March, 2017

CPE Madness in 2Q2017!!!
Fraud, CSX, SOC, Win 10 and VMware

Five great opportunities for local CPE

Thanks to Aaron White for coordinating another experienced group of speakers this quarter. In April we have Sarah Ackerman and Seth Rensberger discussing fraud detection at our monthly meeting. In May we have Daniel Desko discussing SOC report interpretation. At these educational events you will get dinner and some great conversation as well.

Thanks to Lei Zhao for putting together a CSX Fundamentals workshop to be held at NKU on April 6 and 7. For those interested in ISACA's CSX credentials, this is a necessary first step. For those interested in NIST's cybersecurity framework, this is a nice way to learn the intricacies of the framework.

And for two days in May we will have seminars for Windows 10 and VMware auditing. This is another high value, high comfort CPE opportunity for quality local learning. Many thanks to Robert Meyer and Brandon Carey for putting together these

two days of IT audit training.

Date	Speaker	Topic
Tuesday, April 4, 2017	Sarah Ackerman and Seth Rensberger, Clark Schaefer Consulting	Auditing for Fraud: Planning and Approaches
April 6th & 7th	Lei Zhao, First Financial Bancorp	ISACA's Cybersecurity (CSX) Fundamentals Workshop
May 2, 2017	Daniel Desko, Schneider Downs	Interpret SOC Reports Like a Pro
May 4, 2017	John Tannahill, CA, CISM, CGEIT, CRISC	Windows 10 Security & Audit Seminar 8:30 a.m. – 4:30 p.m.
May 5, 2017	John Tannahill, CA, CISM, CGEIT, CRISC	VMware Security & Audit Seminar 8:30 a.m. – 4:30 p.m.

See you at the Original Montgomery Inn!

Robert Ramsay
Greater Cincinnati ISACA Chapter President
rramsay@barnesdennig.com

Greater Cincinnati ISACA Newsletter

Date: April 4, 2017
Location: Montgomery Inn, Montgomery
Time: Networking 5:30; Presentation 6pm; Dinner 7pm.

Topic: Auditing for Fraud: Planning and Approaches
Speaker: Sarah Ackerman (Managing Director at Clark Schaefer Consulting) and Seth Rensberger (Director at Clark Schaefer Consulting)

Sarah Ackerman is the Managing Director at Clark Schaefer Consulting, a regional consulting firm providing IT/Security, Governance/Risk/Compliance, and Accounting/Finance services. Sarah is responsible for the overall engagement quality of all services we provide to clients. She has significant experience providing information security, risk management, IT audit, and other related services within a wide variety of industries and clients.   As a CISSP and CISA, Sarah applies a disciplined approach to managing projects in accordance with industry best practices, with an in-depth knowledge of a variety of frameworks, regulations, and standards.

Seth Rensberger, CPA, CISA, CISM, is a Director at Clark Schaefer Consulting, responsible for overseeing the progress and completion of projects, ensuring that client objectives are met at every step in the process. Seth has significant experience with banking and financial services, including roles as IT Audit Manager, Internal Audit Director as well as VP Internal Audit. He also has consulted with numerous organizations to enhance their financial, systems, and operational processes within a wide selection of industries.

Overview: In today's ever changing business environments, technology is more important than ever. Fraud, while not a new concept, has new challenges. In many audit environments today, IT is separated from Finance. As we discuss fraud, its perpetrators and victims, we also begin to look at how changing your perspective and "thinking like a criminal" can help you determine areas of weakness within your audit program. This presentation discusses how fraud has been impacted with by technological advances and how you can use those same techniques to help deter and detect fraud within your organization.

Please click here to register for the Monthly Meeting.

The Institute of Internal Auditors Cincinnati Chapter
The Information Systems Audit and Control Association Greater Cincinnati Chapter

2017 Annual Scramble
Golf Outing to fund Student Scholarships

2016 sponsors
American Financial Group/Great American Insurance
*TommyWorld enterprises/*Carlisle Tax Service
CHAN Healthcare
Fifth Third Bank
Grant Thornton
Vernovis
Robert Half

Flagg Springs Golf Course
AA Highway Rte 9 and Smith Road Rte 735
California, Kentucky

Friday July 21st $79 per player registered by July 4th

includes green fees, golf cart, refreshments, cookout and prizes
SHOTGUN TEE-OFF 8:30AM
FOURSOME *NOT* REQUIRED/CONFIRMATIONS EMAILED

Player 1 _____email _____
Player 2 _____email _____
Player 3 _____email _____
Player 4 _____email _____
FOURSOME CONTACT NAME_____
FOURSOME CONTACT PHONE_____

TOTAL PAYMENT ENCLOSED: _____
please mail reservation form with check payable to IIA-ISACA Golf
c/o Tyler Regueyra
49 East 4th Street, 6th Floor North
Cincinnati, Ohio 45202

Tyler Regueyra
C: 513-376-1645 | W: 513-333-5117   **Tregueyra@gaig.com**

CSX Fundamentals Exam Review Course

Date/Time: Thursday, April 6th & Friday, April 7th
8:30 – 4:30 (the times may be subject to change, but it will be an all-day program)

Instructor, Lei Zhao, CISA, CSXF

Location: Northern Kentucky University (NKU Digotrium, located in Griffin Hall)

Topic: CSX Fundamentals Exam Review Course

Overview:
Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies (IT). The CSX Fundamental Course is designed for this purpose, as well as to provide insight into the importance of cybersecurity, and the integral role of cybersecurity professionals. Designed as a foundational course, it will also prepare learners for the CSX Cybersecurity Fundamentals Exam.

Attendance at this Course will not guarantee passage of any ISACA offered certification.

By registering you consent to have your name and e-mail address shared with ISACA International. The information will be used in accordance with any applicable laws or regulations governing the collection, receipt, retention and transfer of such Attendee Information.

Cost:
Members: $100, for all ISACA members in good standing as of March 1st

Non-Members: $200. However, if you register to become an ISACA member before March 1st, you will receive the nominal member rate ($25).

Cost of Materials: Included in the cost of registration.

The course/program is designed to cover all of the topic areas necessary to prepare you for taking and passing the CSX certificate exam.

Members and nonmembers alike are welcome to participate in this training program
Click here to register!

2017 Spring Seminar

Course Focus:

Windows 10 Security & Audit Seminar Highlights
This seminar will focus on the security and control issues related to Windows 10 Operating Systems and related technology and infrastructure components.

VMware Security & Audit Seminar Highlights
This seminar will focus on the audit and security issues related to the use of Virtual Machine environments.

Course Outline:

Windows 10 Security & Audit Seminar – May 4, 2017 – 8:30 a.m. – 4:30 p.m. Highlights

Provide an understanding of key Windows 10 security components
Provide and understanding of key Windows 10 security risks

VMware Security & Audit Seminar – May 5, 2017 – 8:30 a.m. – 4:30 p.m.   Highlights

Detailed discussion of VMware Virtual Machine architecture and security components (VMware vSphere)
Detailed discussion of VMware ESXi and vCenter security and control features
Audit objectives and checklists for the ESXi and vCenter environments

Learning Objectives:

At the completion of this course, attendees should have information related to:

Windows 10 Operating System Concepts
Windows10 Security Overview
Understanding Enterprise Components and Infrastructure
Understand Windows Firewall and advanced security features
Securing Windows 10 operating system environment using security baselines
Top 10 Windows 10 Security Risks
Security Tools & Techniques

VMware Security & Audit Concepts
VM Concepts (based on VMware technology)
VMware ESXi Server Audit
VMware vCenter Audit
Security and Audit Tools & Techniques

Instructor: John Tannahill, CA, CISM, CGEIT, CRISC

J. Tannahill & Associate

Click here to register!

Job Opportunities

Company: TriHealth
Position: Lead IT Audit Manager

Principle Accountabilities:

The Lead IT Audit Manager is responsible for conducting independent, objective IT audits in accordance with IIA standards; ensuring effective communication to Management of results/recommendations to assist in achievement of business objectives; and serving as a resource to the audit team during execution of IT procedures on operational, financial or integrated audits, where applicable.
The Lead IT Audit Manager works closely with the IT Audit Manager and Director Internal Audit to develop and execute a comprehensive, risk-based audit program focused on:

- Adequacy and propriety of internal and operational controls
- Assessment of efficiency and effectiveness of processes and systems
- Identification of performance improvement and best practice opportunities. Audit scope includes, but is not limited to, IT general control reviews, application controls reviews and information security assessments as well as client assistance and projects as requested by Management.

Knowledge of the following concepts/framework:

- IT and IS governance (policies and procedures, ITIL) and processes
- IT general and application controls
- SDLC methodology; data governance and integrity
- IS security and related frameworks (i.e. HITRUST, NIST, COBIT 5.0, ISO, DRP, BCP)
- IT risk assessment and management processes (i.e. security, vendor/third party, hosted systems);
  and Data analytics.

Job Requirements:

Minimum Education: Bachelor's Degree

Field of Study: Accounting Field of Study (Other): Information Systems, Finance

Contact Information:

For inquires or to apply, contact Bruce Miller at Bruce_Miller@trihealth.com or 513-703-2253.
To apply, go to http://www.trihealth.com/discover-trihealth/your-trihealth/careers and use
Req #115884.

Job Opportunities

Company: The Cincinnati Insurance Company
Position: Senior IT Internal Auditor
Location: Fairfield, OH

About the Company :

The Cincinnati Insurance Company, a subsidiary of Cincinnati Financial Corporation, stands among the nation's top 25 property casualty insurer groups, based on net written premiums. Our commitment to the independent agency system began in 1950 and is our company's core strength and competitive advantage. We excel by offering agents and policyholders a local presence, unparalleled claims service, loss control consultation services, work-saving technology initiatives, and competitive products, rates and compensation. Selected associates receive a comprehensive salary and benefits package, including a matching 401(k). Equal Opportunity Employer.

Job Description:

Our Internal Audit department is seeking a talented, experienced and motivated senior IT internal auditor to exert meaningful influence over our IT risk assessment and auditing processes. The selected professional's audit scope will include our large, centralized IT department, which manages a complex technology environment and is subject to a variety of federal and state level regulations. Our Internal Audit department reports through the Internal Audit Officer directly to the CEO (administratively) and the Audit Committee of the Board of Directors (functionally).
Little to no travel is required.

Specific Responsibilities:

- researching and understanding our company's IT-related processes, data and systems
- developing and preparing IT audit plans
- conducting IT audits, including Sarbanes-Oxley general IT controls testing
- making innovative recommendations for improving efficiency, effectiveness and internal control
- preparing and presenting reports to management
- using data mining and interrogation tools and techniques
- performing special projects
- participating in overall Internal Audit risk assessment and planning
- building productive working relationships with peers, reviewers and management
- interacting with and assisting our external auditors from Deloitte & Touche LLP
- working with other team members to develop best practices and a base of knowledge for future use
- pursuing and maintaining one or more of a list of selected professional designations
- participating in professional organizations and opportunities to enhance personal and professional growth
- establishing mentoring relationships within Internal Audit and throughout the company
- staying current with emerging issues affecting the IT auditing profession
- seeking opportunities to improve technical and management skills through continuing education, seminars, etc.

Job Requirements:

Experience that includes at least two years with one or more of the following is required:
- IT auditing for a professional services (ideally Big 4) firm
- performing IT control audits, including application and infrastructure, information security, and change management
- conducting and supporting external audits of consolidated financial statements in accordance with AICPA and PCAOB auditing standards
- performing detailed security reviews of various IT environments, including Oracle, DB2, SQL, PeopleSoft, SAP, Unix, and Windows Active Directory
- performing data analytics utilizing ACL, MS Access, Excel (with pivot tables, vlookups, hlookups, and filters) and/or SAS

Job Requirements (Continued):

- using programming languages such as .Net, Java, C# and database management systems such as MS SQL, DB2, and Oracle.
- testing the design/implementation and operating effectiveness of internal controls
- performing SSAE16 (SOC1 or SOC2) planning, testing and reporting

To be considered, candidates must also have the following qualifications:

- bachelor's degree in information systems, computer science, information technology, data analytics, accounting, insurance or a related field that promotes analytical thinking or specific knowledge of our company's business
- undergraduate GPA of 3.0 or better
- commitment to integrity and ethical behavior
- excellent oral and written communication skills
- professional, business-like demeanor
- strong interpersonal and relationship building skills
- ability to work both independently and as part of a team with professionals at all levels
- ability to prioritize tasks, work independently on multiple assignments and manage ambiguity
- ability to think critically, objectively, and analytically with an appropriate level of skepticism
- ability to determine control objectives, identify control procedures that address those objectives, and assess the adequacy of those procedures
- ability to manage project work to meet budgets and agreed timelines
- flexibility to work extended hours when necessary
- working familiarity with various application systems (such as PeopleSoft and SAP), operating systems (such as Windows, AIX and z/OS), network management technologies (such as Active Directory and LDAP), and database management systems (such as MS SQL, DB2, and Oracle)
- at least a basic knowledge of internal control frameworks such as COBIT and COSO

Candidates may be further differentiated based on the following:

- master's degree in a technology or business-related field
- extraordinarily relevant prior work experience
- pertinent professional designations (such as CISA, CISSP, PMP, CPA, CIA, or CMA)
- strong professional references
- Experience with TeamMate and data mining/analysis tools, including ACL or SAS

To find out more or to apply for this position, contact :
Stephanie Kolodzjieski, Corporate Recruiter
Stephanie_Kolodziejski@cinfin.com
513.603.5380

Company: Clark Schaefer Consulting
Position: IT Audit Consultant
Location: Cincinnati and Columbus, OH

About the Company :

Clark Schaefer Consulting is an established professional services firm associated with Clark, Schaefer, Hackett CPAs, one of the top public accounting firms in the region. As a firm, we have been performing consulting services within the Cincinnati business community and surrounding area for 10 plus years and prior to that time, as part of our CPA firm affiliate for 75 years. Due to increased demand from our clients and the outlook for our services in2016, we are currently seeking information systems professionals as consultants for full-time, salaried positions at our Cincinnati and Columbus locations.

By design, we serve a diverse set of regional clients ranging from the Fortune 1000 to privately held corporations. As a regionally based firm, we believe we offer an ideal work-life balance for those who enjoy client service work, but want to avoid the extensive travel and time requirements of the national firms. If you are interested in having
diversity in your work experience; expanding your personal knowledge base; and being part of assisting the top companies in your community as they improve their operations, this is a great opportunity for you.

Job Description:

Based upon skills and experience, the successful candidates will join a team of professionals performing a range of IT audit, internal audit, and other related information system services. These services could include IT audits, process improvement, policy/procedure development, disaster recovery reviews, network architecture assessments, IT risk assessments, application control reviews, systems implementation assistance, and a wide variety of other technology related services. For more details on specific potential projects, please visit our website for a listing of the services we typically perform which might fit your background and skills.

Primary Responsibilities:

• Provide IT auditing and other technology related services to fulfill individual engagement requirements.
• Assist with the development of project plans, methodologies and client proposals as needed.
• Maintain a consistent level of chargeable hours to fulfill annual billable expectations.
• Travel to client locations as required throughout the year.
• Maintain a commitment to continuing education and professional development.

Education & Experience:

• Bachelor's degree in technology or related field.
• Relevant IT audit or information technology experience.
• Professional certifications such as CISA, CISM, CIA, CISSP are a plus.
• Excellent written and verbal communication skills.
• Ideal candidate would have 1-4 years of experience.
To Apply:

Please e-mail your resume, cover letter and salary history to recruiting@clarkschaefer.com . For more information concerning our Firm and services, please visit www.clarkschaefer.com.

Company: Fifth Third Bank
Position: IT Audit Staff or Senior
Location: Cincinnati, OH

About the Company :

Fifth Third Bancorp is a diversified financial services company headquartered in Cincinnati, Ohio. As of December 31, 2014, the Company had $139 billion in assets and operated 15 affiliates with 1,302 full-service Banking Centers, including 101 Bank Mart® locations, most open seven days a week, inside select grocery stores and 2,638 ATMs. Fifth Third operates four main businesses: Commercial Banking, Branch Banking, Consumer Lending, and Investment Advisors.

Job Description:

Conducts IT governance, infrastructure & support, integrated business process and application audits for various lines of business/functional areas within the Bancorp. Primary responsibilities include performing IT audit activities in the planning, fieldwork, reporting and wrap-up phases in accordance with established standards. Seniors will be responsible for supervision of assigned staff personnel (typically leads 1-2 staff per audit) and ensuring that the execution of all audit phases is conducted in accordance with established standards.

Specific Responsibilities:

• Ensure execution of all audit activities in the planning, testing, reporting and wrap-up phases
  are in compliance with the Audit Division's methodology /standards and within the timeframes to
  support department metrics
• Challenge, validate and execute test strategies to determine the effectiveness of internal
  controls and compliance with regulations; incorporating appropriate tools, techniques and technology.
• Establish, foster and maintain working relationships with peers and supervisory management
  within the business line and cross-functional lines to support an effective workflow, continuous
  communication and value to customer.
• Participate in departmental processes and initiatives that promote team effectiveness, employee
  engagement and resource development.
• Attend Bancorp sponsored and other training to build industry knowledge and technical capabilities.
Additional Responsibilities for Senior Auditor:
• Develop audit scope and objectives, risk and control assessments, work programs, and other
  deliverables of audit work.
• Delegate responsibilities to audit staff members, and review audit work papers providing coaching feedback
on   work prepared by staff auditors.
• Communicate information to management through presentations and internal audit reports.
Job Requirements:
• Bachelors degree required; Computer Science or Management Information Systems preferred. Other
related academic majors (e.g., Accounting or Audit) should be accompanied by relevant experience in IT or
IT Audit.
• Encouraged to pursue CISA certification and/or related professional certifications such as
  CISSP, CPA or CIA.
• IT or Financial services industry experience and/or public accounting firm experience desirable.
• Proficient with MS-Windows and other related PC applications. Possess the desire and ability
  to learn mainframe and distributed applications as well as automated data analysis tools and Techniques
• Strong written and verbal communication skills required.
• Senior candidates will demonstrate coaching, leadership and project management skills.
To find out more or to apply for this position, contact :
Reese Gable, Talent Acquisition Consultant
Reese.Gable@53.com
513-534-7527

Company: Fifth Third Bank
Position: Senior IT Risk Analyst (one openings)
Location: Cincinnati, OH

About the Company :

Fifth Third Bancorp is a diversified financial services company headquartered in Cincinnati, Ohio. As of December 31, 2014, the Company had $139 billion in assets and operated 15 affiliates with 1,302 full-service Banking Centers, including 101 Bank Mart® locations, most open seven days a week, inside select grocery stores and 2,638 ATMs in Ohio, Kentucky, Indiana, Michigan, Illinois, Florida, Tennessee, West Virginia, Pennsylvania, Missouri, Georgia and North Carolina. Fifth Third operates four main businesses: Commercial Banking, Branch Banking, Consumer Lending, and Investment Advisors. Fifth Third also has a 22.8% interest in Vantiv Holding, LLC. Fifth Third is among the largest money managers in the Midwest and, as of December 31, 2014, had $308 billion in assets under care, of which it managed $27 billion for individuals, corporations and not-for-profit organizations. Investor information and press releases can be viewed at www.53.com. Fifth Third's common stock is traded on the NASDAQ® Global Select Market under the symbol "FITB."

Job Description:

This position is responsible for implementing information technology risk management strategies identified by the IT Risk Manager. In this role, the Senior IT Risk Analyst will be assigned overall responsibility for key areas and will have accountability for proper planning, prioritization and execution of supporting IT risk responsibilities. This position is responsible for hands-on execution of control/risk assessments and the development of control enhancement recommendations.

Specific Responsibilities:

- Support the IT Risk Manager in the execution of responsibilities to conduct risk assessments, implement self-assessment programs, perform technical research on risk topics, and other activities that support risk management goals for the IT Division. Some of the primary responsibilities include:

- Support the IT Risk Manager on the implementation of information technology risk management strategy and operating priorities.

- Support the integration of the IT Risk Management practices into key Information Technology and business areas.

- Build effective relationships with key individuals who own and support processes you are responsible for evaluating, including the appropriate line-of-business risk managers.

- Perform ongoing planning and prioritization of key projects and activities to ensure that resources are applied to the most critical areas. Communicate with the IT Risk Manager, as needed, to ensure proper prioritization and management of workload.

- Participate on projects and ensure that key IT risks are being adequately addressed. Coordinate with project managers to ensure that issues are identified, action plans are in place and that PLC requirements are being met.

- Perform risk assessments on key IT processes or assets, identify vulnerabilities and propose solutions to mitigate risk. Perform due diligence and risk assessments on IT service providers.

- Work with IT areas in developing an effective self-assessment process for proactively identifying risks associated with processes, applications and technical infrastructure components.

- Support compliance with applicable regulations, which include, but is not limited to the following: the FDIC Improvement Act, the Sarbanes-Oxley Act of 2002 and the Gramm-Leach-Bliley Act of 1999.

- Support the resolution of Internal Audit, regulatory, or Risk Management related issues that could impact the confidentially, availability or integrity of data or processes.

- Create effective risk assessment documentation supporting work performed, including formal communication on risk assessment results. Be able to deliver effective presentations to management on summary of work performed and findings.

Job Requirements:

Two to four years of information technology experience required. Desired experience should include a foundation in IT security and controls. While experience in a number of IT disciplines may provide a solid framework for this position, hands-on results from performing IT risk assessments, information security consulting or IT audits are most beneficial. At least one relevant technical or professional certification, such as CISA or CISSP, is required.

Bachelor's degree required, preferably in computer science or information systems. Must possess excellent written and verbal communication skills, with a proven track record of interacting effectively with end-users and technology professionals. Able to work on multiple projects concurrently, manage time effectively and require minimal supervision in the execution of IT Risk Analyst responsibilities. Must possess strong analytical capabilities and have a desire to learn new things. Less than 10% travel required.

To apply for this position, visit https://www.53.com/careers/index.html

Requisition #: 146609

To find out more, contact :

Justin Hedric, VP – Senior IT Risk Manager

Justin.hedric@53.com

513.534.8648

CGEIT Review Manual 7ᵗʰ Edition

ISACA

The *CGEIT® Review Manual 7ᵗʰ Edition* is designed to help individuals prepare for the CGEIT exam and understand the responsibilities of those who implement or manage the governance of enterprise IT (GEIT) or have significant advisory or assurance responsibilities in regards to GEIT. It is a detailed reference guide that has been developed and reviewed by subject matter experts actively involved in GEIT worldwide.

The *CGEIT® Review Manual 7ᵗʰ Edition* offers any easy-to-use format, organized to assist candidates in understanding essential concepts and studying for the exam following the CGEIT job practice areas . The manual also features commonly used terms and definitions, self-assessment questions and answers and resources for further study. It can be used alone or in conjunction with other CGEIT exam prep publications or review courses. The manual can also be used as a desk reference for GEIT professionals.

ISACA Members and Non-Members can purchase a hard copy or download the eBook at the following prices:

Members- Downloadable Book Format for US $85.00 each

Non-members—Join ISACA today to get your $85.00 Book,

or purchase the book for US $115.00 each.

How to Earn and Report CPE

Did you know that ISACA certified members can earn up to 72 FREE CPEs per year!

ISACA offers opportunities to earn CPE through participation in a variety of programs and events. Several of these choices are listed below with specific instructions.

Webinars and Virtual Conferences: Up to 36 free CPEs per year. CPE quizzes are for members only.

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: 72 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.

Dear Cincinnati ISACA member,

As mentioned by Robert, we have several exciting upcoming events announced which all include the ability to earn CPE. For information on our future events, visit the events page on our chapter's website:

http://www.isaca.org/chapters5/Cincinnati/Events/Pages/default.aspx

In order to better serve our chapter, we are looking for more convenient ways to communicate to our members. Any feedback on current communication methods or possible improvements are always appreciated.

Thank You!

Kyle Schutte, CISA
VP of Communications

Founded in 1973, the Greater Cincinnati ISACA Chapter is a not-for-profit professional organization serving IT Audit, Risk, Security, and Governance professionals in the Greater Cincinnati market. The chapter consists of over 450 professionals that represent a diverse mix of public, private, and not-for-profit business sectors at all levels within those industries. Members of the Greater Cincinnati ISACA Chapter have the opportunity to earn 36 CPE hours annually through various events and seminars. The greatest asset to the Greater Cincinnati ISACA Chapter is its membership community.

Purpose
To promote the education of individuals for the improvement and development of their capabilities relating to IT Audit, Security, Risk, and Governance 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 group.

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