Can we Shift-left security in a CD Pipeline?

Taco Bakker, IT Area Lead Continuous Delivery ING

QCon London, March 4th 2019

ING


Craftsmanship

Can we Shift-left security in a CD Pipeline?

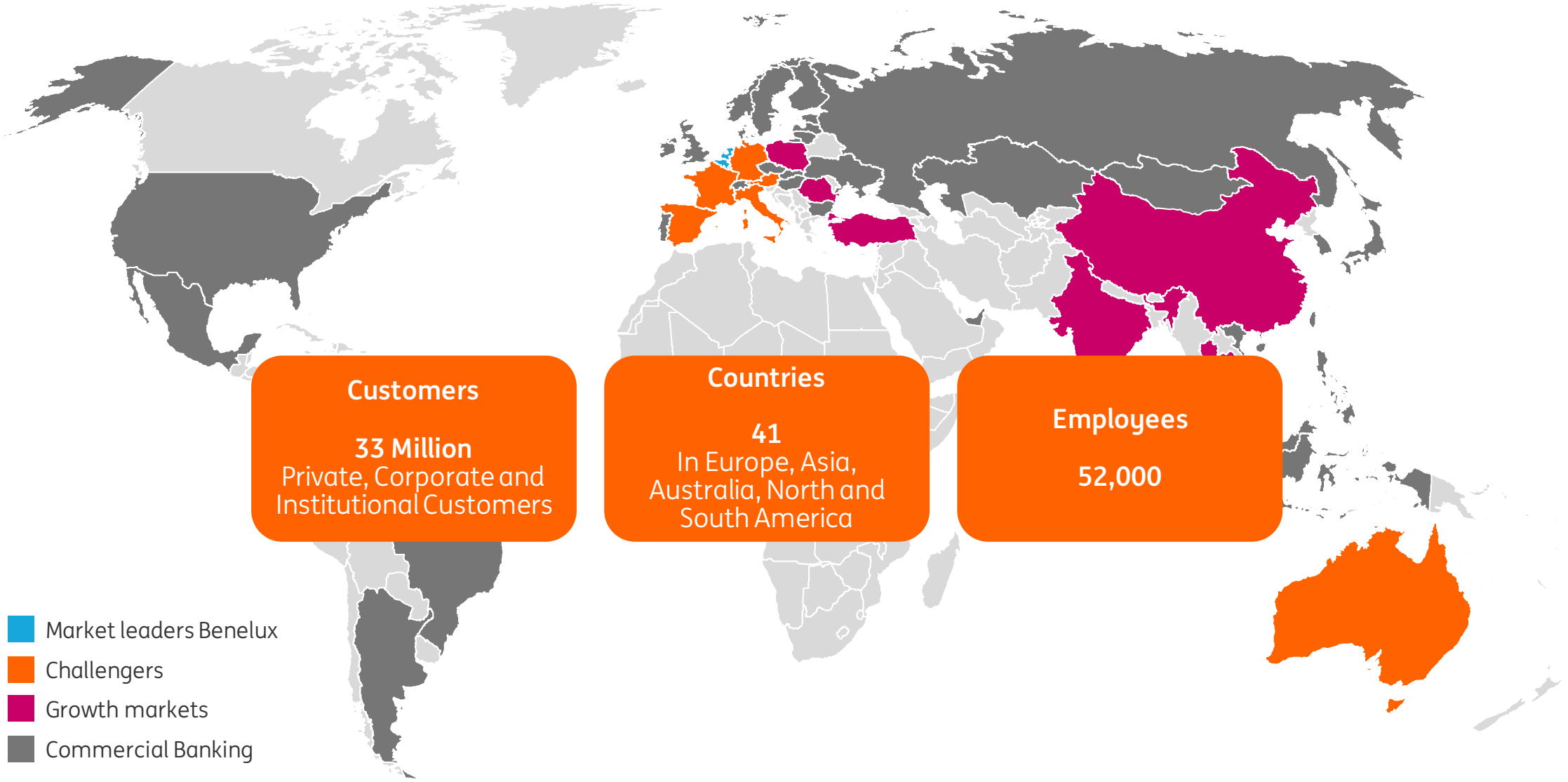
Yes we can!

ING

About me

this.name = “Taco Bakker”;
this.company = “ING”;
this.jobtitle = “IT Area Lead Continuous Delivery”;
this.expertise = {“DevOps”,”Continuous Delivery”,”Lean Six Sigma”};
this.hobby = {“travel”,”photography”};
This.responsibility = “Roll out standard CD pipeline for all IT engineers of ING worldwide”;

ING is a top financial enterprise, operating since 1881



Customers

33 Million
Private, Corporate and Institutional Customers

Countries

41
In Europe, Asia, Australia, North and South America

Employees

52,000

ING is an IT company with a Banking Licence

Agile/Scrum and DevOps are becoming a commodity in many companies

Accelerate Software Delivery is an important reason for adopting Agile

Reasons for Adopting Agile

The reasons stated for adopting agile follow a similar ranking as in the previous year though we did see the biggest change in responses in accelerate software delivery (75% compared to 69% last year), enhancing delivery predictability (46% compared to 30% last year), improving IT/Business alignment (49% compared to 42% last year), and reducing project cost (24% compared to 18% last year).

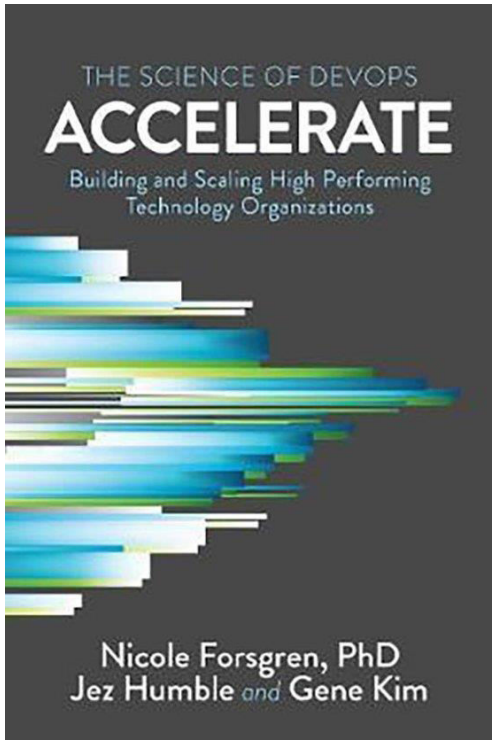
*Respondents were able to make multiple selections.

the 12th annual STATE OF AGILE™ REPORT

ING

Having Dev and Ops working together on a common purpose increases performance

*"The findings from our research program show clearly that the **value** of adopting **DevOps** is even **larger** than we had initially thought, and the gap between **high performers** and low performers continues to grow."*



Been there, done that, got the T-shirt!

DevOps is probably the first step of a journey

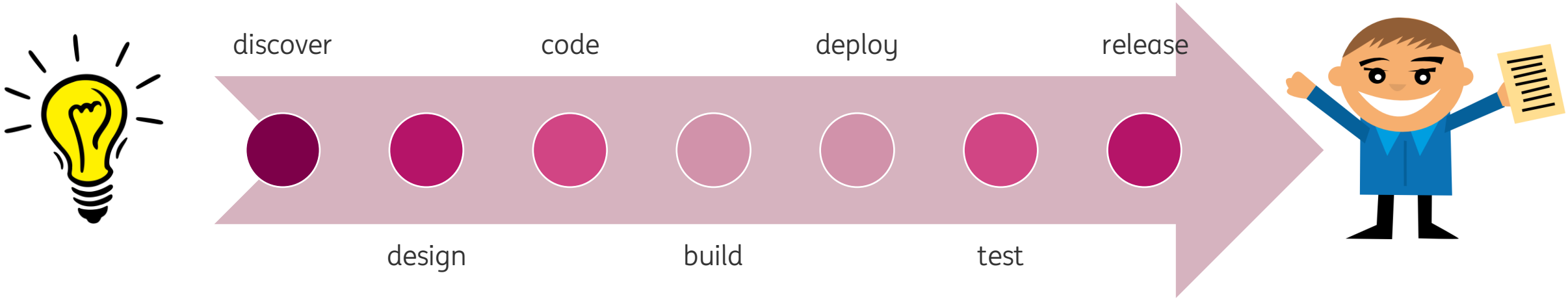
DevOps

BizzDevOps

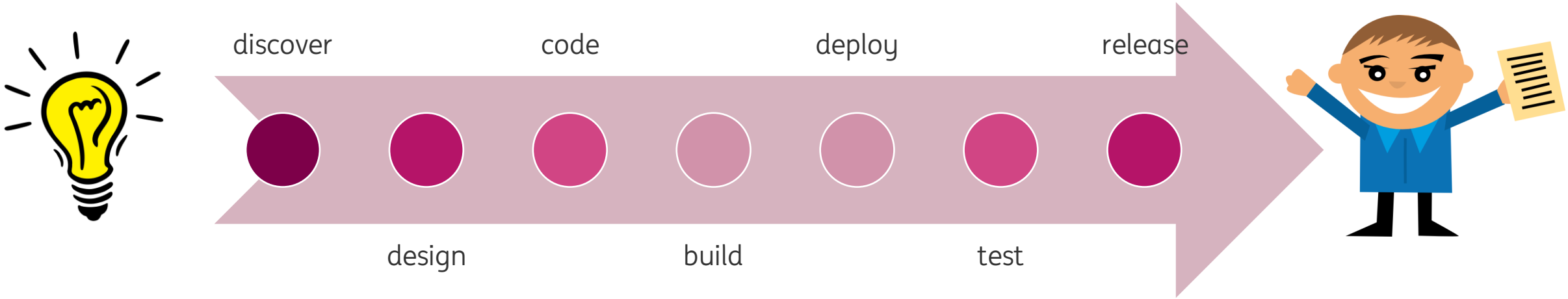
SecDevOps

FinHRBoardRiskTradeLegalControlWhateverBizSecDevOps?

Software Delivery is a Value Stream from “idea” to “customer”

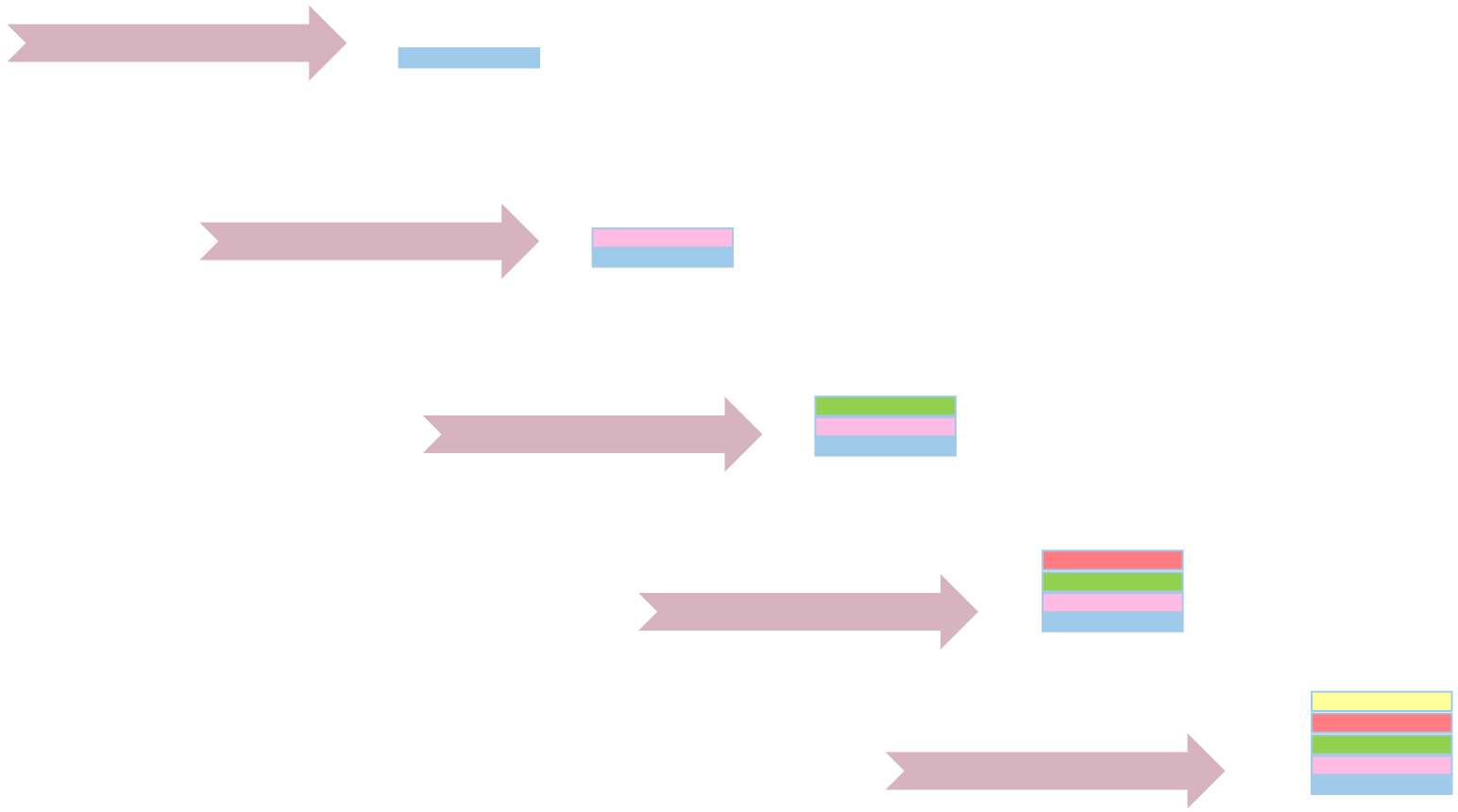


You can optimize (lean) the Value Stream to improve the process



Remove Hand-overs	Remove waiting times	Build quality in	Automate

Automation of the process makes Continuous Delivery possible



Continuous Delivery ensures fast delivery of software to production

Lead time to Production with CD

Less than one hour

Lead time to Production without CD

A week to a month

But what is the use if not everything is software?

Banks have to adhere to (local) rules & regulations

SOX
Sarbanes-Oxley

PAD
Payment Accounts Directive

Basel Accords

PSD 1&2

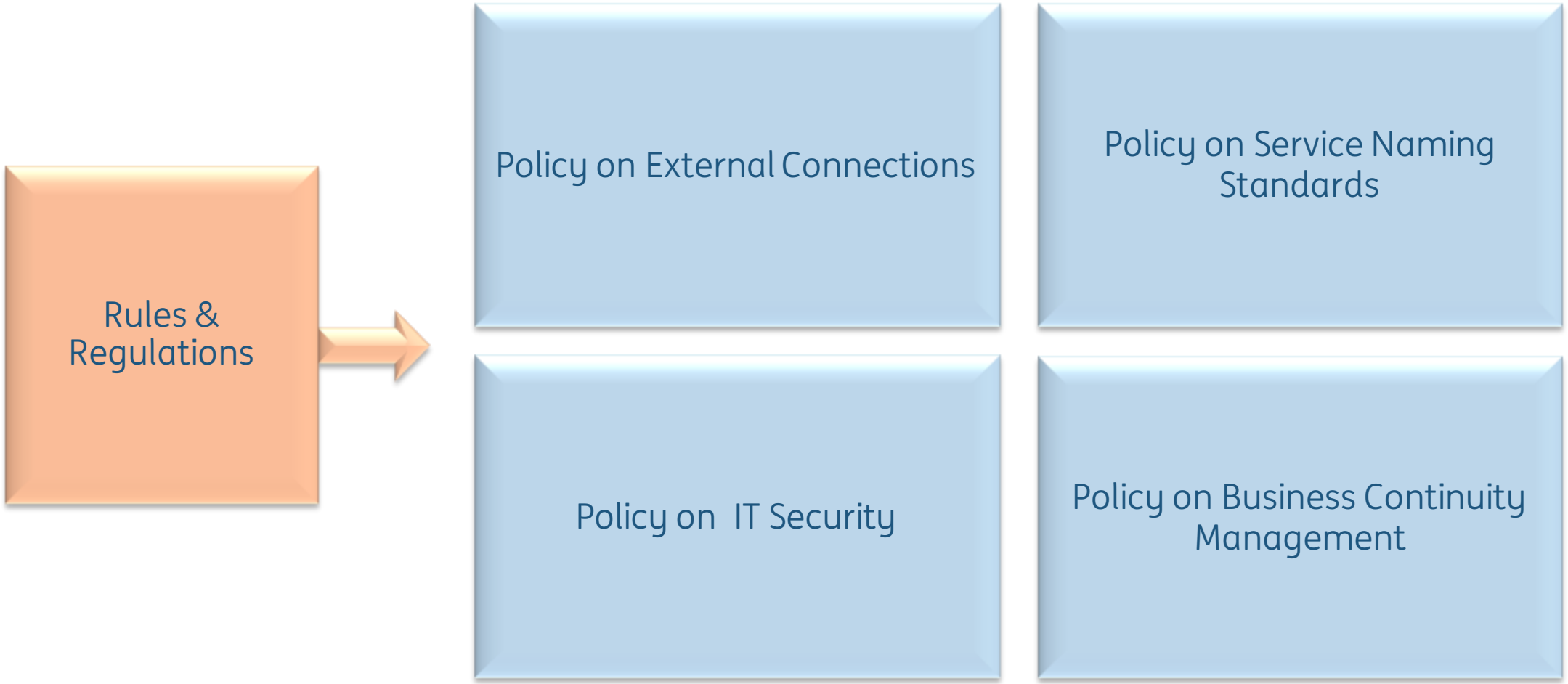
Financial Supervision Act
Wet op het financieel toezicht / Wft

FATCA
Foreign Account Tax Compliance Act

Sanctions Legislation

ING

At ING this has been translated into Policies



Note: this is just a limited set of examples. It does not reflex the real ING Policies!

The Policies identify possible Risks

HA HA HA HA!

Dev

Prod

Controls are put in place to mitigate the risks

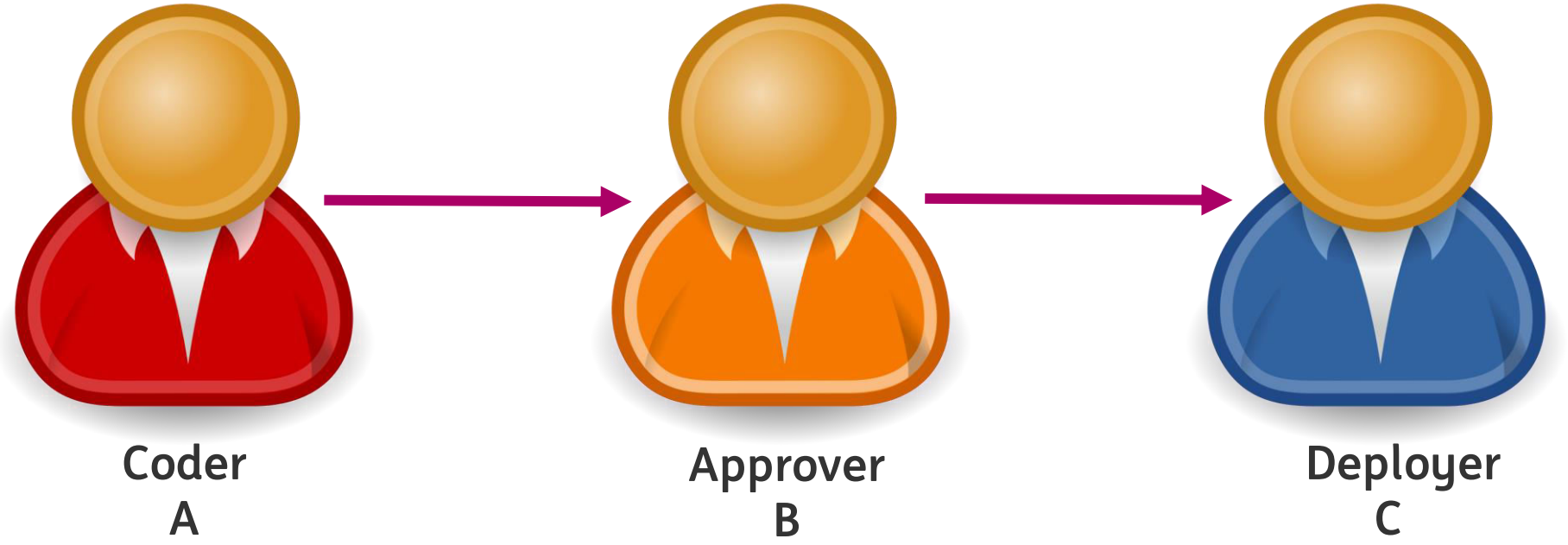
Dev

4-eyes principle

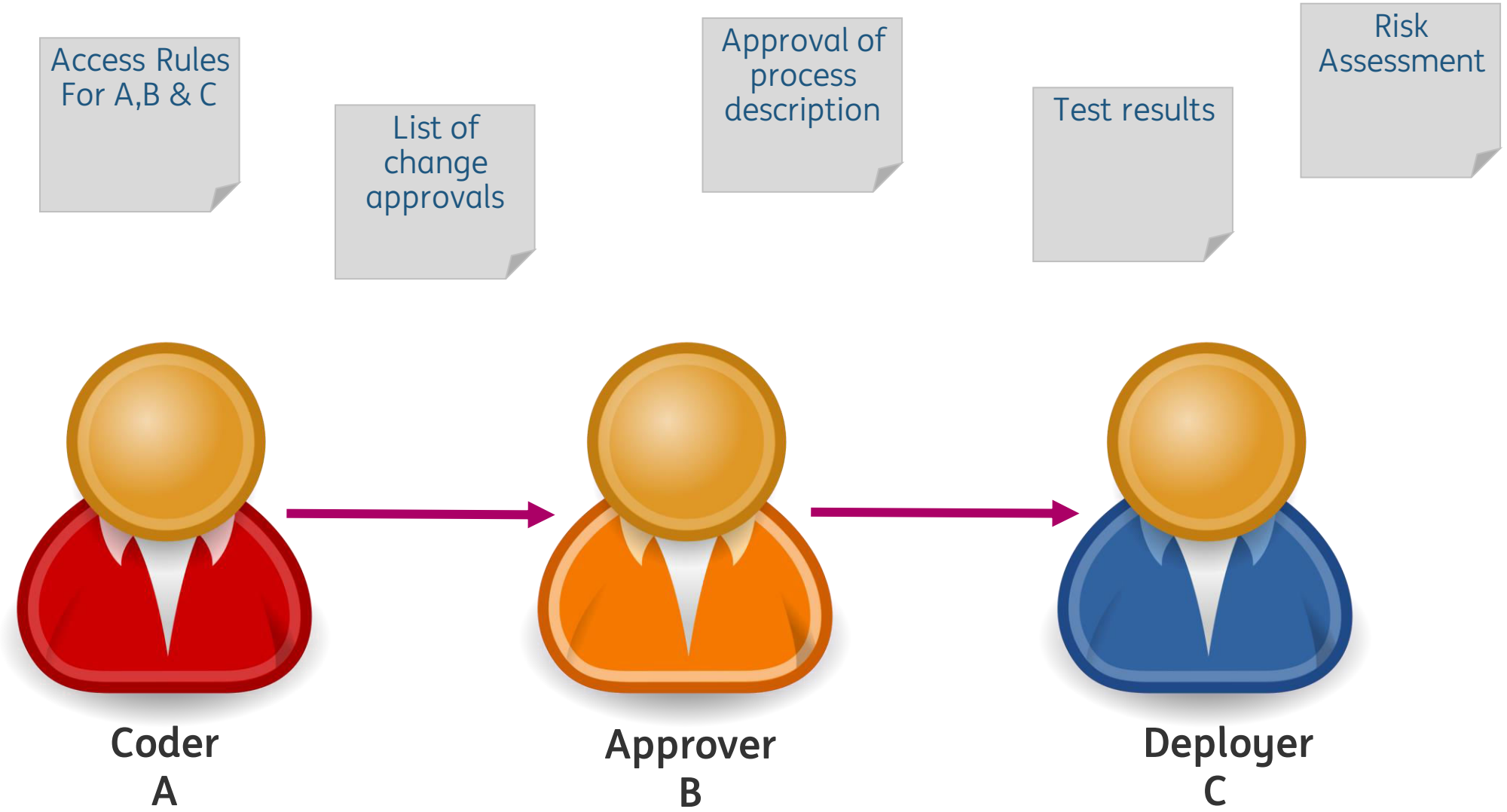
Change Board

Prod

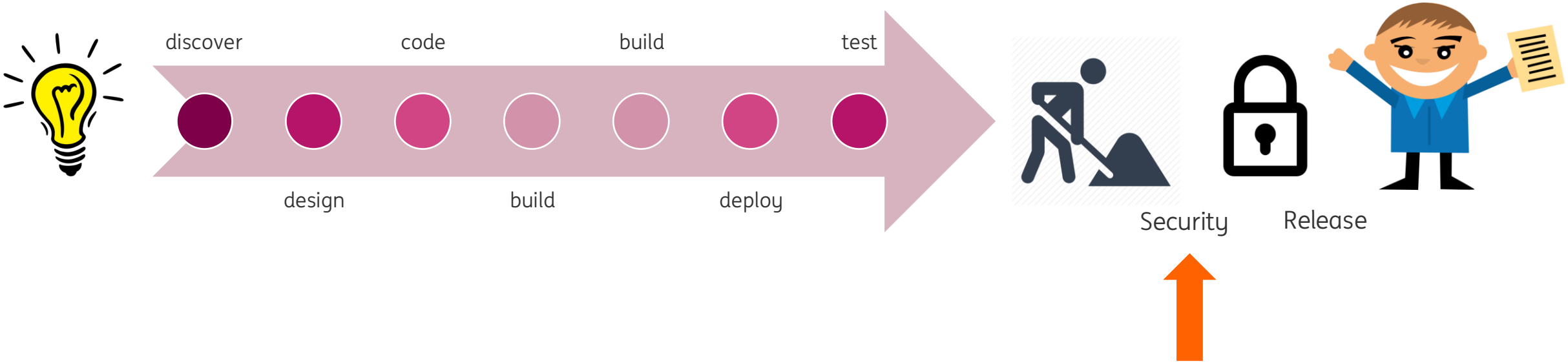
The Controls must be implemented into (local) processes



From the processes we derive evidence for Regulators



Security ends up at the right side of the Value Chain



Big opportunity to make the process faster and the life of engineers better!

To improve we need some principles

Concept of One

Engineering Culture

Everything as Code

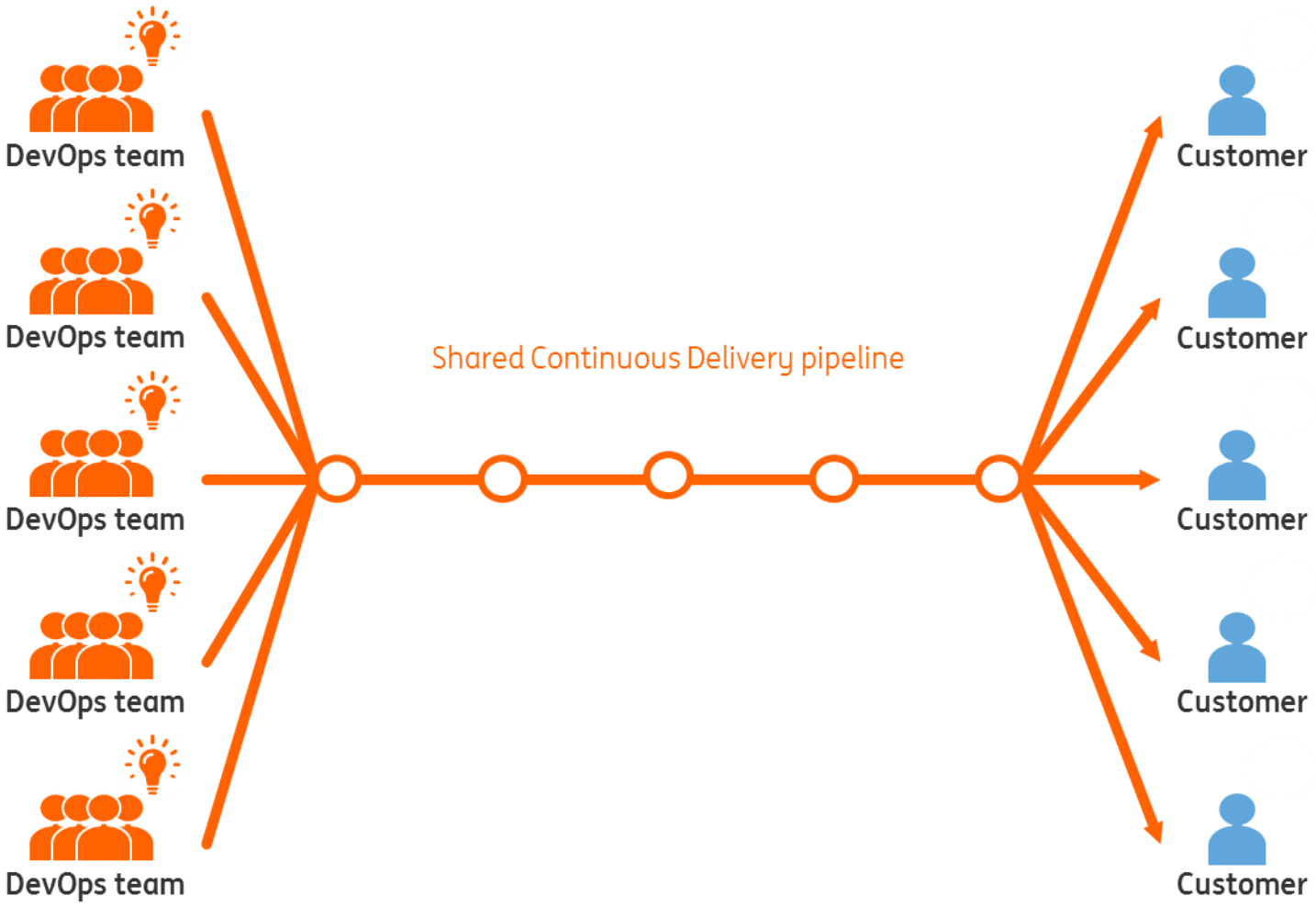
Shift-Left

Immutability

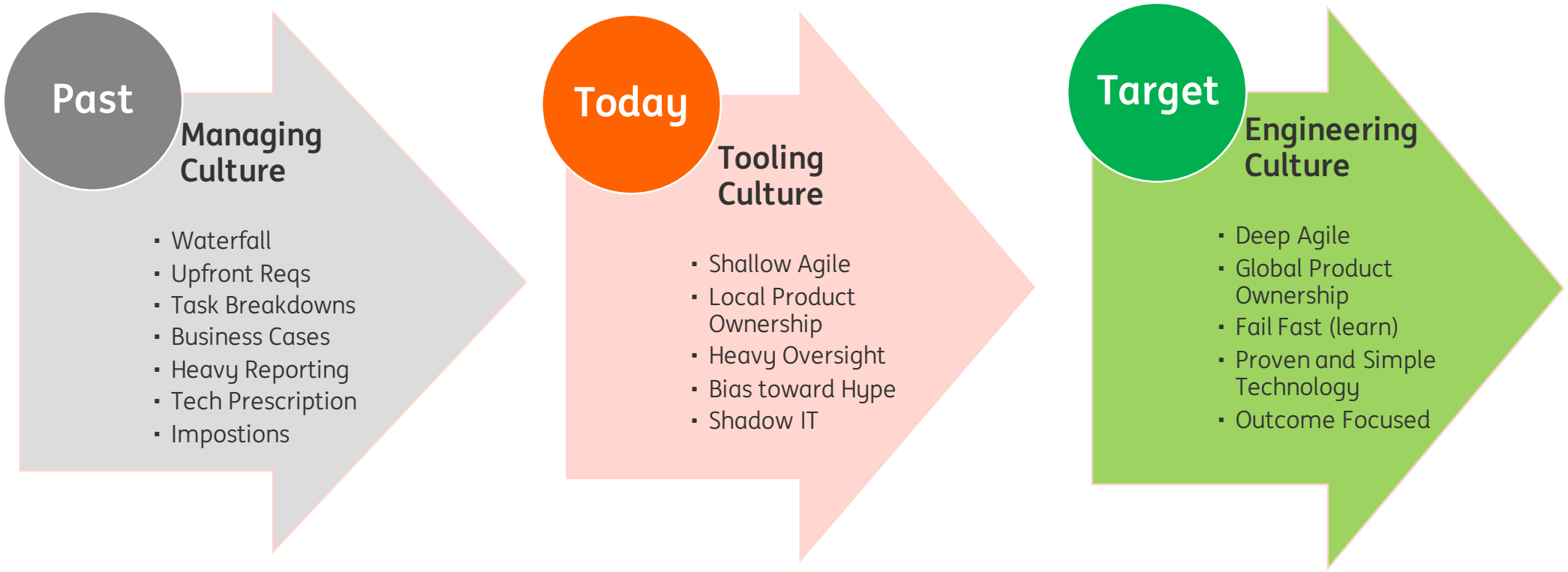
ING

Concept of One

"...**converge** components identified as **commodity** from the existing pipelines **into one** global engineering journey..."



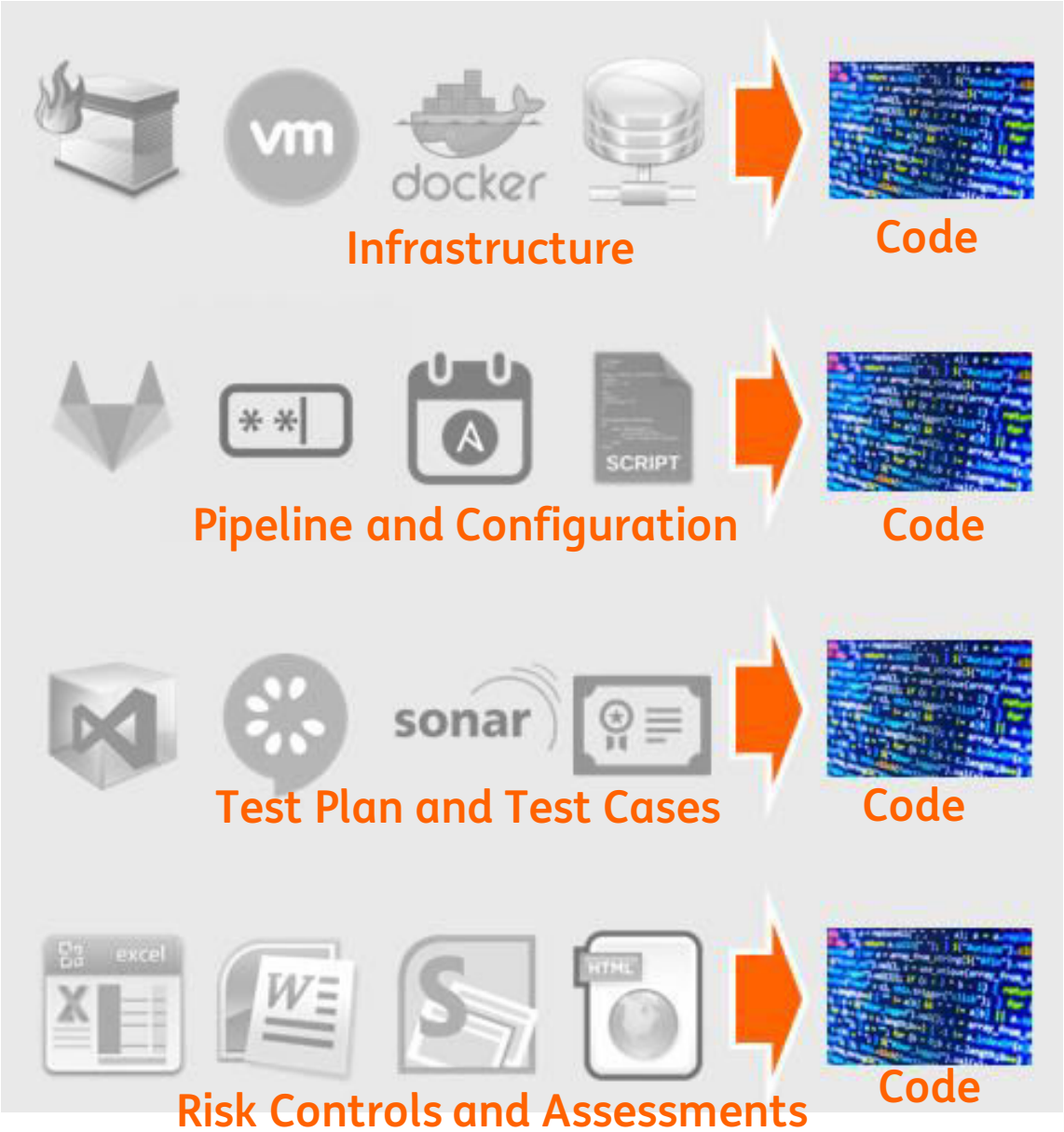
From a tooling culture to an engineering culture



Promote the **global identity** for engineers ahead of **individual team identity**.

Everything as Code

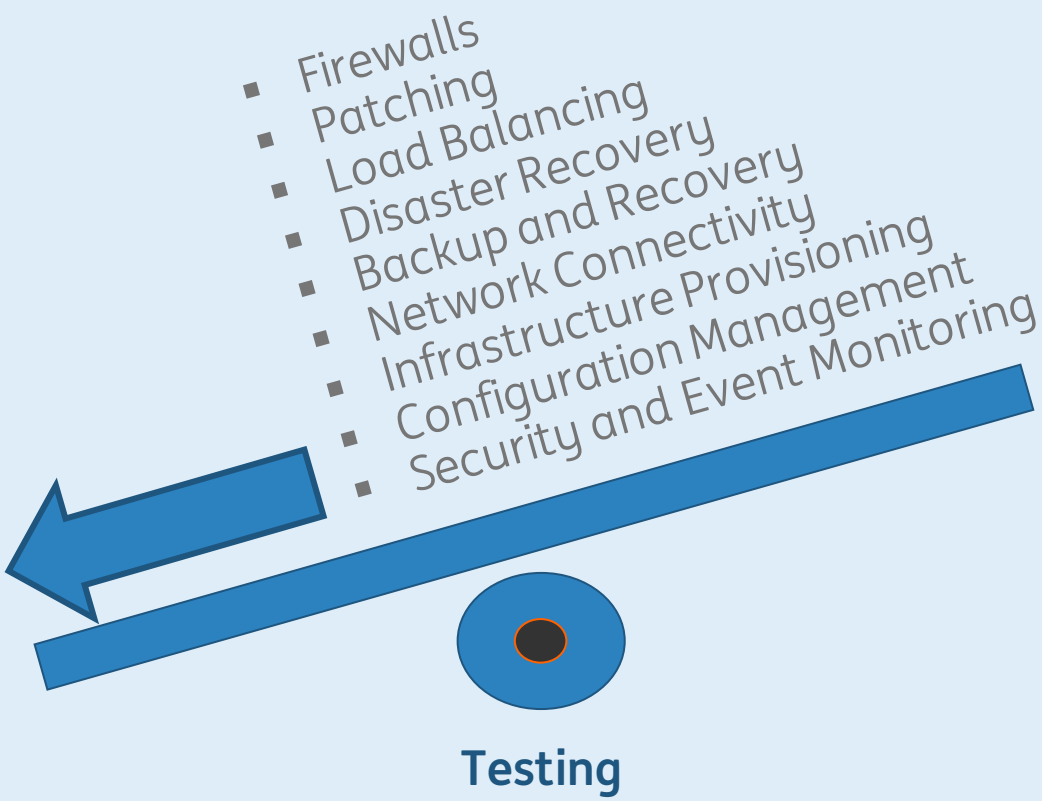
"...transmute repeatable engineering actions and **documentation as code...**"



Shift Left

"...**shift** runtime **complexity into design time** by moving engineering responsibility to the left of testing..."

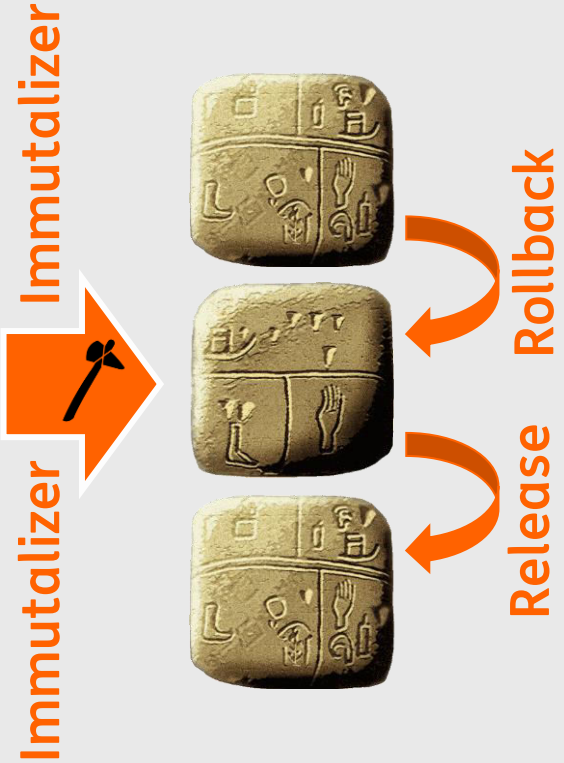
Do not digitize the current process, but redesign and transmute to code or automation



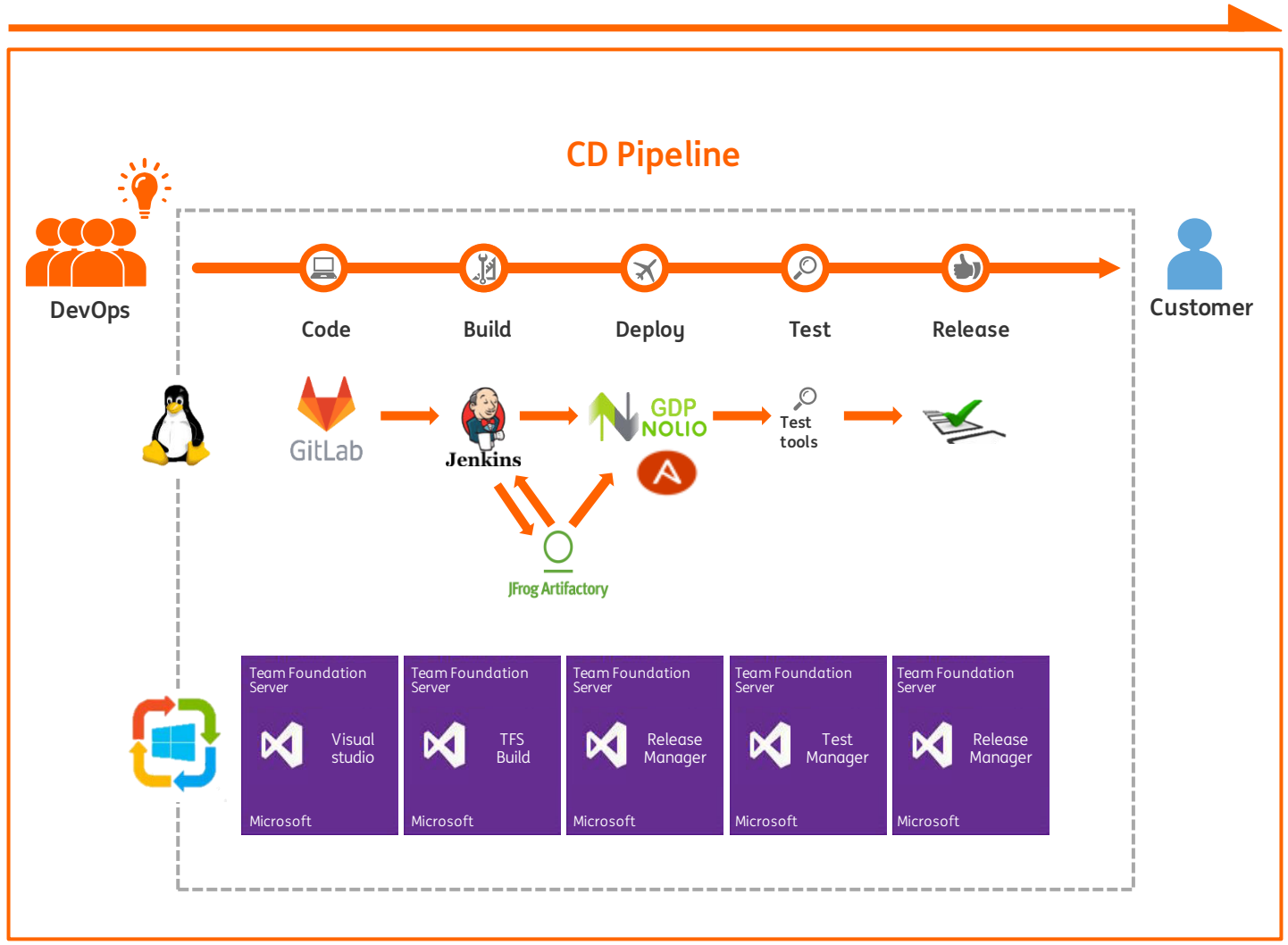
Immutability

"...freeze and protect the state of production assets from change by **apply**ing **immutable patterns** and designs..."

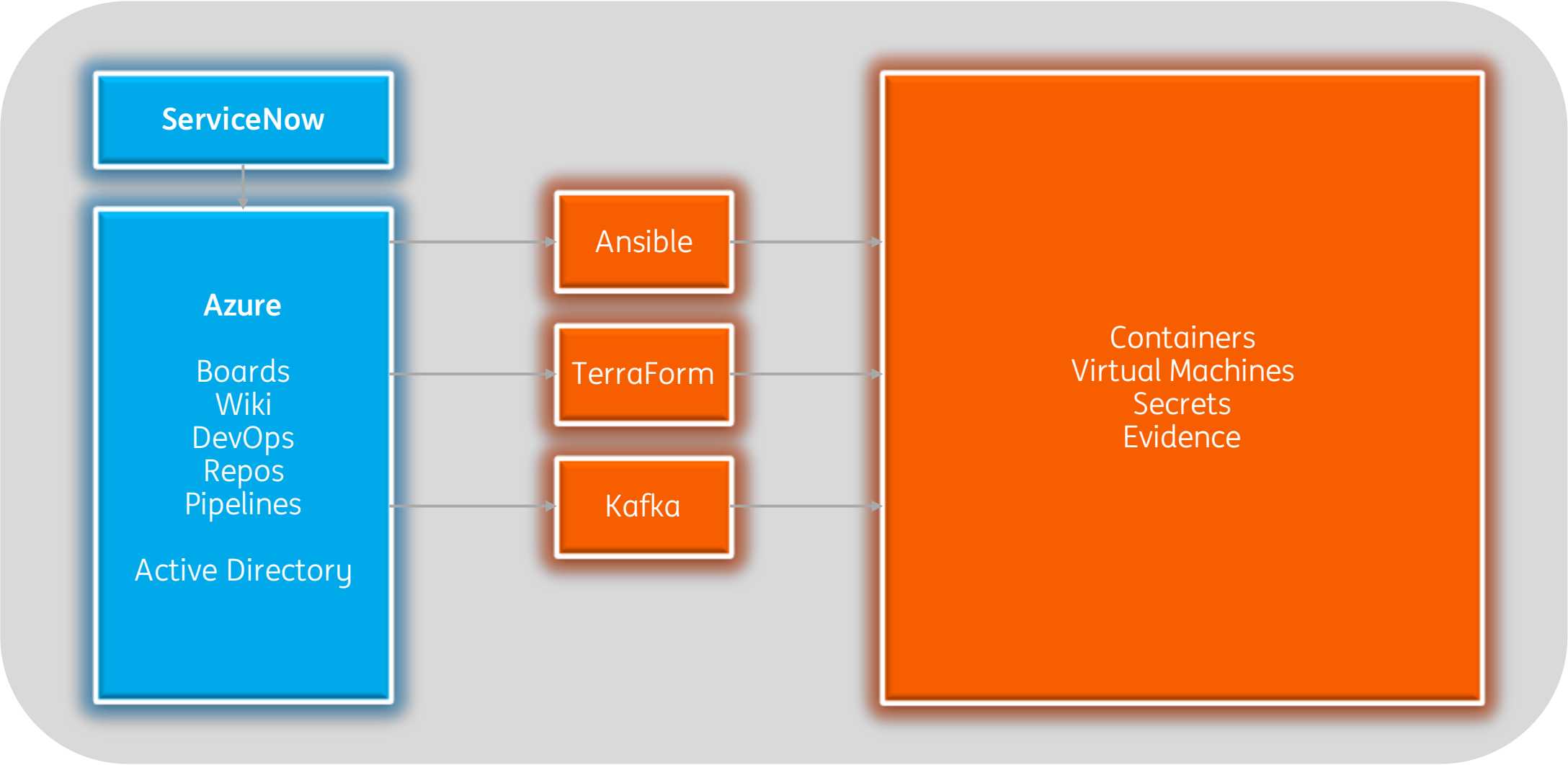
- Applications
- Containers
- Virtual Machines
- Firewalls
- Data Stores
- Data Models
- Authentication
- Authorization
- Systems
- Domains



From a tool-oriented CD Pipeline with paperwork



To an Engineering CD Pipeline



ING

Conclusions

- You can shift-left security if you redesign your controls
- Identify true bottlenecks in your Value Stream
- Set a dot on the horizon, based on your principles
- Change the culture towards true engineering
- Code is Craftsmanship

ING

Questions?

Questions?