

Cloud Computing



Abrar Qureshi, Ph.D.

University of Virginia's College at Wise

Cloud Computing



Cloud Computing – NIST

“A model for enabling 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”

Common Cloud Characteristics

- Cloud computing often leverages:
 - Massive scale
 - Virtualization
 - Non-stop computing
 - Free software
 - Geographic distribution
 - Service oriented software
 - Autonomic computing
 - Advanced security technologies

Conventional vs. Cloud Computing

Conventional

- Manually Provisioned
- Dedicated Hardware
- Fixed Capacity
- Pay for Capacity
- Capital & Operational Expenses
- Managed via Sysadmins

Cloud

- Self-provisioned
- Shared Hardware
- Elastic Capacity
- Pay for Use
- Operational Expenses
- Managed via APIs

Benefits of Cloud Computing

- Reduced Cost
- Pay as you go
- Work from:
 - Home
 - Work or at
 - Client locations
- Free-up IT workers who may have been occupied performing updates, installing patches, or providing application support.

Cloud efficiencies and improvements

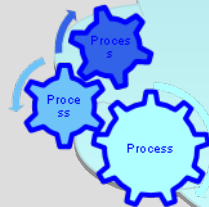
- Cost efficiencies
- Time efficiencies
- Power efficiencies
- Improved process control
- Improved security
- “Unlimited” capacity



- Burst capacity (over-provisioning)
- Short-duration projects
- Cancelled or failed missions



- Procurement
- Network connectivity



- Standardized, updated base images
- Centrally auditable log servers
- Centralized authentication systems
- Improved forensics (w/ drive image)

Five Key Cloud Attributes

1. Shared / pooled resources
2. Broad network access
3. On-demand self-service
4. Scalable and elastic
5. Metered by use

Shared / Pooled Resources

- Resources are drawn from a common pool
- Common resources build economies of scale
- Common infrastructure runs at high efficiency



Broad Network Access

- Open standards and APIs
- Almost always IP, HTTP, and REST
- Available from anywhere with an internet connection



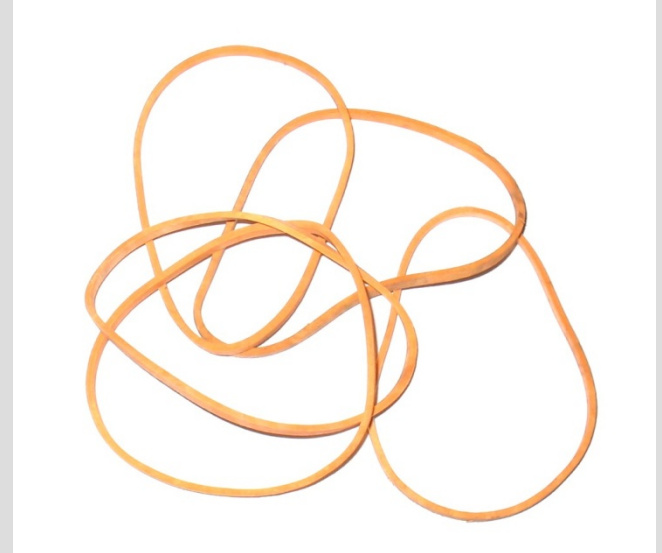
On-Demand Self-Service

- Completely automated
- Users abstracted from the implementation
- Near real-time delivery (seconds or minutes)
- Services accessed through a self-serve web interface

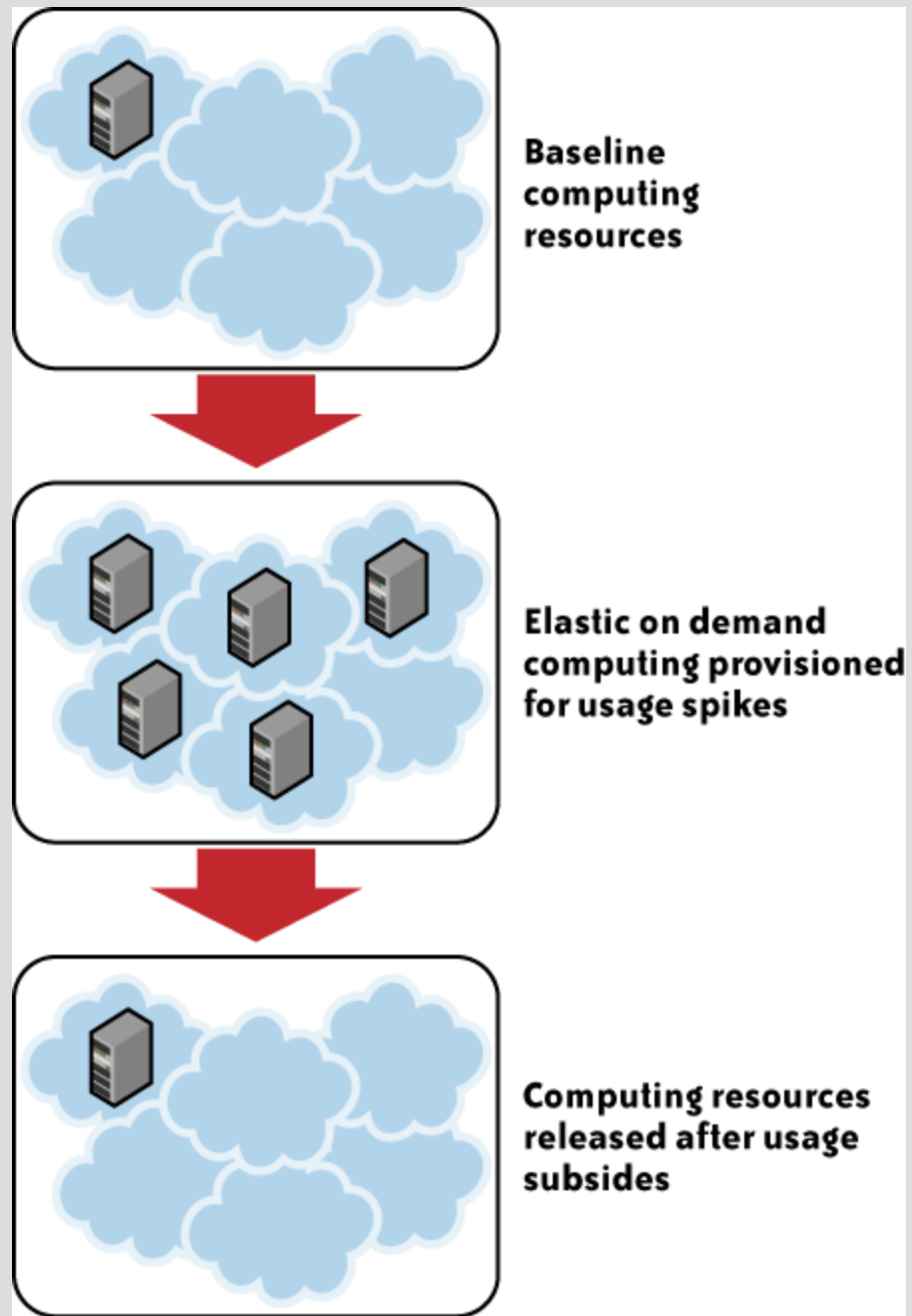


Scalable and Elastic

- Resources dynamically-allocated between users
- Additional resources dynamically-released when needed
- Fully automated



Attribute of elasticity



Metered by Use

- Services are metered, like a utility
- Users pay only for services used
- Services can be cancelled at any time

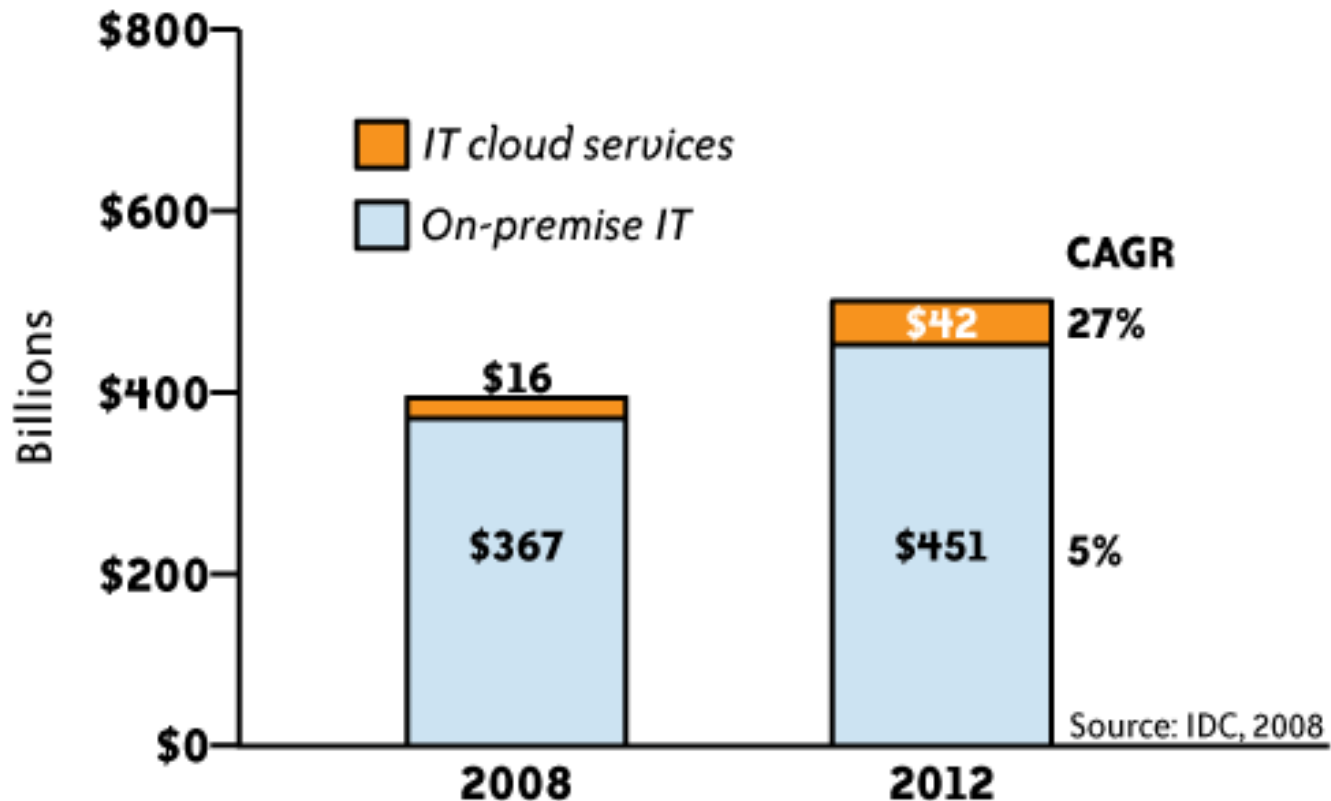


Cloud lunches

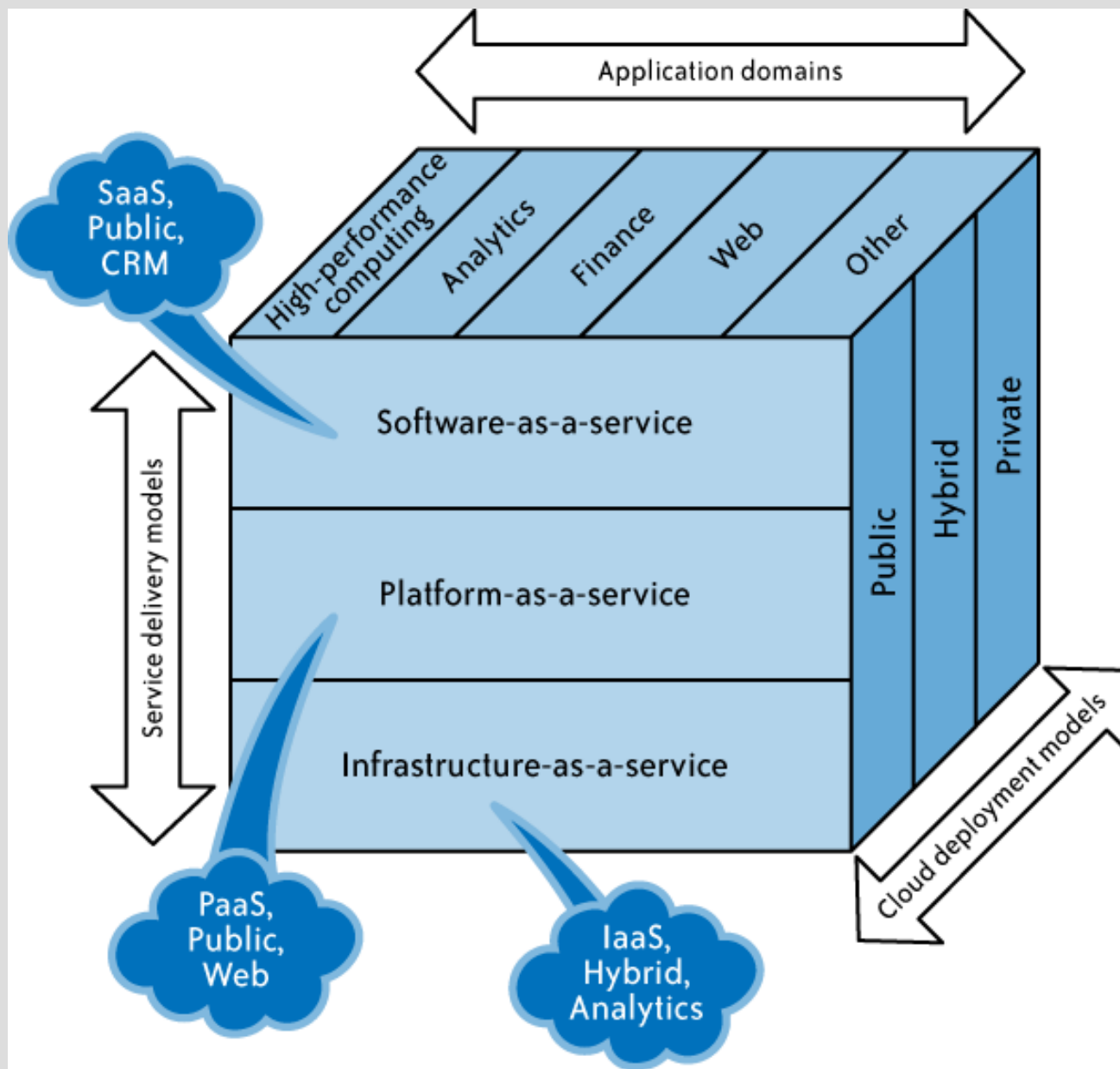
Recent notable cloud launches

Cloud applications	Desktop and business applications
	 
Cloud software development platform	Software platform to host cloud-based enterprise applications
	 Windows Azure™   <small>Success. Not Software.®</small>
Cloud-based infrastructure	Servers, storage, security, databases
	   

Worldwide IT spending by consumption 2008, 2012

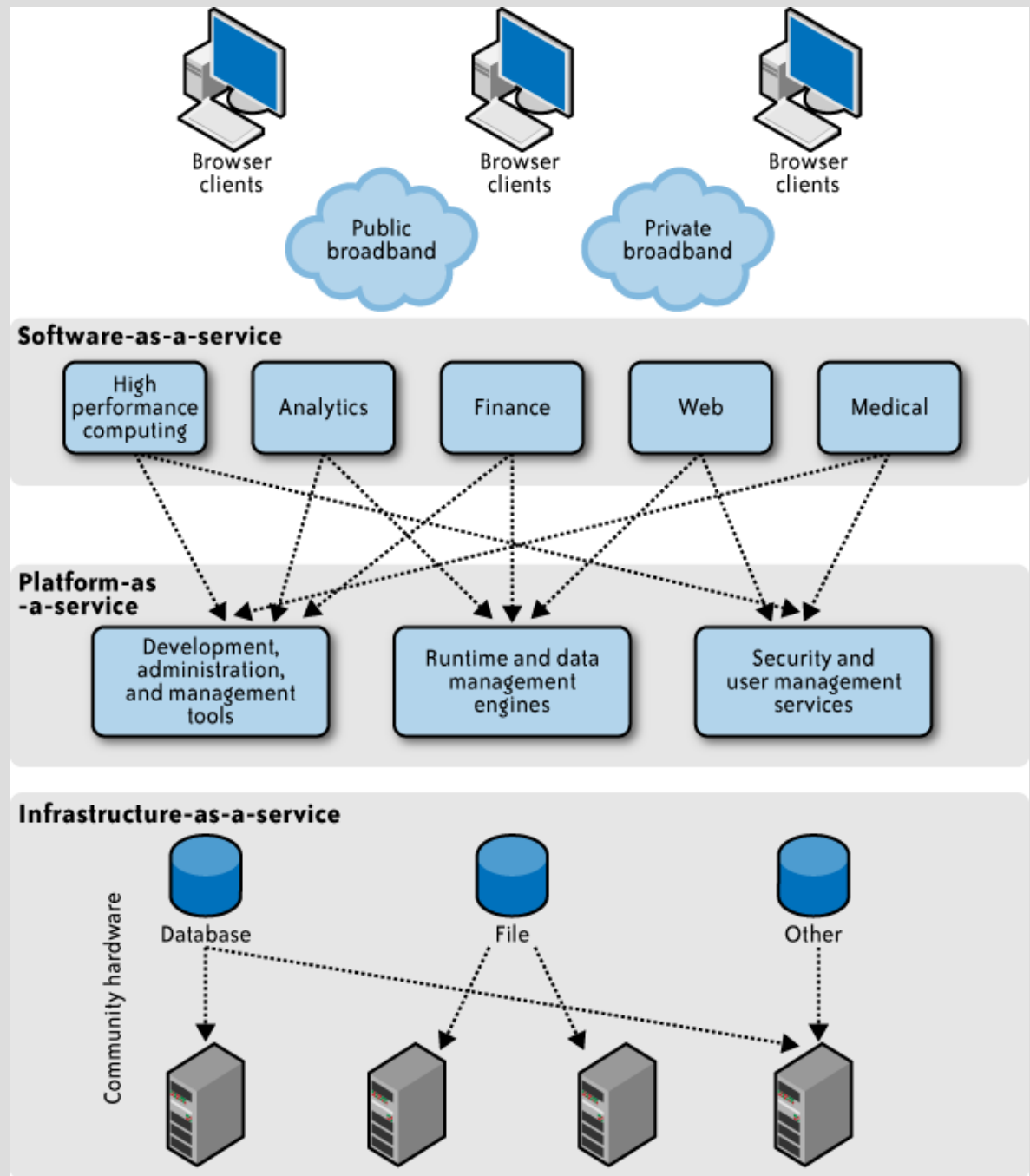


Spending on cloud-based services



SPI service model

Architecture for relevant technologies



Cloud Computing

- **Cloud-based services require large computing capacity and are hosted in data centers and server farms.**
- **These distributed data centers and server farms span multiple locations and can be linked via internetworks providing distributed computing and service delivery capabilities.**

Cloud Computing

- A number of examples today illustrate the flexibility and scalability of cloud computing power.
- For instance, Google has linked a very large number of inexpensive servers to provide tremendous flexibility and power.

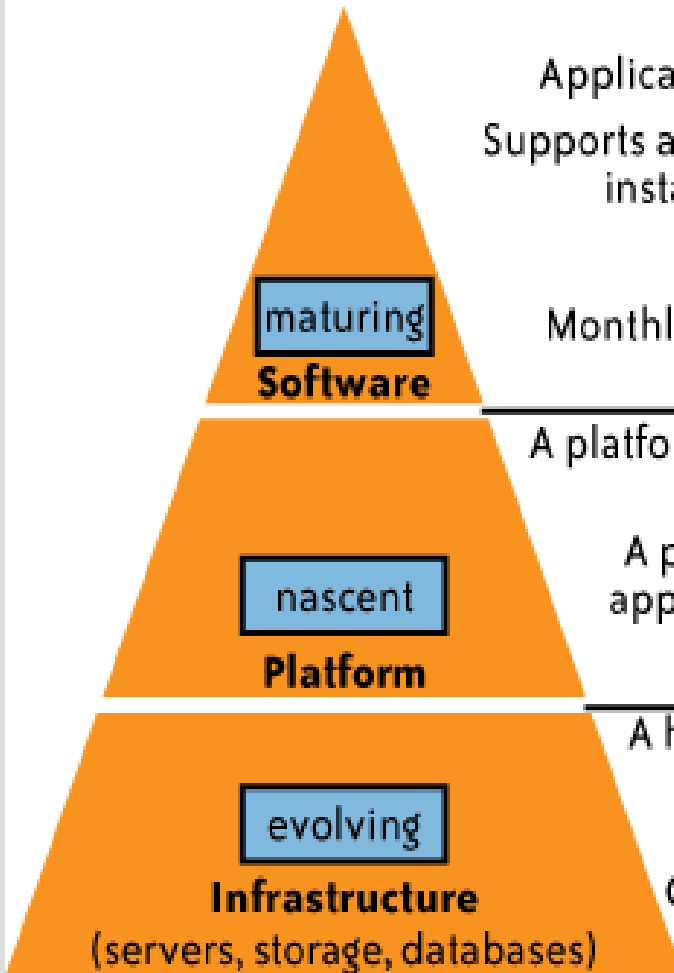
Cloud Computing

- **Amazon's Elastic Compute Cloud (EC2) provides virtualization in the data center to create huge numbers of virtual instances for services being requested.**
- **Salesforce.com provides SaaS to its large customer base by grouping its customers into clusters to enable scalability and flexibility.**

Cloud Computing

- **Virtualization is a foundational technology platform fostering cloud computing, and it is transforming the face of the modern data center.**
- **The term virtualization refers to the abstraction of compute resources (CPU, storage, network, memory, application stack, and database) from applications and end users consuming the service.**

Cloud services delivery model

	Definition	Examples
 maturing Software	Applications that are enabled for the cloud Supports an architecture that can run multiple instances of itself regardless of location Stateless application architecture Monthly subscription-based pricing model	<ul style="list-style-type: none">• Google Docs• MobileMe• Zoho
nascent Platform	A platform that enables developers to write applications that run on the cloud A platform would usually have several application services available for quick deployment	<ul style="list-style-type: none">• Microsoft Azure• Google App Engine• Force.com
evolving Infrastructure (servers, storage, databases)	A highly scaled redundant and shared computing infrastructure accessible using Internet technologies Consists of servers, storage, security, databases, and other peripherals	<ul style="list-style-type: none">• Amazon EC2, S3, etc.• Rackspace Mosso offering• Sun's cloud services• Terremark cloud offering

While cloud-based software services are maturing, cloud platform and infrastructure offerings are still in their early stages

The Software-As-a-Service Model

In a SaaS model, the customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model (an operational expense, known as OpEx).

In some cases, the service is free for limited use.

The Software-As-a-Service Model

SaaS enables the organization to outsource the hosting and management of applications to a third party (software vendor and service provider) as a means of reducing the cost of application software licensing, servers, and other infrastructure and personnel required to host the application internally.

The Platform-As-a-Service Model

In a platform-as-a-service (PaaS) model, the vendor offers a development environment to application developers, who develop applications and offer those services through the provider's platform.

The provider typically develops toolkits and standards for development, and channels for distribution and payment.

The Platform-As-a-Service Model

PaaS systems are useful because they enable lone developers and start-up companies to deploy web-based applications without the cost and complexity of buying servers and setting them up. The benefits of PaaS lie in greatly increasing the number of people who can develop, maintain, and deploy web applications.

The Infrastructure-As-a-Service Model

The IaaS model provides the infrastructure (housing dedicated hardware) to run the applications, but the cloud computing approach makes it possible to offer a pay-per-use model and to scale the service depending on demand.

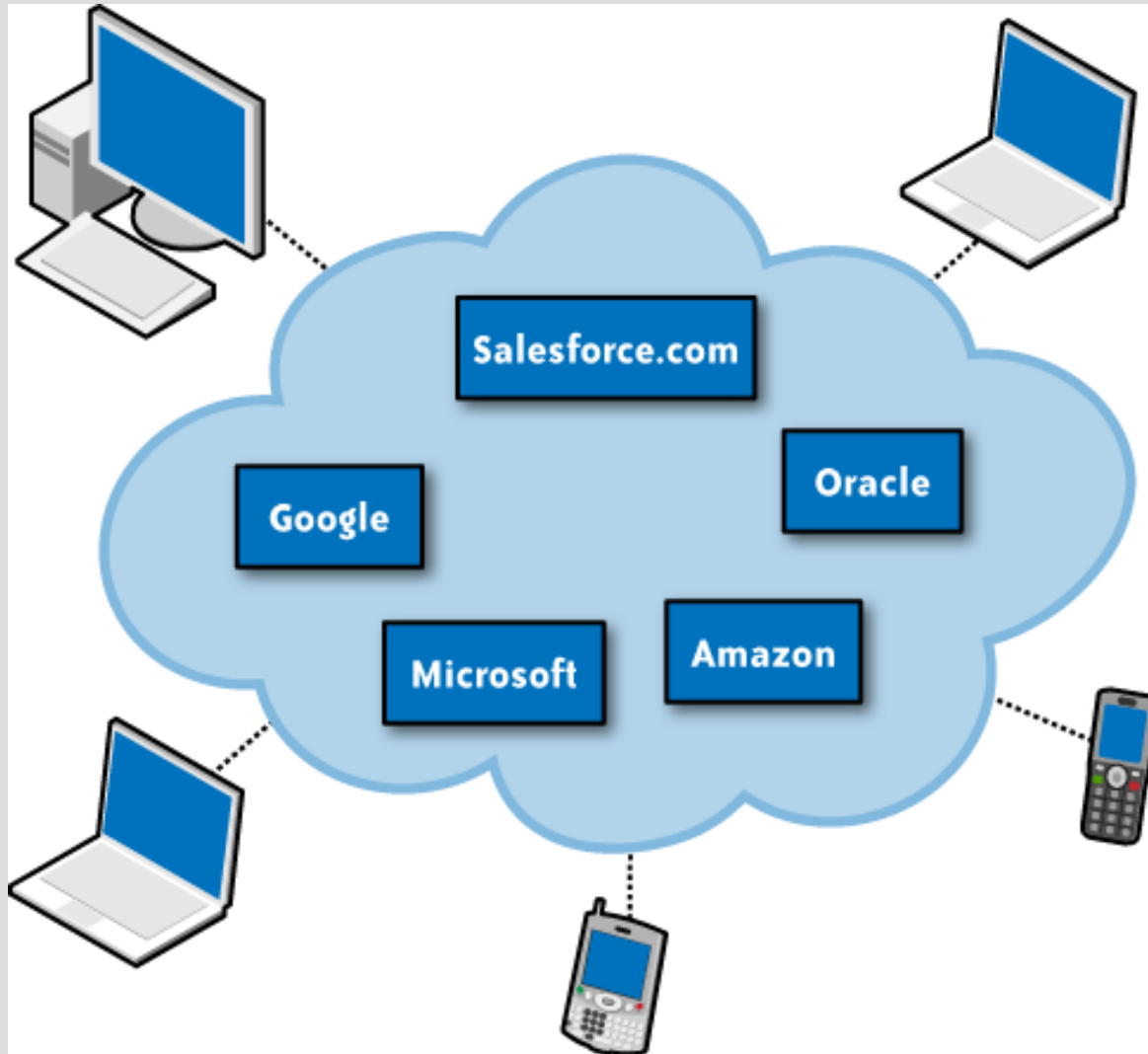
The Infrastructure-As-a-Service Model

From the IaaS provider's perspective, it can build an infrastructure that handles the peaks and troughs of its customers' demands and add new capacity as the overall demand increases.

Cloud Deployment Models

- Private cloud
 - enterprise owned or leased
- Community cloud
 - shared infrastructure for specific community
- Public cloud
 - Sold to the public, mega-scale infrastructure
- Hybrid cloud
 - composition of two or more clouds

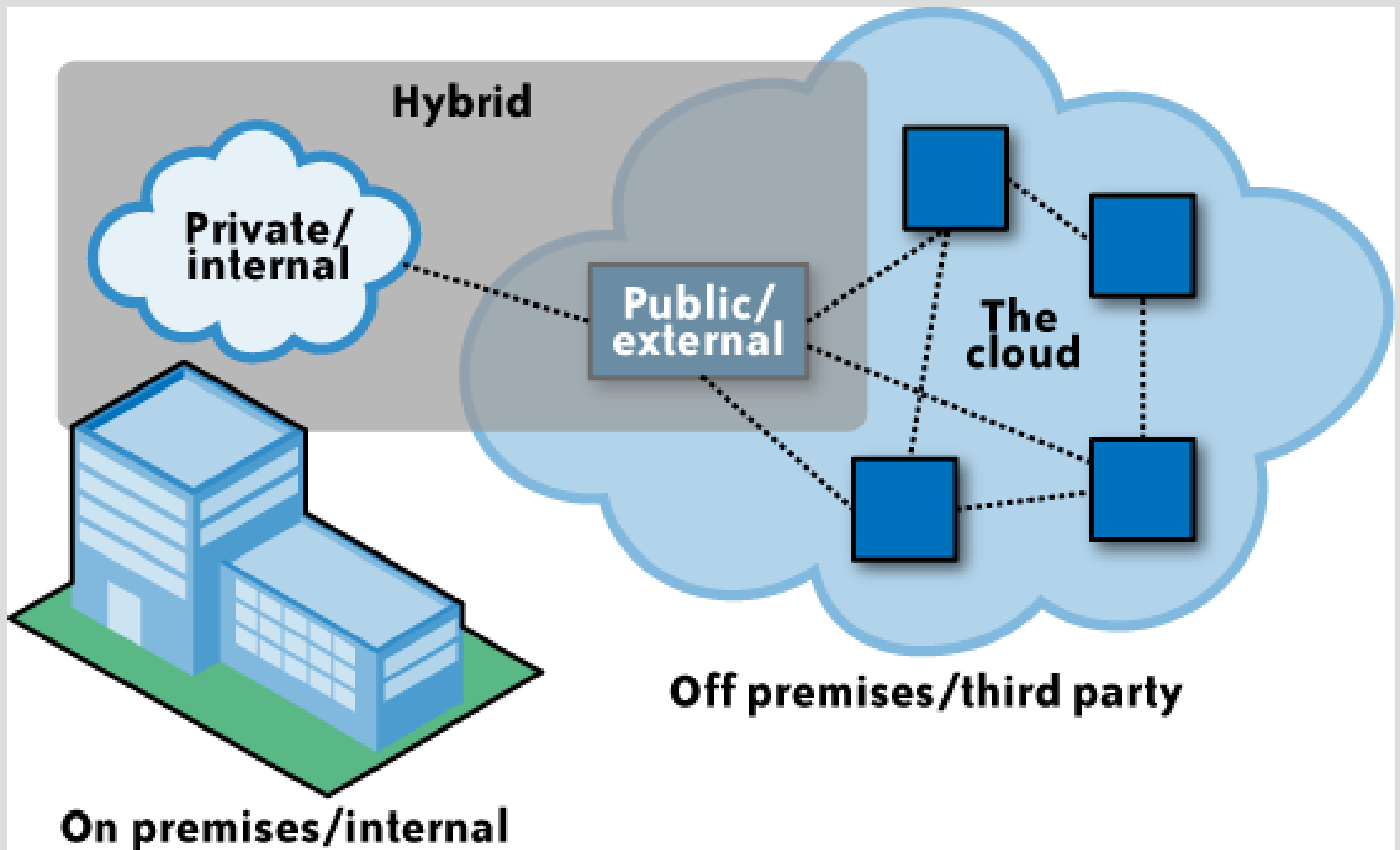
Public cloud



Private cloud

Private clouds and internal clouds are terms used to describe offerings that emulate cloud computing on private networks. Organizations must buy, build, and manage them and, as such, do not benefit from lower upfront capital costs and less hands-on management. The organizational customer for a private cloud is responsible for the operation of his private cloud. increases.

Hybrid cloud



Client/server computing Vs. Cloud computing

Dedicated/traditional IT	Cloud computing
High upfront IT investments for new builds	Low upfront IT investments; pay-for-use model
High cost of reliable infrastructure	Reliability built into the cloud architecture
High complexity of IT environment	Modular IT architecture environments
Complex infrastructure	No infrastructure

Cloud computing challenges

Security

Because cloud computing represents a new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing.

Cloud computing challenges

Security Concerns

1. Where's the data?
2. Who has access?
3. What are your regulatory requirements?
4. Do you have the right to audit?
5. What type of training does the provider offer their employees?
6. What type of data classification system does the provider use?

Cloud computing challenges

Security Concerns

7. What are the service level agreement (SLA) terms?

8. What is the long-term viability of the provider?

9. What happens if there is a security breach?

10. What is the disaster recovery/business continuity plan (DR/BCP)?

Cloud computing challenges

Privacy

Organizations today face numerous different requirements attempting to protect the privacy of individuals' information, and it is not clear (i.e., not yet established) whether the cloud computing model provides adequate protection of such information, or whether organizations will be found in violation of regulations because of this new model.

Cloud computing challenges

Connectivity and Open Access

The full potential of cloud computing depends on the availability of high-speed access to all. Such connectivity, rather like electricity availability, globally opens the possibility for industry and a new range of consumer products.

Cloud computing challenges

Reliability

Enterprise applications are now so critical that they must be reliable and available to support 24/7 operations. In the event of failure or outages, contingency plans must take effect smoothly, and for disastrous or catastrophic failure, recovery plans must begin with minimum disruption.

Cloud computing challenges

Infrastructure Security: The Network Level

- Ensuring the confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider

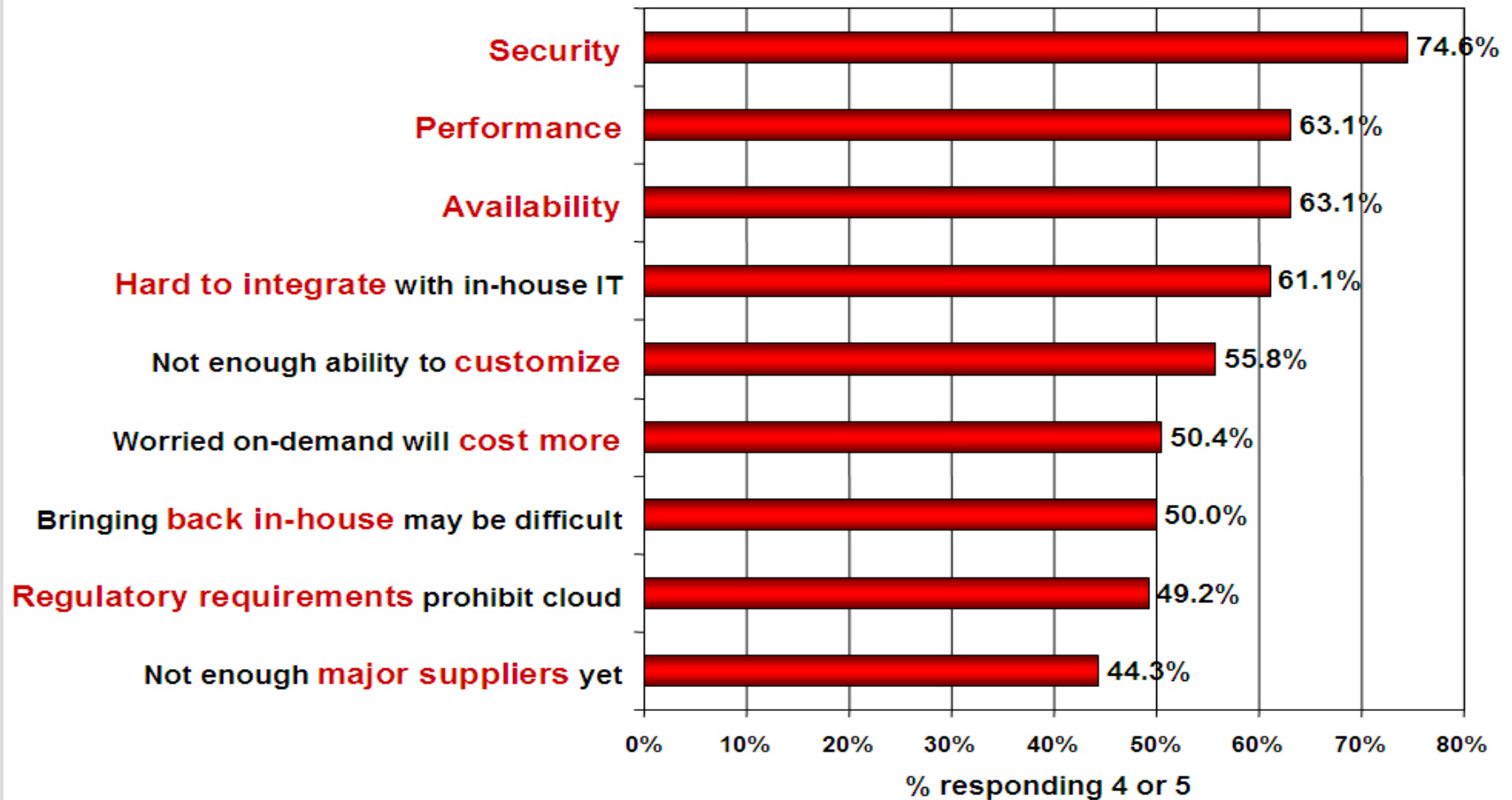
Cloud computing challenges

Infrastructure Security: The Network Level

- Ensuring the availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

Cloud computing challenges

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

Analyzing Cloud Security

- Some key issues:
 - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
 - There are both advantages and challenges

General Security Advantages

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery



General Security Challenges

- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control



Securing Data in the Cloud

- Location of your data
- Control of your data
- Secure transfer of your data



Securing Data in the Cloud

- After data goes into the cloud, you may not have control over where it's stored geographically. Consider these issues:
- **Specific country laws:**
- Laws governing data differ across geographic boundaries.
- Your own country's legal protections may not apply if your data is located outside of the country.

Securing Data in the Cloud

Data transfer across country borders:

- A global company with subsidiaries or partners (or clients for that matter) in other countries may be concerned about cross-border transfer of data due to local laws.
- Virtualization makes this an especially tough problem because the cloud provider might not know where the data is at any particular moment.

Securing Data in the Cloud

Data control in the cloud:

- Controls include the governance policies set in place to make sure that your data can be trusted. The integrity, reliability, and confidentiality of your data must be beyond reproach. (example)
- You must understand what level of controls will be maintained by your cloud provider and consider how these controls can be audited.

Securing Data in the Cloud

Securing data for transport in the cloud:

- Regarding data transport, keep two things in mind:
- Make sure that no one can intercept your data as it moves from point A to point B in the cloud.(example)
- Make sure that no data leaks (malicious or otherwise) from any storage in the cloud.

Provisioning Service

- Advantages

- Rapid reconstitution of services
- Enables availability
 - Provision in multiple data centers / multiple instances
- Advanced honey net capabilities

- Challenges

- Impact of compromising the provisioning service

Data Storage Services

- Advantages
 - Data fragmentation and dispersal
 - Automated replication
 - Provision of data zones (e.g., by country)
 - Encryption at rest and in transit
 - Automated data retention
- Challenges
 - Isolation management / data multi-tenancy
 - Storage controller
 - Single point of failure / compromise?
 - Exposure of data to foreign governments

Cloud Processing Infrastructure

- Advantages
 - Ability to secure masters and push out secure images
- Challenges
 - Application multi-tenancy
 - Reliance on hypervisors
 - Process isolation / Application sandboxes

Cloud Support Services

- Advantages
 - On demand security controls (e.g., authentication, logging, firewalls...)
- Challenges
 - Additional risk when integrated with customer applications
 - Needs certification and accreditation as a separate application
 - Code updates

Cloud Security Challenges Part 1

- Data dispersal and international privacy laws
 - EU Data Protection Directive and U.S. Safe Harbor program
 - Exposure of data to foreign government and data subpoenas
 - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees



Cloud Security Challenges Part 2

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
 - Encrypting access to the cloud resource control interface
 - Encrypting administrative access to OS instances
 - Encrypting access to applications
 - Encrypting application data at rest
- Public cloud vs internal cloud security
- Lack of public SaaS version control





Additional Issues

- Issues with moving PII and sensitive data to the cloud
 - Privacy impact assessments
- Using SLAs to obtain cloud security
 - Suggested requirements for cloud SLAs
 - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
 - FISMA
 - HIPAA
 - SOX
 - PCI
 - SAS 70 Audits

Putting it Together

- Most clouds will require very strong security controls
- All models of cloud may be used for differing tradeoffs between threat exposure and efficiency
- There is no one “cloud”. There are many models and architectures.
- How does one choose?

Three Features of Mature SaaS Applications

- Scalable
 - Handle growing amounts of work in a graceful manner
- Multi-tenancy
 - One application instance may be serving hundreds of companies
 - Opposite of multi-instance where each customer is provisioned their own server running one instance
- Metadata driven configurability
 - Instead of customizing the application for a customer (requiring code changes), one allows the user to configure the application through metadata

Cloud Computing

- Effective trust management,
- guaranteed security,
- user privacy,
- data integrity,
- mobility support, and copyright protection are crucial to the universal acceptance of cloud as a ubiquitous service.

References

- The Cloud at Your Service: The when, how, and why of enterprise cloud computing By: Jothy Rosenberg; Arthur Mateos
- Cloud Security and Privacy By: Tim Mather; Subra
- Cloud Security: A Comprehensive Guide to Secure Cloud Computing By: Ronald L. Krutz; Russell Dean Vines

References

- www.nasa.gov/.../482833main_2010_Tuesday_5_Hunt_Linton_ChweSpence
.
- Effectively and Securely Using the Cloud Computing Paradigm by: Peter Mell, Tim Grance - NIST, Information Technology Laboratory

Questions?