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

November 2011 Volume 4, Issue 3

In this issue:

ISACA-KC Monthly Meeting	1
Upcoming Monthly Meetings, and Events	2
Know Your Board Members, CISA Review Class	3
News from ISACA	4

Application Security Development

Date: November 10, 2011
Time: 7:30 AM Registration | 7:45 – 8:30 AM Breakfast | 8:30 – 10:30 AM Program
Location: Ritz Charles | 9000 W 137th Street | Overland Park KS 66221
CPE's: 2 Credits
Price: $35 members | $50 guests | $5 students
Presenter: Mark Carney, FishNet Security

The arena of application security continues to top CSOs list of challenges. Most organizations still seem to be taking a tactical approach to securing applications within their enterprises. Over years of working with customers, FishNet Security has compiled a comprehensive list of application security program "elements" through their experience in working with and interviewing numerous CSOs, business owners, and application developers. Through this presentation, FishNet Security will be walking through each of the 14 application security elements to share key points and the importance of considering these elements as part of your organization's corporate application security program strategy.

Speaker Overview:

As the Vice President of Strategic Services at FishNet Security, Mark Carney leads a group of seasoned security advisors that interface with CSOs, CROs, and CIOs of FORTUNE 500 and global institutions that assist these organizations with information assurance, managed services, and training professional services needs.

Mark has over 11 years of experience in the information security industry with significant expertise in the information security risk management, regulatory and privacy compliance, vulnerability management, application and database security, and incident management fields. At FishNet Security, Carney has worked with industry practitioners and CISOs to solve business and security challenges. He built the Information Assurance division into a multi-million dollar line of business, started the Payment Card Industry security and compliance practice, and led efforts enabling the company to become a PCI Forensic Investigator (PFI).

Before joining FishNet Security in 2002, Carney spent two years at Anderson in the Technology Risk Consulting division concentrating on information security, enterprise resource planning (ERP), application integrity, data mining analysis, and quality assurance testing. As an industry speaker, he has presented at various regional events and conferences, including ISSA, ISACA, HTCIA and Secure360, has served on the board of directors for the local Kansas City-ISSA chapter, and is a member of the local ISACA and InfraGard.

As an industry thought leader, he has published papers and articles in various journals and periodicals, including Secure Computing (SC) Magazine, Chief Security Officer (CSO) Magazine, ISSA Password Journal, as well as been featured in CRN Magazine, TechTarget.com, Compliance Week, and the Kansas City Business Journal. Carney is a frequent guest lecturer for the Master's Information Security Course at the University of Kansas. Carney holds a both a Bachelors in Business Administration and an MBA, with an emphasis in management information systems, from the University of Missouri-Kansas City. Mr. Carney holds his CISSP, CRISC, and PCI-QSA certifications.

Renew your ISACA membership and record your CPEs by December 31.

Have something for the newsletter? Become published! Contact the newsletter editor at newsletter@isaca-kc.org

Looking for a new opportunity? Check out our Job Board at http://isaca-kc.org/jobs.php.

2011-2012 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
November 10, 2011	Ritz Charles Registration, 7:30 am; Breakfast, 7:45 am; Program, 8:30am	*Application Security Development,* Mark Carney
December 8, 2011	Figlio's Tower	Joint Meeting with ISSA, *Email Archiving as it relates to Governance, Compliance and Regulation and for eDiscovery FCRP*, Don Whitney
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*
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 *Data Breach Security Report from Verizon*

Calendar of Events

November

8 November — Virtual Trade Show, Cloud Security—How Safe is the Cloud? Presented by ISACA

10 November — ISACA Chapter Meeting, *Application Security Development, Mark Carney*

10 November — *Webinar, Limiting Audit Exposure and Managing Risk with Metrics-Driven Identity Analytics*

December

8 December — ISACA Chapter Meeting, Joint meeting with ISSA, *Email Archiving as it relates to Governance, Compliance and Regulation and for eDiscovery FCRP*, Don Whitney

10 December — CISA, CISM, CRISC, CGEIT exams

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

Membership Coordinator
Tim Carroll
membership@isaca-kc.org

Know Your Board Member

Matt Suozzo, Treasurer

Time on Board: *3 years, previously served as the Membership Coordinator*

Employer and Position: *Kansas City Southern Railroad, Sr. Mgr Information Systems Audit*

Time in job: *Just under a year and a half*

First job: *When I was 12 I was a paper boy for the Leavenworth Times*

Books currently reading: *"Unbroken", by Laura Hillenbrand. It's a true story about a POW's survival during WWII*

Favorite indoor or outdoor activity: *Indoor – Trying to keep up with my 15 month old daughter. Outdoor – Playing soccer, BBQ, and skiing. I'm also just getting into brewing my own beer, so I guess that would qualify as both an indoor and outdoor activity!*

What chore do you absolutely hate doing? *It's a tie between doing the dishes and cleaning the leaves out of my gutters*

What is one of your favorite quotes? I like these 2:

"I have not failed. I've just found 10,000 ways that won't work." - Thomas Edison

"Nobody can go back and make a new beginning, but everyone can start here and make a brand new end." – Maria Robinson

CISA Review Class

CISA Certified Information Systems Auditor

Register at http://isacabrcisareview2011.eventbrite.com.

The ISACA Baton Rouge Chapter is hosting a CISA review for the December 2011 CISA Exam. The CISA review will be held via webinar following the schedule noted below so that participants can fit the review into their busy schedules from the comfort of their home.

CISA Review Schedule:

Date(s)	Time	Domain Covered
November 1 & 3, 2011	6-8:30pm	Domain 5 (30% of exam content) – Protection of information assets
November 8 & 10, 2011	6-8:30pm	Domain 4 (23%) – Information systems operations maintenance and support
November 15 & 17, 2011	6-8:30pm	Domain 3 (19%) – Information systems acquisition, development, and implementation
November 22 & 24, 2011	6-8:30pm	Domain 2 (14%) – IT governance and management of IT
November 29 & December 1, 2011	6-8:30pm	Domain 1 (14%) – The process of auditing information systems

The cost to attend the ten webinars listed above will be $50 for members and $75 for non-members. Participants who register for and attend all 10 webinars will receive 25 CPEs. The material covered during the review is provided by the National ISACA Chapter and is best accompanied by the ISACA CISA Review Manual 2011, which is not included with the review. In addition, all participants will receive a practice CISA exam via email to review at their own pace. Once registered for the CISA review, participants will be emailed the necessary information to attend the webinars.

Chasin Frew, CISA, CFE
Information Technology Auditor
BlueCross BlueShield of Louisiana
Office: (225) 298-7847
E-Mail: chasin.frew@bcbsla.com

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

CPE Policy Change Regarding "Contributions to the Profession"

Ensure That You Have Earned Your 2011 CPE Hours

Effective 1 January 2012, the annual continuing professional education (CPE) hour limitation for each ISACA® certification will be increased from 10 hours to 20 hours for qualifying activities that fall under the category Contributions to the Profession. These activities include work performed for ISACA and other bodies that contribute to the IT audit, control, information security and governance professions.

Please note that there are only 2 months remaining to earn required CPE hours for the 2011 reporting year. CPE hours are reported annually during the renewal process. Maintaining certification requires the earning of 120 CPE hours over the 3-year cycle and earning at least 20 CPE hours in each cycle year.

To view the CPE policies and a complete list of qualifying activities, please visit the CISA, CISM, CGEIT and CRISC CPE policy pages of the ISACA web site.

Prepare for the CISA and CISM Exams With Free Self-assessments

ISACA® offers free self-assessments to help Certified Information Systems Auditor® (CISA®) and Certified Information Security Manager® (CISM®) exam candidates gauge their knowledge of the respective job practice areas and determine in which areas they may have strengths and weaknesses. Each self-assessment contains 50 sample items that cover the appropriate proportion of subject matter to match the respective exam blueprint. The items are not actual exam items, but are representative of items that have appeared on the respective exams. (Note that these self-assessments are not substitutes for the actual exams, nor do the results of the self-assessments guarantee or indicate future success on either exam.)

CISA and CISM candidates who are sitting for the December 2011 exams are encouraged to utilize these self-assessments as they prepare. To take either self-assessment, please visit the CISA or CISM Self-assessment page of the ISACA web site. In addition to these resources, additional review materials for the CISA, CISM, Certified in the Governance of Enterprise IT® (CGEIT®), and Certified in Risk and Information Systems Control™ CRISC™ exams are also available on the web site. These resources include review manuals and study questions.

New White Paper and Audit/Assurance Programs are Now Available

The following resources have been released by ISACA:

- ***Web Application Security: Business and Risk Considerations***—The use of web applications in the enterprise has grown exponentially in the last decade. While businesses are benefiting in many ways from the new capabilities of these applications, the prevalence of inherent security vulnerabilities in web applications is creating significant exposure for many enterprises. This white paper explores the root causes of these vulnerabilities, examines the associated risk and impacts, and provides guidance as to how enterprises can alter their practices to mitigate this risk. Although this publication focuses specifically on web application security, the guidance presented applies to all types of software development activities. This and other white papers are available as complimentary PDFs on the White Papers page of the ISACA web site.
- **Audit/assurance programs**—These and other audit/assurance programs are available as complimentary Word documents for ISACA members on the Audit Programs page:

  Microsoft® Exchange Server 2010 Audit/Assurance Program
  Microsoft® SharePoint 2010 Audit/Assurance Program