



www.isaca-centralohio.org



IT Controls & Assurance

Sarbanes-Oxley Act has emphasized the need for CEOs and CFOs of corporations to certify the existence and effectiveness of internal controls over financial processes. Verification of Internal controls over Information Technology deserves equal importance in corporations with the pervasiveness of technology solutions. IT assurance would require effective design and operation of automated internal controls. Audit assurance would validate controls through formal audit and assessment of IT controls.

ISACA has just published the **ITAF (IT Assurance Framework)**- A Professional Practices Framework for IT Assurance. ITAF details three categories of standards: general, performance and reporting. These standards are mandatory and are based on ISACA IS Auditing Standards. ITAF also provides auditing guidelines based on COBIT and also indicates various tools and techniques for IT assurance. ISACA members can download a free copy of ITAF from ISACA website (www.isaca.org). This document will be of great help to IT audit and assurance professionals.

During the April luncheon meeting Steve Romig of OSU presented on Data Breaches and the impact of Ohio State Law on data breach notifications. The presentation was quite informative and interesting. We thank Steve for this.

This month I will be presenting on 'IT Governance'. Governance or Board-level oversight of Enterprise IT has attracted lot of attention because of the dependence on IT by business for operations and the huge investments made in IT. Regulatory compliance issues and risk management are also drivers for governance of enterprise IT. ISACA and ITGI realizing the trend, have promoted IT Governance as a profession. ISACA has introduced a new certification CGEIT (Certified in the Governance of Enterprise IT) to certify IT Governance professionals. Come and learn more about the topic, the profession and the certification.

The nominations for the Officers and Directors of the Board for 2008-2009 ISACA year, are on our website. Please vote for your candidates. The new Board will take charge on June 1, 2008. On behalf of the current Board of Directors of ISACA Central Ohio Chapter, I would like to thank the Officers, Directors, Committee Chairs and every one of you, members, and the supporting organizations for the great cooperation and support that you extended to us during the ISACA year 2007-2008.

Joseph Ponnoly, CISM, CISA, CISSP
President, ISACA Central Ohio Chapter

Chapter Board

President: Joseph Ponnoly, CISM, CISA, CISSP (Resources Global Professionals)

Vice President: Brian O'Brien, CISA (The Ohio State University)

Secretary: Ann Atkinson, CISA (JP Morgan Chase)

Treasurer: Mike Brady, CISA (Clifton Gunderson LLP)

Directors:

Melissa Justice, CISA (State Auditor's Office)

Michael Kirk, CIA, CISA (CitiGroup/Bisys)

Jason McKittrick, CISA, CISSP (Nationwide Financial)

Rich Ridewood, CPA, CISA, CISSP (BWC, State of Ohio)

Matt Schondel, CISA (Alliance Data)

Chuck Imwalle, CPA, CISA, PMP (Crowe Chizek)

Ryan Houk, CISA (AEP)

Committee Chairs:

Membership: Jim D'Innocenzo, CISA (OSU)

Programs: Mike Kirk, CISA (CitiGroup)

Arrangements: Melissa Justice, CISA (State Auditor's Office)

Audit: Greg Mason, CPA, CISA (State of Ohio)

Education: Rich Ridewood, CPA, CISA, CISSP (BWC, State of Ohio)

Website: Ryan Houk, CISA (AEP)

Finance & Academic Relations: Brian O'Brien, CISA (OSU)

Corporate Relations: Lynne Karla, CISA, CIA (Huntington Bank)

Social Committee: Matt Schondel, CISA (Alliance Data)

CISA: Chuck Imwalle, CPA, CISA (Crowe Chizek)

CISM: Joseph Ponnoly CISM, CISA, CISSP (Resources Global Professionals)

Newsletter Editor:

Nelia Pozzuoli, CISM, CISA, CISSP (Resources Global Professionals)



www.isaca-centralohio.org



Chapter News & Events:

Upcoming Chapter Luncheon Meetings (Please register early online at www.isaca-centralohio.org)

Luncheon Meeting on Thursday, May 8 from 11:30 A.M. to 1:30 PM

Topic Summary:

IT Governance- Principles & Best Practices and an overview of CGEIT certification

Synopsis:

ISACA has introduced a new certification-- CGEIT: Certified in Governance of Enterprise IT-- to promote IT Governance as a profession for IT Leaders and Managers. CGEIT brings into focus the importance of IT Governance in organizations. IT Governance is based on the need for IT to provide business value and adequate ROI on IT investments. CGEIT exam and certification are focused on professional knowledge in five critical domains of IT Governance. Certified IT Governance Professionals will be competent to create and implement IT strategies, manage IT resources and implement Program and Portfolio Management with performance measures, based on an IT Governance framework.

This presentation will focus on:

- What IT Governance means and why it is important for organizations
- The five pillars of IT Governance
- The principles and best practices of IT Governance and Case Studies
- COBIT as an IT Governance framework
- VAL-IT framework for IT investments
- How COBIT maps to other standards and frameworks: COSO, ITIL, ISO 27002, CMMI, PRINCE2, PMBOK and TOGAF.
- Auditing IT Governance
- IT Governance Profession, CGEIT exam and certification requirements.

Speaker Bio:

Joseph Ponnoly, CISM, CISA, CISSP (Resources Global Professionals)

Joseph is a Management Consultant with Resources Global Professionals (www.resourcesglobal.com) working in the area of Information Management, specifically Governance, Risk & Controls consulting and advisory services. His areas of expertise include Information Security & Privacy, IS Audit, IT Governance, Regulatory compliance, Fraud management, Business intelligence and DSS and Organizational Knowledge Management.

Joseph has been President of ISACA Central Ohio Chapter during 2007-2008. He holds CISM, CISA and CISSP certifications and has MBA Finance from Ashland University, and Masters in Physics from Kerala (India). He is also pursuing Ph.D. in Computer Information Systems from Nova Southeastern University.

Luncheon Location:

La Scala **Italian Bistro**; 4199 W Dublin-Granville Rd, Dublin, OH (Directions: 670 W to 315 N, Exit on 161 toward Worthington, Turn Left on 161/Dublin-Granville Rd, Turn

Left on Shamrock Blvd, Parking is all around restaurant.)

(Menu will be: Italian Salad, Ciabatta Bread, Homemade Lasagna, Baked Chicken, Meatballs, Garlic Smashed Potatoes, Italian Green Beans, and Spumoni Ice Cream)

Cost is \$15 for members and \$20 for non-members. **NOTE: Beginning January 1, 2008, price for luncheons remained \$15/\$20 for those registering via the website before the deadline; however, the price for non-registrants at the door is \$25 for members and \$30 for non-members.**

Please note that voting of the new Chapter Board for next year will take place at this meeting.

Please note that we are now accepting online payment via PayPal for the luncheon meetings. Please just follow the steps on the website when registering. We are sorry for the inconvenience, but at this time we are not allowing refunds; however, if you pay via PayPal and need to cancel for any reason, you will be allowed to apply the money towards the following month's meeting. We will still be accepting cash or check at the door.

Please RSVP before noon on Monday, May 5, via the ISACA Central Ohio Chapter website <http://www.isaca-centralohio.org/meeting.htm>

Melissa Justice
ISACA Central Ohio Chapter,
Arrangements Chair
(614) 397-9678

Announcements

New ISACA Year starts on June 1, 2008, when the new Board will take charge. There will a summer break during June, July & August and the Chapter meetings will resume in September 2008.



www.isaca-centralohio.org



Certification Update

CGEIT (Certified in Governance of Enterprise IT)



New IT

Governance Certification Offered! ISACA offers a new certification program to recognize professionals for their knowledge and application of IT governance principles and practices. Grandfathering for those eligible is available until October 31, 2008. The first exam will be held in December 2008.

Education



Next ISACA e-symposium is scheduled for

27 May 2008 Data Protection / Data Security

Earn 3 CPE credits.

Register at

www.isaca.brighttalk.com

All previous e-symposia are recorded and archived for viewing on demand. Details at www.isaca.org/webcasts.

Research



- **COBIT® Mapping: Mapping of NIST SP800-53 Rev 1 With COBIT 4.1**
- Mapping ITIL V3.0 with COBIT 4.1
- Mapping COSO ERM with COBIT 4.1
- Information Security Governance: Guidance for Information Security Managers

Conference/Training Week Calendar

1-2 May

IT Control Objectives for Basel II
Las Vegas, Nevada, USA

14 June

CISA/CISM Exams
Worldwide

Sarbanes-Oxley Symposium
19-20 June 2008, Rosemont,
Illinois, USA

27-30 July

International Conference
Toronto, Ontario, Canada

ITGI releases

IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance

COBIT Security Baseline, 2nd Edition
COBIT Quickstart, 2nd Edition
IT Governance Implementation Guide:

Using COBIT

and Val IT, 2nd Edition

COBIT 4.1

COBIT Control Practices: Guidance to Achieve Control

Objectives for Successful IT

Governance, 2nd Edition

Standards



- IS Auditing Guideline G39- IT Organization, effective May 1, 2008, lists attributes for verifying an optimized IT organizational structure
- IS Auditing Standard S10- IT Governance.

Details at

www.isaca.org/standards.

Guideline Exposure Drafts:

Review of Security Management Practices

(Ends May 15, 2008);

G14 Application System Review and

G16 Effect of Third Parties on an Organization's IT Controls (Ends May 23, 2008).



www.isaca-centralohio.org



Member Benefit of the Month

ISACA has just released the new **IT Assurance Framework (ITAF)** as its latest member benefit. To meet the need for clear guidance for IT controls, ISACA has created this comprehensive assurance model incorporating standards and best practices. ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. The framework also:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards, guidelines, and tools and techniques that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct and reporting requirements.

The current version of ITAF incorporates ISACA's IS Auditing Standards and Guidelines and allows for new guidance to be properly indexed as it is developed and issued. It is designed to be a living document to enable relevant tools, techniques, white papers and publications to be placed with the framework.

ITAF is applicable to any formal audit or assessment engagement. Its design recognizes that IT assurance professionals are faced with different requirements and different types of audit and assurance assignments—ranging from leading an IT-focused audit to contributing to a financial or operational audit.

ISACA is pleased to be able to offer ITAF to ISACA members as a complimentary PDF download from the ISACA web site. It can be purchased by non-members for US \$45.

For further information or to download the publications, visit www.isaca.org/itaf

Announcing

1st Annual Central Ohio InfoSec Summit (jointly sponsored by Central Ohio ISSA, ISACA and Infragard Chapters)

Venue: Hyatt Regency Columbus
May 13, 2008 : **8 AM to 4 PM**

Last chance to Register for the Infosec Summit at the discounted price of \$35.00. Final registration ends soon, join us for a full day of information security topics. Lunch is provided.

Registration and Continental Breakfast begins at 8:00, [See agenda for more details](#)

Featuring such notables as:

Howard Schmidt	President, ISSA International , President & CEO, R & H Security Consulting LLC
Dr. Herbert H. Thompson	Chief Security Strategist, People Security
Mark D. Rasch, J.D	Managing Director, Technology, FTI Consulting

The InfoSec Summit will provide information security professionals with the most up-to-date information, tools, trends, legislative information, products, services, and strategies for addressing information security issues. Attendees can earn up to 8 CPEs at the conference which will focus on key topics related to information security and will showcase products and services from some of the nation's leading organizations. Program highlights include:

- Keynote presentations from nationally renowned speakers
- Breakout sessions from top speakers in the industry covering latest trends and issues in the information security industry
- Exhibitor showcase featuring leading security technology and services vendors

To register, or for more information about the event, please <http://www.infosecsummit.org> or email questions to info@infosecsummit.org



www.isaca-centralohio.org

ISACA Kentuckiana Chapter

offers

3 day course on

'Defending and Testing Your Internet DMZ'

INSTRUCTOR: Ken Cutler, CISSP, CISM, CISA from MISTI

July 9 – 11, 2008 (8 am to 5 pm each day)

LOCATION: Hyatt Regency Louisville (320 West Jefferson Street, Louisville, KY, 502.581.1234)

The agenda for this course includes the following topics:

- sizing up the attacks and the risks
- DMZ architectures
- network firewall policies and configuration
- router security
- VPN and remote access security
- Intrusion detection / intrusion prevention systems (IDS / IPS)
- Remote vulnerability testing of your perimeter security / DMZ

For all three days of this seminar, lunch is included and will be provided to you. In addition, you will receive an 800-page course manual to keep and a CPE certificate of completion to evidence your attendance.

WHO SHOULD ATTEND: IT Auditors and Consultants; Information Security Professionals; System and Network Administrators and Architects

CPE: 22 hours

COST: \$725 for members signed up and pre-paid by June 13, 2008;

\$800 for non-members and all registrants after June 13, 2008

REGISTRATION: via the Kentuckiana ISACA Chapter website

(http://www.isauditor.net/isaca/metsem/meets_em.htm)

or e-mail matthew_smith@b-f.com



Internal Audit Auditor (IT)

Department : Finance/Accounting

Job Location : New Albany, OH

Tween Brands is a world-class specialty retailer that builds an exciting and powerful connection with our customer through well-defined fashion brands. We believe we are creating one of the best work experiences in retail. Tween Brands is a place where people can do great work and live great lives! Each area in our company plays an important role in the delivery of quality products for tweens (7 thru 14 years of age).

Position Summary

The Internal Auditor will perform various aspects of the Internal Audit Plan, with a primary focus being to review existing policies and business processes for effectiveness in risk mitigation and efficiency in operation. This review process will include documentation of the current process, testing of certain control activities that mitigate risks within the process and identification/reporting of process improvement recommendations. The Internal Auditor will be required to communicate effectively with all areas of the business, including business process owners and information systems associates. The Internal Auditor will also be required to assist in special projects under the direction of Internal Audit Services management. In addition, this individual is expected to assist in building process and information systems knowledge within Internal Audit Services.

Position Responsibilities

- Develop in-depth knowledge of critical subject matter areas and/or key business processes and information systems; identify and assess key risks and controls with limited guidance.
- Facilitate quarterly updates to the Company's Enterprise Risk Assessment.
- Sarbanes-Oxley controls documentation and testing.
- Participate in subject matter specialist teams and perform consulting activities.
- Perform special projects as requested by Internal Audit Services management.
- Develop clear and concise written recommendations that require minimal editing.

Position Requirements

- **Bachelors Degree in Accounting/Finance or Management Information Systems** (dual major preferred). Certifications including one or more of the following: **CISA, CIA or CPA**.
- Proficient with Microsoft Access, Excel, Word and PowerPoint. Experience with COSO or CoBIT risk assessment framework.
- **2 to 4 years experience in business process consulting or auditing**. Previous experience evaluating information systems, general computer controls and application controls strongly preferred. Previous retail industry experience preferred.
- Ability to plan and execute multiple projects concurrently. Ability to establish and meet tight deadlines
- Excellent verbal and written communication skills. Must be comfortable and confident in interactions with all levels of financial and non-financial associates and be able to build effective working relationships across functions.

Tween Brands is an equal opportunity employer. We invite you to explore career opportunities with us. Please visit our website at www.tweenbrands.com and click on the Careers Section of the site to apply for this position.