

# DERBY CITY DISCLOSURES



**LOUISVILLE IIA CHAPTER**

**March 2007**

## PRESIDENT'S MESSAGE

Dear Louisville IIA Members and Non-Members,

Hi! I hope everyone had a Happy Valentine's Day and President's Day. Dana Spratt from Metro Government did a great job presenting the importance of Disaster Recovery and Business Continuity. Her energy and excitement kept the meeting lively and interesting. Hats off to our members, it was another great turn-out.

The IIA/ISACA Student Reception was a big success. We had fifteen to twenty students attend and twice as many professionals from the IIA and ISACA. The students learned a little about each organization and most importantly were able to make connections with the professionals. I want to thank all of the members from the IIA and ISACA who networked with the students. I really appreciate them taking time out of their busy schedules to come and talk with the students. I hope that this turns into an annual event for the IIA and ISACA. Special thanks goes to Dave Barker, who pulled this all together. Great job Dave!

Our next meeting is on March 13, 2007 at the Bristol Bar and Grill, registration at 11:30am, with the meeting starting at noon. Phil Noble with the Secret Service will be presenting on Credit Card and Purchasing Card Fraud. This is a joint meeting with the IMA. Please welcome them, and I hope to see everyone there!

The last two months of the chapter year are packed with meetings and seminars. We have some really good seminars lined up and I hope everyone will take advantage of these great training opportunities. So mark your calendar for the following dates. On April 19, we have a two hour seminar on Corporate Insecurity: Pillaging Information Assets, Destroying Established Reputations presented by Gordon E. Smith. On April 27, we have two half day seminars. The morning seminar will be presented by Tom Carlisle, with Cinergy Services, on Third Party Vendor/Contract Auditing. The afternoon seminar will be on Contract Fraud presented by George Mullins, Consultant. Then on May 14 -15, we are planning a two day seminar on Continuous Auditing: Making the Change - A New Perspective on Control Evaluation and Monitoring.

It is that time of the year again when we need to elect officers for the next year, September 2007 through May 2008. We would like to see some fresh new faces who are ready for a positive learning experience and a challenge! We really need our members to step up to the plate and nominate new officers. A member can nominate someone else or themselves. We have some officers who have held the same position for several years because, quite frankly, no one else volunteered. I really appreciate their dedication and service, but I really think they could use a well deserved break. So if you are thinking about being an officer please see me or any of the officers and let us know how you are interested in volunteering. Please ask any of our current or past officers of their great experiences volunteering their time and the networking skills they have acquired.

Please do not hesitate to contact me or any of the chapter's officers if you have any questions or suggestions. I look forward to seeing everyone at this month's meeting.

Connie A. Davis  
Chapter President

## **NEXT MEETING:**

**Tuesday, March 13, 2007**

**at the Bristol Downtown**

**Credit Card / Purchasing Card Fraud – w/ IMA**

*See page 2 for details*

# **MARCH MONTHLY MEETING**

## **Credit Card / Purchasing**

### **Card Fraud – w/ IMA**

Phil Noble  
Secret Service

**Tuesday, March 13, 2007**

12:00 noon, 11:30 registration

**1 CPE hour**

(certificates available at the meeting or contact Michelle Beumel)

## **Bristol Bar & Grille Downtown**

614 West Main Street  
(parking will NOT be validated)

**Cost: \$20.00**

Use PayPal at [www.ialou.org](http://www.ialou.org) or remit at meeting

## **RSVP your menu selection by** **THURSDAY, March 8, 2007 to**

Michelle Beumel

Office: 627-2098

Fax: 217-2738

[michelle.beumel@eon-us.com](mailto:michelle.beumel@eon-us.com)

### **Menu selections:**

#### **Chicken Florentine**

*Boneless chicken breast dusted in flour, sautéed & topped with a Parmesan cream sauce enhanced with spinach, mild green chilies & cheddar cheese. Served with rice and the vegetable.*

#### **Portobello Sandwich**

*Grilled Portobello, topped with hot pepper cheese & roasted red peppers, served on a Foccacia bun with a side of red pepper mayonnaise. Served with chips.*

#### **California Club**

*Fresh greens with shrimp, crab, avocado, olives, artichoke hearts and Harry's dressing.*

**PayPal** is a quick and simple way to pay for monthly IIA meetings. From the chapter web site ([www.ialou.org](http://www.ialou.org)), go to the meeting and seminar schedule page. Click the "pay now" button for the meeting you wish to pay for. If you already have a "PayPal" account, simply verify the amount, enter your log-in and password. *If you don't already have a "PayPal" account*, you will need to fill in the information for new members (similar to other e-commerce web sites such as Amazon). Once you have completed the transaction, you will be sent an e-mail receipt by PayPal and be returned to the Louisville IIA web site. The local chapter also receives an e-mail that tells us you have paid. You will **still need to contact Michelle Beumel** with your menu choice. All information is exchanged via HTTPS protocol (secure and encrypted) and remains with PayPal.

# CHAPTER NEWS

Visit [www.ialou.org](http://www.ialou.org) for more details!!

## OFFICERS

### President

Connie Davis  
MSD  
(502) 540-6380  
[davisc@msdlouky.org](mailto:davisc@msdlouky.org)

### Vice President

Roger LeMaster  
LWC  
(502) 569-3647  
[rlemaster@lwcky.com](mailto:rlemaster@lwcky.com)

### Treasurer

Bob Aemmer  
E.ON U.S.  
(502) 627-4033  
[bob.aemmer@eon-us.com](mailto:bob.aemmer@eon-us.com)

### Secretary

Steve Zagar  
Stock Yards Bank  
(502) 625-3744  
[steve.zagar@syb.com](mailto:steve.zagar@syb.com)

### Webmaster

Bruce Edwards  
University of Louisville  
(502) 852-4363  
[Bruce@bruceedwards.com](mailto:Bruce@bruceedwards.com)

## GOVERNORS

James Rose  
Humana, Inc.  
[jrose1@humana.com](mailto:jrose1@humana.com)

Don Whitehouse  
Insight Communications  
[whitehouse.d@insight-com.com](mailto:whitehouse.d@insight-com.com)

Michele Welscher  
Hawkins Company CPA's  
[mwelscher@KHEAA.com](mailto:mwelscher@KHEAA.com)

Heather DiEnno  
E.ON U.S.  
(502) 627-4626  
[heather.dienno@eon-us.com](mailto:heather.dienno@eon-us.com)

Dwayne Dowell  
Dwayne K. Dowell, PSC  
(502) 657-6428  
[dkdowell@dkdcpa.com](mailto:dkdowell@dkdcpa.com)

## WELCOME NEW MEMBERS

Three new members! Please welcome: Alex Branch of Alex Branch Consulting, Brian Long of PricewaterhouseCoopers; and Lisa Greenwell of Commonwealth Credit Union.

## CENTRAL REGION DISTRICT CONFERENCE

The Cincinnati Chapter is hosting the Central Region District Conference (District 1) April 16 & 17, 2007. They are offering a total of 16 CPE hours on three tracks: Critical Issues, Risk Assessment, and Technology.

## CIA EXAM REMINDER

Parts 1 & 2 of the CIA exam will be given on Wednesday, May 16; parts 3 & 4 will be given on Thursday, May 17. The application deadline is Saturday, March 31. For more information, contact Bob Aemmer at [bob.aemmer@eon-us.com](mailto:bob.aemmer@eon-us.com) or visit [www.theiia.org](http://www.theiia.org).

## CORPORATE INSECURITY SEMINAR

The Louisville IIA chapter will have a two-hour seminar on Corporate Insecurity: Pillaging Information Assets, Destroying Established Reputations presented by Gordon Smith of Canaudit, Inc. on April 19, 2007. This seminar is intended for executives and senior managers who need to understand how control structures are defeated, as well as senior information security and audit staff members. The price is \$60 for IIA members, \$65 for non-members. See the last few pages for more info!

## CONTINUOUS AUDITING SEMINAR

On May 14 & 15 we are planning a two day seminar on Continuous Auditing: Making the Change - A New Perspective on Control Evaluation and Monitoring. The price is \$400 for IIA / ISACA members and \$450 for non-members. See the last three pages of the newsletter for additional information.

## CHAIRPERSONS

### Academic Relations

Dave Barker  
University of Louisville  
[dfbark01@louisville.edu](mailto:dfbark01@louisville.edu)

### Audit

Will Metcalf  
University of Louisville  
[wametco@louisville.edu](mailto:wametco@louisville.edu)

### Government Relations

Jenni Schelling  
Louisville, Jefferson Co. Metro  
[jenni.schelling@louisvilleky.gov](mailto:jenni.schelling@louisvilleky.gov)

### Membership/Attendance

Michelle Beumel  
E.ON U.S.  
[michelle.beumel@eon-us.com](mailto:michelle.beumel@eon-us.com)

### CIA Program

Bob Aemmer  
E.ON U.S.  
[bob.aemmer@eon-us.com](mailto:bob.aemmer@eon-us.com)

### Seminars

Norman J. Pfaadt  
Resources US  
[Norman.pfaadt@resources-us.com](mailto:Norman.pfaadt@resources-us.com)

### Newsletter Editor

Corey Koellner  
Ernst & Young  
[corey.koellner@ey.com](mailto:corey.koellner@ey.com)

# NATIONAL NEWS

Visit [www.theiia.org](http://www.theiia.org) for more details!

## Headlines from [www.theiia.org](http://www.theiia.org) . . .

### **IIA Responds to SEC and PCAOB Exposure Drafts**

The Institute of Internal Auditors (IIA) has submitted a response to the Securities and Exchange Commission's (SEC) *Management's Report on Internal Control Over Financial Reporting* exposure draft and the Public Company Accounting Oversight Board's (PCAOB) *Proposed Auditing Standard - An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements and Related Other Proposals* exposure draft. The IIA commends both organizations' initiative and indicated the exposure drafts are an improvement to the existing guidance. Even so, additional enhancements are recommended. Further commentary is included in The IIA's responses.

### **March 6 webcast -- Auditing the Unthinkable: Business Continuity and Disaster Recovery**

Don't miss The IIA's March 6 webcast, *Auditing the Unthinkable: Business Continuity and Disaster Recovery*.

### **IIA Names Executive Director for IIA-Canada**

To strengthen the voice of the internal audit profession in Canada, The Institute of Internal Auditors (IIA) has hired Luc Lavoie, BAA, MBA, CGA, as executive director of the newly established IIA-Canada. Along with an 18-member IIA Canadian Council established last year, Lavoie will work to raise the awareness and professionalism of internal auditing in Canada. The Council and office were created in response to a need for Canadian-specific advocacy efforts.

### **Read the February issue of ITAudit**

For the latest IT news and articles, check out the February issue of ITAudit. This issue provides information that can help internal auditors learn how security architectures work and provides recommendations for an effective continuous audit process. The issue also discusses how organizations can identify instances of fraud and material errors by automating journal entry tests. To read ITAudit, go to [www.theiia.org/itaudit](http://www.theiia.org/itaudit).

### **ADVERTISEMENT POLICY**

**FREE** recruiting advertisements are available on the local IIA Chapter website and in the monthly newsletter! **Any employer is eligible for free advertising IF** at least one employee is a member of the Institute of Internal Auditors, Louisville Chapter. Executive Search Firms will be charged a nominal fee of \$50 for ½ page advertisement and one month of posting open positions on our webpage. Payment must be received prior to advertising / posting. For more information, contact the IIA Louisville Chapter President at [president@iialou.org](mailto:president@iialou.org) or Secretary at [secretary@iialou.org](mailto:secretary@iialou.org).

## *Did You Know . . .*

**The IIA 2007 International Conference will be held July 8-11 in Amsterdam?**

For more information, refer to the IIA's website, [www.theiia.org](http://www.theiia.org)

## **NATIONAL TRAINING CALENDAR**

### **MARCH, 2007**

5 – 9  
Seminar  
Orlando, FL

26 – 30  
Seminar  
Las Vegas, NV

### **APRIL, 2007**

2 – 6  
Seminar  
Dallas, TX

16 – 20  
Seminar  
Miami, FL

23 – 27  
Seminar  
Baltimore, MD

**2006-07 Calendar of Events**  
**Louisville Chapter of the IIA**

|                           |  |
|---------------------------|--|
| <b>3/13/07</b>            | <b>Credit Card/Purchasing Card Fraud w/ IMA</b><br>Phil Noble<br>US Secret Service |
| <b>4/10/07</b>            | <b>QAR</b><br>Brian Kruk<br>Titus Group  |
| <b>4/19/07</b>            | <b>Corporate Insecurity Seminar</b><br>Gordon Smith<br>Canaudit, Inc.              |
| <b>4/27/07 AM</b>         | <b>Seminar-Third Party/Contract Auditing</b><br>Tom Carlisle<br>Cinergy Services   |
| <b>4/27/07 PM</b>         | <b>Contract Fraud</b><br>George Mullins<br>Health South                            |
| <b>5/8/07</b>             | <b>Diversity on the Audit Team</b><br>at the Ali Center                            |
| <b>5/14 &amp; 5/15/07</b> | <b>Continuous Auditing Seminar</b>   |

# Corporate Insecurity: Pillaging Information Assets, Destroying Established Reputations

**COURSE DURATION:** 2 hours  
**CPE HOURS:** 2  
**LEVEL:** Intermediate / Group-Live  
**PREREQUISITES:** None  
**ADVANCED PREPARATION:** None

Corporations, governments, and universities have one thing in common. They have all been targets of hackers and dishonest employees. Bank of America and Wachovia had client data sold by staff. Citi Group, City National and Time Warner lost electronic media; Card System Solutions, USC, California State University Chico and ChoicePoint had customer data taken. All of these institutions not only had to perform costly remediation, but their issues were widely reported in newspapers across the land and around the world. Clearly, traditional control structures have failed! Servers, databases and even outsourced operations are exposed to pillagers!

Executive management is not only embarrassed, but they feel that they have been deceived by incorrect assurances from middle managers, security staff and even auditors that their systems and data were safe. They provided management with a false sense of security based on testing and verifying antiquated controls that are not effective against the skilled cyber-thief. In this highly charged and controversial presentation, Gordon Smith, President and CEO of Canaudit Inc., will demonstrate how old-style controls can be easily defeated. Section by section, control by control, he will demonstrate how easy it is to defeat control structures. This is a session that must not be missed!

## **WHO SHOULD ATTEND**

This seminar is intended for executives and senior managers who need to understand how control structures are defeated. It is also intended for senior information security and audit staff members. There are no prerequisites.

## **SEMINAR OUTLINE**

- |  |  |  |
|--|--|--|
| <b>I Overview</b> <ul style="list-style-type: none"><li>• State laws require disclosure</li><li>• Recent embarrassments</li><li>• Beating controls: Easier than stealing candy from a baby</li><li>• A new approach to risk assessment</li><li>• Testing the absence of control</li><li>• Changing the corporate mindset</li></ul>   | <ul style="list-style-type: none"><li>• Administrative accounts through DoS</li><li>• Web mail and VPN tricks</li><li>• Sniffers in gathering places</li><li>• Self Help – the great new beginning</li><li>• When all else fails, make donations</li></ul>   | <ul style="list-style-type: none"><li>• Compromising laptops</li><li>• Defeating intrusion detection and prevention</li><li>• Inside-out outside-in exploits</li><li>• Cell phone and VOIP issues</li><li>• External links and services</li></ul>  |
| <b>II Defeating Physical Security</b> <ul style="list-style-type: none"><li>• Breaching the Fortress-type security</li><li>• Scamming key card access systems</li><li>• Fooling security staff</li><li>• Social engineering employees and contractors</li><li>• Accessing confidential documents</li><li>• Gaining access to data files</li><li>• Acquiring a valid and authorized access card and badge</li></ul> | <b>IV Gaining Access to Data</b> <ul style="list-style-type: none"><li>• Gleaning "insider" information</li><li>• Shared drives and files</li><li>• Courier and dispatch services</li><li>• Consultants and outsourcers</li><li>• Trading partners</li><li>• Exploiting database and operating system flaws</li><li>• Personal information storage and storage services</li><li>• Social engineering</li><li>• Not-so "public" information</li></ul> | <b>VI The Internet: An Open Door</b> <ul style="list-style-type: none"><li>• Defeating VPN security</li><li>• Utilizing vendor backdoors</li><li>• Web applications: Gateway to the data</li><li>• Extranet exploits</li><li>• Defeating the firewall</li></ul>  |
| <b>III Account and Password Capture</b> <ul style="list-style-type: none"><li>• Beating Active Directory</li><li>• Defaults and service accounts</li></ul>   | <b>V Hitching a Ride on the Information Superhighway</b> <ul style="list-style-type: none"><li>• Trusty old techniques still work</li><li>• Executive and home networks</li><li>• Corporate internet cafés</li></ul>   | <b>VII Staff and Contractors</b> <ul style="list-style-type: none"><li>• "Purchasing" employees and contractors</li><li>• Public postings</li><li>• Hiring and contracting practices</li><li>• Portable data</li><li>• Fear of the auditor</li><li>• Scratching the surface</li></ul> <b>VIII The Canaudit Security Squadron</b> <ul style="list-style-type: none"><li>• We're looking out for you</li></ul> |

## **Gordon E. Smith**

(Home Base: Hamburg, Pennsylvania)



**Gordon Smith**

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

As a practicing auditor with a strong business sense, Mr. Smith is adept at tying critical audit findings to the key objectives of the organization. He has been the keynote speaker at many national and international conferences. His highly energetic and enthusiastic presentations make audit topics interesting, exciting, and informative. His motivating style and dynamic delivery techniques capture the interest of the audience, open their minds, and inspire them to accept new methodologies and techniques. His innovative audit techniques and ability to translate complicated technology into simple English make Mr. Smith one of the most popular speakers on the audit and computer security lecture circuit.

Mr. Smith is a distinguished career auditor with both internal and external audit experience. He founded Canaudit in 1985 to provide professional development and consulting services to the international audit community. Through Canaudit, Mr. Smith has provided training and audit consulting services to many of the larger organizations such as banks, utilities, insurance companies, retail, government and manufacturing concerns and has provided extensive services in the medical services industry.

Mr. Smith pioneered the integrated audit concept and assisted many of the above organizations in making the transition to the integrated audit concept. His unique ability to explain complex information technology concepts has enabled many internal auditors to succeed in becoming "true" integrated auditors. His structured COSO-compliant approach enables integrated auditors to provide increased audit coverage while dramatically reducing the time required to perform integrated application audits.

Mr. Smith was the recipient of the 2002 Wasserman Award for Outstanding Achievement in the field of Information Systems Auditing and Control. He is a Certified Management Accountant (Canada) who graduated in 1981. He is also a Certified Government Financial Manager and a member of The Institute of Internal Auditors and The Association of Government Accountants. Mr. Smith is listed in the WHO'S WHO OF LEADING AMERICAN EXECUTIVES and has published 2 books titled *Network Auditing: A Control Assessment Approach* and *Control & Security of E-Commerce*, both published by John Wiley and Sons.

# Continuous Auditing: Making the Change - ITG221

A New Perspective on Control Evaluation and Monitoring

Learning Level: Intermediate

CPEs: 15 Fee:

\$1,395.00

[Focus and Features](#)

[Who Should Attend](#)

[Agenda](#)

[Register](#)

## Focus and Features

Continuous auditing has been viewed as the “future of audit” for decades. Finally coming to fruition, it is considered by many today as a way to address compliance with the U.S. Sarbanes Oxley Act of 2002, particularly Section 409’s real-time disclosure requirements of complete and accurate current information. However, actually changing the audit process from a historic review activity to a continuous, current basis requires a fundamental shift in the audit department’s approach to its audits.

In this two-day seminar you will cover continuous auditing, its conceptual framework, and the areas you must consider when implementing this approach. You will learn the differences between continuous monitoring and continuous auditing and review the viability of these techniques. You will gain an understanding of the increasing need for available, reliable, timely data; investigate internal control assessment and audit’s role; and benefit from examples of areas that might be the best places to start. You will discover how continuous auditing can help achieve compliance with internal control reporting and other aspects of Sarbanes-Oxley. You will explore how improving definition and retrieval of data will enhance the way you conduct your audits, and examine automated audit procedures, information system requirements, key controls, reporting, and tools and techniques that will help take your audits to the next level. (**Note:** *This seminar covers topics found in Chapter 1 of the CISA Review Manual.*)

## Who Should Attend

Information Technology, Financial, and Operational Auditors; business executives with technical experience who want to understand continuous auditing

## Agenda

### What You Will Learn

#### 1. Defining Continuous Auditing (CA)

- the differences between continuous and traditional auditing
- continuous auditing vs. assurance vs. ongoing monitoring
- CA interaction with system controls
- CA vs. IT system monitoring

#### 2. Understanding CA Benefits and Use

- addressing changing audit expectations
- effectiveness of management monitoring efforts
- leveraging audit and management resources
- regulatory compliance monitoring needs
- managing residual risks
- addressing SAS 99 fraud and SAS 94 IT audit issues
- cost-recovery opportunities

### **3. Using CA to Meet Sarbanes-Oxley Requirements**

- responding to the need for faster, better information
- quarterly assessments (Section 302)
- annual report of controls (Section 404)
- timely reporting of fraud indicators
- real-time reporting of significant changes (Section 409)
- timely reporting of fraud indicators
- relationship to the COSO Report
- using ISACA's COBIT as a resource

### **4. Integrating CA into Other Models**

- enterprise risk management models: COSO ERM
- internal control structure: COSO
- IT control structure: COBIT

### **5. Overcoming CA Challenges**

- management support
- false positives
- implementation and maintenance costs and ROI
- security of confidential information and records
- overcoming management concerns
- addressing independence and objectivity concerns
- record retention issues: S-OX Section 103
- audit evidence issues
- ensuring data integrity
- regulatory and legal implications
- developing a monitoring program for management: is it a good idea?

### **6. IT Enablers to Facilitate Continuous Auditing: What's Available**

- embedded audit modules (EAM)
- business intelligence (BI)
- artificial intelligence
- neural networks
- regression analysis
- data analysis
- query tools
- database management systems (DBMS)
- data warehouses
- data marts
- data mining
- predictive modeling
- middleware
- transaction logging
- audit 'bots

### **7. CA Types**

- embedded audit modules vs. interactive analysis
- business/artificial intelligence
- statistical modeling
- trend analysis

- ratio analysis

- analytics
- primary key indicators
- monitoring “high-risk” transactions

### **8. CA Tools: Pros and Cons**

- ERP query tools: Crystal, Focus, BRIO
- general audit software: ACL, IDEA
- fraud detection software
- network security assessment tools: ISSS, Tripwire

### **9. Developing CA Models**

- creating a “risk” inventory
- understanding key indicators
- identifying data resources
- assigning roles and responsibilities
- determining which CA tool to use
- developing and testing applications
- integrating CA into the audit/ERM model

### **10. Selling the CA Process**

- establishing a business case
- identifying champions
- ensuring timing is right
- determining return on investment

### **11. Making the Transition to Continuous Auditing**

- defining the steps: overcoming the difficulties
- creating a win-win situation
- strategic planning
- methodology required
- turning objectives into actions
- making a business case for continuous auditing
- why this is a business issue
- a phased approach
- example areas
- success factors
- timing issues

### **12. Specific Testing Techniques for Continuous Auditing**

- financial
- operational
- computer security
- fraud
- procurement card