ISACA Is on a Roll With New Benefits and Offerings

Are you up to date with all that is happening at ISACA®? In the first quarter of 2012 ISACA has seen a lot of exciting new developments. When you log in to the ISACA web site, review the ISACA Updates on the home page to see all the latest benefits and offerings.

Read More

Five Ways to Create a Risk-conscious and Security-aware Culture

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

Adversaries and the threats they pose to information are more advanced and daunting than ever and show no sign of becoming less concerning in the future. Creating a risk-conscious and security-aware culture within an enterprise can provide more protection for an enterprise's information infrastructure and associated data assets than any technology or information-security-related control that currently exists.

Read More

Leaders Bring INSIGHTS to ISACA’s Virtual Conference
During ISACA’s March Virtual Conference, Enterprise Risk Management: Provide Security From Cyberthreats, more than 3,000 attendees participated live in online conversations with discussion leaders Ron Ross, Ph.D., Marc Vael, CISA, CISM, CGEIT, and Theresa Grafenstine, CISA, CGEIT, CRISC, about trends in cybersecurity, risk management and vulnerability to cyberattacks.

Read More

ISACA Members Invited to Take Part in a United Nations Study on Cybercrime

The United Nations Office of Drugs and Crime (UNODC) has invited ISACA members to participate in the study, knowing that ISACA members are effective representatives due to their awareness and understanding of current and emerging trends in cybercrime.

Read More

IAASB Strengthens Standard on Using the Work of Internal Auditors

The International Auditing and Assurance Standards Board (IAASB) has recently released the International Standard on Auditing (ISA) 610 (Revised), Using the Work of Internal Auditors, which addresses the external auditor’s responsibilities if using the work of an internal audit function in obtaining audit evidence.

Read More

Insight Into the Audit, Risk, Control and Regulatory Environment: United Kingdom

By Andrew Richardson, CISA, CISM, CRISC, MBCS, MCI

The UK has a long history of auditing, the earliest reference being to the Auditor of the Exchequer in England in 1314. It was with the advent of the Industrial Revolution, from 1750 to 1850, that auditing began its evolution.

Read More
ISACA Is on a Roll With New Benefits and Offerings

Are you up to date with all that is happening at ISACA®? In the first quarter of 2012 ISACA has seen a lot of exciting new developments. When you log in to the ISACA web site, review the ISACA Updates on the home page to see all the latest benefits and offerings.

Some of the recent benefits, by month, that your ISACA membership includes are:

January
- Release of the COBIT 5 Executive Summary
- eSymposium: Identity Protection and Authentication
- Live webinar: Using a Six-step Process to Influence and Understand Behaviors
- Three new COBIT and Risk IT case studies released

February
- eSymposium: Best Practices and Controls for Compliance and Risk Management
- Live webinar: Concerned That Security Investments Still Leave You Vulnerable?

March
- ISACA Journal App now available for Android devices and the Kindle Fire
- Virtual Conference: Enterprise Risk Management: Provide Security From Cyberthreats

April
- Live webinar: Understand Cyberthreats in the ERM Ecosystem
- Release of COBIT 5 with a personalized PDF of all three COBIT 5 deliverables: COBIT 5 (the framework), COBIT 5: Enabling Process and COBIT 5 Implementation (US $225 value), free to members only.
- New COBIT case study: Using COBIT to Aid in Hospital Risk Management, Part 2

Five Ways to Create a Risk-conscious and Security-aware Culture
By John P. Pironti, CISA, CISM, CGEIT, CISSP, CRISC, ISSAP, ISSMP

Adversaries and the threats they pose to information are more advanced and daunting than ever and show no sign of becoming less concerning in the future. Creating a risk-conscious and security-aware culture within an enterprise can provide more protection for an enterprise’s
information infrastructure and associated data assets than any technology or information-security-related control that currently exists. This kind of capability can be a game-changing force multiplier if leveraged effectively.

Here are five things that you can do to help create this kind of culture in your enterprise:

1. **Use risk management to remove the fear of security**—Consider the psychology associated with the words “security” and “risk.” When a businessperson thinks of the word “security,” the first thoughts that come to mind are often prevention, disablement and disempowerment. This is a fundamental result of experiences that he/she has often had when interacting with security, and it negatively drives his/her perception of the functions and capabilities security provides. When that same individual hears the word “risk,” what typically comes to mind is understanding, management, control and empowerment. Therefore, alignment with risk at the onset often leads to greater acceptance than does security—in both terminology and approach.

2. **Work with business leaders and stakeholders to develop a business and information risk profile**—It is important to implement tools that enable business leaders and stakeholders to understand their risk appetite and their risk management requirements, as well as the parameters needed to align and manage their business activities in relation to risk. A key tool that can be used to create a risk-conscious and security-aware culture is the business and information risk profile. This profile establishes the bounds of acceptable loss, compromise, disruption or disablement of key and material business functions, individuals, activities, information and processes for an enterprise. An enterprise’s business and information risk profile also provides a framework and limits for the information risk management and security team to align their own activities to ensure that business expectations are met.

3. **Follow an embrace-and-educate approach**—The adoption and use of an embrace-and-educate approach to new ideas, concepts, technologies and solutions can help change the mind-set and culture; it involves positive feelings of the information risk management and security elements of an enterprise. In this model, the risk management and security elements of enterprises recognize and acknowledge the immediate value of the capabilities the business intends to use. At the same time, this model provides education to the user population regarding the identified risk and expectations of use to ensure that appropriate levels of security exist to align with the enterprise's risk profile. The key to success with this method is to use education and awareness techniques that can be easily understood and internalized by the intended audience. This often means the use of simple and easily understood terms, case studies, and examples that are readily identified as being applicable to the enterprise’s business activities.

4. **Provide personal benefits**—If individuals can derive personal benefit and value from the knowledge, insights and guidance provided to them about risk and security there is a high likelihood they will change their behaviors in both their personal and professional lives to be more risk conscious and security aware. An example of this can be a change in
behavior regarding the use of social networking solutions. These capabilities are often used by individuals for personal activities, but increasingly have business benefits as well. If you can effectively educate users on the risk associated with these solutions, as well as on safe and effective ways to continue to use them, they will most likely appreciate and be more open to your insights and ideas in the future. They will also most likely begin to adopt the safer use techniques in all environments, without even realizing they are doing so.

5. **Employ effective reinforcement methods**—Changing the mind-set and culture of an enterprise requires the use of effective and consistent reinforcement of the desired state. In doing so, it is important to identify the learning style, values and interests of the intended audience. The use of various methods and techniques to deliver messaging is essential to reach a diverse audience. This messaging can include in-person training and seminars, computer-based training and messaging (i.e., screen savers), visually stimulating and thought-provoking strategically placed signage, and positive messaging that demonstrates how the adoption of this new mind-set can promote success and benefit the enterprise as well as the individual.

This tips column draws from a volume 2, 2012, *ISACA Journal* article on the same topic. Learn more about this subject or other tips by reading “Changing the Mind-set: Creating a Risk-conscious and Security-aware Culture.”

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

---

**Leaders Bring INSIGHTS to ISACA’s Virtual Conference**

During ISACA’s March Virtual Conference, *Enterprise Risk Management: Provide Security From Cyberthreats*, more than 3,000 attendees participated live in online conversations with discussion leaders Ron Ross, Ph.D., Marc Vael, CISA, CISM, CGEIT, and Theresa Grafenstine, CISA, CGEIT, CRISC, about trends in cybersecurity, risk management and vulnerability to cyberattacks. These speakers can also be heard at the upcoming World Congress: INSIGHTS 2012.

Here is what attendees had to say about the Virtual Conference, which is now available for archived access, and its speakers:

- “ISACA provided an impressive lineup of speakers covering very relevant topics. I appreciated the opportunity to participate in such events, and I look forward to future presentations.”
- “ISACA virtual conferences enable me to expand my horizon and adapt my perspectives to meet challenges associated with the evolving risk landscape.”
- “Where else could you sit at your own desk, communicate with the top vendors in the fields impacting your business and interact with professionals in your discipline from every part
of the world? There is no other place I can think of.”
• “This Virtual Conference provided an excellent learning opportunity. Listening to industry veterans was simply wonderful. It had a mix of different flavors, all under one screen and at your own convenience.”

The discussion on cybersecurity and cyberattacks continues. Visit World Congress: INSIGHTS 2012, and click on the Conversations tab, where several event speakers are responding to questions.

Register now for ISACA’s World Congress: INSIGHTS 2012 to attend sessions with these speakers on 25-27 June 2012 in San Francisco, California, USA.

---

ISACA Members Invited to Take Part in a United Nations Study on Cybercrime

Cybercrime represents one of the unique global challenges of our time as computer systems and IT are increasingly integral parts of the daily lives of more than one third of the world’s population.

In response to this challenge, the executive director of the United Nations Office on Drugs and Crime (UNODC) recently launched a global comprehensive study on the problem of and response to cybercrime as a result of the United Nations General Assembly (UNGA) resolution. The UNODC has invited ISACA members to participate in the study, knowing that ISACA members are effective representatives due to their awareness and understanding of current and emerging trends in cybercrime.

The study will cover topics related to cybercrime, the challenges posed by cybercrime, and the role and responsibilities of service providers and the private sector. UN member states will look to the completed study with a view to strengthen existing legislation and to propose new national and international legal and other kinds of responses to cybercrime.

The results of the study will be presented to the United Nations Commission on Crime Prevention and Criminal Justice (UNCCPCJ) in 2013 and will inform member states’ responses to cybercrime.

UNODC is gathering information to be included in the study and is inviting interested parties to complete a cybercrime questionnaire. For more details on the study, visit the UNODC data collection portal. The deadline to submit completed questionnaires is 31 May 2012. You may also send questions concerning the UN cybercrime study to cybercrime.study@unodc.org. Your valued participation is appreciated!
**IAASB Strengthens Standard on Using the Work of Internal Auditors**

Many enterprises establish internal audit functions as part of their internal control, risk management and governance structures; effective coordination and communication between the external and internal auditors can contribute positively to the external audit. Recognizing this, the International Auditing and Assurance Standards Board (IAASB) has recently released the *International Standard on Auditing (ISA) 610 (Revised), Using the Work of Internal Auditors*, which addresses the external auditor’s responsibilities if using the work of an internal audit function in obtaining audit evidence.

The revised standard is aimed at enhancing the external auditor’s performance by providing a more robust framework for evaluating and using the work of an enterprise’s internal audit function. Related changes have also been made to *ISA 315 (Revised), Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment* to explain how the internal audit function and its findings can usefully inform the external auditor’s risk assessments.

Both ISA 610 (Revised) and ISA 315 (Revised) are effective for audits of financial statements for periods ending on or after 15 December 2013.

---

**Insight Into the Audit, Risk, Control and Regulatory Environment: United Kingdom**

*By Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI*

The UK has a long history of auditing, the earliest reference being to the Auditor of the Exchequer in England in 1314. It was with the advent of the Industrial Revolution, from 1750 to 1850, that auditing began its evolution. The Joint Stock Companies Act of 1844 was early legislation that showed the need for investors, who might not be involved in the running of their companies, to receive reliable information from those who played a part in company management. The Act required all incorporated companies to produce an audited balance sheet and the auditor was required to report on whether the balance sheet showed a “full and fair view” of the reporting company’s position.

The Companies Act of 1856 was gradually developed as Parliament intervened to impose specific legislation and regulations, including accounting and audit requirements that we see today in the Acts most recent revision in 2006.
Risk has always been important to enterprises in the UK, but with the financial crises since 2007, many enterprises (not just financial enterprises) have focused on the need for effective risk management. Risk management gives comfort to stakeholders (e.g., shareholders, customers, employees) that the business is being effectively managed and helps to confirm its compliance with governance requirements.

Risk management requires a detailed knowledge and understanding of the enterprise and the processes involved in its business. As well as internal specialists, enterprises often rely on a broad range of different advisers and consultants providing support to their risk management program.

In 1992, following a series of high-profile corporate frauds and accounting scandals, the London Stock Exchange (LSE) introduced new regulations covering various aspects of corporate governance. These new rules were based on the Cadbury Committee’s Code of Best Practice for the financial aspects of corporate governance and applied to companies listed on the LSE. At around the same time, a highly influential document was published in the US, written by the accountants at Coopers and Lybrand for the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and called the COSO Internal Control—Integrated Framework.

The original rules have since been revised and the current UK rules are within the Hampel Committee’s Combined Code, with the requirements on internal controls explained and interpreted in the Turnbull guidance issued by the Institute of Chartered Accountants in England and Wales. UK-listed companies now have to evaluate their internal controls, covering all types of risk.

The UK has a strong regulatory framework, some of which originates from the European Union legislation. Various bodies, such as the Financial Services Authority (FSA), Environment Agency and Scottish Environment Protection Agency, and Information Commissioner’s Office, are responsible for the different regulations. Important compliance issues for all enterprises include the Data Protection Act of 1998 and the Freedom of Information Act of 2000, which applies to the public sector. The Combined Code issued by the LSE is the UK’s equivalent to the US Sarbanes-Oxley Act of 2002.

Related reference books from the ISACA® Bookstore include:

•  *Information Technology Risk Management in Enterprise Environments*, by Jake Kouns and Daniel Minoli
•  *Data Protection: Governance, Risk Management, and Compliance*, by David G. Hill
•  *Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition*, by Christian B. Lahti and Roderick Peterson
•  *The Risk IT Framework*
•  *The Risk IT Practitioner Guide*

Selected ISACA® Knowledge Center resources and articles include:
•  “ISACA’s 2011 IT Risk/Reward Barometer”
•  “CISA, CISM, CGEIT and CRISC Certification Recognitions”
•  “ISACA’s EuroCACS Conference Examines Data Protection Issues,” by ISACA UK Chapter
•  “Allen Overy summary document on EU data privacy changes”

This is the third in a series of brief overviews written by members of the ISACA Publications Subcommittee for @ISACA. Read the previous articles: “Insight Into the Audit, Risk, Control and Regulatory Environment: United States” and “Insight Into the Audit, Risk, Control and Regulatory Environment: Canada.”

Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI, is the group information security officer at AEGON UK. He has more than 25 years of experience in IT, information security, audit and risk. He has written a number of articles for the ISACA Scotland Chapter and is a member of the ISACA Publications Subcommittee. He can be reached at andrew.richardson@bcs.org.uk.

©2012 ISACA. All rights reserved.