

CLOUD COMPUTING

**OVERVIEW OF CLOUD COMPUTING
PRINCIPLES AND TECHNOLOGIES**

Peter R. Egli
INDIGOO.COM

Contents

1. What is cloud computing?
2. Why cloud computing?
3. Typical IaaS, PaaS, SaaS providers
4. Cloud provider landscape
5. Technology foundation of cloud computing
6. Cloud computing versus outsourcing
7. Hybrid clouds
8. Cloud scalability
9. Cloud security
10. Cloud risk management
11. Cloud certifications
12. Cloud standards
13. More cloud service models
14. Cloud management platforms (CMP)

1. What is cloud computing? (1/5)

Could computing definition by NIST:

NIST (National Institute of Standards and Technology, US non-regulatory federal agency) published a widely used and accepted definition of cloud computing:

«Cloud computing is a model for enabling **ubiquitous**, convenient, **on-demand network access** to a **shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with **minimal management effort** or **service provider interaction**».

Source: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

NIST defines cloud computing around

5 essential characteristics

3 service models

4 deployment models

1. What is cloud computing? (2/5)

5 essential key characteristics of clouds:

On-demand self-service computing resources (elasticity):

- Automatic provisioning without human interaction with service provider.

Broad network access:

- Availability of cloud resources through various platforms (desktops, mobiles, workstations).

Resource pooling:

- Sharing of provider resources among customers (multi-tenant model).
- Location transparency (customer is not aware of the location of the server resources).

Rapid elasticity:

- Resources can be allocated and released to scale according to demand.

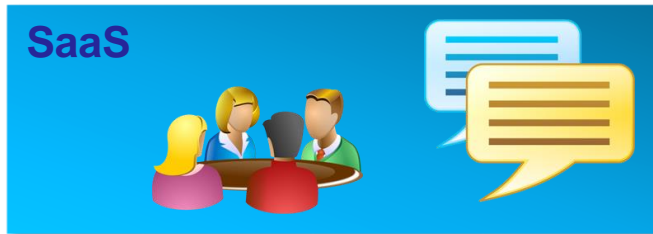
Measured service:

- Monitoring resource usage, service assurance (SLA – Service Level Agreement).

1. What is cloud computing? (3/5)

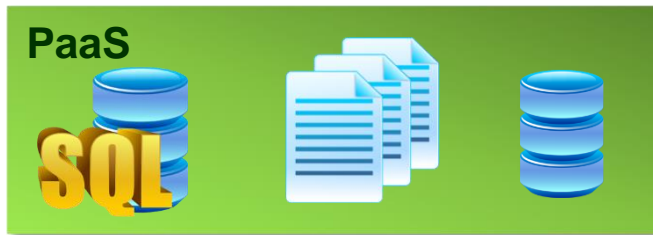
3 service models (1/2):

3 service models define the level of cloud service.



SaaS - Software as a Service:

SaaS builds on top of PaaS and provides application-level services such as collaboration, ERP and document management.



PaaS - Platform as a Service:

PaaS provides platforms and run-time environments including middleware, messaging, databases and identity management.



IaaS – Infrastructure as a Service:

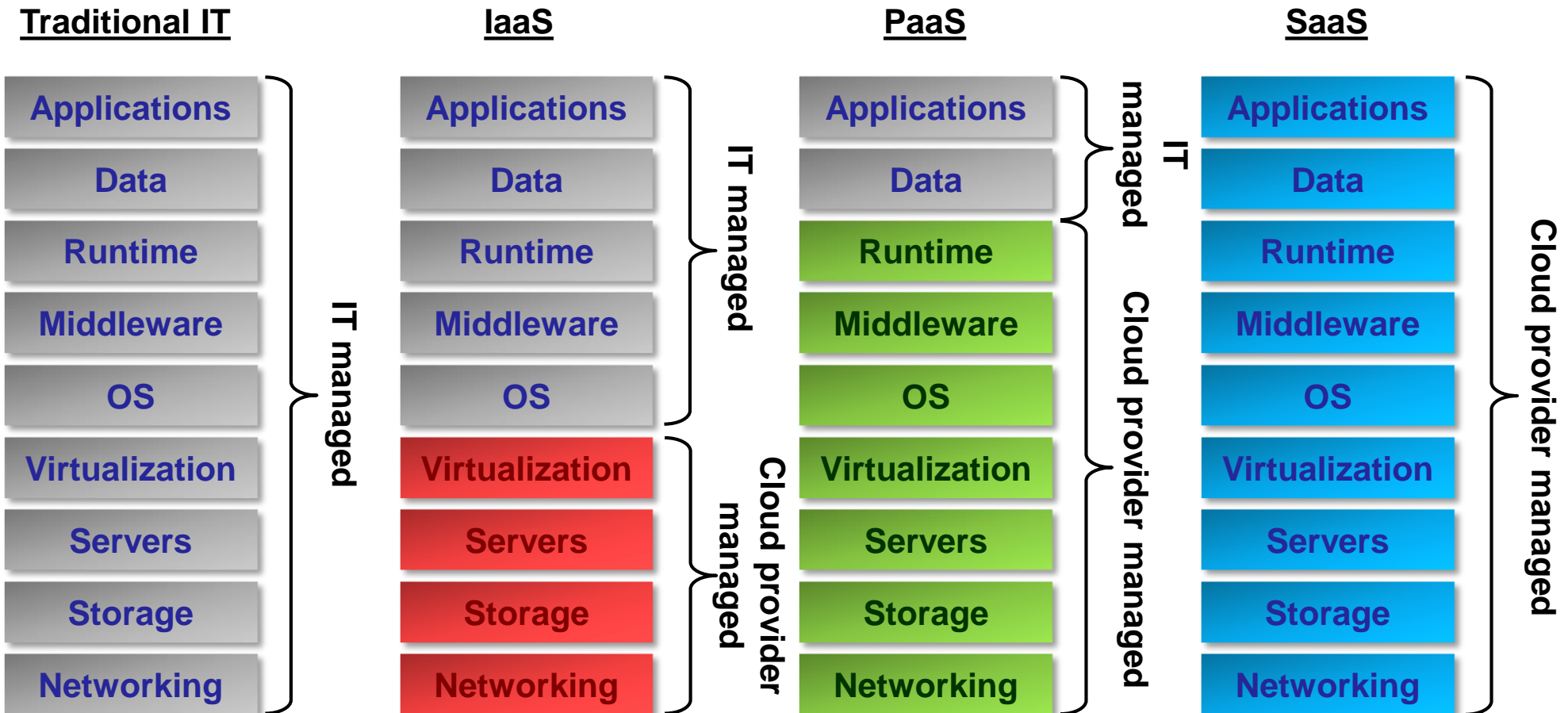
IT infrastructure is provided as a service.

IaaS comprises resources such as servers, network and simple mass storage.

1. What is cloud computing? (4/5)

3 service models (2/2):

IaaS, PaaS and SaaS define different levels of cloud services with regard to the traditional IT stack that is entirely managed by the inhouse IT department.



1. What is cloud computing? (5/5)

4 cloud deployment models:

Private cloud:

- Cloud is enterprise owned or leased.
- Cloud is used by a single enterprise or organization.
- Cloud equipment may exist on- or off-premise.
- Private cloud may be internal (company premises) or external (provider hosted).
- Typically operated by a third-party with the required skills to lower operating costs.

Community cloud:

- Shared infrastructure for a specific community.
- May exist on- or off-premise.

Public cloud:

- Cloud is sold to the public, mega-scale infrastructure.
- Exists on premises of cloud provider.

Hybrid cloud:

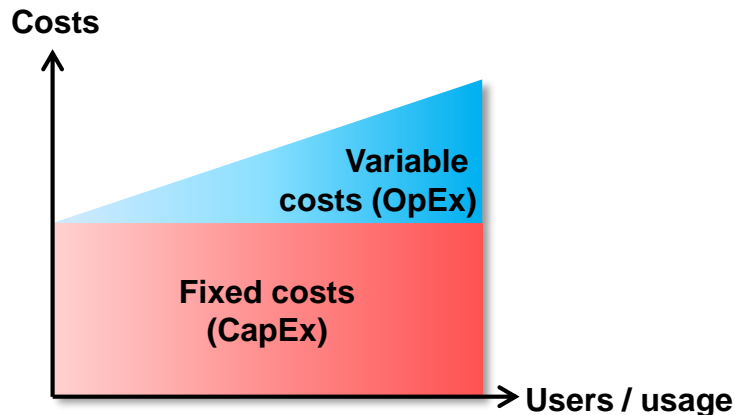
- Different cloud types combined.
- Typically the base load is covered by a private cloud, load bursts handled by a public cloud computing resources («cloud bursting», «pay-as-you-go» cost model).

2. Why cloud computing? (1/3)

The rationale of cloud computing (for the customer) is reduced and linearly scaling costs.

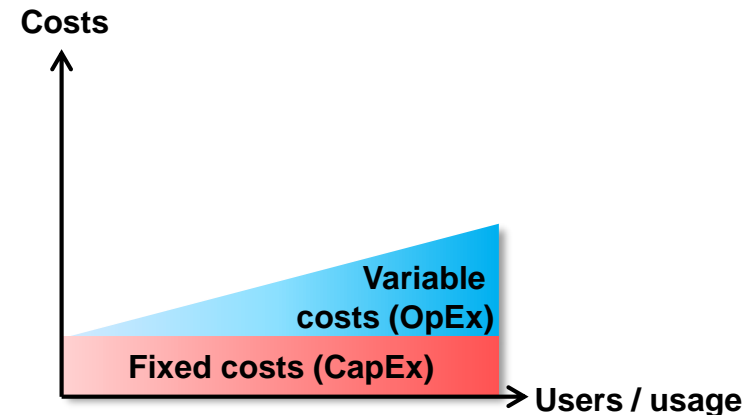
Cloud computing allows allocating required computing resources dynamically to demand. It scales linearly with the number of users, i.e. incurs no or little capital expenses (capex), only operating expenses (opex).

Traditional IT:



Data centers, servers etc. require a large up-front investment (CapEx). The infrastructure must be dimensioned to accommodate a certain peak load. Variable costs incur on top of CapEx (run-time licenses for users etc.).

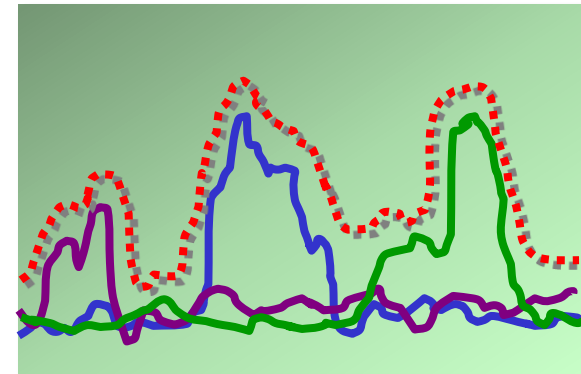
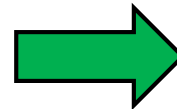
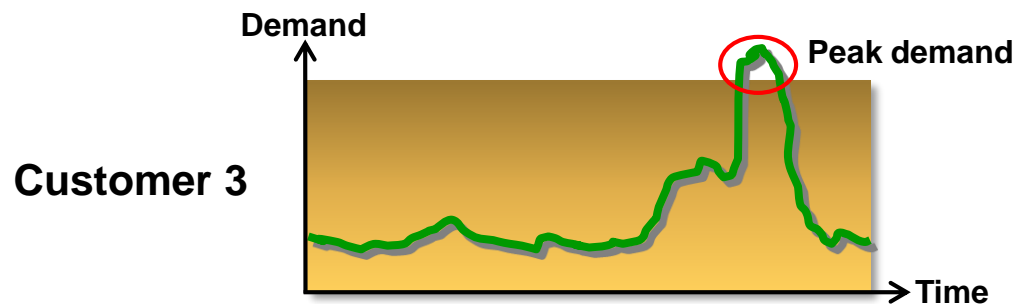
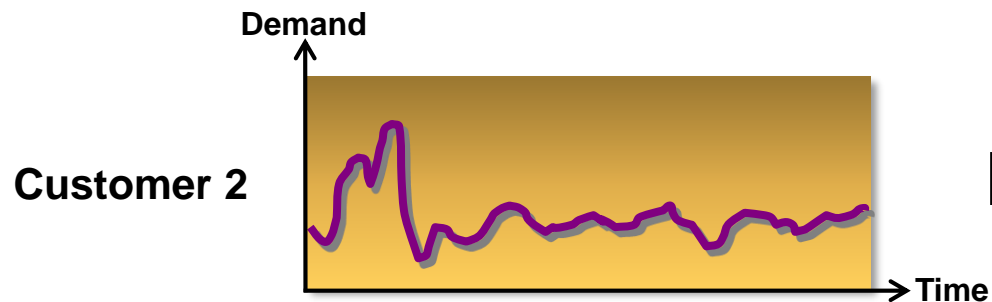
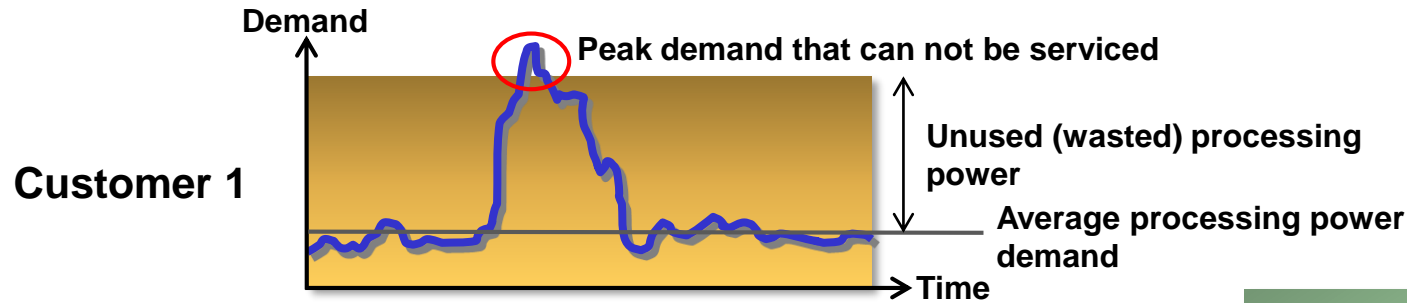
Cloud computing:



Fixed costs are transferred to the cloud provider and thus largely reduced for the customer (customer infrastructure reduced to network, workstations). Variable costs vary according to usage demand. The variable costs are reduced since the cloud provider exploits economy of scale.

2. Why cloud computing? (2/3)

By means of pooling, a reduced number of servers can deliver the processing power demands of multiple customers (scaling effect) because customer's processing demands are distributed over time (statistical multiplexing).



Combined processing power demand profile.
Provisioned server performance can accommodate peak demands of customers.

→ «Peak of sums < sum of peaks».

2. Why cloud computing? (3/3)

Business drivers for cloud computing:

- **High costs due to high server performance requirements to meet peak demands (low average server capacity usage: 15%).**
- **Avoidance of CapEx.**
- **Need for reduction of data center energy consumption.**
- **High IT maintenance costs (IT staff, licenses).**
- **Meet compliance requirements (data protection, security, data center access etc.).**
- **Need for flexible data center usage arrangements (scale up when need arises for peak performance demands).**

Potential cost savings with cloud computing 50 – 90%.

3. Typical IaaS, PaaS, SaaS providers

Some key players in the cloud market:

SaaS



MS Office and collaboration appl.

Cloud based CRM.

Cloud based ERP.

PaaS



OS, node.js platform.

Google App Engine (Java platform).

Development and hosting platform.

IaaS



Cloud servers.

Content Delivery Network.

Simple storage.

4. Cloud provider landscape (1/2)

Cloud Service Providers (CSP):

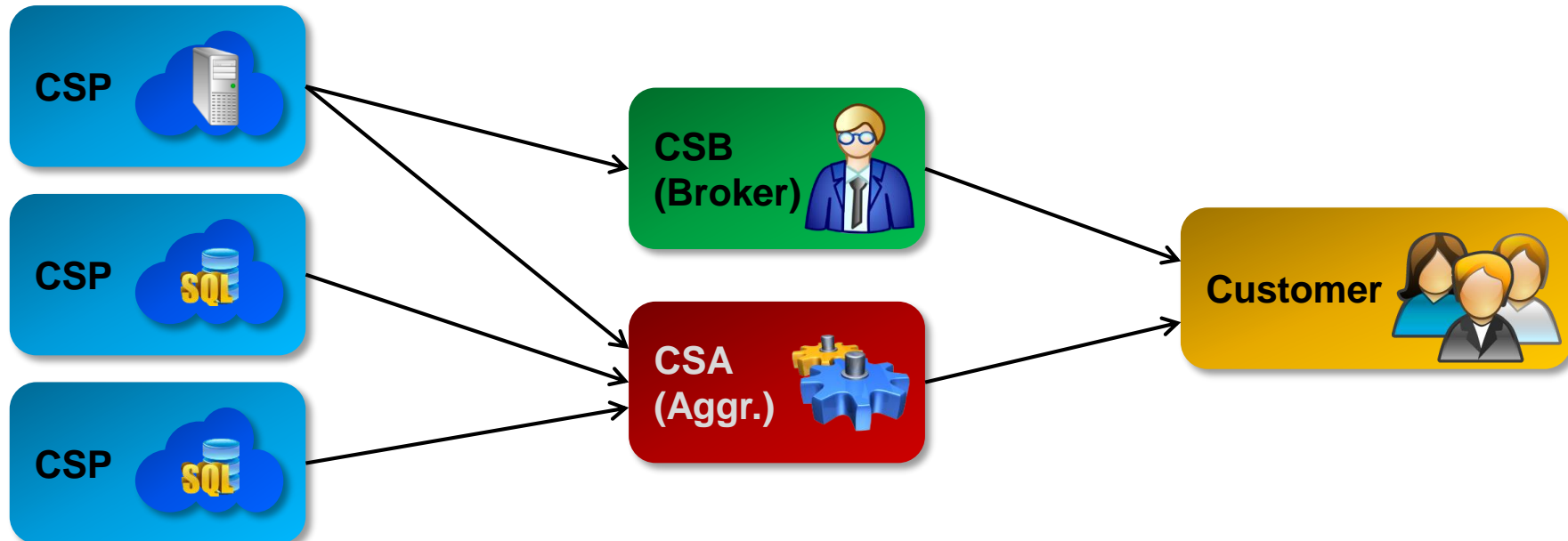
CSPs offer IaaS, PaaS and SaaS services as private, hybrid or public clouds.

Cloud Service Brokers (CSB):

CSBs resell and sometimes integrate CSP cloud services. CSBs focus on consultancy services, (help customers choose the right cloud solution, provide best practices for cloud deployment).

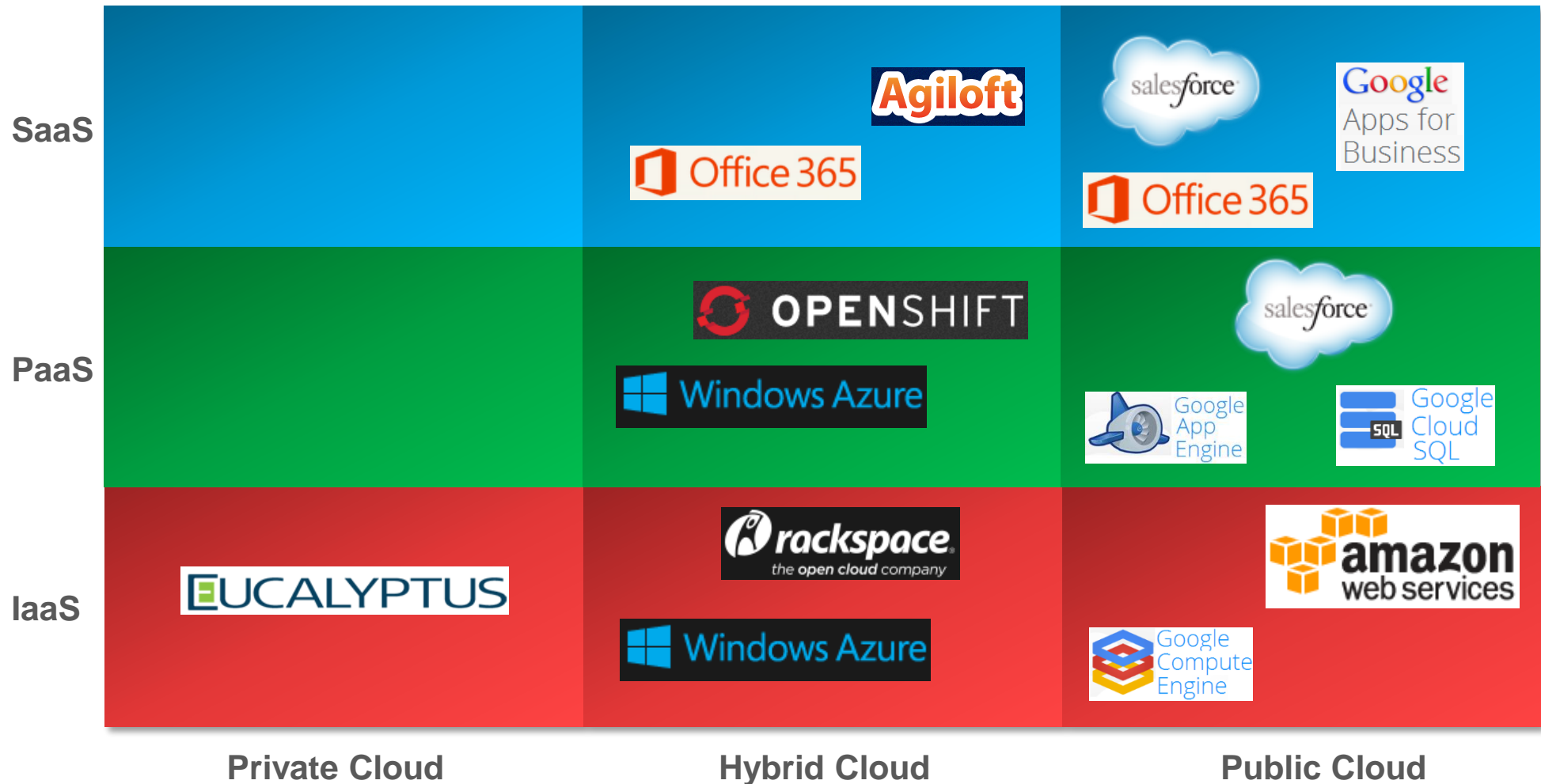
Cloud Service Aggregators (CSA):

CSAs integrate cloud services into value-added services, e.g. bundling storage services from different CSPs into a high-availability offering.



4. Cloud provider landscape (2/2)

IaaS, PaaS and SaaS Cloud Service Providers (CSP):



5. Technology foundation of cloud computing (1/2)

Cloud computing is based on and made possible by a number of technologies.

Virtualization:

Virtualization (VMs – Virtual Machines) is a crucial technology to completely decouple OS and software from the underlying hardware. This allows running multiple OS instances on a single server hardware.

Grid technology:

Often cloud computing is based on some kind of grid computing where a large number of physical servers is available to host and run cloud infrastructures, platforms and applications. When demand arises, services can be moved around the grid environment.

Broadband network access:

Diminishing differences in network bandwidth between LAN and WAN access make it possible to move entire applications to clouds.

Distributed computing:

Middleware and particularly web services provide the necessary interoperability for cloud-based distributed applications.

5. Technology foundation of cloud computing (2/2)

Web technologies:

Web technologies, namely the HTTP/HTML/CSS/Javascript combo, define an interoperable standard client interface.

Security protocols and technologies:

Security is essential for cloud computing. The necessary technologies for authentication, privacy, authorization, key distribution and trust federation are available on different platforms.

Service orientation:

SOA as a core architectural principle allows to compose applications of a collection of services, each of which can be hosted in a cloud-based environment.

Open source software (OSS):

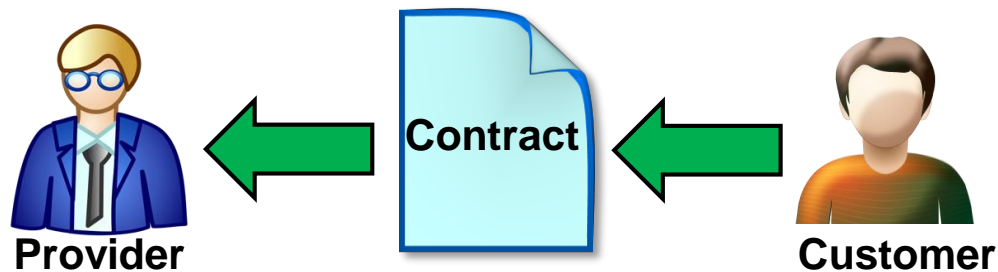
Clouds need tons of software. A wealth of open source software for virtually every aspect in cloud infrastructures is available and allows cloud providers to deliver high-level cloud services at reasonable costs.

6. Cloud computing versus outsourcing

Outsourcing:

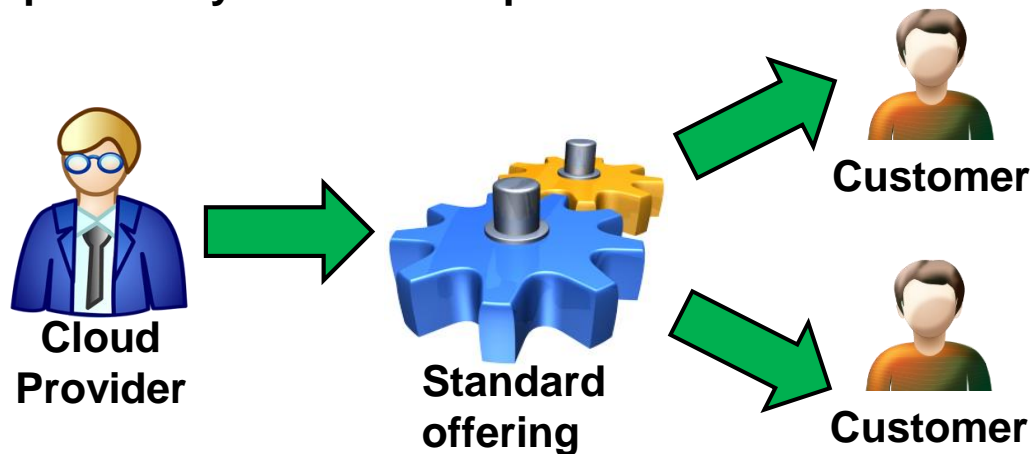
In a typical outsourcing arrangement, the providers offers a service according to the conditions of the customer.

Usually the contracts and SLAs are different for each customer.



Cloud:

Typical cloud providers have a standard offering, usually high-volume commoditized services without the possibility for custom specific extensions.



7. Hybrid clouds (1/2)

Why hybrid clouds?

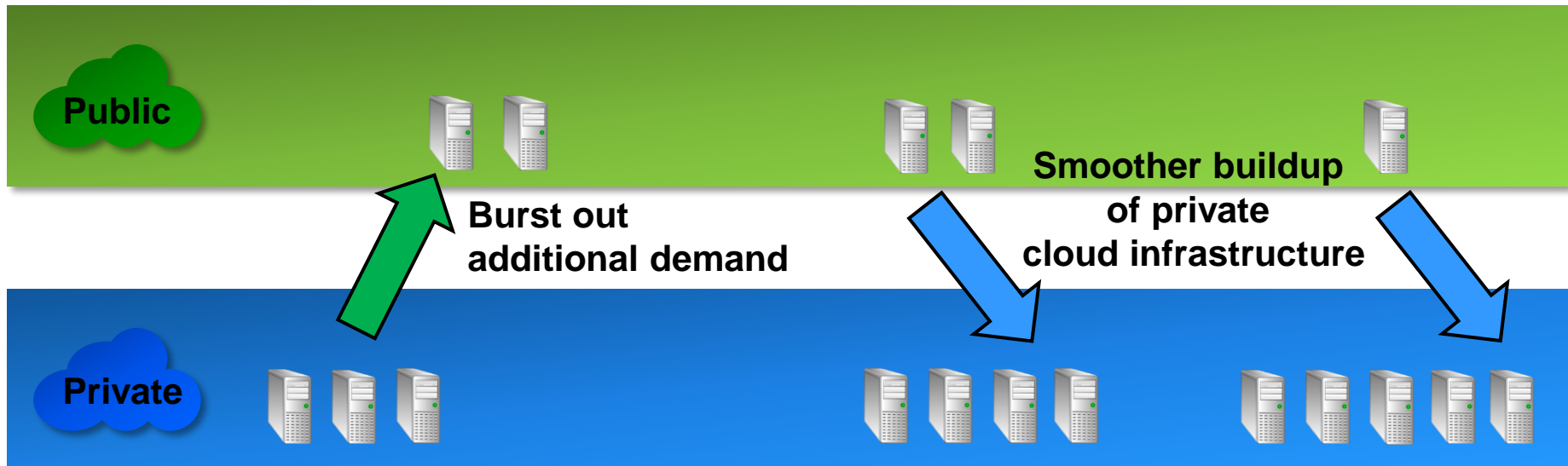
Hybrid clouds combine the benefits of private and public clouds.

Private clouds:

- Mainstay IT resources
- Privacy and security
- Enhanced control

Public clouds:

- Absorb temporal processing demand bursts (**cloud bursting**, load balancing)
- Provide business continuity in case of private cloud outages (disaster recovery)
- Help smooth out private cloud investments over time



7. Hybrid clouds (2/2)

Criteria for offloading to a public cloud:

While combining private and public clouds may bring overall benefit, a number of criteria need to be carefully assessed prior to deploying hybrid clouds.

- a. Level of security provided by public cloud provider
- b. SLA provided by public cloud provider (availability, recovery etc.)
- c. Compliance with data security regulations such as PCI DSS (Payment Card Industry)
- d. Network bandwidth demands between clients, servers and databases
- e. Platform requirements (Linux, Windows, software stacks, middleware and platforms)
- f. Compatibility of authentication, authorization and identity management between private and public cloud
- g. Unified management and administration of private and public clouds

8. Cloud scalability

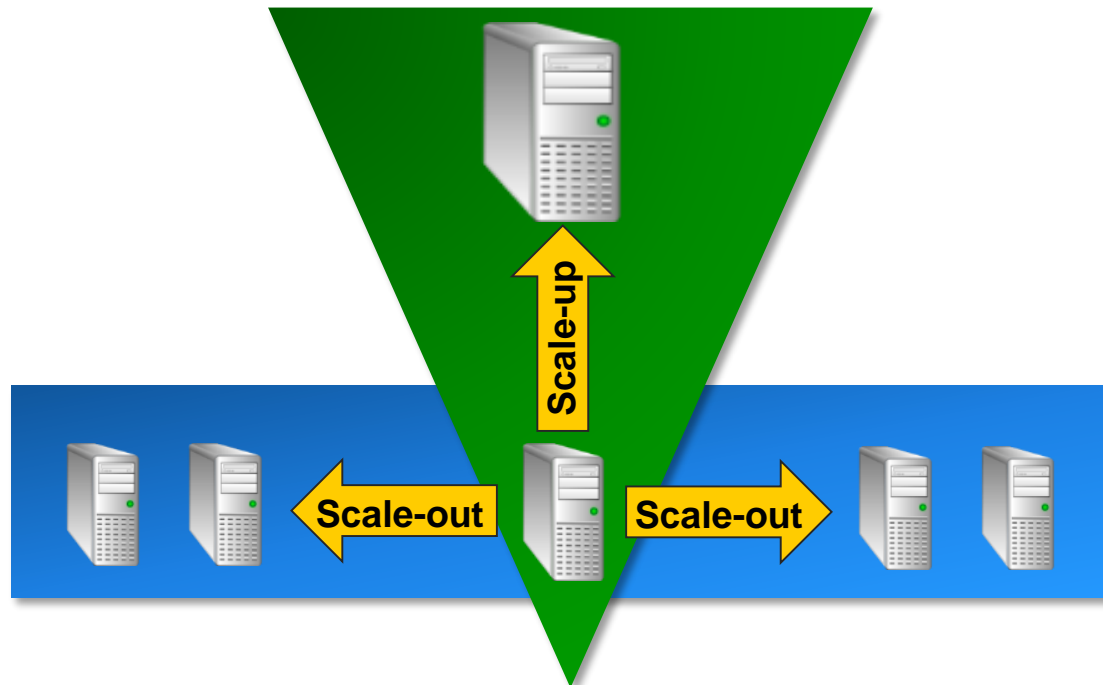
There are two main models for accommodating increased processing demand in clouds:

A. Scale-up (vertical scaling):

Increases in processing demand are accommodated by more powerful cloud server instances (virtual machines).

B. Scale-out (horizontal scaling):

Demand is accommodated with more instances (VMs).



9. Cloud security (1/2)

Typical cloud security concerns of customers:

- **Trust (do we trust the cloud provider?).**
- **Data ownership issues (what happens if cloud provider goes bankrupt?).**
- **Loss of physical control of data, infrastructure.**
- **Customer isolation (how good are customers technically isolated from each other).**
- **Legality of data transfer to an offshore cloud provider (see also «safe harbor»).**
- **Concern about moving data to cloud providers that are attractive targets for hackers and crackers (high value targets).**
- **Security of software components in the cloud infrastructure (are the components secure? Are they regularly updated with the latest security patches?).**
- **Availability concerns (cloud infrastructure outage may bring operations of a company down).**
- **Compliance and regulatory issues (HIPAA, SoX, ISO 27001, Basel II etc.).**

9. Cloud security (2/2)

Cloud security advantages:

Concerning security, clouds may also have advantages.

- **Dedicated security team (people trained for the purpose).**
- **Defined and standardized security, ideally an integrated part of the SLA (service level agreement).**
- **When customers use multiple cloud providers, applications are better isolated and protected than would be the case with BYO (build your own) IT infrastructure.**
- **Greater resilience to outages (often intrinsically supported by cloud infrastructure).**
- **Fault and redundancy mechanisms provided as part of the cloud offering.**
- **Compliance delivered by cloud provider as part of the offering.**
- **Defined monitoring and auditing of services by cloud provider.**

10. Cloud risk management (1/2)

What are the risks in clouds?

Traditional IT has its own set of risks to be addressed.

On top of these risks, cloud computing adds many more risks in various fields such as IT fragmentation ("shadow IT"), infrastructure security, compliance, business continuity and data management.

Deloitte's «Cloud Computing Risk Intelligence Map» provides an excellent overview of potential cloud risk areas.

Risk management frameworks:

A holistic approach for risk management is a must in every cloud strategy.

Risk management frameworks provide a structured and disciplined approach for managing ICT risks including:

- a. risk identification
- b. risk analysis and evaluation
- c. risk classification and prioritization
- d. risk mitigation and control measures
- e. risk monitoring

10. Cloud risk management (2/2)

Risk management frameworks:

Existing IT management frameworks address cloud risks to a varying degree:

Framework	Title	Risk Management	Audit, certification & attest for organizations
COBIT 5	Control Objectives for Information and Related Technology	Risk IT Framework (addresses all IT related risks)	Yes (COBIT assessment)
ITIL V3	Information Technology Infrastructure Library	Yes (risk management for IT services)	No
ISO/IEC 2700X	Information Security Management Systems (Series of standards)	Information security risk management (ISO/IEC 27005)	Yes
PCI DSS	Payment Card Industry Data Security Standard	No, but requires a process for risk management	Yes
CSA	Cloud Security Alliance	GRC Stack (Governance, Risk, Compliance)	STAR Self-assessment STAR Certification STAR Attestation
COSO ERM	Committee of Sponsoring Organizations of the Treadway Commission	ERM – Enterprise Risk Management	No
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Information Security Risk Management	No

11. Cloud certifications

To date, there is no single certification program in place for approving cloud provider's (CSPs) adherence to security and confidentiality guidelines.

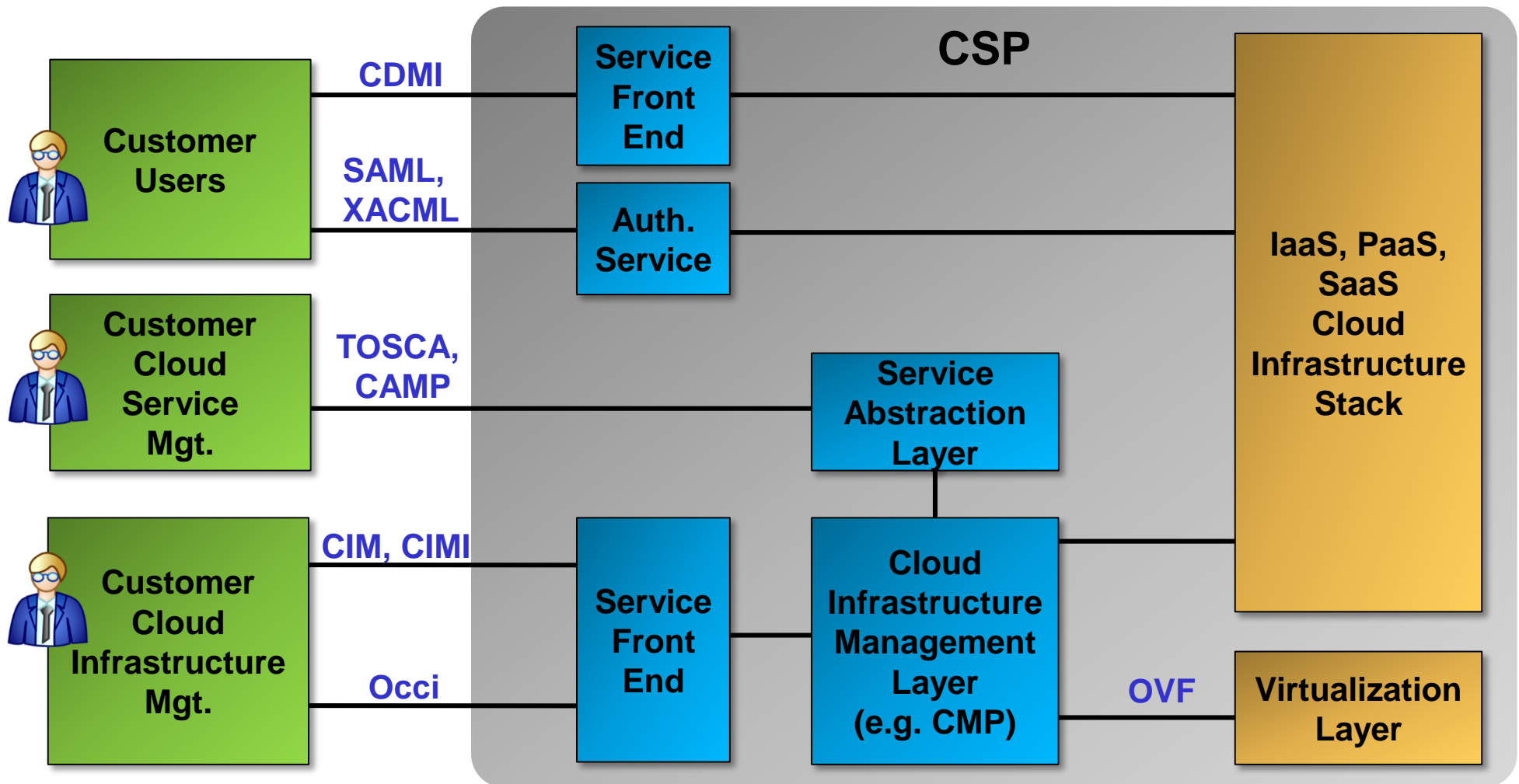
A number of programs and certifications exist that may help to evaluate a CSPs compliance with security best practices.

Certification	Authority / Issuer	Scope	Applicability
IEC27001	IEC / 3rd party audit	Information Security Management	CSPs
HIPAA	US Government, 3rd party audit	Protection of health-related information	Health Care Providers
PCI DCS	Payment Card Industry Security Standards Council	IT security	Payment Service Providers
FedRAMP	Federal Risk and Authorization Management Program	Central certification agency for U.S. agencies. Defined and required criteria for U.S. gov. agencies to use a cloud provider.	US agencies
EU SafeHarbor Compliance	Self-certification	Data protection, information security	All companies exchanging data with the US
SSAE 16, SOC 1-3	Service Organization Control	Operational Controls, Security, Privacy, Confidentiality	Most applicable for CSPs that do financial data processing
EuroCloud Star Audit	Cloud Security Alliance Self-assessment, certification, attestation	Only general statement on cloud provider quality (1-5 stars)	CSPs

12. Cloud standards (1/3)

Clouds still are mostly based on proprietary technology.

However, **standards** are emerging to improve interoperability between customer, CSP and CSA.



12. Cloud standards (2/3)

Body	Standard	Scope / goal	Link
Distributed Management Task Force (DMTF)	OVF – Open Virtualization Format	Portability and deployment of virtual appliances (VMs)	http://dmtof.org/standards/ovf
OASIS	SAML, XACML	Access Control based on XML (authorization of data access)	https://www.oasis-open.org/standards
Open Grid Forum (OGF)	Occi – Open Cloud Computing Interface	Open and standard API for customers to access and manage (mostly) IaaS-type services (infrastructure)	http://occi-wg.org/
Storage Networking Industry Association (SNIA)	CDMI – Cloud Data Management Interface	Standard interface for applications to access data elements (store, retrieve, update, delete)	http://www.snia.org/cdmi
Cloud Management Working Group (CMWG)	CIMI – Cloud Infrastructure Management Interface CIM – Common Information Model	Standard cloud management interface	http://dmtof.org/

12. Cloud standards (3/3)

Body	Standard	Scope / goal	Link
OASIS	TOSCA – Topology and Orchestration Specification for Cloud Applications	Standardization of higher level cloud services so these are easily portable across providers (e.g. standardized storage service, service choreography)	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
OASIS	CAMP – Cloud Application Management for Platforms	Standardization of interfaces (API) for self-provisioning, monitoring and control of cloud services. While CAMP defines the interface (API), TOSCA defines the implementation.	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp

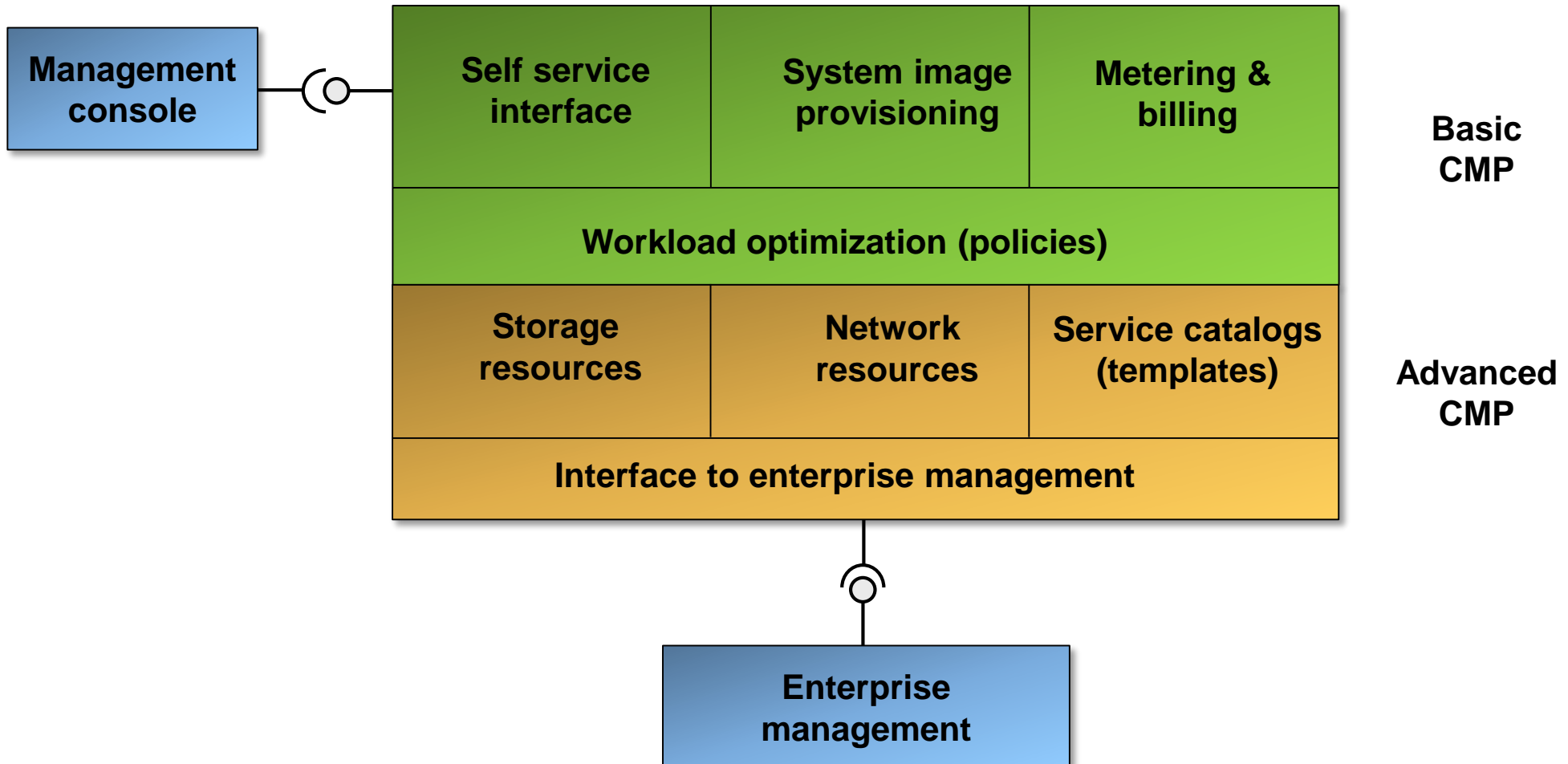
13. More cloud service models

In addition to the IaaS, PaaS and SaaS trinity, specialized cloud service models offer more specific customer services. However, these models are not always strictly cloud services as per NIST's cloud definition.

Cloud service model	Description	Examples
iPaaS	Integration Platform as a Service. Cloud-based integration platform that connects private servers and cloud-based processes, data and applications.	Cloud-based ESB (Enterprise Service Bus) Cloud-based SOA
BaaS MBaaS	Backend as a Service or Mobile Backend as a Service. BaaS is something between a PaaS and SaaS in that it provides higher level functionality such as push notifications to (mobile) clients, user management, storage services and integration with social media services.	parse.com Microsoft Azure
DaaS	Desktop as a Service. Technologically the same as VDI (Virtual Desktop Infrastructure), but virtualized desktops are provided by a cloud provider.	Amazon Workspace
STaaS	Storage as a Service. Mass storage in the cloud.	Amazon S3
DBaaS	DataBase as a Service. Relational DB and NoSQL-based databases run in cloud instances.	Amazon SimpleDB

14. Cloud management platforms (CMP) (1/3)

CMPs provide tools for managing various aspects of clouds in a single integrated suite. Gartner's IT glossary provides a concise definition of CMPs as shown below:



14. Cloud management platforms (CMP) (2/3)

Self-service interface:

Portal through which user manages the cloud infrastructure.

System image provisioning:

This component lets users choose, create, provision and deploy images (VMs) in the cloud.

Metering & billing:

Measuring infrastructure consumption is crucial for optimization (e.g. infrastructure usage trends) and billing purposes. E.g. a company may use this information for billing the services to internal departments based on usage.

Workload optimization:

Workload can be optimized e.g. through defining policies such as "automatically deploy another VM in case the load in a VM exceeds 70%". This allows optimizing resource usage and thus drive down (or at least curtail) costs (electricity, physical CPUs).

Storage and network resources:

Almost any cloud service needs some form of storage and network services. This component provides different choices for storage (NAS, SAN, DAS etc.) and network services to be used by cloud services.

Service catalogs:

This component provides a set of readily available and prefabricated templated services to choose from as well as customizing these to the user's needs.






Enterprise management interface:

Connector to existing management tools such as service management, workflow management and network management to provide a unified and integrated view of the IT infrastructure.

14. Cloud management platforms (CMP) (3/3)

Important OSS and commercial CMPs:

In order to address the various management challenges that clouds entail, different commercial and OSS (Open Source Software) CMPs have emerged of which a few are listed below:

CMP	Comment	License model
	Backed by HP, IBM, Rackspace, Redhat, Suse	OSS Apache 2.0 license
	Developed by Citrix	OSS Apache 2.0 license
	Developed by Eucalyptus Systems Inc.	OSS GPL 3 license
	Backed by C12G Labs.	OSS Apache 2.0 license
 (ICE)	Netflix provides some tools for managing specific aspects of clouds. Not a full-blown CMP.	OSS Apache 2.0 license