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

January 2012 Volume 4, Issue 5

In this issue:

January Meeting Details

Adding Strategic Value with Project Assurance

Date: January 12, 2012
Time: 11:30 AM - 12:00 Registration | 12:00 - 1:00 Lunch | 1:00 - 3:00 Program
Location: Brio Tuscan Grill | 502 Nichols Road | Kansas City MO 64112
CPE's: 2 Credits
Price: $35 members | $50 guests | $5 students

Presentation Overview
Project assurance provides a holistic assessment of risks that could compromise achievement of desired business, project and/or control outcomes. Project auditing enables IT and Internal Audit to add value toward strategic organizational initiatives by:
Identifying key risks and issues, allowing the project team to avoid costly rework or delays.
Providing senior management and stakeholders with an objective and transparent perspective of risks and realization of business benefits.
Confirming alignment of project scope with business objectives and stakeholder expectations.
Providing perspective on the effectiveness and efficiency of the controls designed into new business processes.

During our time with KC ISACA members, PwC will explore various alternatives to evaluate Enterprise Program Governance, strategic alignment, and benefits realization; program level management processes and delivery mechanisms; and evaluation of project level management processes and delivery mechanisms.

Speaker Bio
Vicki Wagoner is a Director in PwC's Risk Assurance practice and the Internal Audit Services leader in the Kansas City market. Vicki has approximately 12 years of collective experience in internal audit, information systems, finance/accounting and operations management. Vicki has provided services to clients in many industries in the public, private and nonprofit sectors.
Vicki has a business-oriented approach to auditing and offers an integrated skill set that has been instrumental in helping her clients design and establish their internal audit and operational management programs, as well as, deliver high quality internal audit out-sourcing and co-sourcing, risk assessment, project assurance, SOX, Information Technology, Financial, Fraud and Compliance services.

Vicki is a Certified Internal Auditor (CIA), Information Systems Auditor (CISA) and Fraud Examiner (CFE).

Have Something of Interest 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 submit or for more information, please contact our Newsletter Editor. Email: Newsletter@isaca-kc.org

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 12, 2012	Brio	*Enterprise Risk Management* Vicki Wagoner - PwC
February 2, 2012	Ritz Charles 9 am—4 pm	Joint Meeting with IIA, *Auditing Social Media*—See notice below
March 8, 2012	Figlio's Tower	*ISACA IT Control Objectives for Cloud Computing* Rob Stroud - CA Technologies
April 12, 2012	The American Restaurant	*Emerging Technologies for Cardholder Data* Ulf Mattsson - Protegrity
May 10, 2012	TBD	Annual Business Meeting Topic TBD

Has Your Email Address or Your Mailing Address Changed ?

Go to the ISACA website (https://www.isaca.org/) and select the tabs "MyISACA"and then "MyProfile" and update your contact information.

February Joint Meeting with IIA

Auditing Social Media

Date: Thursday, February 2, 2012

Time: Registration 8:30am – 9:00am; Presentation 9:00am – 4:00pm

Lunch will be served at 12:00pm

CPE Hours: 6

Location: Ritz Charles, 9000 West 137th Street, Overland Park, KS 66221

Registration will open January 9th and close January 25th. Watch the ISACA website

Welcome to the Kansas City Chapter of ISACA!!

James Heavin
Richard Houston, CISM
George Anthony Jackson
Gary A. Johnson
Allison Mott
Joseph Searle, CISA
Dianna Sleyster
Brian Scott Weese, CISA
Michael Redding, CISA

Ethical Hacking and Network Security-Training

Plan now to attend the Certified Ethical Hacking (CEH v7) onsite training presented by Global Knowledge.

Location: Sprint Campus
Cost: $1,995 for ISSA and ISACA members; $2,195 for non ISSA or non ISACA.
Dates: February 13-17

For more information contact JoAnn Fisher at **joann.fisher@capgemini.com** , cell 816-830-2002 **or** go to: http://kc.issa.org/

Register by clicking on the following link: http://events.constantcontact.com/register/event?llr=olwqokfab&oeidk=a07e4sscq3r0ff1b222 or type http://mcaf.ee/9mvix

2011-2012 Board Members

President
BJ Smith
president@isaca-kc.org

Vice President
Wendy Dobratz
vp@isaca-kc.org

Secretary/Newsletter
Molly Coplen
Secretary@isaca-kc.org

Treasurer
Matt Suozzo
Treasurer@isaca-kc.org

Webmaster
Nila Henderson
webmaster@isaca-kc.org

Directors
Kevan Brewer
Jennifer Harper
Alfie Mahmoud
directors@isaca-kc.org

Programs Committee
Reed Anderson
Heidi Zenger
Michelle Moloney
Dan Sterba
Chin Modha
Anthony Canning
programs@isaca-kc.org

Calendar of Events

January

12 January .....ISACA chapter meeting, *Governance, Risk and Compliance*

12 January .....ISACA webinar, *Mapping Application Security to Compliance, http://www.isaca.org/Education/Online-Learning/*

February

2 February .....ISACA chapter meeting with the IIA, *Auditing Social Media*

8 February .....Deadline, early-bird registration for June 2012 certification exams

9 February .....ISACA webinar

March

8 March.....ISACA chapter meeting, *Qualitative and Quantitative Risk Analysis*

Meet Your Board Member—Kevan Brewer, ISACA Director

Previous Roles: *President, Vice President, Treasurer*

Time on Board:*7 years*

Employer and Position: *Quadis Technologies (Microsoft Dynamics CRM Consultant)*

First Job: *Finance Department at Commerce Bank, assisting with payroll, fixed assets, and tax workpapers*

Books Currently Reading: *the Bible*

Favorite Indoor or Outdoor activity: *Golf*

Chore you hate to do: *Ironing, and timekeeping!*

If you could meet anyone living or dead, who would it be? *My great-grandparents, who came to the US from Belgium*

If you could witness any event, past or future, what would it be? *The creation of the world*

Person you admire most: *My pastor, for his dedication and the work he does.*

What is one of your favorite quotes: *"I'm too blessed to be depressed!"*

State of the Data Center 2011—Emerson Network Power…..

http://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery-planning/GroupDocuments/Emerson%20Network%20Power_Data%20Center%202011%20infographic.pdf

- $53 Billion in CYBER WEEKEND SALES is larger than the entire economy of Bulgaria
- 1 of every 13 people on earth are active FACEBOOK users
- Every second, 1,157 people start watching YOU TUBE, that is 100,000,000 videos per day
- Daily TWEETS, in February 2011, averaged 14 million, almost 3X the 50 million Tweets sent every day February 2010.
- A server purchased in 2011 has an average 45X MORE COMPUTE CAPACITY than a similarly configured server installed in 2001.
- Every hour, enough information is consumed by INTERNET TRAFFIC to fill 7 million DVDs. Side by side, they would scale Mount Everest 95 times.

News from ISACA

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.

Using the ISACA Wiki to Build New Knowledge

Have you ever looked for an audit program only to discover that one is not available? If you could ask hundreds or even thousands of your colleagues to help create the audit program, would you? Using the collaboration tools on the ISACA web site allows you to do just that. By creating a wiki and inviting others to provide input, you can benefit from the experience and expertise of other members. Wikis are available in all Knowledge Center topics. Just find the topic that matches the subject matter and then create your wiki. Here are the steps to create your wiki.

Log on to the ISACA web site and navigate to *www.isaca.org/knowledgecenter*. From there, click on the + button next to Wikis to start a new wiki or to view all existing wiki pages. ISACA members are able to edit any of the existing wiki pages by clicking on the title of the page and then clicking on the Edit button.

1. On the wiki page, click on the Edit link.
2. Add your wiki title at the bottom of the page in [[ ]] and click OK.
3. The page reloads and displays your new wiki as a link. Click on your wiki title.
4. Add content to your wiki page. When you are done, click Create.
5. Your content is now posted to the wiki.

Your final step is to advertise that your wiki is available. ISACA recommends that you start a discussion within the topic and link your wiki within the discussion. This will give the wiki additional visibility. Contact *wiki-help@isaca.org* with any questions you may have.

7 Common Threat Areas

By Leighton Johnson, CISA, CISM, CIFI, CISSP

In the current Internet-based world, there are common threat areas to be aware of and plan for as we provide security services to our customers and clients. They are:

1. **Data breaches**—The current trend of stealing corporate data for financial or ideological reasons has lead to wide-reaching political and economic fallout. There are multiple possible sources for these data thefts including, among others, compromised accounts, web attacks and insider threat realization. There are reports of large-scale data breaches appearing in the press with regularity. Both internal compromised accounts and external attacks against web sites and networks have been the source of these attacks. Always be on watch for potential exfiltration of corporate data as an indication of a potential data breach.
2. **Identity theft**—The current statistics on identity theft are somewhat staggering. The US government is reporting that there is an identity stolen every 3 seconds. The incredible ramifications of personal loss and stress cause many to experience a lack of guidance and policy in this area. The means for such attacks are usually phishing e-mail attachments being sent via personal and corporate e-mail accounts. The best way to handle all e-mail is to "distrust by default" all e-mail attachments, no matter where they come from or who sent them.
3. **Web 2.0 attacks**—The proliferation of embedded malware on legitimate web sites has lead to computers being attacked by unknown assailants from normal web activity. The actual sites are infected by pictures or mashup actions wherein malware is installed via pictures, images, searches or scripts that then install them when these "pictures" are read by the unsuspecting browser.
4. **Messaging attacks**—E-mail and instant message still provide the largest spread of questionable content on the Internet. Standard spam accounts for more than 85% of all e-mails travelling the Internet on a daily basis and these messages provide attackers a way into personal and corporate servers. The incredible range of computing devices and models in the current world require the security professional to constantly be aware of the messaging methods for attack.
5. **Botnets and zombie computers**—The primary reason for computers being infected and the incredible increase in botnets is very simple: money. Given the current economic state globally, these programs allow the criminal element to obtain large sums of money with relative ease and low risk. Always be on the lookout for machines running when they should be off and communicating on new or different channels, which can indicate they are part of a botnet.
6. **Rootkits**—These programs are usually targeted attacks against a specific company or person, very technical in nature, extremely difficult to detect, and even harder to remove once detected. These programs are designed to run below the operating system on the computer, while most security software runs at the operating system level; therefore, such security software will not detect these malicious programs running. One possible way to determine if a rootkit is running is to monitor the system processing channels while the machine is operating; however, the machine would most likely not reflect this activity if it was turned off.
7. **Logic bombs**—Logic bombs are pieces of code or scripts attached to legitimate code that operate in the normal computing environment, but have time-based triggers to cause detrimental or malicious effects. These are almost always loaded by insiders who are disgruntled or angry. Always watch the activity of soon-to-be ex employees or passed-over administrators for these types of activities.

Each area of your computing environments has the potential to be attacked and have a malicious or detrimental effect on you, your organization or a customer. So always be on guard as you provide security services for them and yourself.