

## Who should attend?

The ideal conference for professionals including IT Auditors and Security Personnel with responsibility for the IT function and others with an interest in Auditing and Securing SAP's Enterprise Services Architecture, Audit and Security of Windows 2003, and Understanding the SANS Top 20 Security Vulnerabilities.

## 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 security experts. The format consists of three consecutive in-depth sessions.

Session	Topic	CPEs	Member	Non-Member	Dates
1	Audit and Security Windows 2003	14	\$300	\$400	March 12 – 13
2	SANS Top 20 Security Vulnerabilities Explained	7	\$200	\$250	March 14
3	Auditing and Securing SAP's Enterprise Services Architecture	14	\$550	\$600	March 15 – 16
1, 2, & 3	One person attending 3 sessions	35	\$975	\$1,150	March 12 - 16

**Location:** Hilton Crowne Plaza  
 2349 W Marlton Pike  
 Cherry Hill, NJ 08002  
 856-665-6666

**Directions:** <http://www.ichotelsgroup.com/h/d/cp/1/en/hotel/cpcrw?requestid=944093>

**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:**

<b>07:30 – 08:00</b>	<b>Breakfast Buffet</b>
<b>08:00 – 12:15</b>	<b>Training Session</b>
<b>10:15 – 10:30</b>	<b>Break</b>
<b>12:15 – 01:15</b>	<b>Lunch</b>
<b>01:15 – 05:00</b>	<b>Training Session</b>
<b>02:30 – 02:45</b>	<b>Afternoon Snack Break</b>

### 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, February 26, 2007. Click the following link or copy and paste the link into your browser.



<http://www.acteva.com/booking.cfm?bevaid=126112>

### Contact:

For additional information about the training sessions contact the Conference Program Coordinator, Peter Duranti at [peterduranti@yahoo.com](mailto:peterduranti@yahoo.com) or 610-291-1113.

## Session 1

March 12 - 13, 2007

## Audit & Security of Windows 2003

### Highlights

This session will focus on the audit and security issues related to the use of Windows 2003 Server Operating System.

#### Session Highlights

- Detailed discussion of Windows 2003 architecture and security components
- Use of Windows 2003 server operating systems to demonstrate key security features
- Demonstrations of Windows 2003 security and audit tools
- Discussion of new Windows 2003 Server security features, including default security settings, security hardening steps and use of the Group Policy Management Console (GPMC)

#### Session Duration

- 2 days

### Outline

- 1. Windows 2003 Concepts**
  - Overview of Windows 2003
  - Versions
  - Service Packs and Hotfixes
- 2. Understanding Windows 2003 Security Components**
  - Active Directory Services (ADS)
  - Kerberos Authentication Services
  - Group Policy
  - Security Configuration Toolset
  - Encrypting File System (EFS)
  - IPsec
- 3. Windows 2003 Security and Control Issues**
  - ADS Access Control and Permissions
  - Windows 2003 Domains
  - Trust Relationship Mechanisms
  - Group Policy
  - User Accounts and Groups
  - Kerberos and NTLM Authentication
  - Resource Access Controls
  - Audit Facilities – Event Logs
  - Network Security
  - Security Administration
- 4. Auditing the Windows 2003 Environment**
  - Audit Objectives
  - Automated Tools/ Scripts for Audit Testing
  - Approach to Windows 2003 Security Audit
- 5. Security and Audit Tools and Techniques**
  - Demonstrations of Windows 2003 Security Tools
  - Windows 2003 Resource Kit
  - WWW Sites related to Windows 2003 Security and Control

### Speaker Profile

**John Tannahill** is an independent Information Security and Audit Services Consultant. John's current consulting work areas are focused on information security in large information systems environments and networks. Particular areas of technical security expertise include: Windows 2000/2003; Unix (including Solaris, AIX and Linux); Oracle and Microsoft SQL Server, and Network and Internet security. John is a frequent speaker in Canada, USA and Europe on the subject of Information Security. He is a member of the Institute of Chartered Accountants of Scotland (CA) and a Certified Information Security Manager (CISM).

## Session 2

March 14, 2007

# SANS Top 20 Security Vulnerabilities Explained

Highlights	Outline	Speaker Profile
<p>This fast-paced 1-day session will provide an overview and explanation of the SANS Top-20 2006 consensus list of vulnerabilities. The current focus of this list is Internet Security Attack Targets</p> <p><b>Session Highlights</b></p> <ul style="list-style-type: none"><li>Detailed discussion of vulnerability management using SANS Top-20 as a base</li><li>Use of Unix and Windows operating systems environments to demonstrate vulnerabilities</li><li>Demonstrations of security and audit tools to test for vulnerabilities</li></ul> <p><b>Session Duration</b></p> <ul style="list-style-type: none"><li>1 day</li></ul>	<ol style="list-style-type: none"><li><b>1. Top-20 Overview</b><ul style="list-style-type: none"><li>Overview of 2006 List</li><li>CVE Entries and National Vulnerability Database</li><li>Testing Approach</li><li>Prevention Strategies</li><li>Security Approached</li></ul></li><li><b>2. Operating System Vulnerabilities</b><ul style="list-style-type: none"><li>Windows OS</li><li>Unix OS</li><li>MAC OS X</li><li>Other areas such as Internet Explorer</li></ul></li><li><b>3. Cross-Platform Application Vulnerabilities</b><ul style="list-style-type: none"><li>Web Applications</li><li>Database Management Systems</li><li>File Sharing</li><li>Other areas such as Security Management servers and devices</li></ul></li><li><b>4. Network Devices</b><ul style="list-style-type: none"><li>Configuration Vulnerabilities</li></ul></li><li><b>5. Security Policy and Personnel</b><ul style="list-style-type: none"><li>Excessive Rights</li><li>Users</li></ul></li><li><b>6. Zero Day Attacks</b></li></ol>	<p><b>John Tannahill</b> is an independent Information Security and Audit Services Consultant. John's current consulting work areas are focused on information security in large information systems environments and networks. Particular areas of technical security expertise include: Windows 2000/2003; Unix (including Solaris, AIX and Linux); Oracle and Microsoft SQL Server, and Network and Internet security. John is a frequent speaker in Canada, USA and Europe on the subject of Information Security. He is a member of the Institute of Chartered Accountants of Scotland (CA) and a Certified Information Security Manager (CISM).</p>

## Session 3

March 15 – 16, 2007

## Auditing & Securing SAP's Enterprise Services Architecture

### Highlights

This two-day session is for auditors and security professionals who have to audit the risks associated with the new ESA of SAP™ R/3™.

Enterprise Services Architecture (ESA) is the new model around which SAP is building its solution sets. SAP ERP Central Component (ECC) represents the evolution of R/3 towards an architecture based on Web services that is open and flexible. This shift, however, introduces an element of high risk in a technology that is complex and requires that controls are built into the architecture to protect the underlying organizational data.

#### Session Duration

- 2 days

### Outline

#### Key areas covered:

You will cover the major risk areas for the latest SAP release, including Sarbanes-Oxley compliance controls related to the protection of organizational financial data accessible via the open architecture tool set. You will review each architectural component, including mySAP.com, ECC, WebAS, NetWeaver, Master Data Manager, Enterprise Portal and Exchange and Mobile Infrastructure in terms of risks, system defaults, segregation of duties, and other key controls necessary to ensure the integrity and confidentiality of data are properly established. You will cover penetration testing results and techniques you can use to ensure that your SAP environment is not unduly exposed.

In addition, you will examine the audit feature, log files and compliance reports that help to identify and track suspicious activity. You will review the administration controls surrounding the various components and learn how to protect the development, change, and updates of new services in a controlled manner. Using a risk-based approach for the move to this new architecture, you will gain a solid understanding of the challenges faced by management and implementation teams. You will benefit from stated control objectives, recommendations, and audit control techniques for pre- and post- implementation risks within the architecture. You will define continuous auditing procedures and reports to ensure that your control recommendations remain effective.

### Speaker Profile

#### Frank W. Lyons, CISA, CNDE

Frank Lyons is President of Entellus Technology Group, Inc., a management consulting firm specializing in the audit, security, reliability, tuning, and management of networked computer systems. Mr. Lyons has been involved in information systems, specifically data security and auditing of networked database solutions, for more than 30 years. He has developed more than 100 sessions on audit, security, and control, and has extensive experience consulting for Fortune 500 companies.

Previously, Mr. Lyons was a Partner at Plagman Group, a security and auditing management consulting firm, a Consultant with Coopers and Lybrand; Manager of Advanced Technology for the IIA; and EDP Audit Manager for Blue Shield and for Sun Banks. He was the Manager of Application Development at a large insurance company and worked at Cullinet Database Systems.

## 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, February 26, 2007.

## 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?bevoid=126112>

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

## Travel:

**Hotel:** Crowne Plaza Hotel  
2349 W Marlton Pike  
Cherry Hill, NJ 08002  
856-665-6666

**Directions:** <http://www.ichotelsgroup.com/h/d/cp/1/en/hotel/cpcrw?requestid=944093>

**Parking:** Free

**Philadelphia International Airport:** [www.phl.org](http://www.phl.org)

**Interstate Railroad:** [www.amtrak.com](http://www.amtrak.com)

**Regional Transportation:** [www.septa.org](http://www.septa.org); [www.njtransit.com](http://www.njtransit.com)

- 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, February 26, 2007.
  - Refunds due to cancellations prior to deadline are paid net of all processing fees. No cancellations can be accepted after Monday, February 26, 2007.
  - Substitutions are accepted and encouraged. Substitution of a non-member for a member will result in additional non-member fees being charged.
  - CPEs for the SAP course are NASBA certified. The CPEs provided by the chapter for the other two courses are not NASBA certified but are recognized by the ISACA International organization to meet continuing education requirements for the CISA and CISM certifications.