

Cloud Computing & Security

A Risk / Reward paradigm

Null Bangalore

5th Sept09

C N Shashidhar





Cloud Computing - Overview

- History of Cloud Computing (CC)
- Cloud Computing de mystified
- Business Drivers & Characteristics
- Cloud Delivery models
- Cloud Security concerns
- Cloud Security - Key domain areas

Cloud Computing - History

- A framework & infrastructure model with a long history & a recent past
- 1969 – Leonard Klienrock – one of chief scientists of ARPANET propounded his vision of Cloud Computing
 - *"As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities will service individual homes and offices across the country."*
- Evolved over the last 15 years or so – Cluster Computing, Grid Computing, Distributed Computing, Utility Computing, SaaS, IaaS, PaaS etc.,

Cloud Computing – de mystified

“Cloud” is an emerging consumption and delivery model for many IT-based services, in which the user sees only the service, and has no need to know anything about the technology or implementation

Attributes

Standardized,
consumable
web-delivered
services

Service
Catalog
Ordering

Flexible
pricing

Metering &
Billing

Elastic
scaling

Rapid
provisioning

Advanced
virtualization

VISIBILITY



CONTROL



AUTOMATION

....service oriented and service managed

Business Drivers & Characteristics



1.5x

Explosion of information driving 54% growth in storage shipments every year.

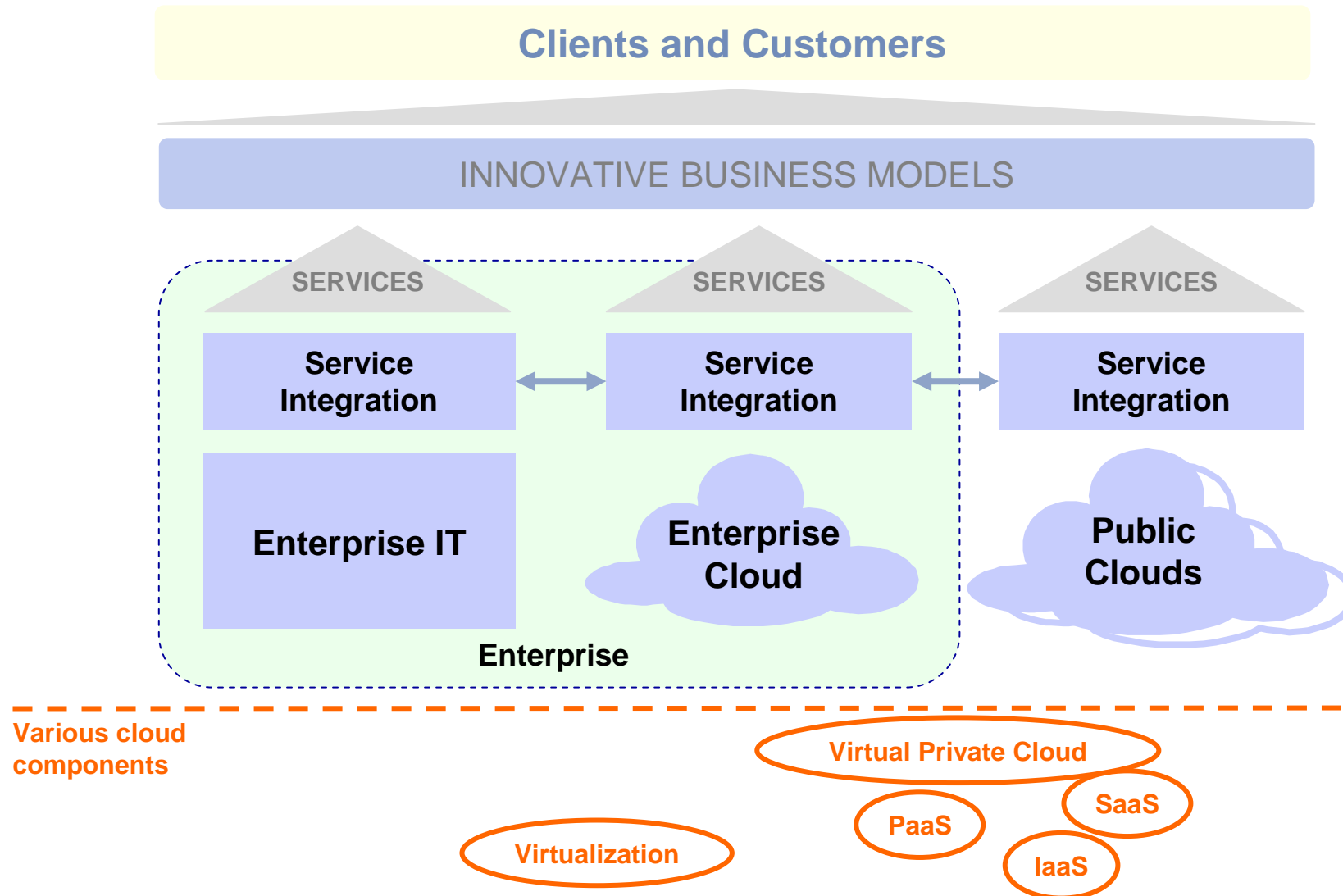
70¢ per \$1

70% on average is spent on maintaining current IT infrastructures versus adding new capabilities.

85% idle

In distributed computing environments, up to 85% of computing capacity sits idle.

Various models of cloud computing





SPI Cloud Delivery model

- Infrastructure as a Service (IaaS)
 - Only IT Infra provided; Customization by customer
 - Greatest openness & least security features
- Platform as a Service (PaaS)
 - Next step after SaaS, on demand delivery of user platform with centralized control of machines
 - Middle level with openness & Security features which must be leveraged by customer
- Software as a Service (SaaS)
 - Software centrally located, presented to user on demand using virtualization
 - Least openness & greatest amount of security responsibility by the cloud provider

Cloud Service deployment & Consumption modalities



- Private Cloud
 - Portion of the cloud exclusively for customer's use
- Public Cloud
 - Common cloud accessed by all customers.
- Managed Cloud
 - Cloud administered by Cloud provider & DC owned/located by customer
- Hybrid Cloud
 - Intermediate state of Private & Public cloud

Cloud Models

	Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Managed	Third Party Provider	Third Party Provider	On-Premise	Trusted or Untrusted
Private				Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: operations, security, compliance, etc...

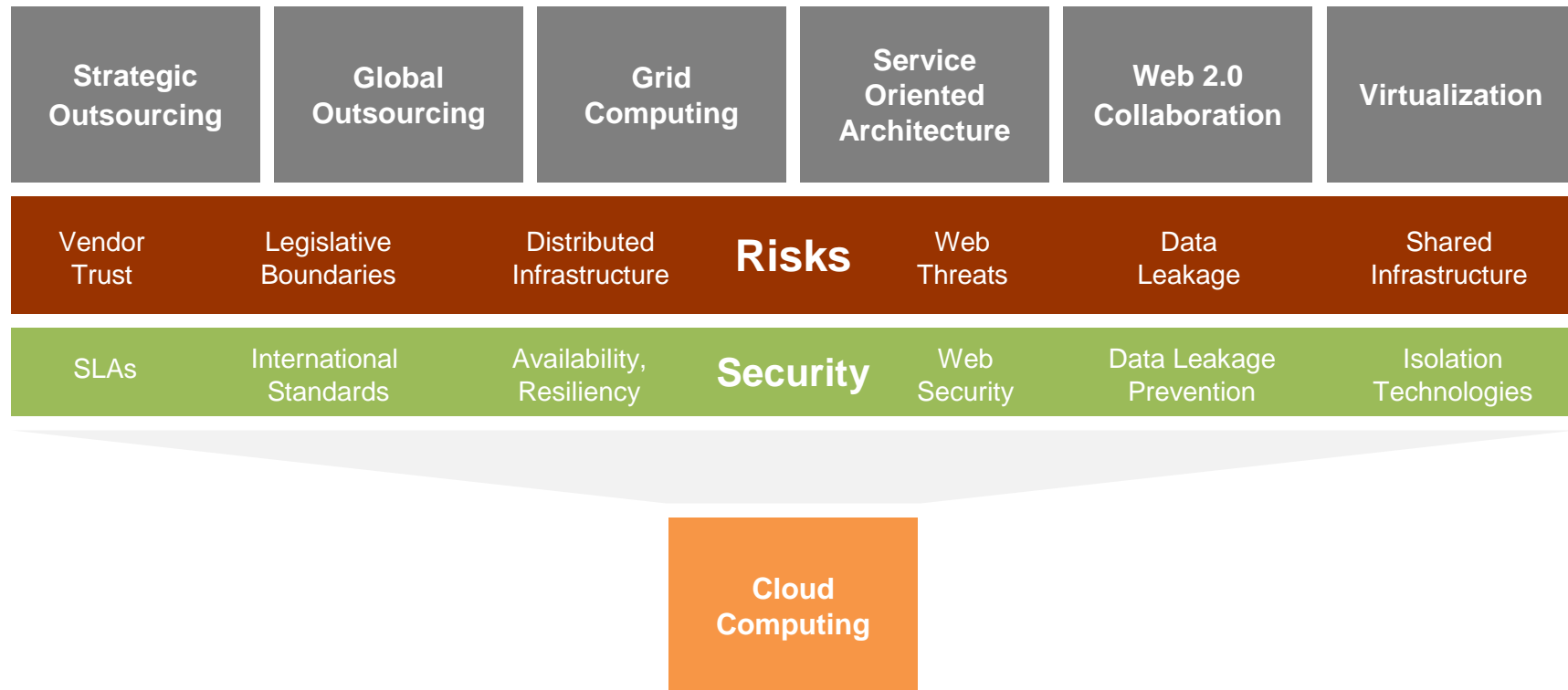
² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

Why is security important?

Security enables companies to pursue new, more efficient IT business models.



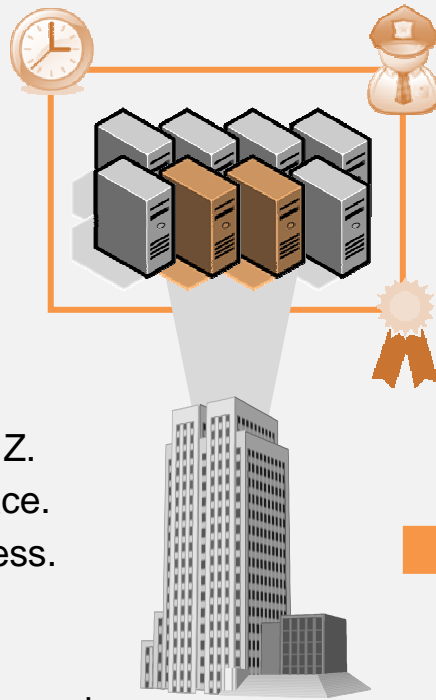
Cloud Computing is a natural evolution of the evolving IT paradigms listed above.

A variety of **security technologies, processes, procedures, laws, and trust models** are required to secure the cloud. **There is no silver bullet!**

Cloud Security 101: Simple Example

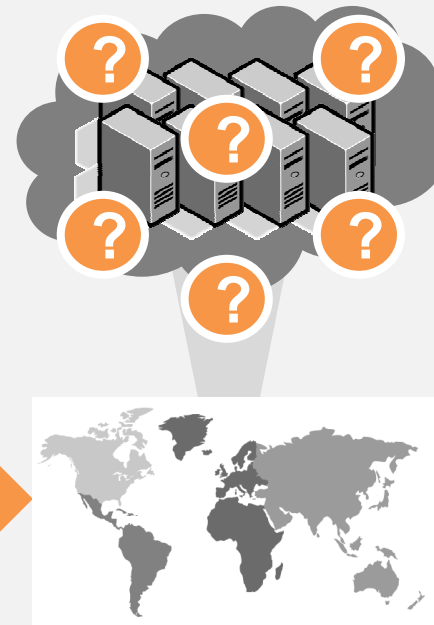
TODAY

TOMORROW



We Have Control

It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.



Who Has Control?

Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

Lesson Learned: We have responded to these questions before... clouds demand **fast, responsive, agile** answers.

High-level cloud security concerns

Less Control

Many companies and governments are **uncomfortable** with the idea of their information located on **systems they do not control**. Providers must offer a high degree of security transparency to help put customers at ease.

Data Security

Migrating workloads to a **shared** network and compute **infrastructure** increases the potential for **unauthorized exposure**. Authentication and access technologies become increasingly important.

Reliability

High availability will be a key concern. IT departments will worry about a **loss of service** should outages occur. Mission critical applications may not run in the cloud without strong availability guarantees.

Compliance

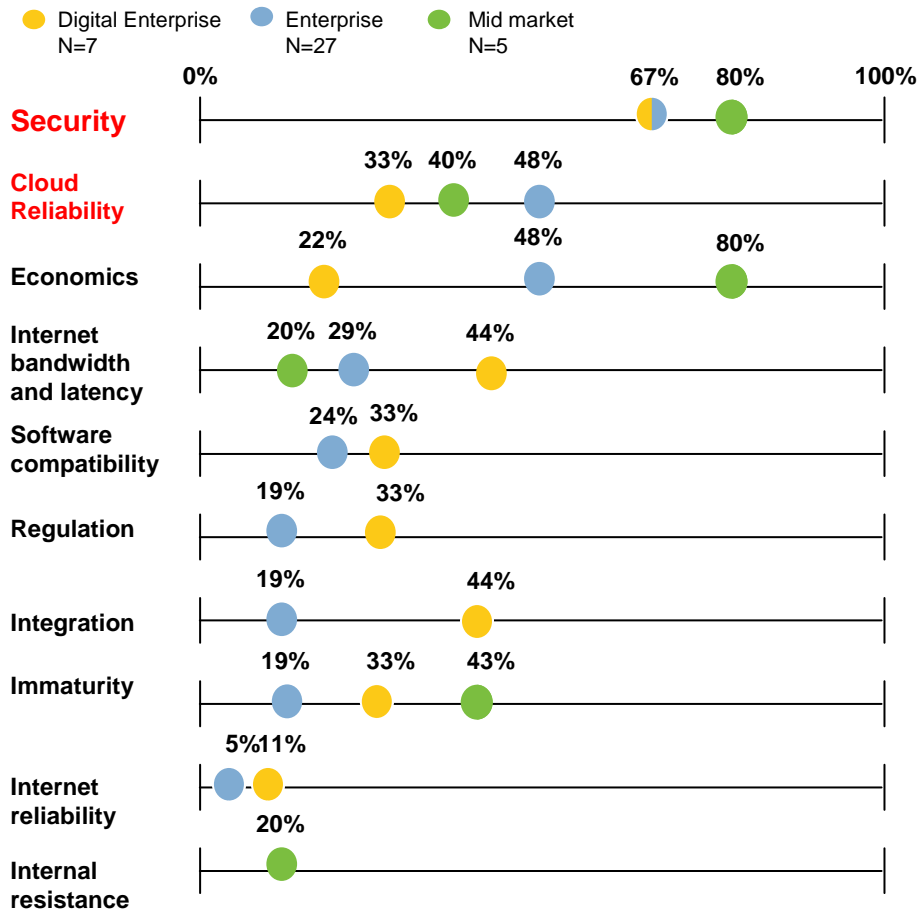
Complying with SOX, HIPPA and other **regulations may prohibit** the use of clouds for some applications. Comprehensive auditing capabilities are essential.

Security Management

Providers must supply easy, visual controls to **manage firewall and security settings** for applications and runtime environments in the cloud.

Customers are perceptive to these risks

Security, Reliability and Economics are the most common concerns with the cloud.



- **Security** is usually the **#1 concern** for any new IT solution, but the additional “external” aspects of the cloud exacerbate this concern
- Customers were mostly concerned about the data security and the reliability of cloud computing in practice
- Large enterprises resonated with the concept of Enterprise Cloud which was considered to be more secure than any external solutions.

Customer quotes on cloud security

“Security will be a big big big issue! If we see it as a warehouse of data, how can you avoid mistakes like sending wrong information to the wrong recipient?”

“How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to **control its employees from stealing** data?”

“It is **not likely that the management will feel comfortable** to keep strategic data such as sales and other financial data outside the company”

“Security is the biggest concern. I don’t worry much about the other “-ities” – reliability, availability, etc.”

“If users are sharing the same platform and used by multiple users, **it is possible that our data will be hacked?**”

“I prefer internal cloud to IaaS. When the service is kept internally, I am more comfortable with the security that it offers.”

The issue of Trust arises in the cloud computing space – centered on how to ensure corporate security and privacy concerns as well as overall brand trustworthiness.

Cloud computing also provides the opportunity to simplify security controls and defenses

People and Identity	<ul style="list-style-type: none">▪ Centralized Identity and Access Control policies▪ Well-defined set of input/output interfaces▪ Consistent enrollment, proofing, validation and management of a trusted user
Information and Data	<ul style="list-style-type: none">▪ Computing services running in isolated domains as defined in service catalogs▪ Default encryption of data in motion & at rest▪ Virtualized storage providing better inventory, control, and tracking of master data
Process & Application	<ul style="list-style-type: none">▪ Autonomous security policies and procedures▪ Personnel and tools with specialized knowledge of the cloud ecosystem▪ SLA-backed availability and confidentiality
Network Server and Endpoint	<ul style="list-style-type: none">▪ Automated provisioning and reclamation of hardened runtime images▪ Dynamic allocation of pooled resources to mission-oriented resources▪ Simplified, built-in security controls
Physical infrastructure	<ul style="list-style-type: none">▪ Closer coupling of systems for management of physical and logical identity/access▪ Strong platform of compute resources with integrated workload-balancing and resiliency▪ Highly-fortified physical data centers



Critical Domain areas

- **15 Domain areas impact Cloud security**
 1. Cloud Computing Architectural Framework
 2. Governance & Enterprise Risk Management
 3. Legal
 4. Electronic Discovery
 5. Compliance & Audit
 6. Information Lifecycle Management
 7. Portability & Interoperability
 8. Traditional security, Business Continuity & Disaster Recovery



Critical Domain areas – Contd.

9. Data Center Operations
10. Incident Response, Notification & Remediation
11. Application Security
12. Encryption & Key Management
13. Identity & Access Management
14. Storage
15. Virtualization

Domain 1 – Architectural Framework

- Abstraction of infrastructure
 - Server, Network & Storage infra is not visible to the customer/user
- Resource Democratization
 - Pooled resources available to anyone/anything authorized using standardized methods
- Service Oriented Architecture
 - Well defined & loosely coupled components with service delivery focus
- Elasticity / Dynamism of resources
 - On demand, self service model enables rapid increase or decrease in computing capacities
- Utility model of consumption & allocation
 - “Pay as you go”, metered, utility-cost usage model

Domain 2 – Governance & Enterprise Risk Management

- Perform thorough Due Diligence of CC provider
- Check financial viability of the CC provider
- Part of savings from CC services to invest in increased scrutiny of security capabilities of CC provider
- Ongoing risk management due to dynamic relationship
- Check all policies, procedures & processes for CC providers' Information Security Management System
- Conduct regular 3P risk assessments
- Monitor & measure CC provider's key risk & performance metrics
- Listing of all 3P relationships of CC provider

Domain 3 – Legal



- Contract is the key legal enforcement mechanism & must reflect customer's unique needs & dynamic nature of CC
- Plan for expected & unexpected termination of CC contract & orderly return + secure disposal of customer assets
- Do Due Diligence & mitigate conflicts in laws applicable for CC provider & CC customer.
- Add clauses in contract to monitor adherence to SLA's
- Add clauses in contract to ensure CC provider's response to legal requests for info
- Add clauses in contract to prohibit secondary use of data by CC provider
- Add clauses in contract to prohibit cross-border data transfers, if necessary

Domain 4 – Electronic Discovery

- Remember, data on cloud is owned by customer & CC provider also has a fiduciary responsibility
- CC model presents challenge to customer's control of data within their legal responsibility
- Clarity of Roles & Responsibilities w.r.t electronic discovery
- IT Sec systems of CC provider tailored to preserve authenticity & reliability of data including primary info, metadata, log files & related information
- Records & Information management domain knowledge to adapt to CC

Domain 5 – Compliance & Audit

- Customer to maintain a right to audit to meet regulatory mandates & business needs
- Perform external risk assessments including Privacy impact assessment
- Classify data & systems to meet compliance requirements
- Greater uniformity in scope of SAS70 & ISO 27001 requirements to increase security assurance & avoid adhoc audits & reduce CC provider's productivity

Domain 6 – Information Lifecycle Management

- Review CC provider's policies for data retention & destruction & compare with internal organizational policy. Mitigate gaps. Data retention is easy to demonstrate, data destruction is very difficult to demonstrate
- Negotiate penalties for data breaches – best option is to recover fully the breach costs from CC contract; alternatively use de-risking options like insurance etc.,
- Perform regular backup & recovery tests to ensure effective logical segregation controls
- Ensure logical Separation of duties for CC provider personnel

Domain 7 – Portability & Interoperability



- Advocate open standards, especially in Application development
- Review capabilities of competitors to CC provider & their migration assistance skills
- Be clear on distinctions between SaaS, PaaS & IaaS to accurately assess portability & interoperability risks
- For SaaS, perform regular data extractions and backups to a format that is usable and not proprietary to the SaaS provider.
- For IaaS, deploy applications in runtime in a way that is abstracted from the machine image. Backups should also be machine independent.
- For PaaS, select application techniques to minimize potential lock in with CC provider using portability as a key design goal & an architecture supporting necessary abstraction layers to achieve goal of portability

Domain 8 – Physical Security, BC & DR

- CC provider to adopt as Security baseline, the most stringent requirements of any customer
- High degree of insider risk due to centralization of data
- Separation of Duties & Compartmentalization of job roles & limit knowledge of customers on need to know basis
- Identify & mitigate physical interdependencies in CC provider's infrastructure
- Customers should conduct onsite inspection of facilities of CC provider
- Review DR & BC plans of CC provider

Domain 9 – Data Center Operations

- Review how the 5 characteristics of CC & technology architecture & infra impacts ability to meet SLA's
- Review BC & DR plans from IT perspective for people & processes. Check for new & unproven methods in CC IT architecture. Cover in customer's BC & DR plans to mitigate impact
- CC provider must demonstrate comprehensive compartmentalization of systems, networks, management, provisioning & personnel
- Review how resource democratization impacts system availability & performance during business fluctuations
- For IaaS & PaaS, review CC providers patch management policies & procedures & their impact on the applications developed for the CC environment. Add specific requirements into the contract
- Test CC providers customer service function to determine effective level of support contracted

Domain 10 – Incident Response, Notification & Remediation

- Sensitive & Private data should be encrypted at rest & move. Specify encryption requirements in contract (Algorithm, Key length & Key management)
- Review policies & procedures of Security Ops center to ensure correct fit for multi-tenant cloud scenarios
- Review application layer logging frameworks to ensure granular narrowing of incidents for specific customer
- Ensure application level firewalls, proxies & application logging tools exist to assist in quick incident response in multi tenant environment
- CC provider must maintain registry of application owners by application interface (URL, SOA service etc.,)
- CC provider & customers need defined processes to ensure clear roles & responsibilities for incident handling, response & remediation to reduce service downtimes

Domain 11 – Application Security

- IaaS, PaaS & SaaS create differing trust boundaries in SDLC & handled appropriately during development, testing & production phases
- Apply the best practices to harden hosts with DMZ to Virtual Machines. Limit services to only support the application stack
- Secure inter host communications
- Manage & protect application “secret keys”

Domain 12 – Encryption & Key Management




- From a Risk Management standpoint, unencrypted data is considered “Lost” in a cloud
- Applications must store data in encrypted form at the backend
- Use encryption to separate data holding from data usage
- Segregate key management from CC provider with chain of separation. This protects both CC provider & customer during a legal mandate to provide data
- Ensure the encryption standards specified in the contract adhere to industry / government standards

Domain 13 – Identity & Access Management



- Key factor for success in managing identities is to have a robust & decentralized identity management structure & strategy
- Review whether CC provider's Identity, Authentication & Password policies meet or exceed customer's relevant policies
- Ensure that granular application authorization for CC providers is either proprietary or non-existent.
- Implement "Single Sign On" for internal applications & leverage this in cloud applications



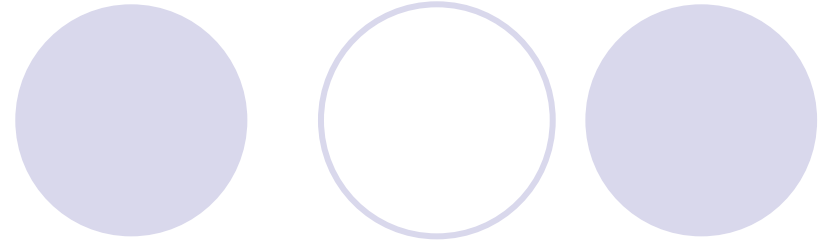
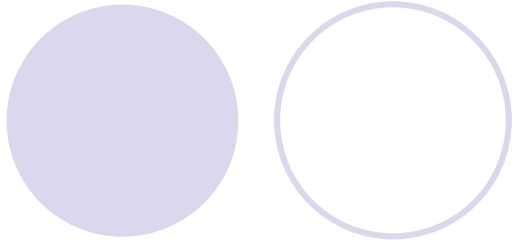
Domain 14 – Storage

- Ensure that storage subsystem does not span domain trust boundaries
- Review the controls for storage provisioning to partition multiple customer data
- Understand the CC provider's data search capabilities
- Find out the geographical location of storage
- Review CC provider's storage retirement processes - data destruction in multi tenant environment
- Ascertain circumstances under which storage can be seized by 3P or Govt. entity
- Ascertain how encryption is handled on multi tenant storage – single key /one key per customer/multiple keys per customer?
- Can CC provider support long term archiving, will data be available several years later, will decryption & associated technologies still be useable?



Domain 15 – Virtualization

- Use 3P Security on Virtualized OS to create layered controls
- Insecure images created during provisioning -
Use secure & standard configurations exceeding industry baselines
- Admin access & control of Virtualized OS -
Use strong authentication coupled with enterprise identity mgt, tamper proof logging & integrity monitoring controls



References

- www.ibm.com
- www.cloudsecurityalliance.org
- www.gartner.com
- www.idc.com



Q & A