ISACA
Serving IT Governance Professionals
Philadelphia Chapter

Training Conference – October 13 - 17, 2008
PCI, Electronic Fraud. & Telecomm Networks
Marriott - Mount Laurel NJ

Who should attend?

The ideal conference for professionals including IT Auditors, Chief Information Officers, Chief IT Security Officers, Chief Financial Officers with responsibility for the IT function and others with an interest in PCI Compliance & Controls, Electronic Fraud Detection & Prevention, & Security & Control of Telecommunication Networks.

Program Outline

This conference will deliver the interactive and practical training IT professionals need to expand their knowledge while maintaining their competitive edge. The conference will feature sessions on state-of-the-art practices and management strategies presented by leading experts on the topics of PCI, Electronics Fraud, and security & control of Telecommunication Networks. The format consists of three consecutive in-depth sessions.

Session	Topic	CPEs	Member	Non-Member	Dates
1	PCI Compliance & Controls	8	$200	$250	October 13, 2008
2	Understanding and Preventing Electronic Fraud	16	$375	$425	October 14 – 15, 2008
3	Control and Security of Telecommunication Networks	16	$375	$425	October 16 - 17, 2008
1, 2, & 3	One person attending 3 sessions	40	**$850**	**$1000**	October 13 - 17, 2008

Location: Marriott – Mount Laurel NJ
915 Route 73, Mt. Laurel, NJ, 08054
(856) 234-7300
http://www.marriott.com/hotels/travel/phlla-mt-laurel-marriott/

Directions: http://www.marriott.com/hotels/maps/travel/phlla-mt-laurel-marriott/

Amenities: Cost includes session, continental breakfast, lunch buffet, and afternoon snack. Continental breakfast and sign in begin at 7:30 AM; sessions begin at 8:00 AM and end at 5:00 PM.

Agenda:

7:30 – 8:00	Breakfast Buffet
8:00 – 12:15	Training Session
10:15 – 10:30	Break
12:15 – 1:15	Lunch
1:15 – 5:00	Training Session
2:30 – 2:45	Afternoon Snack Break

All registrations and payments must be received by October 6, 2008.

Registration:

Due to the high demand for the conference sessions and limited space, participants are encouraged to register as early as possible to reserve a seat. Registration and complete course payment must be received by Monday, October 6, 2008. Click the following link or copy and paste the link into your browser.

http://www.acteva.com/booking.cfm?bevaid=166970

For questions, please contact Jim Scouton at 610-970-4345 or jscouton@comcast.net

Session 1

October 13, 2008

PCI Compliance & Controls

Highlights

The recent release of the PCI Data Security Standard 1.2 has once again ignited spirited discussion among financial institutions, and the processors, merchants and countless other interested parties. In almost 5 years of existence, more has been written about PCI than nearly any other compliance related topic. Yet, questions persist about its purpose, intent, and scope.

- Is PCI only a compliance standard?
- Is it an information security standard? If I am PCI compliant, am I also "card fraud bullet proof?"
- Who must comply?
- How can I intelligently comply without taking unacceptable risks?
- If I am not compliant, how much fraud risk do I really incur? Isn't PCI overkill?
- What will the networks, lawmakers and the regulators do If I am not compliant?

To answer these questions, and provide insight into the PCI Standard, please register for the informative seminar

Outline

"Making Sense of PCI Requirements"

- Why does PCI Exist?
- History, Standards?
- Compliance, validation and reporting requirements
- What Happens During a PCI Compliance Effort?
- How to Construct An Effective PCI Project
- "I am a merchant- What Does PCI mean to me?"
- I am a service provider- What Does PCI mean to me?"
- I issue credit and debit cards? Why should I care about PCI ?
- Anatomy of a Fraud
- Industry Reactions & Current Challenges:
  - Litigation – The legal environment
  - Fraud Proofing Your Institution
  - Technology Planning & Solutions
- Impact to Fraud Management

Speaker Profile

Bruce Sussman is a Senior Manager within Crowe Horwath LLP's Risk Services. He is Crowe's PCI thought leader, assists in development of SAS 70, and provides IT internal audits and audit support for SEC audits of public companies.

Bruce has 20 years of diversified experience in internal audit, professional services, IT security, and anti fraud management. His industry experience includes diversified financial institutions, asset custody, capital markets, transaction processing, payments technology, and mergers and acquisitions. Bruce has built internal audit functions and anti fraud strategies while focusing on enterprise and technical risk management issues.

Bruce is currently Chairman of the New York State Society of CPAs – Technology Assurance Committee. He is a frequent speaker with industry and trade groups such as the Bank Administration Institute, Institute of Internal Auditors and ISACA, on topics which include anti fraud controls, banking and payments technology. Bruce's articles and bylines have appeared in several states and national publications, and he was most recently featured in the AICPA's Journal of Accountancy.

Session 2
October 14 & 15, 2008

Understanding and Preventing Electronic Fraud

Highlights

COURSE DURATION: 2-days
CPE HOURS: 16

Electronic fraud is one of the best-kept secrets of modern business. While it is constantly occurring, most organizations cover up electronic fraud, absorb the loss as a cost of doing business and move on. This not only increases the cost of doing business, but it ensures that the perpetrators can continue their activities, moving from one target to the next without fear of being apprehended, let alone a conviction. If they are caught, the faulty security and shoddy controls enable the defense lawyers to create reasonable doubt. If E-business is to survive, E-fraud and theft must be stopped.

It is time to draw the line in the sand and this course will help you do just that. the instructor will provide the participants with an understanding of the types of E-fraud, how to detect it and how to prevent it. The participants will learn the need for network, application, and server security, as well as the need to build fraud sniffers, monitors, and surveillance applications. They will also learn how to convince management that strong controls must be in place to enable successful apprehension and prosecution of E-fraud cases.

I. INTRODUCTION
• What is electronic fraud
• Types of electronic fraud

II UNDERSTANDING HOW E-FRAUD OCCURS
• Network penetration
• Traps & cyber surveillance techniques
• Compromised record management services, cards, accounts, etc.
• Wireless LAN connections

III HARVESTING THE REQUIRED DATA
• Internet banking approach
• VPN approach
• Application defaults approach
• Gas station and retail outlet approach
• Vendor application flaws
• 401K approach
• ERP, CIS, billing systems
• Purchase and use of “Spy Gear”
• E-mail approach

Outline

IV MOVING THE FUNDS
• Wire and funds transfer Systems
• Cash concentration systems
• Setting up “real” business entities
• “Milking” Internet bank accounts
• Defeating fax back and other confirmation systems
• Using refunds and credits to access cash

V PREVENTION THROUGH NETWORK SECURITY
• Network vulnerability assessment
• Identifying breach points
• Network device security
• Network monitors
• Honey pots
• Intrusion detection systems
• Automated alerts

VI PREVENTION THROUGH SERVER SECURITY
• User and account security procedures
• Windows operating systems
• UNIX and Novell
• AS/400 and Mainframes

VII PREVENTION THROUGH APPLICATION SECURITY
• Vendor default installations
• Transaction risk analysis
• Identify & eliminate fraud prone practices
• Automated alerts
• Transaction delay and approval
• Audit software
• Identifying unusual trends

VIII PROSECUTION VS COVERUP
• Let’s play judge and jury
• Reasonable doubt
• Adverse publicity/customer confidence
• Prosecution

IX PUTTING IT ALL TOGETHER
• Preparing an E-fraud risk assessment
• Creating an effective management briefing
• Staffing and funding
• Building an effective Efraud squad
• Implementing preemptive anti-fraud techniques
• Staff and customer awareness programs

Speaker Profile

Gordon E. Smith
Gordon Smith, President & CEO of Canaudit, Inc., has over a quarter century of progressive audit experience. He continues to explore new audit & security technology as he develops new auditing procedures & techniques. Specializing in high-tech auditing, Gordon is a recognized expert on auditing complex networks, operating systems, databases, & forensic auditing. He is the original developer of the Canaudit Penetration Testing methodology & continues to be a leading member of the penetration audit team.

As a practicing auditor with a strong business sense, Gordon is adept at tying critical audit findings to the key objectives of the organization. He has been the keynote speaker at many national & international conferences. His highly energetic & enthusiastic presentations make audit topics interesting, exciting, & informative. His motivating style & dynamic delivery techniques capture the interest of the audience, open their minds, & inspire them to accept new methodologies & techniques. His innovative audit techniques & ability to translate complicated technology into simple English make Gordon one of the most popular speakers on the audit & computer security lecture circuit. Gordon is a distinguished career auditor with both internal & external audit experience. He founded Canaudit in 1985 to provide professional development & consulting services to the international audit community. Through Canaudit, Gordon has provided training & audit consulting services to many of the larger organizations such as banks, utilities, insurance companies, retail, government, & manufacturing concerns & has provided extensive services in the medical services industry.

For a more information on Canaudit Inc. or a detailed bio, please visit Canaudit.com or http://canaudit.com/personnel.html#gsmith

Session 3
October 16 - 17, 2008

Control and Security of Telecommunication Networks

Highlights

COURSE DURATION: 2-days
CPE HOURS: 16

The Internet, wireless networks, VPN connections, Voice over IP and mobile computing has dramatically changed corporate networks. New threats, such as electronic espionage, cyber terrorism and the normal hacker require preemptive security and effective response countermeasures. This seminar will provide the participants with a sound grounding in modern telecommunications methodologies, performance issues and security. The instructor will demonstrate many of the automated tools required to perform a network audit or security assessment. In addition, each participant will receive the Canaudit Network Audit Guide to enable them to perform a full network review. After this session, the participants will be able to identify potential points of penetration and ensure that the business-computing environment is protected.

This seminar addresses the total network! You will learn about network components and their specific risks, along with control techniques needed to provide a safe processing environment. Handouts include control checklists to help participants identify potential threats and develop a comprehensive risk assessment.

I Understanding Networks
- Evolution of modern networks
- E-business technology
- Wireless connectivity
- Internet and VPN
- Remote VS local access
- Glossary of terminology

II Carrier Related Issues
- Multiple carrier environments
- Selecting required services
- Cost effectiveness
- Business continuance and disaster preparedness
- Network contracts
- Control checklist/ audit program

III Communications Alternatives
- "Wire Line" type circuits
- Broadcast type circuits
- Wireless (802.11A&B & Bluetooth)

Outline

- Voice over IP
- ISDN, B-ISDN
- Frame Relay, ATM & Cell Relay
- Identifying potential points of failure
- Risk/control summaries
- Control checklist/ audit program

IV The Internet
- Internet security
- Measures & countermeasures
- Ports, services & protocols
- Firewall configuration
- Bypassing the firewall
- Managing the firewall
- Monitoring Internet activity
- Intrusion detection & response
- Risk/control summaries
- Control checklist/ audit program

V Network Equipment and Configuration
- Routers, Hubs, & Switches
- Wireless AP's
- Internal firewalls
- Intrusion detection & response
- Risk/control summaries
- Control checklist/ audit program

VI Mapping the Network
- Scanners & Sniffers
- Mapping tools
- Segment mapping
- Server identification & analysis
- Undocumented connectivity
- Security & connectivity contracts
- Identifying vulnerabilities
- Risk/Control Summaries
- Control checklist/ audit program

VII Trading Partner Connectivity
- Identifying trading partner connections
- Trading partner servers
- Title VS connectivity
- Enforcing security arrangements
- Risk/control summaries
- Control checklist/ audit program

VIII Network Operations and Management
- Business continuance and DRP
- Maintenance/Problem reporting
- Load management
- Network monitors
- Network utilization & trend analysis
- Management & exception reporting
- Control summaries
- Control checklist/ audit program

Speaker Profile

IX Network Incident Management
- Network Incident response procedure
- The network response team
- Investigating/ prosecuting intruders

Gordon E. Smith
Gordon Smith, President & CEO of Canaudit, Inc., has over a quarter century of progressive audit experience. He continues to explore new audit & security technology as he develops new auditing procedures & techniques. Specializing in high-tech auditing, Gordon is a recognized expert on auditing complex networks, operating systems, databases, & forensic auditing. He is the original developer of the Canaudit Penetration Testing methodology & continues to be a leading member of the penetration audit team.

As a practicing auditor with a strong business sense, Gordon is adept at tying critical audit findings to the key objectives of the organization. He has been the keynote speaker at many national & international conferences. His highly energetic & enthusiastic presentations make audit topics interesting, exciting, & informative. His motivating style & dynamic delivery techniques capture the interest of the audience, open their minds, & inspire them to accept new methodologies & techniques. His innovative audit techniques & ability to translate complicated technology into simple English make Gordon one of the most popular speakers on the audit & computer security lecture circuit. Gordon is a distinguished career auditor with both internal & external audit experience. He founded Canaudit in 1985 to provide professional development & consulting services to the international audit community. Through Canaudit, Gordon has provided training & audit consulting services to many of the larger organizations such as banks, utilities, insurance companies, retail, government, & manufacturing concerns & has provided extensive services in the medical services industry.

For a more information on Canaudit or a detailed bio, please visit Canaudit.com or http://canaudit.com/personnel.html#gsmith

Training Conference – October 13 – 17, 2008
PCI, Electronic Fraud, & Telecomm Networks

REGISTRATION

Conference Registration:

Due to the high demand for the conference sessions and limited space, participants are encouraged to register as early as possible to reserve a seat. Registration and complete course payment must be received by Monday, October 6, 2008.

Payment Processing:

The ISACA Philadelphia Chapter has changed the registration process to provide additional payment options. Acteva.com has been contracted to provide our participants with the flexibility of online registration and payment processing. Acteva's secure online system adheres to the chapter's policy and protects your personal information and privacy.

We are committed to protecting your privacy and to focus on the chapter's primary purpose of promoting the education of individuals for the improvement and development of their capabilities relating to auditing and/or security management. We welcome you to immediately begin using the registration process with confidence. For your convenience the payment processing steps have been detailed below:

Steps:

1. Click the following link or copy and paste the link into your browser.
   http://www.acteva.com/booking.cfm?bevaid=166970

2.. Specify the number of attendees for the session(s). **Note:** All the sessions are priced for ISACA Members and Non-members. Non-members are encouraged to join ISACA and start enjoying membership benefits.

3. Click the button

4. Enter contact information and ISACA member information

5. Click the button to confirm your order

6. Review the order and select a payment method.
   - Visa
   - MasterCard
   - Discover
   - American Express
   - Any ATM or debit card displaying the Visa or MasterCard hologram and logo
   - Personal or Corporate Check (Make check payable to "Acteva" and mail to: Acteva, 60 Spear St., 9th Floor, San Francisco, CA 94105) Mailed checks may take ten or more business days to be sent, so please plan accordingly. Specify the correct amount on the check and place the **Transaction Number** in the memo section on the check. Your registration will not be complete until the payment is processed.

7. Click the button; a receipt is sent via email once the transaction has completed.

Please Note:

- Registration is contingent upon full payment of the registration fee. To guarantee your registration, course fees must be received no later than the Monday, October 6, 2008.
- Refunds due to cancellations prior to deadline are paid net of all processing fees. No cancellations can be accepted after Monday, October 6, 2008.
- Substitutions are accepted and encouraged. Substitution of a non-member for a member will result in additional non-member fees being charged.
- The CPEs provided by the chapter are not NASBA certified but are recognized by the ISACA International organization to meet continuing education requirements for the CISA and CISM certifications. NASBA Certified CPEs will be provided for both courses being taught by Canaudit (Telecom and Electronic Fraud).