@ISACA
RELEVANT, TIMELY NEWS
Volume 2, 15 January 2014

15-plus Years of Information Security Matters

In 2014, ISACA® is celebrating the 15th anniversary of Steven J. Ross’ Information Security Matters column in the *ISACA Journal*.

Read More

Enhanced Member Benefits for 2014

Thank you for your 2013 ISACA membership. ISACA is committed to ensuring that you are more than satisfied with your membership benefits. In 2014, we will continue to expand and enhance your membership benefits to ensure that you meet the ever-increasing demands of your field.

Read More

The “Yes, And…” Approach to IT Risk Management

By Jack Freund, Ph.D., CISA, CISM, CRISC, CIPP, CISSP, PMP

Far too often information security practitioners have shut the door to business requests. In response, calls have arisen for an end to “just say no” information security. Let us take it a step further: Advocate for a “just say yes, and…” approach to information security.

Read More

Updated CPE Policy for 2014

An important change to the CISA®, CISM®, CGEIT® and CRISC™ CPE policies has been made, effective 1 January 2014. The change applies uniformly to all ISACA certifications.

Read More

Book Review: *Roadmap to Information Security: For IT and InfoSec Managers*

Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

Roadmap to Information Security: For IT and InfoSec Managers, by Michael E. Whitman and Herbert J. Mattord, revisits the pervasive concept of information security in a different manner with a unique style. The book provides the essential body of knowledge required to build an information security program in an organization.

Read More

15-plus Years of Information Security Matters

In 2014, ISACA® is celebrating the 15th anniversary of Steven J. Ross' Information Security Matters column in the *ISACA Journal*. The first installment ran under the header "Security Matters" in volume 6, 1998, titled "If PKI Is the Answer, What Is the Question?" Beginning with volume 1, 1999, the now regular column went under the name IS Security Matters; the column was renamed Information Security Matters in 2010 to better address the growth of technology and the topics covered.

Steve reminisces that the first column was, in many ways, the most influential. "In those days, many people thought that a public key infrastructure was the solution to every IT security problem," he recalls. "I was unconvinced and was one of the first to question the common wisdom. A lot of industry leaders I know quoted that column."

The overwhelming response to that first article led to a regular column that has stood the test of time. "While PKI is no longer the hot topic, I think a lot of what I said in that first article is still relevant, especially a healthy skepticism toward the zealots who try to force their particular solution on everyone, whatever the problem might be." Steve's most recent columns have covered cybersecurity, business impacts of encryption, compliance and privacy.

ISACA thanks Steve for his years of service as an author and contributor, and we look forward

to many more thought-provoking articles. Read the current Information Security Matters column, "Extra, Extra, Read All About It," in volume 1, 2014, of the *ISACA® Journal*, and review previous installments in the *Journal* archives.

Enhanced Member Benefits for 2014

Thank you for your 2013 ISACA® membership. ISACA is committed to ensuring that you are more than satisfied with your membership benefits. In 2013, ISACA expanded membership benefits in many ways, for example:

- New standards in *ITAF, 2nd Edition*, effective 1 November 2013
- More Knowledge Center communities, including communities covering governance and management, cybersecurity, ISACA certification exams, and cloud computing
- An updated collection of more than 525 books from ISACA and third-party publishers in the eLibrary, specifically customized for members
- Increased networking opportunities with a global community of more than 110,000 information systems professionals
- Member-only discounts on more than 25 ISACA events, including training weeks and conferences around the world

In 2014, we will continue to expand and enhance your membership benefits to ensure that you meet the ever-increasing demands of your field.

If you have not yet renewed your membership, stay ahead of the curve and experience more growth. Sign into the ISACA home page and click the renew button on your My ISACA page. The deadline to renew is 15 January 2014.

The "Yes, And…" Approach to IT Risk Management

By Jack Freund, Ph.D., CISA, CISM, CRISC, CIPP, CISSP, PMP

Far too often information security practitioners have shut the door to business requests. In response, calls have arisen for an end to "just say no" information security. Let us take it a step further: Advocate for a "just say yes, and…" approach to information security.

Historically, those who practice improvisational comedy have adhered to several rules. These basic approaches to real-time comedy help keep the show going, and make them funny. Improvisational comics will tell you that the hardest thing to work with is another player who does not know these rules. Too often, they shut down the scene before it even gets started. For example, one may say, "Now Johnny, I've heard that you haven't been behaving well at school. As your father, I need to teach you a lesson." The performer playing Johnny has a

couple of choices about where this scene is going to go: He can immediately shut down the scene by saying, “No, we’re ice skating and I want to race,” or he can say something like, “Yes, and what does that mean for my upcoming ice skating competition?” The latter response keeps the scene going and keeps everyone involved.

Information security practitioners should similarly keep the scene going by saying, “Yes, and….” As an example, if the business says, “Let’s move all of our data to the cloud!,” your answer should be, “Yes, and let’s also talk about how to secure it.” This simple turn of a phrase can keep the actors involved and makes it clear you support the business’s endeavors.

Jack Freund, Ph.D., CISA, CISM, CRISC, CISSP, CIPP, PMP, manages a team of IT risk analysts for TIAA-CREF and chairs the CRISC Test Enhancement Subcommittee.

Updated CPE Policy for 2014

An important change to the Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) continuing professional education (CPE) policies has been made, effective 1 January 2014. The change applies uniformly to all four of these ISACA® certifications.

For those earning a passing score on a related professional examination on or after 1 January 2014, two times the number of CPE hours are earned for each examination hour. Previously, only one CPE hour was earned for each examination hour. For example, if a certified individual passes a related professional examination that was 4 hours in length, 8 CPE hours will be earned. This change in CPE policy does not change what is meant by “related professional examination.”

CISA, CISM, CGEIT and CRISC CPE policies are currently being updated on the web site to reflect this change.

June 2014 exam registration is now open. You can save US $50 by registering on or before 12 February. Learn more about the 2014 CISA, CISM, CGEIT and CRISC exam administrations in the 2014 ISACA Exam Candidate Information Guide.

Book Review: *Roadmap to Information Security: For IT and InfoSec Managers*

Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

Roadmap to Information Security: For IT and InfoSec Managers, by Michael E. Whitman and Herbert J. Mattord, revisits the pervasive concept of information security in a different manner with a unique style. The book provides the essential body of knowledge required to build an information security program in an organization.

It is both a detailed reference script for IT managers delving into the information security role and a dependable reference for expert practitioners. In addition to furnishing extensive foundational information security knowledge, the book guides the user on how to translate theory into practice; this is ultimately the book's strong suit.

Key features of the book include:

- Detailed technical and managerial reference tables throughout the text for deeper insight
- Information security self-assessment checklists enabling users to benchmark their developed/existing models against industry, compliance and continuous improvements norms
- An information security manager's checklist, which includes an international list of information security considerations for use in developing an information security program
- References for further reading at the end of each chapter
- A mapping of the Certified Information Security Manager® (CISM®) and Certified Information Systems Security Professional (CISSP) certification domains, which facilitates easy study for those pursuing these certifications

The book is an extensive repository of information framed into 9 parts with a total of 33 chapters. This book is well constructed to serve as an all-inclusive reference, how-to text that will not disappoint the reader with its rich content and no-nonsense approach.

Roadmap to Information Security: For IT and InfoSec Managers is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in the latest issue of the *ISACA Journal*, visit the ISACA Bookstore online or email bookstore@isaca.org.

Ibe Kalu Etea, CISA, CRISC, ACA, CFE, CIA, CRMA, ISO 9001:2008 QMS LA, is a corporate governance, internal controls, fraud and enterprise risk assurance professional. He also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).