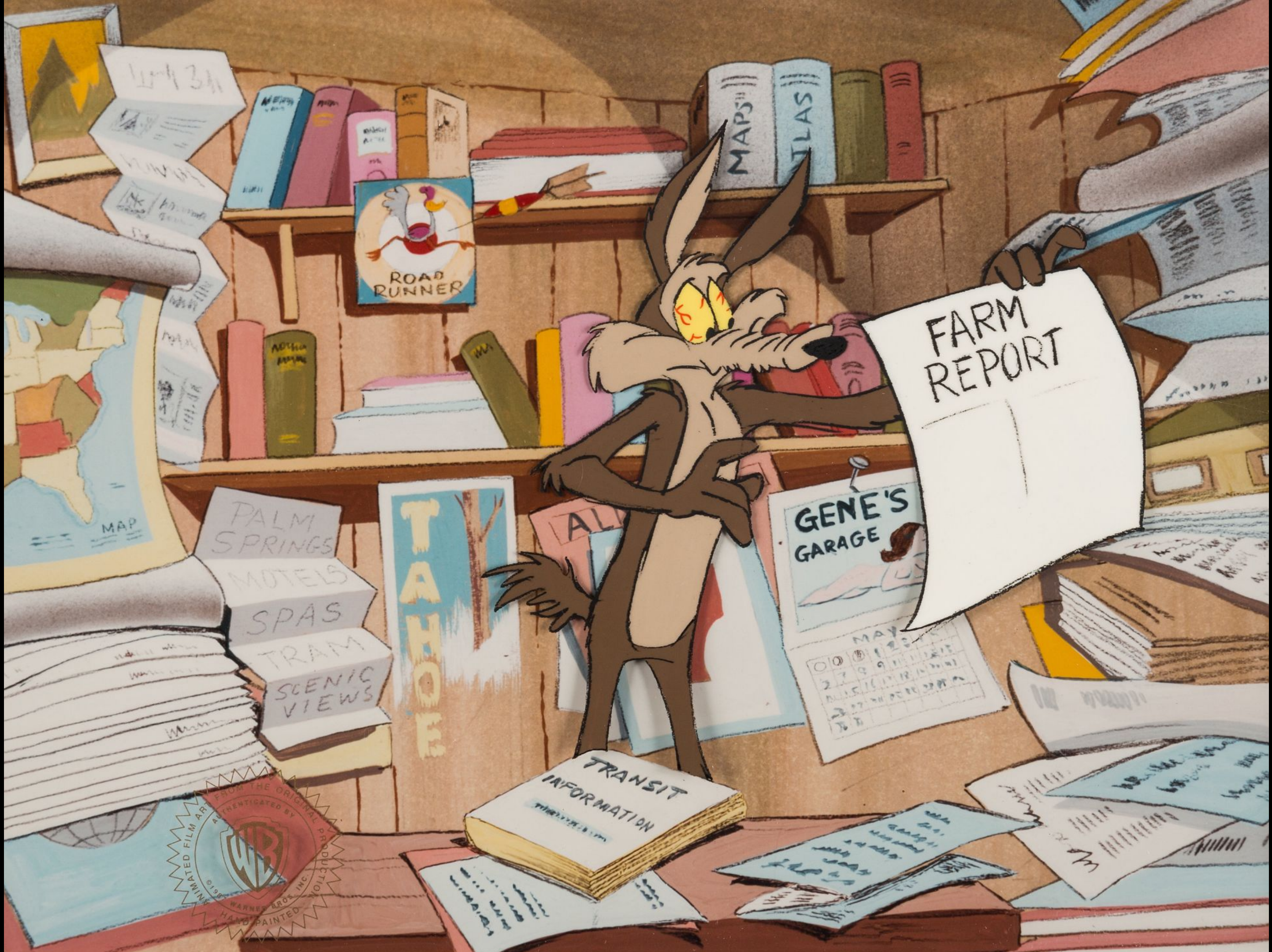
Trust teams

but verify

Trust teams
with the autonomy to do their job well

but verify
their work so that you can be confident

STORY TIME


MAPS
ATLAS
ROAD RUNNER
FARM REPORT
MAP
PALM SPRINGS
MOTELS
SPAS
TRAM
SCENIC VIEWS
TAHOE
GENE'S GARAGE
MAY
TRANSIT INFORMATION
ANIMATED FILM ART FROM THE ORIGINAL PRODUCTION
AUTHENTICATED BY WARNER BROS. INC.
HAND PAINTED

Compliance

Compliance was not the problem.

Compliance was not the problem.

Compliance is just about rules and standards, keeping things consistent.

Compliance was not the problem.

Compliance is just about rules and standards, keeping things consistent.

Compliance is genuinely important.

The problem was process and culture

- Too far away
- Too late
- Too much work
- Too inefficient
- Painful

The problem was process and culture

- **Too far away**
- Too late
- Too much work
- Too inefficient
- Painful

The problem was process and culture

- Too far away
- **Too late**
- Too much work
- Too inefficient
- Painful

The problem was process and culture

- Too far away
- Too late
- **Too much work**
- Too inefficient
- Painful

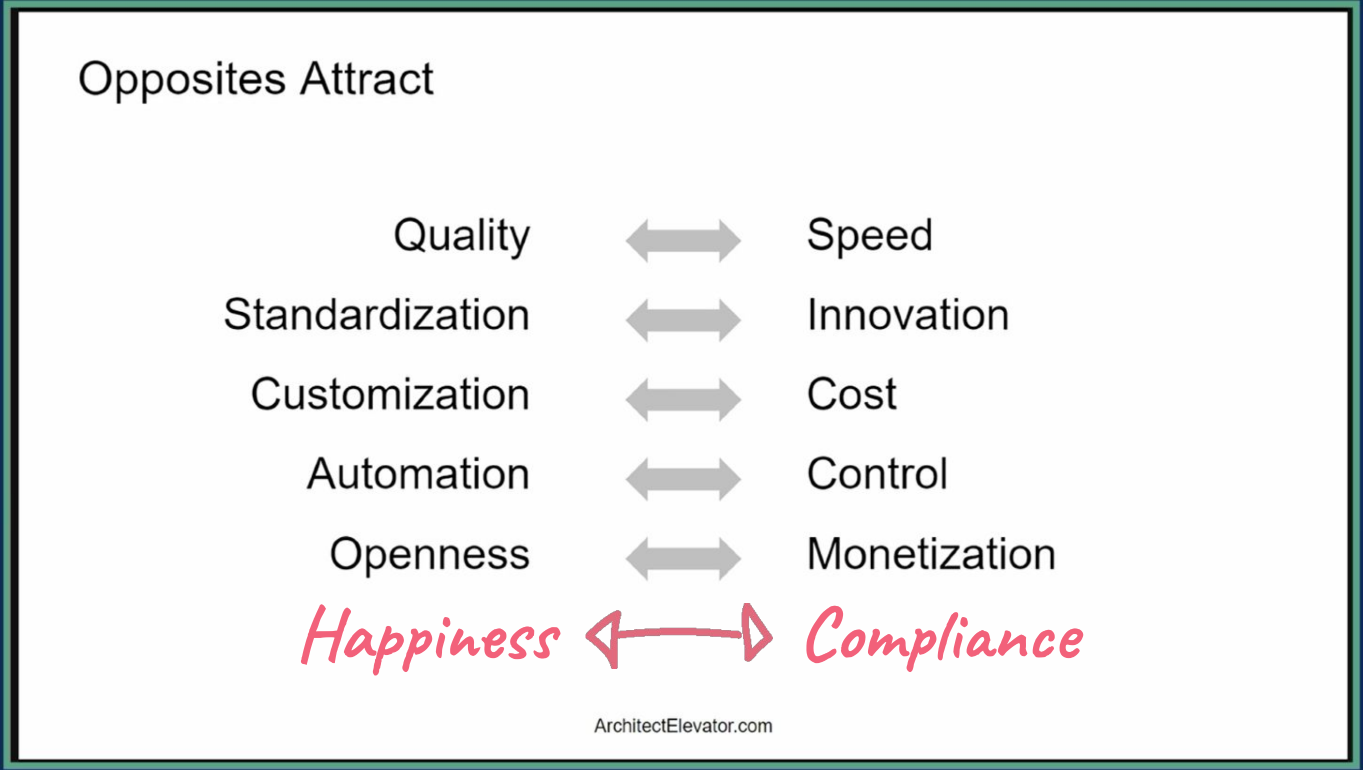
The problem was process and culture

- Too far away
- Too late
- Too much work
- **Too inefficient**
- Painful

The problem was process and culture

- Too far away
- Too late
- Too much work
- Too inefficient
- **Painful**

<this space left as empty as my soul after spending weeks filling out compliance checklists>



Opposites Attract

Quality	↔	Speed
Standardization	↔	Innovation
Customization	↔	Cost
Automation	↔	Control
Openness	↔	Monetization
Happiness	↔	Compliance

ArchitectElevator.com

2021 CONFERENCE
skills matter
YOW!
September

#YOWSeptember

Gregor Hohpe - @ghohpe

The Magic of Platforms

It doesn’t have to be this way!

Compliance *as* Code is...

- Defining controls and rules **in ways computers can understand** (not just humans)
- Developing **automated processes** to **continuously** check compliance
- Applying **modern software development practices** to make compliance easier

Compliance as Code is...

- Defining controls and rules **in ways computers can understand** (not just humans)
- Developing **automated processes** to **continuously** check compliance
- Applying **modern software development practices** to make compliance easier

Compliance *as* Code is...

- Defining controls and rules **in ways computers can understand** (not just humans)
- Developing **automated processes** to **continuously** check compliance
- Applying **modern software development practices** to make compliance easier

Compliance *as* Code is...

- Defining controls and rules **in ways computers can understand** (not just humans)
- Developing **automated processes** to **continuously** check compliance
- Applying **modern software development practices** to make compliance easier

Why should you do Compliance *as Code*?

- **Reduce risk and increase confidence**
- Better scalability
- Shift left and detect problems earlier
- Shared ownership of compliance

Why should you do Compliance *as Code*?

- Reduce risk and increase confidence
- **Better scalability**
- Shift left and detect problems earlier
- Shared ownership of compliance

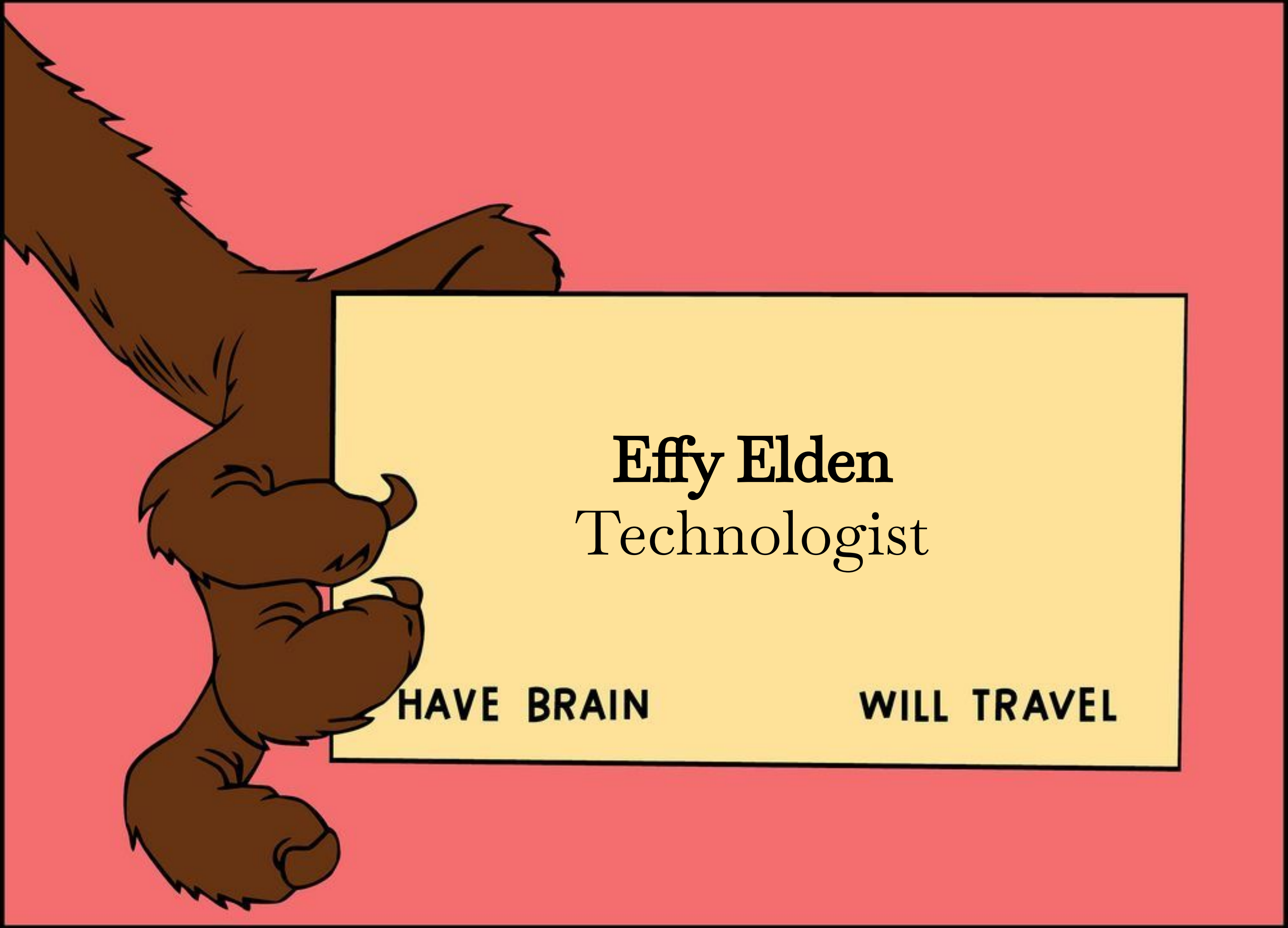
Why should you do Compliance *as Code?*

- Reduce risk and increase confidence
- Better scalability
- **Shift left and detect problems earlier**
- Shared ownership of compliance

Why should you do Compliance *as Code*?

- Reduce risk and increase confidence
- Better scalability
- Shift left and detect problems earlier
- **Shared ownership of compliance**

How can you do Compliance *as Code*? (the right way)



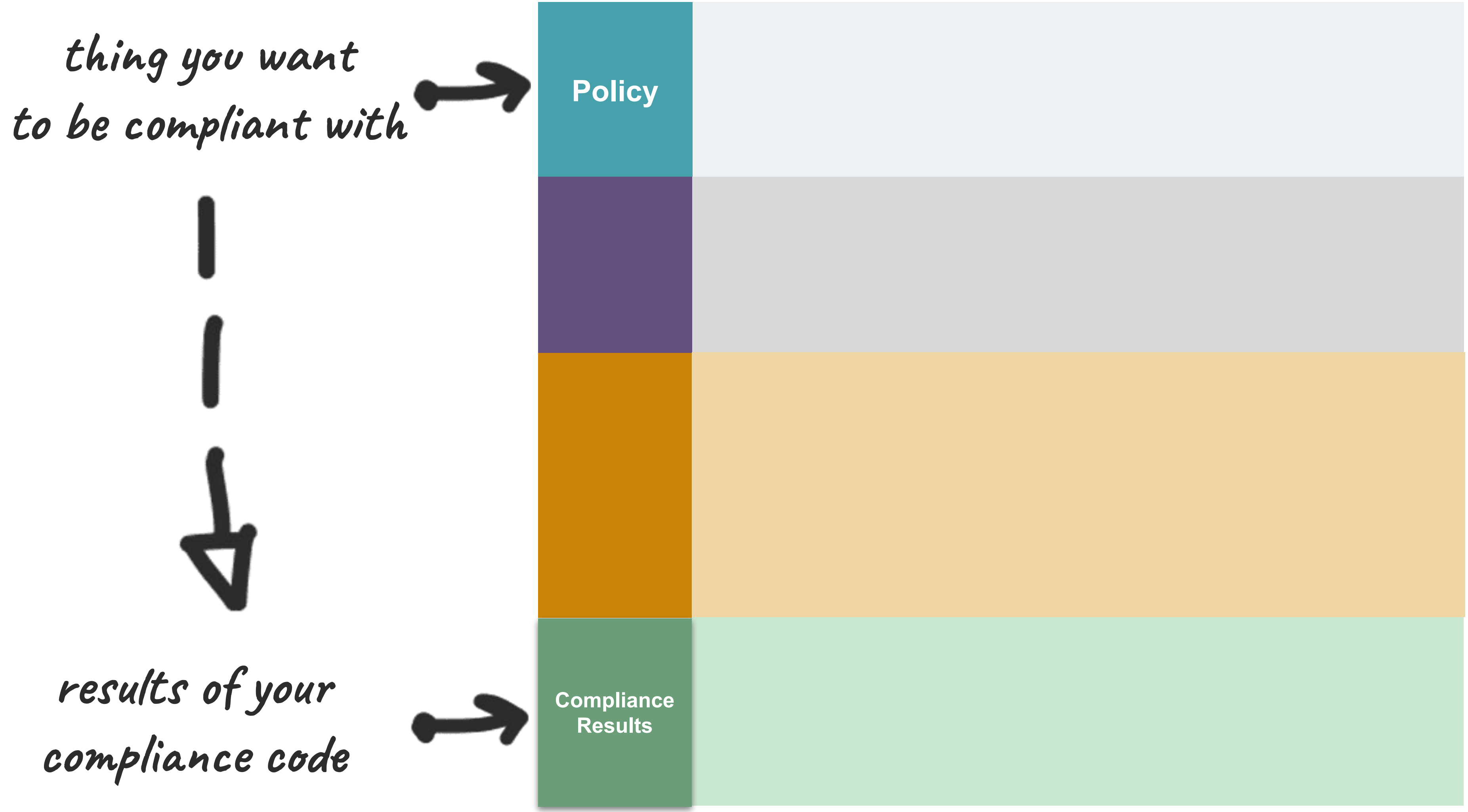
Effy Elden

Technologist

ACME

CORPORATION

ACME
TRIPLE-STRENGTH FORTIFIED
LEG MUSCLE VITAMINS
FAMILY SIZE
Fleet-Foot
JET-PROPELLED TENNIS SHOES
ONE ACME
DO-IT YOURSELF
Tornado Kit
"SEED YOUR OWN TORNADOS"
ACME
DEHYDRATED BOULDERS
JUST ADD WATER
ACME ULTIMATUM DISPATCHER
ACME
SUPER OUTFIT
ACME
DISINTEGRATING PISTOL
ONE
ACME
BAT-MAN'S OUTFIT
ACME MFG. CO.
REG. SIZE
ONE ACME
OUT-BOARD MOTOR
ONE
JIM-DANDY WAGON
SOLID CEMENT
ACME GAS
ONE
ACME
STREET CLEANERS WAGON
ANVIL
WEATHER BALLOON
ACME
PET SHOP
Acme
BIRD SEED
AJAX ESCAPE KIT
ASSORTED PICNIC ANT



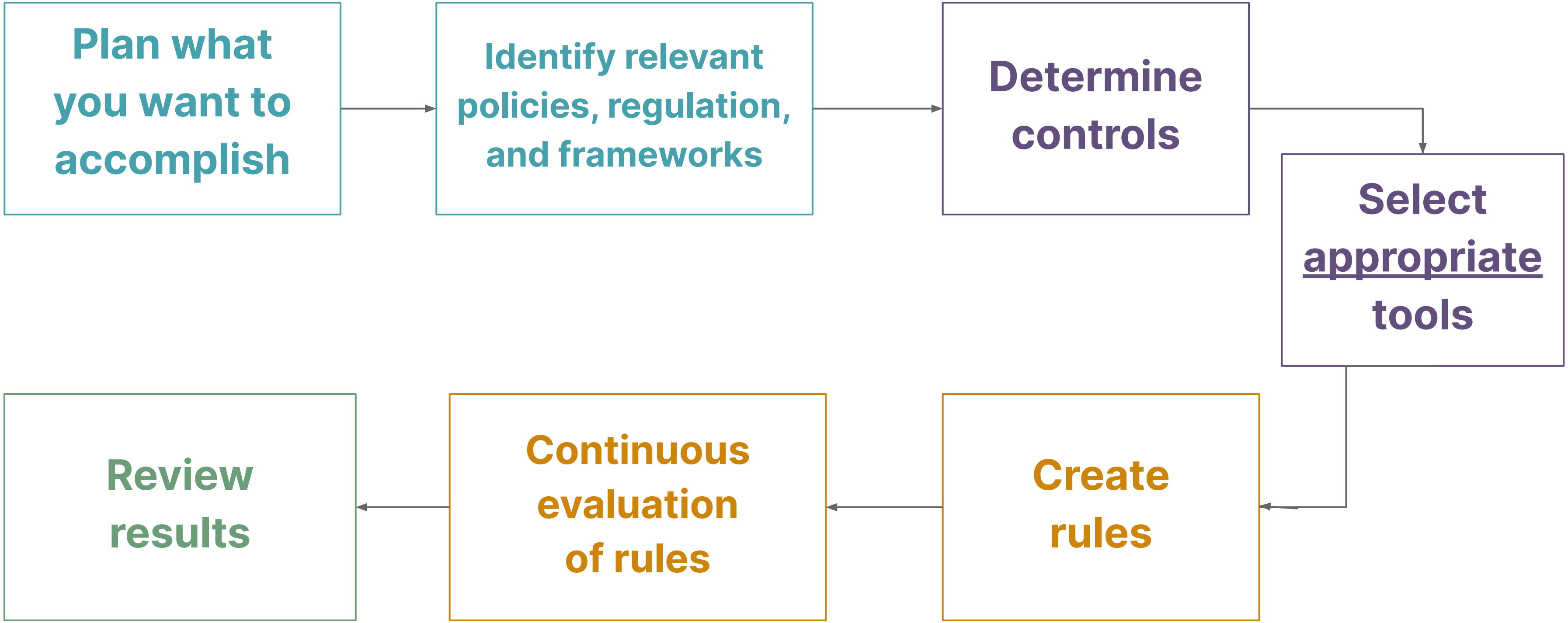
thing you want to be compliant with

Policy

results of your compliance code

Compliance Results

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

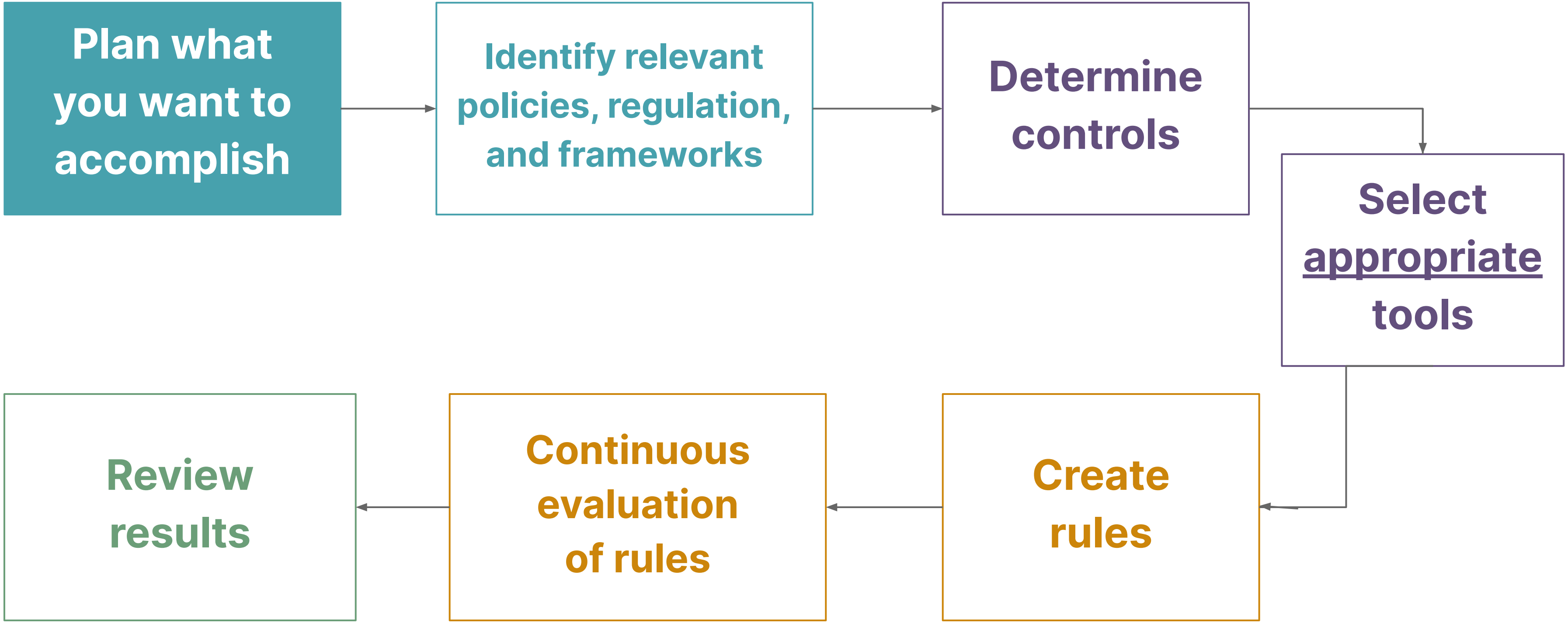
Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

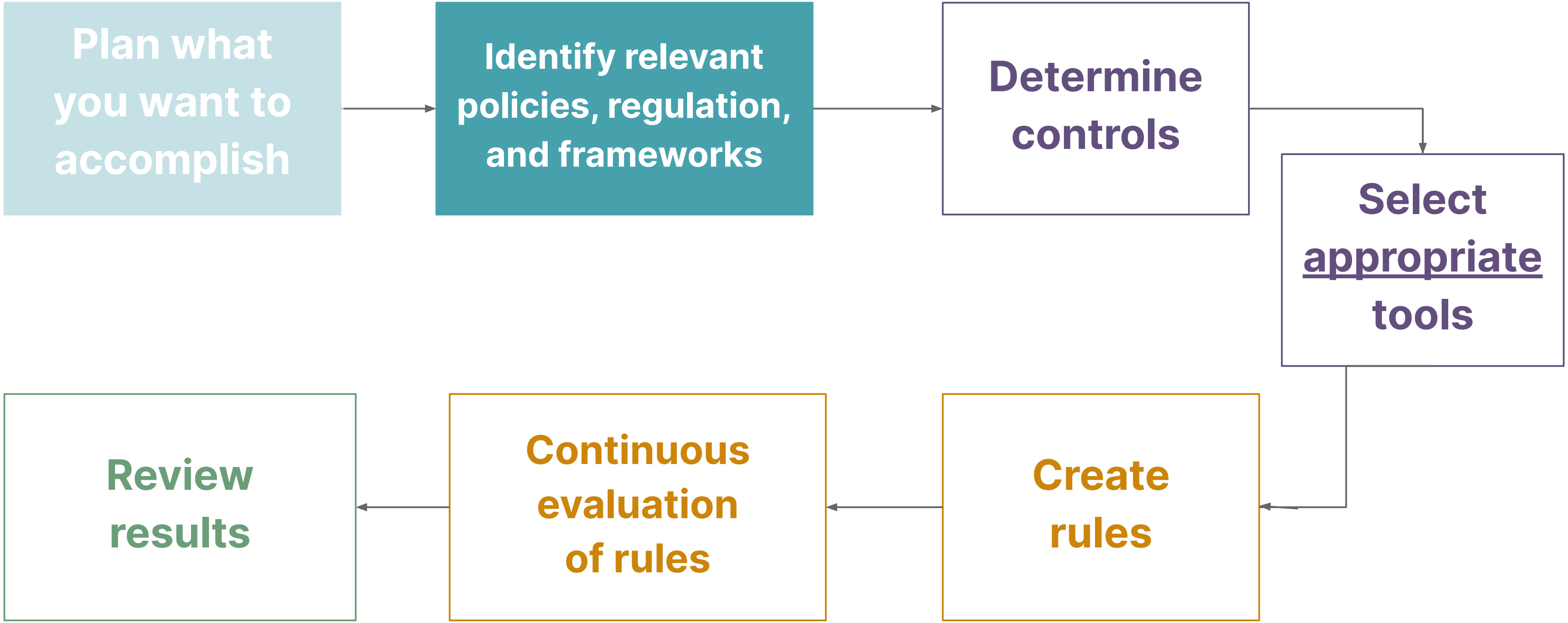
Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

Select appropriate tools

Create rules

Continuous evaluation of rules

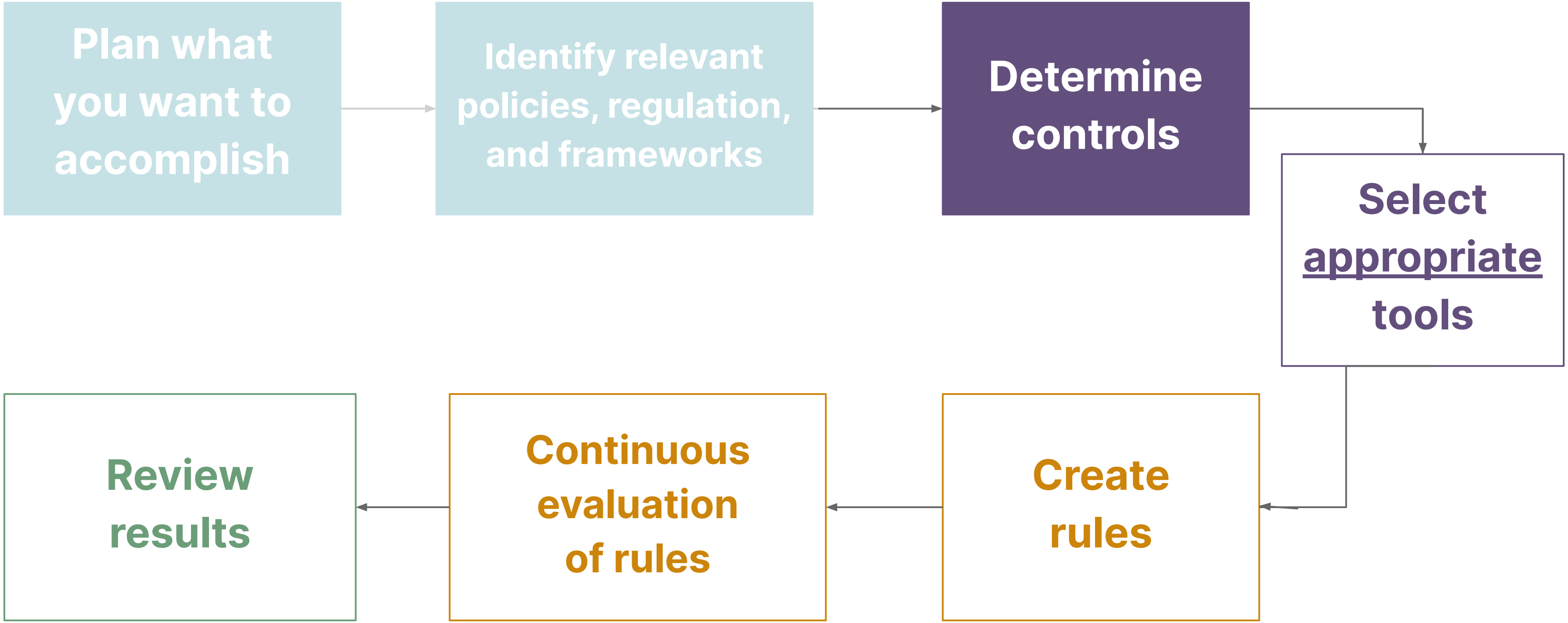
Review results

Policy

ACME Corporation Information Handling Policy 2.0

1. All data must be encrypted at rest.

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

What are controls?

- Policy applied **in a particular context**
- **More specific** than policy
- Accounting for **technical context**

What are controls?

- Policy applied **in a particular context**
- **More specific** than policy
- Accounting for **technical context**

What are controls?

- Policy applied **in a particular context**
- **More specific** than policy
- Accounting for **technical context**

What are controls?

- Policy applied **in a particular context**
- **More specific** than policy
- Accounting for **technical context**

Policy

ACME Corporation Information Handling Policy 2.0

1. All data must be encrypted at rest.

Control

ACME Corporation AWS Cloud Controls

1. All AWS S3 buckets must be configured with AWS KMS encryption.

Policy

ACME Corporation Information Handling Policy 2.0

5. All data must be encrypted at rest.

Control

***ACME Corporation
AWS Cloud Controls***

Control

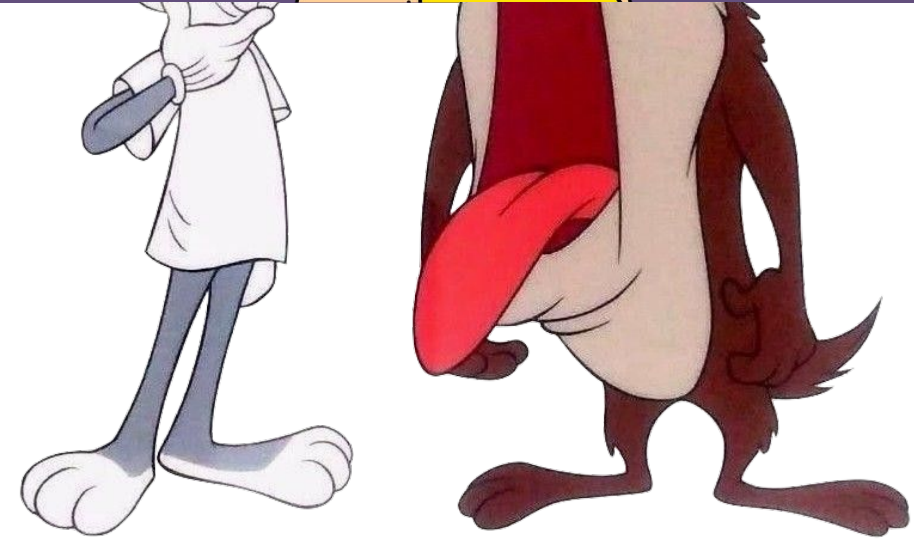
***ACME Corporation
Local Device Controls***

Control

....

Preventative measures

are built to stop a compliance breach from occurring.



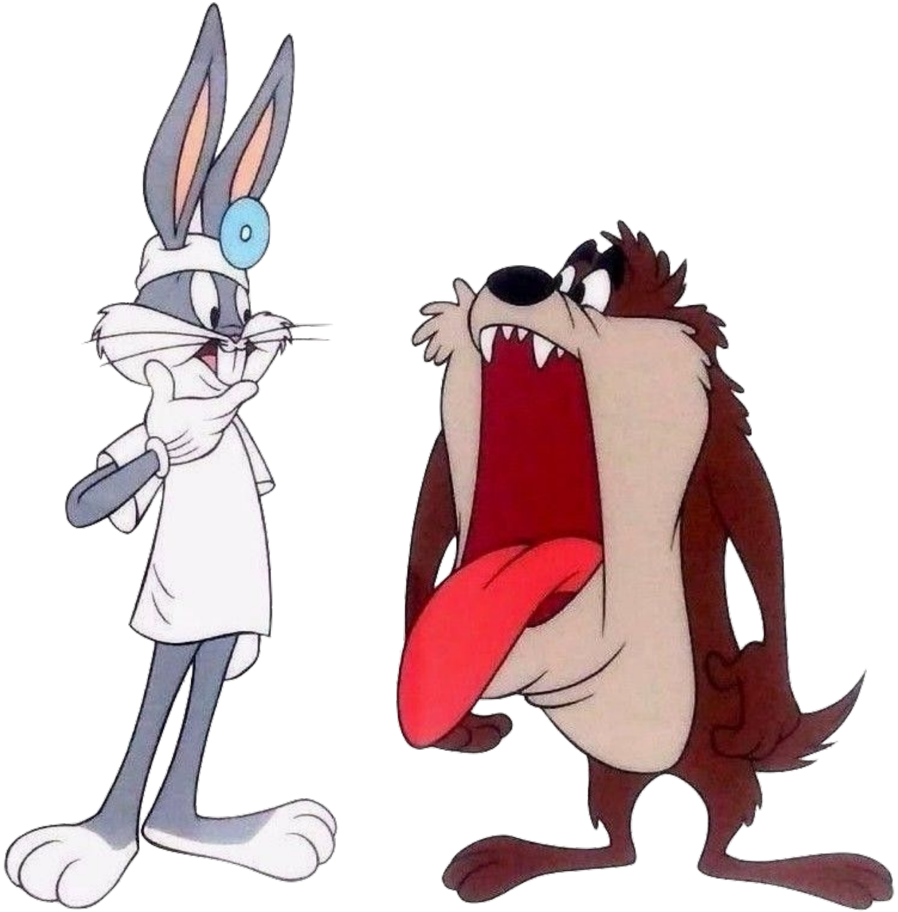
Detective measures

are built to find compliance breaches that have occurred.

Image credit: DeviantArt - Mega-Shonen-One-64

Preventative measures

- Fast feedback, local feedback even possible
- Tends to be tightly coupled to the implementation
- Some limitations on what you can test and how easily



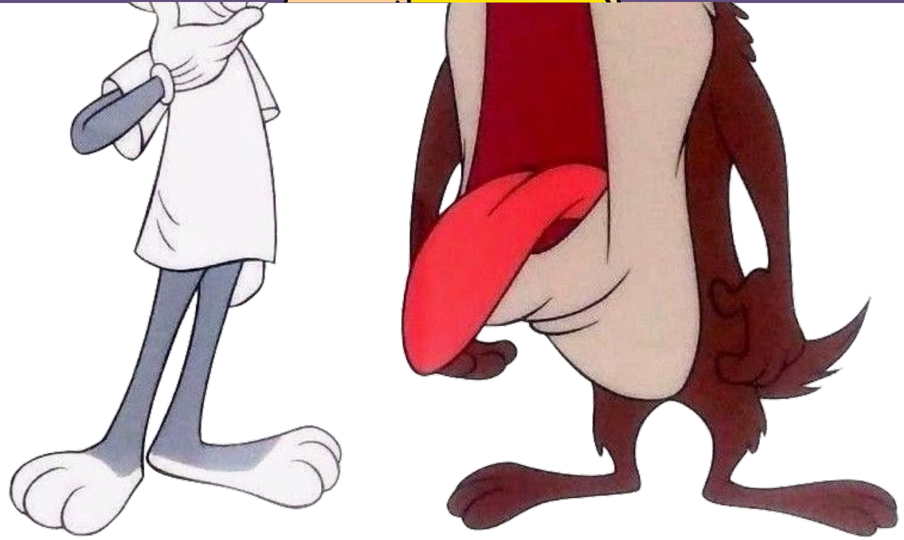
Detective measures

- Often simpler to test and more direct
- Decoupled from the implementation
- Means you have a non-compliant thing for a period of time
- Slower feedback cycles

Preventative measures

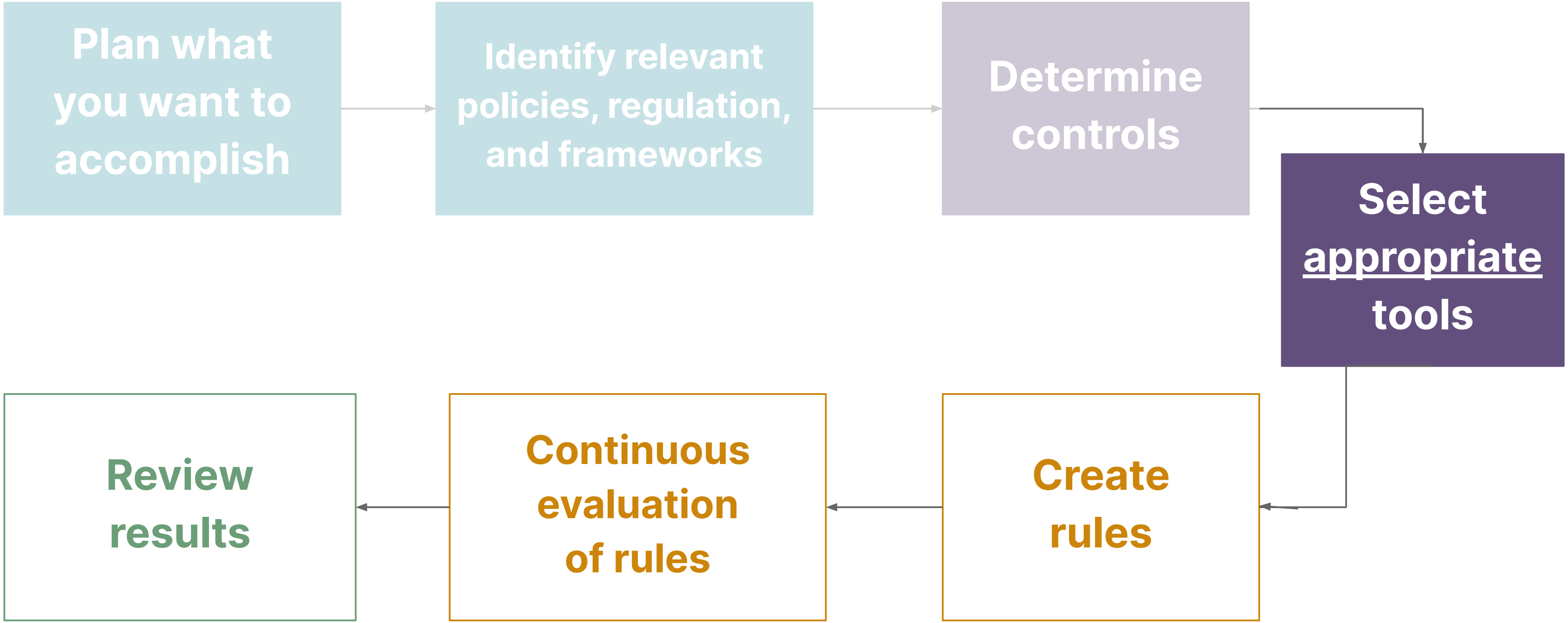
&

Detective measures



Defence In Depth

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

Tools for Compliance as Code

INSPEC
BY CHEF

AWS Config

checkov
by bridgecrew

Open Policy Agent

Google Cloud

Regula

Azure Policy

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results

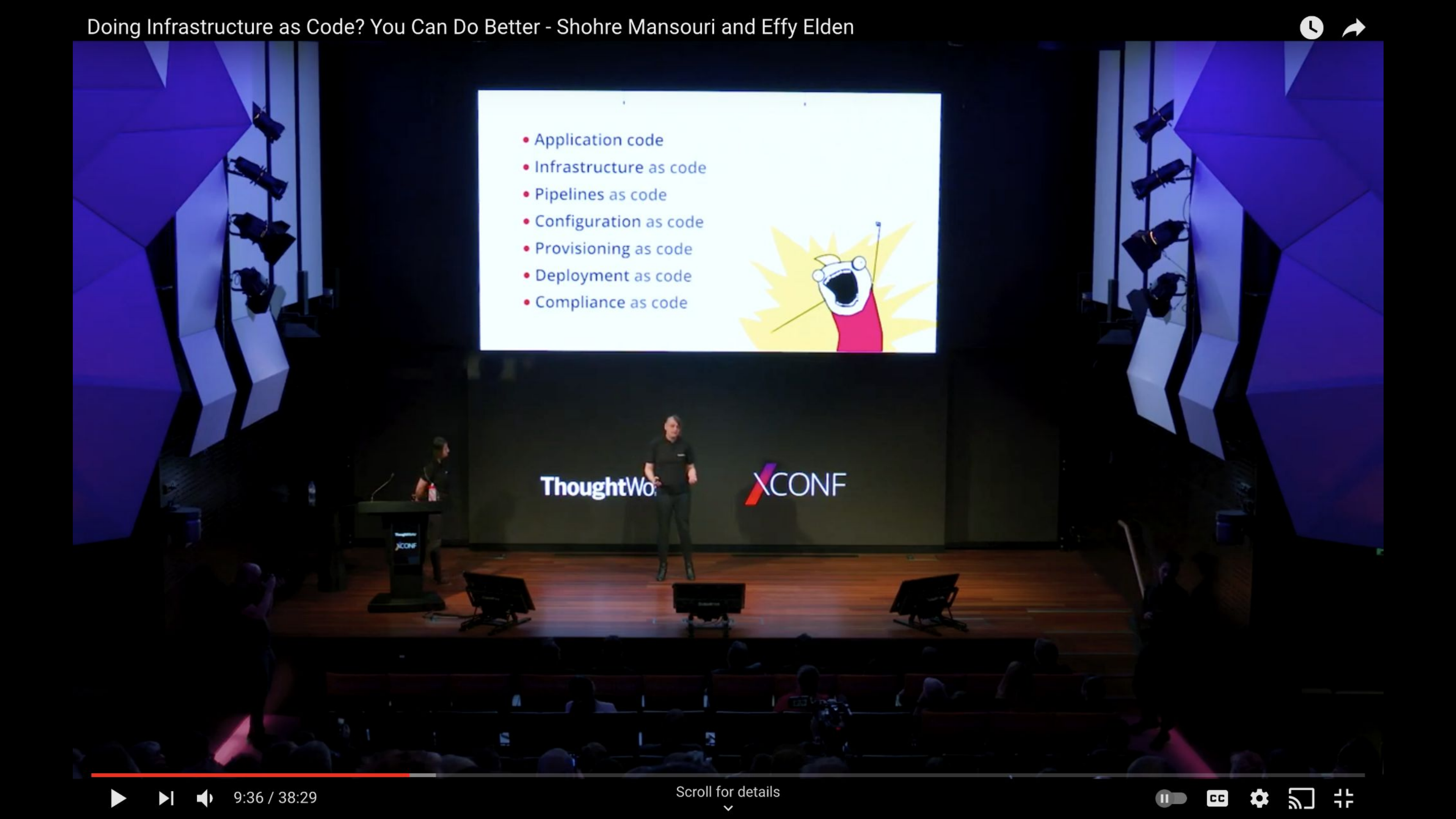
Don’t reinvent the wheel.

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results



Doing Infrastructure as Code? You Can Do Better - Shohre Mansouri and Effy Elden

- Application code
- Infrastructure as code
- Pipelines as code
- Configuration as code
- Provisioning as code
- Deployment as code
- Compliance as code

How to choose tools for Compliance *as Code*

- **Suitability** for your controls
- **Availability** of pre-built rules
- **Extensibility** with custom rules
- **Testability** of your rules
- **Observability** of execution and results

Embrace the polyglot.

Tools for Compliance as Code

INSPEC
BY CHEF

AWS Config

checkov
by bridgecrew

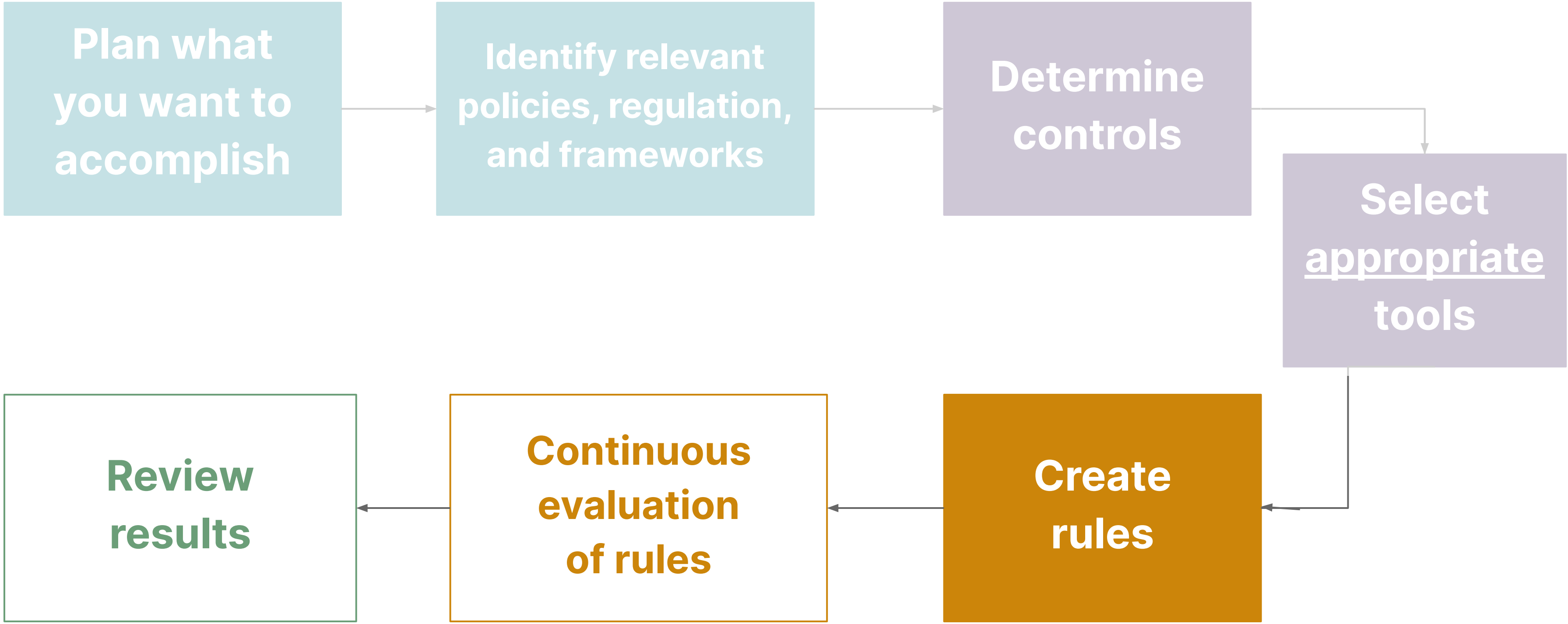
Open Policy Agent

Google Cloud

Regula

Azure Policy

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

Select appropriate tools

Create rules

Continuous evaluation of rules

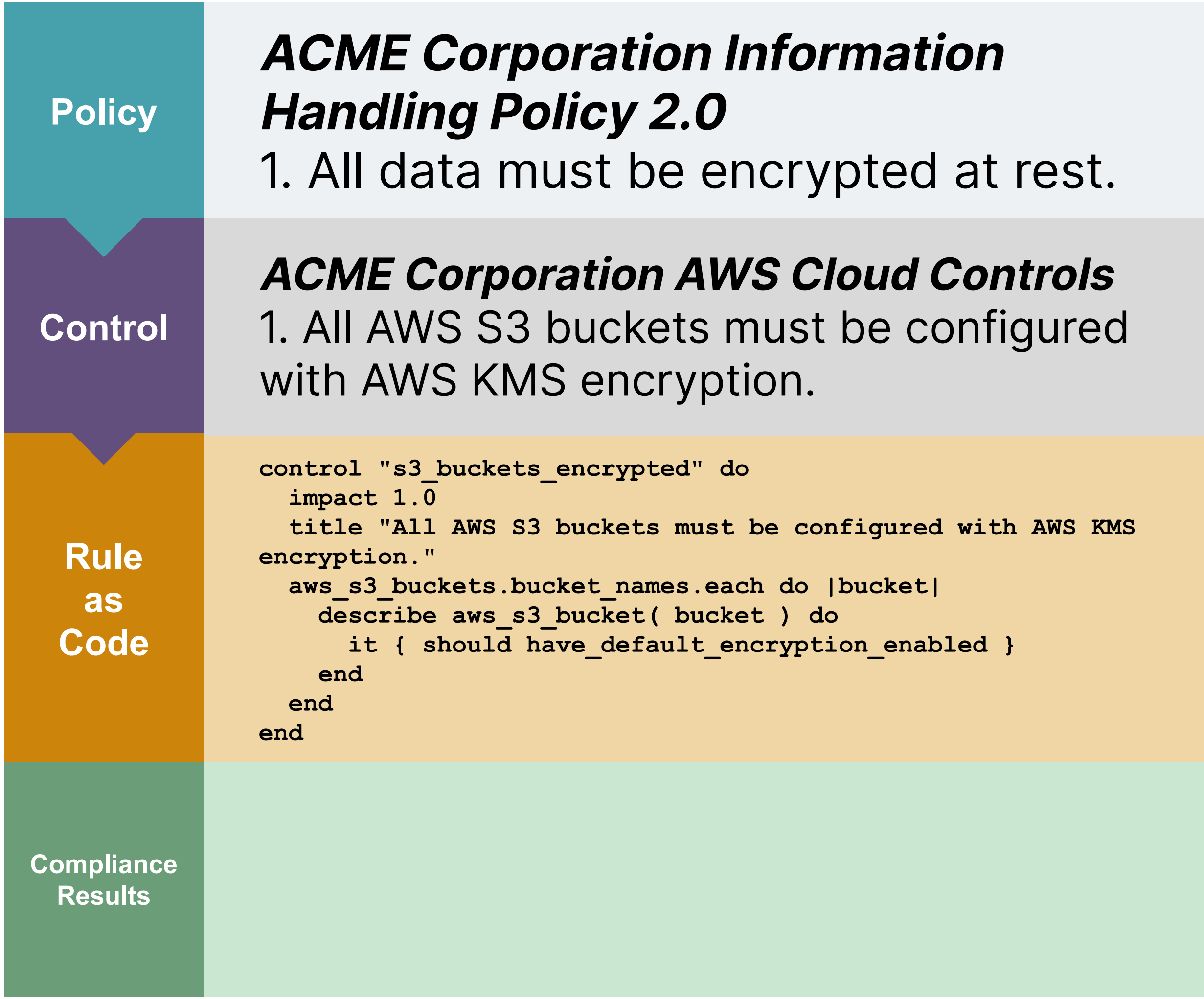
Review results

Rule as Code

```
control "s3_buckets_encrypted" do
  impact 1.0
  title "All AWS S3 buckets must be configured with
        AWS KMS encryption."
  aws_s3_buckets.bucket_names.each do |bucket|
    describe aws_s3_bucket( bucket ) do
      it { should have_default_encryption_enabled }
    end
  end
end
```

Rule as Code

```
control "s3_buckets_encrypted" do
  impact 1.0
  title "All AWS S3 buckets must be configured with
        AWS KMS encryption."
  aws_s3_buckets.bucket_names.each do |bucket|
    describe aws_s3_bucket( bucket ) do
      it { should have_default_encryption_enabled }
    end
  end
end
```



Policy

ACME Corporation Information Handling Policy 2.0

1. All data must be encrypted at rest.

Control

ACME Corporation AWS Cloud Controls

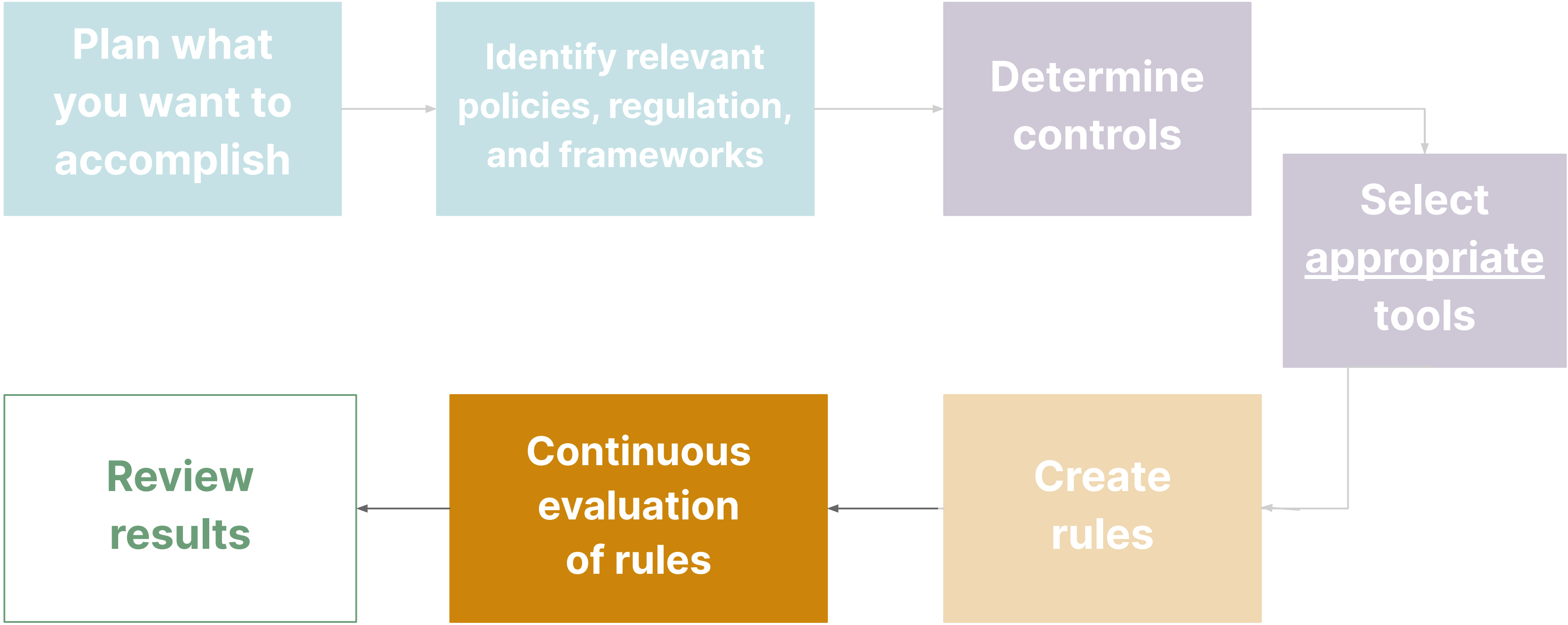
1. All AWS S3 buckets must be configured with AWS KMS encryption.

Rule as Code

```
control "s3_buckets_encrypted" do
  impact 1.0
  title "All AWS S3 buckets must be configured with AWS KMS
encryption."
  aws_s3_buckets.bucket_names.each do |bucket|
    describe aws_s3_bucket( bucket ) do
      it { should have_default_encryption_enabled }
    end
  end
end
```

Compliance Results

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

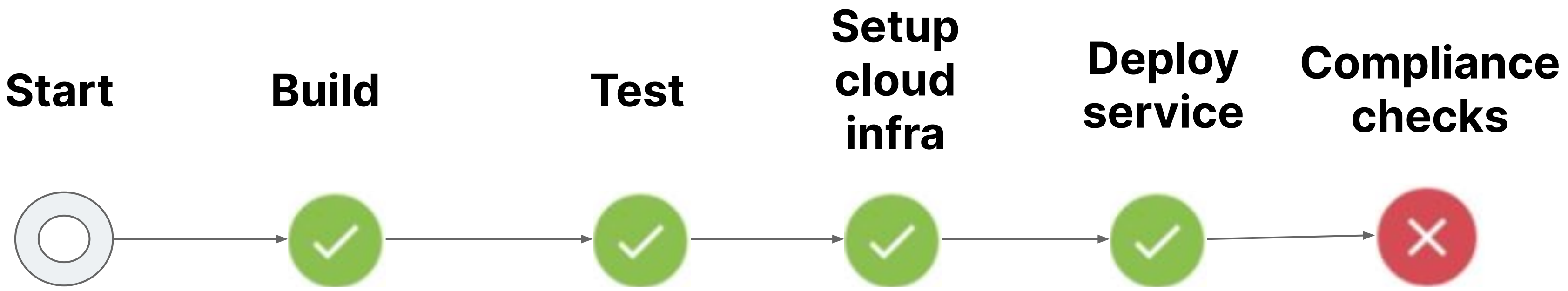
Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

Easy win: put it in your pipeline



Build compliance in at every stage.

Local development & Pipelines

Local development

- Shift left
- Fastest feedback
- Not always possible
- Preventative controls

Pipelines

- Shift left
- Fast feedback
- Shared context
- Preventative controls
- Detective controls

Non-production & Production

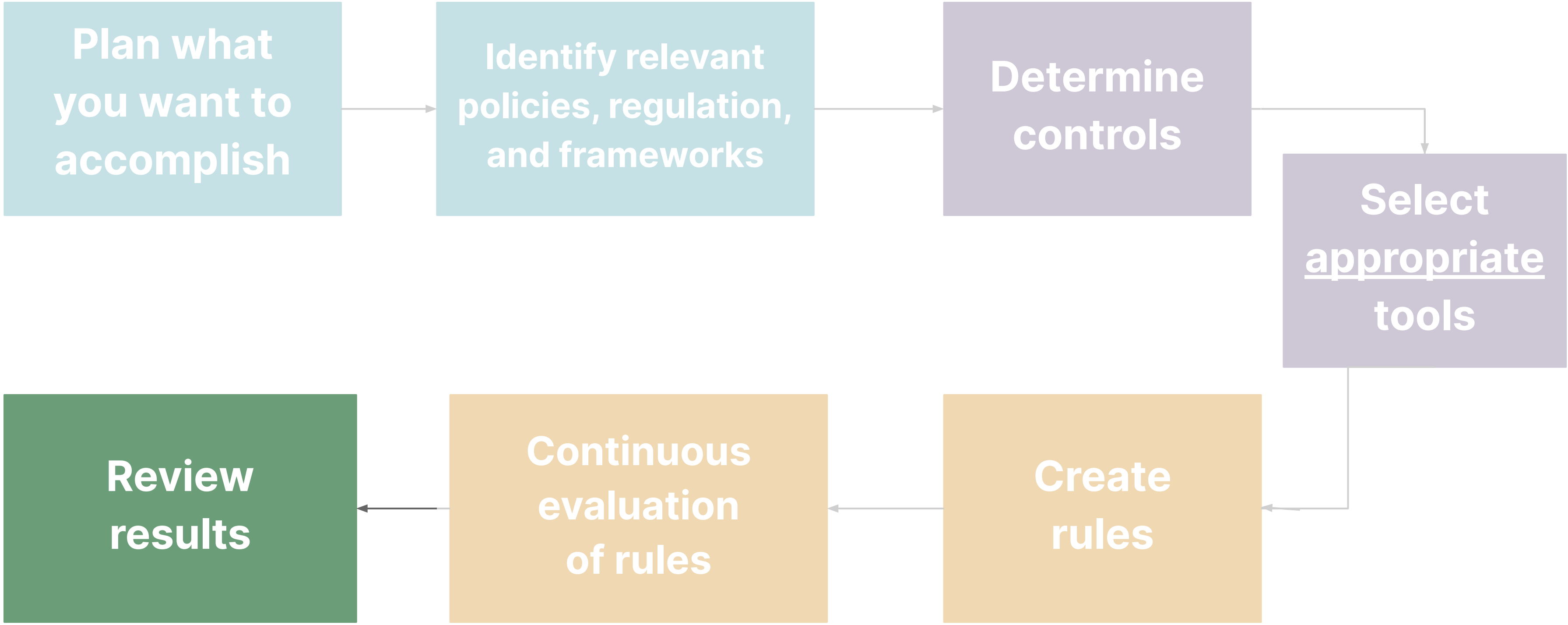
Non-production

- “Continuous compliance”
- Close to production
- Detective controls
- Cloud provider offerings

Production

- “Continuous compliance”
- Most confidence
- Detective controls
- Cloud provider offerings

How to get started with Compliance as Code



Plan what you want to accomplish

Identify relevant policies, regulation, and frameworks

Determine controls

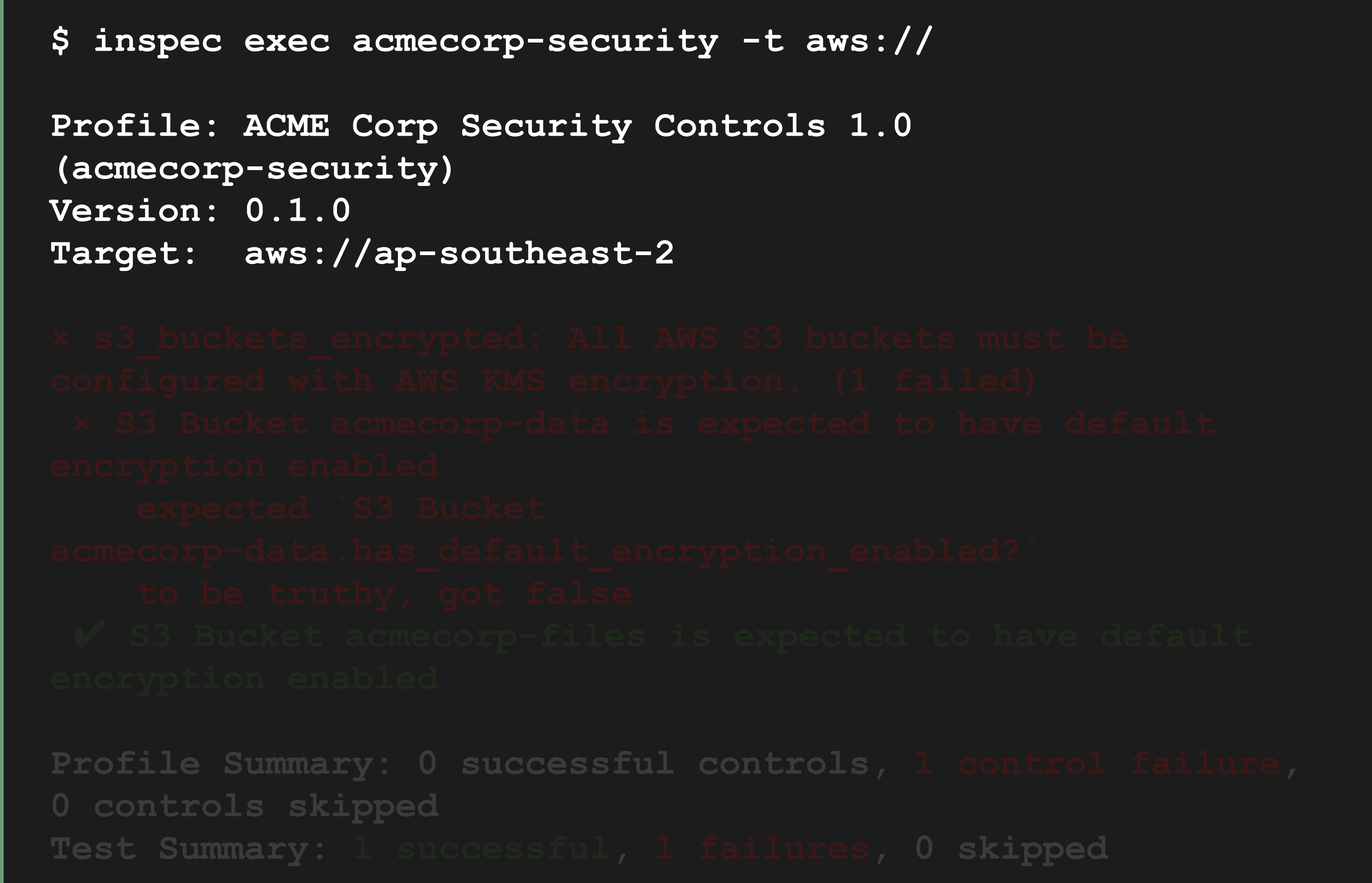
Select appropriate tools

Create rules

Continuous evaluation of rules

Review results

Compliance Results



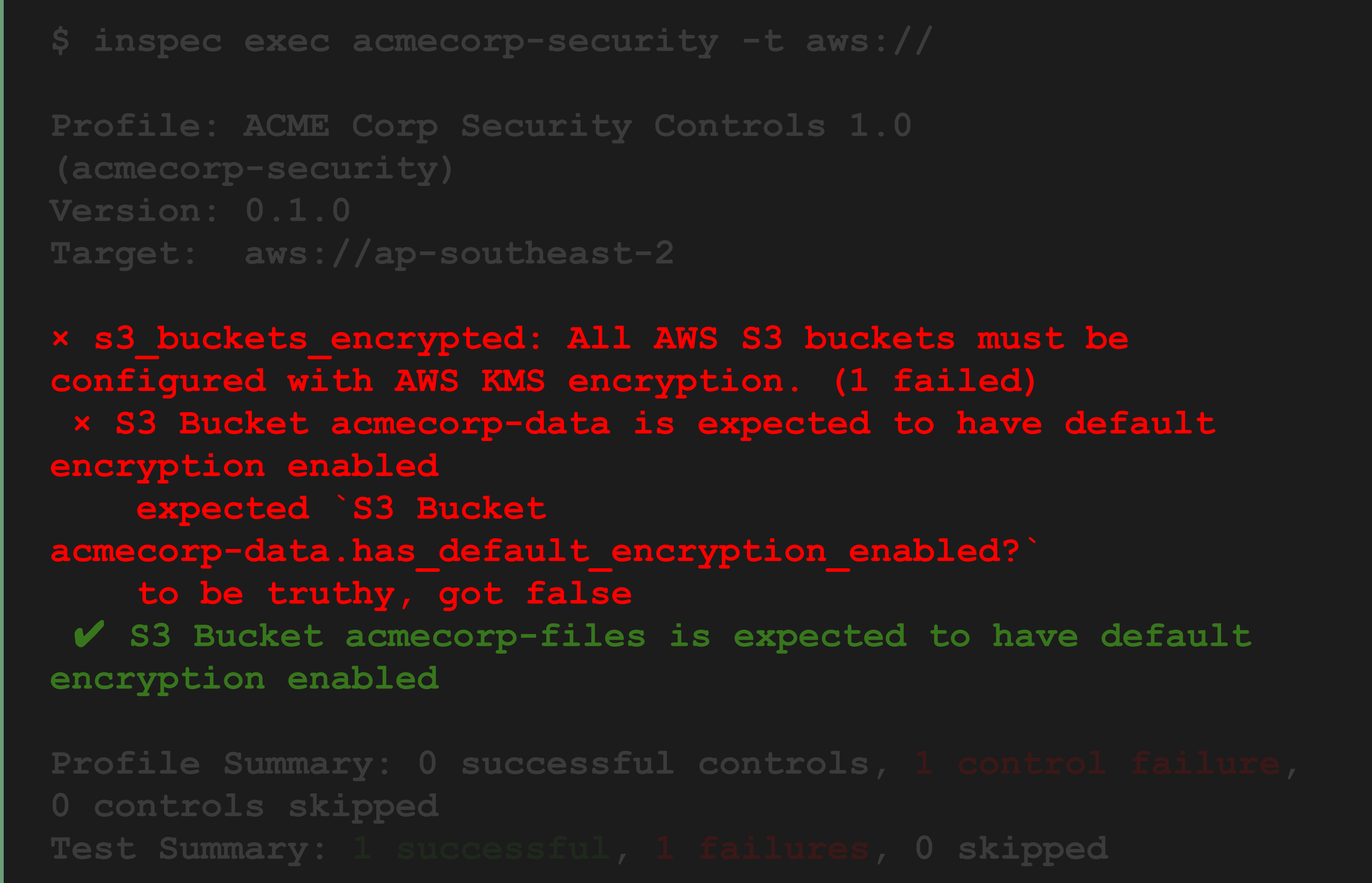
```
$ inspec exec acmecorp-security -t aws://

Profile: ACME Corp Security Controls 1.0
(acmecorp-security)
Version: 0.1.0
Target:  aws://ap-southeast-2

× s3_buckets_encrypted: All AWS S3 buckets must be
configured with AWS KMS encryption. (1 failed)
 × S3 Bucket acmecorp-data is expected to have default
encryption enabled
    expected `S3 Bucket
acmecorp-data.has_default_encryption_enabled?`
    to be truthy, got false
 ✔ S3 Bucket acmecorp-files is expected to have default
encryption enabled

Profile Summary: 0 successful controls, 1 control failure,
0 controls skipped
Test Summary: 1 successful, 1 failures, 0 skipped
```

Compliance Results



```
$ inspec exec acmecorp-security -t aws://

Profile: ACME Corp Security Controls 1.0
(acmecorp-security)
Version: 0.1.0
Target:  aws://ap-southeast-2

× s3_buckets_encrypted: All AWS S3 buckets must be
configured with AWS KMS encryption. (1 failed)
 × S3 Bucket acmecorp-data is expected to have default
encryption enabled
    expected `S3 Bucket
acmecorp-data.has_default_encryption_enabled?`
    to be truthy, got false
 ✔ S3 Bucket acmecorp-files is expected to have default
encryption enabled

Profile Summary: 0 successful controls, 1 control failure,
0 controls skipped
Test Summary: 1 successful, 1 failures, 0 skipped
```

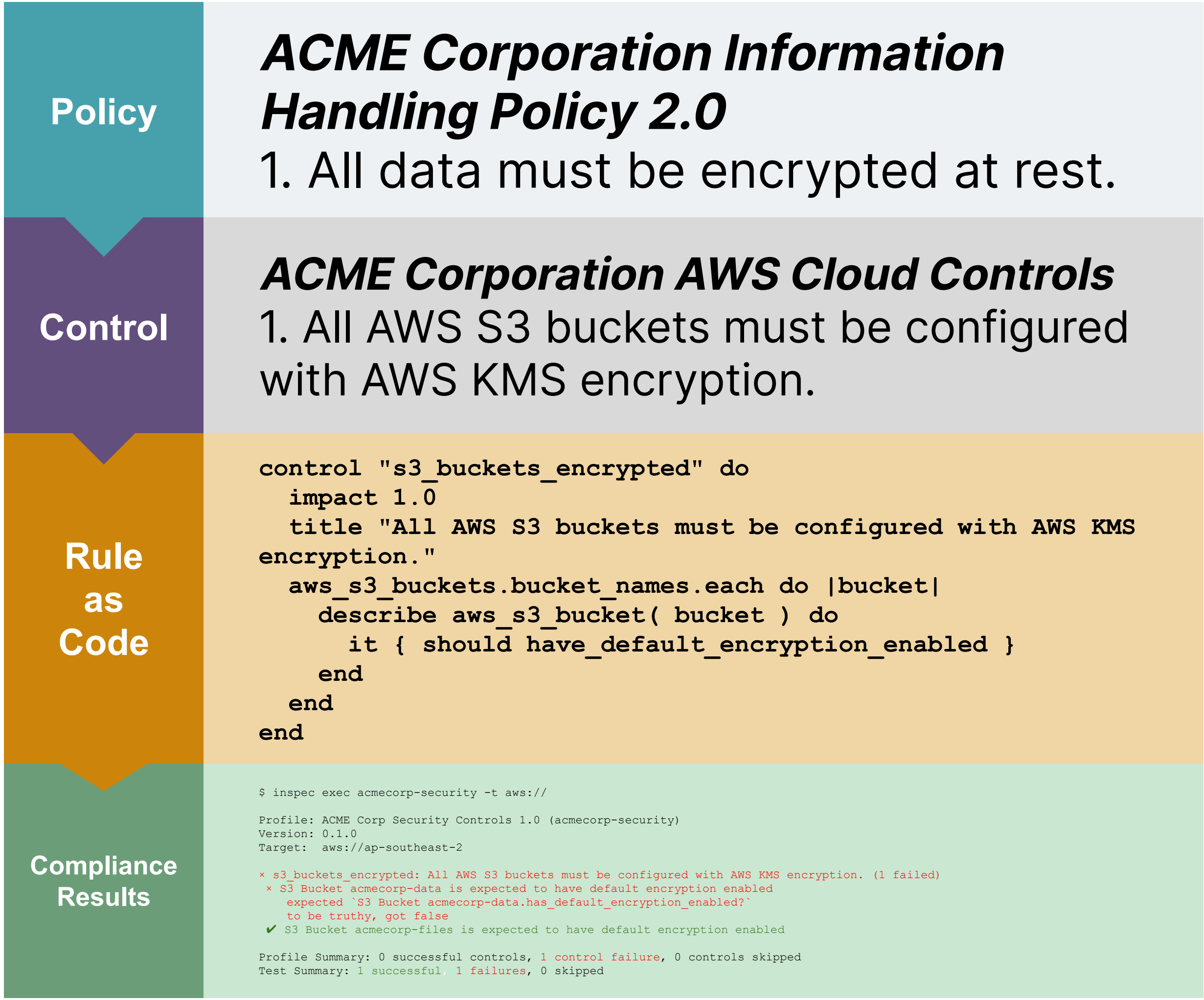
Compliance Results

```
$ inspec exec acmecorp-security -t aws://

Profile: ACME Corp Security Controls 1.0
(acmecorp-security)
Version: 0.1.0
Target:  aws://ap-southeast-2

× s3_buckets_encrypted: All AWS S3 buckets must be
configured with AWS KMS encryption. (1 failed)
 × S3 Bucket acmecorp-data is expected to have default
encryption enabled
    expected `S3 Bucket
acmecorp-data.has_default_encryption_enabled?`
    to be truthy, got false
 ✔ S3 Bucket acmecorp-files is expected to have default
encryption enabled

Profile Summary: 0 successful controls, 1 control failure,
0 controls skipped
Test Summary: 1 successful, 1 failures, 0 skipped
```



ACME Corporation Information Handling Policy 2.0

1. All data must be encrypted at rest.

ACME Corporation AWS Cloud Controls

1. All AWS S3 buckets must be configured with AWS KMS encryption.

```
control "s3_buckets_encrypted" do
  impact 1.0
  title "All AWS S3 buckets must be configured with AWS KMS
encryption."
  aws_s3_buckets.bucket_names.each do |bucket|
    describe aws_s3_bucket( bucket ) do
      it { should have_default_encryption_enabled }
    end
  end
end
```

```
$ inspec exec acmecorp-security -t aws://

Profile: ACME Corp Security Controls 1.0 (acmecorp-security)
Version: 0.1.0
Target:  aws://ap-southeast-2

× s3_buckets_encrypted: All AWS S3 buckets must be configured with AWS KMS encryption. (1 failed)
 × S3 Bucket acmecorp-data is expected to have default encryption enabled
   expected `S3 Bucket acmecorp-data.has_default_encryption_enabled?`
   to be truthy, got false
 ✔ S3 Bucket acmecorp-files is expected to have default encryption enabled

Profile Summary: 0 successful controls, 1 control failure, 0 controls skipped
Test Summary: 1 successful, 1 failures, 0 skipped
```

Handling results

- Remediation
- Collection and storage
- Alerting and feedback
- Monitoring

Handling results

- **Remediation**
- Collection and storage
- Alerting and feedback
- Monitoring

Handling results

- Remediation
- **Collection and storage**
- Alerting and feedback
- Monitoring

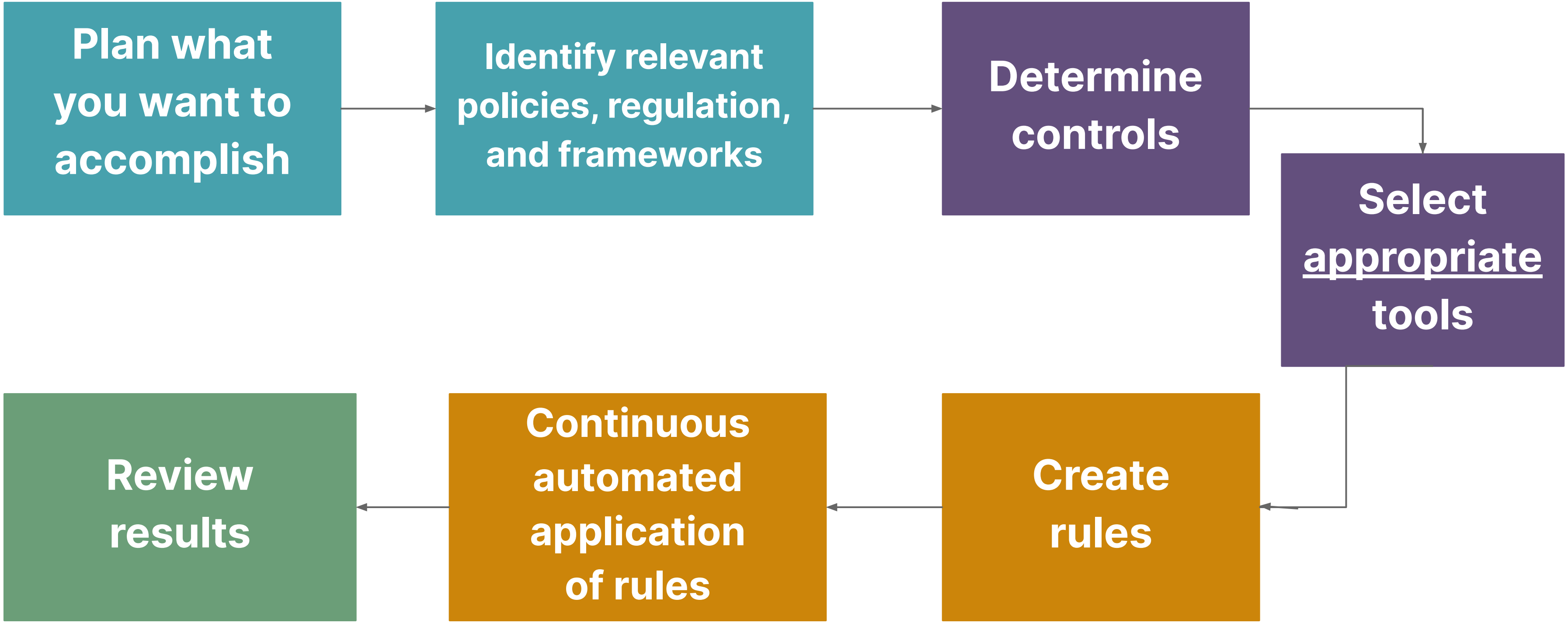
Handling results

- Remediation
- Collection and storage
- **Alerting and feedback**
- Monitoring

Handling results

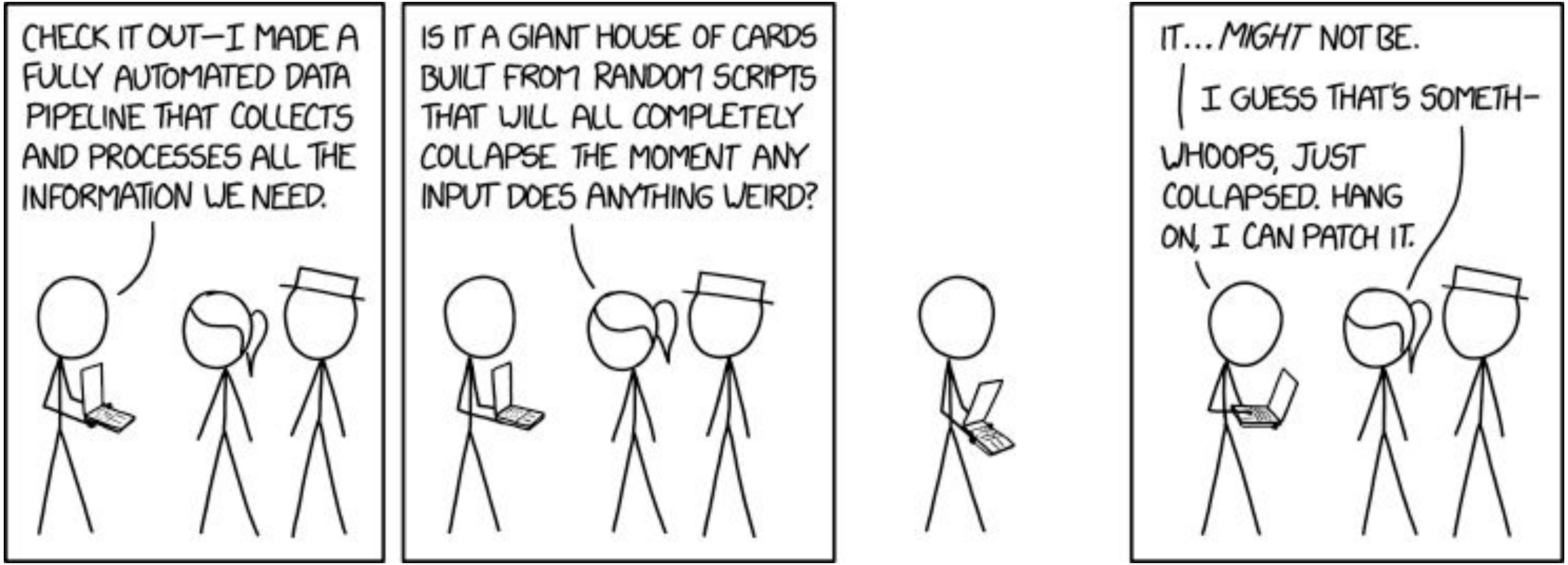
- Remediation
- Collection and storage
- Alerting and feedback
- **Monitoring**

How to get started with Compliance as Code



Plan what you want to accomplish
Identify relevant policies, regulation, and frameworks
Determine controls
Select appropriate tools
Create rules
Continuous automated application of rules
Review results

Compliance *as Code* done wrong


CHECK IT OUT—I MADE A FULLY AUTOMATED DATA PIPELINE THAT COLLECTS AND PROCESSES ALL THE INFORMATION WE NEED.
IS IT A GIANT HOUSE OF CARDS BUILT FROM RANDOM SCRIPTS THAT WILL ALL COMPLETELY COLLAPSE THE MOMENT ANY INPUT DOES ANYTHING WEIRD?
IT... MIGHT NOT BE.
I GUESS THAT'S SOMETH–
WHOOPS, JUST COLLAPSED. HANG ON, I CAN PATCH IT.

XKCD by Randall Munroe, Creative Commons BY-NC, https://xkcd.com/2054/

Compliance *as Code* done wrong

- Brittle preventative rules
- Black box compliance
- Buried compliance dashboard
- Limitation Driven Development
- Sporadic compliance

Compliance *as Code* done wrong

- **Brittle preventative rules**
- Black box compliance
- Buried compliance dashboard
- Limitation Driven Development
- Sporadic compliance

Compliance *as Code* done wrong

- Brittle preventative rules
- **Black box compliance**
- Buried compliance dashboard
- Limitation Driven Development
- Sporadic compliance

Compliance *as Code* done wrong

- Brittle preventative rules
- Black box compliance
- **Buried compliance dashboard**
- Limitation Driven Development
- Sporadic compliance

Compliance as Code done wrong

- Brittle preventative rules
- Black box compliance
- Buried compliance dashboard
- **Limitation Driven Development**
- Sporadic compliance

Compliance *as Code* done wrong

- Brittle preventative rules
- Black box compliance
- Buried compliance dashboard
- Limitation Driven Development
- **Sporadic compliance**

Key takeaways

- Build compliance in at every stage
- Don’t reinvent the wheel
- Embrace the polyglot
- Build a culture where you trust teams but verify

That's all Folks!

Questions?