Cloud Computing: Critical Security and Control Issues

Cloud computing has been described as “the ultimate form of outsourcing.” This refers to the fact that moving into the cloud allows the enterprise to outsource or rent infrastructure, IT services, application software, or any combination of these. In other words, IT services are purchased using a linear utility model.

Although the cloud model is attractive, chief information officers express near-universal concern about one issue: security. This concern includes unauthorized access to sensitive business data (by outsiders or insiders at the cloud ISP); availability and performance; location of the data (certain sensitive data may be prohibited by law from being stored outside the enterprise’s country boundaries); ability to retrieve the data in the event of contract termination; auditability; physical security at the ISP; and more.

The cloud model uses three models, each with their own security, control, and operational concerns. This seminar addresses these issues and explores how to protect the enterprise assets.

In this course, we will discuss the critical issues to be considered:

- Before the cloud contract is signed.
- For the duration of the contract.
- At contract change or renegotiation.
- At the end of the contractual relationship.
Course Duration:
1 day

CPE Hours Available:
7

Knowledge Level:
Intermediate

Field of Study:
Auditing

Prerequisites:
Participant should have a general understanding of IT processes, business and accounting applications, and IT outsourcing processes.

Advance Preparation:
None

Delivery Format:
On-site
Course Outline:

Audit Evidence

- Why evidence is important
- Different types of evidence
- Methods to gather evidence
- Best types of evidence
- Determine and review audit evidence that is appropriate, sufficient, and persuasive to support audit conclusions — examples provided

Understanding the Cloud Model

- The pay-as-you-go (PAYG) model for IT services
- The three basic models: IaaS, PaaS, SaaS
- Business value of cloud computing
- Corporate goals for each model
- Motivation for each model
- Necessary partnership with ISPs and other vendors

Business Risks With the Cloud Models

- Contractual issues
- Strategic risk
- Standards and lack thereof
- Maintaining the same level of control
- Tactical issues
- Privacy and confidentiality
- Data Integrity
- Availability and recoverability
- Risks with virtual machine environments

Managing the Cloud

- Encryption, encryption, encryption
- Scalability
- Data interchange
- Key management
- Meaningful metrics
- SLAs
- Security and risk assessment
- Mutual responsibilities
- Billing
Other issues

- Public vs. private clouds
- International: privacy, data location, data dispersal
- Litigation
- End of life / termination of agreement
- Compliance with laws and regulations
- Independent auditing
- Insurance