ISACA
Trust in, and value from, information systems
Greater Cincinnati Chapter

March, 2015

Welcome...

Greetings Fellow Greater Cincinnati ISACA Members,

INSIDE THIS ISSUE

It looks like spring is finally here. At our March meeting, Sayontan Basu-Mallick provided an excellent presentation on recent and proposed changes to SOC reports impacting service organizations and user organizations. See our website for his presentation. The CPEs for this meeting have been uploaded to ISACA's web site. If you have not already done so, you can logon and apply this CPE to your certification(s).

Our programs committee has organized our April 7, 2015 meeting. Registration is available on our web site. Sarah Ackerman from Clark Schaefer Consulting will be giving a presentation on Social Media as a Vector for Cyber Crime. Please see page 2 for the meeting details.

Our education committee has organized our spring seminar. The price will be the same as for our fall seminar. Ken Cutler, a Senior Teaching Fellow, specializing in Technical Audits of IT Security and related IT controls, will be presenting training on CyberAudits of Identity & Access Control Management. Registration is available on our web site. Please see page 3 for more details about this training opportunity.

The 2015 ISACA membership renewal period is in progress. The Greater Cincinnati ISACA Chapter Board has set a goal of achieving an 87% renewal rate by April 30, 2015. Thanks to all renewed members, our Chapter's renewal rate is currently at 82.2%. If you haven't done so, please renew your ISACA membership with us by April 30, 2015.

We can't celebrate without YOU. To show the Chapter Board's appreciation to all Chapter members, if the Chapter meets the renewal goal, members will be eligible for receiving special prizes during the September meeting.

I encourage you to join our LinkedIn group if you are not a member. I post training opportunities in the group that I learn about from other ISACA chapters. This will give you additional options for earning CPEs. If you know anyone in the audit or security profession who might benefit from ISACA membership, please invite them to one of our meetings or put them in touch with our board so they can find out more!

Do you have any coworkers that are not receiving this newsletter and would like to? If so, have them send an e-mail to our Newsletter Editor, Buky Thorpe (buky.thorpe@gmail.com) and request to be included on the e-mail distribution list. If you are interested in becoming a member of the chapter, please contact our VP of Membership, Mike Smith (mrsmith@gaig.com). As a reminder, our website is the best place to learn about upcoming events and available job opportunities in the Greater Cincinnati ISACA area! Check it out at: www.isaca-cincinnati.org! As always, I am happy to hear any comments you have, so feel free to e-mail me at rkrickisaca@gmail.com.

Russell Krick, CISA,
Greater Cincinnati ISACA President

Social Media as a Vector for Cyber Crime

Speaker: Sarah Ackerman, CISSP, CISA, CICP, Director of Technology for Clark Schaefer Consulting
Date & Time: Tuesday, April 7, 2015, 5.30pm
Location: The Original Montgomery Inn, Montgomery, OH

Overview
As social networking becomes more a part of our daily lives, individuals find this technology an attractive vehicle to perpetrate cyber crimes. Anonymity provided via social networks allows a person to easily portray another user's identity. Cyber criminals exploit such vulnerabilities to steal user credentials, which in turn can be used to breach a company's network infrastructure. This presentation will focus on the following: Process – Various steps and methods used to carry out cyber attacks; Effect (or result) – Possible ramifications of a cyber attack to a company/network; and Safeguard – Demonstrate methods individuals can use to limit cyber attacks and identify possible threats.

About the Speaker
As the Director of Technology for Clark Schaefer Consulting, Sarah Ackerman provides the Firm with extensive experience and knowledge regarding information security, IT audit, and other technology and control related services. Sarah's work in security operations has resulted in a proven track record of success in identifying system control weaknesses, protecting information assets, and leading clients to successful organizational changes. She is well versed in internal controls and has successfully served in a variety of roles including consulting, risk management, and internal audit.

Cincinnati ISACA members and non-members can register by using this link .
For those who prefer to pay at the door, please select that option when you register at the link above.

2015 Spring Seminar

Cyber Audits of Identity & Access Control Management

Summary:

The road to reliable internal control and CyberSecurity compliance can be very treacherous, full of potholes and rocks and many forks to ponder. Compliance requirements come from all directions, shapes, and sizes not to mention heightened attention to the protection of payment card data, personally identifiable information (PII), identity theft, and security breach disclosure legislation. Logical access controls represent the single most significant safeguard to protect valuable data from unauthorized access and the most common area of important findings by internal and external auditors.

This seminar will provide a framework for consistent and effective auditing of logical access controls. Case studies will be used to demonstrate real examples of common access controls and data collection methods for operating systems, database servers, and other software environments, emphasizing free and/or low-cost audit software procedures. Attendees will receive sample work programs and checklists that can be used to perform effective logical access audits in any context.

About the Instructor : The instructor, Ken Cutler, CISA, CISSP, CISM is a Senior Teaching Fellow, specializing in Technical Audits of IT Security and related IT controls. He is the President and Principal Consultant for Ken Cutler & Associates (KCA) InfoSec Assurance, an independent consulting firm delivering a wide array of Information Security and IT Audit management and technical professional services. He is also the Director – Q/ISP (Qualified Information Security Professional) programs for Security University.

An internationally recognized consultant and trainer in the Information Security and IT audit fields; he is certified and has conducted courses for the CISSP, CISM, CISA, and CompTIA Security+. In cooperation with Security University, he recently was featured in two full length training videos on CISSP and Security+. Ken was formerly Vice-President of Information Security for MIS Training Institute (MISTI), Chief Information Officer of Moore McCormack Resources, a Fortune 500 company. He also directed company-wide IS programs for American Express Travel Related Services, Martin Marietta Data Systems, and Midlantic Banks, Inc. Ken has been a long-time active participant in international government and industry security standards initiatives, including: The President's Commission on Critical Infrastructure Protection, Generally Accepted System Security Principles (GSSP), Information Technology Security Evaluation Criteria (ITSEC), US Federal Criteria, and Department of Defense (DOD) Information Assurance Certification Initiative. He is a prolific author on many information security topics.

Date & Time: Thursday, May 28th and Friday, May 29th, 2015 from 8:30am - 4:30pm

Location: Montgomery Inn Boathouse: 925 Riverside Drive, Cincinnati, OH 45202

Free Parking is available . Continental Breakfast and lunch will be provided on both days. Montgomery Inn is noted for its food!

Tuition $500 for members of ISACA ($600 for non-members) until April 30, 2015

$600 for members of ISACA ($700 for non-members) after April 30, 2015

Please register early! To ensure an interactive and comprehensive course, space has been limited to 40 participants.

Registration: Please click on this link to register or find out more details about the seminar.

Cancellations:

Attendees will not be registered or 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, an individual may attend in your place with communication of the substitution.

For enrollment, questions, or cancellations, email (joseph.lairson@hill-rom.com) or Holly Johnson (hajohnson@gaig.com).

Upcoming Webinars

ISACA Members can earn free CPEs by attending a 60 minute ISACA webinar. Increasing your knowledge of important and relevant IT and IS topics is just a bonus.

Here are the upcoming Webinars:

Topic: **86% of Data Breaches Miss Detection, How Do You Beat The Odds?**

Speaker: **Troy Kitch, CISSP**

Sr. Principal Director, Product Marketing, Security Software, Oracle

Melody Liu

Sr. Principal Product Manager, Oracle Database Security

Date: Thursday, 9 April 2015

Time: 12PM EST / 11AM CST / 9AM PST / 17:00 UTC

Overview: Information security is simply not detecting the bad guys, according to the Verizon Data Breach Investigations Report. Antivirus, intrusion detection systems, and log review all pick up less than 1% of data breach incidents. In fact, very few companies do proactive monitoring and those that do are simply troubleshooting problems they already know about. The result is that 86% of data breach incidents were ultimately detected by someone other than the victimized organization; an embarrassing statistic. Only 35% of organizations audit to determine whether privileged users are tampering with systems. As well, for nearly 70% of organizations, it would take greater than one day to detect and correct unauthorized database access or change. With average data breach compromises taking less than a day, the majority of organizations could lose millions of dollars before even noticing. Join Oracle and learn how to put in place effective activity monitoring including:

- Privileged user auditing for misuse and error
- Suspicious activity alerting
- Security and compliance reporting

Click on this link to find out more details or to register

You can register ahead of time for up to two new webinars each month; presented live by subject matter experts and accessible to you free of charge. Enjoy interaction with the presenter in the live format or view the entire webinar after the event on your schedule. These brief, yet extremely informative, web-based, education sessions are available in ISACA archives for up to a year after the event.

CPE Opportunity

Join COSO Chairman, Bob Hirth, for a Complimentary Breakfast and discussion on the revised COSO Framework

You're invited to join IIA, FEI, ISACA, Robert Half, and Protiviti on Thursday, May 21, for a complimentary breakfast with Bob Hirth, Chairman of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Bob will discuss the Updated COSO Framework, including lessons learned, its impact on your organization, and plans for the future. The session will conclude with a distinguished panel including, among others, Dr. Sandra Richtermeyer, COSO Board Member and Chair of the Department of Accountancy at Xavier University, and moderated by Michael Thor, Managing Director at Protiviti. All qualified participants will also receive two CPE credits. Don't miss the chance to discuss the Updated COSO Framework with this panel of experts. Registration is now open.

Date: Thursday, 21 May 2015

Location: The Cintas Center at Xavier University
1624 Herald Avenue
Cincinnati, OH 45207
Conference Room: Banquet "B"

Agenda: **7:15 – 8:00 a.m.**
Breakfast and Networking
8:00 – 10:00 a.m.
Presentation and Panel Discussion

CPE: 2 credits

Cost: Complimentary

ISACA 2015 Certification

Registration for the June 2015 ISACA certification is now open. Registration is open for the following exams:

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)

	Member	Non-Member
Online* final registration deadline fee	$490	$675
Mailed/faxed final registration deadline fee	$565	$750

Important Dates:

Exam date: *June 13, 2014*

Final registration deadline: *April 10, 2015*

To register or find out more details visit this link

*Online fees reflect a savings of US $75 off the registration rate for mailed or faxed registrations!

The online registration process will enable you to register for an exam, and purchase study aids and an ISACA membership, which will immediately provide significant exam-related discounts. The final step of the process will enable you to pay online using a credit card, or indicate that payment will follow by check or wire.

Job Opportunities

Company: Fifth Third Bank
Position: Senior IT Risk Analyst
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.

…..Continued from page 7

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

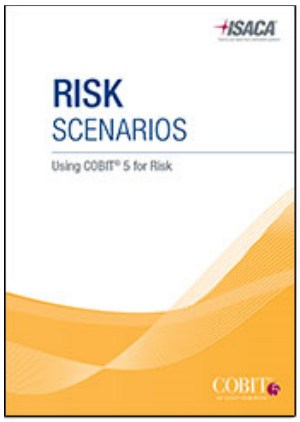
513.534.8648

Risk Scenarios Using COBIT 5 for Risk

Risk Scenarios Using COBIT 5 for RISK is now available!

Scenario analysis has become an important component of enterprise risk management. Risk scenarios are recognized as powerful tools that help risk professionals prepare for the unexpected. Risk Scenarios Using COBIT 5 for Risk provides:

- Detailed guidance on the development of IT-related risk scenarios
- Guidance on how to use COBIT 5 for Risk to solve for current business issues
- An overview of risk concepts and how the COBIT 5 enablers can help in risk management activities



The accompanying toolkit contains interactive risk scenario templates.

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

Members- Download your free PDFs here

Non-members—Join ISACA today to get your Free PDF, or purchase the pdfs for US $60.00 each.

To download or purchase a copy of Cobit 5, members and non members can go nere.

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.

In today's hectic and challenging business environment, where we are faced with so many different sources of information, competing for our attention, it is increasingly challenging to create a relevant newsletter that members have the inclination to read. As we begin this new chapter year, one of our goals is to provide content that is the most beneficial to you our members and that is where you come in.

With over four hundred members in a broad range of industries, we have a vast source of experience and knowledge to harness within our chapter. If you have a brief article that may be of interest to your fellow members, I would like to hear from you.

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.

These are just a few ideas and not meant to be all inclusive. If you have any ideas for other content you'd like to see, let me know. The articles or content can be sent to buky.thorpe@gmail.com.

Finally, please 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? I would love to hear from you.

Thank you,
Buky Thorpe, 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.