exoscale

Cloud Security Frameworks

GITI

May 8, 2014

about: me

CEO: Antoine Coetsier

- Infrastructure and datacenters expert
- Team and datacenter Manager for more than 10 years

Experience

- Managing Director of exo**scale** since inception (2011)
- Responsible for strategy and cloud offering at VeePee (2008-2012)
- Systems Architect and Project Manager of large IT operations at Bouygues Telecom

Education

- IT Engineer degree at École centrale d’Electronique (1999-2002)
- CCSK: Certificate of Cloud Security Knowledge (2012)

exoscale in a nutshell...

The safe home for your cloud applications

... an IaaS provider and beyond

- **Cloud hosting based on latest technology**
  - Flexible server and storage infrastructure
  - Trimmed for performance, intuitive usability and tooling
- **Market place for value added applications**
  - One-stop-shop to reduce infrastructure complexity for developers and sysadmins

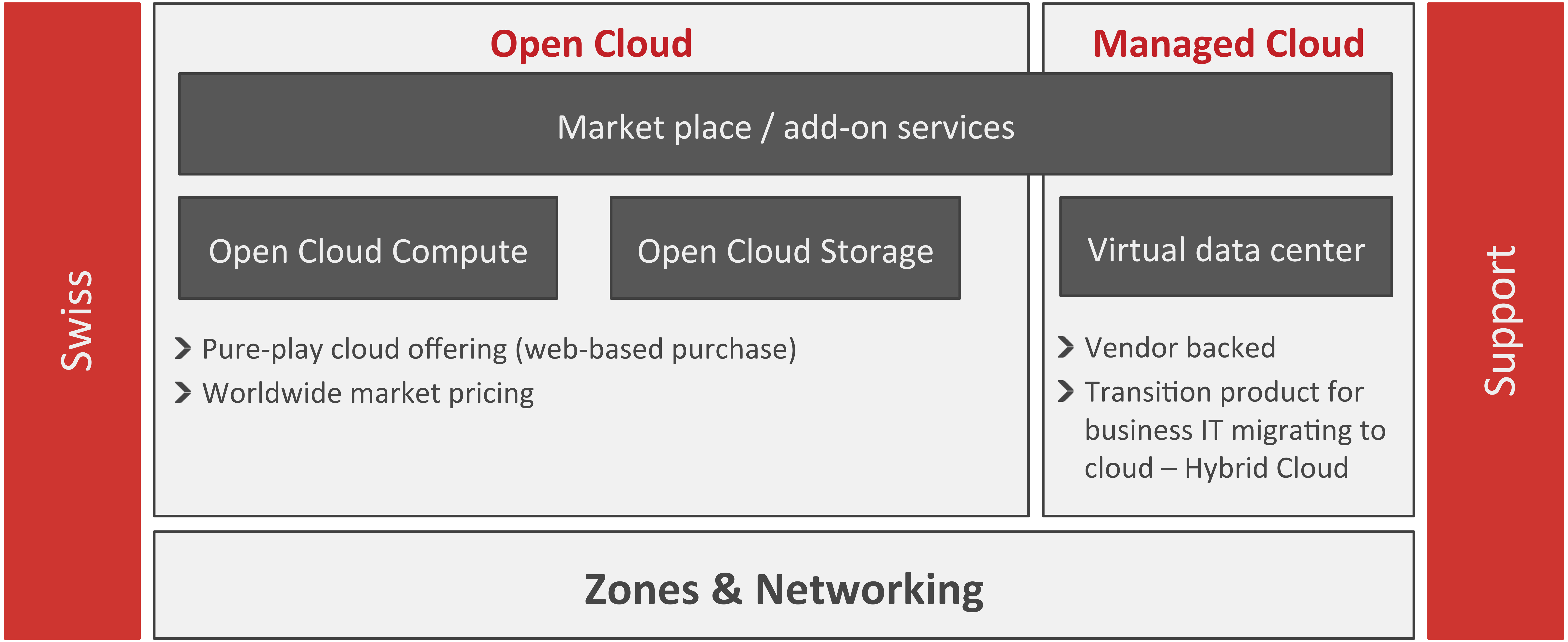
... with a solid background

- **Spin-off from Veltigroup**
  - Started 2011 within Veltigroup
- **Swiss company**
  - Proximity to EMEA clients
  - Swiss data privacy standards

IaaS: Infrastructure-as-a-Service
EMEA: Europe, Middle East and Africa

exoscale offering overview

Solid cloud hosting and add-on services



Swiss

Open Cloud

Managed Cloud

Market place / add-on services

Open Cloud Compute

Open Cloud Storage

Virtual data center

- Pure-play cloud offering (web-based purchase)
- Worldwide market pricing

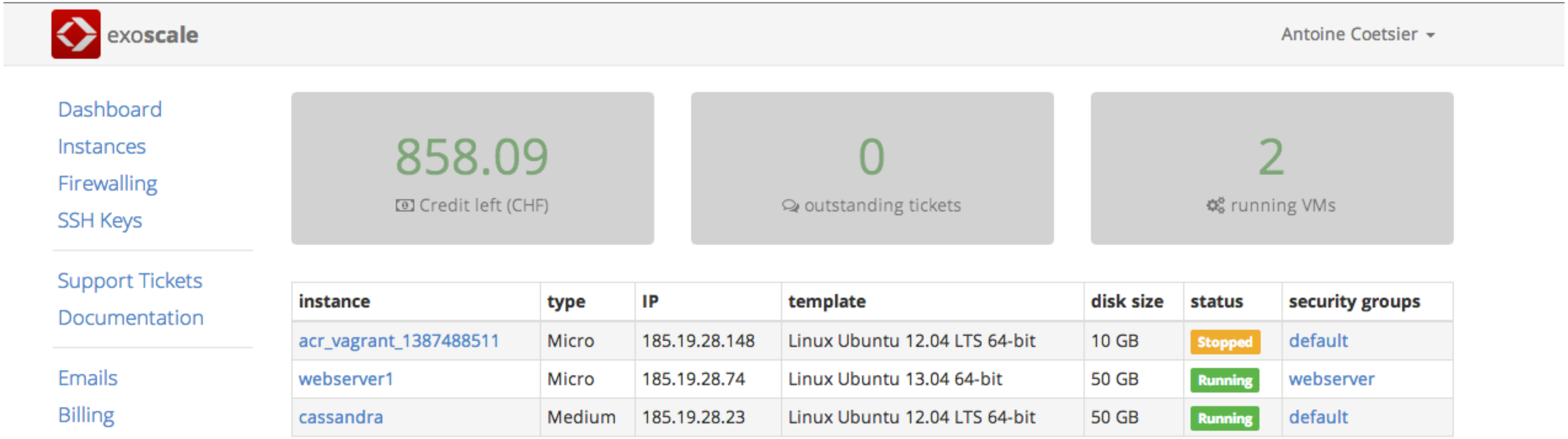
- Vendor backed
- Transition product for business IT migrating to cloud – Hybrid Cloud

Zones & Networking

Support

Open Cloud compute: a unique portal

- One comprehensive portal for instance management, support, documentation and billing information



exoscale

Antoine Coetsier

858.09
Credit left (CHF)

0
outstanding tickets

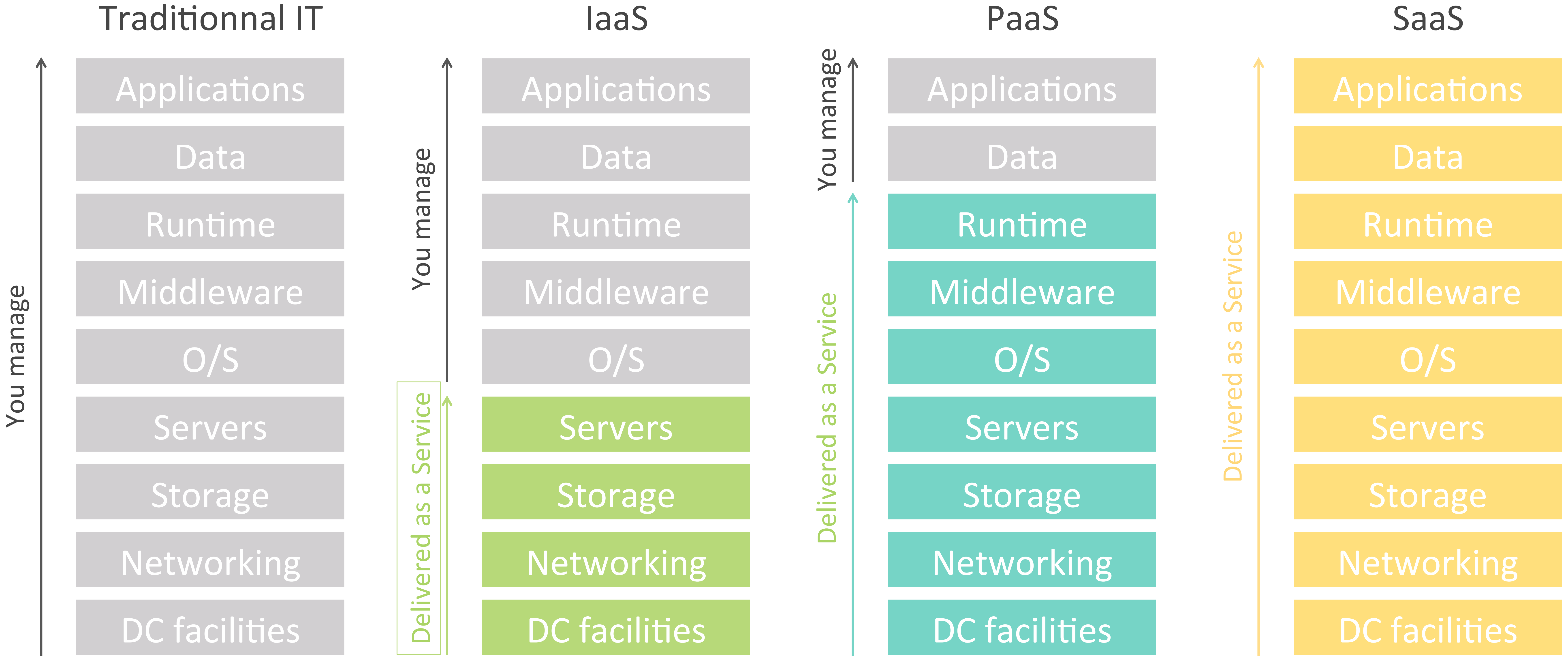
2
running VMs

instance	type	IP	template	disk size	status	security groups
acr_vagrant_1387488511	Micro	185.19.28.148	Linux Ubuntu 12.04 LTS 64-bit	10 GB	Stopped	default
webserver1	Micro	185.19.28.74	Linux Ubuntu 13.04 64-bit	50 GB	Running	webserver
cassandra	Medium	185.19.28.23	Linux Ubuntu 12.04 LTS 64-bit	50 GB	Running	default

Migrating to a cloud service

- 1st concern is always security
- Existing guidelines are not fit for purpose
  - ISO 27001
  - ...
- What is the data at stake ?
- Dealing with issues

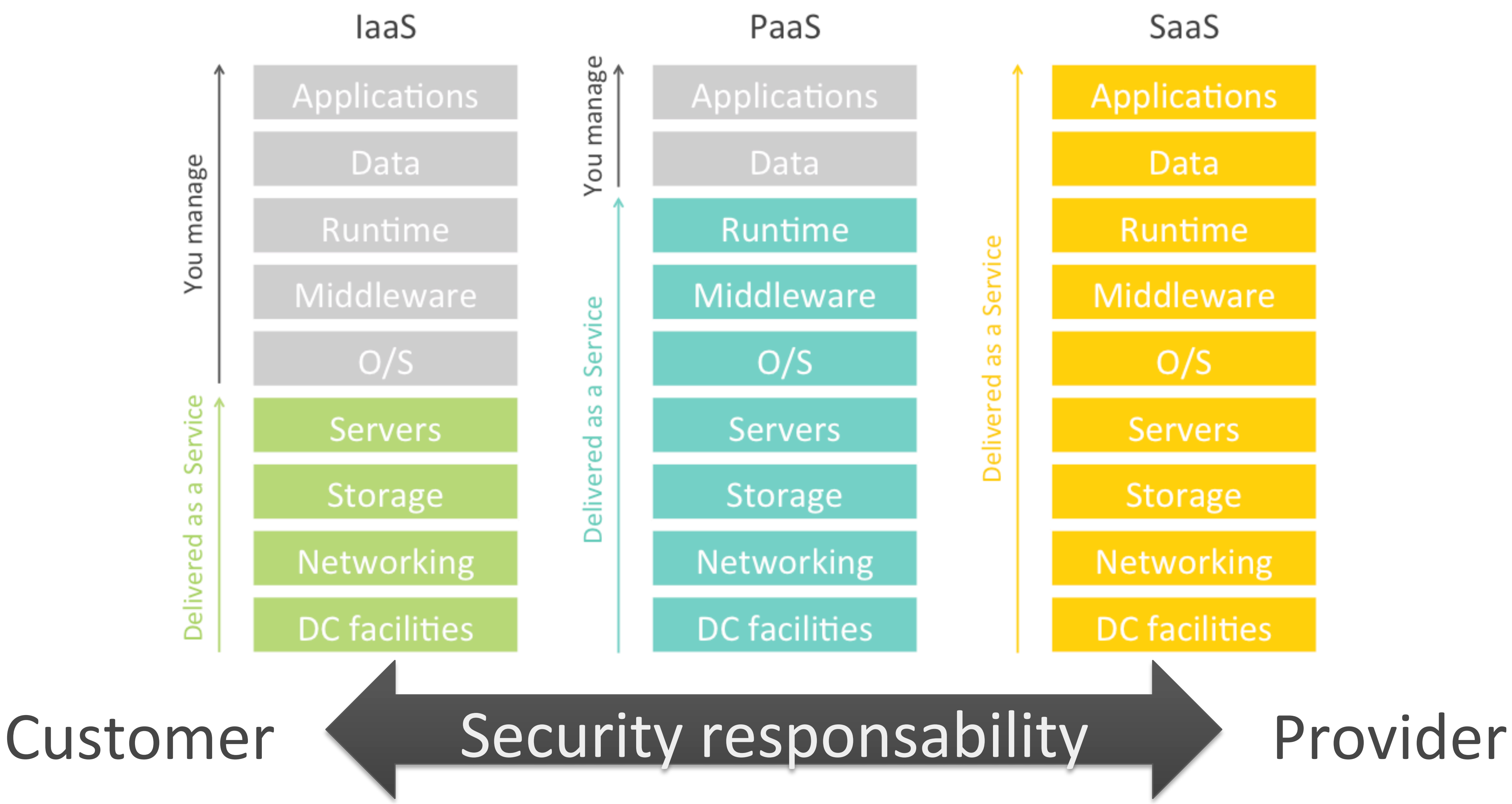
Cloud computing segmentation



Traditionnal IT	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
DC facilities	DC facilities	DC facilities	DC facilities

Roles and responsibilities

- Roles and responsibilities vary upon the cloud model chosen :
  - “The lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.”



IaaS	PaaS	SaaS
Applications	Applications	Applications
Data	Data	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking
DC facilities	DC facilities	DC facilities

IaaS: You manage (Applications to O/S); Delivered as a Service (Servers to DC facilities)

PaaS: You manage (Applications, Data); Delivered as a Service (Runtime to DC facilities)

SaaS: Delivered as a Service (Applications to DC facilities)

Customer ⟷ Security responsability ⟷ Provider

Existing frameworks

- They focus on on aspect:
  - Datacenter
  - Acces control process
  - …

- Not on the service

SCOPE PROBLEM

Framework for cloud services

Non profit organization formed to promote

- Best practices for providing security within the Cloud,
- Provide education for the use of Cloud solutions
- Define guidance and actionable documents

Alliance

- Established in 2008, gained significant traction in 2011
- Not (too) commercial or one sided governed

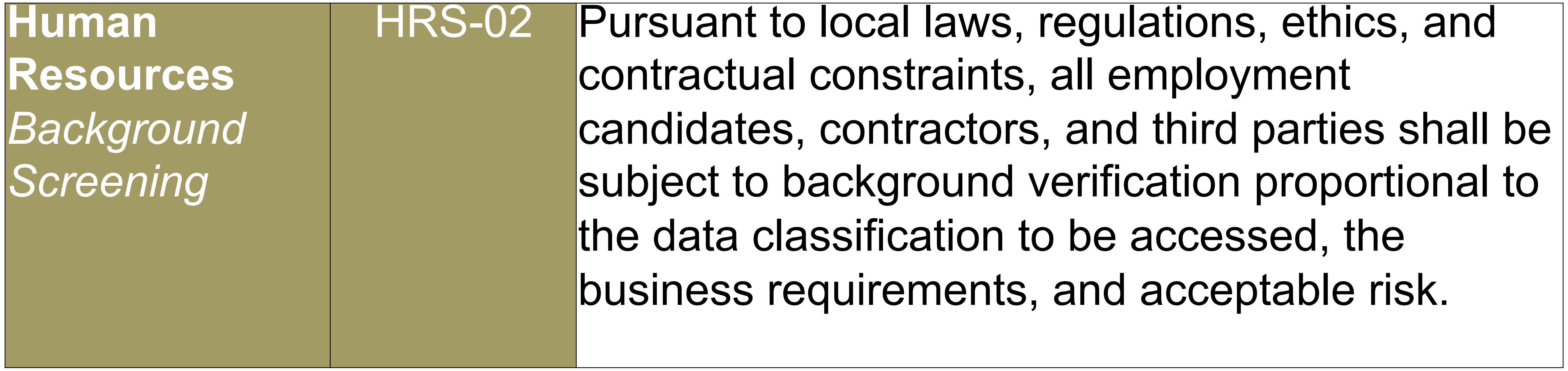
Cloud Security Alliance

Define best practices in a Cloud Control Matrix (CCM)

- +130 points dealing with a large scale of competences :
  - Data Governance
  - Facility
  - HR
  - Information Security
  - Legal
  - Risk Management
  - Security Architecture

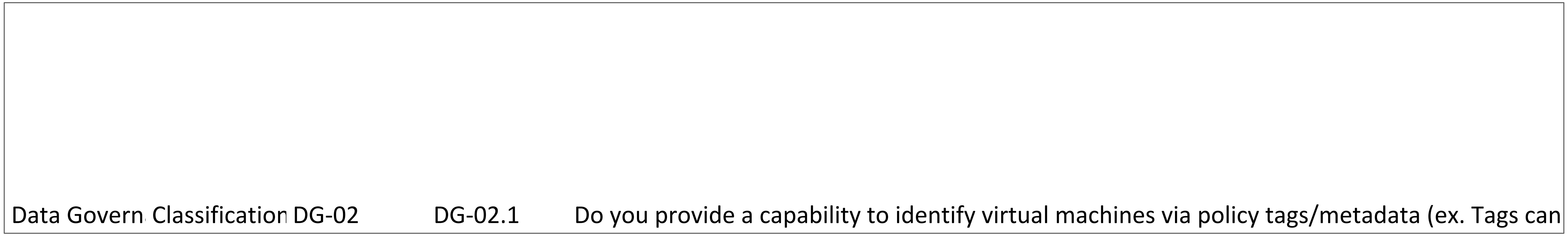
Commercial note: exoscale has documented all points of the CCM

Example



Human Resources *Background Screening*	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.

CAIQ: consensus assessments initiative questionnaire

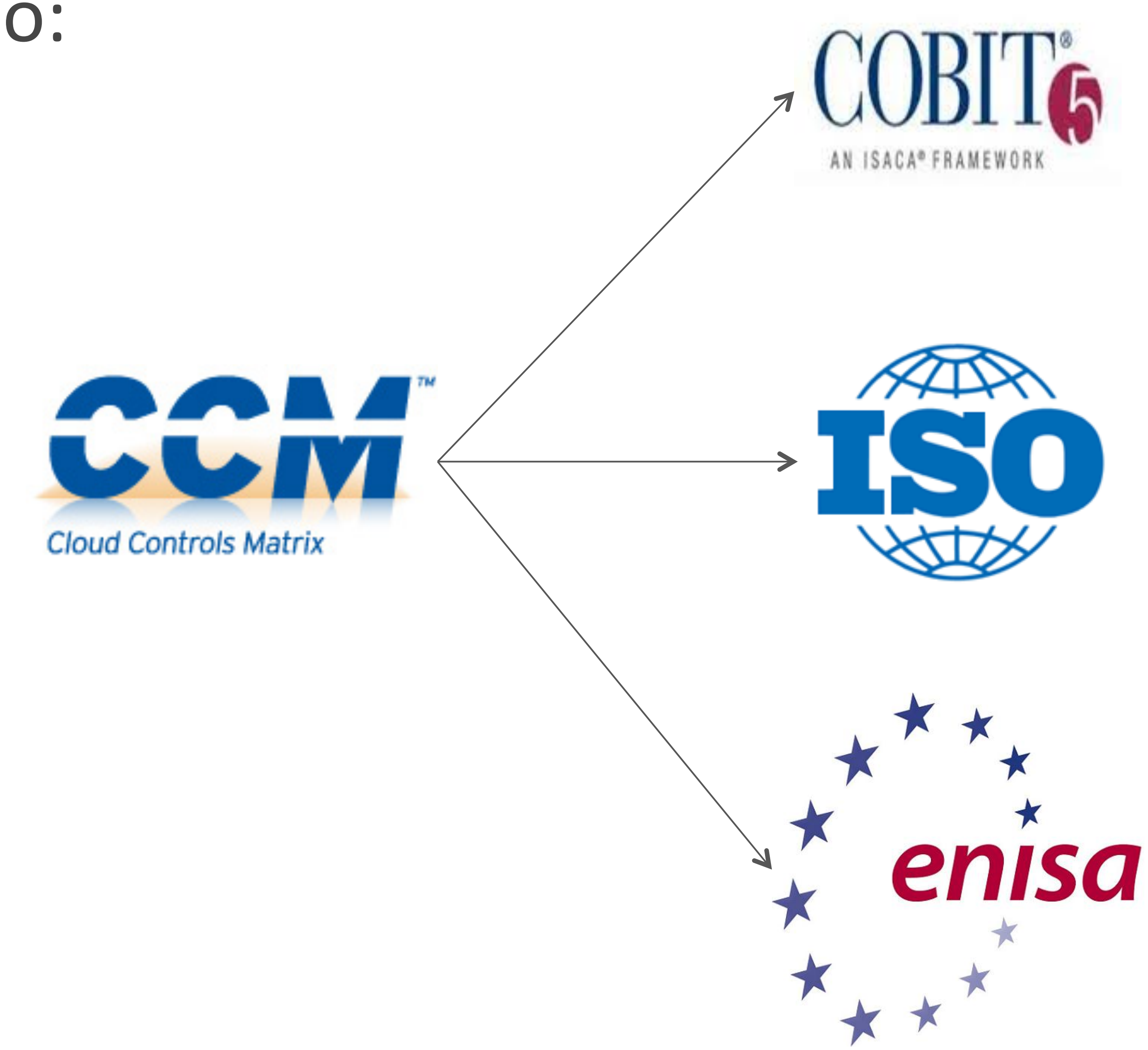


Data Govern	Classification	DG-02	DG-02.1	Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can

Cloud Security Alliance mapping

OCF Level 1 : The Cloud Control Matrix

- v 3 Released
- Controls baselined and mapped to:
  - COBIT
  - HIPAA / HITECH Act
  - ISO/IEC 27001-2005
  - NISTSP800-53
  - FedRAMP
  - PCI DSSv2.0
  - BITS Shared Assessments
  - GAPP ...



Risk Management regarding data

- What is the data at stake ?
- Personal/employees data
- Sensible data
- Regulated data
- Is this data meaning full or valuable to someone else ?

Data classification

- Any data we handle, has been classified in our systems and been given policies regarding the following actions:
  - Create
  - Store
  - Use
  - Share
  - Archive
  - Destroy

- Each class has its own rules and level of protection:

- Standard classes:
  - Low: civility,...
  - Medium: logs,...
  - High: authentication secret

- Special classes:
  - Credit card information: not stored
  - Forbidden information: racial, political,...

Reversibility

Ownership

- Using a cloud service, should not enable the transfer of ownership of the data
- As a general rule:
  - IaaS and PaaS services must stipulate that the data remains your property
  - SaaS services: look closely, especially for main stream services

Reclaim

- Can I reclaim/transmit data at any time?
- What happens in case of contract breach, bad SLAs, change of control of the provider, discontinuation of the service,...
- The answer has to be both technical and legal

The key is contractual

- Read the contract or terms and conditions

- Track changes
  - –Initiatives like http://tosdr.org/ “Terms of Services: didn’t read” emerged

Wrap up

- Classify your data
- Request a security alignment
- Review your contracts
  - Reversibility
- Hosting locally (in Switzerland) is easier
  - But does not prevent all the above

My recommendations

- Be ready !

1. **Test** even if you do not have a business case
2. Make a proof of **concept**
3. Rent a **tenant**
4. **Security is about CONTROL**

☑ **PROACTIVE**

□ **~~REACTIVE~~**