

In This Issue:

- eBay Security Executive to Open ISACA Conference
- Five Tips for Better Communication With “the Business”
- Strategy Implementation Progresses With COBIT 5, CRISC and Other Initiatives
- Certifications Elicit Respect and Provide Competitive Edge
- Evolving Role of the IT Auditor

eBay Security Executive to Open ISACA Conference

ISRM North America • Las Vegas, Nevada, USA • 13-15 September 2010

This year's Information Security and Risk Management (ISRM) Conference will open with a keynote address titled “Building Trust in the Cloud,” presented by Dave Cullinane, chief information security officer (CISO) for eBay.

[Read More](#)

Five Tips for Better Communication With “the Business”

By Brian Barnier, CGEIT

When I teach sessions at ISACA's main conferences or local chapters, I often take a few minutes to talk about improving communication with “the business.” Here are five tips:

1. Realize that “the business” has many aspects—business lines (products or services), functional areas (e.g., IT, finance, human resources, marketing) and geographic areas. Each leader and team has its own objectives.

[Read More](#)

Strategy Implementation Progresses With COBIT 5, CRISC and Other Initiatives

Early in 2009, ISACA® adopted a new strategy and immediately began working toward the objectives it outlined. A great deal of progress was made throughout the rest of that year and into the first part of 2010.

[Read More](#)

Certifications Elicit Respect and Provide Competitive Edge

Bala Natarajan, CISA, CISM, ACA, CIA, CPA, Director, SOAPProjects Inc., Shares His Experiences as a CISA and CISM

In an environment that was booming with IT governance, risk and control professionals, Bala Natarajan attended a seminar in 2002 by a local IT professional organization and found that it was packed to capacity by eager participants. The topic was “What Is an Information Systems Audit?”



[Read More](#)

Evolving Role of the IT Auditor

By Kris Budnik, ITIL, Deloitte & Touche, South Africa

Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0 was developed to help the IT auditor to expand the assurance program beyond the traditional operational aspects and into the realm of IT value management.

[Read More](#)

eBay Security Executive to Open ISACA Conference

ISRM North America • Las Vegas, Nevada, USA • 13-15 September 2010

This year's Information Security and Risk Management (ISRM) Conference in Las Vegas will open with a keynote address titled “Building Trust in the Cloud,” presented by Dave Cullinane, chief information security officer (CISO) for eBay. He will share his experiences in the security

arena at this leading Internet retailer.

The conference will also include many sessions on the cloud computing topic. These discussions are being offered to foster a greater understanding of information security within the cloud. ISACA and the [Cloud Security Alliance](#), along with the many speakers presenting at the conference, offer assistance to enterprises to help ensure effective governance and control over cloud computing.

The conference is an educational event geared specifically toward information security professionals and provides an opportunity for earning up to 32 continuing professional education (CPE) hours. Through its real-world solutions and interaction with industry leaders, the ISRM Conference will give security professionals tools that cannot be learned from textbooks.

On Monday, 13 September, join Oracle in the first Lunch and Learn at the ISRM Conference. This session is sponsored and presented exclusively by Oracle. Earn one CPE hour for this session. Arrive in the meeting room, where lunch will also be served, early as space is limited to 100 people. Check your program guide for room assignments.

[Click here](#) for more information about preconference workshops and sessions.

Five Tips for Better Communication With “the Business”

By Brian Barnier, CGEIT

When I teach sessions at ISACA’s main conferences or local chapters, I often take a few minutes to talk about improving communication with “the business.” Here are five tips:

1. Realize that “the business” has many aspects—business lines (products or services), functional areas (e.g., IT, finance, human resources, marketing) and geographic areas. Each leader and team has its own objectives.
2. Look at IT from the business leader’s view. Consider the plant manager who sees the equipment, people and materials coming together in a process to create a product. Think about the role IT plays in enabling that process. Be able to clearly explain the dependencies of that process on IT.
3. Express benefits in business terms. “Business terms” means market share, sales, costs, expenses, quality and customer satisfaction—criteria by which the person to whom you are talking is personally measured.
4. Remove abbreviations or IT shorthand from your documents. Get your materials to pass

the “spouse test” (i.e., test to ensure that your non-IT spouse understands what you are saying).

5. Use organizationally accepted presentation and report formats. Using familiar layouts, tables and graphs can make it easier for others to understand your point.

If these seem like common sense, that’s good. You are ahead of the game. Yet, obvious or not, they are difficult for busy, technically minded people to consistently do. Imagine working in a country with another language. You might still think in your native language, but must constantly translate. Your opportunity to shine is to be the person who translates.

Brian Barnier, CGEIT, is a principal at ValueBridge Advisors. He teaches, speaks and researches widely. [Click here](#) to view a presentation by Barnier on the Risk IT: Based on COBIT® framework. Barnier can be reached at <mailto:brian@valuebridgeadvisors.com>.

Strategy Implementation Progresses With COBIT 5, CRISC and Other Initiatives

Early in 2009, ISACA® adopted a new strategy and immediately began working toward the objectives it outlined. A great deal of progress was made throughout the rest of that year and into the first part of 2010. A few highlights include:

- COBIT® 5—A volunteer task force created a [design plan](#) (exposure draft), outlining what COBIT 5 will encompass, and posted the plan for expert review. Many comments and suggestions were gathered, revealing strong support of the direction COBIT will take in its next iteration. The comments are being considered as development continues. COBIT 5 is scheduled for release in 2011.
- Pragmatic guidance—The strategy recognizes that ISACA members and constituents need practical assistance they can use immediately. New audit programs will be issued later in 2010. Also, work is underway on a series of white papers, designed to be brief (about 10 pages) and pragmatic, providing members a quick, high-level understanding of a topic and an indication of how it affects them. The white papers will be offered as free downloads from ISACA’s web site. White papers on [cloud computing](#) and [social media](#) are already available, and additional papers on the new service auditor standard and securing mobile devices are close to completion.
- Add-on certificates—These are certificates to be “added on” to an existing ISACA certification, to recognize a particular area of expertise. Topics are still under study, as is the notion of partnering with other organizations to develop the certificates.
- [Certified in Risk and Information Systems Control® \(CRISC®\)](#)—ISACA’s newest certification was identified in the strategy as a way to recognize 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. It is designed particularly 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. The **grandfathering period** has begun and the first exam will be offered in June 2011.

- Viral marketing—"Word of mouth" marketing is occurring on various social media sites and is really taking off. ISACA and its products average more than 1,000 messages per month through various sites such as Twitter, Facebook, LinkedIn and deli.ci.ous.
- **Open source platform**—This became available on 3 June 2010, when the new web site went live. Members are encouraged to participate; sharing your experience and expertise makes the ISACA knowledge community unique and strong.

Certifications Elicit Respect and Provide Competitive Edge

Bala Natarajan, CISA, CISM, ACA, CIA, CPA, Director, SOAProjects Inc., Shares His Experiences as a CISA and CISM



In an environment that was booming with IT governance, risk and control professionals, Bala Natarajan attended a seminar in 2002 by a local IT professional organization and found that it was packed to capacity by eager participants. The topic was "What is an Information Systems Audit?"

This piqued his interest in the IT profession and was his first step toward pursuing the Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) certifications. "I was truly impressed as I observed how people flocked to learn about audit, risk and compliance," Natarajan recalls.

"Ever since I obtained the world-renowned and respected CISA and CISM certifications, the opportunities to enhance my career in the field of information systems audit, risk, governance and compliance have increased tremendously," explained Natarajan. "I have become more confident as an individual and my professional colleagues look up to me with respect, which has infused in me a sense of pride."

Natarajan feels that more companies are realizing that managing an effective information security function within the organization is critical to improve their security posture, reduce risks of unauthorized access and, at the same time, align security requirements to ever-changing business needs. "With the CISM designation, I have found there has been a spurt of opportunities in my professional career over the last three to four years," he said. "Managing

the security function can be a challenge and, thanks to the CISM designation, my outlook toward that function has changed a lot," Natarajan said. "Management at my company now perceives the value that I bring to the table as a CISM holder."

To remain current in the IT environment, Natarajan feels continuing education is key. As the adage says, "Knowledge is strength." And, considering the recent global economic crisis, he feels it is more important than ever to think about how to stay competitive. However, Natarajan finds that staying abreast with the latest trends, technology and best practices can be a challenge. "Thanks to ISACA's top-notch, quality educational programs, the challenges have been largely addressed," he said.

Among the many opportunities for ISACA® members to earn continuing professional education (CPE) hours, Natarajan has discovered what he feels are fun and easy ways of earning them. "I write items for CISA, CISM and Certified in the Governance of IT® (CGEIT®) examinations; participate in quality reviews conducted by ISACA; volunteer for local ISACA chapter activities; mentor students for examinations; and attend programs conducted by local chapters. Using a combination of these activities makes it fun because I get an opportunity to interact with professional peers and discover how to do things differently, all while achieving the objective of getting CPEs to adhere to the Continuing Education Policy and retain my certifications," he explained.

For graduating students of the IT profession, Natarajan says success can be achieved by adopting a career path in information systems audit, control and governance, as there are many untapped opportunities. "Earning ISACA certifications have become a benchmark for employers to short-list potential candidates to fill job positions," he added. "In addition, active participation with the local ISACA student chapter and/or with the local ISACA chapter can help students interact with experienced professionals who can guide them regarding their career options."

Bala Natarajan, CISA, CISM, ACA, CIA, CPA, is a member of the ISACA Silicon Valley Chapter (California, USA) and has been the chapter's president, treasurer and a member of the finance committee.

Evolving Role of the IT Auditor

By Kris Budnik, ITIL, Deloitte & Touche, South Africa

The role of the IT auditor must evolve, moving beyond the assessment of adherence to processes, to providing insight and assurance in respect to IT's contribution to the achievement of business objectives. In my experience, much of the focus behind IT audit has been on operations—the evaluation of the adequacy of operating procedures against so-called "best practices"—often without much consideration of the context that drives IT to perform in a particular manner. That is not to say that this aspect of IT audit is unimportant; however,

without context, much of the value of the audit is diminished. The opportunities to foster an improved control culture, highlight risks and introduce mitigating practices are lost, because recommendations (even the good ones) are seen as irrelevant and are ignored.

The publication of the Val IT™ 2.0 framework brought with it a great opportunity to position IT as a significant business enabler (deserving close operational oversight and management) and to place it squarely into the context of core business, deserving critical assessment of the strategic value that IT-related investments deliver. *Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0* was developed to help the IT auditor to expand the assurance program beyond the traditional operational aspects and into the realm of IT value management.

Gaining an understanding of the risks that may erode IT value and/or its operational effectiveness sets an important foundation for the context-specific assurance program. A vital tool at the assurance professional's disposal to facilitate this is Risk IT: Based on COBIT®. This new framework provides guidance on effective techniques for the identification of risks to the IT environment, which, in turn, enable the identification of relevant mitigating controls in respect to the preservation of optimum IT benefit/value enablement, IT program/project delivery, and IT operations and service delivery.

IT Assurance Guide: Using COBIT, Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0 and *The Risk IT Framework* are like three legs of a table—each is essential to ensure that the IT audit/review can stand up to scrutiny. These publications are available in the [ISACA Bookstore](#). For information, see the ISACA Bookstore Supplement in the latest issue of the *ISACA Journal*, visit the [ISACA Bookstore](#) or e-mail bookstore@isaca.org. [Click here](#) to learn more about recently released ISACA research publications.

Kris Budnik, ITIL, is director of security and privacy at Deloitte & Touche, South Africa.

