Cloud is here to stay

Dr. Peter van Eijk

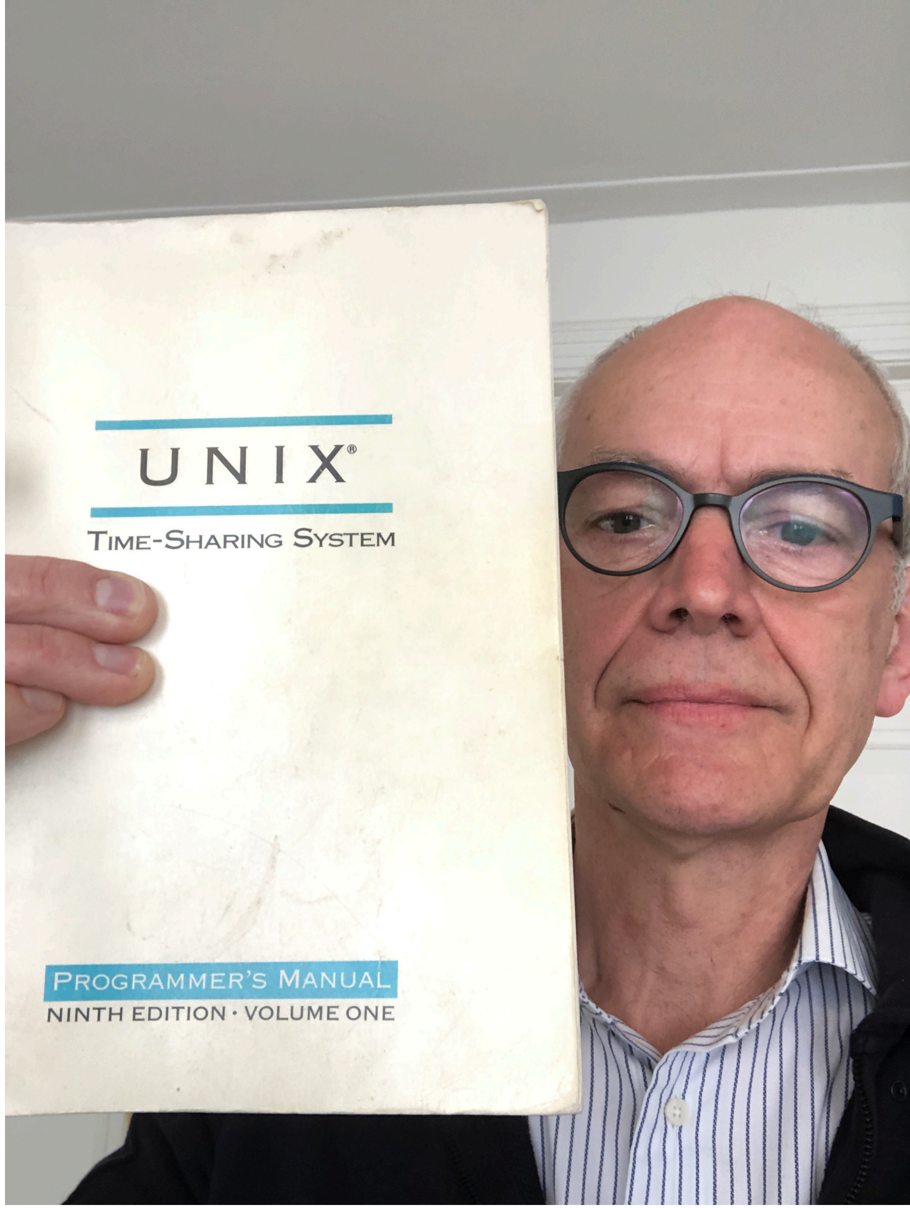
Secure Cloud Adoption Coach & Instructor

+ Hogeschool Hoofddocent HU

ClubCloudComputing

About me

- Uni Twente
- AT&T Bell Labs
- CVI/EDS
- EUnet
- Bakkenist/Deloitte
- Digital Infrastructures
- TheCloudInstructor CCSK.eu
- Hogeschool Utrecht



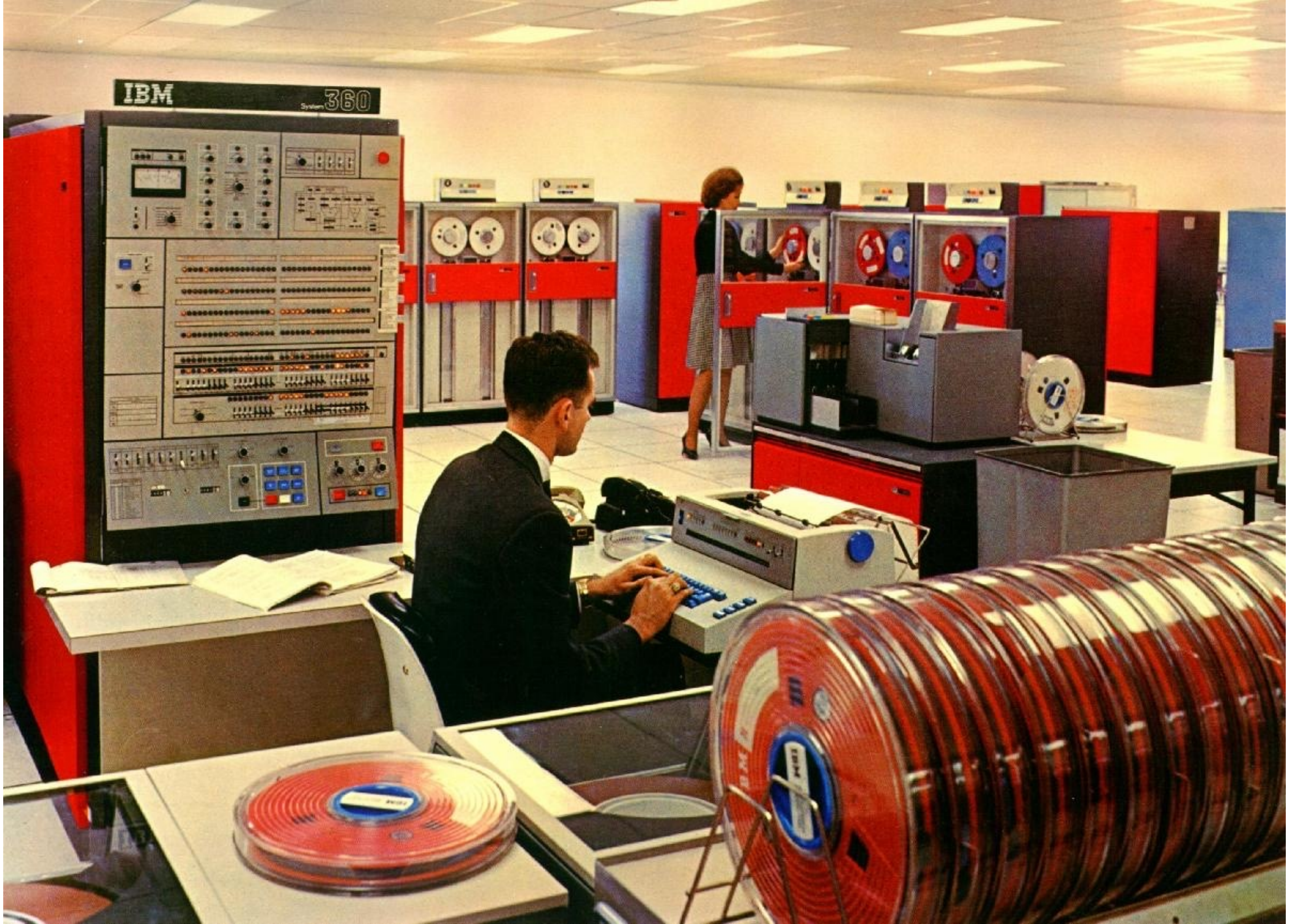
About you

- Vragen?

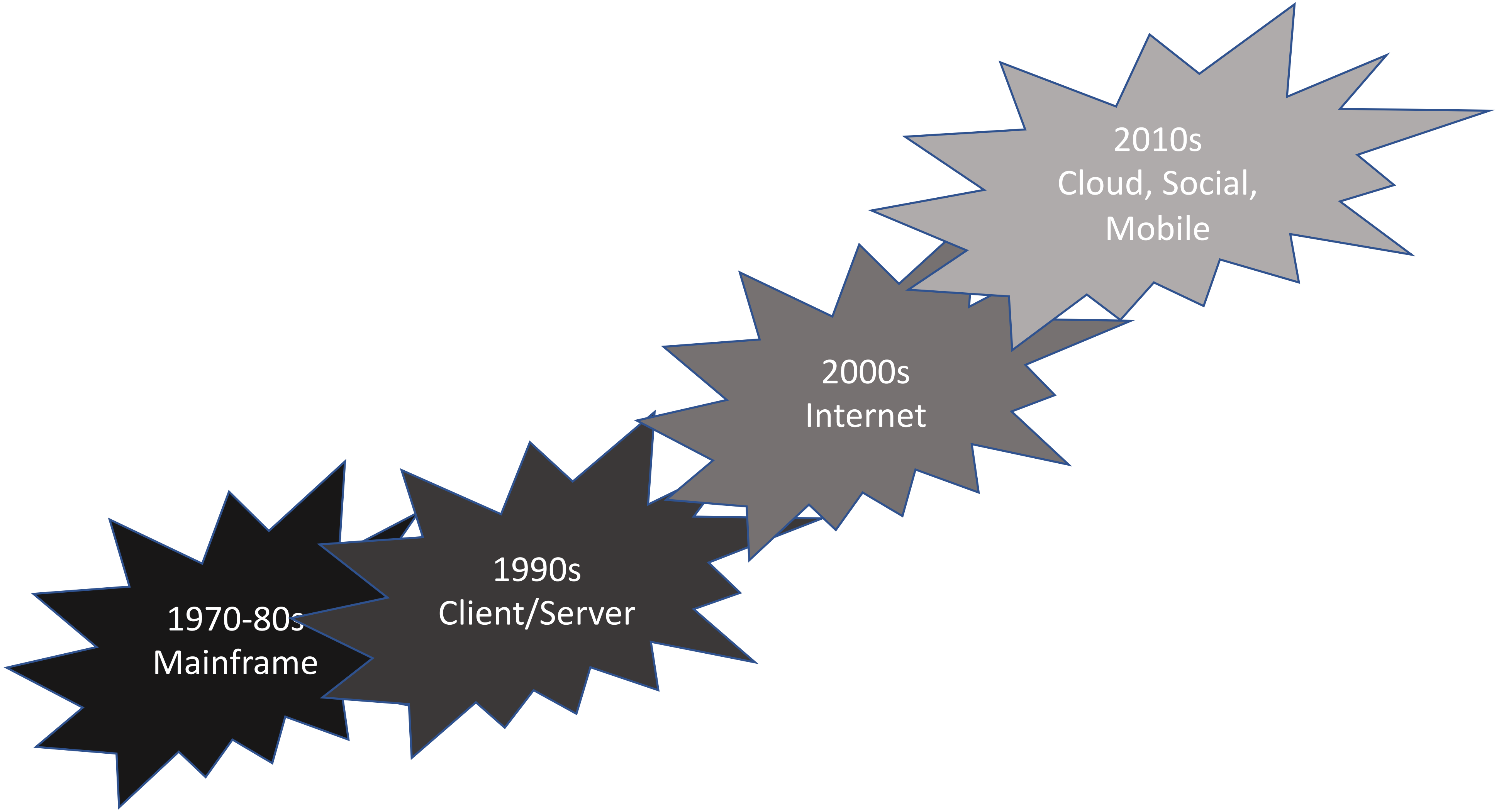
- Wat is cloud?

Cloud: the new IT model

Cloud is a state of mind


IBM
System 360

How did we get here?



Each of these steps was a disruptive innovation …

Disruptive innovations

Characteristics

- Not as good (initially)
- Much cheaper
- Addresses ‘over-served’ customers
- Rapidly improving
- Eventually drives original out of the market

Examples

- Wikipedia
- PC
- Internet
- Cloud computing

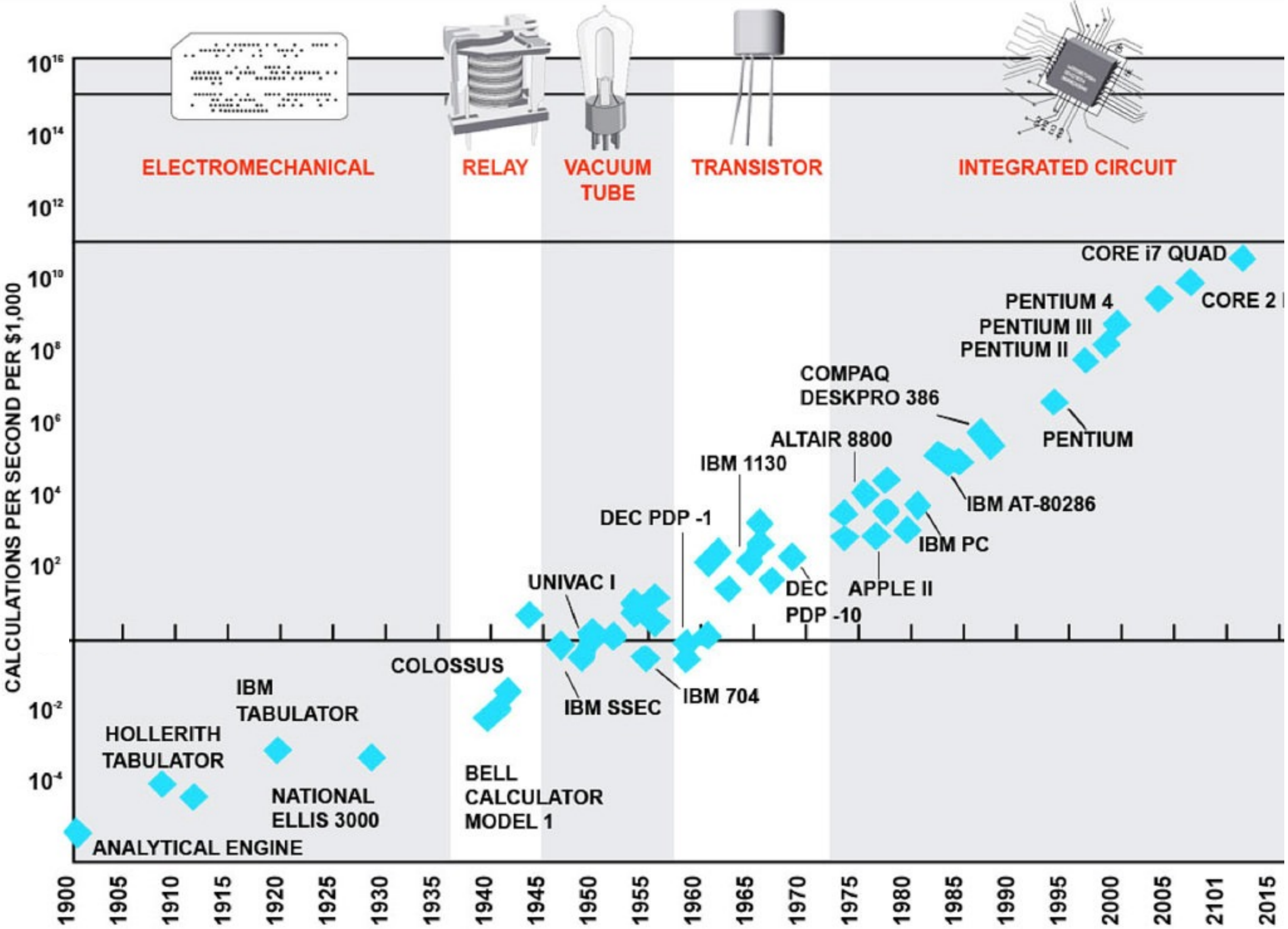
https://en.wikipedia.org/wiki/Disruptive_innovation

Tipping Points

Your daddy’s datacenter

The new cloud world: everything is connected

115 Years of Moore's Law

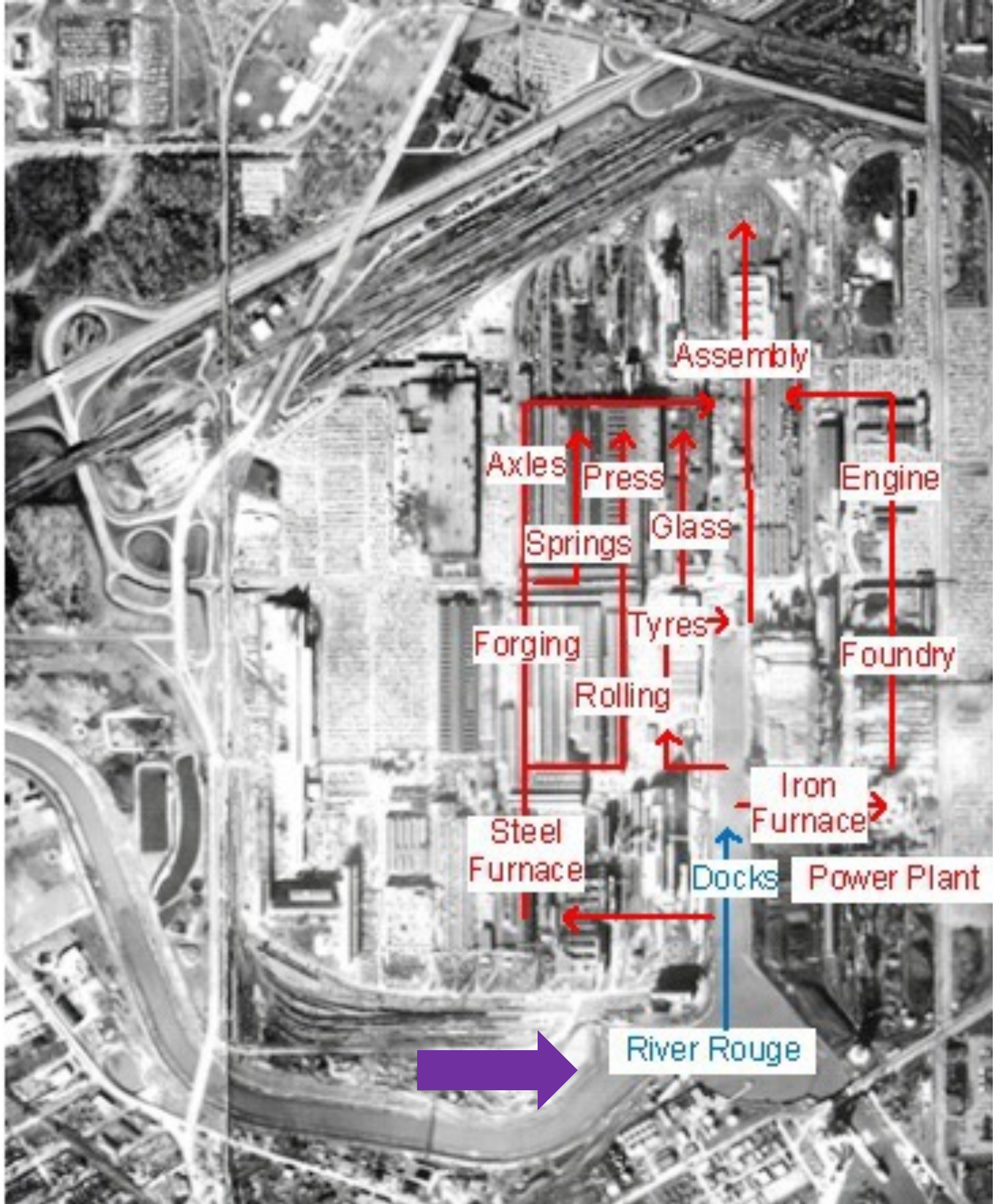


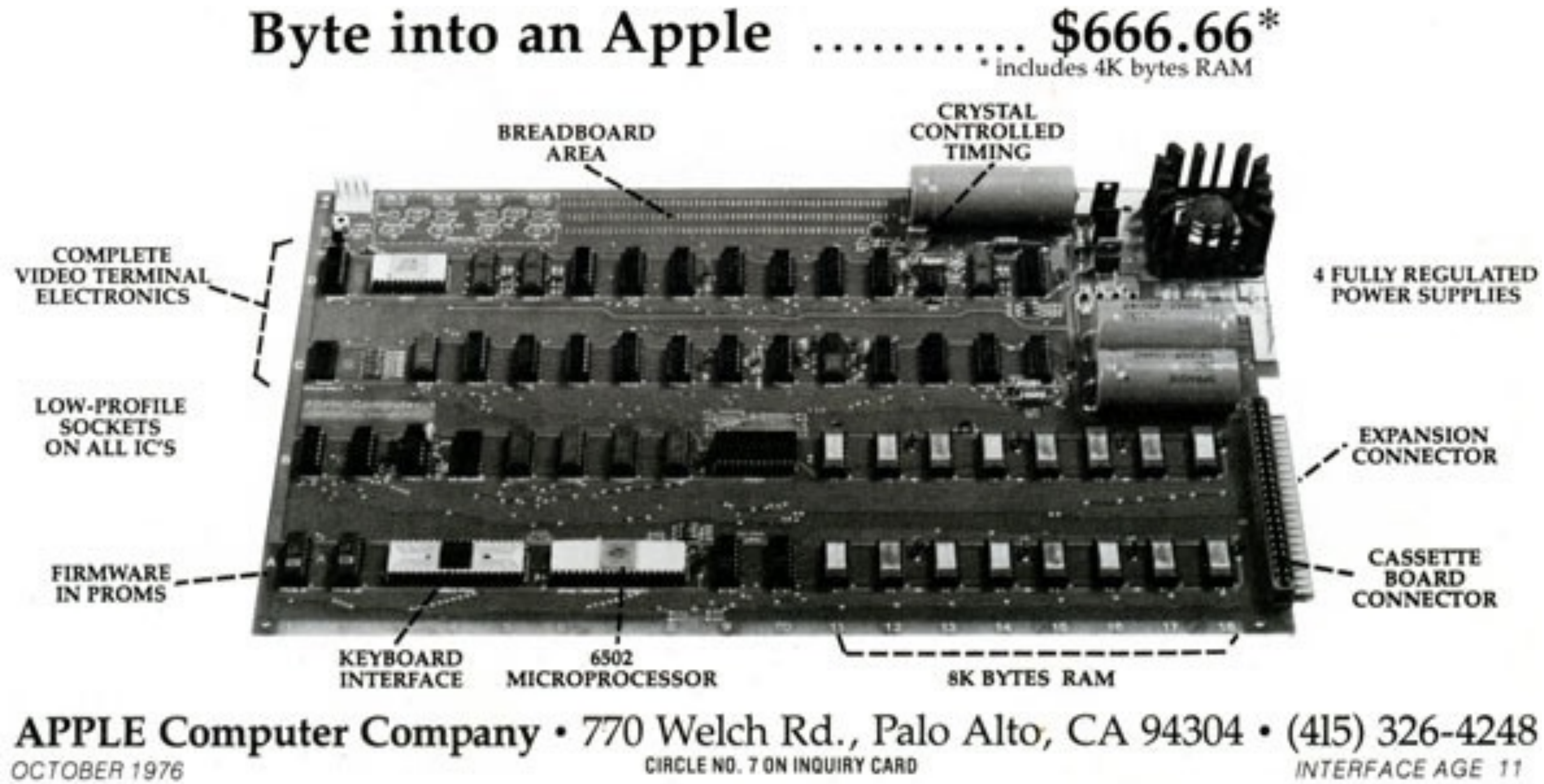
IT is getting more complicated

- Moore’s law
- More technology
- More components
- More programming languages
- More interfaces and devices
- More pervasive IT
- More threats
- More brainpower required
- More productivity required

Ford
BM 18 AP

Ford River Rouge plant





Byte into an Apple $666.66*

* includes 4K bytes RAM

APPLE Computer Company • 770 Welch Rd., Palo Alto, CA 94304 • (415) 326-4248

OCTOBER 1976

CIRCLE NO. 7 ON INQUIRY CARD

INTERFACE AGE 11

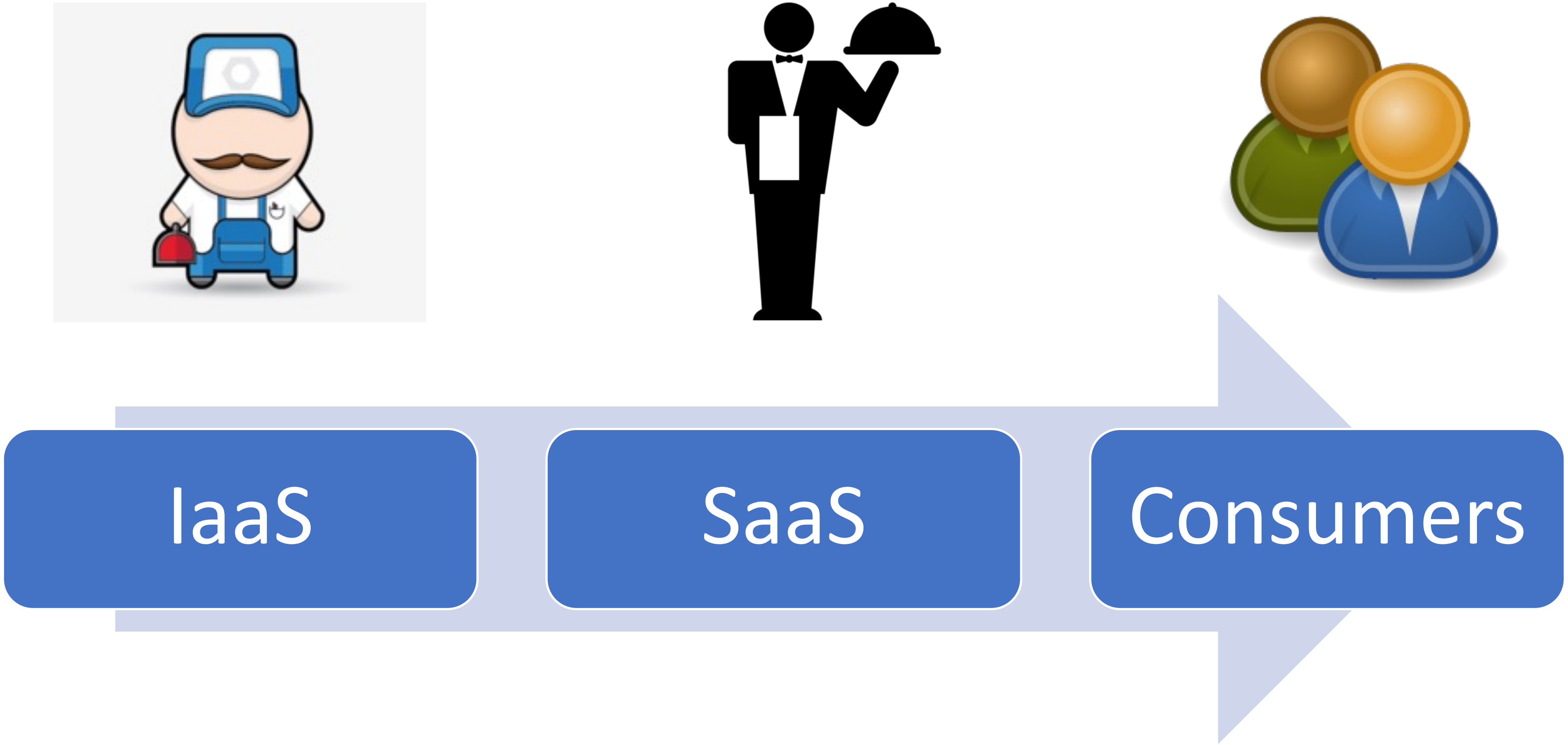
iPhone 6
Anchorage
Canada
United States
New York
Los Angeles
Houston
Mexico
CO
VE
Brazil
SE
NO
PL
UA
FR
ES
DZ
LY
EG
ML
NG
SD
ET
CD
KE
SA
IR
TR
KZ
UZ
PK
MN
Urumqui
China
India
MM
TH
Dubai
Hong Kong
Komatsu
Kuala Lumpur
Indonesia

Control in the supply chain

Today’s car

- Cheaper
- More fuel efficient
- More functional
- Safer
- Better
- More colors

A simple cloud supply chain

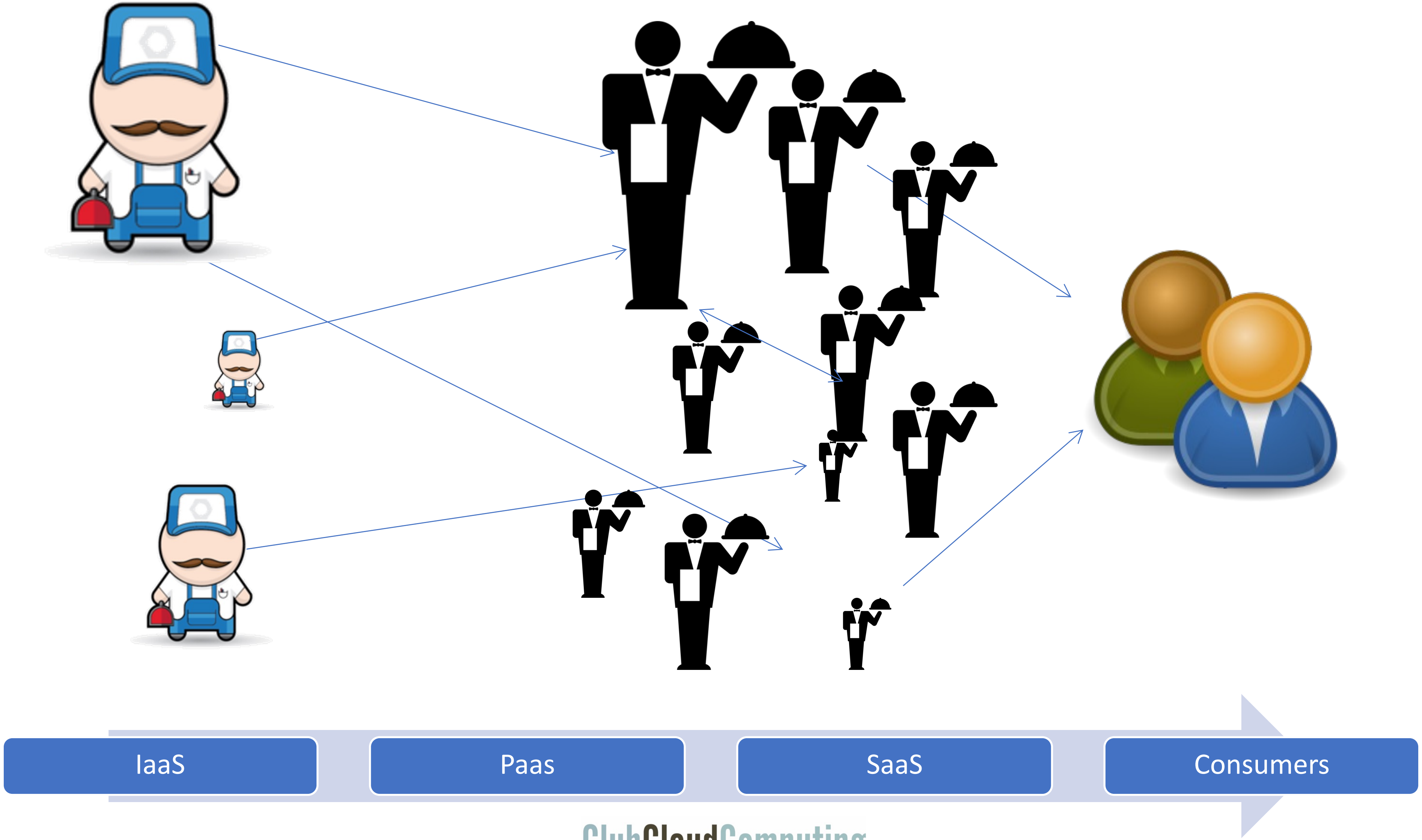


IaaS

SaaS

Consumers

A more realistic supply chain



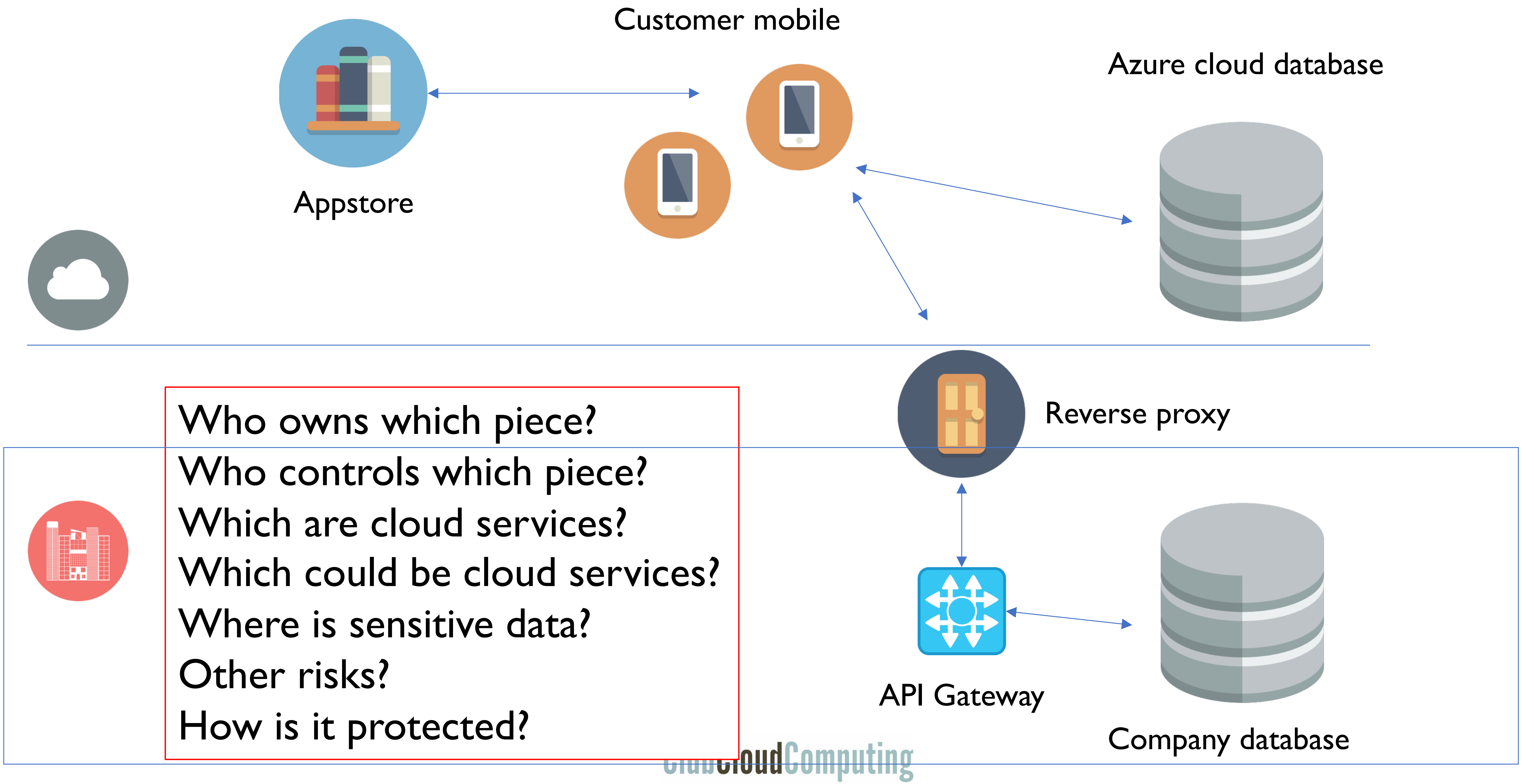
IaaS

Paas

SaaS

Consumers

Hybrid mobile app architecture and supply chain



Who owns which piece?
Who controls which piece?
Which are cloud services?
Which could be cloud services?
Where is sensitive data?
Other risks?
How is it protected?

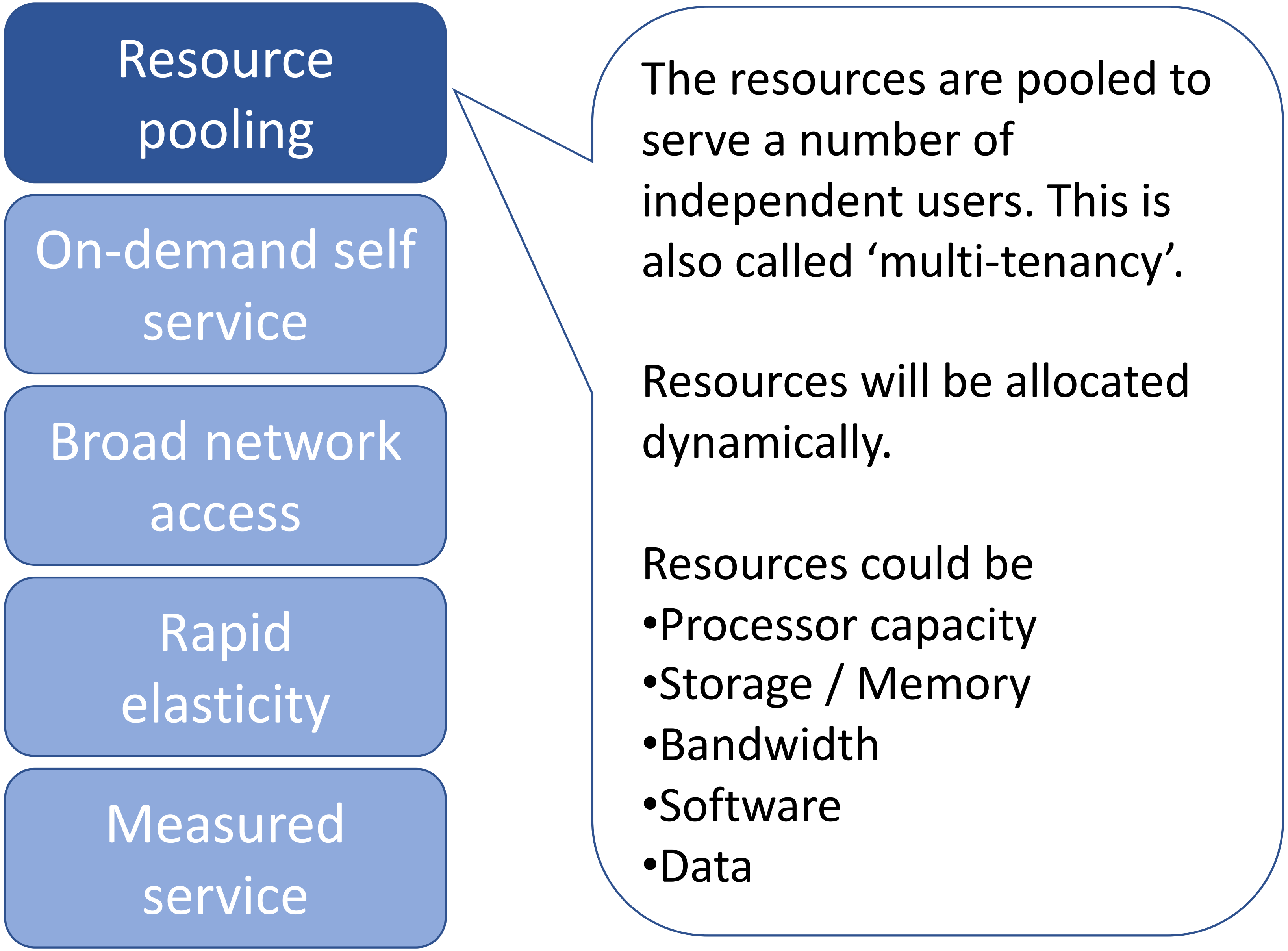
Cloud is here to stay

- Imagine: 10 times the amount of computers and software from what we have today
- How much staff does that take to manage?

- The cloud **business case** is about productivity
- Efficiency of people
- Faster delivery and time to market
- DevOps
- Big Data

5 essential characteristics bring benefit

- **Resource pooling**. Multiple customers
- **On-demand self-service**. Unilateral provisioning
- **Broad network access**. Network and client
- **Rapid elasticity**. Speedy provisioning and deprovisioning
- **Measured Service**. Pay per use



Resource pooling

On-demand self service

Broad network access

Rapid elasticity

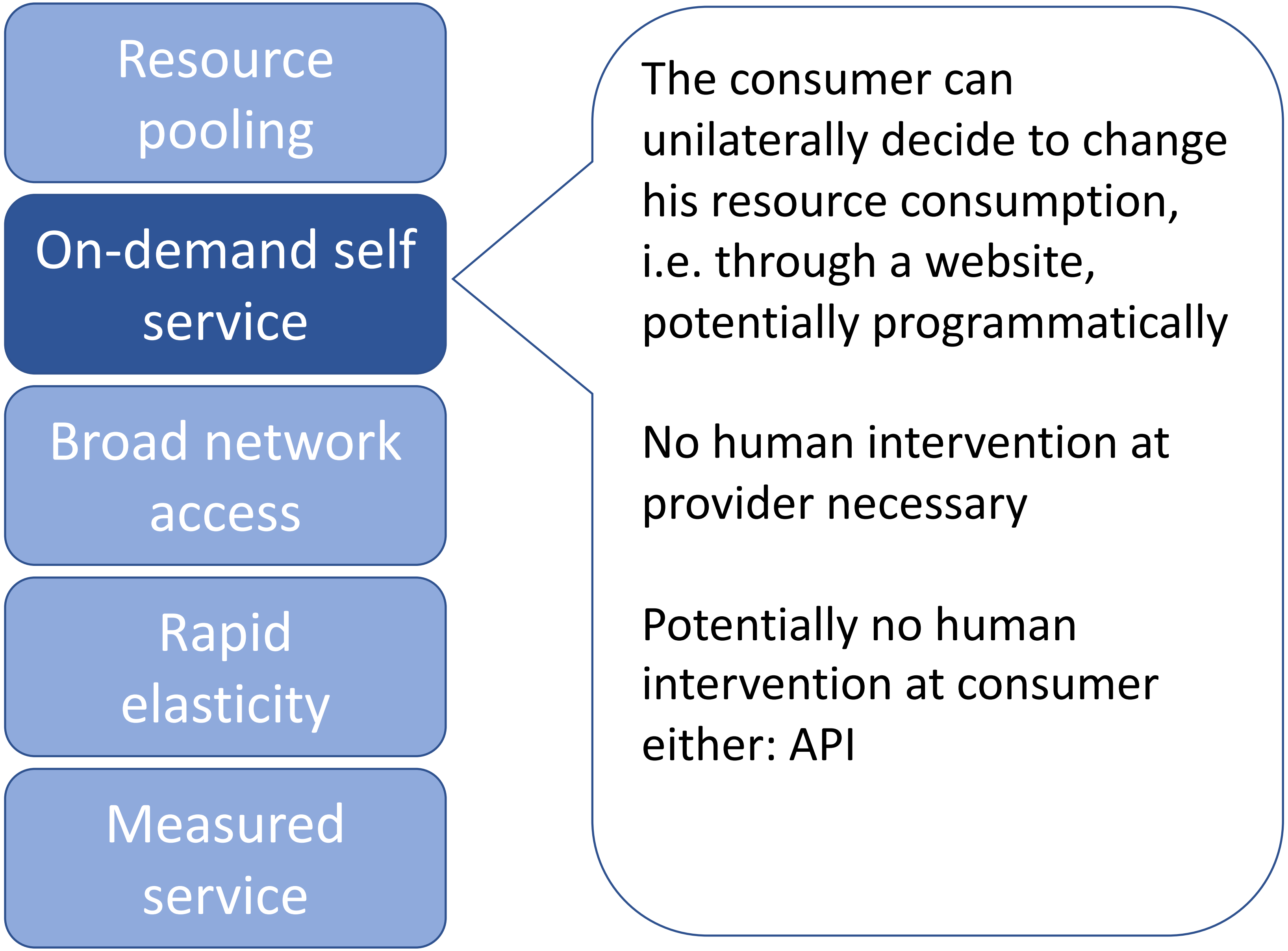
Measured service

The resources are pooled to serve a number of independent users. This is also called ‘multi-tenancy’.

Resources will be allocated dynamically.

Resources could be

- Processor capacity
- Storage / Memory
- Bandwidth
- Software
- Data



Resource pooling

On-demand self service

Broad network access

Rapid elasticity

Measured service

The consumer can unilaterally decide to change his resource consumption, i.e. through a website, potentially programmatically

No human intervention at provider necessary

Potentially no human intervention at consumer either: API

What if you don’t get self-service?

- What would happen to the business value?

Resource pooling

On-demand self service

Broad network access

Rapid elasticity

Measured service

The service is accessible
- through a variety of networks
- by a variety of devices: PC, server, mobile

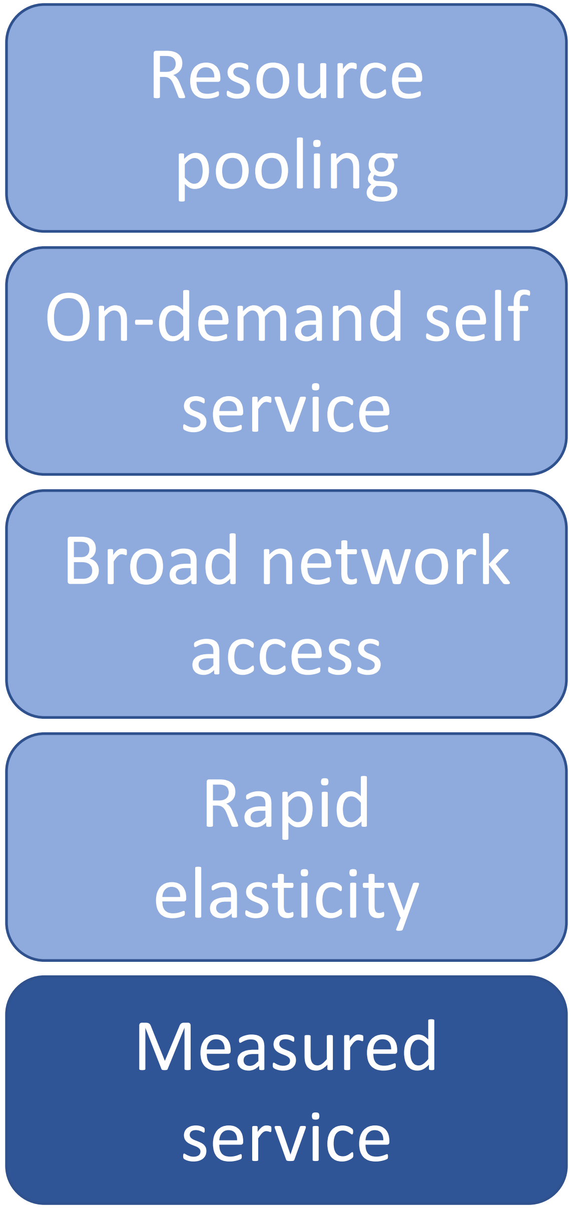
The network is a given

- Resource pooling
- On-demand self service
- Broad network access
- **Rapid elasticity**
- Measured service

The resources can be scaled up and down quickly.

This is done without provider intervention, through the on-demand self service.

Rapid as in ”rapid enough for the business process it supports”



Resource pooling

On-demand self service

Broad network access

Rapid elasticity

Measured service

The consumption of the resource is measured in a meaningful way, e.g.

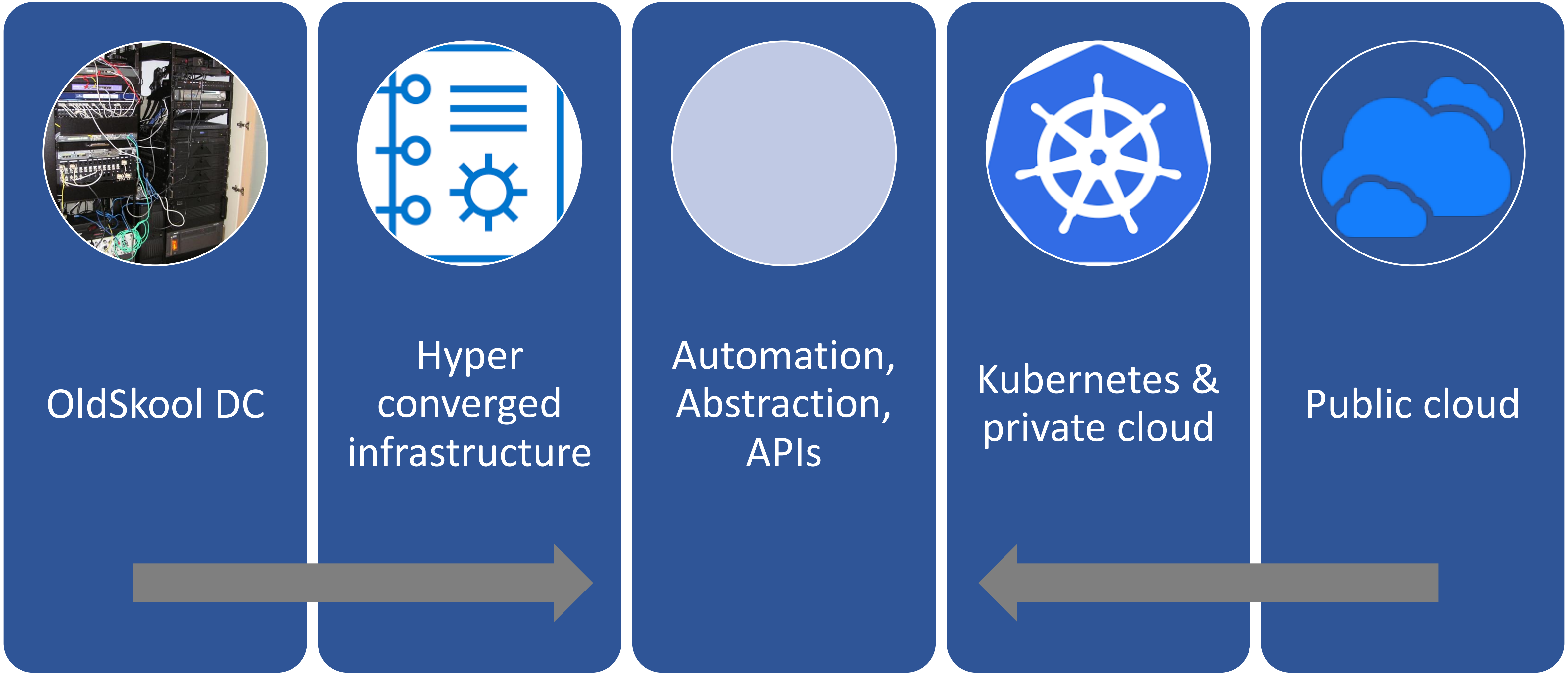
- memory,
- processor capacity,
- user counts.

This usage can be the basis for the billing of the consumer.

Characteristics lead to benefit and risk

- Rapid provisioning, benefit:
  - Quick leverage of innovative services
- Rapid provisioning, risk:
  - Uncontrolled spend

Blurring line between cloud and OldSkool DC



OldSkool DC

Hyper converged infrastructure

Automation, Abstraction, APIs

Kubernetes & private cloud

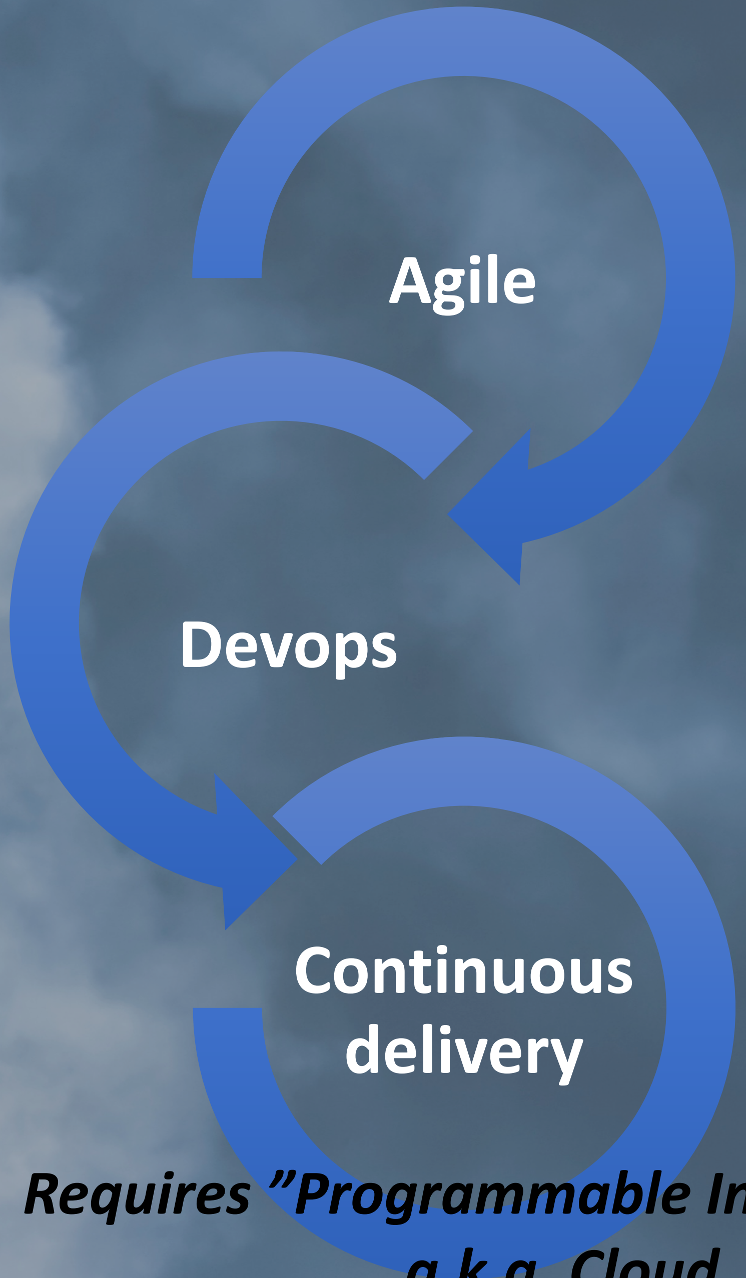
Public cloud

Feature velocity through devops and continuous delivery

Number of deployments per day
(source: “The Phoenix Project”, 2012)

Company	Deploy Frequency	Deploy Lead Time
Amazon	23.000/day	Minutes
Google	5.500/day	Minutes
Netflix	500/day	Minutes
Twitter	3/week	Minutes
Typical enterprise	1/9 months	Months

At higher deploy frequency, reliability increases



Agile

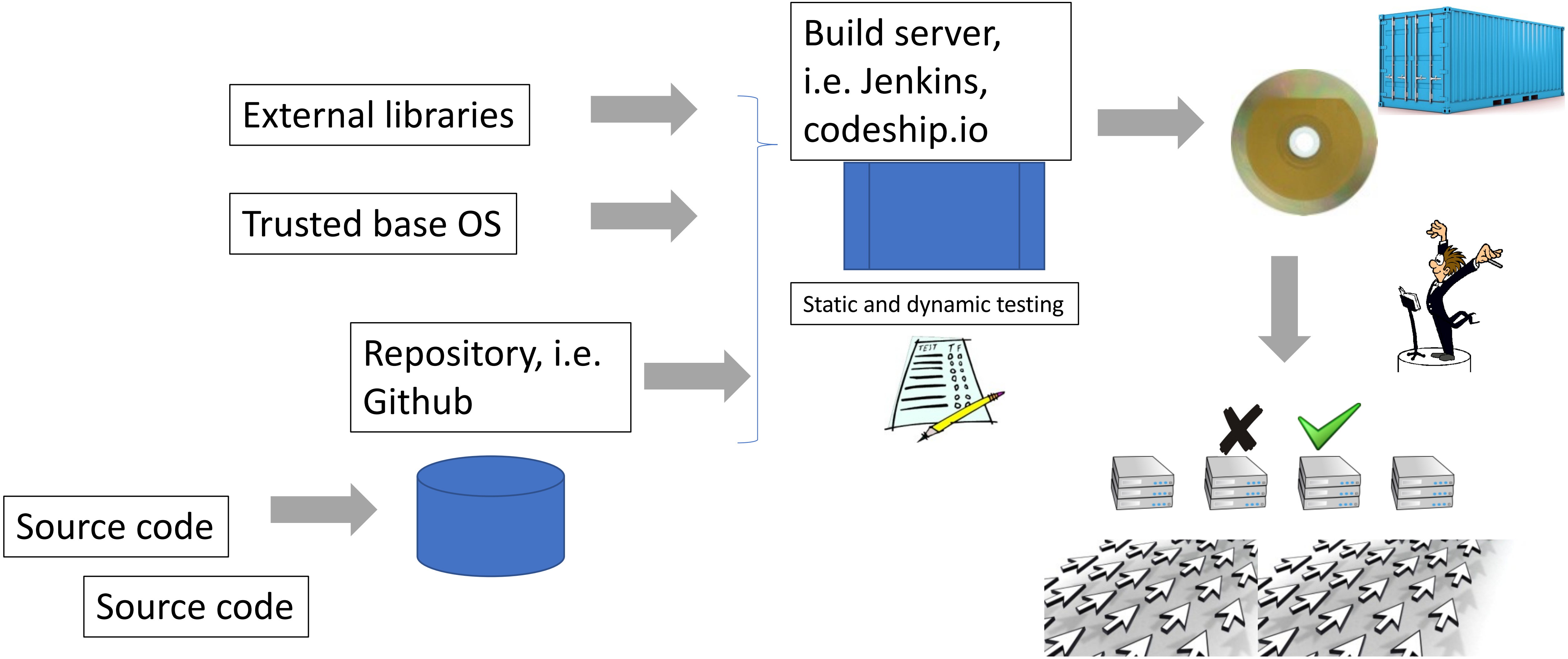
Devops

Continuous delivery

- quick response on customer feedback
- integration of development and operations
- automatic and frequent push from development to production

Requires ”Programmable Infrastructure” a.k.a. Cloud

From code to production



External libraries

Trusted base OS

Repository, i.e. Github

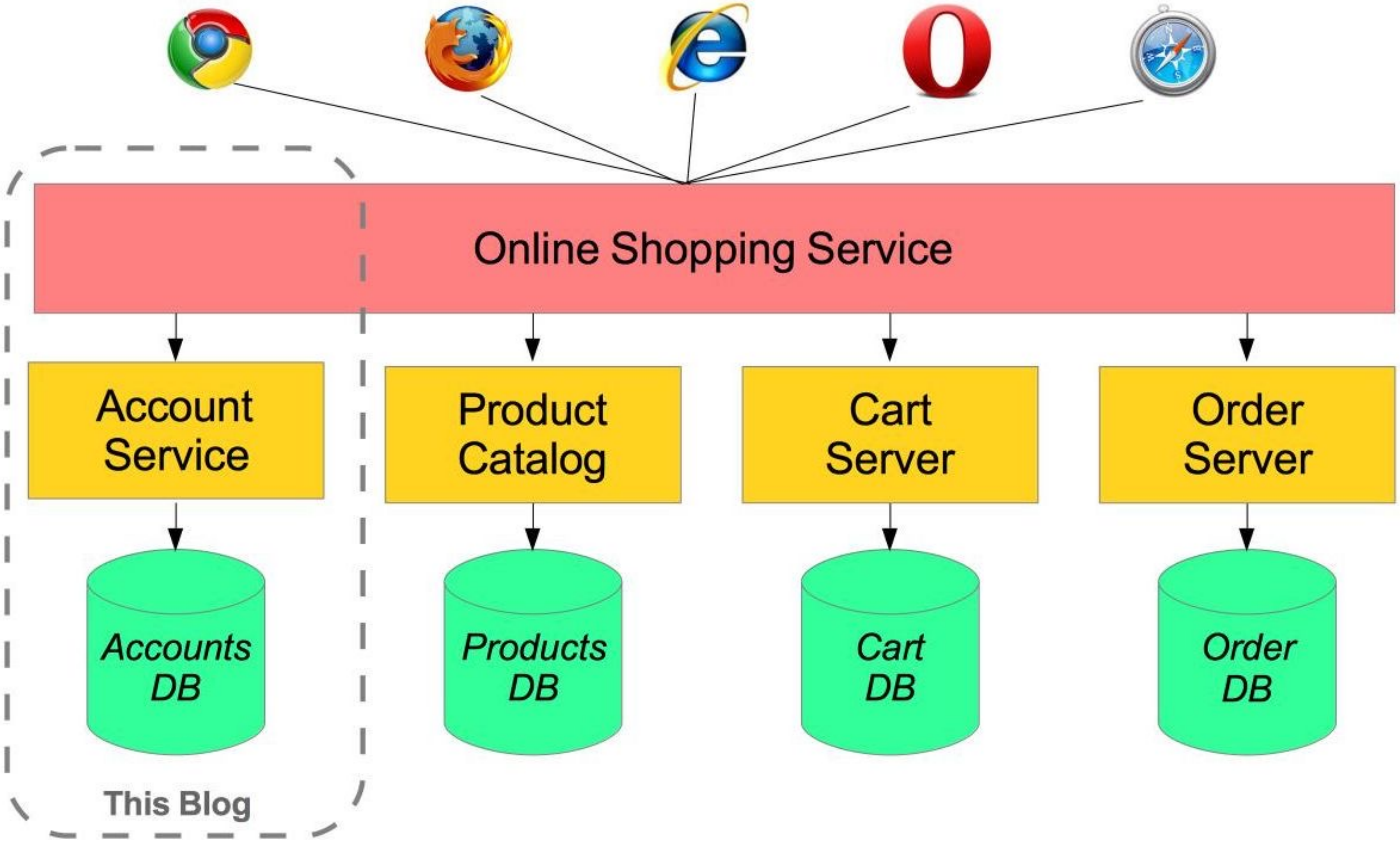
Source code

Source code

Build server, i.e. Jenkins, codeship.io

Static and dynamic testing

Cloud native: microservices

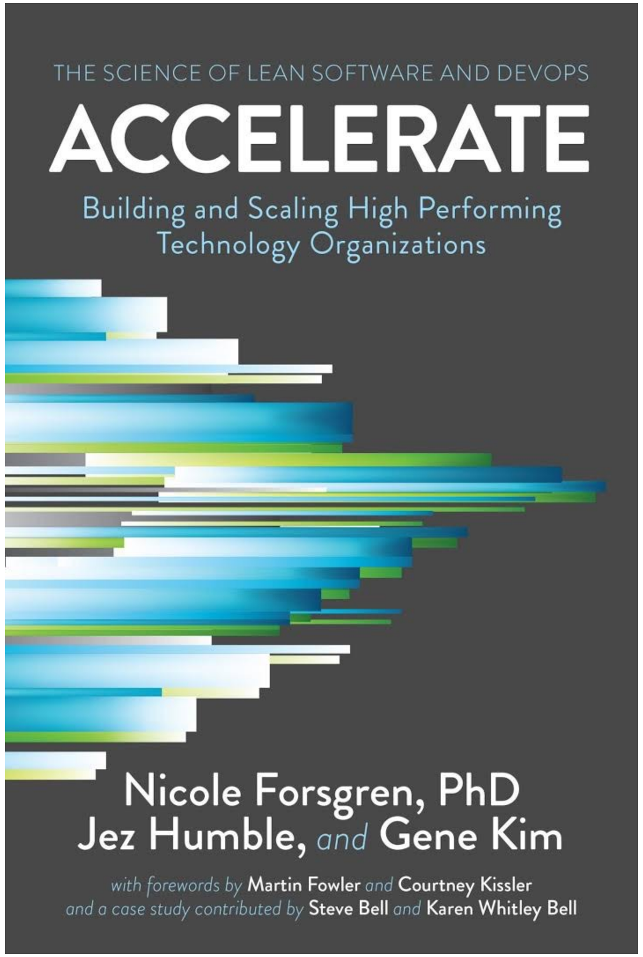


Source: Spring.io

ClubCloudComputing

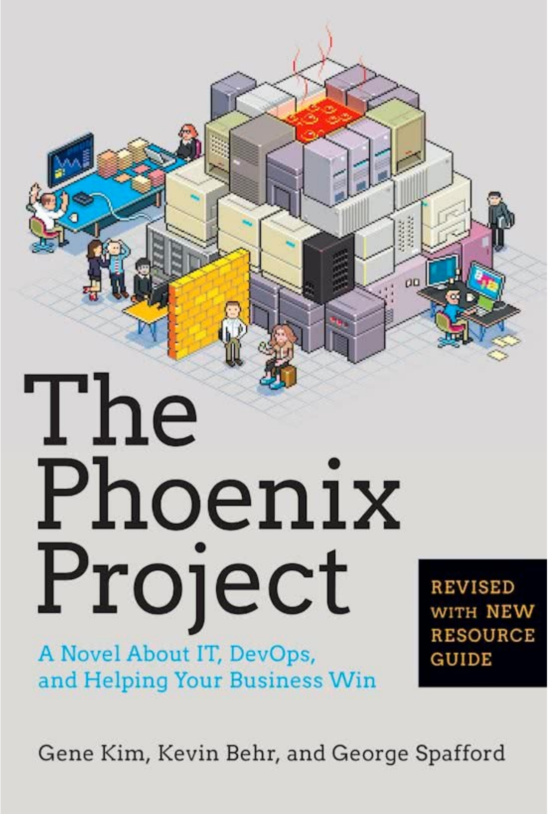
Science of DevOps

- Four measures of software delivery performance:
  - Deploy frequency
  - Lead time
  - Mean time to restore
  - Change fail percentage
- High performers spend 50% less time remediating security issues


THE SCIENCE OF LEAN SOFTWARE AND DEVOPS
ACCELERATE
Building and Scaling High Performing Technology Organizations
Nicole Forsgren, PhD
Jez Humble, and Gene Kim
with forewords by Martin Fowler and Courtney Kissler
and a case study contributed by Steve Bell and Karen Whitley Bell

Lean production & the three ways of DevOps

1. Systems thinking:
   reduce Muda, Mura, Muri
2. Rapid feedback loops: Jidoka
3. Continuous improvement:
   Kaizen, Chaos engineering


The Phoenix Project
REVISED WITH NEW RESOURCE GUIDE
A Novel About IT, DevOps, and Helping Your Business Win
Gene Kim, Kevin Behr, and George Spafford

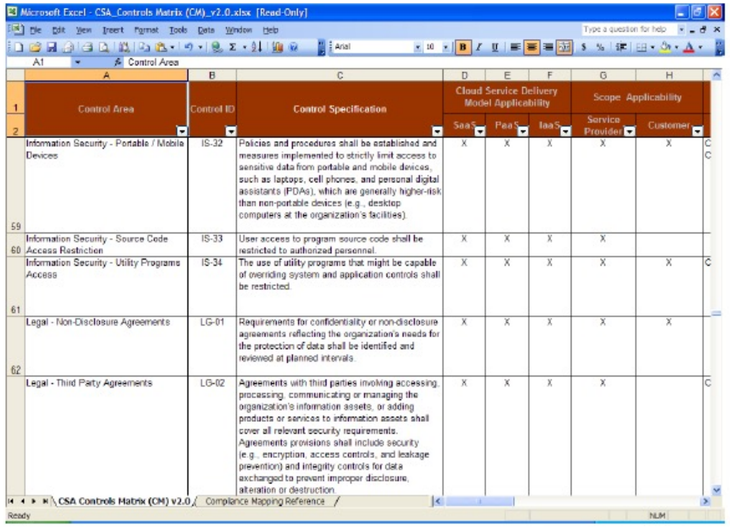
ClubCloudComputing

CD controls sample

- IDE based Static Testing
- Automated unit testing
- Digitally signing binary artefacts and storing them in secure repositories.
- Secure, automated configuration management and provisioning
- Infrastructure is code, version it
- Targeted dynamic scanning (DAST)
- Production monitoring
- Chaos Monkeys
- Source code, library and OS provenance

Cloud Security Alliance
Cloud Control Matrix

- CSA: dominant industry coalition
- Cloud Controls Matrix version
  - Aligned with CSA Guidance
- CCM features:
  - 16 control areas, ~132 controls
  - Selectable by S-P-I, Provider/Tenant
  - Cross referenced to ISO 27001, COBIT, HIPPAA, PCI-DSS etc.

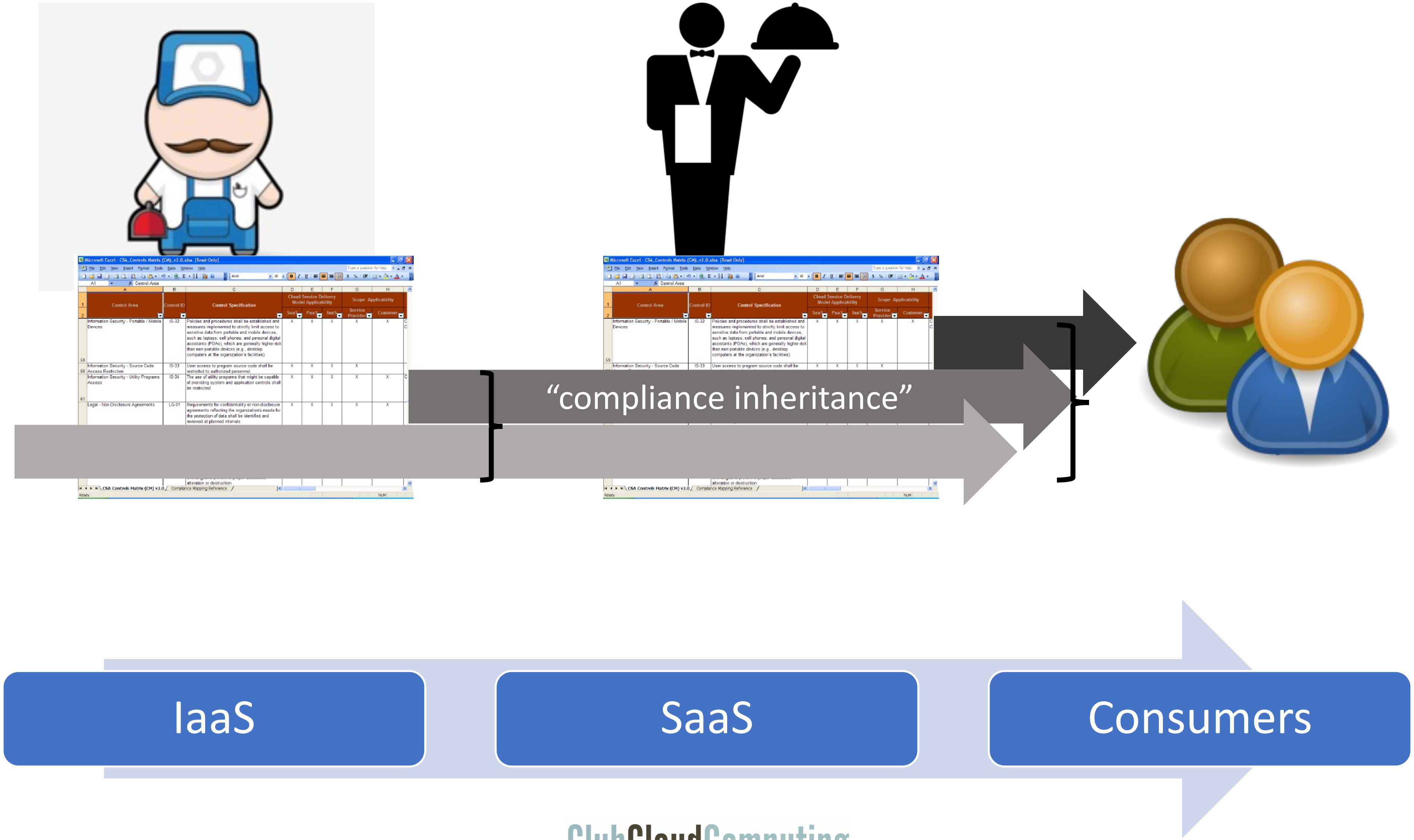

Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial
10
A1
Control Area
CSA Controls Matrix (CM) v2.0
Compliance Mapping Reference
Ready
NUM

	A	B	C	D	E	F	G	H	
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
2				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

cloud CSA security alliance

CCM™ Cloud Controls Matrix

CCM in a simple supply chain



Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

A1 Control Area

	A	B	C	D	E	F	G	H
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
2				SaaS	PaaS	IaaS	Service Provider	Customer
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X
	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X
			alteration or destruction.					

CSA Controls Matrix (CM) v2.0 / Compliance Mapping Reference

Ready NUM

Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

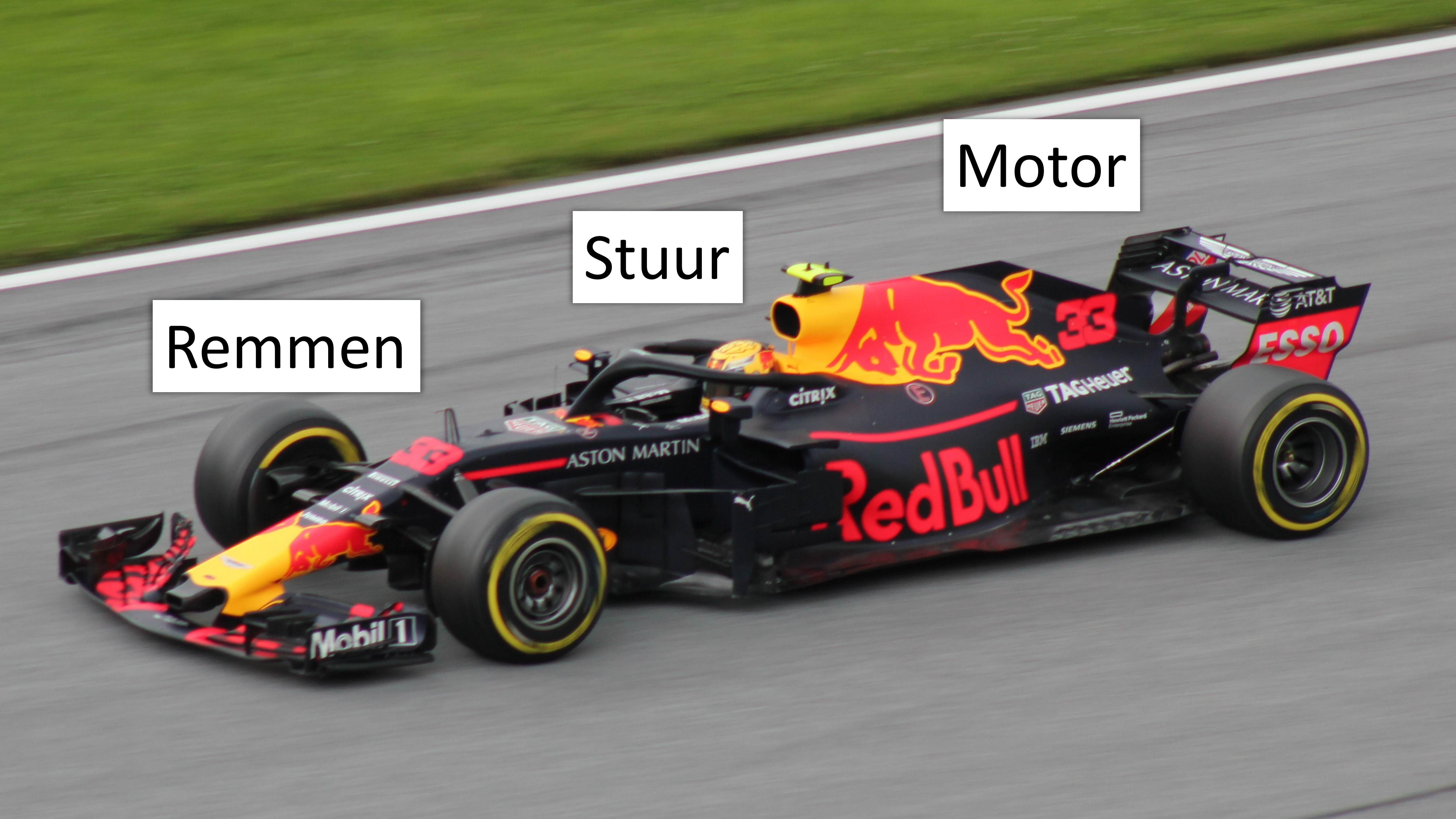
A1 Control Area

	A	B	C	D	E	F	G	H
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
2				SaaS	PaaS	IaaS	Service Provider	Customer
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
60	Information Security - Source Code	IS-33	User access to program source code shall be	X	X	X	X	

CSA Controls Matrix (CM) v2.0 / Compliance Mapping Reference

Ready NUM

ClubCloudComputing



Remmen

Stuur

Motor

Continued education

CCSK™

Certificate of
Cloud Security Knowledge

CCAK™

Certificate of Cloud Auditing Knowledge

A Cloud Security Alliance® and ISACA® Credential

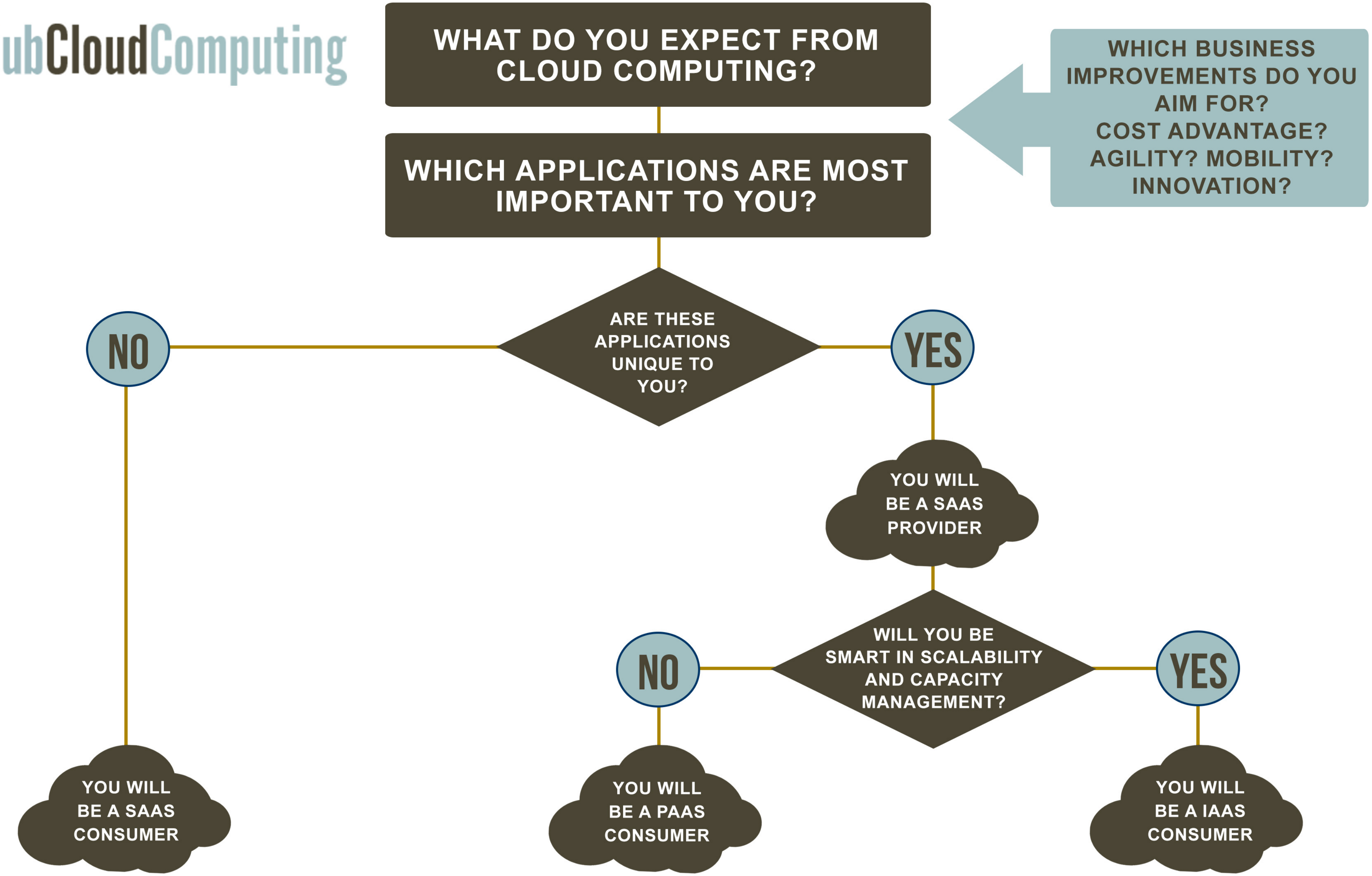
Dank U

- Vragen?

- LinkedIn: Peter H J van Eijk
- YouTube: ClubCloudComputing
- www.clubcloudcomputing.com
- Workshop.clubcloudcomputing.com

WHICH CLOUD SERVICE MODEL IS RIGHT FOR YOU?

ClubCloudComputing



WHAT DO YOU EXPECT FROM CLOUD COMPUTING?

WHICH BUSINESS IMPROVEMENTS DO YOU AIM FOR?
COST ADVANTAGE?
AGILITY? MOBILITY?
INNOVATION?

WHICH APPLICATIONS ARE MOST IMPORTANT TO YOU?

ARE THESE APPLICATIONS UNIQUE TO YOU?

NO

YOU WILL BE A SAAS CONSUMER

YES

YOU WILL BE A SAAS PROVIDER

WILL YOU BE SMART IN SCALABILITY AND CAPACITY MANAGEMENT?

NO

YOU WILL BE A PAAS CONSUMER

YES

YOU WILL BE A IAAS CONSUMER

READ MORE ON HTTP://WWW.CLUBCLOUDCOMPUTING.COM/2014/04/CLOUD-SERVICE-MODEL-RIGHT/

Lift & shift risks

- cost optimization (e.g. network cost)
- performance (latency)
- visibility (logging)
- implicit security controls missing (access control)
- legal risk (jurisdiction)
- missing opportunities (scalability)
- lack of migration planning