



2010 - 2011 Officers:

- President
Kevan Brewer
- Vice-President
BJ Smith
- Secretary
Wendy Dobratz
- Treasurer
Nila Henderson
- Director
Jennifer Harper
- Director
Alfie Mahmoud

In this issue:

ISACA-KC Monthly Meeting	1
Upcoming Monthly Meetings and Calendar of Events	2
News from ISACA	3
Article on Data Leakage	4

March Meeting Details

Enterprise Risk Management

Mrs. Suzanne Williams, Vice President and Chief Audit Executive, from Sprint will be joining the March 10 ISACA chapter meeting to review Sprint's leading practices regarding Enterprise Risk Management (ERM). The internal audit function at Sprint is responsible for facilitating ERM. However, management owns the process, with the board of directors providing oversight and governance. ERM is integrated with Sprint's audit planning process. Sprint conducts an enterprise-wide risk assessment and an audit risk assessment together. The results of the assessments are reviewed with the CEO and the company's lead team to select the top risks that focus on strategy, operations, financial and compliance. The top risks are assigned executive owners who then create mitigation plans and key measurements. Top ERM risk are monitored and reported up through the board of directors quarterly. All ERM risks are continuously evaluated / monitored by Sprint's internal audit function, risk council and risk steering committee. Suzanne will share with local chapter members Sprint's approach as to how ERM is integrated into the audit planning process; how ERM risk are identified, evaluated and selected; how ERM risks are continuously evaluated; and how top ERM risks are monitored and reported up through the board of directors.

Date: March 10, 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

Parking: Valet parking provided at no charge. Garage parking validated for up to 3 hours.

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

CPE: 2 Credits

Menu: TBD

The information presented and included in accompanying materials (if any) is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although the speaker and content authors endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Mrs. Williams began her career with Sprint almost 18 years ago as a management trainee and has moved quickly through the ranks of leadership with the Corporation. Prior to her promotion as an Officer at Sprint in 2008, Suzanne had served in a variety of roles in the Finance Organization, including the role as Director of Corporate Audit Services. In her current executive position she is responsible for risk assessment and internal audits throughout the corporation, reporting to the Audit Committee of the board of directors. Under Suzanne's direction, her Audit team delivered over \$100 million in cost avoidance and in the same year was honored with the Corporate Leadership Award for an audit of the Customer Care organization.

Suzanne is a member of the Institute of Internal Auditors (IIA) and previously served on the Kansas City Chapter IIA Board. She served as the 2009 United Way Executive Champion for the Finance Organization at Sprint. Suzanne is also a member of The Children's Place Board of Directors. Suzanne is a certified public accountant and received a bachelor's degree in accounting from Kansas State University in 1993. In 2008, she received a Certificate in Executive Education from Georgetown McDonough School of Business. Suzanne and her family reside in Leawood, Kansas.

Save the Date!



KC Chapter Spring Training

Securing and Auditing PeopleSoft Applications

16 CPE
May 9-10, 2011
Intermediate Level

More Information
Coming! Check the
KC ISACA website at
<http://www.isaca-kc.org/>

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 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
March 10, 2011	The American Restaurant	<i>Enterprise Risk Assessments</i> Suzanne Williams, VP of Internal Audit - Sprint
April 14, 2011	Doubletree Hotel Overland Park 7:30 am registration 7:45 am breakfast 8:30 –10:30 am program	<i>eDiscovery</i> BJ Stephan - Fishnet Security
May 12, 2011	Plaza III Steakhouse	<i>Annual Business Meeting</i> <i>Topic TBD</i>

Calendar of Events

March

- 10 MarchKC ISACA meeting, *Enterprise Risk Assessments*
- 10 MarchISACA Webinar, *Address Regulatory Mandates for Data Encryption without Changing Your Applications*
- 14-18 March.....ISACA Training Week, New Orleans
- 31 MarchCRISC Grandfathering Deadline

April

- 6 April Certification Exam Deadline
- 14 April KC ISACA meeting, *eDiscovery*

May

- 9-10 May KC ISACA Spring seminar, *Securing and Auditing PeopleSoft Applications, 16 CPE*
- 12 May KC ISACA *Annual business meeting, and program TBA*
- 15-19 May.....North America CACS, Las Vegas, NV



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

Report Says Best-Performing Organizations Are Using COBIT

A new report by the IT Policy Compliance Group (ITPCG), titled "How the Masters of IT Deliver More Value and Less Risk," reveals findings from research conducted on organizations with the best-performing IT and what they are doing differently with IT to deliver the most value and least risk, compared with all other organizations. The major findings reveal several management practices, tools and supporting IT systems that are unique to the "masters of IT."

According to the report, the masters of IT are using COBIT, IT balanced scorecards and IT portfolio management to improve alignment and deliver more value. The report states, "The use of COBIT, IT portfolio management, IT balanced scorecards and IT strategy maps were found to be emerging management tools in 2005 and 2006, were more widely adopted by 2008, and by 2010 are the principle strategic tools being employed by the best-performing organizations to manage and govern value and risk related to the use of IT."

This widespread adoption confirms previous findings, including the use of COBIT to manage and govern the value being delivered by IT and the use of IT governance, risk and compliance (GRC) systems with COBIT. According to the report, "COBIT is now the principle strategic tool employed to manage value and risk related to the use of IT."

The report points out that the COBIT management tools go beyond strategic alignment by including delivery of value, management of risk, measurement and assessment of performance. Because of this, the report states, when it comes to managing value and risk related to the use of IT, the best-in-class organizations consistently take the same actions: governance of IT via the use of COBIT and the preservation of value and management of risk through the use of IT GRC systems, COBIT, ISO and CIS benchmarks.

The full report is on the [ITGI Global Survey Results](#) page of the ISACA web site. More information on COBIT can be found on the [COBIT](#) page.

Deadline for CRISC Grandfathering is March 31, 2011

Until 31 March 2011, IT professionals who have significant experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance can apply for certification as a CRISC without being required to pass the CRISC examination. See the ISACA website, <http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/Grandfathering-Program.aspx>

Congratulations to ISACA Members for Passing the December 2010 CISA Exam



Carl D. Clift
Bonnie L. Lilly
Saadia N. Mahmood
Mr. Thomas Scuderi
Stephen Craig Evans

2010-2011 Board Members

Kevan Brewer
President
kevan_brewer@yahoo.com

BJ Smith
Vice President
BJSmith@dtsystems.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
membership@isaca-kc.org

Molly Coplen
Newsletter
Newsletter@isaca-kc.org

Jennifer Harper
Director
j1211biz@gmail.com

Alfie Mahmoud
Director
amahmoud@kpmg.com

5 Ways to Limit Data Leakage and Exposure

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. **Develop a clean-desk policy that includes a clean-white-board policy for conference rooms and public areas.** Data leakage and exposure can come from the most obvious and innocent of oversights by personnel who have access to or handle sensitive data. A clean desk policy will ensure that sensitive information that is being used during the business day is not viewed or removed by unauthorized personnel when not under the direct control of the authorized personnel. A clean-white-board policy (which includes nightly cleaning of conference rooms and public areas) will ensure that sensitive information is not viewed by personnel who are appropriately using facilities but are not authorized to view sensitive data.
2. **Implement secure printing.** Even in the age of the paperless office, more and more people are printing sensitive materials than ever before. Sensitive documents are often left at communal printers for long periods of time where anyone can read them or collect the printouts. Using secure printing capabilities, such as follow-me printing or PIN-required printing for sensitive documents, will ensure that the printer only activates when the authorized user is near the printer and ready to pick up the printout.
3. **Implement and maintain an asset inventory.** Data leakage and exposure often occur when sensitive or controlled data are unaccounted for and not in the direct control of the data owners. Implementing and maintaining an asset inventory of both physical and logical data assets will allow an organization to identify and classify data and apply appropriate controls.
4. **Implement trust-but-verify policies and procedures for sensitive data.** The unfortunate reality of data leakage often is the fact that an insider either knowingly or unknowingly contributed to the incident. Individuals are less likely to act upon a malicious action, such as data theft, if they know their activities are being monitored. Implementing trust-but-verify policies and procedures for access to and handling of sensitive data will provide protection to both the individual and organization. The individual with privileged access will not have to worry about wrongful prosecution and the organization can quickly identify the scope as well as methods and practices used if a data leakage incident were to occur. Examples of trust-but-verify policy and procedures are pervasive and consistent logging and monitoring of all access and activities to technical infrastructure and environments that contain sensitive data.
5. **Establish hardware configuration password protection.** The ability for data leakage and exposure to occur has been greatly enhanced by the advanced technologies organizations deploy to their users and the vast amount of data that they store on these technologies. One area that should be protected in these situations but is often neglected is the hardware configuration's basic input/output system (BIOS) settings. Once an organization has established the settings for its users, the settings should be password-protected to prevent the user from changing them. This is especially important in the case of Bluetooth-enabled devices, which can allow a user to establish a short-range data network connection to mass storage devices (including smartphones) without being detected by typical network or application controls such as network-based intrusion detection or data leak prevention tools.

More information on data leak prevention is available in ISACA's [Data Leak Prevention](#) white paper, as a complimentary download to members and nonmembers.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC. Reprinted from @ISACA Volume 3: 2 February 2011