ISACA®
Trust in, and value from, information systems
Greater Kansas City Chapter

January 2011 Volume 3, Issue 5

In this issue:

January Meeting Details

The Changing SAS70 Landscape

During this session, Dan and Rebecca will discuss the key changes, considerations, and differences between SSAE 16, ISAE 3402 and the existing SAS 70 standard. They will review how the changes to the standards impact both service organizations and user entities alike and the important things to consider now, including alternatives for reporting on controls that do not relate to a user's financial statements.

Date: January 13, 2011

Time: 11:30 AM - 12:00 PM Registration | 12:00 - 1:00 PM Lunch | 1:00 - 3:00 PM Program

Location: The American Restaurant | 2511 Grand Street | Kansas City | Missouri | 64108

Price: $35 members | $50 guests | $5 students

CPE: 2 Credits

Speakers: Dan Hirstein and Rebecca Goodpasture, Deloitte

Dan is a Director in the Advisory Services practice in Kansas City, specializing in controls and governance. He has 12 years of experience at Deloitte with focus on business process and information technology controls. He has significant experience helping clients prepare for regulatory and compliance requirements including Sarbanes-Oxley and SAS 70's. Dan has over 19 years of Internal Audit experience and worked in a large telecommunications company for 16 years in both their Information Technology and Internal Audit organizations. He also has significant experience assisting companies with their Governance and Risk processes. Dan is a Certified Information Systems Auditor (CISA) as well as a Certified Internal Auditor (CIA).

Rebecca is a Senior Manager in Deloitte's Advisory practice specializing in internal control. Rebecca has more than ten years of experience managing internal control projects including internal audits, Sarbanes-Oxley compliance, SAS70, information technology audit, and business process reviews.

Feedback Forum

Have an idea for a program? We want to hear from you! Please contact Reed Anderson, our Programs Chair, at Reed.Anderson@centurylink.com.

If you have any suggestions regarding newsletter content, please contact the newsletter editor at molly.coplen@yahoo.com

Did You Know …
By the Numbers ….
Top 5 IT Security Priorities - 2011 [1]

- End-user Firewalls
- Biometrics
- Data Leakage Prevention
- Encrypting Removable Media
- Locks & Keys for Computer Hardware

[1] *Bill Brenner, "Reset, Global Information Security Survey," www.cio.com, October 15, 2010 Submitted by Jerry Wistrand*

2010—2011 Monthly Meetings

Unless otherwise noted, registration begins at 11:30 am, lunch at noon, and the presentation at 1:00 pm. Register at http://www.isaca-kc.org

Date	Location	Topic and Speaker
January 13, 2011	The American Restaurant	*SAS 70 Changes* Deloitte
February 10, 2011	Lidia's	*PCI DSS 2.0*
March 10, 2011	Figlio's Tower	*Enterprise Risk Assessments*
April 14, 2011	The American Restaurant	*Topic TBD*
May 12, 2011	TBD	*Annual Business Meeting* *Topic TBD*

Tech Article Spotlight: Popular Web 2.0 Attack Methods

Here are a few of the methods attackers use to exploit Web 2.0 systems:

- **Cross-site AJAX scripting**: A malicious Website infects a victim's browser with code, and then the code is executed on the client systems. Attackers also use incorrectly written scripts to exploit systems.
- **XML poisoning**: Attackers use XML to exploit systems as data is passed back and forth during Web 2.0 transactions.
- **RSS/ATOM injection**: Uses RSS feeds to inject malicious JavaScripts
- **AJAX code execution**: Uses cookies to compromise sites that a person remains logged into after leaving the initial page and browsing into a malicious site.
- **Validation of AJAX routines:** As AJAX conducts client-side validations, it is supposed to be backed up by server-side validations. Developers sometimes forget this step, which opens the door to an SQL or LDAP injection.
- **WSDL scanning:** Web Services Definition Language services as an interface to Web services. An unprotected WSDL file can expose sensitive data and lead to a security breach.

Read more! Source: Samuel Greengard, "Web 2.0 Security," www.baselinemag.com, September/October 2010, pp. 21-26. *Submitted by Jerry Wistrand*

Interesting Links…….

PCI DSS
http://go.techtarget.com/r/13057161/9528296/1
http://go.techtarget.com/r/13057162/9528296/2

New biometric: eye movements instead of eye structures [2]— http://www.technologyreview.com/computing/26700/
Another piece of the Stuxnet puzzle:[2]
http://www.symantec.com/connect/blogs/stuxnet-breakthrough
http://www.wired.com/threatlevel/2010/11/stuxnet-clues/
http://www.theregister.co.uk/2010/11/15/stuxnet_jigsaw_completed/

[2] Reprinted from CRYPTO-GRAM, 12.15.2010 http://www.schneier.com/crypto-gram.html

The Certified Information Systems Auditor (CISA) is ISACA's cornerstone certification. .Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

The Certified Information Security Manager (CISM) certification is a unique management-focused certification that has been earned by more than 13,000 professionals since its introduction in 2003. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise's information security.

The Certified in the Governance of Enterprise IT (CGEIT) certification program was designed specifically for professionals charged with satisfying the IT governance needs of an enterprise. Introduced in 2007, the CGEIT designation is designed for professionals who manage, provide advisory and/or assurance services, and/or who otherwise support the governance of an enterprise's IT and wish to be recognized for their IT governance-related experience and knowledge.

The Certified in Risk and Information Systems Control™ (CRISC) certification is designed for IT professionals who have hands-on experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance. CRISC recognizes a wide range of professionals for their knowledge of enterprise risk and their ability to design, implement, monitor and maintain IS controls to mitigate such risk.

News from ISACA

Code of Professional Ethics

Effective January 1, 2011

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders. Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

The ISACA Code of Professional Ethics has been updated and will be effective 1 January 2011. The changes to the Code include more specific recognition of ISACA constituents as well as modification of wording to reflect current practice and terminology

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

ISACA IT Professional Networking and Knowledge Center

http://www.isaca.org/Knowledge-Center/Pages/default.aspx

ISACA's IT Professional Networking and Knowledge Center is a meeting place for IT professionals who share common professional interests. The Knowledge Center offers you the opportunity to join a group on a specific topic and participate through the exchange of information, sharing of expertise and experience, and building new understanding through collaboration. Browse over 100 topics, and collaborate with other professionals with similar interests.

ISACA Adds eLibrary Member Benefits

www.isaca.org/elibrary

ISACA has developed the ISACA eLibrary to provide on-demand access to a wealth of readily usable information. The ISACA eLibrary is a comprehensive collection of content from nearly all ISACA/ITGI-published books and more than 250 additional titles all available free-of-charge as a benefit of ISACA membership.

- Access to all books and the ability to browse the content immediately
- Downloads of up to five chapters per month from the available book titles
- A private bookshelf for the most frequently accessed book titles for each individual user
- The ability to easily purchase a book after browsing online
- Bookmarking ability of the content a user needs most
- Effortless creation of citations

Contact Information

Kevan Brewer
President
kevan_brewer@yahoo.com

BJ Smith
Vice President
BJSmith@dstsystems.com

Wendy Dobratz
Secretary
wevans@naic.org

Nila Henderson
Treasurer/Webmaster
treasurer@isaca-kc.org

Reed Anderson
Chair, Programs Committee
Reed.Anderson@centurylink.com

Heidi Zenger
Programs Committee
hzenger@deloitte.com

Michelle Moloney
Programs Committee
michelle.j.moloney@sprint.com

Matt Suozzo
Membership
mattsuozz@gmail.com

Molly Coplen
Newsletter
molly.coplen@yahoo.com

Jennifer Harper
Director
j1211biz@gmail.com

Alfie Mahmoud
Director
amahmoud@kpmg.com

Calendar of Events

January

5 January.....Early Bird Deadline, ISACA Training Week, New Orleans

7 January.....Deadline for nominations for the ISACA Board of Directors for 2011-2012

13 January .....KC ISACA meeting, *SAS 70 Changes*

20 January .....Webinar, *Database Auditing Best Practices*

24-25 January ....Omaha ISACA Chapter, COBIT Foundation Course; 16 CPE

26-27 January ....Omaha ISACA Chapter, Implementing IT Governance Using COBIT and ValIT; 16 CPE

February

9 February.....Deadline, Early Registration, CISA, CISM, CGEIT Exams

10 February.....KC ISACA meeting, *PCI DSS 2.0*

10 February.....Early Bird Deadline, *North America CACS Conference*

March

10 March .....KC ISACA meeting, *Enterprise Risk Assessments*

14-18 March.....ISACA Training Week, New Orleans

Write an Article for the Newsletter!

We are always looking to add new and interesting content to the newsletter and are accepting article submissions from our members for consideration! To be considered for publication, articles must meet the following criteria:

- Word or text document format
- 500 or less words
- Relevant to ISACA, IT Governance, IT Audit, Security, etc.
- References to all applicable sources, including the title, author, and date written.

To submit or for more information, please contact the newsletter editor.