ISACA
Trust in, and value from, information systems
Greater Kansas City Chapter

Training Opportunity

Topic: Auditing and Securing Cloud-Based Services
Dates & Times: April 19 11:00 AM – 5:00 PM (Note: Updated Start Time)
April 20 8:00 AM – 5:00 PM
Location: Sprint Nextel World Headquarters – Overland Park, Kansas (Bldg. 6360 Room 1C269)
Parking: Included
CPE: 15 Credits
Price: *Regular ISACA member*: $450 – Deadline is April 13
Non-member: $585 – Deadline is April 13

Seminar Summary
Offering Internet-based computing and on-demand resources, software, and data, cloud-based services are rapidly changing the landscape of IT. With Software as a Service (SaaS) delivering application software, Platform as a Service (PaaS) available to design and develop software, and Infrastructure as a Service (IaaS) providing the equipment upon which to support other services, cloud computing offers IT a way to increase capacity and capabilities minus a huge investment.
In this two-day seminar you will explore the current state of cloud computing and its common architecture, and examine the major SaaS, PaaS, and IaaS providers in the market today. You will cover the security and control deficiencies that exist in cloud-based services and look at Security as a Service as a way to protect against them. You will review a risk-based approach to audit and controls for cloud based-services and investigate such areas as cloud-based network models, cloud brokers, and disaster recovery and governance in a cloud-services environment. Throughout the seminar, class exercises will reinforce what you learn and help you identify the risks, controls, and gaps in cloud services.

Registration
Registration is available online: http://www.isaca-kc.org/meetingReg.php
Registration fees must be paid promptly following registration to secure your seat and course materials if you are paying by check. Credit Card payment must be made at the time of registration.

Registration Includes
Course materials and lunch will be provided. More details forthcoming.

Cancellation Policy
The Greater Kansas City Chapter of ISACA reserves the right to cancel the training seminar if the instructor is unable to attend, the facilities are not available, or other unforeseen circumstances arise. If this occurs, a reasonable effort will be made to reschedule the seminar or refunds will be issued.
If a registrant cannot attend the seminar, the chapter requests an email notification two (2) weeks prior to the date of the event. Refunds will not be granted for cancellation requests received after this date. Generally, the chapter does not charge registrants a cancellation fee or penalty. Substitution of another individual for a confirmed registrant will be accepted at any time prior to the date of the event.

Speaker
Stan Fromhold, CISSP, CISA
Stan Fromhold is a member of the BT Security practice, where he is responsible for the design and bid of major customer security and governance programs. These programs include commercial pricing of customer engagements, technology selection for solution architectures, negotiations with suppliers, and risk analysis and risk management planning for proposal and project activities.
Mr. Fromhold has worked in information security for more than 25 years, specializing in enterprise security architecture solutions for converged networks, vulnerability assessments, security education, and security compliance audits. He has significant experience in helping organizations define and implement security architectures and policies for vulnerability and threat management, enterprise security event monitoring, and intrusion detection and prevention architectures. In addition, Mr. Fromhold is a much in-demand speaker at major security conferences.
Previously, Mr. Fromhold was Global Director of Security for Dun & Bradstreet, where he was responsible for all facets of global network security, including firewall architecture; security policy; and compliance for Windows, UNIX, routers, firewalls, security event monitoring, and Web security. In addition, he was responsible for the administration of SecurID, RACF, and for performing network vulnerability assessments. Prior to joining D&B, Mr. Fromhold was Director of Security for Munich Re/Americas Internet Services, where he was responsible for their network security architecture, including the design, implementation, and administration of firewalls, Web servers, proxy servers, SecurID servers, and other network security components. Prior to that, he was a Manager for Coopers & Lybrand's (now PricewaterhouseCoopers) IT Audit Risk and Assurance practice.

Agenda
What You Will Learn
1. Cloud-Based Computing: An Architectural Overview
- application architectures
- the SPI Cloud Computing Model
- key drivers for moving towards cloud-based services

2. Software as a Service (SaaS)
- key enterprise applications
- the SaaS transaction model(s)
- SaaS security and audit concerns

3. Platform as a Service (PaaS)
- major development providers/platforms
- PaaS security and audit concerns

4. Infrastructure as a Service (IaaS)
- host security in the cloud
- network security in the cloud
- data storage/SAN in a cloud IaaS environment
- cloud bursting
- virtualization models for cloud-based services: Hypervisor VM and inter VM isolation
- cloud-based security domains: virtualized security/firewalls
- IaaS security and audit concerns

5. Cloud-Based Network Models
- private cloud architectures
- hybrid architectures
- public architectures
- de-perimiterization of networks: secure access from any device, anywhere

6. Brokered Cloud Services

- cloud aggregators
- cloud brokers
- cloud management service portals

7. Security as a Service

- identity management as a service
- security event monitoring/IDS as a service
- vulnerability management as a service
- data leakage prevention as a service/Web filtering, e-mail filtering

8. Cloud-Based Security Standards and Dependencies

- directories and identity management
- federated identities
- emerging security Standards: SPML, XACML, OAuth, OpenID, others

9. Governance in a Cloud Services Environment

- key performance indicators
- audit trails for cloud-based services
- service level agreements, licensing
- legal complexities: data privacy, globalization, trans-border constraints
- third-party assessments and certifications: SAS70, ISO 27001

10. Disaster Recovery in a Cloud-Based Environment

- SPI HA architectures
- virtualized environments and their impact on disaster recovery
- updating and testing disaster recovery plans

11. Cloud Security and Audit

- key risks and audit concerns
- identifying key controls and mitigations
- cloud-based risk analysis models: ENISA, NIST, CSA
- security best-practices models for cloud-based services
- audit techniques and tests in a cloud-based environment