Help Yourself, Help Your Employer

Nominations for the ISACA® Board of Directors for the 2011-2012 term are open. Serving on the board is a great way to build your skills and expertise, expand your professional network, influence the direction of the association, and give back to the profession.

Read More

10 Things to Consider Before Providing a Vendor Security Questionnaire or Examination Result

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

Vendor security questionnaires and assessments have become a popular and normal aspect of organizations’ vendor security programs. Here are 10 things you should consider before providing these data to a requesting organization:

Read More
ISACA Volunteers Motivated by “Giving Back”

ISACA is so aware of its dependence on volunteers, it has identified “volunteer support and retention” as one of its top three risks. To ensure that the risk receives appropriate attention, a response plan was created, one element of which calls for learning more about volunteer motivation and attitudes toward recognition. To accomplish this, ISACA recently conducted a survey.

Read More

Certifications Demonstrate Understanding of IT Governance, Risks and Controls

Dustin Bradley, CISA, CISM, CRISC, CFE, Shares His Experiences as a CISM

“Earning ISACA certifications has added to my credibility and the knowledge I need to perform my job as an IT audit and controls/risk professional.”

Read More

Virtualizing Your Business Offers Risks and Benefits

Virtualization was originally used primarily to facilitate server consolidation, but now many other approaches present themselves. Virtualization: Benefits and Challenges, a new white paper from ISACA, examines some of the security concerns and possible solutions when moving to a virtualized environment and provides practical guidance on auditing a virtualized system.

Read More

Building in Trust and Value

ISACA’s tagline promotes trust in, and value from, information systems. It refers primarily to the outcomes created by the association’s members and constituents: the work they do helps ensure that their enterprises and/or their clients can trust the information generated by their information systems and realize optimal value from the investment in those systems.
But, it also refers to ISACA itself, as evidenced by the recent web site redesign.

**View Recent ISACA Virtual Seminar and Tradeshow**

**On-demand**

**Managing IT Enterprise Risk Available for Viewing for Limited Time**

On 19 October 2010, ISACA presented a free, one-day virtual seminar that focused on how to manage IT enterprise risk. The speakers took a practical approach to risk by examining three different perspectives.

**Book Review: *Effective Project Management: Traditional, Agile, Extreme, 5th Edition***

Reviewed by Sarathy BSP Emani, CISA, CISM

*Effective Project Management: Traditional, Agile, Extreme, 5th Edition,* by Robert K. Wysocki, Ph.D., is a learning guide for the education and training of the professional segments of software engineering. The chapters are organized to suit introductory educators, intermediate trainers and advanced professionals.

**Help Yourself, Help Your Employer**

Nominations for the ISACA® Board of Directors for the 2011-2012 term are open. Information about serving on the board, the attributes for office (both international president and vice president) and the nomination form itself are available on the [Volunteering](#) page of the ISACA web site.

Serving on the board is a great way to build your skills and expertise, expand your professional network, influence the direction of the association, and give back to the profession. The experience is bound to help you, and it can help your employer as well. Employers will enjoy the benefits of having an employee who is more self-assured, who can access information from professional colleagues worldwide and who can use his/her expanded understanding of
ISACA’s offerings to enhance activities within the enterprise. It is the classic definition of a win-win situation.

Members may nominate themselves and/or other members they believe match the attributes of the office. Nominations for the Board of Directors close on 7 January 2011. Interested parties are encouraged to submit their nomination form as early as possible, however, to provide the Nominating Committee ample time for evaluation.

---

**10 Things to Consider Before Providing a Vendor Security Questionnaire or Examination Result**

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

Vendor security questionnaires and assessments have become a popular and normal aspect of organizations’ vendor security programs. They often ask for detailed information about the security and risk management capabilities of organizations they are evaluating. Here are 10 things you should consider before providing these data to a requesting organization:

1. **How are these data going to be used by the requesting organization?** Most often, vendor security data are used by information security and risk management organizations to assess the risk of working with third parties and allowing them access to sensitive data and an information infrastructure. These data can also be used by organizations for business activities such as leveraging negotiations, benchmarking their own capabilities, and identifying weaknesses and trends in information security and risk management. It is important to have a clear understanding of how the data are going to be used prior to disclosing the information and to ensure that you are comfortable with its use.

2. **How are the data provided to the requesting party going to be secured once they have been received?** Vendor security questionnaires and audit methods used by many organizations now include large amounts of sensitive information that can become an invaluable intelligence source and, potentially, a road map that an adversary could use to successfully attack your organization. It is important to understand what security and data handling standards and controls are going to be applied by the requesting organization prior to transmitting the data to them. These controls should include (but not be limited to) restricted access control procedures, encryption of data in transit and at rest, access to control logs, and regular access to log reviews by management.

3. **Legal agreements and acceptable use procedures between organizations are not sufficient for securing security questionnaires and audit reports.** Legal agreements that are in place between two organizations typically have provisions for data security
that favor the requesting party and often do not have the same provisions for protecting data provided by the vendor. Even if these provisions do exist, typically, they are applicable only in the recovery of damages in litigation, in the event of a misuse of the data, a data disclosure incident, or a malicious attack as a result of inappropriate access to or compromising of this information. If you are going to provide sensitive and detailed information about your information security and risk management capabilities to third parties, you should have legal language in place in agreements between both organizations that require mutually agreed-upon security measures be implemented to protect the data. The existence and appropriate operation of these measures should be verified on a regular basis during the time the requesting party has access to these data.

4. **Ensure that you are not in breach of contract with other arrangements as a result of disclosing vendor security questionnaires to third parties.** Many organizations are interested in maintaining the confidentiality, integrity and availability of the data they provide to vendors as well as the access they provide them to the information infrastructures. They also would like as few people as possible to have access to information about the information security and risk management capabilities of an organization that they are working with to enhance their own security posture. Organizations may include provisions in their contracts that prevent the disclosure of information about the organization’s information security and risk management capabilities.

5. **Request a vendor security questionnaire and performing a vendor security audit of the requesting organization.** To ensure the proper handling and storage of the sensitive information, you should perform a vendor security audit, which can include your own questionnaire of the requesting party. If they are unwilling or unable to comply with this requirement, you should not transmit the security questionnaire to them. Instead, allow the requesting organization to review the completed vendor security questionnaire in person with an authorized member of your organization who can address questions or concerns that may arise as part of the review.

6. **Relay only the information that is relevant to the products and services that you provide to the requesting party.** Many vendor security questionnaires are extremely comprehensive and request information about your information security and risk management capabilities that exceed the scope of services you provide the requesting organization. To limit the exposure of sensitive data associated with your capabilities, relay only the information that is applicable to the security of the services that will be provided to the requesting organization. If the organization requests information outside of this scope, provide it only when an appropriate business justification for its need has been presented and verified.
7. **Understand how the questionnaire or assessment will be evaluated by the reviewing organization.** Different organizations have different requirements and areas of interest regarding information security and risk management expectations of the vendors with which they work. It is important to understand these in advance of providing information to ensure that your current capabilities and approach are in alignment with their expectations. If you believe that they are not, it is important to contact the requester in advance of any response or examination to come to a mutually agreed-upon set of capabilities that will be used to meet their requirements.

8. **Do not be afraid to ask questions or push back on requirements identified in vendor security questionnaires or assessments.** Consider a vendor security questionnaire or examination a starting point in the conversation with a requesting party, instead of the authoritative set of requirements that you must meet to conduct business with them. Many organizations will use a generic security questionnaire for all vendors they work with that may not be applicable or appropriate to your business activities with them. If you disagree with or are unsure of some of the requesting organization’s questions or requirements, engage the organization in a conversation. This will allow you to understand the threat it is trying to mitigate or the requirement it is trying to meet. Then, you can determine if you have an equivalent alternative that it has not yet considered.

9. **Utilize third-party examinations and certifications when possible to reduce the need for extensive data disclosure.** When possible, work with vendors to define a mutually agreed-upon examination or certification to be performed by a third party whose formal opinion will meet the requester’s requirement of a review of your information security and risk management capabilities without having to disclose sensitive information to the requester. This can be to the benefit of both parties since it removes the liability and overhead associated with maintaining the security of this information from the requester and ensures an appropriate evaluation has been completed. Often, this approach will work with multiple vendors, which will reduce the time and expense associated with responses to individual requests from numerous organizations.

10. **Ensure provisions exist for the destruction of questionnaires and assessment results if you no longer do business with a requester.** If you choose to provide questionnaires or allow assessments of your information security and risk management capabilities, it is important that you ensure that this information is destroyed once you no longer do business with the requesting organization. This assurance should not be limited to contractual obligations alone. It should also include a requirement of a certificate of destruction to be provided by the requesting party attesting that all existing and known copies of these questionnaires and assessments, including hard copies,
electronic copies and all associated backups, have been destroyed in a manner that has been mutually agreed upon and accepted by both organizations.

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

---

**ISACA Volunteers Motivated by “Giving Back”**

During a typical year more than 500 volunteers participate in an ISACA® activity of some kind: working on one of the many boards, committees, subcommittees and task forces; planning conference events, leading one of the communities of practice in the Knowledge Center on the web site, or offering subject-matter-expert review of draft documents, books, and articles. ISACA is so aware of its dependence on volunteers, it has identified “volunteer support and retention” as one of its top three risks.

To ensure that the risk receives appropriate attention, a response plan was created, one element of which calls for learning more about volunteer motivation and attitudes toward recognition. To accomplish this, ISACA recently conducted a survey, which was sent to all of the current oversight board, committee and subcommittee members, and was responded to by an astonishing 80 percent.

In response to the question, “What motivates you the most to volunteer for ISACA?” more than 90 percent indicated the opportunity for professional development (learning from peers) and giving back to the profession. The remaining 7 percent was divided among earning continuing professional education (CPE) hours, enjoying the opportunity to travel, engaging in social networking and other motivators.

Most of the comments provided supported the percentages, a typical response being, “I had the opportunity to evolve and grow in the professional field of IT audit, security and control with my local chapter and ISACA for over 25 years. It feels right to give back and to share knowledge and experience.”

The predominant response to the second question, “What form of recognition/appreciation matters most to you?,” pointed to the satisfaction of being considered an expert as a result of work done for ISACA (78 percent). Chapter and employer recognition were also acknowledged as important, as was the certificate of appreciation given by ISACA. Among the “other” responses were CPE hours, seeing one’s name on a publication, and no recognition needed.

These results indicate that ISACA volunteers participate for the very reasons that make their efforts meaningful to the membership at large: the feeling of being part of something bigger than themselves, something that helps others and advances the profession. ISACA is fortunate to engage these special individuals in meaningful ways and is grateful to all who volunteer.
their time and expertise.

To apply to be an ISACA volunteer in 2011-2012, review the application form included with volume 6 of the *ISACA Journal*, mailed this month. Then, visit the Volunteering page of the ISACA web site to fill out the online application. The deadline for applying is 25 February 2011, but we welcome and encourage early applications.

---

**Certifications Demonstrate Understanding of IT Governance, Risks and Controls**

Dustin Bradley, CISA, CISM, CRISC, CFE, Shares His Experiences as a CISM

Dustin Bradley wanted to develop a better understanding of enterprise-wide information security, related IT governance and compliance controls and risks, and the impact these areas have on an organization. After some research, he decided that earning the Certified Information Security Manager® (CISM®) certification would provide him with the frame of reference he was seeking and enhance his career.

“Earning ISACA® certifications has added to my credibility and the knowledge I need to perform my job as an IT audit and controls/risk professional,” said Bradley.

“And, I have access to ISACA’s knowledge base, which helps me alert my company’s management of emerging risks.” Bradley finds this especially helpful since a difficult part of his job is obtaining IT management/stakeholders’ agreement on information security risk exposures and the impacts resulting from IT security weaknesses.

Bradley continues his education by participating in ISACA’s online training webcasts and training events sponsored by his local New York Metro Chapter. He also enjoys volunteering for local ISACA chapter initiatives, which provides him with additional current information and networking opportunities.

For those interested in pursuing a career in IT or audit consulting, Bradley highly recommends earning ISACA certifications. “Companies are requiring successful completion of ISACA credentials for career advancement and promotion,” he said. “Having a CISM designation will help anyone differentiate him/herself from other candidates.”

Dustin Bradley, CISA, CISM, CRISC, CFE, is the treasurer and ISACA certification coordinator for ISACA’s New York Metro Chapter.
Virtualizing Your Business Offers Risks and Benefits

Virtualization was originally used primarily to facilitate server consolidation, but now many other approaches present themselves. Enterprises looking to save money and generate value from their IT investments are attracted to the benefits of virtualized storage, processors, memory, desktops and networks.

*Virtualization: Benefits and Challenges*, a new white paper from ISACA®, examines some of the security concerns and possible solutions when moving to a virtualized environment and provides practical guidance on auditing a virtualized system.

*Virtualization: Benefits and Challenges* is available as a complimentary PDF to members and nonmembers on the Research page of the ISACA web site.

Building in Trust and Value

ISACA’s tagline promotes trust in, and value from, information systems. It refers primarily to the outcomes created by the association’s members and constituents: the work they do helps ensure that their enterprises and/or their clients can trust the information generated by their information systems and realize optimal value from the investment in those systems. But, it also refers to ISACA® itself, as evidenced by the recent web site redesign.

Anyone who has been to ISACA’s web site since early June 2010 must have noticed the radical overhaul of the site. It not only looks very different from what it did before, it also takes full advantage of Web 2.0 technologies, offering visitors multiple opportunities to collaborate and customize the content. What started as a simple redesign became a long-term, complex project, as ISACA and its vendors worked together to ensure that the site offered functionality the site visitors could trust and content that would deliver value.

Using itself as an example of a small to medium-sized enterprise, ISACA has created a case study, “Building Trust and Value into the ISACA Web Site Redesign,” outlining the steps undertaken to bring the site to fruition, in the hope that the information might prove useful to other organizations or individuals contemplating a similar project. The case study describes the situation that existed with the previous site, the challenges faced during the course of the project, the ways members and other constituents were involved in the process, and the help provided by ISACA's own guidance (COBIT® and Val IT™: Based on COBIT®).
View Recent ISACA Virtual Seminar and Tradeshow
On-demand
Managing IT Enterprise Risk Available for Viewing for Limited Time

On 19 October 2010, ISACA presented a free, one-day virtual seminar that focused on how to manage IT enterprise risk. The speakers took a practical approach to risk by examining three different perspectives. First, they looked at the enterprise to determine how best to manage security risks within and, perhaps more important, outside the enterprise. Next, they considered how to assess risk and the unique problems inherent with the human factor. Finally, they discussed the strategic issues associated with risk and the balance between meeting business goals while minimizing potential loss and unintended consequences.

The presenters included Nancy DeFrancesco from U.S. National Environmental Satellite, Data and Information Service; Ninette Caruso from Nationwide Mutual Insurance Company; Atul Shah, senior security strategist at Microsoft Corp.; and Todd Tucker, senior director of marketing at Net IQ.

It was an educational experience and exciting opportunity for all attendees, as they were able to ask questions, have live conversations with speakers and sponsors, and connect one-on-one with other ISACA members and staff. Attendees also earned up to four continuing professional education (CPE) credits for their participation in this event.

If you missed it and want to view it on demand, you can access the archived sessions through 17 January 2010. Please visit the eLearning page of the ISACA web site for a link to registration.

Join us 8 December 2010 for the next ISACA Virtual Seminar and Tradeshow, Security and Compliance in the Cloud: Define, Defend and Regulate.

Book Review: Effective Project Management: Traditional, Agile, Extreme, 5th Edition
Reviewed by Sarathy BSP Emani, CISA, CISM

Today, any software project is influenced by several factors including high speed to market, rapid change in requirements, budget for low costs, application and technical complexity, and associated uncertainty. Under these circumstances, effective project management is the one factor that is flexible and adaptable, given a sufficient understanding of business and its
Effective Project Management: Traditional, Agile, Extreme, 5th Edition, by Robert K. Wysocki, Ph.D., is a learning guide for the education and training of the professional segments of software engineering. The chapters are organized to suit introductory educators, intermediate trainers and advanced professionals.

This fifth edition is a reorganized and improved version of the highly acclaimed fourth edition, and is based on the latest experiences of the author and requests from educators, trainers and professionals.

This book uses two parameters—goal setting and problem solving—to determine the life cycle of a project. Termed as “landscaping a project,” this is the most valuable guidance provided in the book.

At the end of each of the 17 chapters, there are discussion questions and case study matter. Appendix A specifies what is available on the web site as downloads, including presentation slides for each chapter and class exercises. A bibliography, arranged according to the major areas in the book, is also included.

In spite of significant value added in the fifth edition, the author modestly considers the book a work-in-process. He plans to continue to improve the contents based on his further experiences and inputs from his clients, trainers, faculty and project management professionals.

Effective Project Management: Traditional, Agile, Extreme, 5th Edition 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 or e-mail bookstore@isaca.org.

Sarathy BSP Emani, CISA, CISM, has more than 25 years of experience and is the proprietor of MEQPRIMA Advisory Services, an organization doing research in software process and quality improvement. He is a member of the ISACA Publications Subcommittee.