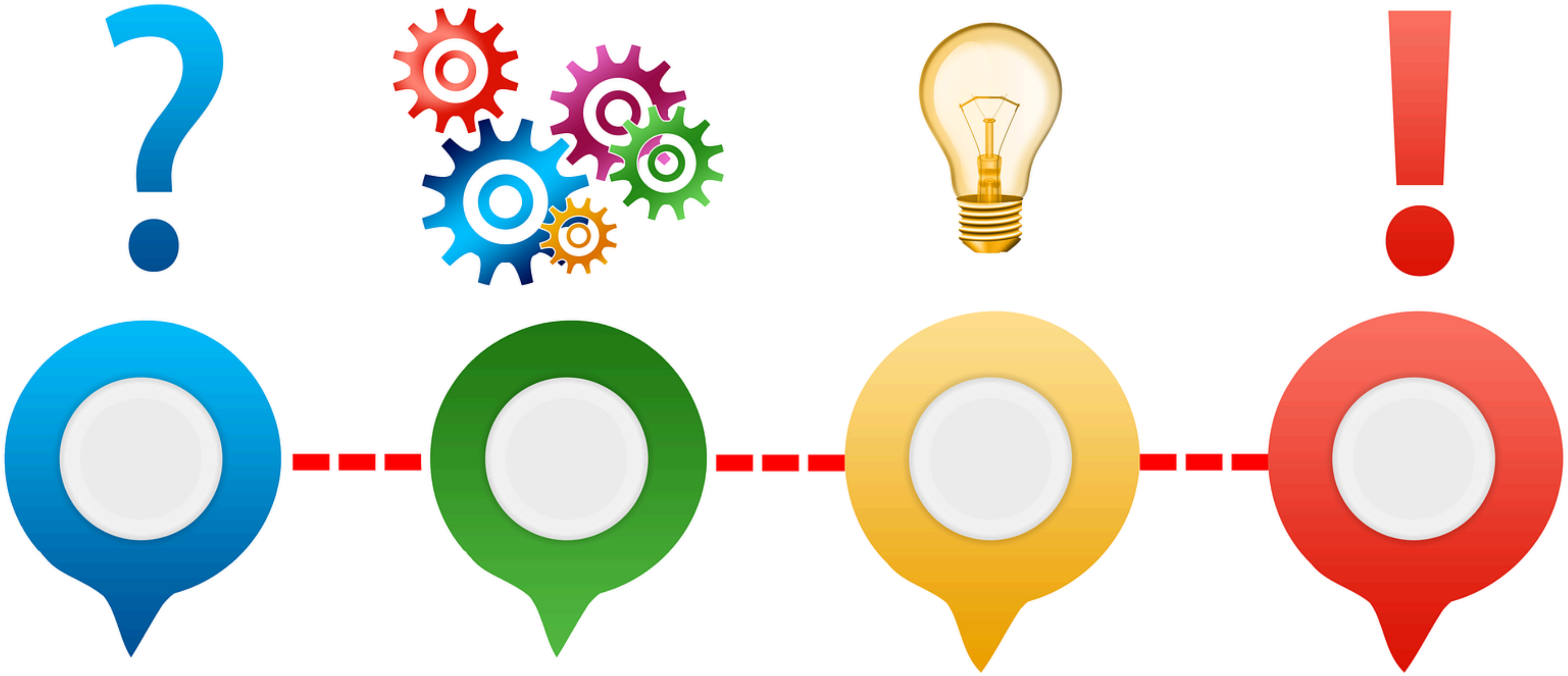
Pixabay / 4423750

Automated Governance

DB Systel
Moving the digital future. Together.

DB Systel GmbH | Schlomo Schapiro | Chief Technology Office | 12.11.2020

@schlomoschapiro



https://pixabay.com/i-3303396

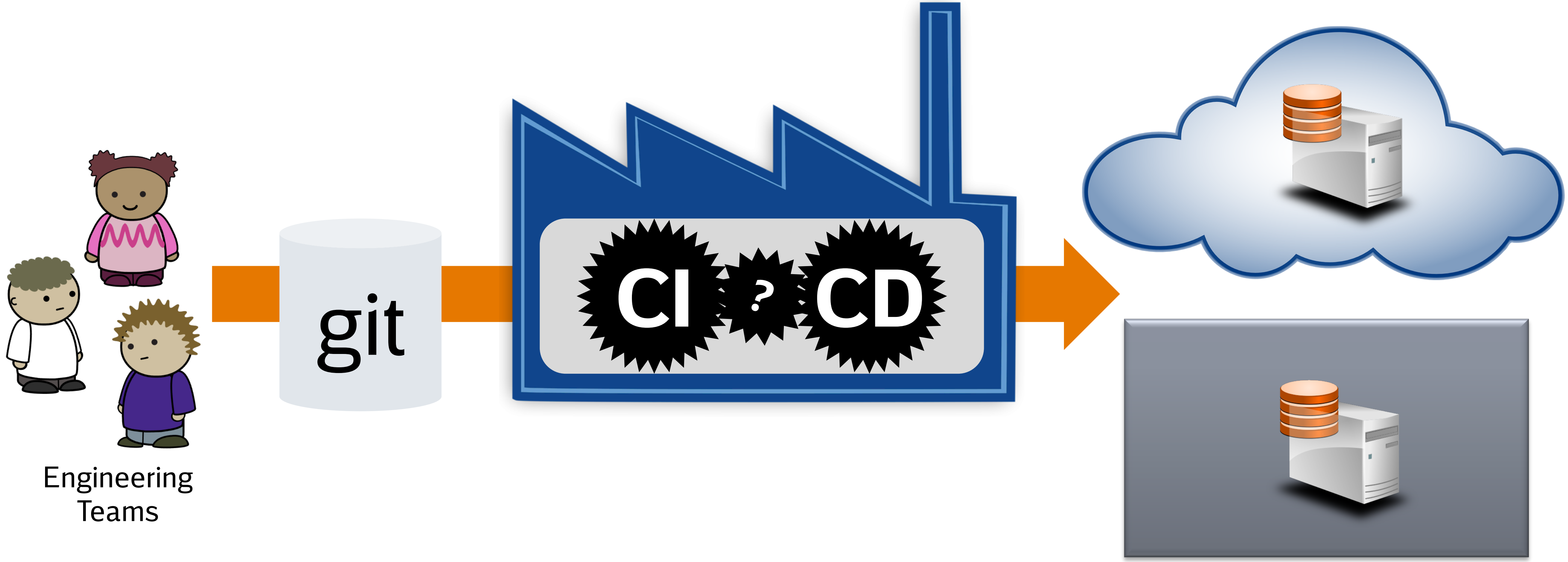
Governance

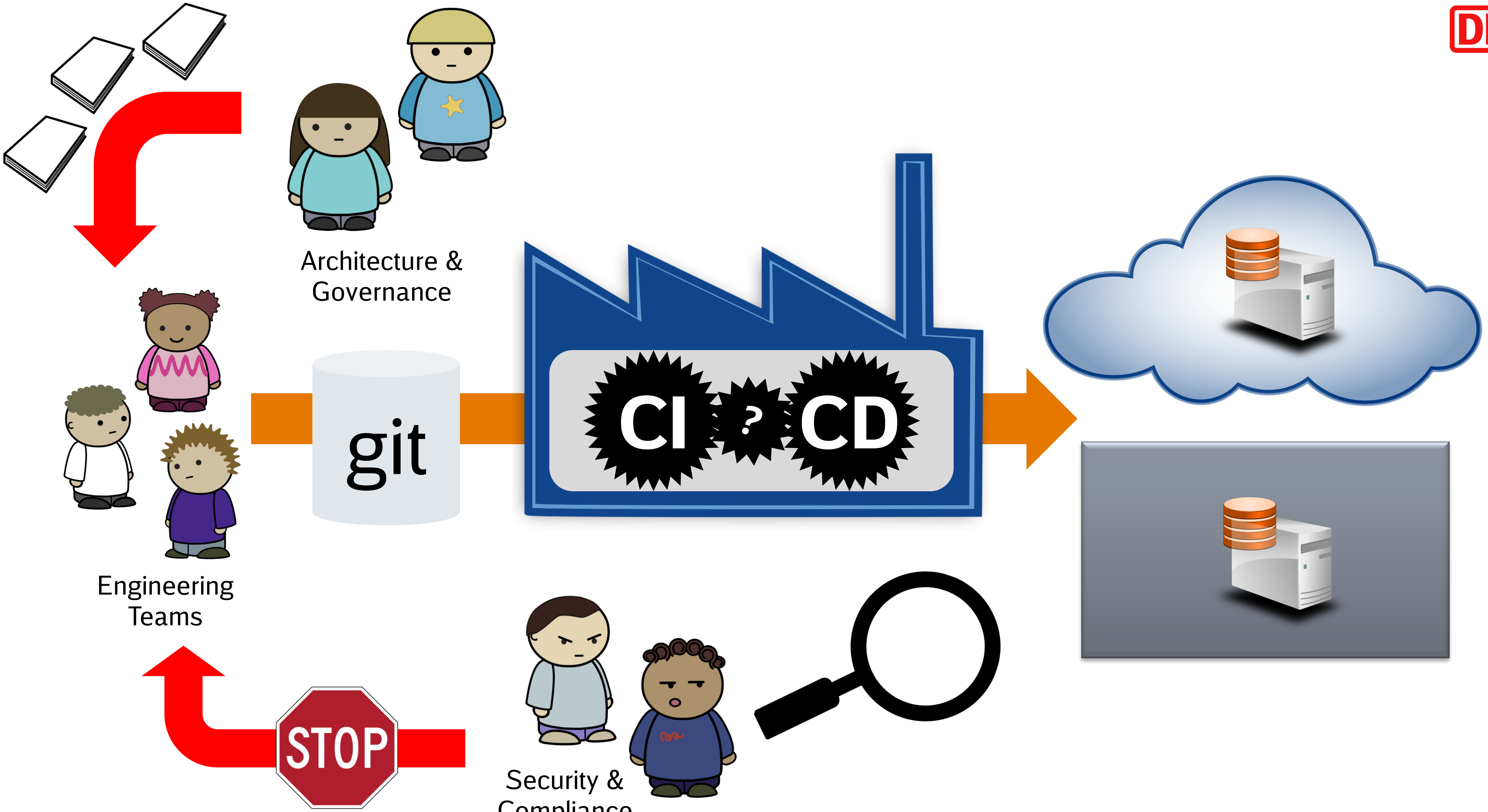
Problem?

What is governance?

- Align IT strategy with business strategy
- Make sure we **have** and **keep** rules

Happy DevOps Campers





Architecture & Governance

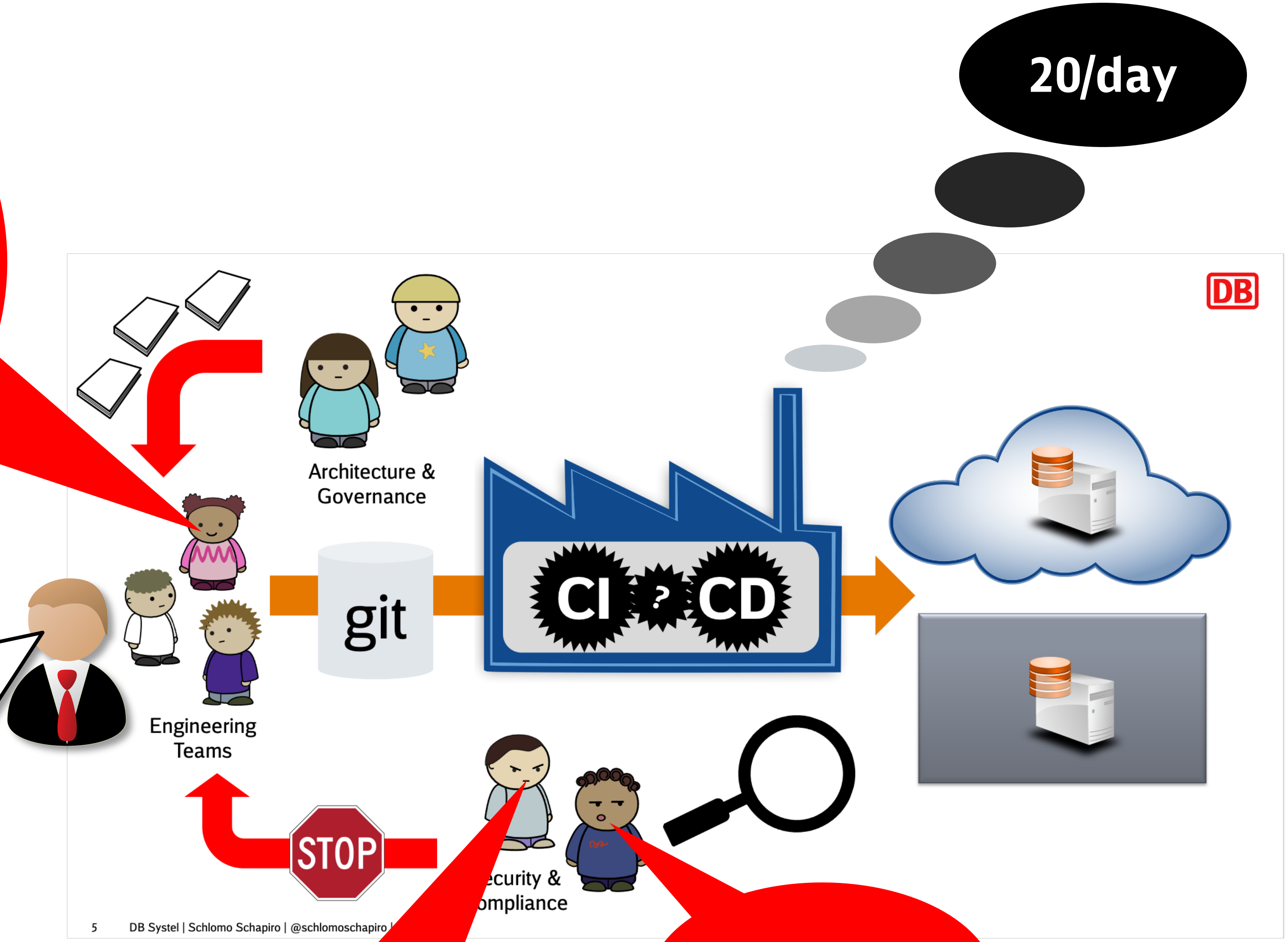
Engineering Teams

Security & Compliance

We can‘t work!

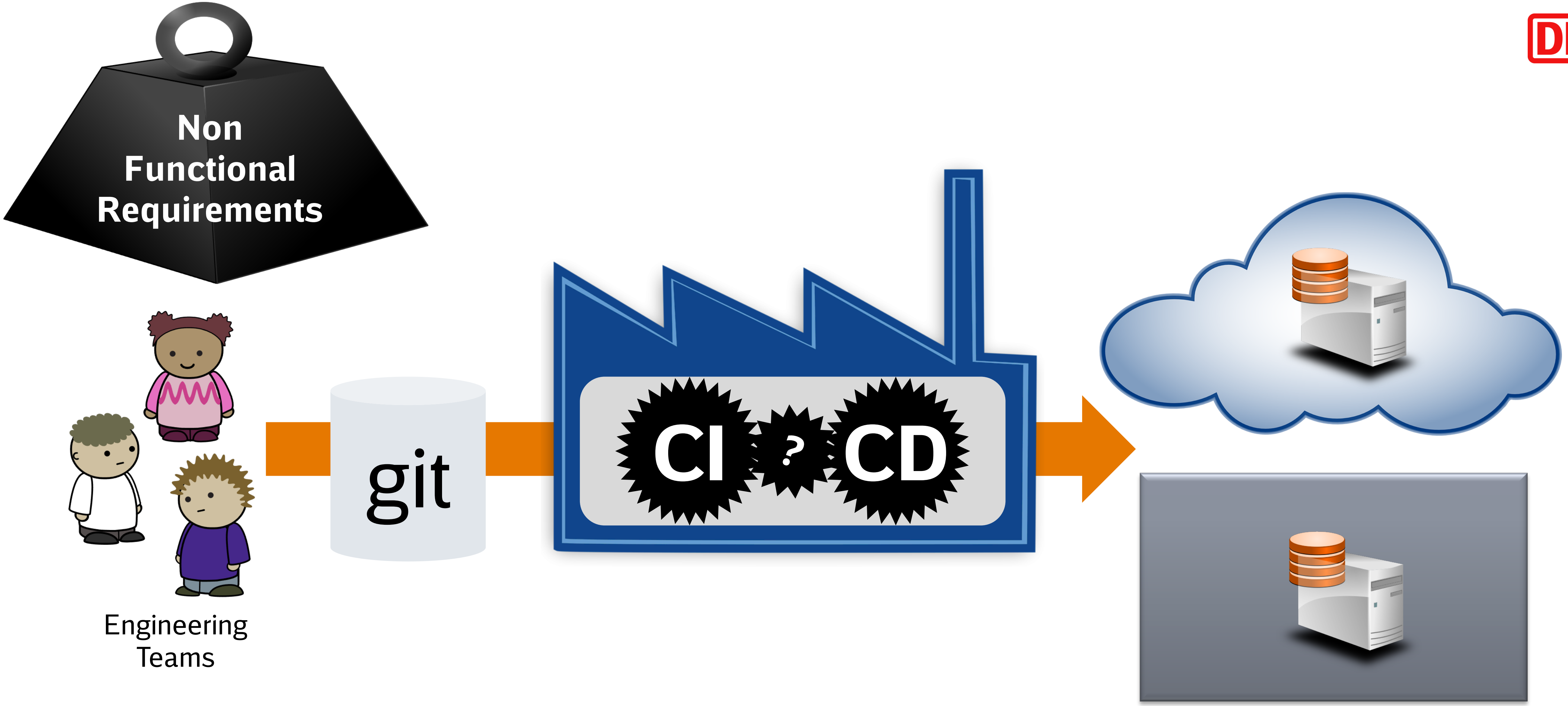
Challanges:

- Time to Market vs. Stability?
- Change Frequency vs. Risk & Security?
- Governance & Compliance?
- You build it – you run it?
- DevOps???


20/day
Architecture & Governance
git
CI ? CD
Engineering Teams
STOP
ecurity & ompliance
5 DB Systel | Schlomo Schapiro | @schlomoschapiro

We can´t check everything!

20 / day / team ???

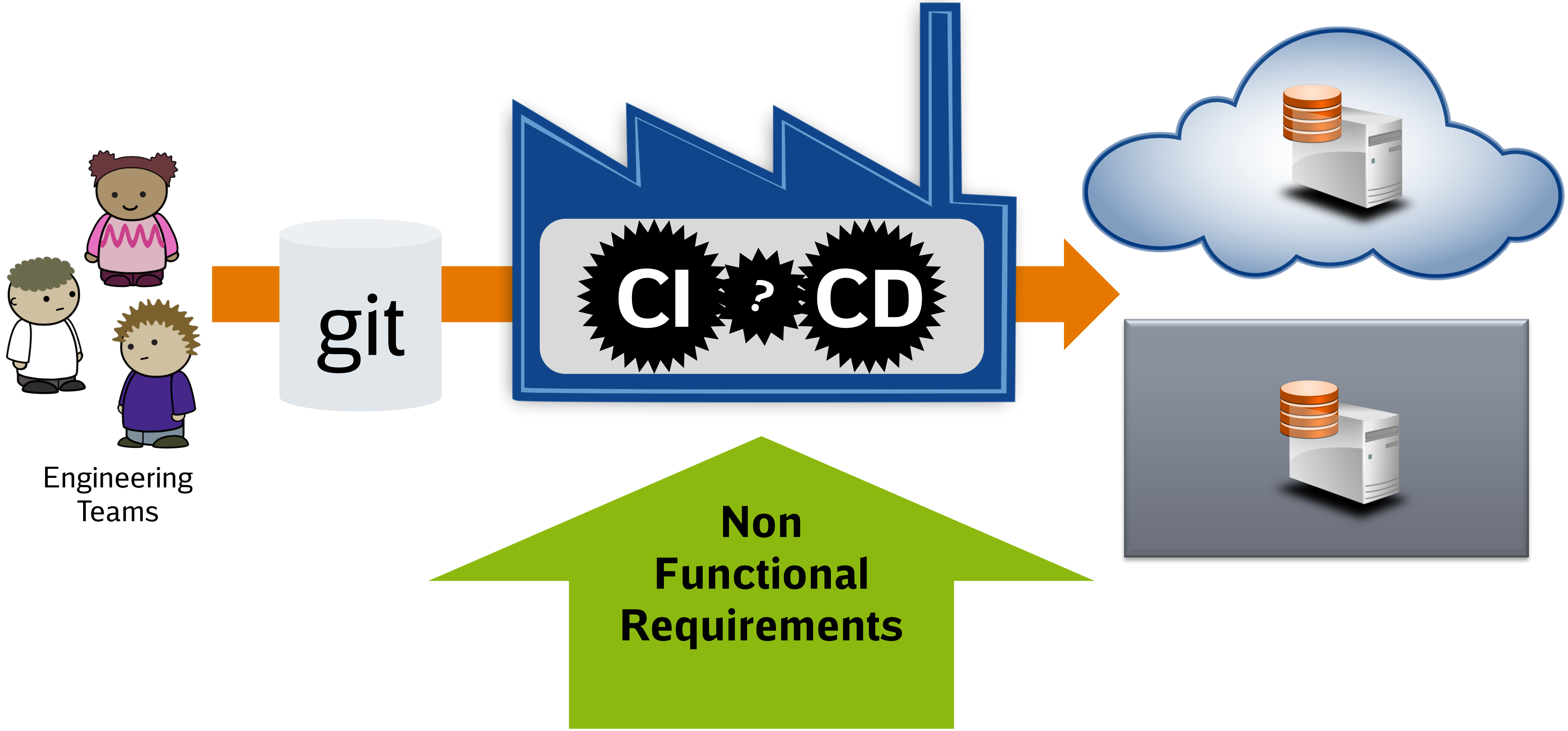


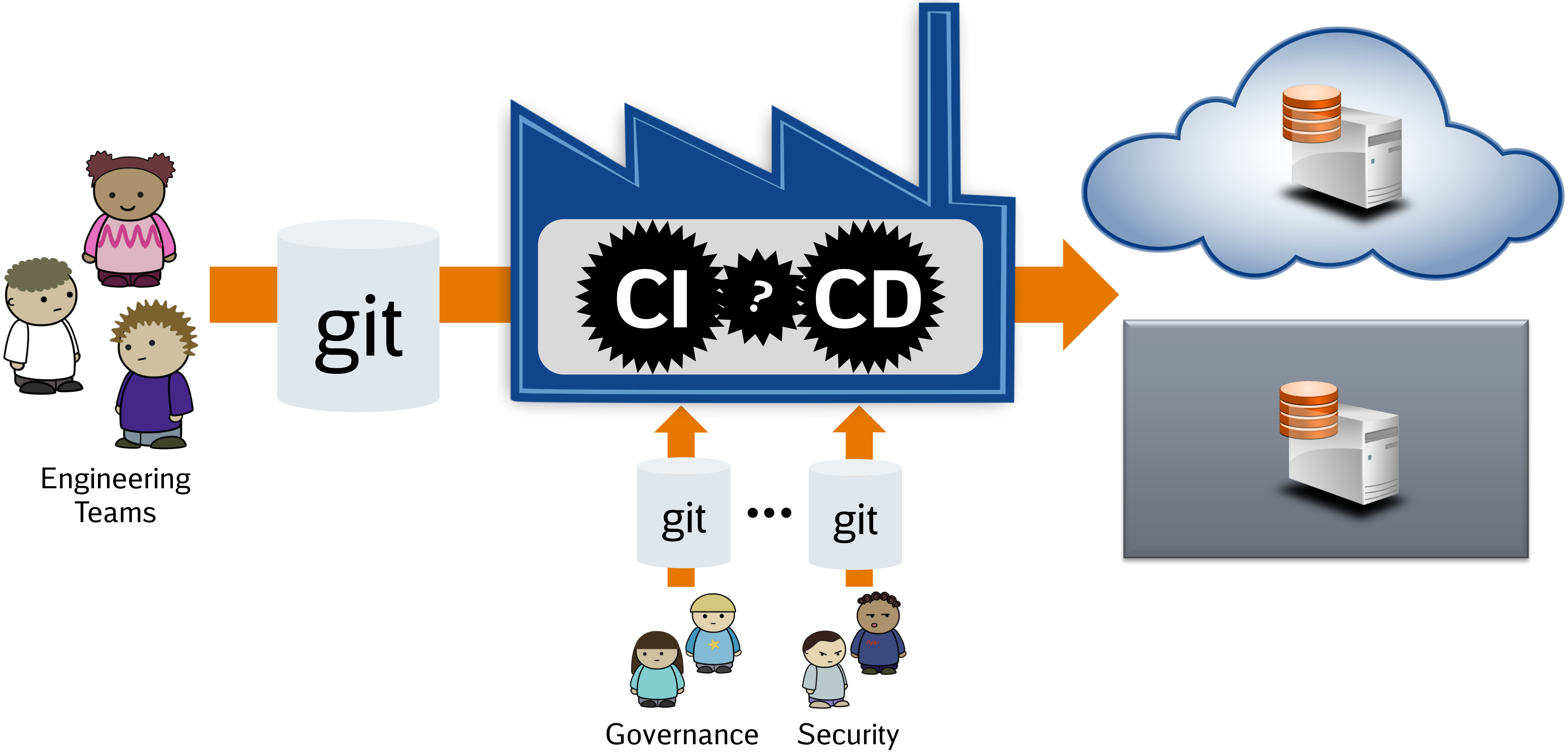
Non Functional Requirements

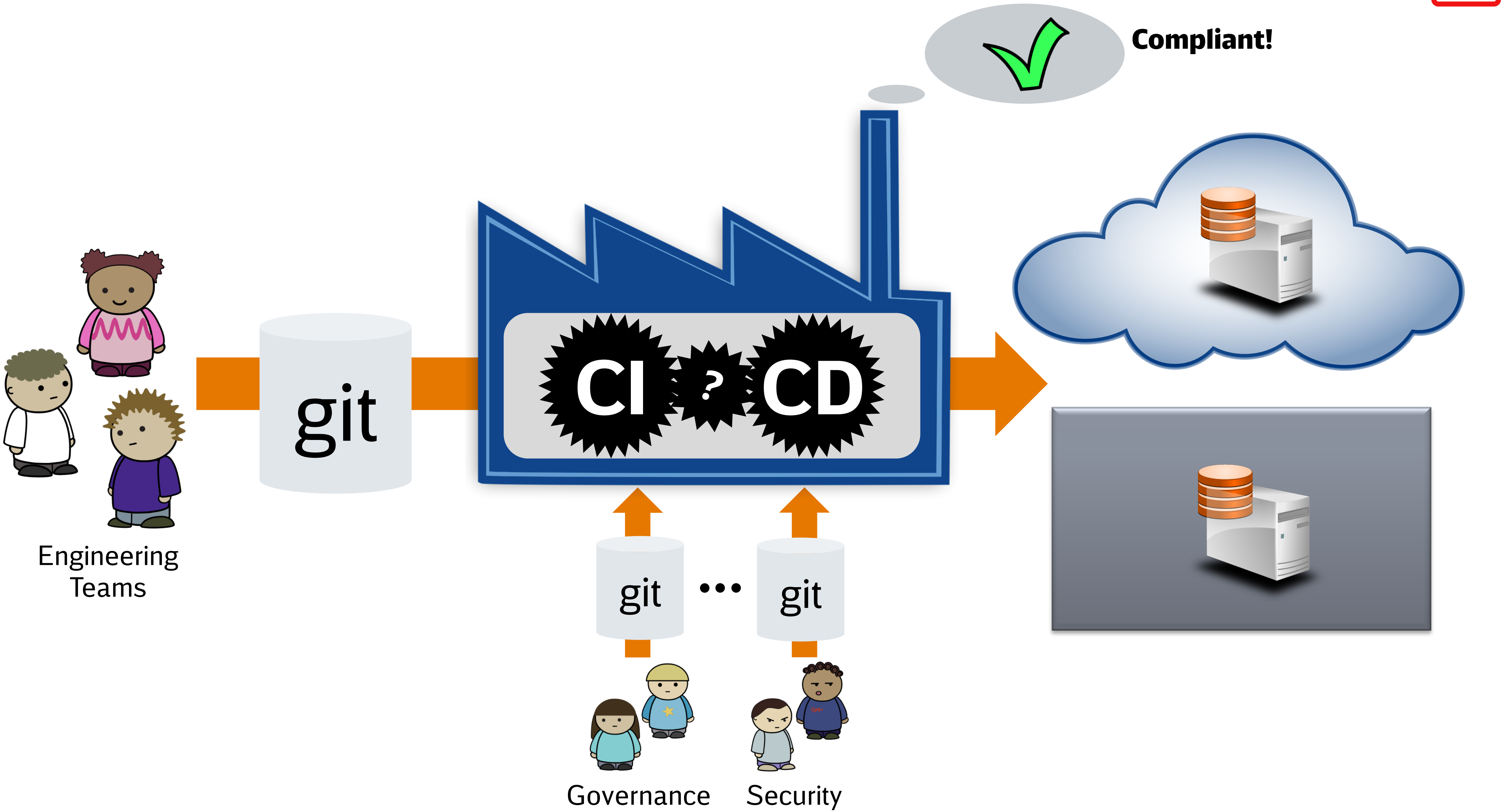
Engineering Teams

git

CI ? CD


Engineering Teams
git
CI
?
CD
Non Functional Requirements


Engineering Teams
git
CI
?
CD
git
•••
git
Governance
Security



Compliant!

Engineering Teams

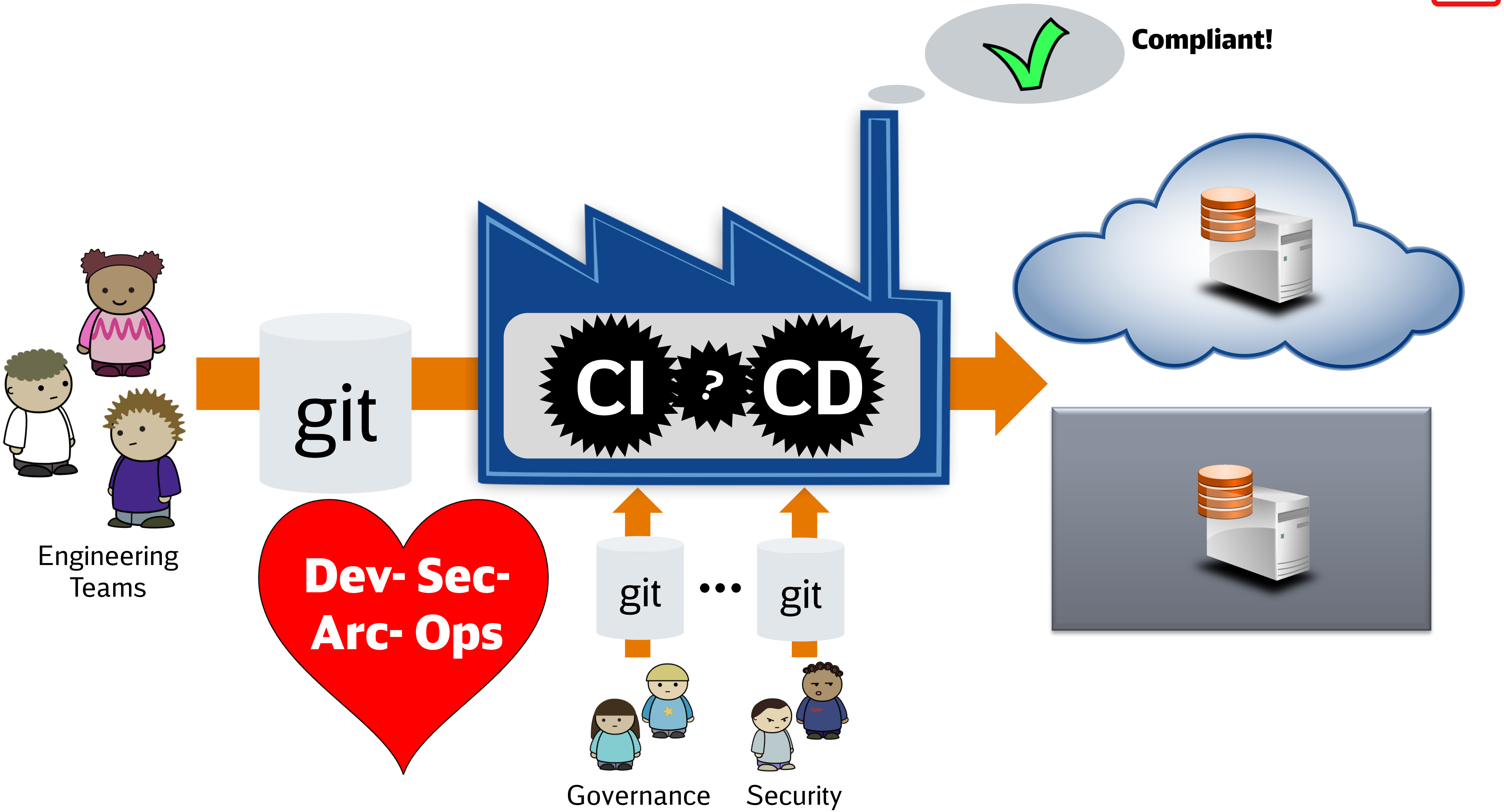
git

CI ? CD

git ••• git

Governance

Security



Engineering Teams

git

Dev- Sec- Arc- Ops

CI ? CD

git ••• git

Governance

Security

Compliant!

Automated

What is automated?

- „operated automatically“
- Synonyms: automatic, laborsaving, robotic, self-acting, self-operating, self-regulating
- Not people doing it manually

Source: https://www.merriam-webster.com/dictionary/automated

Compliance Automation is Very Hard!

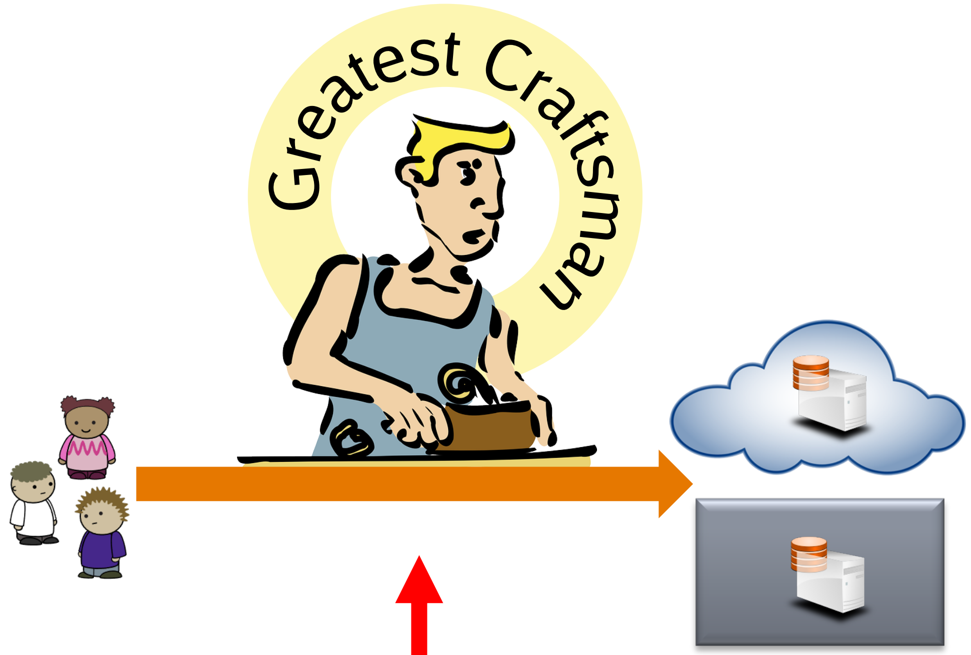
Governance

Problem?
What is governance?

- Align IT strategy with business strategy
- Make sure we **have** and **keep** rules

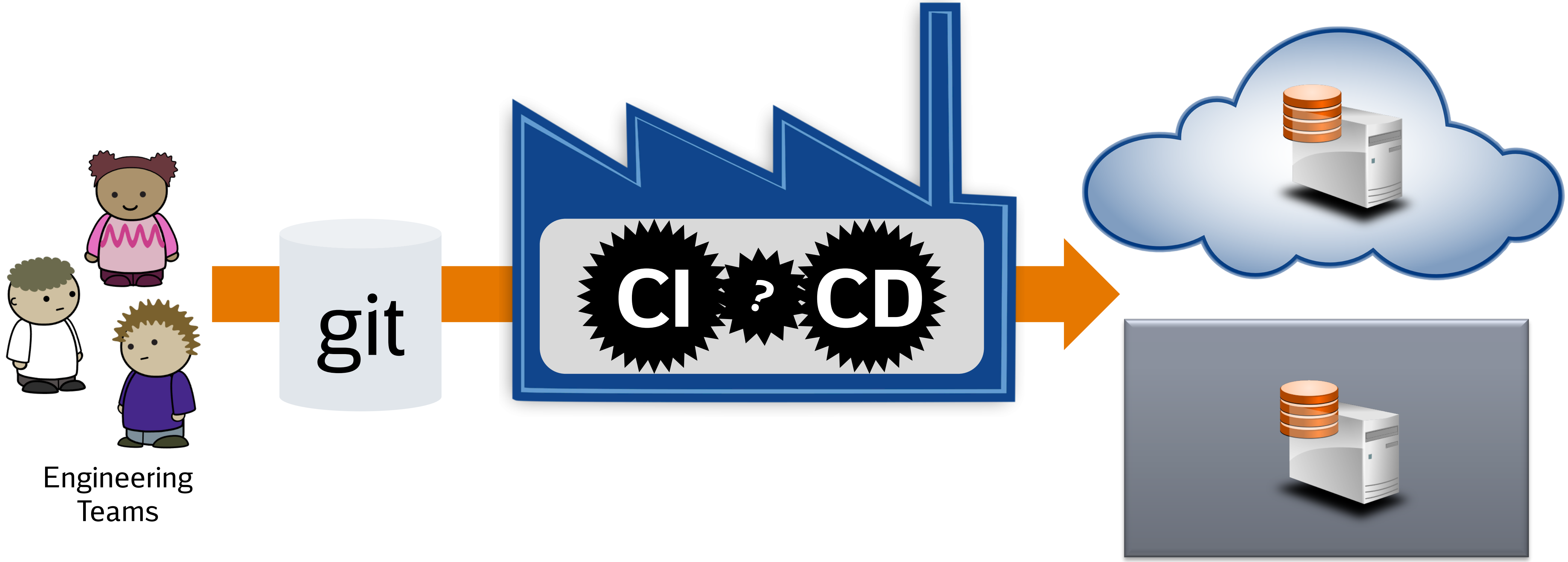
3 DB Systel | Schlomo Schapiro | @schlomoschapiro | 13-14.11.2019

Automation friendly?

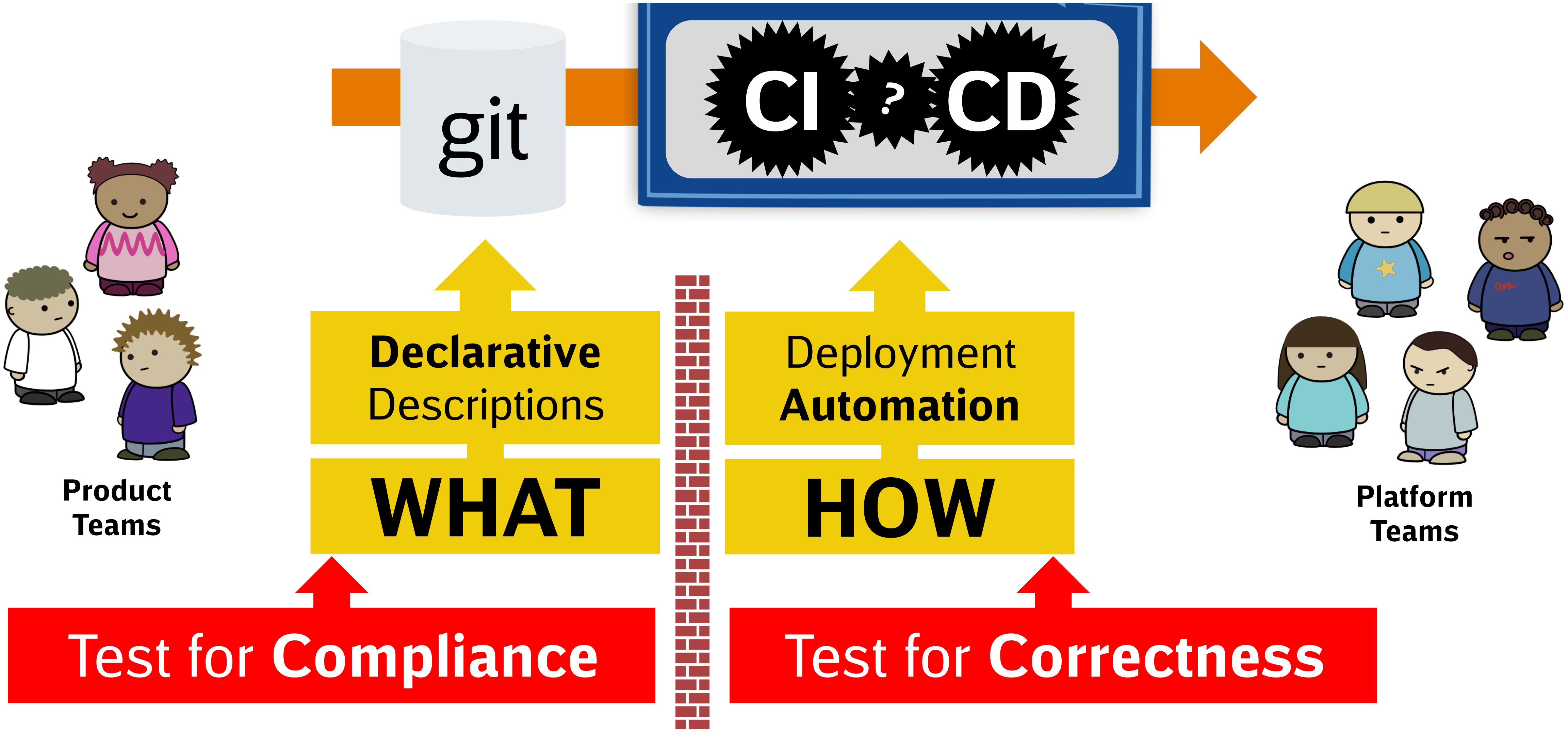


How to check?

GitOps to the Rescue



GitOps to the Rescue



Product Teams

Declarative Descriptions

WHAT

Test for **Compliance**

Deployment **Automation**

HOW

Test for **Correctness**

Platform Teams

Declarative Descriptions Example

gitlab-ci.yaml

Source: https://docs.gitlab.com/ee/ci/examples/deployment/composer-npm-deploy.html

```
stage_deploy:
  script:
    - ssh user@host "mkdir htdocs/_tmp"
    - scp -r build/* user@host:htdocs/_tmp
    - ssh user@host "mv htdocs/live htdocs/_old && mv htdocs/_tmp htdocs/live"
    - ssh user@host "rm -rf htdocs/_old"
```

config.properties

```
TARGET=user@host
SRC=build
DIR=htdocs
NAME=live
```

Docker Image deploy_with_ssh ENTRYPOINT

```
#!/bin/bash
source "$1"
ssh $TARGET "mkdir $DIR/_tmp"
scp -r $SRC/* "$TARGET:$DIR/_tmp"
ssh $TARGET "mv $DIR/$NAME $DIR/_old && mv $DIR/_tmp $DIR/$NAME"
ssh $TARGET "rm -rf $DIR/_old"
```

gitlab-ci.yaml

```
stage_deploy:
  image: deploy_with_ssh
  script: config.properties
```

Test for **Compliance**

Test for **Correctness**

Declarative Descriptions Example

gitlab-ci.yaml

Source: https://docs.gitlab.com/ee/ci/examples/deployment/composer-npm-deploy.html

```
stage_deploy:
  script:
    - ssh user@host "mkdir ht          p"
    - scp -r build/* user@h          cs/_tmp
    - ssh user@host "mv           ve htdocs/_old &&           cs/_tmp htdocs/live"
    - ssh user@host "r           ocs/_old"
```

Config (What)

Code (How)

config.properties

```
TARGET=user@
SRC=build
DIR=htdocs
NAME=live
```

Docker Image deploy_with_ssh EN

```
#!/bin/bash
source "$1"
ssh $TARGET "mkdir $DIR/_tmp"
scp -r $SRC/* "$TARGET:$DIR/_tmp"
ssh $TARGET "mv $DIR/$NAME $DIR/_old && mv $DIR/_tmp $DIR/$NAME"
ssh $TARGET "rm -rf $DIR/_old"
```

gitlab-ci.yaml

```
stage_deploy:
  image: deploy_with_ssh
  script: config.properties
```

Test for **Compliance**

Test for **Correctness**

Declarative Descriptions → Automated Governance

Config

Cloud Formation

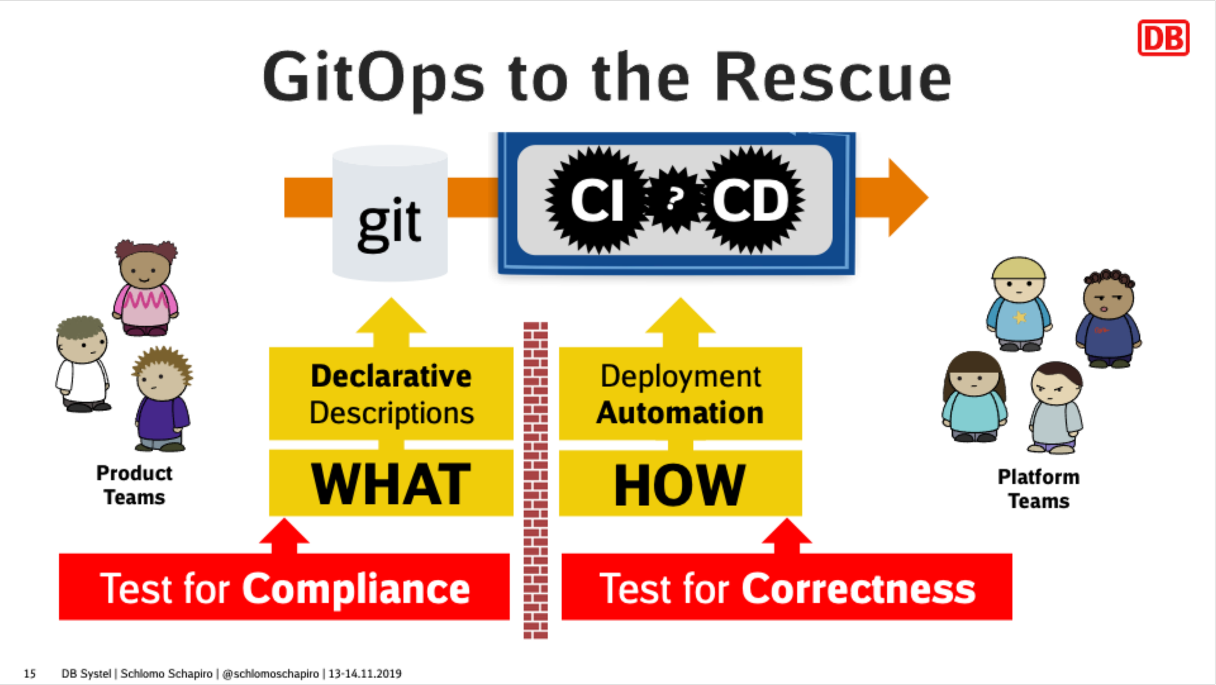
Kubernetes Manifest

Swagger YAML

Terraform YAML

AndroidManifest.xml

…



GitOps to the Rescue

git

CI ? CD

Product Teams

Declarative Descriptions

WHAT

Deployment **Automation**

HOW

Platform Teams

Test for **Compliance**

Test for **Correctness**

15 DB Systel | Schlomo Schapiro | @schlomoschapiro | 13-14.11.2019

Tools

aws cf create

kubectl apply

…

Test Strategy

Linting

Static Code Analysis

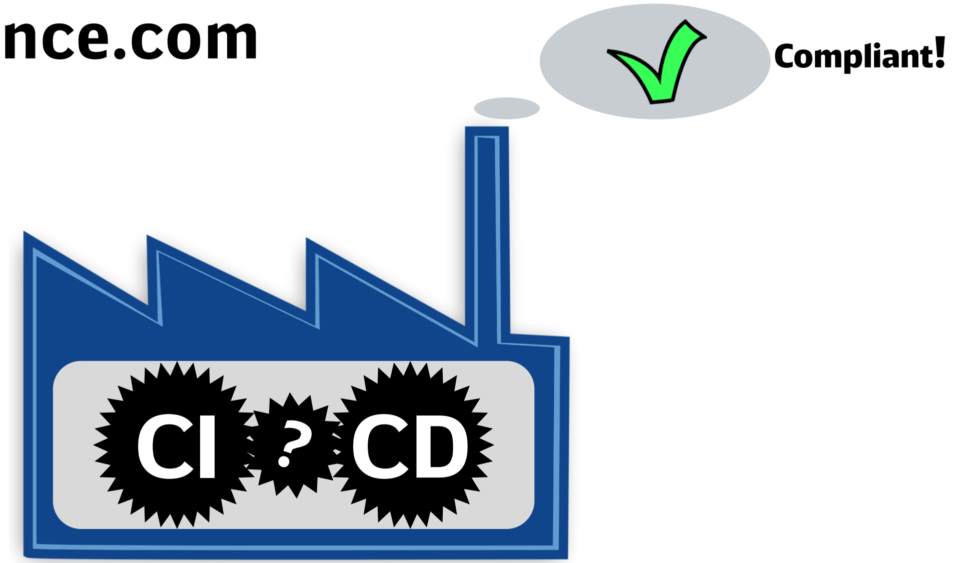
Unit Tests

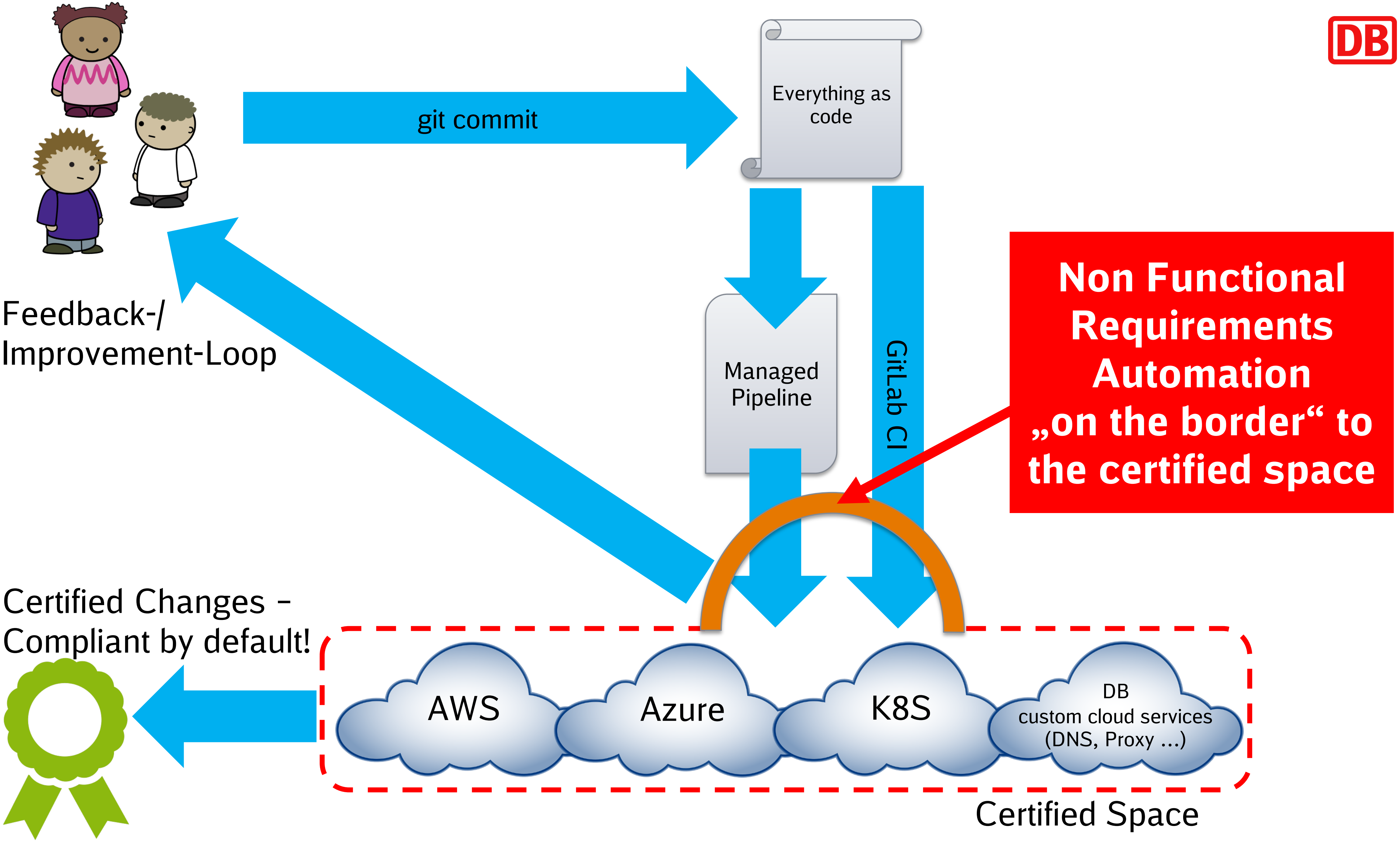
Integration Tests

Declarative Descriptions → Automated Governance

Config	Compliance Check	Tools
Cloud Formation	**cfn-nag: Linting tool for CloudFormation templates**	aws cf create
Kubernetes Manifest	**K8S Admission Controller / OPA Gatekeeper**	kubectl apply
Swagger YAML	**zally: A minimalistic, simple-to-use API linter**	…
Terraform YAML	**terraform-compliance.com**	
AndroidManifest.xml	**. . .**	
…		

Automated Compliance Checks as Quality Gate for Deployments





git commit

Everything as code

Managed Pipeline

GitLab CI

Feedback-/ Improvement-Loop

Non Functional Requirements Automation „on the border“ to the certified space

Certified Changes – Compliant by default!

AWS

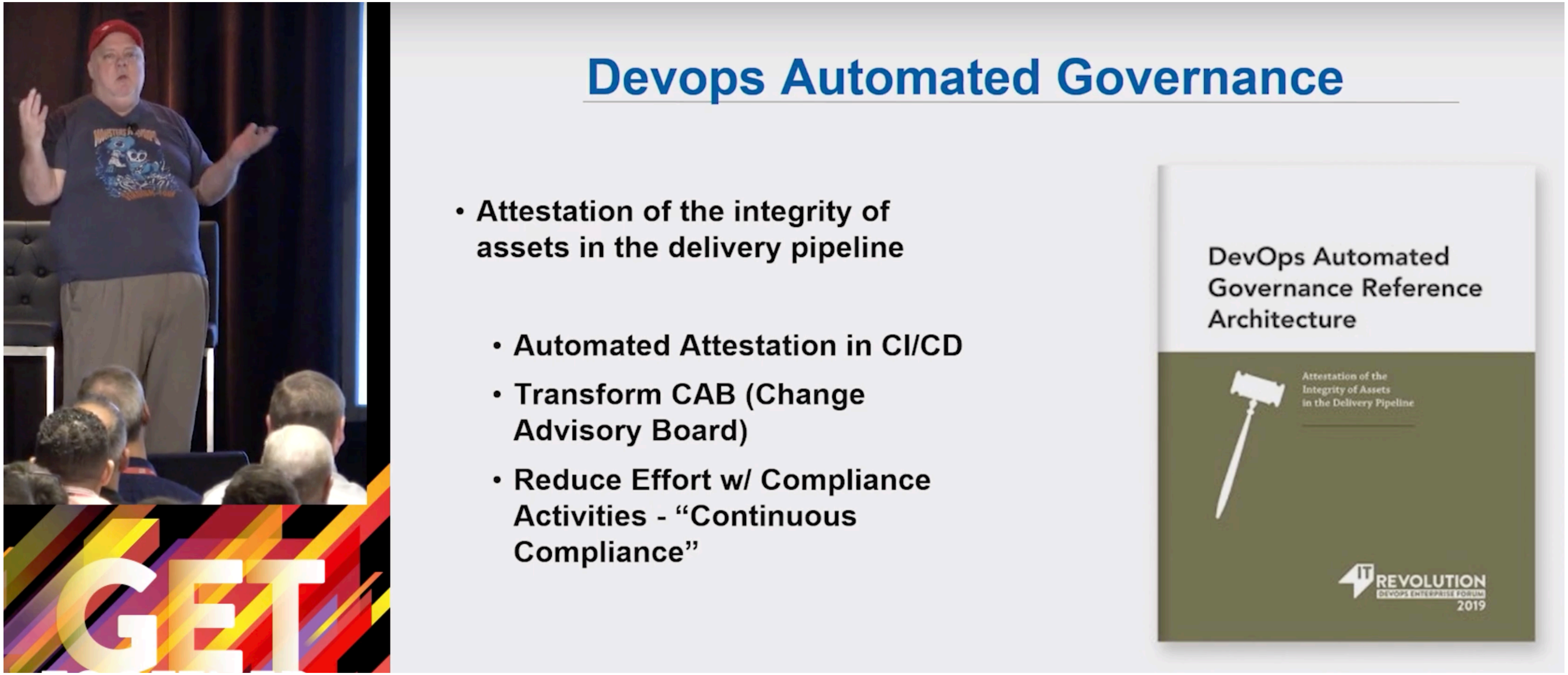
Azure

K8S

DB custom cloud services (DNS, Proxy ...)

Certified Space

DevOps' Seven Deadly Diseases - John Willis



Devops Automated Governance

- Attestation of the integrity of assets in the delivery pipeline
  - Automated Attestation in CI/CD
  - Transform CAB (Change Advisory Board)
  - Reduce Effort w/ Compliance Activities - "Continuous Compliance"

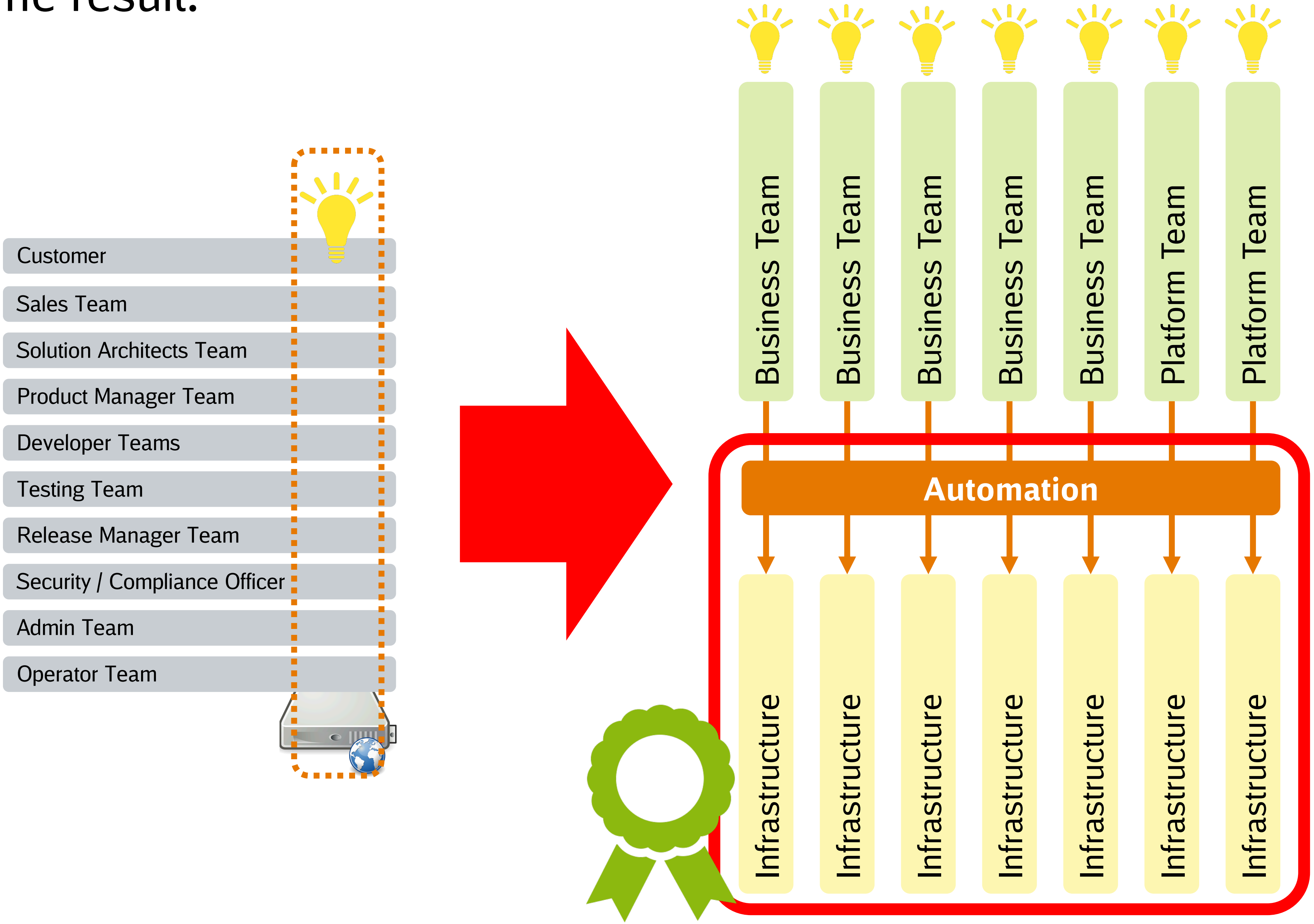
DevOps Automated Governance Reference Architecture

Attestation of the Integrity of Assets in the Delivery Pipeline

IT REVOLUTION
DEVOPS ENTERPRISE FORUM
2019

https://youtu.be/jdN3E9OwFoE
https://itrevolution.com/book/devops-automated-governance-reference-architecture/

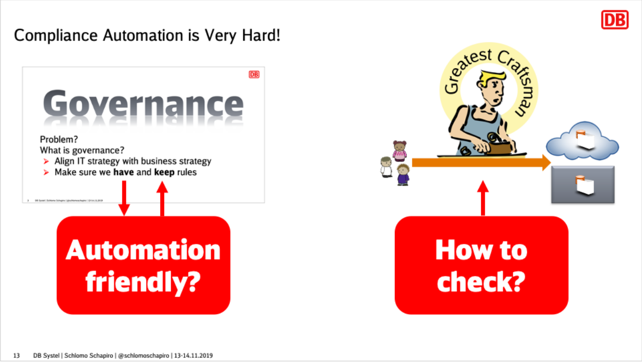
The result:



DevOps
+
Continuous Delivery
+
Cloud Platforms

Compliant by default!

Summary: Compliant by Default!



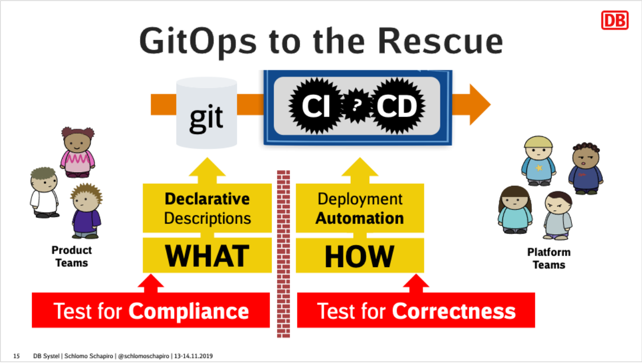
Compliance Automation is Very Hard!

Governance

Problem?
What is governance?

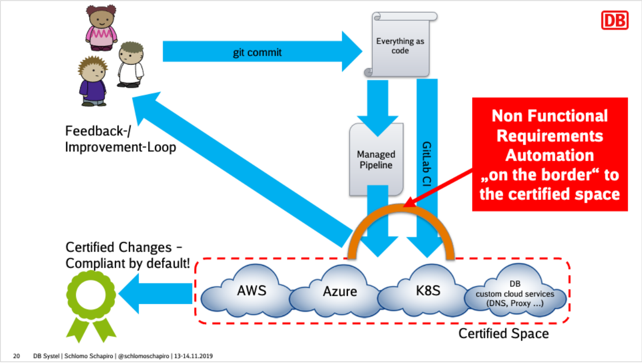
- Align IT strategy with business strategy
- Make sure we **have** and **keep** rules

13 DB Systel | Schlomo Schapiro | @schlomoschapiro | 13-14.11.2019



GitOps to the Rescue

15 DB Systel | Schlomo Schapiro | @schlomoschapiro | 13-14.11.2019



git commit
Everything as code
Managed Pipeline
GitLab CI
Feedback-/ Improvement-Loop
Certified Changes – Compliant by default!
AWS
Azure
K8S
DB custom cloud services (DNS, Proxy …)
Certified Space

Non Functional Requirements Automation „on the border“ to the certified space

20 DB Systel | Schlomo Schapiro | @schlomoschapiro | 13-14.11.2019

1. **Think in Code: Build Tools**
2. **Craft precise policies: Easy to automate checks**
3. **Production is Your Certified Space**
4. **Every Change in Production Starts in git**
5. **Declarative Descriptions**

Vielen Dank für Ihre Aufmerksamkeit