

**ISACA NEW ENGLAND
BOARD
2006-2007**

OFFICERS

PRESIDENT

Erica Hague-Antos, CISA
Harvard Pilgrim Health Care

**EXECUTIVE VICE
PRESIDENT**

Tricia O'Donnell, CISA
Boston College

**ASSISTANT VICE
PRESIDENT**

Tony Giroti
Brookedge Technologies

TREASURER

Mark Rosa, CPA, CISA
Staples, Inc

**RECORDING &
CORRESPONDING
SECRETARY**

Valerie Fitton-Kane
Harvard Pilgrim Health Care

BOARD MEMBERS

Program and Seminar

Tricia O'Donnell, CISA
Boston College
Martin Dolphin, CISA
Ernst & Young

**Breakfast Meetings -
Chairperson**

Dennis Huaman, CISA, CISM,
CSA

CISA

Tony Giroti
Brookedge Technologies

CISM

Marybeth Panock
American Student Assistance

Hospitality & Attendance

John Morency
Transitional Data

University Liaison

John Beveridge, CISA, CFE
State Auditor's Office

Webmaster

Matthew J. Putvinski, CPA,
CISA, CISSP
Wolf & Company, P.C.

Membership

Robert A. Buchanan
State Auditor's Office

**By-Laws, Policies and
Procedures**

Jane Graffum
Blue Cross Blue Shield of
Massachusetts

**Past-President 2004-05 and
2005-06**

Mike Field
Liberty Mutual Insurance

Advisor/Consultant

Norm Kelson, CISA, CPA
Ahold USA



Newsletter
January 2007

President's Message

Happy New Year to all!

Coming up over the next two months ISACA New England has several seminars and breakfast meetings. In January, we have two seminars, "Risk Management Technology Concerns and Future" and "Compliance." We also have a breakfast meeting scheduled in both the Boston and Providence areas. Please check our website at www.isacane.org for locations, dates, and times.



For those who sat for the December CISA exam, your results should be available to you in early February. Candidates will receive an email result only if they consented to item 25 on the registration form and the exam fee has been paid in full. Please ensure your contact information (postal and email) are current with ISACA International so as not to delay your results. ISACA International would also like to remind people to add certification@isaca.org to your email address book, safe list, or white list to prevent the email from ending up in your spam folder.

For the upcoming CISA and CISM exams in June 2007, registration began on November 8, 2006. The early registration deadline ends on February 14, 2007. The final registration deadline is April 11, 2007. These dates apply to both certifications. Candidates may view or print a copy of the CISA or CISM Bulletin of Information for the June 2007 exams at www.isaca.org/cisaboi and www.isaca.org/cismboi. For those interested in a review course, ISACA New England will be offering review courses for both the CISA and CISM exams this spring. More details to follow. Please check our website for updates!

--Erica Hague-Antos,
2006-2007 President
ISACA New England

Did you know?

ISACA NE offers an online credit card payment option when you register for a seminar or for CISA/CISM review courses. We accept VISA, MasterCard, Discover, and American Express. Advertisers are also welcome to pay for website and newsletter ads by credit card.



50,000th CISA Granted

The 50,000th CISA certification was granted in October 2006.

Congratulations to ISACA New England chapter member, Robert Emsing Jr., of PricewaterhouseCoopers in Boston, who earned the distinction.

Other new chapter CISA/CISMs will be honored at the annual meeting in May.

Featured Chapter Events

Breakfast Meetings

Planning for this year is still underway, but it's not too early to mark calendars and save dates. Breakfast meetings provide a great opportunity to stay current and network with professional colleagues. Unless noted otherwise, there is no charge to members to attend, and each meeting provides two CPEs. Pre-registration is required.

See the 2007 Chapter Calendar in this issue for other planned breakfast meeting dates and locations. To view the latest schedule online or to register, click [here](#).

Metrowest

Date: February 15, 2007

Speaker: John Morency, CISA, Transitional Data

Time: 8:30-10:30 a.m.

Location: Staples, Inc., 500 Staples Dr., Framingham, MA.

Topic: Strategies for Control Consolidation, Testing & Automation

The focus of this presentation will be on techniques that internal auditors can use to develop an effective set of shared authentication, authorization and data integrity management controls that could be used to simultaneously support several key compliance standards such as Sarbanes-Oxley, HIPAA, PCI, GLBA and FISMA.

The presentation will also cover key quantitative considerations such as reducing the costs of testing, ongoing monitoring, event log management and centralized reporting.

Providence

Date: February 20, 2007

Speakers: Javed Ikbal and Craig Brown, zSquad

Time: 8:00 a.m. Breakfast,
8:30-10:30 a.m. Session

Location: Johnson & Wales University, Johnson Hall,
Providence, RI

Topic: Preventing Web Application Security Issues with Secure Coding

We all understand firewalls and access control lists. But there is a whole class of attacks against applications that ordinary firewalls are powerless against, because they happen at the application layer.

As more applications move to the web, more attacks will target HTTP or HTTPS-- and pass through firewalls with impunity to wreak havoc at the application layer. This presentation will discuss some common web application vulnerabilities and attacks, show how to identify them using free tools, and discuss secure coding methods to ensure they don't occur in the first place.

Boston

Date: February 21, 2007

Speaker: Don Ulsch, Jefferson Wells

Time: 8:00 a.m. -10:30 a.m.

Location: Jefferson Wells, One Liberty Square,
Suite 207, Boston, MA

Topic: Privacy and Identity Theft

Board Meetings

ISACA New England board meetings are open to members interested in becoming more involved with the chapter. Pre-registration is requested. Meetings are planned on February 22, April 5 and June 28 from 8:30 a.m. – 10:30 a.m.

For more information and directions, please contact Erica Hague-Antos at president@isacane.org.

Featured Chapter Events

Forensics Seminar

Three Sessions:

Digital Forensics

The goal of this session is to provide attendees with an overview of the Digital Forensics investigative process, as well as supporting tools and techniques. The instructor will discuss the importance of digital evidence controls and the key techniques used to process electronic crime and incident scenes.

Developing & Creating a Computer Forensic Policy as Part of a Cyber Response Plan

Computer forensics is a critical component of any comprehensive cyber response program. This session will include how to train the security team in computer forensics, develop a comprehensive enterprise forensics policy and response plan, identify and verify security breaches, and strategies for handling a breach.

The Enemy Within: Protecting Information Assets from Insider Threats

Insider incidents cost US businesses \$600 billion dollars annually. This presentation is designed to provide attendees with information on identifying potential insider threats and strategies to manage them, including a taxonomy of insider threats, profiling the malicious insider, and recommended practices to mitigate insider threats.

Instructors: Dr. Vijay Kanabar, Associate Professor of Computer Science, Boston University and Kerry Anderson, CISSP, CISM, CISA, CFE, VP of Technology Risk with Fidelity Investment Brokerage Company

Date: Wednesday, March 7, 2007

Location: Boston College – Heights Room, Corcoran Commons, 140 Commonwealth Ave, Chestnut Hill, MA

Time: 8:30am – 4:30pm

CPE's: 7.5

Cost: \$75 Members, \$150 Non-Members

Registration Deadline: Thursday, March 1st

For more information and to register, click [here](#).

CISA Review Course

Gain an edge in preparing for the CISA exam with this three-day review course covering the six content areas on the exam:

- IS audit process – IS audit standards, guidelines and best practices
- IT governance – organizational structure, policies, accountability and monitoring to achieve corporate governance requirements
- Systems and infrastructure lifecycle - management of systems and infrastructure from acquisition to disposal
- IT service delivery and support – assuring that service management practices provide the level of services required to meet organizational objectives
- Protection of information assets – information security practices to assure confidentiality, integrity and availability of information assets
- Business continuity and disaster recovery

Contacts: Primary: Tony Giroti 617-480-6550 giroti@brookedge.com; Jing Dai, jing.dai@staples.com; Mandy Pahooja, pahooja@brookedge.com

Date: Three Saturdays: tentatively April 14th, 21st, and 28th. Dates will be confirmed in February.

Time: 8 a.m. - 4:30 p.m.

Cost: Members: \$295, Non Members: \$395

Location: To be announced.

Course Materials: Students will receive a printed version of the ISACA CISA review slides as course material, as well as printed copies of review questions from the ISACA CD.

Students should purchase their own copies of the 2006 CISA review manual.

For more information and to register, click [here](#).

2007 Chapter Calendar

Calendar Key:

★ Breakfast Meeting

✿ Seminar

✦ Board Meeting

★ Annual Meeting / Training Day

✦ CISA Review Course (tentative)

✿✿ CISA & CISM exam date

\$ Fee to attend

FEBRUARY 2007

SUN	MON	TUE	WED	THU	FRI	SAT
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15 ★ Metro-West Breakfast Meeting	16	17
18	19	20 ★ Providence Breakfast Meeting	21 ★ Boston Breakfast Meeting	22 ✦ Board Meeting	23	24
25	26	27	28			

MARCH 2007

SUN	MON	TUE	WED	THU	FRI	SAT
				1	2	3
4	5	6	7 ✿ \$ Forensics Seminar	8	9	10
11	12	13	14	15 ★ Metro-West Breakfast Meeting	16	17
18	19	20	21 ★ Boston Breakfast Meeting	22	23	24
25	26	27	28	29	30	31

APRIL 2007

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5 ✦ Board Meeting	6	7
8	9	10	11	12 ✿ \$ Computer Forensics Hands-on Lab	13	14 ✦ \$ CISA Review*
15	16	17	18 ★ Boston Breakfast Meeting	19	20	21 ✦ \$ CISA Review*
22	23	24	25	26	27	28 ✦ \$ CISA Review*
29	30					*tentative

MAY 2007

SUN	MON	TUE	WED	THU	FRI	SAT
		1	2	3	4	5
6	7	8	9	10	11 ★ Metro-West Breakfast Meeting	12
13	14 ★ Providence Breakfast Meeting	15	16 ✦ \$ Annual Meeting & Training Day	17	18	19
20	21	22	23 ★ Boston Breakfast Meeting	24	25	26
27	28	29	30	31		

JUNE 2007

SUN	MON	TUE	WED	THU	FRI	SAT
					1	2
3	4	5	6	7	8	9 ✿✿ \$ CISA/CISM Exam
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28 ✦ Board Meeting	29	30

CISA and CISM Certification



The CISA designation has been a globally accepted standard of achievement in the information systems (IS) audit, control and security field since 1978, and has been recognized by many governments and major business groups around the world.

Earning the CISA designation helps assure a positive reputation as a qualified IS audit, control and/or security professional.

CISM, the Certified Information Security Manager is ISACA's next generation credential and is geared toward experienced information security managers.

CISM is designed to provide the assurance that those earning the designation have the required knowledge to provide effective security management and consulting.

The next CISA and CISM exams will be offered on **Saturday, June 9th, 2007**.

Early registration deadline is February 14, 2007. Final registration deadline is April 11, 2007.

Visit ISACA's website for more information about the CISA and CISM certification programs or click [here](#).

Preparing for CISA and CISM Certification Exams

What do the CISA and CISM exams cover?

Both exams test a candidate's knowledge of IS audit principles and practices as well as technical content areas.

The CISA exam covers six content areas (domains) and tasks that are routinely performed by a CISA. For specific details, see <http://www.isaca.org/cisacontentareas>.

The CISM exam covers five information security management areas, each of which is further defined and detailed through task and knowledge statements.

Specific details can be found at www.isaca.org/cismcontentareas. Both certifications also require candidates to meet minimum requirements for professional experience.

The recommended Examination Reference Materials include:

- CISA and CISM Review Manuals
- CISA and CISM Review Questions, Answers and Explanations
- Self-study materials can be found by going to the ISACA web site at <http://www.ISACA.org>.
- Web sites for additional study materials are available at: <http://www.srvbooks.com> and <http://www.micromash.net>.

See "Upcoming Chapter Events" in this issue for ISACA New England's CISA review course.

Invitation to Participate

Board and Committee Service

ISACA's and ITGI's key boards and committees depend upon member participants to ensure that all members receive the high-quality resources they have come to expect from these organizations. Participants on key boards and committees help ensure successful certification programs, professional conferences and education, research, online resources, professional standards, and financially sound infrastructures. Serving on a key board or committee carries with it several benefits, including:

- A role in the future of the association and institute
- Networking and sharing expertise with peers around the globe
- Enhancement of leadership and professional skills

The selection of members for board and committee service is based upon the current needs of those groups, the relevant professional background of the candidates and the need to reflect a global perspective. All appointments are for one-year terms and are ratified by the Board of Directors at the first meeting of the administrative year (this year, in July). To apply, complete the application form included with volume 1, 2007, of the *Information Systems Control Journal*. Forms may also be downloaded from <http://www.isaca.org/participate>. The deadline is April 6, 2007.

Nominations to Board of Directors

Maintaining a strong and devoted Board of Directors is crucial to ISACA's ongoing success. Recruitment of candidates for ISACA's Board of Directors reflects input from many sources, including nominations submitted by members. ISACA is looking to its members to recommend individuals for board leadership who can help carry the organization to new heights of excellence and innovation.

When considering nominations, members should review the specific responsibilities for each position listed on the nomination form. Each board member is expected to:

- Attend three Board of Directors meetings per year and the leadership conference in his/her own geographic area
- Possess strong leadership, strategic planning, volunteerism and innovative thought capabilities
- Maintain a global perspective on professional issues and ISACA matters
- Be motivated to accomplish board-mandated initiatives and be willing to participate in all aspects of fundraising activities
- Possess a significant network of professional contacts
- Adhere to the ISACA Code of Professional Ethics

International board members serve a one-year term. To submit a nomination, members should complete the Board of Directors nomination form that is included with volume 1, 2007, of the *Information Systems Control Journal*[®]. The form is also available online at www.isaca.org/nominate. Nominations are due March 23, 2007.

Feedback on Draft IS Auditing Guideline *Return on Security Investment (ROSI)*

Feedback is sought on the exposure draft for the IS Auditing Guideline titled *Return on Security Investment (ROSI)*. The draft can be reviewed at www.isaca.org/standardexposure, where comments may also be provided via the online questionnaire posted with the exposure document. All comments received will be carefully considered by the Standards Board. The deadline to submit comments is January 31, 2007. Please note that to substantiate CISA/CISM CPE credits claimed for exposure draft review under the category "contributions to the IS audit and control profession" (10-hour annual limitation), a copy of comments should be kept as no formal certificate is awarded.

ISACA Conferences and Training

Distance Learning Opportunities

Next ISACA e-Symposium to address COBIT 4.1 update

The next monthly ISACA e-Symposium will be presented on January 30, 2007 and will focus on the COBIT 4.1 release update and accompanying COBIT tools. Presenters will include Debbie Lew, Gary Hardy, Jimmy Heschl and Roger Debreceeny.

To register for an ISACA e-Symposium and earn three CPE credits at no charge, please visit www.isaca.e-symposium.com.

Last month's e-Symposium covered identity and access management and offered suggestions on how to use these to reduce costs and increase business efficiency.

2007 Conferences and Training Weeks

ISACA is offering a full calendar of conferences and training weeks for audit, governance and security professionals this year. US-based events include Training Weeks in February, May, November and December, the North America CACs in April, and the Information Security Management Conference in September.

For more information and to register, visit the Education and Conferences link on ISACA's website, www.isaca.org or click [here](#).

ISACA 2007 North American Conferences and Trainings

						
	ISACA Training Week	North America CACS	ISACA Training Week	Information Security Management Conference	ISACA Training Week	ISACA Training Week
Dates*	26 February-2 March 2007	22-26 April 2007	7-11 May 2007	10-12 September 2007	5-9 November 2007	3-7 December 2007
Location	Washington DC	Grapevine, Texas	Denver, Colorado	Las Vegas, Nevada	San Antonio, Texas	Scottsdale, Arizona
CPE Hours	38	44	38	TBA	38	38

* As of January 2007. Check ISACA's website, [TUwww.isaca.orgTU](http://www.isaca.org), throughout the year for additional offerings or updates.

ISACA New England Sponsors

Air Defense

<http://www.airdefense.net>



Vatchfire

<http://www.watchfire.com>



Resources for Job Seekers

To review previous months' career advertisements, visit the archive on the ISACANE website at <http://www.isacane.org/jobs.php>. Members can also benefit from career resources and job listings on the ISACA International website. Click [here](#) to link to the ISACA Career Centre online.

Resources for Employers and Recruiters

The fee to post an ad on the website and next newsletter is \$100 per month per ad. To place a career advertisement with the ISACA New England Chapter please email the following information to the webmaster@isacane.org:

- 1) Number of Months you would like to post the ad
- 2) Company Name
- 3) Job Title
- 4) Job Description
- 5) Contact Name and Address
- 6) A Link (if applicable) for the reader to get more information

Note: No refunds will be provided if the position is filled prior to the end of the period requested.

Editor's Note

Views and opinions contained in this e-newsletter are solely those of the author and do not necessarily represent or reflect the views or opinions of the New England Chapter of ISACA. In the event you have any questions concerning articles in the newsletter, please contact the author directly.

The e-newsletter is published September through May. Members are invited to submit brief articles, book reviews or IT audit or security management tips. Submissions should generally not exceed one page and must be received by the 15th of the month for consideration for the following month's e-newsletter.

For more information, please contact the editor, Heather Fowles, CISA, CISSP at newsletter@isacane.org.