CRCA CONFERENCE

NOVEMBER 13 & 14, 2014 - TORTOLA, BVI

CARIBBEAN REGIONAL COMPLIANCE ASSOCIATION

Privacy hacking & Data Theft

Cloud Computing risks & the Compliance Professional

Patricia A RoweSeale CIA, CISA, CISSP, CRISC, CRMA
The IIA (Barbados Chapter)
Internal Audit Portfolio Director
CIBC FirstCaribbean

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Objectives

- Cloud Computing 101
- Typical Risks associated with Cloud Computing
- The Compliance Professional response

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Definition of Cloud Computing

The US National Institute of Standards and Technology (NIST)

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 is composed of five essential characteristics, three service models , and four deployment models

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Five Essential Characteristics of Cloud Computing

On-demand self-service

Computing capabilities can be provisioned without human interaction from the service provider.

Broad network access

Computing capabilities are available over the network and can be accessed by diverse client platforms

Resource pooling

Computer resources are pooled to support a multitenant model.

Rapid elasticity

Resources can scale up or down rapidly and in some cases automatically in response to business demands.

Measured service

Resource utilization can be optimized by leveraging charge-per-use capabilities

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Three Service models (reference #2)

Infrastructure as a Service (IaaS)	Platforms as a Service (PaaS)	Software as a Service (SaaS)
• In an IaaS solution, the Cloud Service Provider (**CSP)** provides cloud users with processing, storage, networks and other fundamental computing resources. Operating systems and applications, however, are the responsibility of the user and are not included in the service offering of the CSP. ***Example: Amazon Web Services LLC***	• PaaS entails the CSP making available infrastructures and platforms on which cloud users deploy their own applications. This requires the CSP to support programming languages, libraries, services and tools. ***Example: Google App Engine™***	• When opting for SaaS, cloud users not only hire infrastructure and platforms from the CSP, but also run CSP-provided applications on them. ***Example: Salesforce***

CRCA CONFERENCE

Four Deployment models (reference #2)

Public

- The infrastructure is made available to the general public (e.g., Google Apps, Apple® iCloud).
- It is deployed within the CSP infrastructure, offsite to the enterprise infrastructure.

Community

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from enterprises or interest groups (e.g., schools, researchers, software developers) that have shared concerns.
- It can be deployed onsite (within the enterprise infrastructure) or offsite (within the CSP infrastructure, also called “outsourced”).

Four Deployment models (reference #2)

Private

- The infrastructure can be used only by one single enterprise.
- As for community clouds, it can be deployed onsite or offsite enterprise premises.

Hybrid

- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities.

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Risk associated with Cloud Computing

Typically risk events would impact the information assets by impairing one or more the following:

- **Confidentiality / Privacy**
- **Availability**
- **Integrity**

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Cloud Computing risks: Confidentiality / Privacy

- Who has access to your data?
- Where is your data?
  - Is your CSP obligated to handover your data if requested (Governments, Law enforcement)?
  - Is it possible for your data to be mistakenly disclosed, when another company's data is requested?
  - Is your CSP compliant with laws and regulations – at collection and storage jurisdictions?
  - Who has physical and logical access?
  - Who owns the data?

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Cloud Computing risks: Availability

- Is appropriately formatted data available at requested times for compliance monitoring and reporting?
- How portable is your data / applications?
- Is a Business Continuity Plan in place and was it tested?
- Is the CSP a going concern?

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Cloud Computing risks: Integrity

- **Who has access to your data / applications**
  - ◊ How are users provisioned?
  - ◊ Who controls user provisioning?
  - ◊ Are security and application events logged and monitored
- **Change management**
  - ◊ Who approves and validates changes made to systems

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

Compliance Professional response

- Early involvement in the decision
- Regular review of exceptions reports, with predefined corrective measures
- Review and action of independent auditor reports
- Current with emerging risks, laws and regulations
- Active monitoring of the CSP

THANK YOU!

Questions?

Cloud Computing risks & the Compliance Professional

CRCA CONFERENCE

References

1. IT Governance and the Cloud: Principles and Practice for Governing Adoption of Cloud Computing - (Ron Speed, CISA, CRISC, CA) – www.isaca.org
2. Security Considerations for Cloud Computing – www.isaca.org
3. Cloud Computing Risk Assessment: A Case Study – (Sailesh Gadia, CISA, ACA, CPA, CIPP) – www.isaca.org
4. Risk landscape of Cloud Computing – (Vasant Raval, CISA, DBA)- www.isaca.org

Patricia RoweSeale
CIBC FirstCaribbean International

bernardpat@caribsurf.com
246-231-9816
patricia.roweseale@cibcfcib.com
246-367-5946

CRCA CONFERENCE

CRCACONFERENCE.COM