Key Considerations of Regulatory Compliance in the Public Cloud

W. Noel Haskins-Hafer
CRMA, CISA, CISM, CFE, CGEIT, CRISC
10 April, 2013
w_haskins-hafer@intuit.com

Disclaimer

Unless otherwise specified, the views expressed in this presentation are my own, and not those of any other individual or individuals connected with my current or former employers.

All names, logos, and other outside material attributed to other sources remains the property of their respective copyright owners and are used here in accordance with the Fair Use doctrine.
Agenda

- Speaker Qualifications
- Setting the Stage
- The Regulatory Environment
- Considerations for Compliance in the Cloud

Speaker Qualifications

- Compliance Program Manager for Intuit Financial Services Product Development
  - Formerly with Intuit’s Computer Information Security and Internal Audit Teams
  - Manager, Enterprise Risk Services (Deloitte & Touche, LLP)
- Member of BITS Cloud Computing and Data Governance SIGs
- Charter member of CSA’s Financial Services SIG
- ISACA-SD CGEIT and CRISC Coordinator
- ISACA International’s review committee member for certification study materials and COBIT 5 framework
The Challenge

- Regulatory Environment
- Business
- Cloud Computing

Many Industries are Regulated

- Bank
- Drugstore
- Casino
- Tax
- Shopping Cart
Most Participants are also Businesses

- Accounting
- Finance
- Human Resources
- Information Technology Service Delivery
- Legal
- Sales and Marketing

A Typical Simplified Supply Chain
Common Goals for the Cloud

- Simplify IT operations
  - Infrastructure, platform and software
- Increase agility
- Save money
  - Transfer capex to opex
- Improve global operations service delivery
- Focus on core business

All While Maintaining Legal & Regulatory Compliance

The NIST Cloud Definition Framework

<table>
<thead>
<tr>
<th>Deployment Models</th>
<th>Service Models</th>
<th>Essential Characteristics</th>
<th>Common Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>Software as a Service (SaaS)</td>
<td>On Demand Self-Service</td>
<td>Massive Scale</td>
</tr>
<tr>
<td>Community Cloud</td>
<td>Platform as a Service (PaaS)</td>
<td>Rapid Elasticity</td>
<td>Resilient Computing</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>Infrastructure as a Service (IaaS)</td>
<td>Measured Service</td>
<td>Geographic Distribution</td>
</tr>
</tbody>
</table>

From NIST's *Effectively and Securely Using the Cloud Computing Paradigm* (Presentation Oct 7, 2009)
The Essence of Cloud Computing

“Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.”


Accountability in the Cloud Is...

- Customer satisfaction
- Data integrity and reliability
- Increased partnership throughout the supply chain
- Inherited 3rd party controls over operations
- Lower visibility into operations
- Regulatory compliance
Let’s Keep Things Simple

Banking Industry in 2013

- Evolving and uncertain regulatory environment
- Continued focus on risk management
  - Including infrastructure and risk strategy
- Expansion of products and services
- Expense management and restructuring
- Security and privacy risks
- Data integrity and data management

Protiviti FS Insights, February 2013
Banking Adoption of the Cloud

- Back-office functions
  - IaaS
    - Archive and Disaster Recovery
    - IT Management
    - Security as a Service
  - PaaS
    - Application development and testing
    - Web Server
  - SaaS
    - Analytics
    - Customer Relationship Management
    - Collaboration within the business

Very little core business adoption

Regs and Laws and Standards, Oh My!

- FFIEC
  - Federal Reserve
  - Office of the Comptroller of the Currency
  - National Credit Union Association
  - Federal Deposit Insurance Corporation
  - Consumer Financial Protection Board
- State Banking Regulators
- Federal Credit Reporting Agency
- Federal Trade Commission
But Wait… There’s More!

- Graham-Leach-Bliley Act
- US Patriot Act
- Bank Secrecy Act
- Bank Service Company Act
- Sarbanes-Oxley Act
- Fair and Accurate Credit Transactions Act
- Foreign Account Tax Compliance Act
- Americans with Disability Act
- Payment Card Industry Data Security Standard

…And even more if you’re doing business internationally

Let’s Not Forget…

- Company policies
- Operating principles
- Covenants and other company legal obligations
- Existing contracts with 3rd Parties
Add It All Together And…

What To Do?

Don’t Panic!
Stop, Think and Plan

- Identify the end goal
- Focus on what changes
- Follow a methodical process to
  - Understand the complexity of the environment
  - Analyze and assess inherent risks
  - Know who’s responsible for what
  - Develop an approach to address and manage risks
- Collaborate with SMEs
  - Internal and external (Cloud Service Provider (CSP) and other 3rd parties)

What Regulators Want

Assurance that management has identified, assessed, evaluated and addressed risks throughout the supply chain and that data is appropriately safeguarded

It’s Still About Risk Management
What Stays the Same

- What the customer sees and does
- The need to safeguard customer and end-user data
- Most of the internal business structure
- FFIEC Guidance

What Changes

- Technical architecture
  - Applications
  - Data
  - Security
  - Network
  - Identity management
- Data Governance
- Reliance on 3rd Parties
Technical Architecture

- Application independence from infrastructure
- Asset management
  - Infrastructure component ownership
  - Virtualization
- Server maintenance / patching
  - Who, what, and when
- Configuration management and drift

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Program Interface (API) or Graphical User Interface (GUI)</td>
<td>The interface used by the client or their customer to interact with the application. The current most common API is REST or HTTPS. The current most common GUI is an HTTP or HTTPS based Web site.</td>
</tr>
<tr>
<td>Application</td>
<td>The actual application being used by one or more clients or their customers.</td>
</tr>
<tr>
<td>Solution stack</td>
<td>This is the programming language used to build and deploy applications. Some examples include: .NET, Python, Ruby, Perl, etc.</td>
</tr>
<tr>
<td>Operating systems (OS)</td>
<td>In a virtualized environment, the OS runs within each VM. Alternatively, if there is no underlying hypervisor present, the operating system runs directly on the storage hardware.</td>
</tr>
<tr>
<td>Virtual machine (VM)</td>
<td>The virtual machine assigned for client use.</td>
</tr>
<tr>
<td>Virtual network infrastructure</td>
<td>For communications within and between virtual machines.</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>When virtualization is used to manage resources, the hypervisor is responsible for dividing resources to each virtual machine. It may also be developed for implementing security.</td>
</tr>
<tr>
<td>Processing and memory</td>
<td>The physical hardware that supplies CPU time and physical memory.</td>
</tr>
<tr>
<td>Data storage</td>
<td>The physical hardware used for data storage.</td>
</tr>
<tr>
<td>Network</td>
<td>This can be a physical or virtual network. It is responsible for carrying communications between systems and possibly the Internet.</td>
</tr>
<tr>
<td>Physical facility</td>
<td>The actual physical building where the cloud systems are located.</td>
</tr>
</tbody>
</table>

Information Supplement PCI CSS Cloud Computing Guidelines (Feb 2013)
Enterprise Security and Risk Framework for Cloud Contracts

- Credential management: Issuance of, access to, and end-user identities for access to virtual components and applications in the cloud
- Privilege management: Definition and assignment of resource access privileges and roles for cloud components and applications
- Authorization: Validation of identities (user, group, system, operation, and data) on the basis of cloud credentials
- Data assurance: Confidentiality, integrity, and availability of data at rest, in transit, and in use in a cloud environment
- System platform security: Maintaining the OS, hypervisors, VMs, application, database, and network servers
- Physical and virtual perimeter: Hardening of network perimeter against unauthorized access, penetration, and data exfiltration detection
- Monitoring, logging, auditing, reporting: Monitoring of infrastructure configuration, management events, and policy changes; security of the logging, auditing, and reporting environment
- Environment security: Protection and recoverability of physical infrastructure and system-level assets
- Policy security: Protections and controls over policy metadata and processes that define, enforce, and report on security operating environment and application-related aspects regardless of location
- Risk management framework: Framework and process for determining inherent risk, security controls, and residuals

Source: IDC Financial Insights, 2013
© IDC Financial Insights. Visit us at IDC.com
Additional Security Challenges

- Encryption and tokenization
- Key management
- Application security
- Network segmentation and traffic isolation
- Data flows between internal and public networks
- Operational and control responsibilities
- Authentication

Figure 3: Example of how PCI DSS responsibilities may be shared between clients and CSPs.
Identity and Access Management

- End users
- Customers
  - Product administrators
- Internal employees
- Cloud employees
  - CSP administrators
Data Governance Considerations

- Suitability for the cloud
- Classification and characteristics
- Location
- Usage rights
- Cloud exit strategy
- Retention and destruction

Suitability for the Cloud

- Type of application and transactions
- Type of data
- Legal requirements
- Street value of data
Data Classification and Characteristics

- Taxonomy
- Data element dependencies
- Data architecture and model
- Volume
- Data life cycle
- Data roles
  - Stewardship
  - Ownership
  - Custodian

Data Location

- Geographic location
  - Processing
  - Storage
  - Backups
  - Recovery
- Transmission path
- Segregation from CSP’s other clients’ data
- Segregation of transaction processing
- Segmentation and partitioning
Data Usage and Exit Strategy

- CSP data usage rights
- Investigation practices
  - Forensics
  - Legal investigations
  - Incident management response and processes
- Data exit strategy
  - End of contract
  - Cancellation of contract

Data Retention and Destruction

- Retention period and formats
- Return mechanisms and formats
- Disposal
  - Erasure / destruction of all copies
CSP and 3rd Party Considerations

- Viability and reliability
- Lock-in
- Transparency
- Technical capability
  - Capacity and storage
  - Processing power
  - Latency
- CSP’s downstream third parties

CSP Considerations, continued

- Cloud management and integration
  - Interoperability of enterprise and CSP tools
  - Maintenance schedules
  - Sufficient data and reporting to manage and monitor enterprise business
  - End-to-end incident response and management
- Audits
CSP Considerations, continued

- Privacy principles and data protection expectations
- Security measures and responsibilities
- Cloud asset and resource ownership
- Jurisdiction and legal compliance
  - Data movement and data storage
- Service Level Agreements
  - Recovery objectives and priorities
  - Acceptable actions to take for non-performance

Challenges Beyond CSP

- Software licensing
  - Terms relative to the cloud
  - License pricing
    - By seat
    - Peak vs non-peak usage
  - Growth projections and pricing
  - International restrictions
- User control considerations
- Separation of monitoring and application functions
It’s More than IT

**Governance**
- Governance and Enterprise Risk Management
- Third Party Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability

**Operational**
- Traditional Security, BCP & DR
- Data Center Operations
- Incident Management
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

Adapted from Cloud Security Alliance (CSA) – Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Dec 2009

Meeting the Cloud Challenge

- **Understand**
  - Relevant regulations and laws
  - The end-to-end supply chain
  - Role and position within the supply chain
  - CSP roles and responsibilities
  - Security boundaries and responsibilities
  - Data characteristics and value
- **Focus on the governance goal**
- **Plan and manage the risks throughout the supply chain**
Questions, Answers & Discussions

APPENDIX
Resources

- Effectively and Securely Using the Cloud Computing Paradigm (NIST Presentation, October 7, 2009)
- FS Insights (Protiviti, February 2013)

FFIEC IT Handbooks

- Audit
- Business Continuity Planning
- Development and Acquisition
- E-Banking
- Information Security
- IT Management
- Operations
- Supervision of Technology Service Providers (3rd Party Management/Outsourcing)
- Retail and Wholesale Payment Systems
<table>
<thead>
<tr>
<th>FFIEC Document Request Letter Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Financial Information</td>
</tr>
<tr>
<td>• Business and Technology Environment</td>
</tr>
<tr>
<td>◦ Hardware, Software, Network</td>
</tr>
<tr>
<td>• Internal and External Audit</td>
</tr>
<tr>
<td>• IT Management</td>
</tr>
<tr>
<td>• Development and Acquisition</td>
</tr>
<tr>
<td>◦ SDLC, Customer Support, User Groups, Customer base</td>
</tr>
<tr>
<td>• Support and Delivery</td>
</tr>
<tr>
<td>◦ Performance and Security Monitoring, DRP, Physical Security</td>
</tr>
</tbody>
</table>