Cloud Concepts and Security

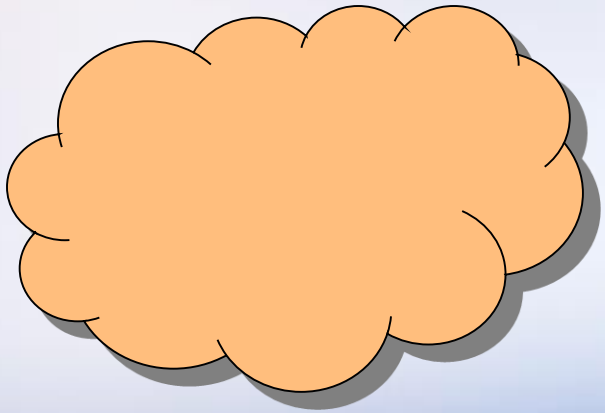
IIA Lansing Chapter
Sajay Rai, CPA, CISSP, CISM
President & CEO, Securely Yours LLC
sajayrai@securelyyoursllc.com
April 14, 2014

Agenda

- What is cloud computing?
- Cloud Service Models
- Cloud Deployment Models
- Public Cloud Security Upside
- Public Cloud Security Downside
- Other Cloud Computing Security Concerns

Cloud Computing

Cloud computing can be defined as virtual servers, services, or anything you consume over the Internet. Cloud computing gets its name from the representation of the Internet.



The Conceptual Reference Model

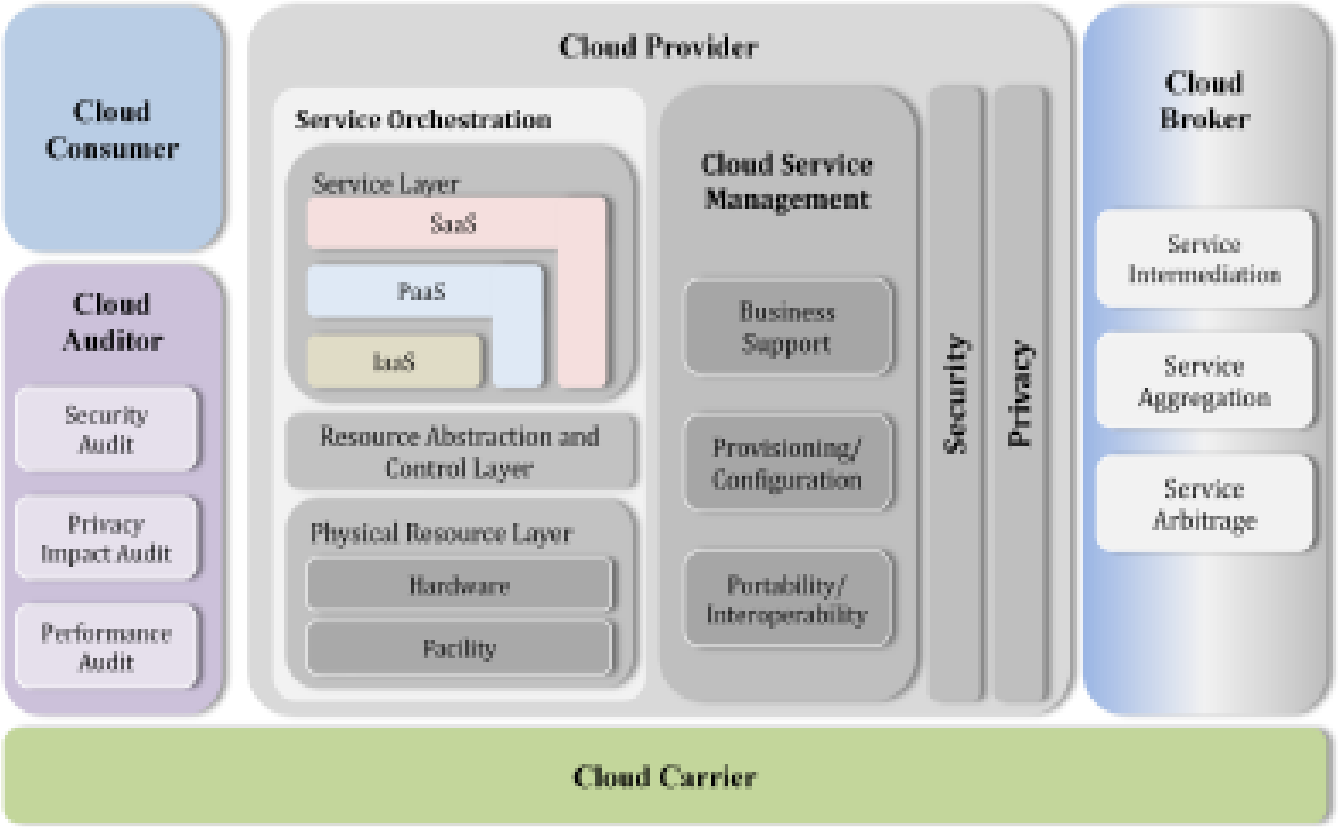
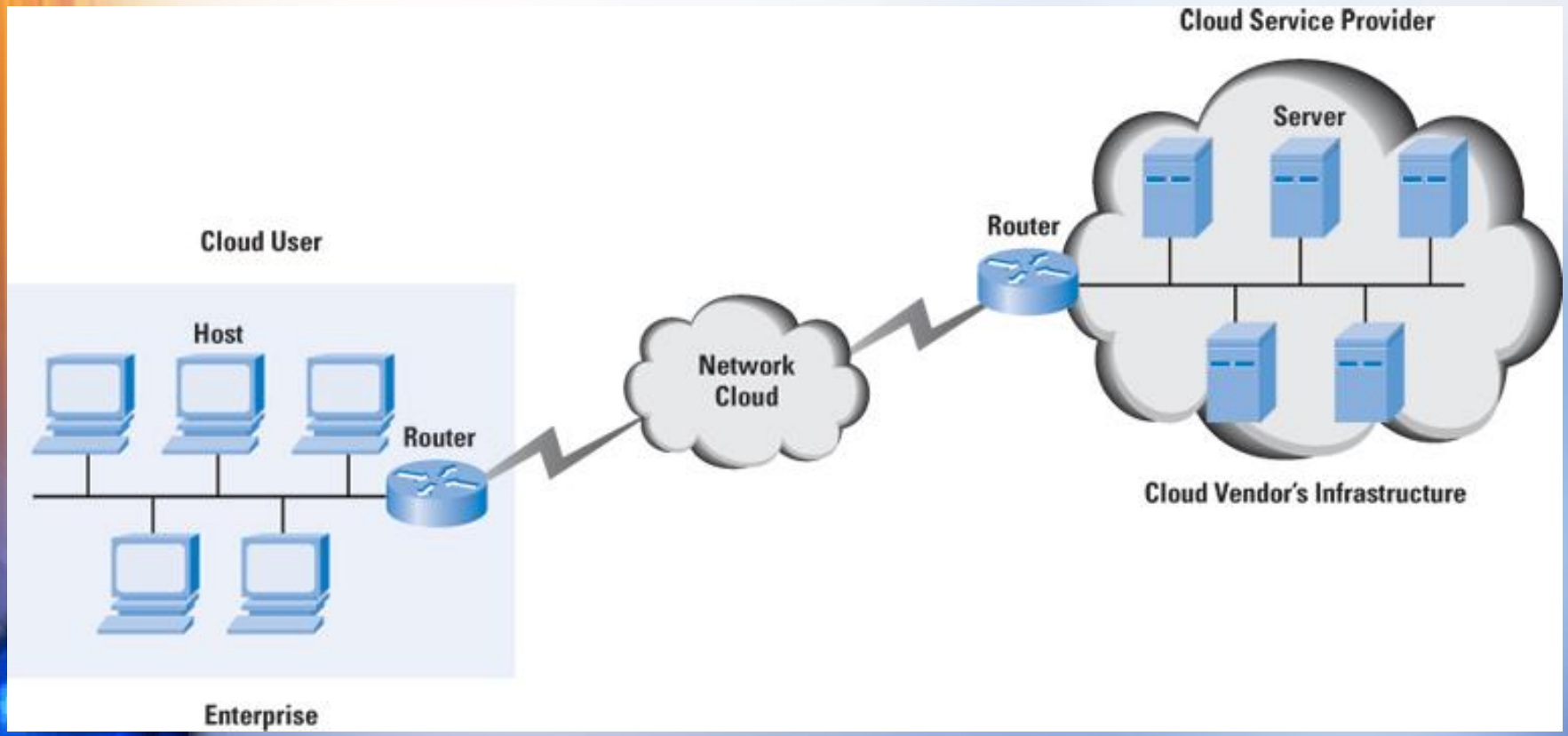


Figure 1: The Conceptual Reference Model

Another View



The NIST 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.
- This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models

Essential Characteristics:

- On demand self service
  - Consumers provision computing capabilities, not service providers
  - Compute power, storage, bandwidth, etc.
- Broad network access
  - Available of the “network”
  - Accessible by thin clients
- Resource pooling
  - Provider provides resources dynamically, assigning and reassigned according to demand
  - Typically no consumer control or knowledge of location or assignment to hardware

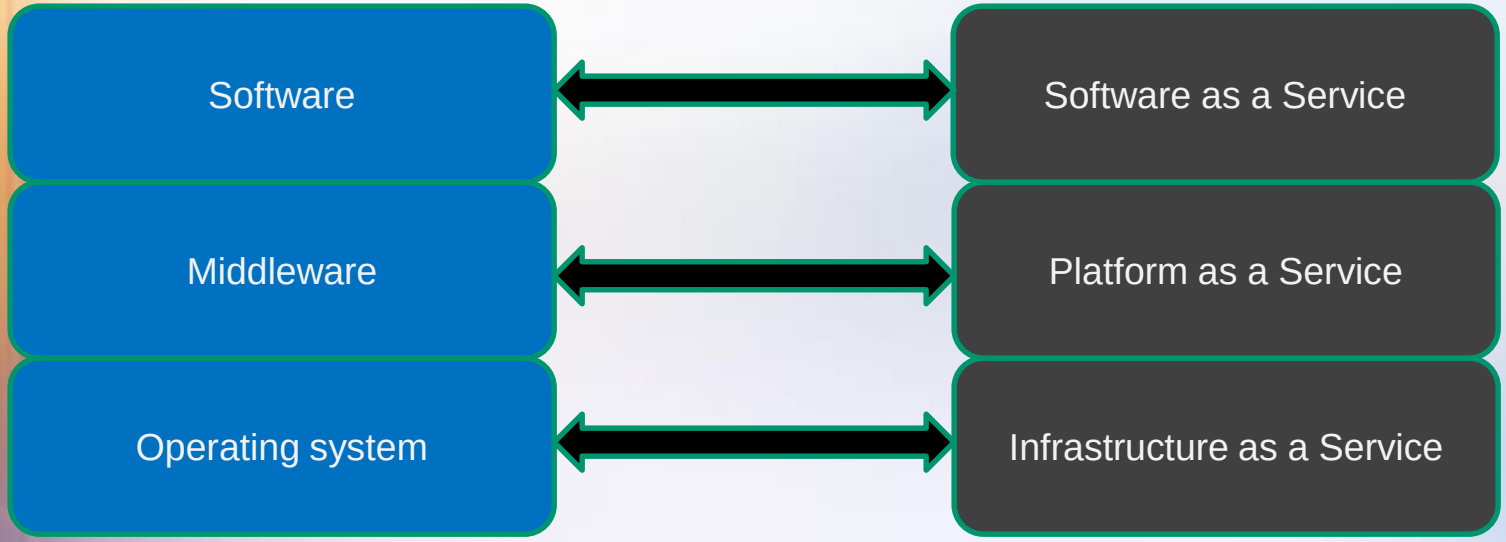
Cloud Characteristics (continued)

- Rapid elasticity
  - Resources provisioned and de-provisioned quickly and often automatically to scale up and down
  - Appearance of unlimited capacity
- Measured service
  - Meter usage by various parameters depending on service (e.g., storage, processing, bandwidth, user accounts)
  - Reporting usage available
- Multitenancy
  - Multitenancy and multitenant amortization of the shared compute resource is part of the reason for the economic benefits of cloud computing

Cloud Characteristics (continued)

- Economics
  - Consumer is charged for the amount of time used on the resource
  - Cloud computing changes the computing barrier to entry for high performance resources
  - Organizations can respond to peak demands for computing resources without having resources sitting idle most of the time
- Abstraction
  - The operational aspects of the layer supporting the service is insulated from the customer. A SaaS customer will interact with the application, not with the operating system or the hardware of the cloud.

Traditional Model versus Cloud Computing Model



Cloud Service Models

- According to NIST, there are three service models for the cloud
  - Software as a Service
  - Platform as a Service
  - Infrastructure as a Service
- I have discovered that there are two more:
  - Monitoring as a Service
  - Data as a Service
- They differ in interface, access, control, and transparency
- The details of who manages systems, networks, and applications vary significantly
- Consequently, so do compliance requirements

Deployment Models:

- Deployment models determine who has access to the cloud and what a cloud is used for
  - Single/multiple organization use
  - Single/multiple purpose
  - Single multiple provider
- The deployment models can have a significant impact on security and compliance
- The co-location of data, services, providers can complicate security mechanisms and assurances

Cloud Deployment Models

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

Private Cloud

- Operated solely for an organization
- Administered by the organization or a third party
- On or off premise
- Private cloud provides the best opportunity for achieving compliance with most regulations and contracts
  - Single organization control
  - Configurable transparency and audit
  - Storage, network, administration, access control, monitoring, and vulnerability management can be accomplished according to regulatory / contractual requirements

Community Cloud

- Shared by several organizations and supports a specific community with shared concerns
  - Mission, security, policy, compliance
- May be possible to comply with regulations and contracts
- Highly dependent on service model
- Need specific guarantees from provider
  - Storage protection
  - Administration (who has access?)
  - Network mechanisms (encryption, segregation, intrusion detection)
  - Monitoring (who monitors? How reliable)

Public Cloud

- Available to the general public or a large industry group
- Sold as cloud services
- Another challenging configuration
- Again, compliance difficulty depends heavily on service model
  - SaaS may be possible
  - PaaS difficult
  - IaaS difficult as well
- Resource recycling could pose a problem?
- What constitutes the private versus the public environment?
- What guarantees does the provider give regarding administrative control, access, encryption, storage cleanup?

Hybrid cloud

- Composition of two or more clouds that remain unique but support data and application portability
- Compliance is complicated by multiple entities and multiple environments
  - Who is responsible for what?
  - How does data move?
- Possibilty that each environment is designed for particular service, data protection, and security requirements (unlikely)

Cloud Computing Models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Monitoring as a Service (MaaS)
- Software as a Service (Saas)

Infrastructure as a Service (IaaS)

- Consumer can provision processing, storage, networks, and other computing resources
- Cloud infrastructure is managed by provider
- Consumer can deploy and control operating systems, applications, and possibly networking
- Given the level of platform control, this model leaves most of the compliance burden on the consumer
- The issue becomes understanding the access and control that the cloud provider has
- Evaluation of security practice, auditing of control, and contractual requirements for compliance remain important

Platform as a Service

- Consumer deploys developed or acquired applications using languages and tools provided by the platform provider
- Consumer does not manage or control the underlying infrastructure (network, servers, operating systems, or storage), but controls application
- Compliance burden is split between consumer and provider with evaluation and contract requirements on consumer

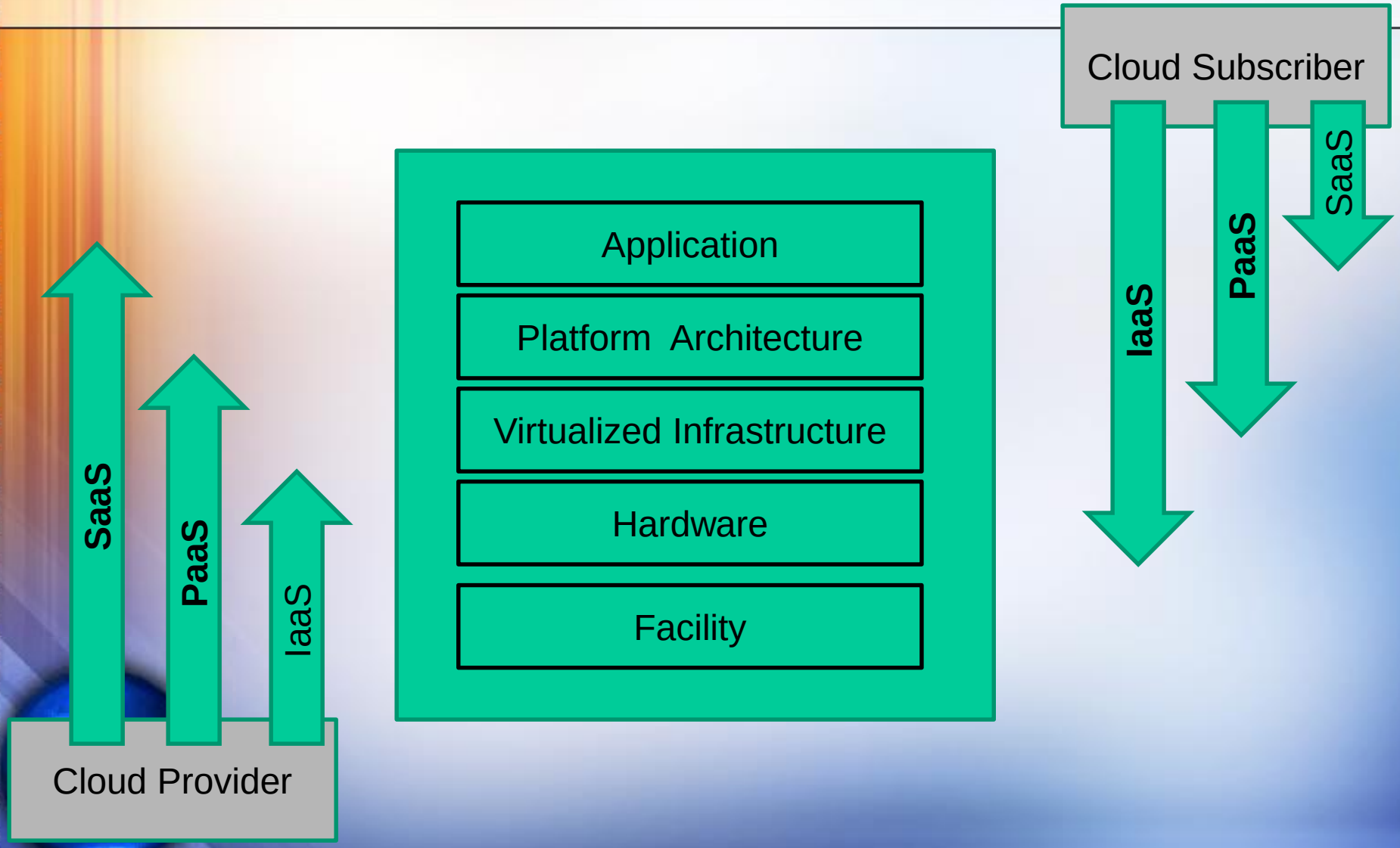
Software as a Service

- Service provider's application runs in the cloud
- Consumer does not manage or control the underlying infrastructure or application capabilities
- Direct compliance is the service provider's problem
- Most regulations require consumers to verify compliance and maintain contracts

Compliance Requirements

- Privacy laws (state privacy laws)
- Financial integrity (SOX)
- Industry specific regulations
  - Health (HIPAA, HITECH)
  - Payment Card (PCI DSS)
  - Financial (GLB, FFIEC Guidelines)
- Regulations may be relative general to prescriptive
  - GLB –general
  - PCI DSS –extremely prescriptive
  - Trend in state laws and federal laws is more prescriptive

Difference in Scope and Control among Cloud Service Models



Video

Video

Public Cloud Security Upside

- The biggest obstacle facing public cloud computing is security
- Cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations.
- Potential areas of improvement where organizations may derive security benefits from transitioning to a public cloud computing environment include the following:
  - Staff Specialization
  - Platform Strength
  - Resource Availability
  - Backup and Recovery
  - Mobile Endpoints
  - Data Concentration
  - Data Center Oriented
  - Cloud Oriented

Public Cloud Security Upside – cont.

- Staff Specialization - Cloud providers, just as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization
- Platform Strength - The structure of cloud computing platforms is typically more uniform than that of most traditional computing centers.
- Greater uniformity and homogeneity facilitate:
  - platform hardening,
  - configuration control,
  - vulnerability testing,
  - security audits, and
  - security patching of platform components.

Public Cloud Security Upside – cont.

  - Information assurance and security response activities can also be improved
  - Many cloud providers meet standards for operational compliance and certification in areas like healthcare, finance and audit.
- Resource Availability - The scalability of cloud computing facilities allows for greater availability.
  - Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents

Public Cloud Security Upside – cont.

- Backup and Recovery - The backup and recovery policies and procedures of a cloud service may be superior to those of the organization.
  - Data maintained within a cloud can be more available, faster to restore, and more reliable in many circumstances.
  - Cloud services could also serve as a means for offsite backup storage for an organization's data center
- Mobile Endpoints - The architecture of a cloud solution extends to the client at the service endpoint, used to access hosted applications
  - Cloud clients can be browser-based or applications-based.
  - The main servers held by the cloud provider,
  - Clients are generally lightweight computationally and easily supported on laptops, notebooks, netbooks, smart phones, and tablets

Public Cloud Security Upside – cont.

- Data Concentration - Data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur
- Data Center Oriented - Cloud services can be used to improve the security of data centers.
- Cloud Oriented - Cloud services are available to improve the security of other cloud environments.
  - For example, reverse proxy products are available that enable unfettered access to a SaaS environment, yet maintain the data stored in that environment in encrypted form.
  - Cloud-based identity management services also exist, which can be used to augment or replace an organization's directory service for identification and authentication of users to a cloud.

Public Cloud Security Downside

- System Complexity
- Shared Multi-tenant Environment
- Internet-facing Services
- Loss of Control

Public Cloud Security Downside

- System Complexity - A public cloud computing environment is extremely complex compared with that of a traditional data center
- Internet-facing Services - Public cloud services are delivered over the Internet, exposing both the administrative interfaces used to self-service an account and the interfaces for users and applications to access other available services.
- Loss of Control - While security and privacy concerns in cloud computing services are similar to those of traditional non-cloud services, they are amplified by external control over organizational assets.
- Shared Multi-tenant Environment - Public cloud services offered by providers have a serious underlying complication—subscribing organizations typically share components and resources with other subscribers that are unknown to them.

Other Cloud Computing Security Concerns

- Governance
- Compliance
  - Compliance requirements
- Data Location
- Electronic Discovery
- Data Access, Location and Ownership
- Composite Services
- Visibility
- Risk Management
- Architecture
- Attack Surface
- Ancillary Data
- Client-Side Protection
- Identity and Access Management
- Software Isolation
- Data Protection
- Incident Response

Governance

- Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services.
- With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems.
- While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Compliance

- Compliance involves conformance with an established specification, standard, regulation, or law.
- Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Compliance Requirements

- Privacy laws (state privacy laws)
- Financial integrity (SOX)
- Industry specific regulations
  - Health (HIPAA, HITECH)
  - Payment Card (PCI DSS)
  - Financial (GLB, FFIEC Guidelines)
- Regulations may be relative general to prescriptive
  - GLB –general
  - PCI DSS –extremely prescriptive
  - Trend in state laws and federal laws is more prescriptive
    - Cloud providers are becoming more sensitive to legal and regulatory concerns, and you may be able to negotiate that they store and process data in specific jurisdictions and apply required safeguards for security and privacy.
    - However, the degree to which they will accept liability for exposure of content under their control remains to be seen.
    - Bottom line the subscriber is ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

- One of the most common compliance issues facing an organization is data location. Use of an in-house computing center allows an organization to structure its computing environment and to know in detail where data is stored. data.
- In contrast, a characteristic of many cloud computing services is that detailed information about the location of an organization’s data is unavailable.
- This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met.
- External audits and security certifications can to some extent alleviate this issue, but they are not a panacea.

Electronic Discovery

- Electronic discovery involves the identification, collection, processing, analysis, and production of electronic documents in the discovery phase of litigation.
- Organizations also have other incentives and obligations to preserve and produce electronic documents, such as complying with audit and regulatory information requests
- The capabilities and process of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner
  - For example, a cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Who can access the data?

- Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider.

Insider Access

- Data processed or stored outside the confines of an organization, its firewall, and other security controls bring with it an inherent level of risk.
- The insider security threat is a well-known issue for most organizations and, despite the name, applies as well to outsourced cloud services.
- Moving data and applications to a cloud computing environment operated by a cloud provider expands the insider security risk not only to the cloud provider's staff, but also potentially among other customers using the service.
  - For example, a denial of service attack launched by a malicious insider was demonstrated against a IaaS cloud
  - The attack involved a cloud subscriber creating an initial 20 accounts and launching virtual machine instances for each, then using those accounts to create an additional 20 accounts and machine instances in an iterative fashion, exponentially growing and consuming resources beyond set limits.

Data Ownership

- The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust.
- Ideally, the contract should state clearly that:
  - the organization retains ownership over all its data;
  - the cloud provider acquires no rights or licenses through the agreement to use the data for its own purposes, including intellectual property rights or licenses;
  - the cloud provider does not acquire and may not claim any security interest in the data
- For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Composite Services

- Cloud services themselves can be composed through nesting and layering with other cloud services.
  - For example, a SaaS provider could build its services upon the services of a PaaS or IaaS cloud.
- The level of availability of the SaaS cloud would then depend on the availability of those services
- Trust is often not transitive, requiring that third-party arrangements be disclosed in advance of reaching an agreement with the cloud provider.
  - Liability and performance guarantees can become a serious issue with composite cloud services.
    - For example, a consumer storage-based social networking service closed down after losing access to a significant amount of data from 20,000 of its subscribers.

Visibility

- Migration to public cloud services relinquishes control to the cloud provider for securing the systems on which the organization's data and applications operate.
- Management, procedural, and technical controls used in the cloud must be commensurate with those used for internal organizational systems or surpass them, to avoid creating gaps in security.
- Cloud providers are typically reluctant to provide details of their security and privacy, since such information might be used to devise an avenue of attack.
- Ideally, you would want control over aspects of the means of visibility, such as the threshold for alerts and notifications or the level of detail and schedule for reports, to accommodate this requirement.

Visibility – cont.

- Moreover, detailed network and system level monitoring by a cloud subscriber is generally not part of most service arrangements, limiting visibility and the means to audit operations directly .
- Transparency in the way the cloud provider operates is a vital ingredient for effective oversight over system security and privacy.
- To ensure that policy and procedures are being enforced throughout the system lifecycle, service arrangements should include some means for gaining visibility into the security controls and processes employed by the cloud provider and their performance over time.

Risk Management

- With cloud-based services, some subsystems or subsystem components are outside of the direct control of a subscribing organization.
- Public cloud-based systems, as with traditional information systems, require that risks are managed throughout the system lifecycle.
- Assessing and managing risk in systems that use cloud services can be a challenge.
- To the extent practical, the organization should ensure that security controls are implemented correctly, operate as intended, and meet its security requirements.

Risk Management – cont.

- Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls.
- However, verifying the correct functioning of a subsystem and the effectiveness of security controls as extensively as with an organizational system may not be feasible in some cases, and other means (e.g., third party audits) may be used to establish a level of trust.
- Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

- The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud.
- The physical location of the infrastructure is determined by the cloud provider as is the implementation of the reliability and scalability logic of the underlying support framework.
- Virtual machines often serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture.
- Applications are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces.

Attack Surface

- The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines.
- Besides virtualized resources, the hypervisor normally supports other application programming interfaces to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances.
- Compared with a traditional non-virtualized implementation, the addition of a hypervisor causes an increase in the attack surface.

Ancillary Data

- While the focus of protection is placed mainly on the application data, as guardians of the realm, cloud providers hold significant details about the service users' accounts that could be compromised and used in subsequent attacks.
- Payment information is one example; other, more subtle types of information, can also be involved.
  - For example, a database of contact information stolen from a SaaS cloud provider, via a targeted phishing attack against one of its employees, was used in turn to launch successful targeted electronic mail attacks against subscribers of the cloud service.
  - The incident illustrates the need for cloud providers to promptly report security breaches occurring not only in the data the cloud provider holds for its subscribers, but also the data it holds about its subscribers.

Client-Side Protection

- A successful defense against attacks requires securing both the client and server side of cloud computing.
- Web browsers, a key element for many cloud computing services, and the various available plug-ins and extensions for them are notorious for their security problems.
- Moreover, many browser add-ons do not provide automatic updates, increasing the persistence of any existing vulnerabilities.

Client-Side Protection – cont.

- Maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones.
- Their size and portability can result in the loss of physical control.
- Built-in security mechanisms often go unused or can be overcome or circumvented without difficulty by a knowledgeable party to gain control over the device.
- Smart phones are also treated more as fixed appliances with a limited set of functions, than as general-purpose systems.
- No single operating system dominates and security patches and updates for system components and add-ons are not as frequent as for desktop clients.

Client-Side Protection – cont.

- The increased availability and use of social media, personal Webmail, and other publicly available sites also have associated risks that are a concern, since they can negatively impact the security of the browser.
  - For example, spyware was reportedly installed in a hospital system via an employee's personal Webmail account and sent the attacker more than 1,000 screen captures, containing financial and other confidential information, before being discovered.

Client-Side Protection – cont.

- Having a backdoor Trojan, keystroke logger, or other type of malware running on a client does not bode well for the security of cloud or other Web-based services it accesses.
- As part of the overall security architecture for cloud computing, organizations need to review existing measures and employ additional ones, if necessary, to secure the client side.
- Banks are beginning to take the lead in deploying hardened browser environments that encrypt network exchanges and protect against keystroke logging.

Identity and Access Management

- Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern
- One recurring issue is that the organizational identification and authentication framework may not naturally extend into the cloud and extending or changing the existing framework to support cloud services may be difficult.

Identity and Access Management

- The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication.
- Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard

Authentication

- A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data.
- SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains.
- SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the eXtensible Markup Language (XML) for its format.
- SOAP messages are digitally signed

Software Isolation

- High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits.
- To reach the high scales of consumption desired, cloud providers have to ensure dynamic flexible delivery of service and isolation of subscriber resources.
- Multi-tenancy in cloud computing is typically done by multiplexing the execution of virtual machines from potentially different users on the same physical server.
  - This was dramatically exemplified by a botnet found operating out of an IaaS cloud computing environment.

Data Protection

- Data stored in the cloud typically resides in a shared environment collocated with data from other customers.
- Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure.
- Access controls are one means to keep data away from unauthorized users; encryption is another.
- Access controls are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing

Data Protection

- Data Sanitization - The data sanitization practices that a cloud provider implements have obvious implications for security.
  - Sanitization is the removal of sensitive data from a storage device in various situations, such as when a storage device is removed from service or moved elsewhere to be stored.
- Data sanitization also applies to backup copies made for recovery and restoration of service, and also residual data remaining upon termination of service.

Data Protection – cont.

- In a cloud computing environment, data from one subscriber is physically commingled with the data of other subscribers, which can complicate matters.
  - For instance, many examples exist of researchers obtaining used drives from online auctions and other sources and recovering large amounts of sensitive information from them.
  - With the proper skills and equipment, it is also possible to recover data from failed drives that are not disposed of properly by cloud providers.

Availability

- In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable.
- Availability can be affected temporarily or permanently, and a loss can be partial or complete.
- Denial of service attacks, equipment outages, and natural disasters are all threats to availability.
- The concern is that most downtime is unplanned and can impact the mission of the organization.

Availability – cont.

- Temporary Outages. Despite employing architectures designed for high service reliability and availability, cloud computing services can and do experience outages and performance slowdowns.
- A number of examples illustrate this point:
  - February 2008, a popular storage cloud service suffered a three-hour outage that affected its subscribers, including Twitter and other startup companies.
  - June 2009, a lightning storm caused a partial outage of an IaaS cloud that affected some users for four hours.
  - February 2008, a database cluster failure at a SaaS cloud caused an outage for several hours, and in January 2009, another brief outage occurred due to a network device failure.
  - March 2009, a PaaS cloud experienced severe degradation for about 22 hours due to networking issues related to an upgrade.

Availability – cont.

- Prolonged and Permanent Outages. The possibility exists for a cloud provider to experience serious problems, like bankruptcy or facility loss, which affect service for extended periods or cause a complete shutdown.
  - For example, in April 2009, the Federal Bureau of Investigation raided computing centers in Texas and seized hundreds of servers, when investigating fraud allegations against a handful of companies that operated out of the centers.
  - The seizure disrupted service to hundreds of other businesses unrelated to the investigation, but who had the misfortune of having their computer operations collocated at the targeted centers.

Incident Response

- The cloud provider's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration.
- Collaboration between the service subscriber and provider in recognizing and responding to an incident is essential to security and privacy in cloud computing.
- The complexity of the service can obscure recognition and analysis of incidents.
  - It reportedly took one IaaS provider approximately eight hours to recognize and begin taking action on an apparent denial of service attack against its cloud infrastructure, after the issue was reported by a subscriber of the service.
  - Understanding and negotiating the provisions and procedures for incident response should be done before entering a service contract, rather than as an afterthought.

Security and Privacy Issues and Precautions

Areas	Precautions
Governance	Extend organizational practices pertaining to the policies, procedures and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiative, particularly those involving data location, privacy and security controls, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements
Trust	Incorporate mechanisms into the contract that allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance overtime. Institute a risk management program that is flexible enough too adapt to the continuously evolving and shifting risk landscape.
Architecture	Understand the underlying technologies the cloud provider uses to provision services, including the implications of the technical controls involved on the security and privacy of the system, with respect to the full lifecycle of the system and for all system components.

Security and Privacy Issues and Precautions

Areas	Precautions
Identity and Access Management	Ensure the adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions
Software Isolation	Understand virtualization and other software isolation techniques that the cloud provider employs, and assess the risk
Data Protection	Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned
Availability	Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed and that all operations can be immediately resumed and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	Understand and negotiate the contract provisions and procedures for incident response required by the organization.

Questions to ask Cloud Providers

- Who has access to the data?
- How many employees have root, database and infrastructure access?
- What policies are in place to prevent the cloud provider's employees from getting access to your company's data?
- Is the data encrypted at rest and in motion?
- Is the environment a multi-tenant one and if so, what controls data segmentation?
- Will data be stored on servers in other countries? If so, how does this impact compliance?
- What controls are in place to prevent data loss (i.e., a vendor insider downloading customer data on a USB drive)?
- What information is captured in audit/security event logs and is it available to the customer?
- What Disaster Recovery and continuity procedures does the cloud provider has?

Conclusion

- Cloud computing promises to have far-reaching effects on the systems and networks of organizations now and into the future.
- Emphasis on the cost and performance benefits of cloud computing, however, tend to overshadow some of the fundamental security and privacy concerns
- Many of the features that make cloud computing attractive can also be at odds with traditional security models and controls.
- Several critical pieces of technology, such as a solution for federated trust, are not yet fully realized, impinging on successful cloud computing deployments.

Conclusion – cont.

- Determining the security of complex computer systems composed together is also a long-standing security issue that plagues large-scale computing in general, and cloud computing in particular..
- Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. The organization must ensure that security and privacy controls are implemented correctly and operate as intended.
- Organizations should work to ensure an appropriate balance between the number and strength of controls and the risks associated with cloud computing solutions.

Final Thoughts

- Organizations are starting to use public clouds for many critical applications
  - Sharing of folders e.g. Box.net
  - Email e.g. Google mail
  - Marketing and Sales e.g. Salesforce.com
- Organizations either access these applications in the cloud by creating a separate account or link to their identity stores like Active Directory or LDAP
- Organizations usually nominate an administrator within their organization to manage the users (addition, deletion and changes)

Final Thoughts

What auditors must know?

- How the users within your organization access the application
  - How are they authenticated?
  - How the access to resources are provided?
- How the activities are logged and monitored?
- What data breach procedures does the service provider has?
- What access protocols does the service provider has in place to prohibit their employees to look at your critical data?
- What Disaster Recovery and continuity procedures does the service provider has?
- Does your organization use Single Sign-on (SSO) vendors in the public cloud to make access easier to cloud applications (e.g. Ping Identity, OneLogin)?
- Does the organization have a right to audit the provider?

Final Thoughts

What auditors must do?

1. If using SSO vendors, verify that the passwords are not being copied or stored in the service provider systems. If they are, a verification test should be performed that the passwords are encrypted (using appropriate encryption protocols) at all times.
2. Verify that the appropriate documents are provided by cloud application providers (vulnerability scan reports, SOC2 type 2 etc.)
3. If possible, conduct periodic audits of the service provider (big companies probably won't let you conduct audits)
4. Verify that your IAM process extends to the cloud service providers as well (getting rid of ids when employee leaves)
5. Verify that the logs are being reviewed either by service providers or by your organization (monitor activity and anomalies)