Hybrid and Private Clouds

What it Means to the Auditor

Scott Lowry & Hassan Javed

VMware

Professional Techniques – T24

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

CRISC

CGEIT

CISM

CISA

2013 Fall Conference – “Sail to Success”

Hybrid and Private Clouds

Objectives:

- ❑ Explain the technology and benefits of public, private and hybrid cloud adoption
- ❑ Introduce the concept of Cloud Hybrid Service
- ❑ Provide a framework for assessing risks and auditing private and hybrid clouds
- ❑ Demonstrate “real world” Private/Hybrid cloud computing

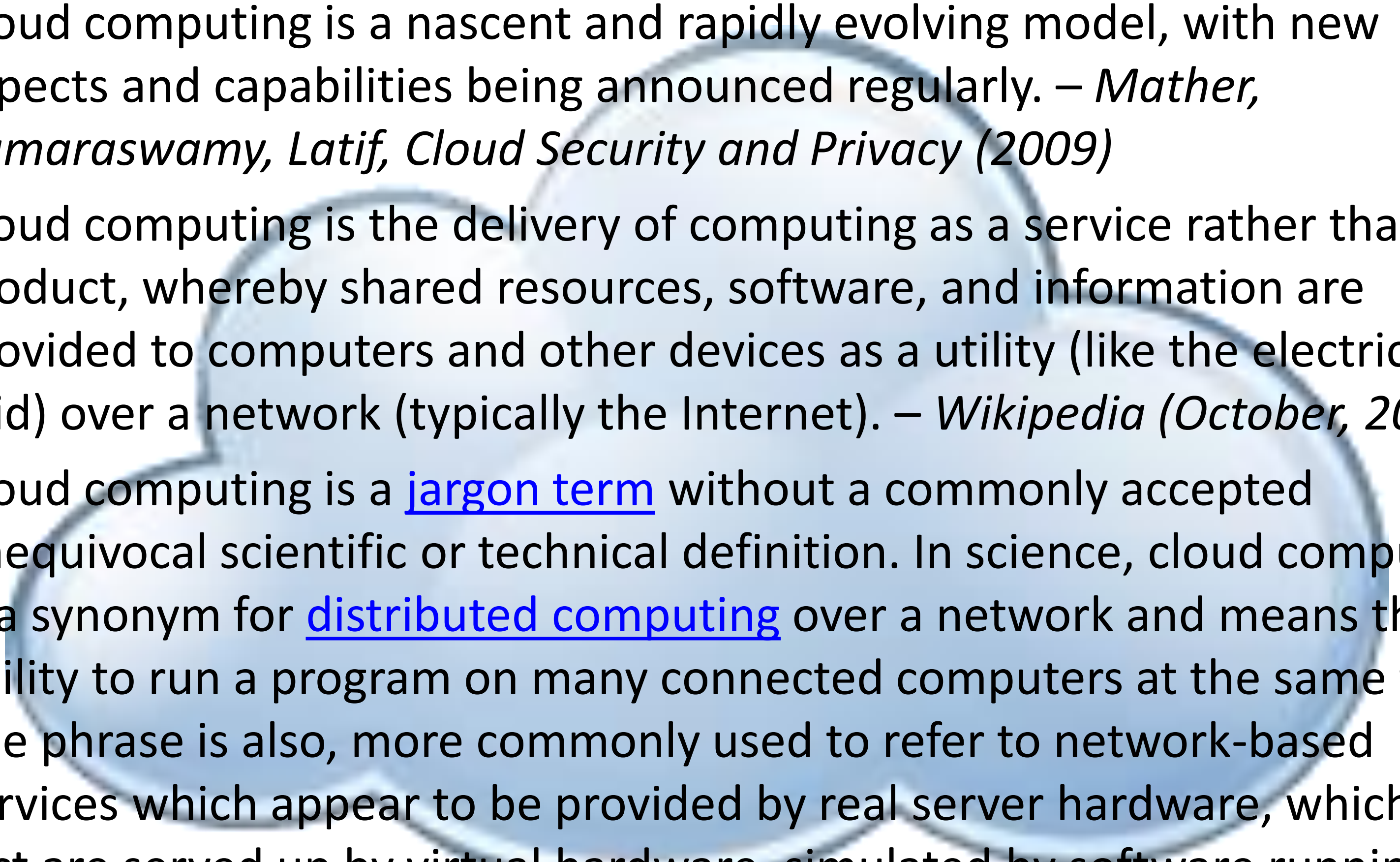
Hybrid and Private Clouds

Agenda

- □ Understanding the Cloud
- □ Cloud Computing Models
- □ Future of Cloud Computing
- □ The "Real Life" Hybrid Cloud
- □ Private & Hybrid Cloud Risk Assessment
  - □ Governance
  - □ IT Strategy
  - □ Roadmap
  - □ Cloud Service Layer
  - □ Application Portfolio
- □ Maturity Assessment
- □ Cloud Demonstration

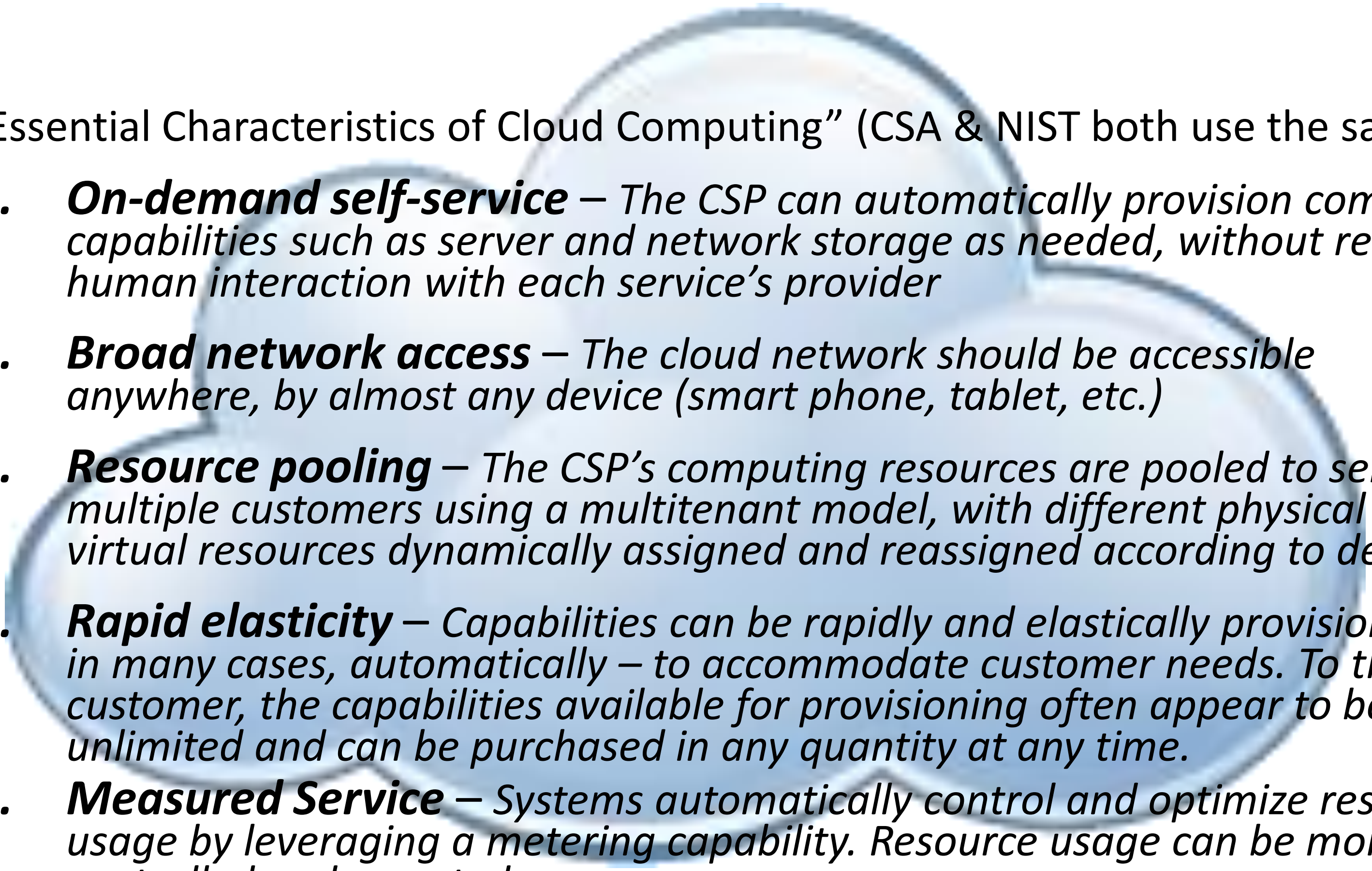
UNDERSTANDING THE CLOUD

The Cloud – an evolving definition



- ❑ Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. – *Mather, Kumaraswamy, Latif, Cloud Security and Privacy (2009)*
- ❑ Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). – *Wikipedia (October, 2011)*
- ❑ Cloud computing is a jargon term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also, more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. – *Wikipedia (September, 2013)*

Defining the Cloud – CSA & NIST

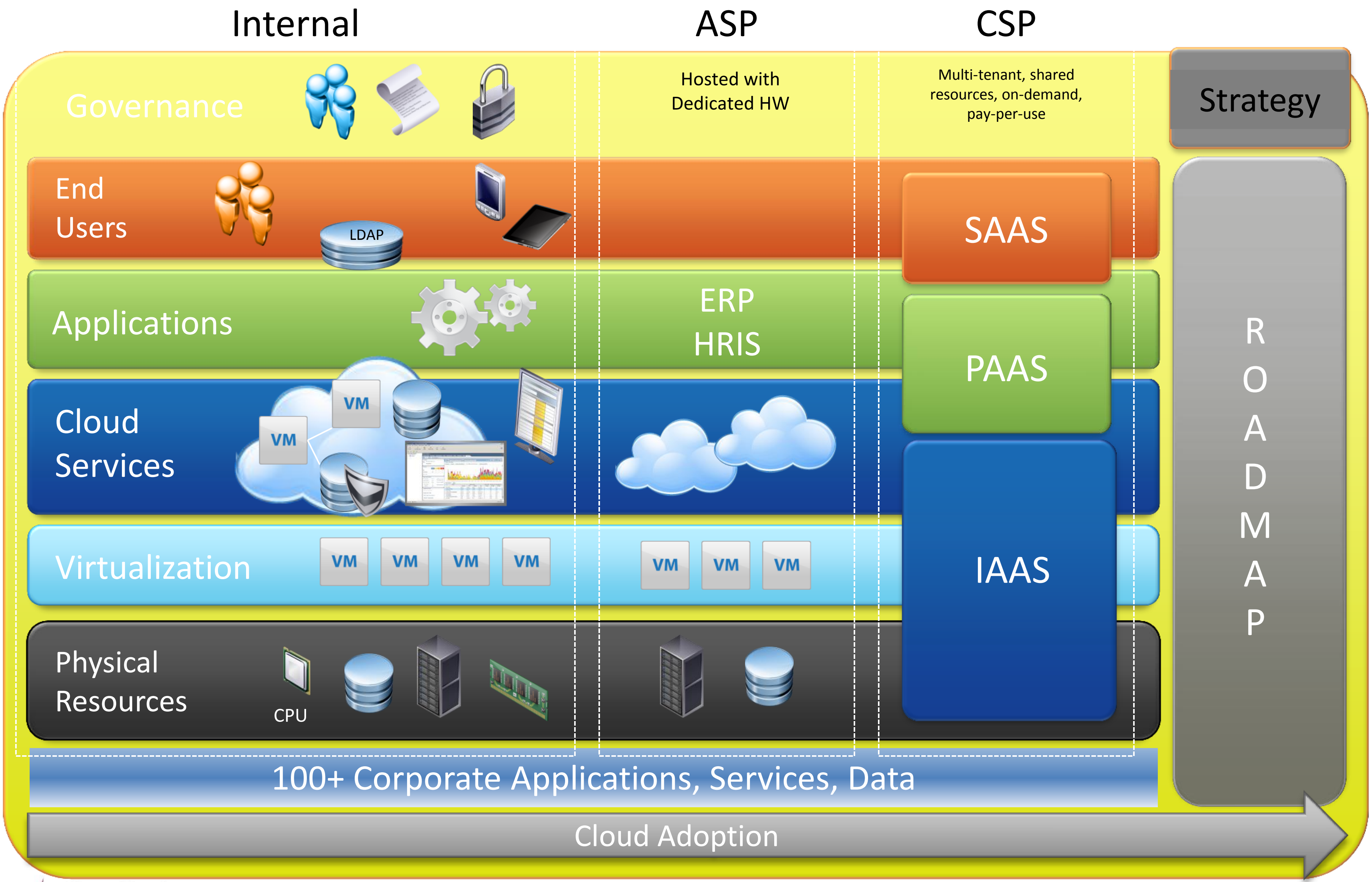


Five "Essential Characteristics of Cloud Computing" (CSA & NIST both use the same):

1. ***On-demand self-service*** *– The CSP can automatically provision computing capabilities such as server and network storage as needed, without requiring human interaction with each service's provider*
2. ***Broad network access*** *– The cloud network should be accessible anywhere, by almost any device (smart phone, tablet, etc.)*
3. ***Resource pooling*** *– The CSP's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand.*
4. ***Rapid elasticity*** *– Capabilities can be rapidly and elastically provisioned – in many cases, automatically – to accommodate customer needs. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.*
5. ***Measured Service*** *– Systems automatically control and optimize resource usage by leveraging a metering capability. Resource usage can be monitored, controlled and reported.*

CLOUD COMPUTING MODELS

Cloud Computing Model – History



Internal

ASP

CSP

Hosted with Dedicated HW

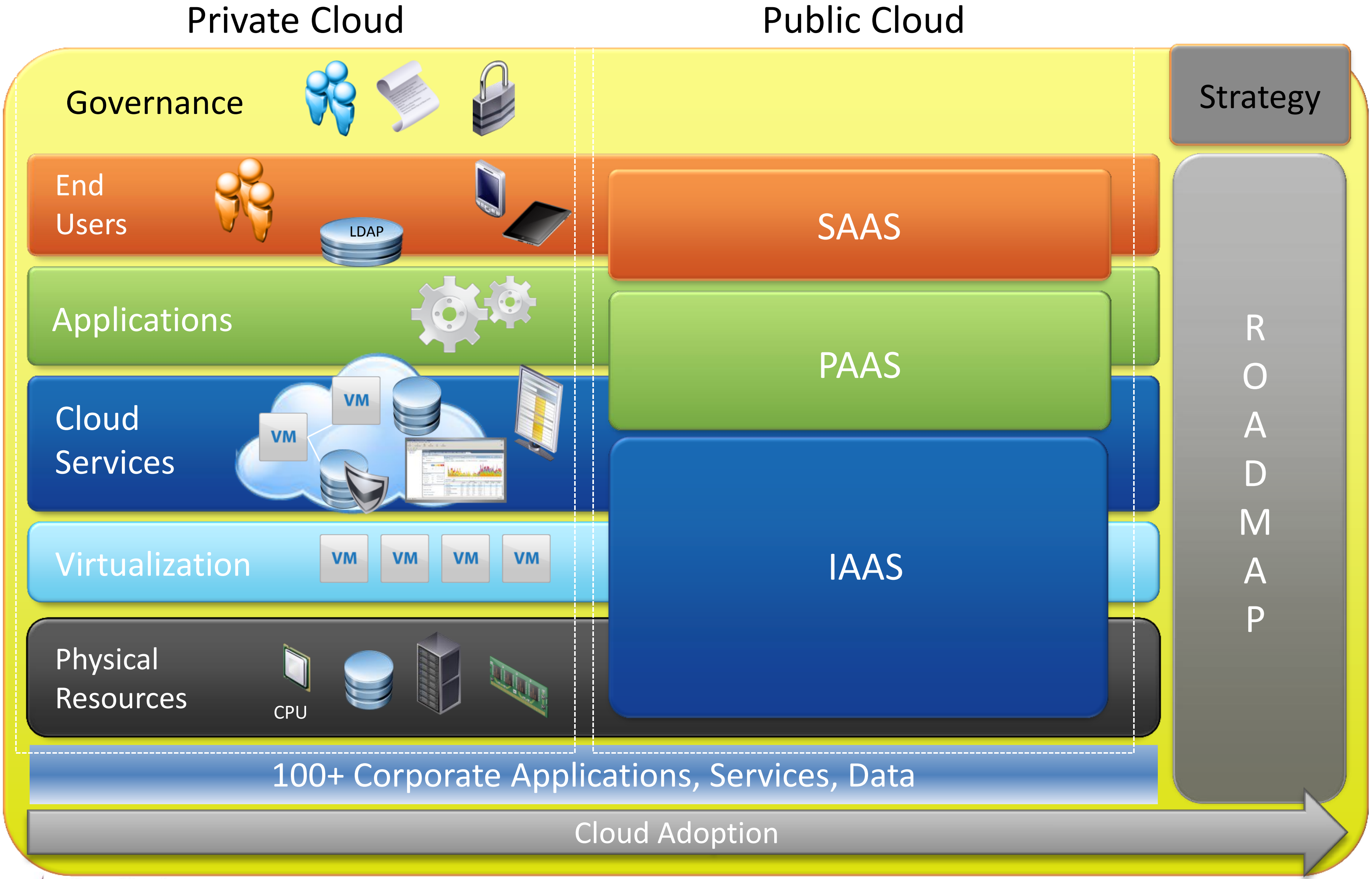
Multi-tenant, shared resources, on-demand, pay-per-use

Strategy

100+ Corporate Applications, Services, Data

Cloud Adoption

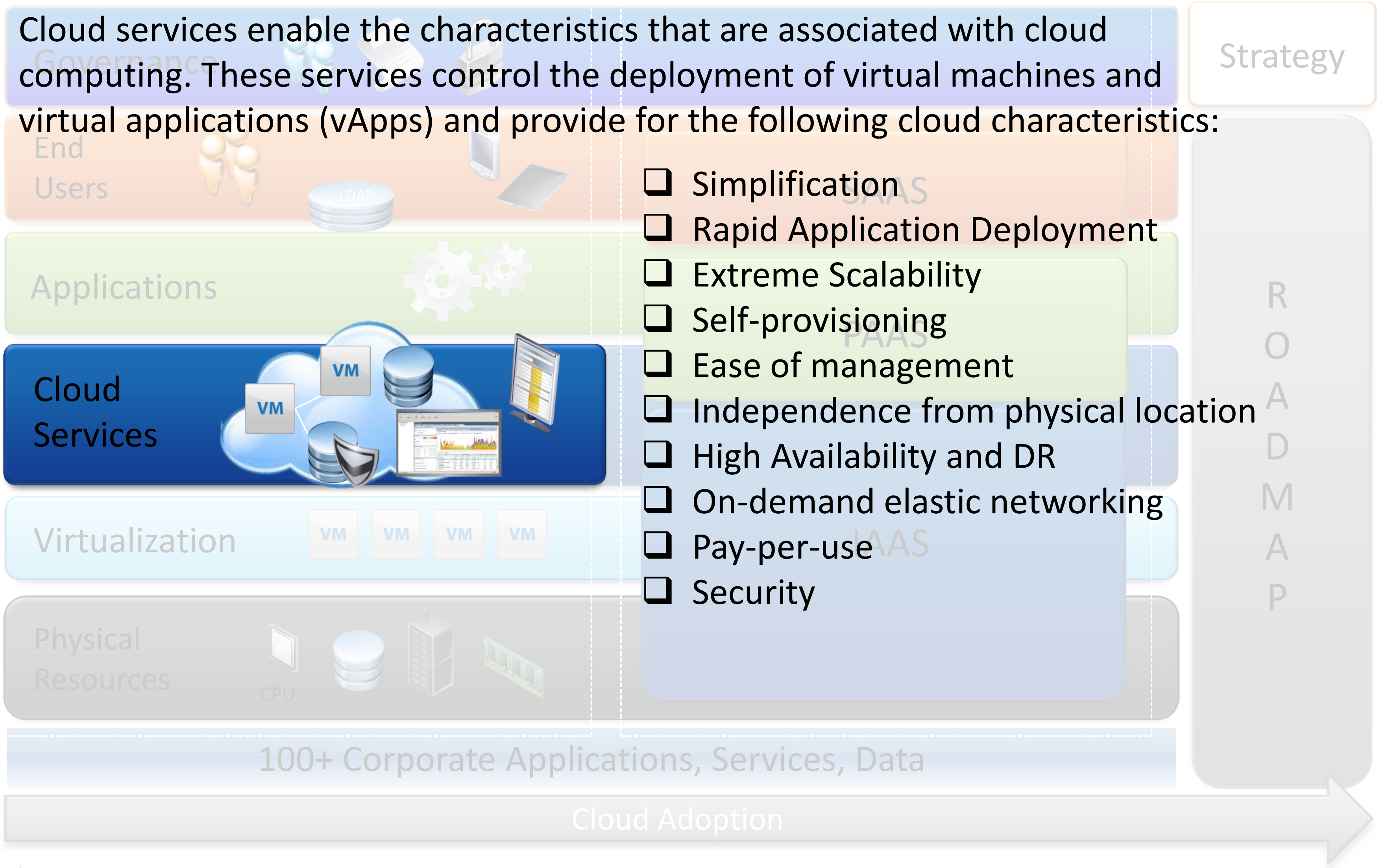
Cloud Delivery Model – Simplified



Cloud Computing Model – Cloud Services

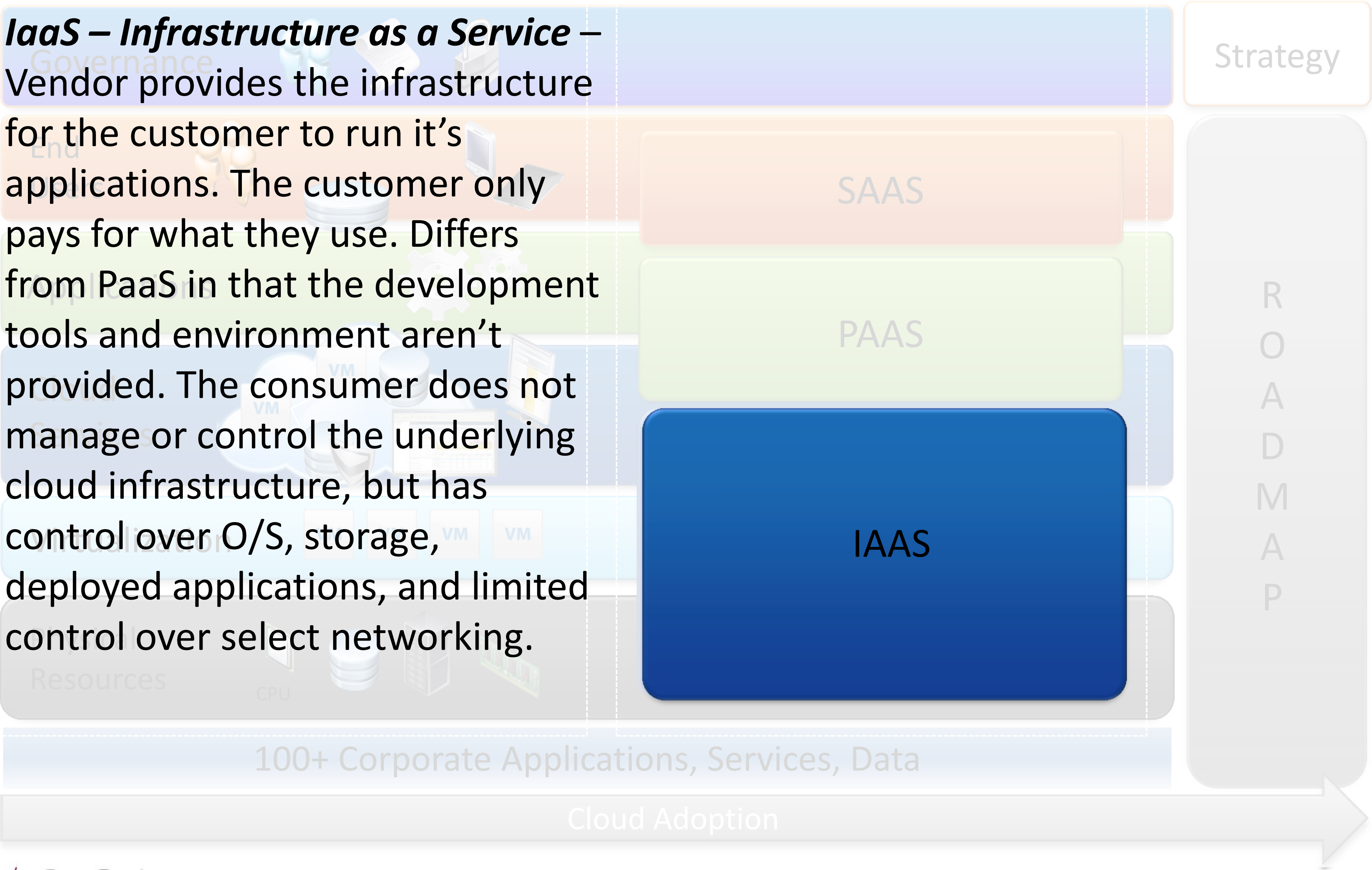
Cloud services enable the characteristics that are associated with cloud computing. These services control the deployment of virtual machines and virtual applications (vApps) and provide for the following cloud characteristics:

- ❑ Simplification
- ❑ Rapid Application Deployment
- ❑ Extreme Scalability
- ❑ Self-provisioning
- ❑ Ease of management
- ❑ Independence from physical location
- ❑ High Availability and DR
- ❑ On-demand elastic networking
- ❑ Pay-per-use
- ❑ Security



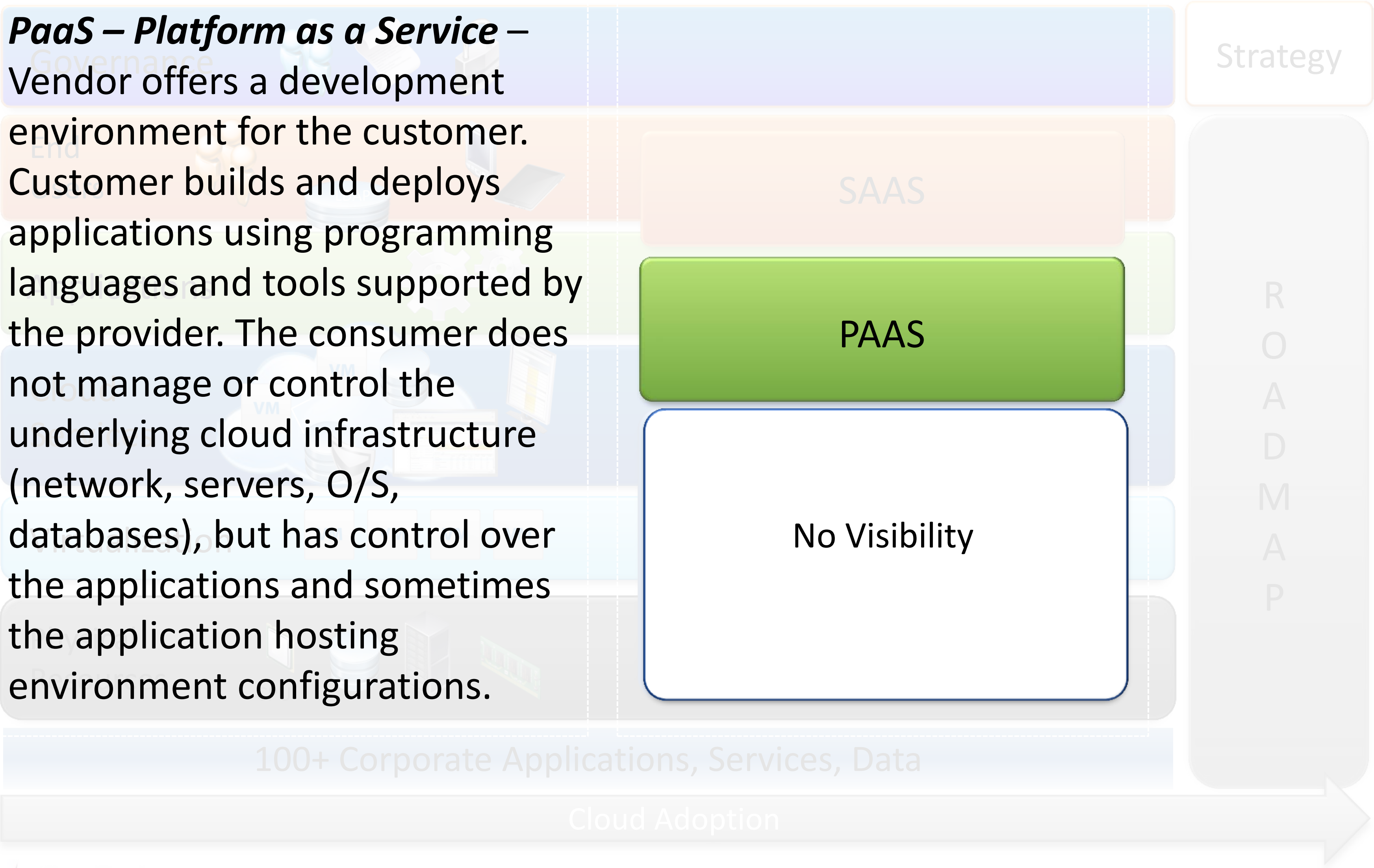
Cloud Computing Model – *SPI Service Model*

IaaS – Infrastructure as a Service – Vendor provides the infrastructure for the customer to run it’s applications. The customer only pays for what they use. Differs from PaaS in that the development tools and environment aren’t provided. The consumer does not manage or control the underlying cloud infrastructure, but has control over O/S, storage, deployed applications, and limited control over select networking.



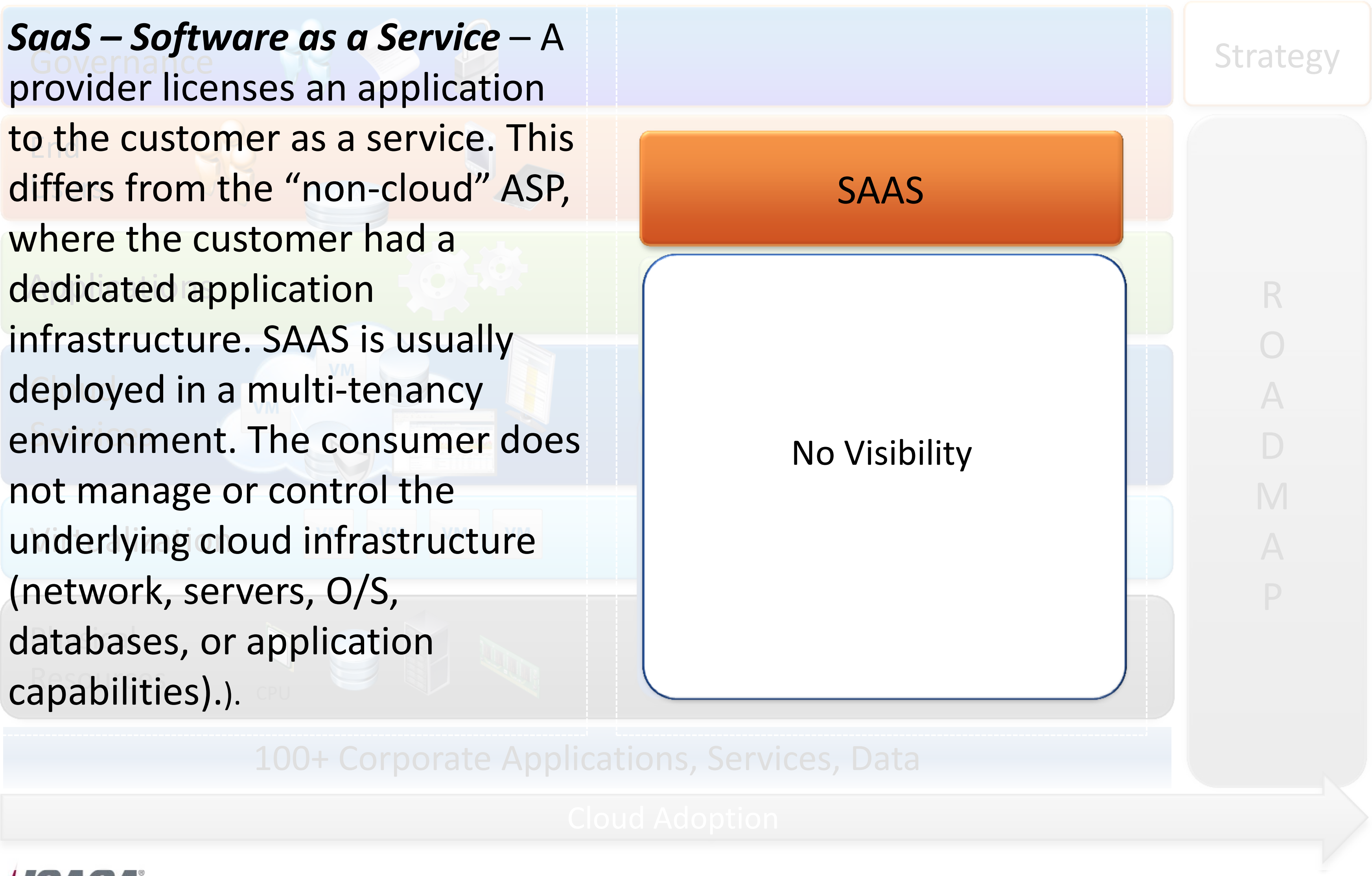
Cloud Computing Model – *SPI Service Model*

PaaS – Platform as a Service – Vendor offers a development environment for the customer. Customer builds and deploys applications using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (network, servers, O/S, databases), but has control over the applications and sometimes the application hosting environment configurations.



Cloud Computing Model – *SPI Service Model*

SaaS – Software as a Service – A provider licenses an application to the customer as a service. This differs from the “non-cloud” ASP, where the customer had a dedicated application infrastructure. SAAS is usually deployed in a multi-tenancy environment. The consumer does not manage or control the underlying cloud infrastructure (network, servers, O/S, databases, or application capabilities).).



Cloud Computing Model

Private Cloud

Deploys cloud computing services on private networks.

Delivers many of the same benefits of cloud computing without relinquishing control.

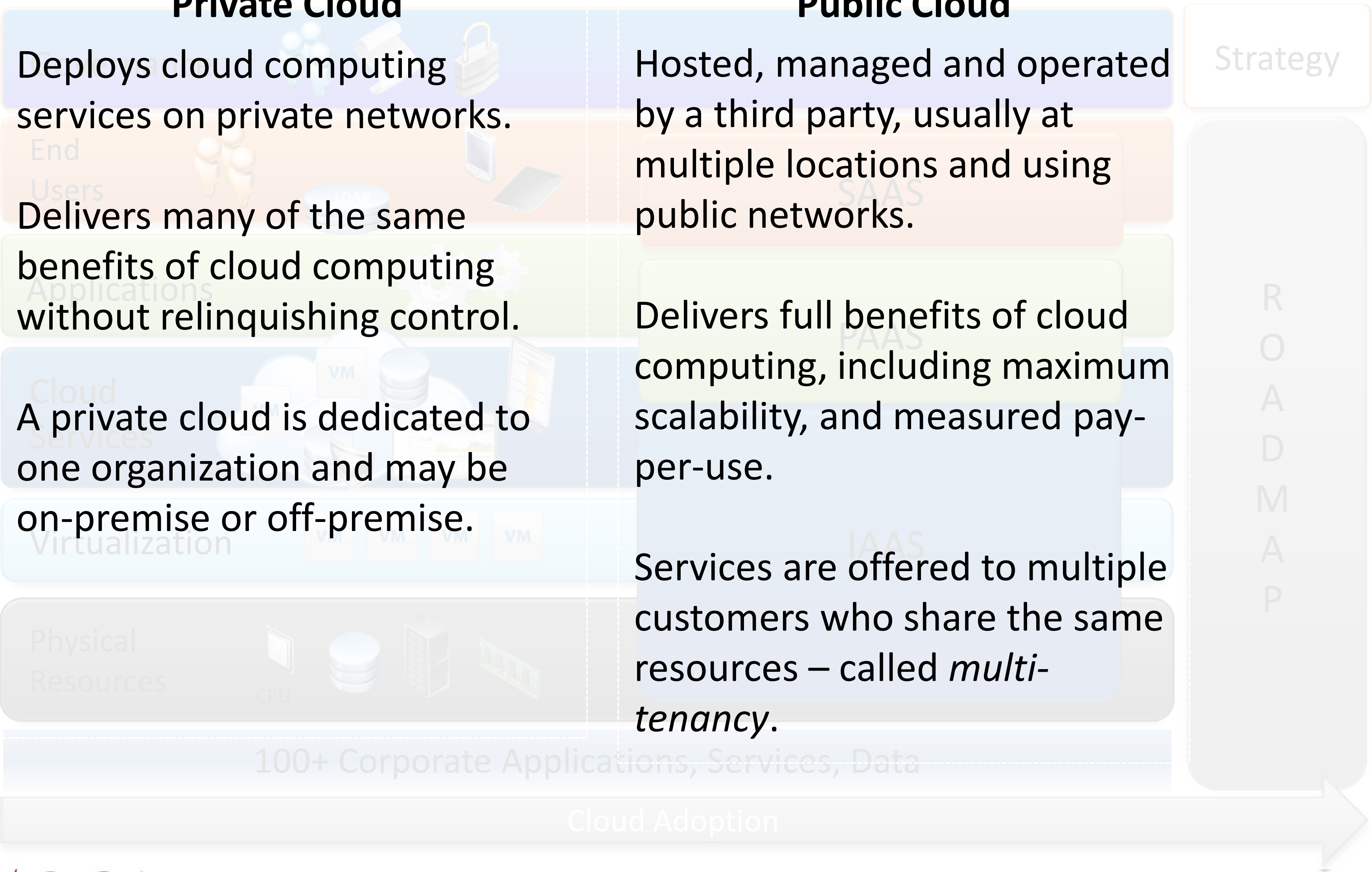
A private cloud is dedicated to one organization and may be on-premise or off-premise.

Public Cloud

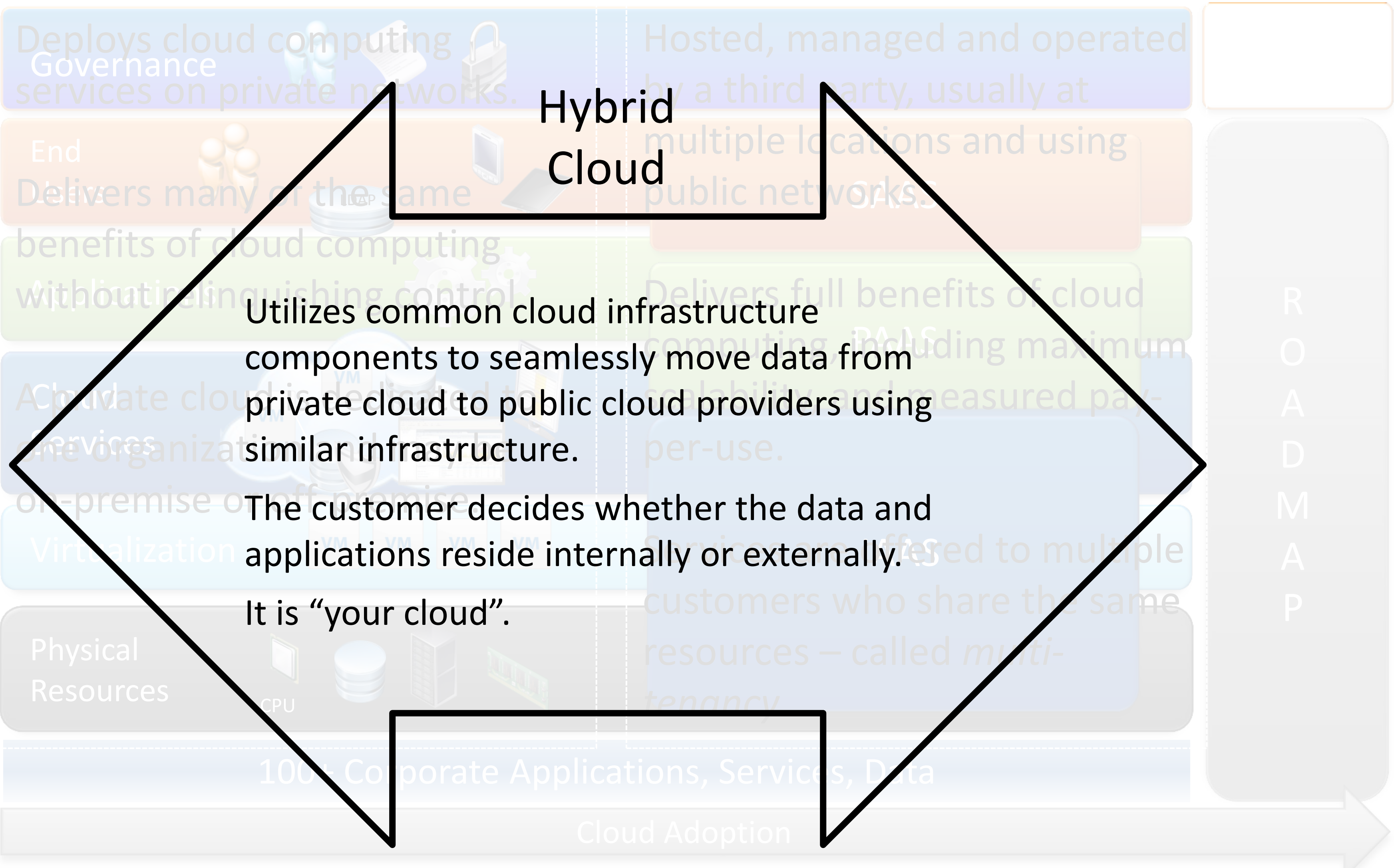
Hosted, managed and operated by a third party, usually at multiple locations and using public networks.

Delivers full benefits of cloud computing, including maximum scalability, and measured pay-per-use.

Services are offered to multiple customers who share the same resources – called *multi-tenancy*.



Cloud Computing Model



Private Cloud

Deploys cloud computing services on private networks.

Delivers many of the same benefits of cloud computing without relinquishing control.

A private cloud is dedicated to one organization and may be on-premise or off-premise.

Public Cloud

Hosted, managed and operated by a third party, usually at multiple locations and using public networks.

Delivers full benefits of cloud computing including maximum scalability and measured pay-per-use.

Services are offered to multiple customers who share the same resources – called *multi-tenancy*.

Hybrid Cloud

Utilizes common cloud infrastructure components to seamlessly move data from private cloud to public cloud providers using similar infrastructure.

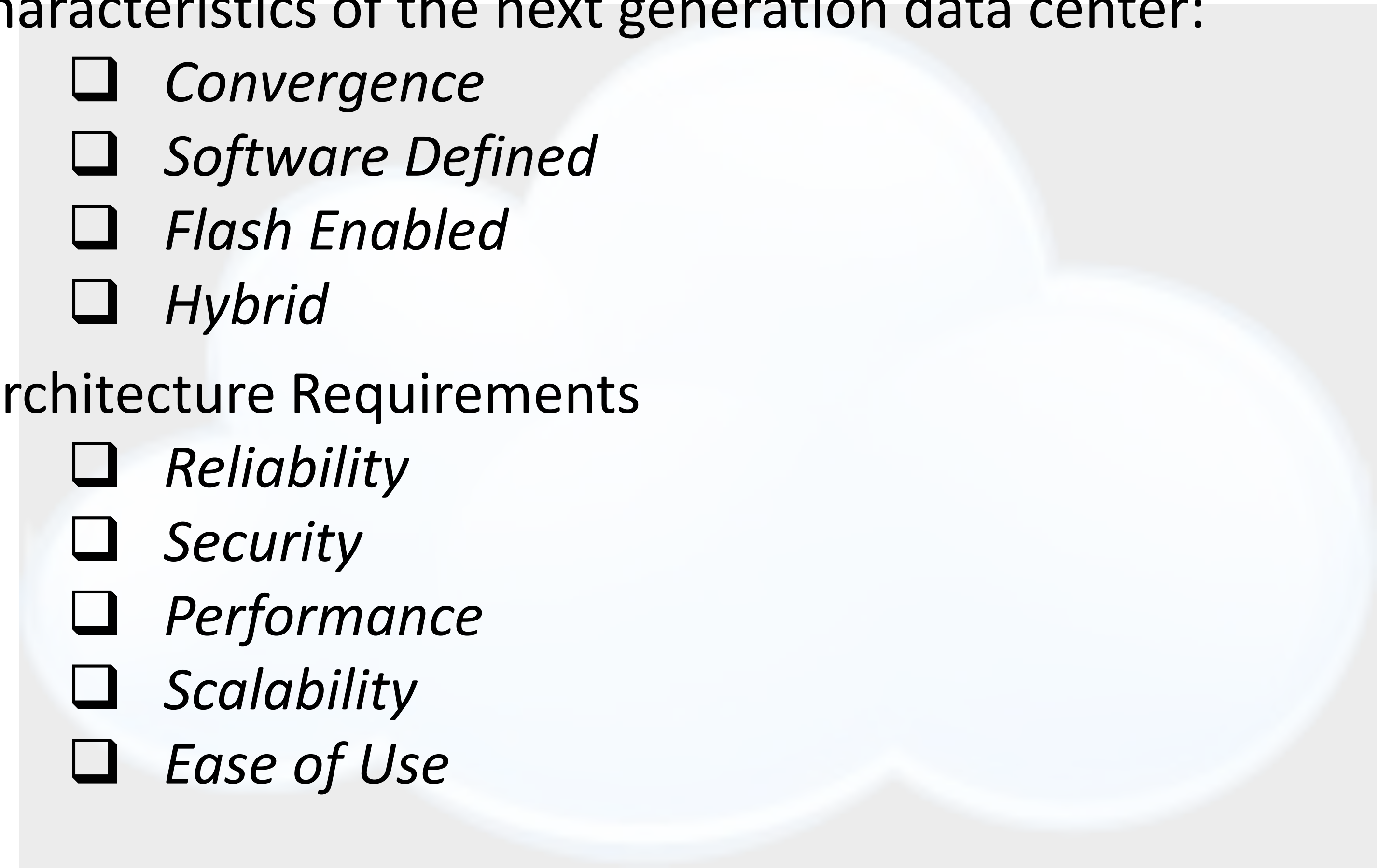
The customer decides whether the data and applications reside internally or externally.

It is “your cloud”.

FUTURE OF CLOUD COMPUTING

16

The Software Defined Data Center



- ❑ Characteristics of the next generation data center:
  - ❑ *Convergence*
  - ❑ *Software Defined*
  - ❑ *Flash Enabled*
  - ❑ *Hybrid*
- ❑ Architecture Requirements
  - ❑ *Reliability*
  - ❑ *Security*
  - ❑ *Performance*
  - ❑ *Scalability*
  - ❑ *Ease of Use*

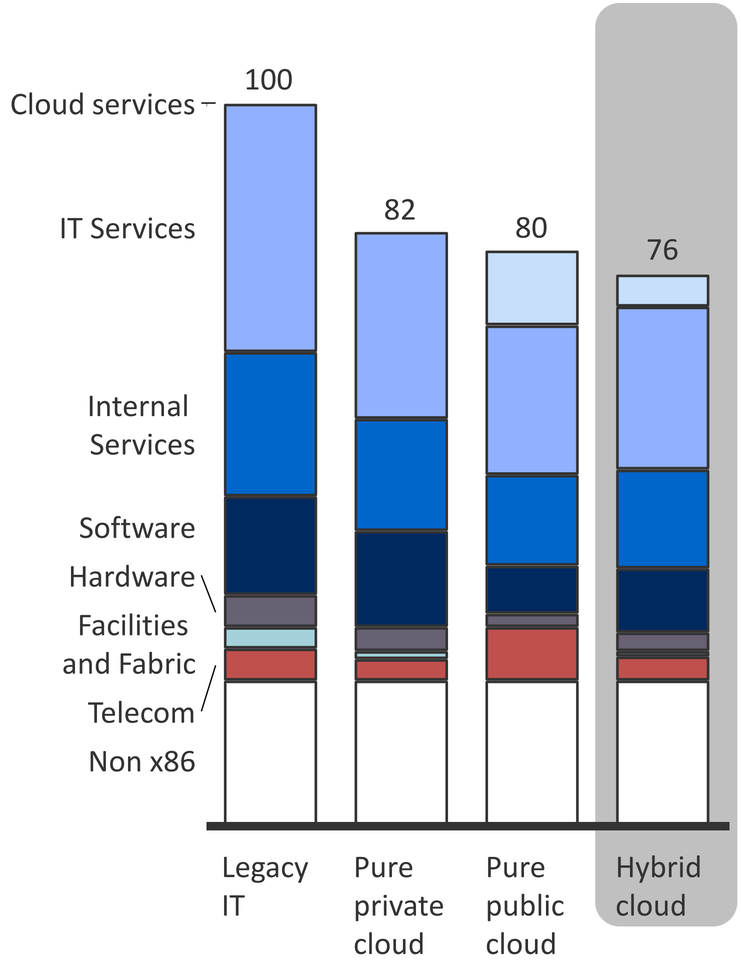
THE "REAL LIFE" HYBRID CLOUD

WHERE ARE WE NOW

18

Hybrid cloud is the most elastic and cost effective model

Annual total IT spend
(100=Total IT spend with all on-premise infrastructure)



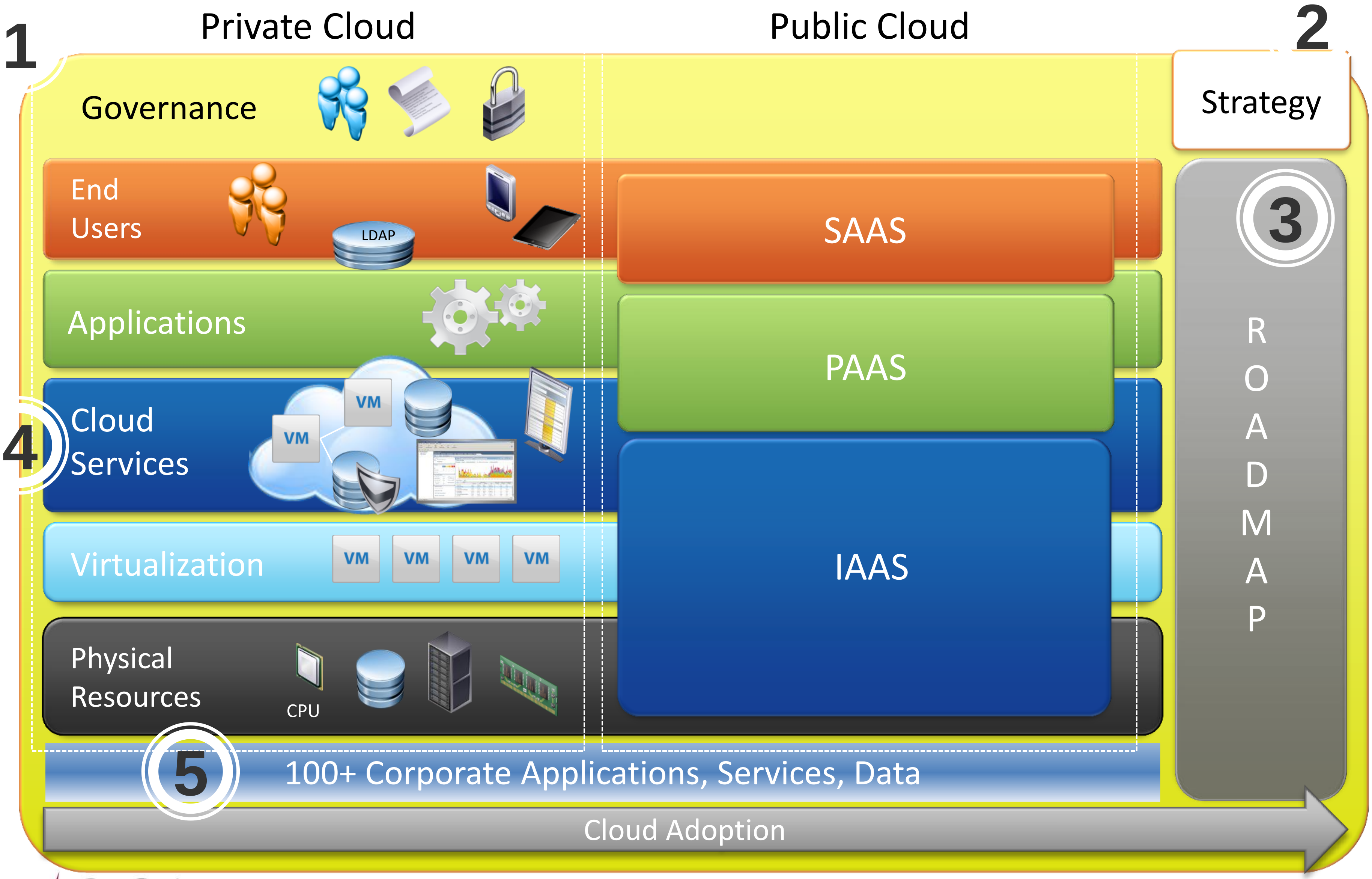
- Hybrid cloud offers lower IT spend through:
  - Virtualization and consolidation
  - Optimized workload sourcing
  - Optimized provisioning
  - Higher productivity in application development and maintenance

- This requires standardization of frameworks & infrastructure across public and private cloud:
  - Common platform
  - Common management
  - Common security

PRIVATE & HYBRID CLOUD RISK ASSESSMENT

20

Cloud Computing Model – Assessing the Journey



1

Cloud Governance

Risks

- ❑ Failure to deliver value from cloud technology
- ❑ Non-compliance with laws and regulations
- ❑ Loss of data, intellectual property
- ❑ Contractual non-compliance
- ❑ Reputational damage associated with data loss, non-compliance
- ❑ Abdicating security and risk decisions to third parties, losing control and increasing the chances of all of the above

Considerations

- ✓ Cloud service decisions are made at the right level in the organization and involve cross-functional stakeholders (eg., legal, security, etc.)
- ✓ The organization has defined it's needs for confidentiality, integrity and availability of systems and data and has designed appropriate controls
- ✓ Roles and responsibilities are defined and understood between the organization and service provider for various service deployment models

Cloud Strategy

Risks

- ❑ Making short-term gains that hurt in the long-term
- ❑ Misalignment of IT Technological Direction and Business Risk Tolerance
- ❑ Failure to align technologies with overall cloud strategy
- ❑ Business units pursue their own cloud initiatives creating silos and incompatible technologies
- ❑ Vendor lock-in or buyer's remorse

Considerations

- ✓ Involve cross-functional roles in Cloud Strategic Discussions
- ✓ Integrate cloud initiatives into IT Steering Committee discussions
- ✓ Examine how IT Org structure will change with cloud
- ✓ Examine how strategic vendor relationships will be transformed
- ✓ Evaluate early adoption benefits and risks
- ✓ Create and document viable exit strategies

Cloud Roadmap

Risks

- ❑ Increased costs, failure to achieve benefits
- ❑ Disruption of service to customers
- ❑ Loss of competitive advantage
- ❑ Fines from failed regulatory compliance
- ❑ Loss of revenue
- ❑ Negative impact on reputation
- ❑ Loss of expected return-on-investment
- ❑ Excessive project costs

Considerations

- ✓ Move applications/data in the right order to maximize value, reduce risk
- ✓ Implement cloud processes and dependent technologies prior to migrating high governance applications and data
- ✓ Utilize DR to facilitate path to cloud services
- ✓ Implement security and monitoring controls on the front end
- ✓ Coordinate roadmap with end-users and cross-functional stakeholders

Cloud Services Layer

Risks

- ❑ Unauthorized access to data and applications
- ❑ Data loss
- ❑ Disruption of service to customers

Considerations

- ✓ Assess cloud management tools the same way we would assess other management applications. Who has access, what can they do with the access
- ✓ Understand how the cloud management tools work – are they using a superuser account
- ✓ Log and monitor access at the cloud layer
- ✓ Implement logical security in the cloud layer
- ✓ The cloud layer enables very fast change to the environment – this should be controlled

5

Cloud Applications

- ❑ Inventory applications, data and technologies
- ❑ Determine characteristics of each
- ❑ Use attributes to determine the risks associated with each

Application	Developed	Virtual	Cloud	SPI	Public	Hosted
ERP System	In	No	No	N/A	Private	Internal
CRM	Out	Yes	Yes	SAAS	Public	Amazon
HR	Out	Yes	Yes	SAAS	Public	Acme
BI	In	Yes	Yes	PAAS	Public	Rackspace
Ticketing	In	Yes	Yes	IAAS	Private	Internal
Expense	In	Yes	Yes	IAAS	Private	Internal

MATURITY ASSESSMENT

27

Maturity Assessment (Benefits)

	Benefit	1	2	3	4	5
	Simplification					
	Rapid Application Deployment					
	Extreme Scalability					
	Self-provisioning and Quick-provisioning					
	Ease of Management					
	Independence from Physical Location					
	Availability, SLAs, Disaster Recovery					
	On demand, elastic Networking					
	Pay-per-use					
	Security					

Maturity Assessment (Processes)

	IT Process	1	2	3	4	5
	System Development Lifecycle					
	Configuration Management					
	Service Desk Management					
	Incident and Problem Management					
	Change and Release Management					
	Information Security					
	Disaster Recovery					
	Capacity Planning					
	Availability Management & SLAs					
	Financial Planning and Management					

CLOUD DEMONSTRATION

QUESTIONS

31