



[www.isaca-centralohio.org](http://www.isaca-centralohio.org)



## Risk Assessment and Black Magic

get impacted heavily, then all "predictions" or estimates go awry and the "professionals" go into hiding.

Risk assessment is fundamental to information security and information systems audit. IS Audit focuses on high risk areas based on risk assessment and audits controls that must have a correlation to the risks identified. Various risk assessment methodologies and standards are out there: NIST 800-30, OCTAVE, AZ/NZS 4360:2004, and so on. Assessing risk ultimately boils down to identifying the impact or loss to information assets resulting from adverse events (threat events) exploiting vulnerabilities of systems, processes, people or technologies. Microsoft has come up with a threat modeling framework called 'STRIDE'. Success of risk assessment depends on assessment of probabilities of threat events occurring and the assessment of the impact.

Jack Jones, a well known figure in the information security field, is currently Founder and President of Risk Management Insight, LLC. He is associated with his 'FAIR' methodology for risk assessment. His methodology considers various factors contributing to risk using a tree model detailing various risk factors and their relationships and the model uses statistical techniques such as Monte Carlo simulation to arrive at a fairly accurate estimate of risk to information systems. Jack Jones will present to our Chapter this month (on March 13) on 'IT Risk Management'.

Last month we had a presentation from Patrick Shaw of Department of Homeland Security on the taxonomy of critical infrastructure protection. We would like to thank Patrick Shaw for a highly informative presentation.

I would like to remind again those members who have forgotten to renew their membership for 2008 to renew the membership at the earliest. Membership renewal would help members to avail of all membership benefits and to maintain their certification, if they are CISAs or CISM's.

We will be holding our CISA and CISM weekly review classes during April and May 2008 to help those who are appearing for the exams in June 2008. Please register on our website. Our Spring Seminar on 'Web Application Security & Audit' by MIS Training is being held on March 17 and 18 at Platform Labs.

The ISACA year is drawing to a close on May 31, 2008. Nominations for Chapter leadership for 2008-2009 are on. Please step in to take leadership of the Chapter in whatever role you feel you can contribute. Please refer to our newsletter for details. The elections are due on May 8, 2008.

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

Assessing risks was a black magic art for a long time. Professionals with their magic wand would categorize something as high risk or low risk without assigning any reason. Ultimately when security incidents do happen and the organizations or businesses

### Chapter Board

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

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

**Secretary:** Ann Atkinson (JP Morgan Chase)

**Treasurer:** Mike Brady, CISA (UHY Advisors)

#### Directors:

Melissa Justice, CISA (State Auditor's Office)

Michael Kirk, 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](http://www.isaca-centralohio.org)



## Chapter News & Events:

### March Luncheon Meeting

**Topic:** IT Risk Management

**Presented by:** Jack Jones, Risk Management Insight (RMI)

**Date:** Thursday, March 13, 2008, 11:30 AM to 1:30 PM

**Location:** [Brio Tuscan Grill at Polaris](#)

#### Topic Summary:

Any grade school graduate can cite a published standard or compare a checklist against what they see in front of them. As professionals, we provide maximum value to our employers by being able to apply our subject matter expertise as well as critical thinking skills to work toward optimum solutions of the complex security-related problems our employers face. In this session, Jack will discuss the value proposition risk management offers to an organization, as well as the important value proposition opportunity we can offer as professionals.

#### Speaker Bio:

**Jack Jones**, Risk Management Insight (RMI) has been employed in technology for the past twenty-five years, and has specialized in information security and risk management for eighteen years. During this time, he's worked in the military, government intelligence, consulting, as well as the financial and insurance industries. Jack spent over five years as CISO for a Fortune 100 financial services company where his work was recognized at the 2006 RSA Conference with ISSA's Excellence in the Field of Security Practices award. In 2007 he was selected as a finalist for the Information Security Executive of the Year, Central United States and participated as a judge for the Information Security Executive of the Year, National award. As an invited member of an international ISACA task force, Jack is helping to develop global standards for IT risk management in the enterprise. He also regularly speaks at national conferences and has developed and published an innovative risk analysis framework called Factor Analysis of Information Risk (FAIR).

#### Luncheon Menu:

Roasted Garlic, Spinach & Artichoke Dip; Brio Chopped Salad; Penne Mediterranean; Chicken Milanese Pomodoro; Grilled Asparagus; Tiramisu; and Apple Crostata.

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

**Spring Seminar:** March 17, 18: Web **Application Security & Audit** by MIS Training at Platform Labs (Contact: Rich Ridewood)

**Thursday, April 10, 2008:** Steve Romig of OSU on "Lessons Learned: Ohio's HB 104, Data Breach Notification."

**Thursday, May 8, 2008:** Joseph Ponnoly on 'IT Governance Principles and Best Practices and an overview of the CGEIT Certification.'

**AGM & Chapter Elections:** Thursday May 8, 2008

## 2008 CISA & CISM Review Class Information

[Register Online Today!](#)

Below you will find the schedule of the CISA & CISM Review Classes that will be held by ISACA Central Ohio Chapter at The Ohio State University, Columbus, OH, in preparation for the exams scheduled for **June 14, 2008**.

If you are interested in taking these review sessions, please [register online](#) or email [Chuck.lmwalle](mailto:Chuck.lmwalle).

**CISA Review Class Schedule**



**Day & Time:** Tuesdays, 6PM to 9PM  
**Fees:** Members - \$ 100 , Non-Members - \$200 (Checks payable to ISACA Central Ohio Chapter)  
**Required Course Material:** CISA Review Manual 2008 (Please purchase online from ISACA bookstore)  
**Location:** The Ohio State University, Scott Laboratories, Room SO 056  
**Map & Directions:** [Scott Laboratory](#), Bldg 148  
**Parking:** Fees to be paid by participants

Date(s)	Time	Topic
April 1, 2008	6pm - 9pm	IS Audit Process
April 8, 2008	6pm - 9pm	IT Governance
April 15, 2008	6pm - 9pm	Systems and Infrastructure Life Cycle Management
April 22, 2008	6pm - 9pm	Business Continuity & Disaster Recovery
May 6, 2008	6pm - 9pm	Protection of Information Assets, Part 1
May 13, 2008	6pm - 9pm	Protection of Information Assets, Part 2
May 20, 2008	6pm - 9pm	IT Service Delivery & Support
May 27, 2008	6pm - 9pm	Mock Test & Discussion

[Register Online Today!](#)

For further information please email [Chuck Imwalle](mailto:Chuck.Imwalle).

**CISM Review Class Schedule**



**Day & Time:** Thursdays 6PM to 9 PM  
**Fees:** \$ 150 for members \$ 250 (Non Members) payable to ISACA Central Ohio Chapter  
**Required Course Material:** CISM Review Manual 2008 (to be purchased from ISACA online bookstore)  
**Location:** OSU, Scott Lab (Building 148) SO 056, 201 W 19th Ave, Columbus, OH, 43210  
**Map & Directions:** [Scott Laboratory](#), Bldg 148  
**Parking:** Fees to be paid by participants

Date(s)	Time	Location	Topic
April 10, 2008	6pm - 9pm	OSU, Bldg 148	Information Security Governance
April 17, 2008	6pm - 9pm	OSU, Bldg 148	Information Risk Management
April 24, 2008	6pm - 9pm	OSU, Bldg 148	Information Security Program Management
May 8, 2008	6pm - 9pm	OSU, Bldg 148	Information Security Management
May 15, 2008	6pm - 9pm	OSU, Bldg 148	Incident Management & Response
May 29, 2008	6pm - 9pm	OSU, Bldg 148	Mock Test & Discussion

[Register Online Today!](#)

For further information please contact:  
 Joseph Ponnoly - [jponnoly@yahoo.com](mailto:jponnoly@yahoo.com)

**Central Ohio Information Security Summit (May 13, 2008)  
Protecting Information Through People Process and  
Technology...**

Please join us on May 13th, 2008 at Hyatt Regency in downtown Columbus as the Central Ohio ISSA, and the Central Ohio ISACA chapters have joined together to promote the first annual Central Ohio Information Security Summit. The goal of this event is to educate regional Information Security professionals and support collaboration by bringing leading speakers in the information security field together to educate the community on the latest industry trends and issues.

The first keynote will be delivered by Howard Schmidt, President ISSA International, President & CEO R & H Security Consulting LLC.

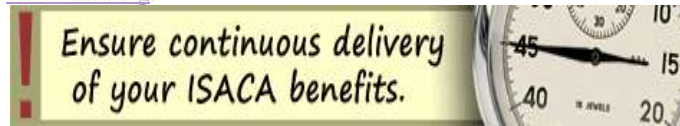
More internationally known security speakers will be announced shortly.

We look forward to seeing everyone at this event. For more details, registration, and up-to-date speaker announcements, please visit:

<http://www.infosecsummit.org>

**Renew Your Membership Today**

The annual purge of members will take place in April. After that time, nonrenewed members will no longer have access to the ISACA web site and will not receive any further issues of the *Information Systems Control Journal*<sup>®</sup>. Until the purge occurs, members can renew online at [www.isaca.org](http://www.isaca.org).



Please log in and click the "My renewals tab" on the left navigation panel to complete the renewal process.

[Join Today!](#)

Or send questions to [membership@isaca.org](mailto:membership@isaca.org)

**International Updates (Courtesy:  
ISACA ExpressLine)**



**Member-Get-A-Member**

**Contest Extended**

Due to high demand, ISACA has extended its 2008 Member-Get-A-Member contest for two weeks! The contest will end 15 April. All new member payments must be received and posted at ISACA by 5:00 p.m. (17.00) (Central Standard Time) on 29 April 2008. For details, click on the link:

[www.isaca.org/mgam](http://www.isaca.org/mgam). Results will be available in May 2008.

The easiest way to participate in the contest is by using the special Member-Get-A-Member e-mail sent from ISACA in February. That e-mail contains a unique membership link to the specially designed web site where members can initiate e-mail invitations. Using this e-mail and the web site ensures that the participating member will receive full credit for recruiting each new full-dues-paying member. Members may also access the Member-Get-A-Member contest by logging in at [www.isaca.org](http://www.isaca.org). ■

**Distance Learning**



The March ISACA e-Symposium is scheduled for 25 March 2008 and will focus on PCI compliance issues. To register for the 25 March 2008 e-Symposium and take the first step toward earning three free continuing professional education (CPE) credits, please visit [www.isaca.e-symposium.com](http://www.isaca.e-symposium.com).

All e-symposia are recorded and archived for viewing on demand. Registration is required to view an archived (on-demand) or live event and earn free CPE credits. The ISACA E-learning Library now holds more than 12 e-symposia. For more information, please visit [www.isaca.org/webcasts](http://www.isaca.org/webcasts). ■



**Member Benefit of the Month:  
Listservs/Discussion Forums**

ISACA and IT Governance Institute® (ITGI™) have established several listservs to enable interested parties to find the group most suited to their professional interests. Each of the five listservs offers excellent opportunities to share advice, seek assistance and raise pertinent questions. Information on each listserv and how to join is available at [www.isaca.org/listserv](http://www.isaca.org/listserv). ■

## Calendar of Events

Dates of conferences are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

### March

- 9-12 March .....**EuroCACS<sup>SM</sup>**  
Stockholm, Sweden
- 11 March .....Deadline to submit articles for consideration for vol. 2, 2008, of *COBIT® Focus*
- 21 March .....Deadline to submit articles for consideration for vol. 4, 2008, of the *Information Systems Control Journal*
- 25 March .....ISACA e-Symposium on PCI compliance issues
- 28 March .....Deadline to submit Invitation to Participate application for 2008-09 key boards and committees

### April

- 2 April.....Early-bird registration deadline for the Training Week in Vancouver, British Columbia, Canada
- 7-11 April.....**ISACA® Training Week**  
Dallas, Texas, USA
- 15 April .....Last day to use the Member-Get-A-Member web site to recruit new full-dues-paying members and gain a chance to win valuable prizes
- 16 April .....Early-bird registration deadline for the Training Week in Minneapolis, Minnesota, USA
- 27 April-1 May .....**North America CACS**  
Las Vegas, Nevada, USA
- 29 April .....Deadline for receipt of dues payment for Member-Get-A-Member contest

information, available at [www.isaca.org/cisaboi](http://www.isaca.org/cisaboi) and [www.isaca.org/cismboi](http://www.isaca.org/cismboi), respectively.

## Certification Update



### CISA/CISM Leads ISO/IEC 27001 Certification

Under the direction of a CISA- and CISM-certified professional, the Credit Union Central of British Columbia will be the first online banking system in Canada to become ISO 27001-certified. The Credit Union Central's program also utilizes COBIT and ITIL to establish an extremely effective IT governance framework. The framework provides a formal process that assures conformance to ISO/IEC 27001 and compliance with contractual agreements, statutes, regulations and information security standards while reducing the over all operational cost of compliance.



### Exam and Certification Renewal Reminders

- **CISA and CISM exam highlights:** The results of the December 2007 exams were released by one-time e-mail notification, posted to the candidate's profile on the ISACA web site and sent by post in early February. To ensure confidentiality, exam results are not reported by phone or fax.
- **CISA and CISM applications:** To speed up certification processing time, applicants should gather all application documents and send them together in one package.
- **June exam registration:** Registration for the June 2008 CISA and CISM exams closes 9 April 2008. To view additional details, please refer the latest bulletins of
- **CISA and CISM certification renewals:** Please renew and report CPE hours, as soon as possible, to avoid revocation. Final reminder invoices have been mailed. The renewal process can be completed online by logging into [www.isaca.org](http://www.isaca.org) and going to "My Renewals."
- **CPE policies:** The CISA and CISM CPE policies are available at [www.isaca.org/cisacpepolicy](http://www.isaca.org/cisacpepolicy) and [www.isaca.org/cismcpepolicy](http://www.isaca.org/cismcpepolicy).

## Research Update

### COBIT® Mapping: Mapping ITIL v3 With COBIT® 4.1

ITIL is frequently referred to as a consistent and comprehensive best practice for IT service management to deliver high-quality IT services. This mapping shows that all ITIL processes can be mapped to their *Control Objectives for Information and related Technology* (COBIT®) counterparts; however, some COBIT processes are not covered by ITIL. This publication is part of the COBIT Mapping series, available as complimentary downloads exclusively for ISACA members, and is scheduled for release in April 2008.

### Recent/Upcoming ISACA/ITGI Releases

- *IT Assurance Framework™ (ITAF™)* (March 2008)
- *COBIT® Mapping: Mapping COSO ERM With COBIT® 4.1* (April 2008)
- *COBIT® Mapping: Mapping FFIEC Framework With COBIT® 4.1* (April 2008)

- 17-20 August—Latin America CACS, Santiago, Chile

More information on these books and, in some cases, member downloads are available at [www.isaca.org/deliverables](http://www.isaca.org/deliverables). Those books available for purchase can be found in the ISACA Bookstore at [www.isaca.org/bookstore](http://www.isaca.org/bookstore). ■ Bookstore Update

An additional nine new peer-reviewed and three new ISACA/ITGI books have been added to the ISACA Bookstore this quarter:

- *Audit Procedures 2008*
- *Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 2<sup>nd</sup> Edition*
- *Essentials of Sarbanes-Oxley*
- *Gobierno de las Tecnologías y los Sistemas de Información*
- *Gray Hat Hacking, 2<sup>nd</sup> Edition*
- *Information Technology Ethics: Cultural Perspectives*
- *IT Control Objectives for Basel II\**
- *IT Governance Global Status Report 2008\**
- *Network Security Fundamentals*
- *Reinventing Project Management*
- *Service-Oriented Architecture: A Planning and Implementation Guide for Business and Technology*
- *Stepping Through the InfoSec Program\**
- *XSS Exploits—Cross Site Scripting Attacks and Defense* (\*ISACA/ITGI publication)

For more information on these and other titles, please visit the ISACA Bookstore web site at [www.isaca.org/bookstore](http://www.isaca.org/bookstore) or see the *Information Systems Control Journal* Bookstore insert for additional information. Please contact the Bookstore at [bookstore@isaca.org](mailto:bookstore@isaca.org) or +1.847.660.5650. ■

## Conference Spotlight

### North America CACS

27 April-1 May 2008

Las Vegas, Nevada, USA

The 38<sup>th</sup> annual North America CACS conference is customized to meet the needs of IT audit, control, security and governance professionals. A keynote address will be given by Randy Melby, senior vice president and general auditor of Washington Mutual Inc. Melby established and executed a best-in-class vision that transformed his audit department from irrelevant to highly relevant in three short years. In his keynote address he will share his 28 years of financial services experience, and provide insight on how IT audit, information security and IT governance can and must be relevant in the ever-changing business environment.



### Note from the Editor

If you would like to submit news, photos or articles to be published in this newsletter, please send them to me by the end of each month.

We are also inviting advertisements for publication in this newsletter. This newsletter is received by over 435 members of this Chapter who represent major organizations in and around Columbus, Ohio.

Nelia Pozzuoli, CISM, CISA, CISSP

Editor

Conference tracks will include IT Audit Core Competencies, IT Audit Tools and Competencies, IT Audit Techniques for Evaluating Business Practices, Compliance Issues, Control Methodologies and IT Governance, Information Security Practices, and IT Risk Management. For more information and to register, please visit [www.isaca.org/nacacs](http://www.isaca.org/nacacs).

### Future Conferences and Training Weeks

Upcoming events are noted in the Calendar of Events. Other future 2008 events to keep in mind include:

- 27-30 July—International Conference, Toronto, Ontario, Canada