Pulse Comes to You 2012

Business without **LIMITS**

Aug 2012 | Bangkok, Hanoi

IBM Cloud Security

Collin Penman

Business Unit Executive
IBM Security Systems

Cloud solutions accelerate the delivery of new business value and fundamentally change the economics of IT

Tops Concerns for Cloud Adoption

80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

33%

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"**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?"*

*"**Security is the biggest concern.** I don't worry much about the other "-ities" – reliability, availability, etc."*

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

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

Specific Customer Concerns Related to Security

Protection of intellectual property and data	**30%**
Ability to enforce regulatory or contractual obligations	**21%**
Unauthorized use of data	**15%**
Confidentiality of data	**12%**
Availability of data	**9%**
Integrity of data	**8%**
Ability to test or audit a provider's environment	**6%**
Other	**3%**

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

Cloud computing tests the limits of security operations and infrastructure

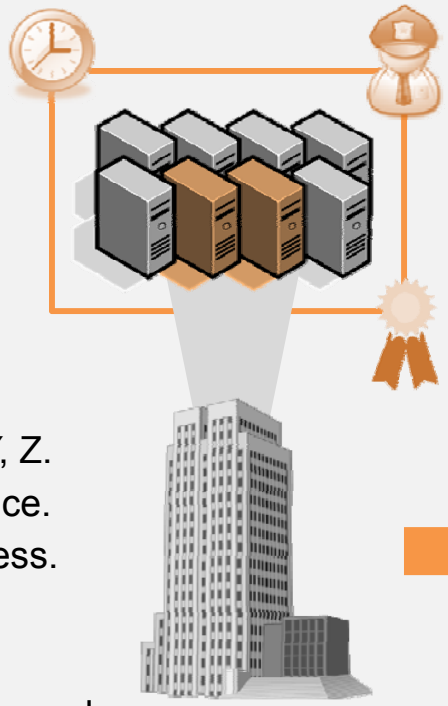
Security and Privacy Domains		To cloud
People and Identity	Self-Service	Multiple Logins, Onboarding Issues
Data and Information	Highly Virtualized	Multi-tenancy, Data Separation
Application and Process	Location Independence	External Facing, Quick Provisioning
Network, Server and Endpoint	Workload Automation	Virtualization, Network Isolation
Physical Infrastructure	Rapid Elasticity	Provider Controlled, Lack of Visibility
Governance, Risk and Compliance	Standardization	Audit Silos, Compliance Controls

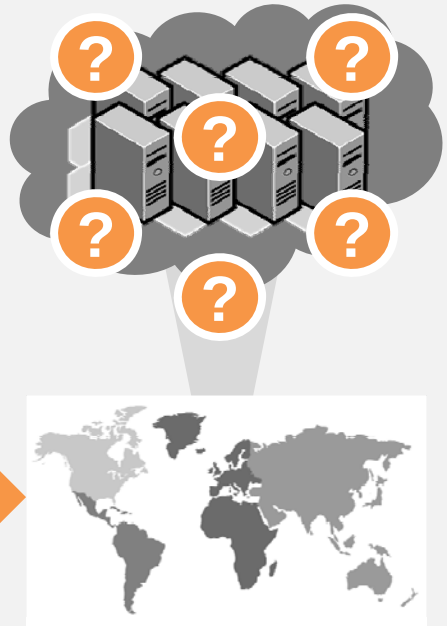
In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resources and applications increases - **greatly affecting all aspects of IT security**.

Simple Example

Today's Data Center

Tomorrow's Public Cloud





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?

Attributes and Benefits of Cloud Computing

VIRTUALIZATION

AUTOMATION

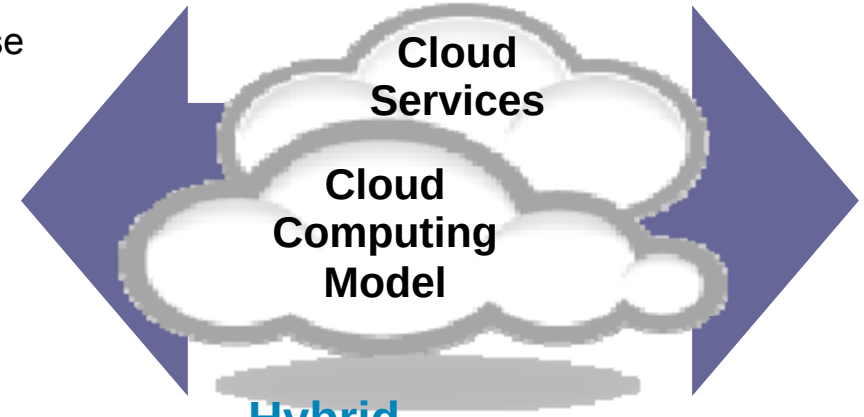
STANDARDIZATION

Attributes	Characteristics	Benefits
Advanced virtualization	IT resources can be shared between many applications. Applications can run virtually anywhere.	Providing more efficient utilization of IT resources. Reducing hardware cost through economy of scale
Automated provisioning	IT resources are rapidly provisioned or de-provisioned on demand.	Reducing IT cycle time (real-time provisioning) and management cost
Elastic scaling	IT environments scale down and up by large factors as the need changes.	Optimizing IT resources utilization Increasing flexibility
Service catalog ordering	Defined environments can be ordered from a catalog.	Enabling self-service, consumer concerns are abstracted from provider concerns through service interfaces
Metering and billing Flexible pricing	Services are tracked with usage metrics to enable multiple payment models.	Improving cost transparency Offering more flexible pricing schemes
Internet Access	Services are delivered through use of Internet.	Access anywhere, anytime

Cloud Computing Delivery Models

Private …

- Access limited to enterprise and its partner network
- Dedicated resources
- Single tenant
- Drives efficiency, standardization and best practices while retaining greater customization and control
- Might be managed or hosted by third party



Hybrid …

- Private infrastructure, integrated with public cloud

Public …

- Access open to everybody, subject to subscription
- Shared resources
- Multiple tenants
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis
- Always managed and hosted by 3rd party

Customization, efficiency, availability, resiliency, security and privacy …

Standardization, capital preservation, flexibility and time to deploy …

Categories of Cloud Computing Risk

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

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 regulations may prohibit the use of clouds for some applications.

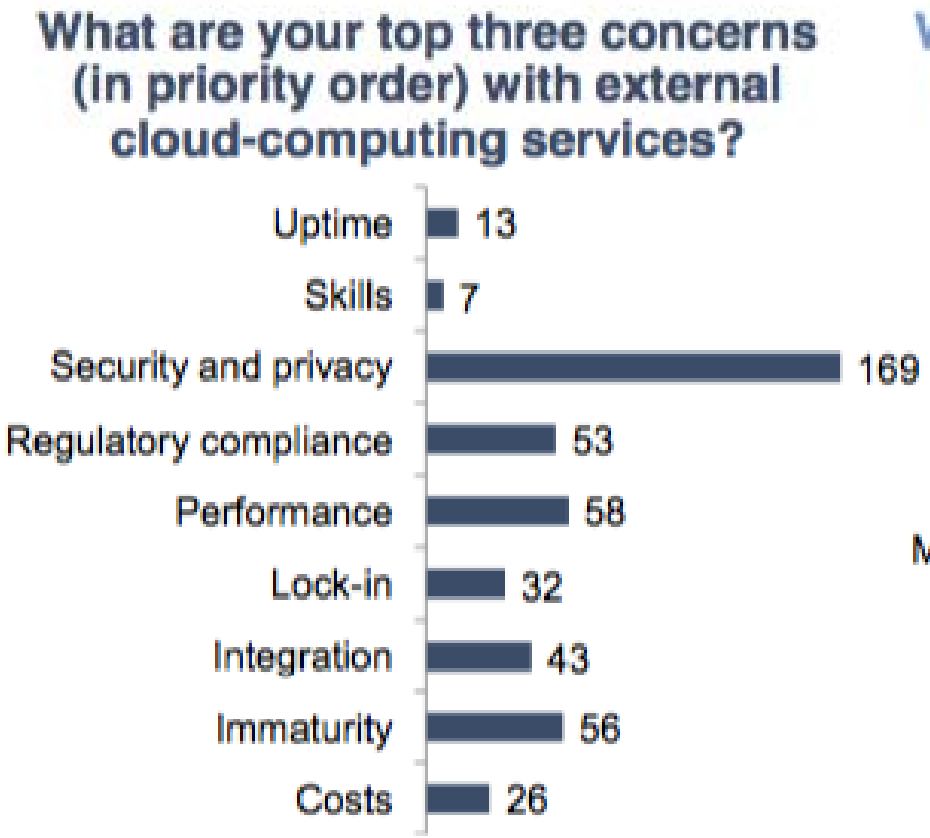
Comprehensive auditing capabilities are essential.

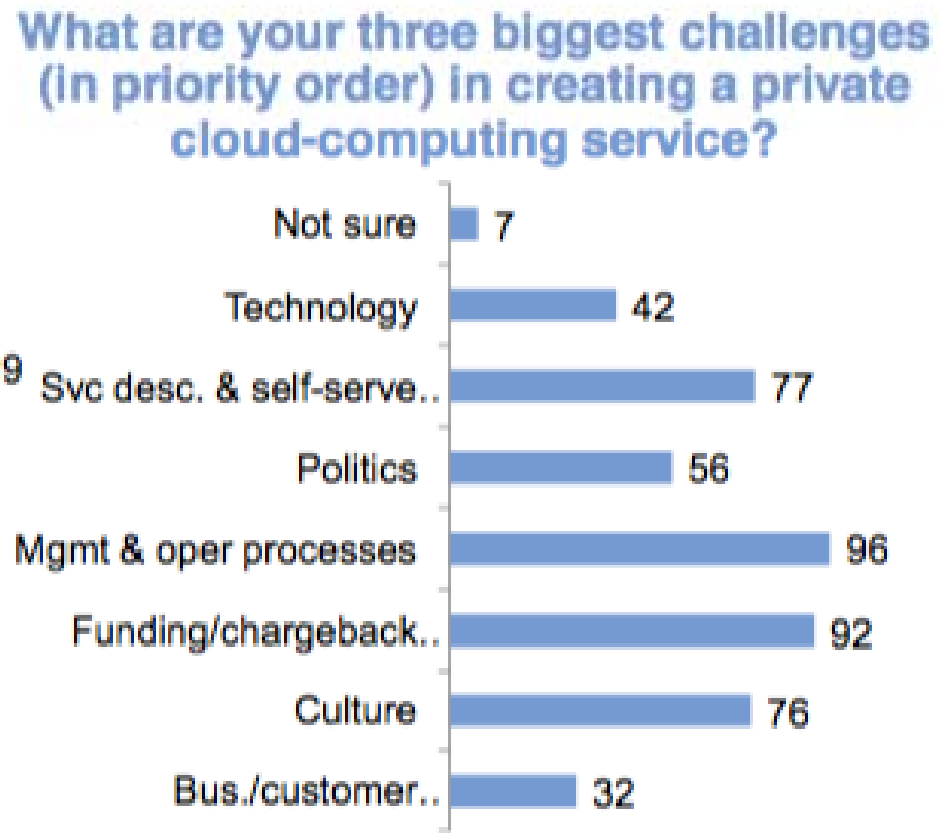
Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

Providers must supply easy controls to manage security settings for application and runtime environments.

Use your Private Cloud as a Test-bed for Public Cloud





Pulse Comes to You 2012

Business without **LIMITS**

IBM Point of View: Cloud CAN be Secure.

As with most new technology paradigms, **security concerns surrounding cloud computing** have become the most widely talked about inhibitor of widespread usage.

To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

The same way transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.

Different cloud deployment models also change the way we think about security

Private cloud

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party

Hybrid IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability

Public cloud

Available to the general public or a large industry group and owned by an organization selling cloud services.

Changes in Security and Privacy

- *Customer responsibility for infrastructure*
- *More customization of security controls*
- *Good visibility into day-to-day operations*
- *Easy to access to logs and policies*
- *Applications and data remain "inside the firewall"*

- *Provider responsibility for infrastructure*
- *Less customization of security controls*
- *No visibility into day-to-day operations*
- *Difficult to access to logs and policies*
- *Applications and data are publically exposed*

Each pattern has it own set of security concerns

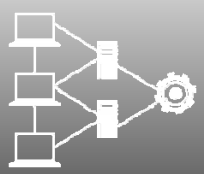
Infrastructure as a Service (IaaS): Cut IT expense and complexity through cloud data centers

Platform-as-a-Service (PaaS): Accelerate time to market with cloud platform services

Innovate business models by becoming a cloud service provider

Software as a Service (SaaS): Gain immediate access with business solutions on cloud

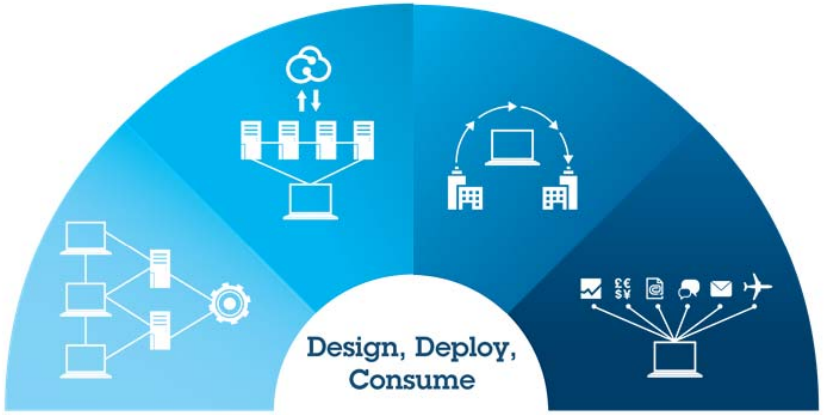
Cloud Enabled Data Center	Cloud Platform Services	Cloud Service Provider	Business Solutions on Cloud
Integrated service management, automation, provisioning, self service	*Pre-built, pre-integrated IT infrastructures tuned to application-specific needs*	*Advanced platform for creating, managing, and monetizing cloud services*	*Capabilities provided to consumers for using a provider's applications*
Key security focus: **Infrastructure and Identity**	Key security focus: **Applications and Data**	Key security focus: **Data and Compliance**	Key security focus: **Compliance and Governance**
▪ Manage datacenter identities ▪ Secure virtual machines ▪ Patch default images ▪ Monitor logs on all resources ▪ Network isolation	▪ Secure shared databases ▪ Encrypt private information ▪ Build secure applications ▪ Keep an audit trail ▪ Integrate existing security	▪ Isolate cloud tenants ▪ Policy and regulations ▪ Manage security operations ▪ Build compliant data centers ▪ Offer backup and resiliency	▪ Harden exposed applications ▪ Securely federate identity ▪ Deploy access controls ▪ Encrypt communications ▪ Manage application policies



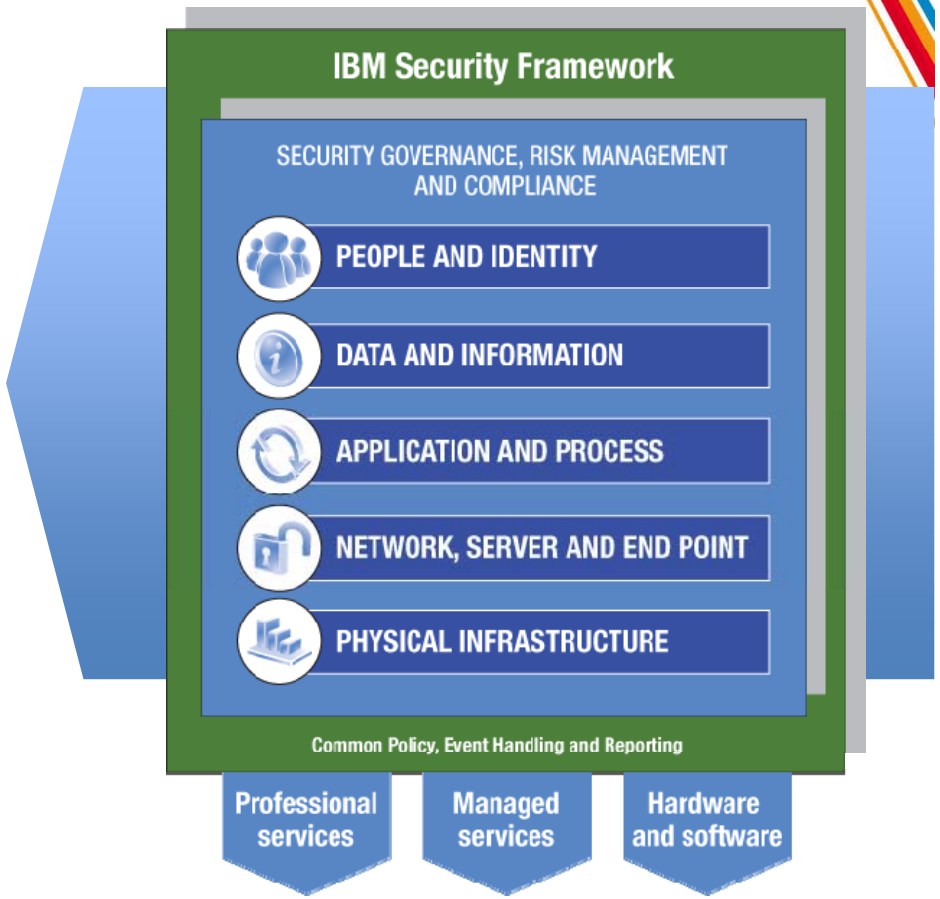
IBM Security Framework – Mapping into Cloud Security

IBM Cloud Security

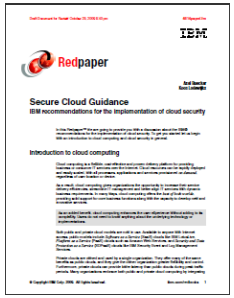
One Size Does Not Fit All



Different security controls are appropriate for different cloud needs - the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.



IBM Security Framework



IBM Cloud Security Guidance Document

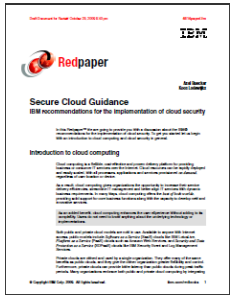
Network, Server and End Point

Customers expect a **secure** cloud **operating environment**.

Maintain environment testing and vulnerability/intrusion management

- Implement vulnerability scanning, anti-virus, intrusion detection and prevention on all appropriate images
- Ensure isolation exists between tenant domains
- Trusted virtual domains: policy-based security zones
- A secure application testing program should be implemented.
- Develop all Web based applications using secure coding guidelines.
- Ensure external facing Web applications are black box tested

IBM Security Framework



IBM Cloud Security Guidance Document

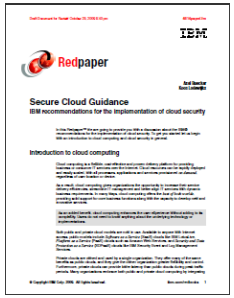
People and Identity

Customers require **proper authentication** of cloud users.

Implement strong identity and access management

- Implement least privilege model for user's access
- Strong Identity lifecycle management
- All administrative access over secure channels
- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems
- A standards-based, single sign-on capability

IBM Security Framework



IBM Cloud Security Guidance Document

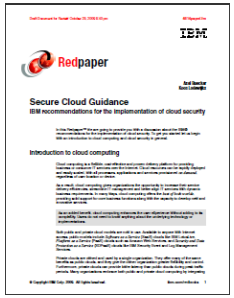
Application and Process

Customers require **secure cloud applications** and **provider processes**.

Establish application and environment provisioning

- Implement a program for application and image provisioning.
- Ensure provisioning management is strictly controlled
- Protect machine images from corruption and abuse
- Ensure all changes to virtual images and applications are logged.
- Ensure provisioned images apply appropriate access rights
- Ensure destruction of outdated images

IBM Security Framework



IBM Cloud Security Guidance Document

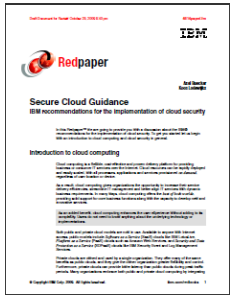
Data and Information

Customers cite **data protection** as their **most important** concern.

Ensure confidential data protection

- Protect PII and Intellectual Property
- Implement a secure key management program
- Use a secure network protocol when connecting to a secure information store.
- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.
- Sensitive information not essential to the business should be securely destroyed.

IBM Security Framework



IBM Cloud Security Guidance Document

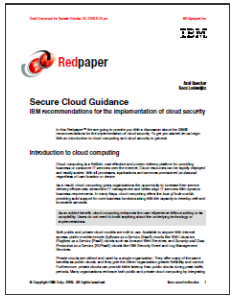
Physical Security

Customers expect **cloud data centers** to be **physically secure**.

Implement a physical environment security plan

- Ensure the facility has appropriate controls to monitor access.
- Prevent unauthorized entrance to critical areas within facilities e.g. servers, routers, storage, power supplies
- Biometric access of employees
- Ensure that all employees with direct access to systems have full background checks.
- Provide adequate protection against natural disasters.

IBM Security Framework



IBM Cloud Security Guidance Document

Security governance, risk management and compliance

Customers require **visibility** into the security posture of their cloud.

Implement a governance and audit management program

- Establish 3rd-party audits (ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Create policies for PII and for data crossing International boundaries
- Understand applicable regional, national and international laws
- Support for forensics and e-Discovery

IBM Providing Cloud Leadership

LIMITS

Summary

- “Cloud” is a new consumption and delivery model inspired by consumer Internet services.
- Security Remains the Top Concern for Cloud Adoption
- One sized security doesn’t fit all
- Take a structured approach to securing your cloud environment
- Documented guidance is available for download to assist you in securing your cloud environment

Pulse Comes to You 2012

Business without **LIMITS**

Thank You