Cloud and Regulations:  
A match made in heaven, or the worst blind date ever?

Vinod S Chavan  
Director – Industry Cloud Solutions,  
IBM Cloud  
October 28, 2015
Customers are faced with challenge of balancing innovation and risk

1. Cloud creates opportunities for enhanced security

2. Cloud security is a shared responsibility between customers and Cloud providers
Traditional perimeter-based security controls …
Traditional perimeter-based security controls ...  
... are changing to security centered around applications and data
Challenge: Adapt our understanding of risk management to allow adoption of secure, compliant, business friendly cloud

<table>
<thead>
<tr>
<th>Perceived “Biggest Risks”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software as a Service (SaaS)</strong></td>
</tr>
<tr>
<td>▪ SaaS provider doesn’t have adequate (up to “my” standards) practices around data protection, identity management, intrusion protection</td>
</tr>
<tr>
<td>▪ <em>Focused on risks of “managed by other” and not enough on security basics for integrating with other providers and solutions</em></td>
</tr>
<tr>
<td><strong>Platform as a Service (PaaS)</strong></td>
</tr>
<tr>
<td>▪ PaaS provider won’t have the same types of basic controls (up to “my” standards) that I need for my developers in my environment</td>
</tr>
<tr>
<td>▪ <em>Focused on what the developer will do when removed from the training wheels of internal IT controls (developers let lose on the Internet!)</em></td>
</tr>
<tr>
<td><strong>Infrastructure as a Service (IaaS)</strong></td>
</tr>
<tr>
<td>▪ IaaS provider doesn’t have adequate (up to “my” standards) practices around physical security</td>
</tr>
<tr>
<td>▪ <em>Tends to think in context of a traditional data center with physical cages</em></td>
</tr>
</tbody>
</table>
We see three sets of security capabilities to help enterprise clients:

- **Identity**: Manage identities and govern user access
- **Protection**: Protect infrastructure, applications, and data from threats
- **Insight**: Auditable intelligence on cloud access, activity, cost and compliance

**Cloud Security Capabilities**

- **SaaS**: Secure usage of business applications

  - Kenexa
  - Google
  - Workday
  - Salesforce
  - Dropbox

- **PaaS**: Secure service composition and apps

  - Bluemix
  - Windows Azure
  - force.com

- **IaaS**: Securing infrastructure and workloads

  - SoftLayer
  - openstack
  - VMware
  - Amazon Web Services
## Top 10 Things You Should Know

| Cloud Adoption | 1. Cloud environments can use the same security tools, policies, and procedures as traditional IT to satisfy the compliance requirements of Cloud hosted applications and workloads |
| Security concerns | 2. Leverage cloud provider’s APIs and logs for complete visibility into your cloud environment  
3. Identity: manage your users to identity lifecycle best practices  
4. Protection: leverage IaaS/PaaS structure to move to a High Availability == Disaster Recovery == Business Continuity architecture  
5. Insight: use move to cloud as a means to improve your overall IT asset management: know where your servers and what they are doing at all times |
| Compliance concerns | 6. Adopt “composite compliance” thinking in your organization  
7. Learn how to use an IaaS/PaaS SOC2 or ISO27001/2 certification as basis for your workload compliance assertions  
8. Learn how to evaluate SaaS security and compliance |
| Cyber Security | 9. TRUE/FALSE: “It is harder for me to detect and respond to attacks in a Cloud environment  
10. TRUE/FALSE: “Cloud is LESS secure than my traditional IT environment
Cloud environments can use the same security tools, policies, and procedures as traditional IT to satisfy the compliance requirements of Cloud hosted applications and workloads.

**Identity**

SAME: Continue to act as authoritative source of user status, privileges:
ADD: push user status, including employment status and privileges to provider

**Protection**

SAME: Deploy protective tools (IDS, AV, Firewalls, etc) in cloud provisioned environment following same best practices as in a traditional environment
OPTIONALLY: Use cloud provided or BYO solutions

**Insight**

SAME: Maintain on-premises SIEM systems for insight on environment
ADD: Pull cloud provider information including authentication logs, device status from cloud for additional insight on your entire environment

Existing tools may need to be adapted (deployed as virtual tools or used as SaaS) but assuming you are already following best practices, you shouldn’t have to develop new best practices.
What Changes? (Compliance Handled by Multiple Parties)

- SoftLayer is compliant with major industry and regulatory standards

**SoftLayer Manages To:**
- **US NIST SP800-53 standard**
- **EU Model Clauses**

**SoftLayer Compliance Demonstrated Through (~):**
- **PCI DSS v3.0 AOC for Physical Security**
- **EU Data Privacy**

**Supported Workloads Include**
- **PCI Security Standards Council**
- **EUROSYSTÈME**
- **FFIEC**
- **DHHS**
- **FDA**
- **European Commission**
- **GxP Compliant Cloud**

**Targeted for 2015**
- **GCC – GxP Compliant Cloud**
- **ATO from FCC**

- So a list of shiny stickers is great, how do I use this given that I have to demonstrate compliance for my workload?
- → **ENTER COMPOSITE COMPLIANCE**
Composite Compliance leverages the compliance of Cloud providers as part of workload compliance

- Composite compliance is the means by which we demonstrate security and compliance of a cloud hosted workload by building on and trusting the security and compliance of underlying levels
  1. Client uses the third-party audit assertions provided by their service provider as the basis for demonstrating overall compliance of the environment hosting a service-provider hosted client workload
  2. Client then adds additional information from their hosted workload and its management to demonstrate security and compliance of the configuration and operational management of the client’s IaaS/PaaS hosted workload
    - Typically a SaaS provider will own the entire compliance stack and will provide you with the appropriate audit reports and compliance certifications

- Cloud providers perform extensive audit and compliance examinations of the controls (policies, processes, procedures) used to security their cloud-provided infrastructure
  - This is true whether cloud is IaaS, PaaS, SaaS
- Cloud customers build their cloud-hosted application’s compliance statements on the foundation of cloud provider’s compliance statements
Composite compliance: Making a bigger, better cake metaphor

- Transitive trust is the means by which we do most cryptographic relationships
  - Provides guidelines that allow building blocks to work together
  - “Secret sauce” is evidence that trust is deserved
- Composite compliance: emerging approach for cloud
  - Provides guidelines for making bigger building blocks out of smaller starter-set building blocks
  - “Secret sauce” is evidence that composition doesn’t change individual characteristics
    - Critical to this evidence are clear boundaries and communications between A, B

<table>
<thead>
<tr>
<th>Transitive Trust</th>
<th>Composite Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice Trusts Bob</td>
<td>Chocolate cake</td>
</tr>
<tr>
<td>Bob Trusts Carol</td>
<td>Vanilla Cake</td>
</tr>
<tr>
<td>Means that because of Transitive Trust Alice Trusts Carol</td>
<td>Means that with Composition (proper combination) Vanilla Cake layered with Chocolate Cake is also a cake</td>
</tr>
</tbody>
</table>
Composite Compliance – Finding the common ground and work with the incremental requirements

Security Control:

All users are required to change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords.

Regulations and Standards:

- HIPAA's Security Rule: 42 administrative, physical, and technical safeguard requirements
- PCI Standard: 12 high-level requirements with approximately 212 detailed requirements
- The U.S. Federal Information Security Management Act of 2002: 17 areas of security requirements, each of which references controls from the National Institute of Standards and Technology's 800-53 Special Publication
- CobiT: Four domains, 34 high-level objectives, and 318 control objectives
- GLBA and the Federal Financial Institutions Examination Council's interagency guidelines: Seven high-level requirements, each of which comprises numerous detailed requirements

Mappings:

- ISO 17799:2005 > Access Control > User Responsibilities > Password Use (11.03.01)
- COBIT 3rd Edition > Delivery & Support > Ensure Systems Security > User Control of User Accounts (DS5.6)
- PCI Data Security Standard 1.0 December 15 2004 > Implement Strong Access Control Measures > Restrict data access by need-to-know (PCI Requirement 7)

Mapping a user authentication control to ISO 17799:2005, CobiT, and PCI requirements

Automation of the compliance processes provides:

- Eliminate human errors
- Common base across multitude of regulations
- Centralization of compliance information,
- Manage third-party risks more effectively
- Risk management decisions based on real-time information,
- An increased confidence in the company's security compliance posture.
- Workflow capabilities to assist in managing all aspects of compliance, including self-assessments, control analyses, corrective action planning and management, and controls testing.
How to use CSP’s compliance assertions

Customers use SOC1, SOC2 audit reports and ISO27001 certification to provide evidence for physical and environmental security controls required for their workload.

Customer uses additional requirements, such as signing of EU Model Clauses and Data Protection Acts to provide contractual obligation and evidence of regionally required controls.
Cloud is as secure as you make it...

10. TRUE/FALSE: “Cloud is LESS secure than my traditional IT environment. This is TRUE if you do not apply the same discipline to your users as they move to cloud (HINT: allowing users with little to no operational management experience to stand up Internet facing servers is a recipe for disaster).

Cloud IS LESS SECURE if
- You allow developers to order their own servers and retain full responsibility for their security configuration and management
- You leave your environment as Internet-facing and unprotected while you are in the process of configuring that environment/servers

Cloud is NO MORE OR LESS secure IF
- You impose discipline on your users in a Dev/Ops world
- You employ the same types of controls for your cloud applications as your traditional applications (firewalls, gateways, intrusion protection, anti-virus, strong authentication, logging and monitoring, etc)

Cloud is MORE secure IF
- You use this opportunity to reinforce discipline within traditional environment and close gaps that may have been raised during Cloud readiness reviews
Cloud presents the opportunity to radically transform security practices and adopt new approaches to workload compliance.

**IBM Point of View:**

*Cloud compliance allows us to rethink risks based on the comprehensive hybrid cloud and transitive compliance*

**Traditional Compliance**
Client dictated and driven control of risks for end-to-end operational stack

**Dynamic Cloud Compliance**
Compliance statements provided by each layer build up an end-to-end compliance statement

**Traditional Security**
Manual, static, and reactive

**Dynamic Cloud Security**
Standardized, automated, agile, and elastic

**IBM Point of View:**

*Cloud security is not only achievable, it is an opportunity to drive the business, improve defenses and reduce risk*