

- Time Is Running Out for VP Nominations
- 6-step Approach to Implementing PCI DSS
- Board Holds Midyear Meeting
- ISACA Certifications Help to Navigate Information Security Waters
- ISACA Congratulates Nalin Wijetilleke, BCM Manager of the Year
- IAASB to Review Its Clarified ISAs, Invites Stakeholder Input
- Book Review: *Security Strategies in Windows Platforms and Applications*

Time Is Running Out for VP Nominations

The deadline for nominations for the position of vice president on the ISACA® Board of Directors for the 2012-2013 term is 9 January 2012. Submitting the form is just the first step, so don't delay.

[Read More](#)

6-step Approach to Implementing PCI DSS

By Tara Kissoon, CISA, CISSP

PCI DSS provides a set of requirements for securing cardholder data that are stored, processed and/or transmitted. The PCI Security Standards Council provides a prioritized implementation approach to assist organizations in understanding how to reduce risk earlier in the compliance process.

[Read More](#)

Board Holds Midyear Meeting

The ISACA/ITGI Board of Directors/Trustees held its midyear meeting in November 2011 in Chicago, Illinois, USA. Following are the significant outcomes of the discussion...

[Read More](#)

ISACA Certifications Help to Navigate Information Security Waters

Paschalis Pissarides, CISA, CISM, CRISC, CFE, CPA, Shares His Experiences

Paschalis Pissarides, information security officer for Marfin Laiki Bank, Nicosia, Cyprus, had been working in his position for 6 years when he decided that earning the CISM® certification would validate his professional competency in information security management and further help him navigate information security.

[Read More](#)

ISACA Congratulates Nalin Wijetilleke, BCM Manager of the Year

Asia's best and most promising practitioners made their mark at the recently held BCI Asia Business Continuity Awards 2011 in Singapore. ISACA congratulates Nalin Wijetilleke, CISA, CGEIT, CBCP, immediate past president of ISACA's UAE Chapter, who was named BCM Manager of the Year.

[Read More](#)

IAASB to Review Its Clarified ISAs, Invites Stakeholder Input

The IAASB released its plan for a postimplementation review of the clarified International Standards on Auditing (ISAs). The review is focused on whether the clarified ISAs are being consistently understood and implemented in a way that achieves the IAASB's goals in revising and redrafting them.

[Read More](#)

Book Review: *Security Strategies in Windows Platforms and Applications*

Reviewed by Bright Munongwa, CISA, CGEIT, CRISC, CIA

Microsoft Windows® is the most common operating system in use today. Such widespread use also implies that there is an ever-increasing number of threats to violate Windows security. The need to understand the threats, risk and vulnerabilities associated with Windows systems is the focus of the book *Security Strategies in Windows Platforms and Applications*.

[Read More](#)

Time Is Running Out for VP Nominations

The deadline for nominations for the position of vice president on the ISACA® Board of Directors for the 2012-2013 term is 9 January 2012. (Nominations for international president closed on 31 October 2011.) Visit the [Volunteering](#) page to download information that describes the time commitments, responsibilities, meetings, attributes of the VP office and, of course, the form you will need to complete and submit to start the process.

You may nominate yourself or others (or both). Once your nomination form is received, you will be asked to complete a candidate profile form that confirms your willingness to serve if selected and provides the Nominating Committee with the information it needs. If you nominate yourself, you will also be asked to submit a letter of recommendation from an ISACA member describing how you demonstrate the attributes of office (listed on the nomination form). Information on you will be gathered in other ways as well, including review of public web sites (e.g., Google, Facebook, LinkedIn) and a possible phone interview.

As you can see, submitting the form is just the first step; there is other paperwork to submit, which must be received by the official close date of 9 January 2012. Therefore, it is important not to wait until the 9 January date to submit your nomination form; waiting that late will make it very difficult for you to get the remaining paperwork in on time. If you have questions, please e-mail nominate@isaca.org.

6-step Approach to Implementing PCI DSS

By Tara Kissoon, CISA, CISSP

The Payment Card Industry Data Security Standard (PCI DSS) provides a set of requirements for securing cardholder data that are stored, processed and/or transmitted. The PCI Security Standards Council (SSC) provides a prioritized implementation approach to assist organizations in understanding how to reduce risk earlier in the compliance process.

Here is the 6-step approach to implementing PCI DSS in your organization:¹

1. Remove sensitive authentication data and limit data retention.
 - Targets removing valuable data; "if you do not need it, do not store it"
2. Protect the perimeter, internal and wireless networks.
 - Focuses on controlling points of access into the cardholder data environment (CDE)
3. Secure payment card applications.
 - Targets applications, application processes and application servers
 - Includes secure coding practices, application firewalls and Payment Application Data Security Standards (PA-DSS)
4. Monitor and control access to your systems.
 - Includes controls that limit access and provides detection mechanism for unusual activity within the CDE
5. Protect stored cardholder data.
 - Targets specific protections mechanisms for stored data
6. Finalize remaining compliance efforts, and ensure all controls are in place.
 - Focuses on finalizing the remaining related policies, procedures and processes needed to protect the CDE

Tara Kissoon, CISA, CISSP, is a director at Research in Motion. Her expertise is focused in payment security across mobile systems.

¹ PCI Security Standards Council, PCI DSS Prioritized Approach for PCI DSS 2.0, May 2011

Board Holds Midyear Meeting

The ISACA/ITGI Board of Directors/Trustees held its midyear meeting in November 2011 in Chicago, Illinois, USA. Following are the significant outcomes of the discussion:

- **Strategy activity**—Since August 2011, ISACA has been engaged in reviewing the strategy adopted three years ago. This review encompasses a longer-term view—a 10-year

horizon—and indicates that the vision/tagline identified in the 2009 strategy, focusing on trust and value in information systems, is still on target as ISACA continues building on its mission and leadership position and pursues new opportunities to expand on the value provided to constituents.

At this meeting, the board approved a strategic aspirational view to guide ISACA's activities through 2022. It calls for global leadership in educating and informing individuals and enterprises on the topic of trust in information and information systems. The specific activities involved in moving toward that view will be examined in detail by the board and approved on a case-by-case basis, given the business and association environment over the 10-year period. Input from chapter leaders and international volunteers will constitute a significant component of the board's review and evaluation.

- **Knowledge**—COBIT 5 will be released by the end of the first quarter of 2012. *COBIT for Security* (working title) will be completed by June 2011, and will be a benchmark for other discipline-specific versions of COBIT 5 to be developed.
- **Finance**—New investment guidelines were approved; they will enable ISACA to be more flexible in responding to the fluctuating global economy. Review of the new guidelines to gauge effectiveness will be undertaken in 12 months.

The next meeting of the board, which will be the final meeting of the 2011-2012 term, will be held in March.

ISACA Certifications Help to Navigate Information Security Waters

Paschalis Pissarides, CISA, CISM, CRISC, CFE, CPA, Shares His Experiences



Paschalis Pissarides, information security officer for Marfin Laiki Bank, Nicosia, Cyprus, had been working in his position for 6 years when he decided that earning the **Certified Information Security Manager® (CISM®)** certification would validate his professional competency in information security management and further help him navigate information security.

"Given its global recognition, being a CISM provided me with a way to maintain my competencies and enhance my professional credibility and recognition, not only within my company, but also among my peers in the marketplace," said Pissarides. "I have always been a strong believer in achieving professional excellence and high ethical standards in my professional life."

Pissarides began his career as a senior information systems auditor at USA Group Inc., an Indianapolis (Indiana, USA)-based financial services company. To enhance his technical

knowledge and professional skills, he became a **Certified Information Systems Auditor® (CISA®)**. He also became involved with the local ISACA Central Indiana Chapter and served in various positions on the board of directors, including chapter president from 1995 to 1996.

"I returned to my home country (Cyprus) in 1997 with the experience and globally recognized certifications necessary to be employed by the largest bank in Cyprus (Marfin Laiki Bank) as an information security officer—the job I hold today," Pissarides noted. "In my role, I need to have skills to develop security policies and standards, analyze security risk and implement appropriate security controls and monitor their effectiveness. Becoming certified as a CISM and **Certified in Risk and Information Systems Control™ (CRISC™)** helped me to better develop these additional skills."

Given the world financial crisis and that fact that financial institutions are in the center of the economic hurricane, Pissarides finds the single most important challenge in working for a bank these days is managing risk—a challenge he feels is rewarding. "The best part of my job is being able to engage on a daily basis in the areas of risk identification, assessment and evaluation; risk mitigation; and risk monitoring. These processes all enable businesses to achieve strategic goals, competitiveness and profitability in an ever-changing business environment."

Pissarides suggests that prior to pursuing the CISM credential, you need to do an assessment of your career plans. "If you want to remain on the technical track of the profession, you should focus on improving technical skills and product-specific knowledge via certifications that cater to these needs—CISM is not one of those certifications," he said. "If you have been in the security profession for 3 to 5 years and want to move toward the information security management track, CISM is the most appropriate certification to pursue because it does not focus on specialist skills or technical aspects of the profession. Rather, it focuses on the tasks performed by an information security manager, such as managing and overseeing an organization's information security program," he explained.

When Pissarides is not navigating the world of information security, he enjoys exploring the underwater world. If he had chosen a different professional path, he "would have pursued a career in marine archaeology, exploring the depths of the ocean for the lost treasures of human civilization."

ISACA Congratulates Nalin Wijetilleke, BCM Manager of the Year

Asia's best and most promising practitioners made their mark at the recently held **BCI Asia Business Continuity Awards 2011 (ABCA)** in Singapore. ISACA® congratulates Nalin Wijetilleke, CISA, CGEIT, CBCP, immediate past president of ISACA's UAE Chapter, who was named BCM Manager of the Year.

Considered some of the most prestigious accolades in the industry, the awards recognize achievements made in business continuity management (BCM) this year. "It was a memorable moment in my professional career," said Wijetilleke. "I hope this will be an inspiration to upcoming ISACA professionals."

BCI ABCA was coorganized by the Business Continuity Institute (BCI) and the Business Continuity Planning Asia Pte Ltd. Based on nominations received from all Asian, Middle East and African countries—including China, Japan and Pacific countries—winners are selected after a rigorous assessment, for individual and business categories.

IAASB to Review Its Clarified ISAs, Invites Stakeholder Input

The International Auditing and Assurance Standards Board (IAASB) released its plan for a postimplementation review of the clarified International Standards on Auditing (ISAs). In 2009, the IAASB concluded its five-year Clarity project to redraft and revise the ISAs. The postimplementation review is the second phase of the IAASB's efforts to monitor the implementation of these standards. The review is focused on whether the clarified ISAs are being consistently understood and implemented in a way that achieves the IAASB's goals in revising and redrafting them.

"When this review is completed in 2013, the IAASB will be better able to assess whether there is need for further changes to the ISAs," said Arnold Schilder, chairman of the IAASB. "Timely feedback on the clarified ISAs from a variety of stakeholders is essential for this purpose and the IAASB's objective of ensuring that its standards continue to be of the highest quality."

To access the plan and details on how to provide input, visit the [IAASB's web site](#). Input for the purpose of the review is requested by no later than 31 October 2012. Features of the postimplementation review, which involves gathering information about the use of the clarified ISAs during 2012, are set out in the IAASB's [Plan for a Post-Implementation Review of the Clarified International Standards on Auditing](#).

Book Review: *Security Strategies in Windows Platforms and Applications*

Reviewed by Bright Munongwa, CISA, CGEIT, CRISC, CIA

Microsoft Windows® is the most common operating system in use today. Such widespread use

also implies that there is an ever-increasing number of threats to violate Windows security. The need to understand the threats, risk and vulnerabilities associated with Windows systems is the focus of the book *Security Strategies in Windows Platforms and Applications*. The book addresses issues with Windows XP, Vista, Windows 7, and Windows Server 2003 and 2008.

This book assumes basic or minimal technical background. Professionals and students with limited information security knowledge will find the book useful in gaining a basic understanding of the Windows operating system and the threats to and vulnerabilities within Windows systems. The book also provides step-by-step guidance on how to protect Windows systems from attack.

Each chapter begins with learning objectives and concludes with a summary and practice questions. Solutions to the practice questions are found at the end of the book. Numerous tips, notes and sidebars are provided to alert readers to additional information. The use of numerous step-by-step examples facilitates practice and implementation of lessons learned.

The key feature is the book's emphasis on tools and techniques to decrease risk from Windows' vulnerabilities. The material is presented in a way that makes it easy for readers with limited knowledge of Windows security to understand and implement the tools and techniques.

This book is part of the Jones & Bartlett Learning Series. It is written by Michael G. Solomon, a full-time security speaker and former college professor who specializes in information security.

Bright Munongwa, CISA, CGEIT, CRISC, CIA, is a specialist IT auditor at Nedbank Ltd., one of South Africa's Big Four banks. Munongwa serves on the ISACA Publications Subcommittee.



©2011 ISACA. All rights reserved.