

INSIDE THIS ISSUE

Welcome Message.....1
Monthly Meeting.....2
Fall Seminar.....3
Job Opportunities.....5
Education9
Editor's Corner.....10
About Our Chapter....11

Welcome...

Greater Cincinnati ISACA Chapter Members,

With the ISACA Certification tests rapidly approaching, there are some additional preparation courses that are being offered. Please visit http://www.isaca-cincinnati.org/Events/Review_Courses.htm to learn more.

Our November meeting will be held on November 6, which is Election Day. Please remember to vote prior to attending the meeting. ISACA will also hold an election at the November meeting; we will vote on the proposed changes to the Chapter Bylaws. The Bylaws are being updated to more accurately align with ISACA International's latest template. These changes have been posted to the website and are available for review by clicking on the links here: http://isaca-cincinnati.org/Our_Chapter/Bylaws.htm.

Our first seminar will be held on November 27th and 28th at the Montgomery Inn in Montgomery, OH. The Greater Cincinnati ISACA Chapter is proud to present a two-day seminar by CPE Interactive: ***Evaluating IT Security Management*** with Jeff Kalwerisky presenting. This is a 16 CPE event, two more CPEs than seminars in the past. We welcome both members and non-members to the seminar. Pricing has been set at \$400 for ISACA members and \$500 for non-members for those who register by November 12. Please see page 3 in this newsletter for more details and information on registration. Please contact Joe Lairson (Joseph.Lairson@omnicare.com) if you have any questions regarding this or any future seminars.

We are always looking for great speakers. Please send any proposals or ideas to our VP of Programs, Sandy Burden (sandy_burden@cinfin.com). As a reminder, there will be no regularly scheduled meeting in December 2012.

Do you have anything to contribute to this newsletter? Please send it to our Newsletter Editor, Buky Thorpe (buky.thorpe@gmail.com).

If you are interested in becoming a member of the chapter, or would like additional information on membership please contact our VP of Membership, Mike Smith (mrsmith@gaic.com).

Remember, the greatest asset to the Cincinnati ISACA Chapter is our member community. If you have any questions or comments, please direct them to me (jhanfordisaca@gmail.com).

Jesse A. Hanford
Greater Cincinnati ISACA President

Network Perimeter Security and Remote Access

Speakers: Joe Bazeley, Miami University

Date & Time: November 6th, 2012, 5.30pm

Location: The Original Montgomery Inn, Montgomery, OH

Overview:

The network boundary has become fuzzier over time, thanks to telecommuting, bring your own device, and other changes. This talk will start with traditional network perimeter security and remote access, move into a discussion of the new problems your IT security staff are facing (and which they likely have been unable to solve either due to political or financial reasons), and the types of questions you should consider adding to your audits to more clearly surface these issues.

About the Speakers

Joe Bazeley is Miami University's Information Security Officer (ISO). He has responsibility for ensuring Miami University's compliance for IT resources, and coordinating their response when information security incidents occur. He is also the Assistant Vice President for Infrastructure & Operations, so he has the responsibility for the network, servers, data center, and other operational pieces. He has been at Miami University since October 2008. He was previously the ISO for Loyola University Chicago and prior to that he ran the Computer Incident Response Team for Accenture.

Please register by October 31.

Cincinnati ISACA members and non-members can register by using the [link](#) at the chapter website or by sending an email to isaca_meetings@yahoo.com if you prefer to pay at the door.

The Cincinnati ISACA Chapter is proud to present.

Evaluating IT Security Management

Mark your calendar and register for this two-day course on Evaluating IT Security Management. Earn **16 Continuing Education (CPE) credits** for this course.

A good percentage of internal and external IT auditors' scope relates to information security. The assurance function must either place reliance on the management of the information function or perform extensive substantive procedures to satisfy compliance requirements. Where reliance is placed, the auditor must depend on their assertions and records of the information management function. A mature information security function will translate into reduced fieldwork. The internal auditor also is responsible for evaluating the effectiveness and efficiency of the information security function as part of their audit universe. ISO 31000 is the new standard (2009) for managing and assessing risk. But what is the risk associated with IT security management itself? An inadequate level of skill or competence in IT security management can lead to serious negative consequences for the enterprise, including:

- Inability to comply with statutes and regulations, such as Sarbanes-Oxley, HIPAA, FISMA, PCI-DSS, GLBA, Basel II, and governmental entities
- Lack of preparedness for security incidents and/or inability to execute a timely recovery
- Higher audit and insurance costs

Instructor

The instructor, Jeff Kalwerisky is the Senior Director of Information Security and Technical Training at CPE Interactive. Jeff has specialized in information security, information risk management and IT auditing for over 20 years. He currently focuses on information risk, IT security governance and frameworks, and secure software development. He has held executive positions in information security and risk management with Accenture and Booz Allen Hamilton consulting firms. In both of these capacities, he has consulted with Fortune 100 companies and national governments. As manager of global security for VeriSign, Jeff was responsible for ensuring that affiliate companies in 30 countries adhered to VeriSign's military-grade security standards appropriate to a global certification authority, which he helped to design and deploy. Jeff was a partner with a major audit firm in South Africa and a consultant with PricewaterhouseCoopers. He has published security and audit guides, and has developed training courses throughout the USA and internationally on a wide range of technical topics.

Jeff is originally from South Africa, where he received a Bachelor of Science in Physics and Math, a Master's of Science in Computer Science from University of Witwatersrand, Johannesburg, and Masters in Finance and Auditing from the University of South Africa, Pretoria. He is a Chartered Accountant (SA) and Certified Information Systems Auditor.

Evaluating IT Security Management...CONTD.

Timing and Location

Two days: Tuesday, November 27th and Wednesday, November 28th, 2012 from 8:30 a.m. to 5:00 p.m.
Montgomery Inn (513-791-3482), 9440 Montgomery Road, Montgomery, Ohio 45242
Free Parking is available behind the restaurant and across the street.
Continental breakfast and lunch provided both days. Montgomery Inn is noted for its food!

Tuition

The ISACA Greater Cincinnati Chapter is helping to provide this training at a much reduced price; technical training from a comparable source is typically \$1500 or more. To ensure an interactive and comprehensive course, space has been limited to 25 participants.

Our deadline to cancel with the instructor is November 13, 2012. Please register by this date so that we can best measure interest in the seminar. Price incentives have been applied to recognize your timely response.

\$400 for members of ISACA (\$500 for non-members) until November 12, 2012

\$500 for members of ISACA (\$600 for non-members) after November 12, 2012

Registration

To register, send a note to the coordinators below with the name of the participant and email.

Register and pay on-line at the website (www.isaca-cincinnati.org) or send your checks with attendee name to: Greater Cincinnati ISACA Chapter, P.O. Box 54752, Cincinnati, Ohio, 45254.

Cancellations

You are not registered nor will you have a guaranteed spot until payment is received. A cancellation fee of \$100 will be applied to the refund if notification is less than 15 days prior to the course to pay for non-refundable materials and venue costs. If you are unable to attend, you may send someone in your place and inform us of the substitution.

For enrollment, questions, or cancellations, email any of the following contacts.

Joe Lairson (Joseph.Lairson@omnicare.com); Holly Johnson (hajohnson@gaic.com); Lei Zhao (lzhaoisaca@gmail.com).

Information Technology Audit Director

Vantiv Inc. has an immediate opportunity for an Information Technology Audit Director.

About Vantiv Inc.

Vantiv is a leading integrated provider of payment processing strategies and advanced technology solutions for businesses and financial institutions. Services include: Payment Processing, Advisory Services, Legislation and Compliance, ATM Solutions, Mobile Services, Merchant Services for Financial Institutions, Fraud and Data Security, Loyalty Programs, Terminals and Gateways

Detailed Responsibilities:

- Develop and execute strategic and tactical programs to identify and quantify current and evolving IT risk and other exposures to Vantiv for key areas of responsibility.
- Oversee and manage the design, development, and implementation of the risk-based audit plan focusing upon critical risk areas, including assessments of risk-controlling activities and risk monitoring systems, evaluation of internal controls, compliance with laws and regulations and conformity with industry and regulatory best practices and standards.
- Present results of work performed to senior management and prepare applicable reporting for inclusion in Audit Committee reporting and actively participate on cross-functional teams for new systems, process improvements, and entity acquisition and conversion activity.
- Provide ongoing oversight, liaison, and follow-up ensuring that key business processes and issues are addressed and appropriate management involved.
- Provide objectivity, independence and creative solutions in the resolution of material issues.
- Participate in pre-acquisition due diligence as needed.
- Manage Co-sourcing relationships for assigned areas of responsibilities with technical audit service providers.
- Develop and monitor budgets, and ensure appropriately experienced and knowledgeable resources are retained for co-sourced engagements.
- Interact and maintain relationships with external reviewers that relate to the key areas of responsibility.
- Ensure Compliance reviews are performed using Vantiv policies, FFIEC, Federal, and appropriate regulatory guidelines and confirm that key controls are functioning effectively.
- Manage IT Audit team members to ensure optimal performance in meeting the Audit Division's goals and the objectives. Develop all team members within the context of the career development framework, with direct supervision and coaching responsibilities for multiple IT Audit team members.
- Develop technical and leadership skills for all team members while customizing education needs for individuals.
- Aggressively prepare all levels of team for future opportunities, by identifying challenging work assignments, mentoring and education programs to give employees exposure to proactive enterprise-wide problem solving.
- Develop and maintain ongoing two-way timely and clear performance feedback to maintain healthy, proactive work relationships.

Experience and education requirements.

- Background in financial services technology is required; payment card industry experience is highly desirable.
- Demonstrated responsibility at the Director Level is necessary, including sound judgment, relationship building across various levels of management, and decision making skills.
- Technical experience in managing audit groups within a multi-platform, networked environment is essential.
- Ideal candidate will have robust experience with Windows, UNIX, and Mainframe environments.
- Bachelor's degree in Computer Science or Management Information Systems is required; other related academic majors (e.g., Accounting or Finance) should be accompanied by applicable work experience in IT or IT Audit. Master's degree is highly desirable.
- Technical Certifications such as CISA or CISM are required; other related professional certifications such as CISSP, CRISC, CPA or CIA are highly desirable.
- Sound written and oral communication skills.
- Demonstrated project management skills in a dynamic work environment that often requires management and completion of multiple demands, shifting priorities, and rapid change.
- Inspire teamwork and responsibility with team members and use technology and tools to enhance the effectiveness of the audit process and deliverables.
- Results and goal oriented and ability to apply logical/critical thought processes when developing business solutions.
- Demonstrated ability to display a positive business presence with management and external personnel.

To find out more or to apply for this position, please click [here](#) .

Deloitte Career Opportunities

Information Technology Audit Specialist

- **Manager**
- **Senior Consultant**
- **Consultant**

Locations: *Cincinnati, Detroit, Cleveland, Pittsburgh*

About Deloitte.

Deloitte is one of the leading professional services organizations in the United States specializing in audit, tax, consulting and financial advisory services with clients in more than 20 industries. We provide powerful business solutions to some of the world's most well-known and respected companies, including more than 75 percent of the Fortune 100.

At Deloitte, you can have a rewarding career on every level. In addition to challenging and meaningful work, you'll have the chance to give back to your community, make a positive impact on the environment, participate in a range of diversity and inclusion initiatives, and get the support, coaching, and training it takes to advance your career. Our commitment to individual choice lets you customize everything from your career path to your educational opportunities to your benefits. And our culture of innovation means your ideas on how to improve our business and your clients' will be heard.

Financial Statement & Internal Control Audit services provide audits and reviews of financial statements and reporting on internal controls in accordance with applicable professional standards. Our audits are planned to be responsive to our assessment of the risk of material misstatement based on the understanding we gain of the organization and its environment, including its internal control. We utilize this understanding to design the nature, timing, and extent of our audit procedures, while maintaining an objective and independent attitude. We also strive to provide timely communications regarding professional developments, and insights regarding matters that may affect the organization's business.

We are currently seeking IT Audit professionals for Manager, Senior Consultant and Consultant positions. For more information about these opportunities and to apply, please visit our web site at www.deloitte.com/us/careers

Senior Information Technology Internal Auditor

Western & Southern Financial Group has an immediate opportunity for a Senior Information Technology Internal Auditor.

Summary of Responsibilities

Performs and supervises risk-based internal audit activities for the Company and its subsidiaries. Performs risk-based integrated reviews of financial, operational, systems and management controls of the Company. Provides assistance to the external auditors and regulatory auditors while maintaining effective working relationships with business unit management. Provides consulting services to management. Serves as in-charge auditor on various audit projects. Works with minimal supervision and is responsible to make and established range of decisions, escalates to manager when necessary and updates manager on a regular basis.

Detailed Responsibilities

- Performs and supervises risk-based integrated audit procedures on scheduled audit projects in accordance with approved risk-based integrated audit programs and in a timely, efficient, and professional manner.
- Demonstrates a working knowledge of internal control concepts for each audit project and provides timely information to the Director, Internal Audit during the audit project regarding weaknesses noted and recommendations for corrective action.
- For assigned audit projects, demonstrates the ability to clearly document and evaluate the internal controls present in the manual and automated systems being reviewed, identifying internal control strengths and weaknesses.
- Prepares and reviews audit work papers that accurately and sufficiently document audit tests performed, in accordance with departmental guidelines (i.e., Audit Procedures Manual (APM)).
- Drafts and reviews written audit reports which accurately describe results of tests performed, the nature of control weaknesses and exposures, expresses an opinion on the adequacy of internal controls and overall procedures and identifies practical recommendations for improvements.
- Completes the Internal Audit self-study program in order to gain advanced knowledge of internal control concepts, audit testing techniques, data processing knowledge, financial, systems and operational audit knowledge and human relations skills.
- Assists external auditors and regulatory auditors in the performance of scheduled audit activities.
- Assists in the performance of a periodic risk assessment of all Company functions in order to recommend appropriate audit projects as part of the audit planning process.
- Develops specifications for automated audit software working closely with Information Systems personnel to satisfy audit software needs.
- Provides internal controls consulting on significant Company initiatives to our customers as requested.
- Performs special reviews/projects as requested.
- Implements computer-assisted audit techniques and practices auditing by exception techniques to improve audit effectiveness and efficiency.
- Supervises work product of one or more internal auditors and one college intern on audit assignments.
- Performs other duties and projects as assigned by management.

.....*Continued on next page*

Senior Information Technology Internal Auditor....Continued from previous page

Western & Southern Financial Group has an immediate opportunity for a Senior Information Technology Internal Auditor.

Selection Criteria.

- Proven experience as an Auditor in a “Big Four” accounting firm or Fortune 500-type company with demonstrated knowledge of internal control concepts and risk-based integrated audit techniques.
- Thorough knowledge of accounting and risk-based integrated auditing.
- Proven ability to develop or adapt risk-based audit programs/procedures on an as-needed basis.
- Proven experience coordinating multiple projects/assignments (3 to 4) simultaneously and completing assigned tasks accurately and on a timely basis. Possesses a strong attention to detail with excellent organization skills. Solid project management with proven experience successfully planning, executing and maintaining a project from start to finish.
- Strong verbal and written communication skills with demonstrated success interpreting and communicating business needs between internal groups and external vendors in a clear, focused and concise manner. Will be expected to provide examples of written audit reports.
- Proven work experience directing others to initiate a recommended course of action to solve a problem or increase efficiency.

Qualifications.

- Bachelor’s degree in accounting, business administration, information systems, computer science or related field of study.
- Computer skills and knowledge of hardware & software required.
- Proficiency in the use of Microsoft Office (Word, Excel, Access, Visio).
- Significant experience auditing automated systems, including mainframes and LAN- and WAN-based applications.
- Significant experience with utilizing automated audit tools, including ACL, Easytrieve Plus, etc.
- Certifications & licenses (i.e. Series 6 & 63, CPA, etc.).
- Certification as a Certified Public Accountant (CPA), Certified Internal Auditor (CIA) or Certified Information Systems Auditor (CISA).
- Willingness to travel 10 to 15% annually.

To find out more or to apply for this position, please contact.

Amy Gellen, Corporate Recruiter

amy.gellen@westernsouthernlife.com

How to Earn and Report CPE

Did you know that ISACA certified members can earn more than 70 FREE CPEs per year!

ISACA certified members have several options to obtain their continuing professional education credits. Several of these choices are listed below with specific instructions.

Journal quizzes. Earn one CPE for each of six [journals](#) per year. 6 FREE CPEs per year

Serving as an ISACA Volunteer. Participate on an ISACA or ITGI board, committee, task force or as an officer of an ISACA chapter, and gain one CPE credit (up to 20 per year) for each hour of active participation. (Consult Qualifying Educational Activities for CISA, CISM, CGEIT and CRISC members.) 20 FREE CPEs per year

Mentoring. Earn one CPE for each hour of mentoring efforts directly related to coaching, reviewing or assisting an individual with CISA/CISM/CGEIT/CRISC exam preparation or providing career guidance through the credentialing process. 10 FREE CPEs per year

TOTAL Possible FREE CPEs for ISACA Certified Members. 36 FREE CPEs per year

How to Report CPEs in your Profile

CPEs are reported annually during the renewal process. CPEs earned in the current year may be entered in your profile once the next year's renewal period opens. Reporting of CPEs can be done online or by submitting the information on the annual renewal invoice.

To update CPE hours through the ISACA website, log on using your personalized log in credentials and follow the steps below.

Click on the **MY ISACA** tab at the top of the page

Click on the **MY CERTIFICATIONS** tab

Click on the **EDIT MY CPE Hours** link

The CPE reporting is located on the My Demographic, Certification CPE and Other Information tab. Scroll to the bottom of the page to view and edit the appropriate CPE fields. If you do not see a CPE section, CPE hours are not being accepted or you are not required to report CPEs yet.

Enter CPE hours – then click SAVE at the bottom of the page

For more information about the specific Continuing Professional Education (CPE) requirements for your certification, please see the following [link](#).

I hope you have enjoyed reading this newsletter. As you can tell from the several job postings in this edition, the word is getting out that firms and recruiters can post their available audit and security-based openings in our newsletter and on our website without charge. Help bring jobs and job seekers together by promoting opportunities at your organization, your fellow ISACA members will appreciate it.

Email me at buky.thorpe@gmail.com and the Webmaster at andrew.selig@53.com with the details of any job opportunities you are aware of. Please note that positions may have been filled or new positions added prior to the newsletter publication, so always see our website for any updates and for complete details.

As always, I would like to hear from any member that is willing to write a brief article for the newsletter that would be of interest to fellow members.

Some examples of articles/content include:

1. A description of a productive or cost-saving audit/security technique that your organization uses
2. Your take and/or opinion on the latest PCAOB standard/update
3. A review of an audit/security tool used by your organization
4. A review of a book that you have read recently that has helped you do your job better
5. Tips and techniques for auditing/securing a particular risk area
6. A summary of an emerging technology being used in your organization and how you are controlling it
7. Live or virtual opportunities to earn CPE credits.

The articles or content can be sent to buky.thorpe@gmail.com.

Finally, you can also reach out to me to let me know what you think of the newsletter; What do you like? What don't you like so much? What other content would you like to see in the newsletter? I would love to hear from you.

Thank you,
Buky Thorpe

About Our Chapter

The Greater Cincinnati ISACA Chapter is a not-for-profit professional association serving the information technology audit, security, and control community. We support the areas of Cincinnati & Dayton, Ohio and Northern Kentucky. The chapter consists of over 400 professionals that represent a cross-section of the public, private, and not-for-profit business sectors at all levels within those industries.

Purpose

To promote the education of individuals for the improvement and development of their capabilities relating to the auditing of and/or management consulting in the field of Information Technology audit and control.

Please visit the chapter website at www.isaca-cincinnati.org to learn more. Connect with other chapter members by joining the Greater Cincinnati ISACA LinkedIn and Facebook groups!

Visit www.isaca.org to learn more about the organization.