



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



## You can't fix stupidity

"You can lock down admin. You can disable thumb drives. But you can't fix stupidity." This was the message that was driven home by the movie "The PCI Ultimatum: A Data Security Thriller" that was premiered on December 4, 2007 at Nationwide Arena Grand Theater by CISCO Systems, RSA Security and Trend Micro.

Our November presentation by Jack J Schiller of Jefferson Wells on 'PCI Data Security Standards and Compliance' served to be a timely reminder to all those who store, process or transmit credit card information to comply with the PCI data security standards.

This month we are addressing another important area of assurance and IT Governance. Robert Brett of Protiviti will be presenting on 'SAP/R3 Audit and Application Controls'. This may help large corporations such as Cardinal Health, Limited, etc. that are spending hundreds of millions of dollars to implement ERP using SAP/R3. The presentation will be on Thursday December 13, 2007 from 11.30 AM to 12.45 PM. Please register today on our website ([www.isaca-centralohio.org](http://www.isaca-centralohio.org)).

We will be having our annual social get-together and lunch in Beulah Park on Saturday December 15, 2007. Please register on our website or contact Matt Schondel of Alliance Data. Come and enjoy the horse races and try your luck, if you like.

I would like to remind everyone to register early for the 2 day Spring

Seminar on 'Web Application Security & Audit' scheduled for March 17 and 18, 2008. Please register on our website or contact Rich Ridewood of BWC, State of Ohio.

December is the time to renew your ISACA Membership and also remit your CISA and CISM maintenance fees. Those certified also have to submit to ISACA the CPEs earned for maintaining the certifications.

2007 is coming to a close. Let us ring in the new year 2008 with renewed hope and confidence.

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

## Chapter News & Events:

### Upcoming Chapter Luncheon Meetings:

**Thursday, December 13, 2007** – SAP/R3 Audit & Application Controls (Robert Brett of Protiviti)

**Thursday, January 10, 2008**- Identity & Access Management & Security Architecture (Dan Houser, Sr. Security Architect, Cardinal Health)

**Saturday December 15, 2007:** Beulah Park Social Get-together.

**Spring Seminar:** March 17,18: Web Application Security & Audit by MIS Training at Platform Labs

### Chapter Board

**President:** Joseph Ponnoly, CISM, CISA, CISSP (Cinfodens Consulting)

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

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

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

#### Directors:

Melissa Justice, CISA (State Auditor's Office)

Michael Kirk, CISA (CitiGroup)

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, 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)

**Newsletter Editor:** Nelia Pozzuoli, CISM, CISA, CISSP (Global Resource Professionals)

**Social Committee:** Matt Schondel, CISA (Alliance Data)

**CISA:** Chuck Imwalle, CPA, CISA (Crow Chizek)

**CISM:** Joseph Ponnoly CISM, CISA, CISSP (Cinfodens Consulting)



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



## International Updates

### Certification Update

#### CISA and CISM Exam Admission Tickets

Candidates who have not received their admission ticket by 1 December 2007 should contact the certification department immediately at [examregistrant@isaca.org](mailto:examregistrant@isaca.org). Please put "admission ticket" in the subject header for quicker processing.

#### June 2008 Exam Registration

Registration for the June 2008 CISA and CISM exams has begun. Please visit ISACA web site at [www.isaca.org/examreg](http://www.isaca.org/examreg). We will schedule review classes for April and May 2008.

#### CGEIT Certification Grandfathering Application

ISACA developed the Certified in the Governance of Enterprise IT™ (CGEIT™) certification for professionals charged with satisfying the IT governance needs of an enterprise. The certification program recognizes those who have the necessary level of professional knowledge, personal skills and business experience to maximize the contribution made by information technology to an enterprise's success while managing and mitigating risks posed by IT. The CGEIT Grandfathering Application is now

available on the ISACA web site at [www.isaca.org/cgeitgfapp](http://www.isaca.org/cgeitgfapp).

Additional information about the new certification can be found at [www.isaca.org/cgeit](http://www.isaca.org/cgeit).

### Member Benefit of the Month

#### COBIT 4.1

ISACA members have access to a complimentary download of COBIT® 4.1, as well as to certain COBIT-related documents including **IT Assurance Guide: Using COBIT®** and its appendices in Excel, **IT Governance Implementation Guide: Using COBIT® and Val IT™**, 2nd Edition, and the content of its accompanying IT Governance Implementation Guide—Supplemental Tools and Materials CD-ROM. Members can also browse most areas of COBIT Online®. Available at [www.isaca.org/downloads](http://www.isaca.org/downloads)

### Research Spotlight

#### IT Control Objectives for Basel II

Identifying and measuring operational risk are formidable challenges for banks and financial services organizations. To help organizations meet these challenges, the IT Governance Institute® (ITGI™) has released **ITControl Objectives for Basel II**.

Developed by individuals from a range of financial services organizations and other banking advisors, IT Control Objectives for Basel II follows the format and intent of ITGI's popular IT

Control Objectives for Sarbanes-Oxley publication. The book provides unambiguous guidance to operational and information stakeholders—including risk managers, IT practitioners, banking regulators, financial services experts and internal/external auditors—regarding operational and information risk management and their application to the Basel II Capital Accord framework.

Additionally, the publication:

- Maps Basel II principles for operational risk against IT risk
- Highlights the need for operational and information risk management and IT controls from the perspective of bankers and financial experts
- Provides a framework for managing information risk in the context of the Basel II Capital Accord
- Highlights steps toward convergence

A PDF download, complimentary for ISACA members, of IT Control Objectives for Basel II is available at [www.isaca.org/downloads](http://www.isaca.org/downloads). It is also available in print from the ISACA Bookstore

([www.isaca.org/bookstore](http://www.isaca.org/bookstore)), with a discount available to members.

#### IT Assurance Framework (ITAF)

The recent attention to the assessment of enterprise IT controls by the marketplace has led ISACA to refocus its existing IT standards, guidelines and procedures to better support assurance professionals. ISACA has developed ITAF to serve as the professional standards framework for the IT assurance professional. The



framework will help identify gaps in guidance needed by IT assurance professionals and areas where research and development of new guidance should be considered.

Comments submitted during the exposure period are being addressed. The framework is scheduled for issue by January 2008.

#### Bookstore Update

The latest CISA and CISM study aids for the 2008 exams are now available. CISA exam reference materials are available at [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks). CISM exam reference materials are available at [www.isaca.org/cismbooks](http://www.isaca.org/cismbooks).

#### The newest research releases from ISACA and ITGI include:

- COBIT® Quickstart, 2nd Edition
- COBIT® Security Baseline, 2<sup>nd</sup> Edition\*
- IT Control Objectives for Basel II\*
- Stepping Through the InfoSec Program

(\*Also available to ISACA members as complimentary PDF download at [www.isaca.org/downloads](http://www.isaca.org/downloads))

#### News Briefs

##### Journal Update

The Information Systems Control Journal is seeking articles for volume 3, 2008—themed Addressing Business Challenges. The copy deadline for drafts for volume 3 is 22 January 2008. For more information, please view the 2008 editorial calendar at [www.isaca.org/journal](http://www.isaca.org/journal) or e-mail

[jhajgeorgiou@isaca.org](mailto:jhajgeorgiou@isaca.org).

##### Conference/Training Week Update

New 2008 ISACA conference and educational event dates have been released. Please update chapter web sites and inform constituents about the available programs. For the latest information, please visit

#### December e-Symposium

The December ISACA e-Symposium is scheduled for **11 December 2007** and is titled **Making Data Protection Compliant**. To register for the 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 contains the 12 most recent e-symposia. For more information, please visit [www.isaca.org/webcasts](http://www.isaca.org/webcasts).

[www.isaca.org/conferences](http://www.isaca.org/conferences).

#### 2007-2008 Conference/Training Week Calendar

##### ISACA Training Week

3-7 December 2007  
Scottsdale, Arizona, USA

##### Information Security Management Forum

10-11 December 2007  
Scottsdale, Arizona, USA

[www.isaca.org/securityforum](http://www.isaca.org/securityforum).

##### IT Audit Management Forum

10-11 December 2007  
Scottsdale, Arizona, USA

##### Information Security Conference

28-29 January 2008  
Panama, Republic of Panama  
[www.isaca.org/infosecuritypanama](http://www.isaca.org/infosecuritypanama).

##### North America CACS

27 April-1 May 2008  
Las Vegas, Nevada, USA  
[www.isaca.org/nacacs](http://www.isaca.org/nacacs).

##### Additional Upcoming ISACA Conferences

27-30 July 2008—International Conference, Toronto, Canada

#### Research Update

##### Stepping Through the InfoSec Program

This publication includes a case study and steps to:

- Compose an information security program
- Cement a relationship between an information security program and IT governance
- Design roles and responsibilities to ensure accountability
- Identify and allocate resources to achieve information security program objectives
- Determine if an information security program is achieving objectives

It is available from the ISACA Bookstore at [www.isaca.org/bookstore](http://www.isaca.org/bookstore).



www.isaca-centralohio.org



**COBIT Mapping: Mapping NIST SP800-53 Rev 1 With COBIT**

The application of the security controls defined in NIST SP800-53 Rev 1 represents the current state-of-the-practice safeguards and countermeasures for US federal information systems. In this mapping, NIST SP800-53 Rev 1 was divided into the major family controls, which were mapped to one or more COBIT control objectives. NIST SP800-53 should be used in conjunction with COBIT to provide more detailed guidance in the area of security.

This is another publication in the series of detailed COBIT mapping publications available as complimentary downloads exclusively for ISACA members. It is scheduled to be available by the end of 2007.

K-NET® is an Internet-based database of knowledge specifically developed to provide ISACA® members with direct access to educational opportunities, books and CDs, articles and papers, and web resources relevant to information systems governance, control, security and assurance.

	<p><b>Information Technology Audit Senior</b>  <b>Available for Contract Work</b>  <b>Need Additional Help? Contact me.</b>  <b>(216) 459-9272</b>          Daniel J. Leo, CPA, CMA, CIA          Independent Contractor of IT/IS Audit Services          Ohio Based - Will travel to your location(s)</p>	
<p><u>Why Contract with me?:</u></p> <ul style="list-style-type: none"> <li>&gt; SAVE \$\$ -Implement AS5 &amp; Reduce Audit Costs</li> <li>&gt; Meet Deadlines</li> <li>&gt; Save Your Staff, I'll do the Traveling</li> <li>&gt; Both IT/IS and Internal Audit (Financial) Skills</li> </ul>		<p><u>Highest Quality Services:</u></p> <ul style="list-style-type: none"> <li>&gt; Certified Quality – CPA, CMA, CIA</li> <li>&gt; Successfully Passed the CISA exam</li> <li>&gt; Experienced-17 yrs as Indep. Contractor</li> <li>&gt; Excellent References -Satisfied Clients</li> </ul>

If you would like to contribute articles relevant to IT Governance, Assurance & IS Audit, Information Risk Management, please contact:

Nelia Pozzuoli, CISM, CISA, CISSP

Newsletter Editorial Committee Chair