@ISACA
RELEVANT, TIMELY NEWS
Volume 12, 8 June 2011

In This Issue:

Survey: Employee-owned Mobile Devices Are Riskiest

2011 ISACA IT Risk/Reward Barometer Shows Increase in Cloud Adoption and Information Security Jobs

Forty-five percent of IT leaders worldwide believe that any employee-owned mobile device poses a greater risk to the enterprise than mobile devices supplied by the company, according to the 2011 ISACA IT Risk/Reward Barometer, a survey of 2,765 ISACA® members and IT professionals. Yet, approximately a quarter of the respondents still believe that the benefits of employees using mobile devices at work outweigh the risks.

Read More

Ask Five Questions Before Assessing Your Controls

By Brian Barnier, CGEIT

Risk and control assessments are basic tools. Everyone uses them and most struggle with them. These assessments can quickly become wasteful or distracting if key prerequisites are not met.

Read More

Security Field Offers Abundance of Opportunities

Anjali R. Atanacio, CISM, CRISC, CISSP, Shares Her Experiences As a CISM

"The security field offers an abundance of opportunities for learning and work areas to pursue. The challenges of the interconnected world through computers and networks brought about the continuous need for more skilled and knowledgeable people…"

Read More

ISACA Offers Multiuser Discounts for COBIT Online

Did you know that ISACA offers a corporate multiuser subscription for COBIT® Online? The corporate pricing model provides a discount off the annual full subscription rate for both members and nonmembers. The more users a company subscribes, the greater the discount.

Read More

Knowledge Center Topics Exceed 5,000 Unique Members—Join a Topic Now!

Among Its Features: Rate Discussions

ISACA's Knowledge Center welcomed its 5,000th topic member. With more than 10,000 total community members (users frequently join more than one topic) and the regular addition of new topics, such as cybersecurity in recent weeks, growth in the Knowledge Center is expected to continue to increase.

Read More

ISACA Survey: Employee-owned Mobile Devices Are Riskiest

2011 ISACA IT Risk/Reward Barometer Shows Increase in Cloud Adoption and Information Security Jobs

Forty-five percent of IT leaders worldwide believe that any employee-owned mobile device poses a greater risk to the enterprise than mobile devices supplied by the company, according to the 2011 ISACA IT Risk/Reward Barometer, a survey of 2,765 ISACA members and IT professionals. Yet, approximately a quarter of the respondents still believe that the benefits of employees using mobile devices at work outweigh the risks.

The survey found that IT organizations are increasingly being asked to manage the growing trend of "BYOD" (bring your own device), as employees take advantage of more powerful and affordable mobile devices that let them work from any location. "BYOD presents both opportunities and threats," said John Pironti, CISA, CISM, CGEIT, CRISC, CISSP, advisor with ISACA and president of IP Architects LLC. "Organizations should educate their employees on their BYOD security requirements and implement a comprehensive mobile device policy that aligns with the organization's risk profile."

The IT Risk/Reward Barometer, now in its second year, helps gauge current attitudes and organizational behaviors related to the risks and rewards associated with IT projects and emerging trends. To see the full results, visit the Risk/Reward Barometer page of the ISACA web site.

Another key finding is that cloud computing is growing in acceptance. "Because security is still a concern with cloud services, organizations recognize that they must take measured risk in cloud deployment. But it is a calculated risk they will take because they know that stifling the use of cloud computing to avoid risk could actually stifle business growth," said Robert Stroud, CGEIT, international vice president of ISACA and service management, cloud computing and governance evangelist at CA Technologies.

ISACA's World Congress: INSIGHTS 2011 conference 27-29 June near Washington DC will cover many of the issues featured in the IT Risk/Reward Barometer, including cloud computing. Senior-level government officials and executives from Fortune 500 companies will share expertise on emerging technologies in the context of business value and compliance at this inaugural event.

The survey also indicated that, despite a sluggish economic recovery, a surprisingly high percentage of respondents expect their organization's staffing requirements for information security and risk management to increase over the next year.

Ask Five Questions Before Assessing Your Controls

By Brian Barnier, CGEIT

Risk and control assessments are basic tools. Everyone uses them and most struggle with them. Ask five people at a conference and you will find that even the name is not uniform—risk *and* control self-assessment, risk control self-assessment, control self-assessment. These assessments can quickly become wasteful or distracting if key prerequisites are not met.

To avoid problems, ask yourself five key questions:

1. Do we "know the business"? Many assessments are focused only on known risks, controls and weaknesses ("watched pots"); they miss weaknesses that are less apparent and those in the underlying process.
2. How sound was the risk evaluation that led to the controls being designed and implemented? Assessments depend on properly completed prior steps in risk evaluation and response, including environment and enterprise capability evaluation, scenario analysis, root-cause analysis, dependency analysis, control design, and control implementation. If not sound, it is likely that the wrong controls are assessed and that the findings have little value.
3. Does the assessment cycle keep pace with real-world change? If change in risks (environment and process, or controls) is more frequent than the evaluation period, the assessments will miss real risk. For example, if your IT environment changes every few months, business continuity test cycles should match that cycle—anything else gives a false sense of confidence.
4. Do control assessments actually focus on controls or do they mix in policies, procedures or rules? "Green" ratings for the existence of policies is a long way from examining a control that can detect an out-of-bounds conditions and act on that information.
5. Do assessments divert attention from daily *use* of risk management? Both lag time and emphasis on control (rather than environment or business capabilities) have a tendency to cause organizations to see risk management as only a "bandage" assurance function, rather than a valued management function that fixes root causes.

If they fall into the traps noted here, risk or control assessments probably also divert resources from more helpful risk management activities and create a false sense of assurance. These traps have led to serious harm. Consider data breaches, frauds, network outages, robo-signings and other problems that occurred when controls were, on paper, acceptable. Of

course, assessments and tests must be applied with appropriate rigor to drive meaningful action. The good news is that these problems are relatively easy to fix.

This article was adapted from Brian Barnier's upcoming book *The Operational Risk Handbook for Financial Companies*.

Brian Barnier, CGEIT, is a principal at ValueBridge Advisors, where he analyzes trends and advises/mentors business and IT leaders to help them accelerate business performance improvement, including risk management. In the past, he has held business, IT and risk roles. Barnier teaches, speaks and researches widely. He can be reached at brian@valuebridgeadvisors.com.

Security Field Offers Abundance of Opportunities

Anjali R. Atanacio, CISM, CRISC, CISSP, Shares Her Experiences As a CISM

Anjali Atanacio, information risk management consultant with Chevron, is an information security professional with more than 18 years of experience. A member of the San Francisco Chapter of ISACA®, she is the Certified Information Security Manager® (CISM®) coordinator and has been involved with training for the CISM exam. She finds the CISM and other ISACA certifications to be growing in importance and need.

"The ISACA certifications with a focus on security management (CISM) and risk management (Certified in Risk and Information Systems Control™ [CRISC™]) are timely since there is more adoption now of risk-based management of information and systems," Atanacio said. "The role of security managers demands the ability to determine areas of greater importance and impact to the business so there is more balance on security implementation and spending."

Professionals in the field seem to share Atanacio's view. "I have noticed the growing number of CISM-certified individuals," she said. "The increased registration at our CISM review workshop at the San Francisco Chapter of ISACA also shows increasing popularity and recognition of the value of the certification."

Atanacio also said certifications are top-of-mind during interviews. They command respect and appreciation, and can open doors to significant positions. "Some recruiters and hiring managers have asked me how current my certifications are," she explained. "With CISM in particular, you can be considered for more expansive positions, as they know those who pursue it have the security management credential that validates knowledge and experience."

Atanacio encourages those interested in entering the security field to take advantage of the growing industry. "The security field offers an abundance of opportunities for learning and work

areas to pursue," she said. "For me, since I am keen on learning new things, the security field has been a good avenue, given the continuous emergence of new technology, and, of course, the corresponding challenges."

When winding down from the demands of her job, Atanacio finds tending to her garden to be a very calming activity. She also enjoys reading and having cookouts with family, friends, and neighbors for good food and laughter. "I also love to travel, whether to nearby towns or the farthest country that my time (and bank account) will allow."

If Atanacio were not in the information security industry, she would have pursued a career in the public relations, advertising, marketing or sales field, and finds parallels to the two areas. "I love interacting with people, being creative and coming up with ideas to market or advertise something," she explained.

ISACA Offers Multiuser Discounts for COBIT Online

Did you know that ISACA offers a corporate multiuser subscription for COBIT® Online? The corporate pricing model provides a discount off the annual full subscription rate for both members and nonmembers. The more users a company subscribes, the greater the discount. There is a five-user minimum requirement.

COBIT Online allows you to construct and download a personalized version of COBIT, tailored to your enterprise. Components such as the framework, control objectives, inputs/outputs, RACI charts, goals and metrics, maturity models, control practices, and assurance steps can be chosen and filtered based on several search criteria.

Additional COBIT Online features include:

- Access to the knowledge base of COBIT
- Access to a search of COBIT's best practices
- Ability to perform benchmarking online
- Access to discussion forums

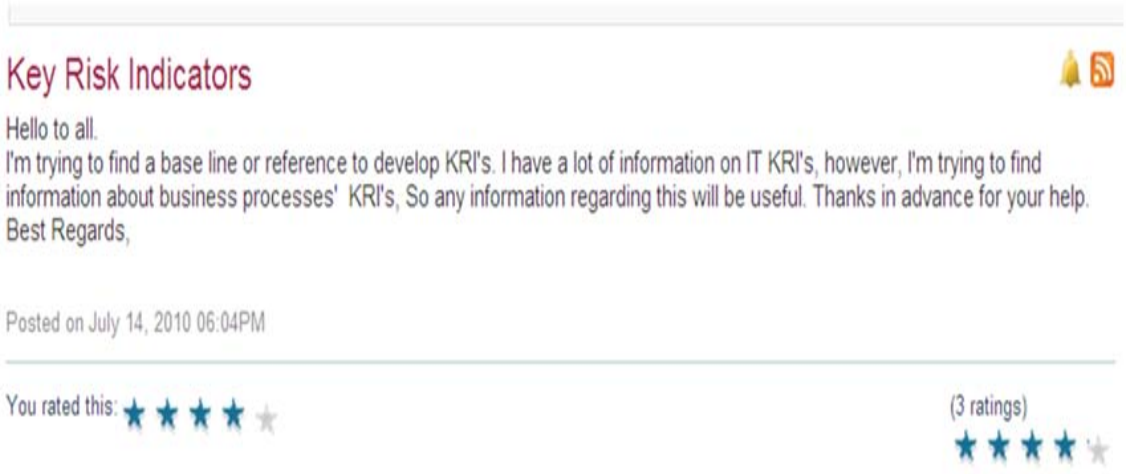
For more information, please view the Corporate Multiuser Subscription Conditions and the COBIT Online pages on the ISACA web site.

Knowledge Center Topics Exceed 5,000 Unique Members—Join a Topic Now!

Among Its Features: Rate Discussions

ISACA's Knowledge Center welcomed its 5,000th topic member. With more than 10,000 total community members (users frequently join more than one topic) and the regular addition of new topics, such as cybersecurity in recent weeks, growth in the Knowledge Center is expected to continue to increase. Topic members are contributing to ISACA by adding and responding to discussions, uploading documents, adding links to third-party resources, and creating blogs and wikis. Visit the Knowledge Center on the ISACA web site and join a topic today.

One of the many features of the Knowledge Center allows you to rate discussions. This is a great way to start participating if you are not quite ready to post or respond to a discussion. If you like or dislike what the author has posted, you can give the post from 1 to 5 stars. Each discussion and comment can be rated. Click on the number of stars you want to award the discussion on the left side of the screen. The page will refresh and your rating will show on the right side, averaged with all other ratings for the discussion. Here is an example:



Ratings benefit everyone in the Knowledge Center. A rating attracts attention to a discussion or a reply. It gives credibility for the author and can promote quality discussions. Which discussions get your attention?