ISACA Mourns Founding President

Stuart Tyrnauer, ISACA’s first president, who served from 1969 to 1972, has passed away. Tyrnauer participated in the formation of the association, then known as Electronic Data Processing Auditors Association (EDPAA), in California (USA) in 1969.

Read More

Announcing the COBIT 5 Certified Assessor Program

There is a new opportunity for professionals to show their competency in COBIT-based IT process assessments. Those who successfully complete the COBIT Assessor requirements may apply through ISACA® to become a COBIT 5 Certified Assessor.

Read More

ISACA Escalates Its Green Initiatives

While the environment and “going green” have long been important to ISACA, the association is renewing its focus on activities aimed at decreasing its footprint where possible. As a result, ISACA is implementing new green initiatives.
Compliance Vs. Security

By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP

Today, many enterprises have the misconception that they are achieving security through compliance. Enterprises are expending an incredible amount of resources on compliance in pursuit of the risk avoidance culture that the statement represents. However, the gap between compliance and security calls for a risk management approach.

Book Review: Robust Control System Networks—How to Achieve Reliable Control After Stuxnet

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

Robust Control System Networks—How to Achieve Reliable Control After Stuxnet is for security professionals who work with industrial automation and control systems. This book provides a well-explained methodology for creating reliable and dependable control systems.

Be Prepared for Big Data’s Impact on Privacy

Big data implementation provides many benefits across the enterprise, such as improved decision making, better customer service and increased profits. With its vast potential comes the additional responsibility to protect the privacy of the personal data gathered and analyzed.

“What Does a Topic Leader Do?” Learn More

When considering whether to become an ISACA Knowledge Center topic leader, the first question most members ask is, “What does a topic leader do?” Good practices of topic leaders have been analyzed in a case study that clearly explains the activities of ISACA’s
most successful topic leaders.

Read More

What Should We Do Next in Risk Management?

Despite all of the efforts and considerable investment in time and money, difficulties in information systems appear frequently in news headlines, leaving information systems staff and risk managers wondering, “What is next?”

Read More

Renew Your 2014 Certification Now

Take charge of your professional recognition. Renew your CISA®, CISM®, CGEIT® and/or CRISC™ certification in 2 easy steps—pay the annual certification maintenance fee and report your continuing professional education (CPE) hours earned.

Read More

ISACA Mourns Founding President

Stuart Tynauer, ISACA’s first president, who served from 1969 to 1972, has passed away. Tynauer participated in the formation of the association, then known as Electronic Data Processing Auditors Association (EDPAA), in California (USA) in 1969.

Recently, Eugene Frank, another early president and a driving force behind the association’s formation, reminisced about the organization’s inception and Tynauer’s role:

I made up a list of large companies that I knew were heavily into computerizing operational systems. Most were defense contractors or utility companies. The first company I called was McDonnell Douglas. I was referred to Stuart Tynauer, I reached him and explained my idea. While not overwhelmingly excited by the idea, he did agree to meet with me.

Frank went on to relate that, after considerable discussion and review of work papers, he and Tynauer agreed there were benefits to be gained, and arranged for a second meeting.

In future meetings, Tynauer had the nonprofit incorporation documents prepared and he and 6 others (including Frank) signed the documents, thus becoming the founders of EDPAA. Tynauer volunteered to serve as president and was duly elected.

“It is important to fully appreciate the farsightedness of these pioneers of our profession,” said
ISACA International President Tony Hayes. “EDP auditing was barely a recognized endeavor at that time, yet Tyrnauer and the others had enough vision to know that it would become a cornerstone of good computing practice. We are grateful to them for their courage and commitment.”

ISACA expresses its deep sympathy to Tyrnauer’s wife, Donna, and its thanks for the foundational role he played in the organization’s creation.

Announcing the COBIT 5 Certified Assessor Program

There is a new opportunity for professionals to show their competency in COBIT-based IT process assessments. Those who successfully complete the COBIT Assessor requirements may apply through ISACA® to become a COBIT 5 Certified Assessor.

A COBIT 5 Certified Assessor is characterized as a competent IT or business professional who is trained in performing COBIT-based IT process assessments and experienced in planning, building, running and/or monitoring IT processes. As such, a COBIT 5 Certified Assessor can provide a reliable, consistent and repeatable assessment of IT process capabilities, which can help IT leaders gain C-suite and board member buy-in for change and improvement initiatives.

Additional information is available on the COBIT 5 Training & Accreditation page of the ISACA web site. Contact cobittraining@isaca.org to request an application.

ISACA Escalates Its Green Initiatives

While the environment and “going green” have long been important to ISACA, the association is renewing its focus on activities aimed at decreasing its footprint where possible. As a result, ISACA® is implementing new green initiatives.

As you renew your 2014 membership and certifications, which you are encouraged to do now, you have the opportunity to opt out of the printed copy of the ISACA® Journal, which is mailed to you every other month. Opting out of the printed copy does not mean that you give up your access to this valuable content. Just as you do now, you will receive notice when the Journal is posted for viewing online. All of the content in the hard-copy Journal is visible online, and the electronic versions of the Journal will be enhanced in 2014 to offer more content and more interactivity. Currently, you can access the Journal through its digital replica (from which you can download a full PDF), the mobile app, the Journal web pages and individual article PDFs. Funds accrued as a result of those who opt out of the hard copy will be funneled back into the Journal—adding enhancements to the digital version.
ISACA is also offering a going-green discount to members on 2014 membership and certification renewal. If you renew online and by credit card early—prior to the first hard-copy invoice being sent in October—you will receive a US $5 discount in the online shopping cart on your total 2014 membership and certification dues. The online renewal and payment of all fees for membership and ISACA certifications you hold must be completed at once and before invoicing begins in order to receive the discount. Renew now and take advantage of this green payback. If you are unable to renew early, please use the first invoice mailed in October or renew online at your earliest convenience.

Furthermore, ISACA will decrease the number of hard-copy invoices it sends for the 2014 renewal period—instead of three hard-copy invoices, members and certification holders who have yet to renew will receive only two. The first hard-copy invoice will be sent in October and will be followed by a final hard-copy invoice in 2014 for those whose membership and/or certification is about to end at the conclusion of the courtesy grace period.

---

**Compliance Vs. Security**

*By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP*

Today, many enterprises have the misconception that they are achieving security through compliance. Enterprises are expending an incredible amount of resources on compliance in pursuit of the risk avoidance culture that the statement represents. There is an old adage that says, “A standard, no matter how well defined, is the lowest level one has to achieve.” This adage says a lot about the differences between security and compliance. The gap between compliance and security calls for a risk management approach.

Compliance is comparing a standard to the unknown. The compliance standard is typically derived from the governance and management frameworks complemented by good business practices. The unknown is the implementation of a governance framework traced through a management framework, which must be reflected in business processes and technology. In general, this is accomplished by implementing security-based requirements from the governance framework and the corresponding management framework. The requirements are then reflected in protection strategies, such as security architecture designs based on an approved budget and approved security architecture reflected in business processes and technology. In the end, we believe that while compliance and security take 2 similar but different paths, the enterprise is nonetheless compliant and secure. Here is a list of tips to help close the gap between compliance and security:

1. Do not put solutions in governance frameworks. This guarantees that vulnerabilities will arise as your protection strategies become dated.
2. Understand your enterprise’s corporate culture. Is it based on trusting processes or people?
3. As role-based training is critical to closing the compliance and security gap, instill a sense
of craftsmanship in staff. This pushes security and compliance into the corners of the enterprise that were only vaguely referenced in policy.

4. Ensure the use of open standards. Open standards in all facets of technology reduce costs and allow nonengineers to participate in compliance activities. Open standards also provide a common base for risk.

5. If your enterprise develops unique software applications, ensure that the development and implementation of a known software architecture is reflected in the software development and compliance tool kits.

6. Use innovation adoption cautiously. Although providing the potential for great improvement, it can also negatively impact security management throughout the enterprise.

7. Address the root causes of vulnerabilities, not the symptoms. Be wary of compensating and detective controls. Although necessary, they are often reactions to a flawed product or an inadequate implementation of security in the technology.

8. Treat development and delivery of technology as a business process. Excessive security organizations and processes are often added to address security at the end of the process in hopes of achieving more assurance. This can be a symptom of a broken business process and not a feedback loop.

9. Do not view risk as something unique to security. Develop an enterprise risk registry. Risk should be viewed across all disciplines throughout the enterprise.

For additional information on this topic, visit the Enterprise Risk Management page on the ISACA web site. Additional content on this topic is available in the Knowledge Center and the ISACA Bookstore.

Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP, is the chief executive officer of TWM Associates Inc. In this capacity, Wilkins provides his customers with secure engineering solutions for innovative technology and cost-reducing approaches to existing security programs.

---

Book Review: Robust Control System Networks—How to Achieve Reliable Control After Stuxnet

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

Robust Control System Networks—How to Achieve Reliable Control After Stuxnet is for security professionals who work with industrial automation and control systems. This book provides a well-explained methodology for creating reliable and dependable control systems. It does not negate or take away from current practice and can be considered a source of information for plant planners, operators and systems maintenance engineers.
This book touches on Stuxnet but focuses more on a method and a process for creating reliable control systems, which, if designed correctly, will behave in a robust and reliable manner during unexpected conditions.

Chapters 1, 2 and 3 explain 3 different methods for looking at risk and define cyberfragility and cyber-robustness. The author presents 3 different risk models and explains the differences among them. Rather than referring to high and low risk, the book uses the terms “fragility” and “reliability.”

Chapters 4 and 5 focus on building a model of the system and creating a requirements and system specification. Key points of discussion include understanding the system before it can be controlled and knowing why a system is designed in a certain manner.

Chapters 6, 7 and 8 look at imposing structure, enforcing and reinforcing structure, and modifying structure. Imposing structure covers reduction strategies that can help create order by reducing variability. Enforcing and reinforcing structure looks at surplus strategies for ensuring continued operation when faced with atypical conditions. Modifying structure focuses on change management and notes that the vast majority of problems have been the result of deliberate and well-intended changes, rather than malicious cyberattacks.

Robust Control System Networks relates its theories back to practical examples, not just with reference to Stuxnet but also with examples from varying industries that rely on control systems. The book also has a comprehensive appendix that describes numerous subtle, unanticipated cyberfragility effects and provides real-world examples of how these effects have manifested themselves.

Robust Control System Networks—How to Achieve Reliable Control After Stuxnet 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.

Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI, is the group information security officer (ISO) at AEGON UK. Richardson has more than 25 years of experience in IT, information security, audit and risk.

Be Prepared for Big Data’s Impact on Privacy

Big data implementation provides many benefits across the enterprise, such as improved decision making, better customer service and increased profits. With its vast potential comes the additional responsibility to protect the privacy of personal data gathered and analyzed.

ISACA’s Privacy and Big Data white paper emphasizes the impact that big data has on privacy, privacy risk, big data privacy strategies, and governance of and assurance
considerations for big data privacy. It addresses privacy risk and controls associated with big data and empowered by computers and limitless storage.

Information on current research projects is posted on the Current Projects page of the ISACA web site.

“What Does a Topic Leader Do?” Learn More

When considering whether to become an ISACA Knowledge Center topic leader, the first question most members ask is, “What does a topic leader do?” While the roles and responsibilities are outlined in the Become a Topic Leader page in the ISACA Knowledge Center, good practices of topic leaders have been analyzed in a case study that clearly explains the activities of ISACA’s most successful topic leaders.

Three categories will assist you in becoming a successful topic leader:

1. **Involvement in discussions**—To maximize discussions, a topic leader should initiate, as well as be involved in, conversations along with the topic members.

2. **Subject matter expertise**—To speak knowledgeably about a topic, candidates must be subject matter experts on the particular topic; this is determined during the topic leader application process and should be maintained as the field evolves.

3. **Open communications**—During the application process, candidates are introduced to ISACA staff members. When a candidate’s application is approved, the candidate is introduced to fellow topic leaders if there is more than one topic leader in the topic. Open communication with fellow topic leaders, members and staff provides a cohesive and supportive environment.

Help ISACA maintain a vibrant online community. Read the full case study and visit the Become a Topic Leader page to learn more.

What Should We Do Next in Risk Management?

Despite all of the efforts and considerable investment in time and money, difficulties in information systems appear frequently in news headlines, leaving information systems staff and risk managers wondering, “What is next?” In his closing keynote presentation at the North America Information Security and Risk Management (ISRM) Conference 2013, Robert Bigman, retired chief information security officer (CISO) for the US Central Intelligence Agency (CIA), will discuss the state of computing technology by examining the historical development of current technologies and software. Bigman will also share his experiences with vulnerabilities found during his research for the US government to help organizations move forward.
Join Bigman as he shares his experiences and knowledge of today’s most significant risk topics in data privacy and security, cybersecurity, risk management, and compliance at North America ISRM, 6-8 November, in Las Vegas, Nevada, USA.

Renew Your 2014 Certification Now

Take charge of your professional recognition. Renew your CISA, CISM, CGEIT and/or CRISC certification in 2 easy steps—pay the annual certification maintenance fee and report your continuing professional education (CPE) hours. You have until 31 December 2013 to earn CPE hours for your 2014 renewals. The deadline is nearing—visit the My Certification page of the ISACA web site and review the status of your annual and 3-year CPE reporting requirements.

The CPE policy requires earning a minimum of 20 CPE hours each year and 120 CPE hours during your 3-year reporting cycle. With the new simplified CPE reporting system, CPE hours for your ISACA credentials can be entered individually as they are earned or as a total for the year.

If you find yourself needing CPE hours to meet the requirements, your ISACA membership provides you with a number of free and low-cost opportunities, including via ISACA Journal CPE quizzes, mentoring and online learning. To learn more about CPE opportunities and recording CPE hours, please visit the How to Report and Earn CPE page of the ISACA web site.

©2013 ISACA. All rights reserved.