

**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

September/October 2006

President's Message

As the summer comes to a close and the ISACA 2006 – 2007 year begins, I would like to extend a welcome to this year's ISACA New England board. I would also like to thank Mike Field, past president 2004 – 2006 for his dedication and hard work over his two years as president, thank you Mike!



Over the summer several of our committees were hard at work preparing for the fall. The web team redesigned our website. It looks fantastic and I would encourage everyone to check it out at www.isacane.org! We hope to continue to expand the website in the future.

Our programs and seminars committee was hard at work putting together the seminar schedule for this year. In addition to our annual offering of the ACL beginner's and advanced classes, a one day "Data Analysis Strategies and Methodologies" class has been added to the schedule. We are also hosting a cocktail hour right after our November 1st seminar on wireless security. Come join us and network with your fellow ISACA members.

Our CISA committee has also been busy. We are offering a CISA review class this fall. For those planning to take the CISA exam in December, the review course is an additional study option.

In addition to the seminars we also have a breakfast committee that has organized several Breakfast meetings scheduled on various topics such as compliance and assessing application providers. You can find information on the seminars, CISA review, and breakfast meetings on our website. Enjoy the fall!

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

Did you know?

Seminar fees can be paid by credit card. We can accept major bank credit cards including VISA, MasterCard, Discover, and American Express. **ISACA NE offers an online credit card payment option when you register for a seminar or for the CISA/CISM review courses.** If desired, participants can continue to pay for seminars with personal or company check, or cash. Advertisers are also welcome to pay for their web and newsletter ads by credit card.



Upcoming Chapter Events

CISA Review Course

Gain an edge in preparing for the CISA exam with this 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 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 – service management practices
- Protection of information assets – information security practices to assure confidentiality, integrity and availability of information assets
- Business continuity and disaster recovery

Instructors: John Beveridge, Tony Giroti

Date: 3 Full Days: Saturday October 14 and 28, Sunday, November 12

Time: 8 a.m. - 4:30pm (arrive 15 minutes for first meeting for registration). Lunch will be served.

Cost: Members: \$275, Non Members: \$375

Registration Deadline: October 6, 2006 (Late registration, add \$25 to cost.)

Location: Northeastern University, Henderson House, 99 Westcliff Road, Weston, MA

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](#).

Breakfast Meetings

Managing Compliance

Speaker: Jack Morency

Date: October 18, 2006

Location: Boston, Jefferson Wells

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

CPEs: 2

Cost: Free to ISACA New England members

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

Assessing Application Service Providers

Speaker: Anne Oribello, Genzyme

Date: November 14, 2006

Location: Johnson & Wales

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

CPEs: 2

Cost: Free to ISACA New England members

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

Social Engineering

Joint meeting with ACFE Rhode Island Chapter

Speaker: Jerry Hughes, Lighthouse Computer Services

Date: December 4, 2006

Location: Chelo's, 2225 Post Rd, Warwick, Rhode Island

Time: 8:00-11:00 a.m.

CPEs: 3

Cost: \$17—ACFE & ISACANE members, \$27—non-members

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

Upcoming Chapter Events

Wireless Security Seminar

This session will provide information security auditors with the tools and knowledge to prepare for and perform assessments of wireless networks and interpret the results. It will also help security managers understand their wireless risks and how to pass a wireless audit.

The seminar will provide an introduction to the types of wireless, with a focus on 802.11a/b/g and Bluetooth, as well as a discussion of the future of wireless. Risks in using wireless will be discussed as well as controls to mitigate them. Tools and techniques that are used to perform wireless security assessments will be presented along with how to interpret the results and secure the environment.

Instructor: Martin Dolphin, CISA, CISM, CISSP, Senior Manager within Ernst & Young's Technology, Security & Risk Services Practice, based in Boston, MA.

Mr. Dolphin has been responsible for a variety of security audit projects ranging from wireless audits, operating system audits and web-based architecture audits, to application controls assessments, security policy development, and security awareness training with clients in a wide variety of industries. While at Ernst & Young, Mr. Dolphin has co-developed methodologies and tools for Microsoft Windows NT/2000 attack and penetration and for audit work programs for assessing risks and control within Windows NT/2000 and Novell Netware. Mr. Dolphin is also co-instructor and co-author for the Ernst & Young's eXtreme Hacking course. He has presented on many security topics at SANS, TISC and Usenet, and is a technical editor for the 'Hacking Exposed' book (Vol. I and II). He also is a board member of the Information Systems Audit and Control Association (ISACA), member of International Information Systems Security Certification Consortium, Inc. (ISC2) and Information Systems Security Association (ISSA).

This timely seminar will offered in two locations as follows:

Rhode Island and Southeast Massachusetts

Date: Monday, October 30, 2006

Time: 9 a.m. – 3 p.m.

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

CPE's: 5

Registration Deadline: Thursday, October 26th

Location: AMICA

100 Amica Way

Lincoln, RI 02865

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

Boston and Metro West

Date: Wednesday, November 1, 2006

Time: 12 p.m. – 5 p.m.

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

CPE's: 5

Registration Deadline: Thursday, October 26th

Location: Marriott Newton

2345 Commonwealth Avenue

Newton, MA 02466

Please note: the Metro-west seminar will be followed by a cocktail hour from 5 p.m. to 7 p.m.

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

Security Manager's Corner

Computer Security Institute Road Show

Results of the 11th Annual CSI/FBI Computer Crime and Security Survey

CSI Director Robert Richardson brought a road show on the results of the 2006 CSI/FBI Computer Crime and Security Survey to Boston's Marriott Copley on September 13th.

This year's findings included responses from 616 of CSI's 5000 U.S. members, representing both large and small organizations and a variety of industries.

Richardson noted that while viruses remained the top category of incidents, totals continued to decline from their 2001 peak. Laptop theft was in the second place, followed by insider abuse of Net access, unauthorized access to information and denial of service.

Estimated losses from incidents also continued to drop in this year's survey, with average loss reported per respondent decreasing from \$203,606 to \$167,713, a decline of 18%. Richardson cited other surveys and data in support of the trend and considered that the explanation may lie in a shift in focus from attacks on commercial businesses to consumers.

FBI Special Agent Jim Burrell, who spoke following Richardson's presentation, concurred with this view, citing improved defenses in industry and the growth in the number of poorly defended home computers with high bandwidth connections that can be exploited.

Burrell blamed implementation issues, not the lack of technology or tools, for the information security problems that companies do

experience. He stressed the importance of conducting risk assessments to understand the weak points in company's defenses.

"Hackers won't try to break into your AES encrypted production database," he said. "They'll go after your unencrypted back up copies."

Burrell urged "following the money" to understand the threat landscape. "Data theft is where the money is," he said. He also pointed to the profits hackers can realize from botnets.

"Data theft is where the money is."

--FBI Special Agent Jim Burrell

Burrell recommended that information security professionals join an "information security sharing group" such as the Infragard program sponsored by the FBI, to help understand what issues are occurring in the field and to establish contacts within law enforcement in advance of an incident. "The last thing you want to do," he said, "is try to establish that relationship in the middle of an incident."

He also urged companies to report incidents, which can be critical for the FBI in building cases against repeat offenders. The 2006 survey noted a continuing reluctance by companies to report incidents to law enforcement.

The complete 2006 CSI/FBI Computer Crime and Security survey and other resources are available from CSI's website, www.gocsi.com.

-- Heather Fowles, CISSP, CISA,

IT Security & Governance Manager, DentaQuest

Any opinions expressed are the author's and do not represent the views of ISACA New England.

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.

The next CISA and CISM exams will be offered on Saturday, December 9th, 2006.

Registration for the December exam closed September 27th, 2006.

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



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.

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.

ISACA New England Sponsored Conference

MISTI Annual Conference on Control and Audit of Information Technology

Learn about best practices and how to overcome IT auditing challenges with six concurrent tracks that span everything from the latest regulations to the latest version of COBIT. This conference has something for the entire audit team.

Featured Speakers:

Simson Garfinkel

Author of 12 books including Database Nation, Columnist for CSO Magazine, and award-winning commentator and researcher, will speak on forensics and how it can be used by auditors.

Edward Robinson, CPA, CSP

Chief Executive Officer of The Robinson Group, will offer advice and inspiration on how to cope, survive, and thrive through the myriad changes that IT auditors experience.

Michael Rogers

MSNBC columnist "The Practical Futurist," former technical guru for Newsweek, and former Vice President of The Washington Post Company's new media division, will gaze into the crystal ball and predict what to expect from technology in the near and not-so-near future.

Dennis Treece

Director of Corporate Security, Massachusetts Port Authority, will examine digital video surveillance, how it promotes homeland security, and how it affects employees and the public.

Date: November 13 - 15, 2006

Time: 8:30 a.m. - 5 p.m.

Cost: Register as an ISACA Member and receive a 10% discount off the regular conference registration fee.

CPE's: 18

Registration Deadline: November 13, 2006

Location: Boston Marriott Copley Place, 110 Huntington Ave, Boston, MA 02116

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

Sarbanes-Oxley Symposium

This symposium will help companies attain the new paradigm for controls demanded by the Sarbanes-Oxley regulation

If there is one thing that the first round of attestations has made abundantly clear, it is that the Sarbanes-Oxley Act of 2002 does not disappear once a company is in compliance.

This symposium is designed for professionals from companies that are now in compliance with Sarbanes-Oxley and have had a compliance audit.

The symposium will:

- Identify best practices, lessons learned and common pitfalls to continue to improve the process into the next round of attestation audits.
- Explore ways companies can leverage the work and resources of the compliance project to achieve efficiencies and continue to improve processes.
- Take a look at potential regulations and guidelines that the Public Company Accounting Oversight Board (PCAOB) may be issuing in the near future.

The participant will learn more about:

- The latest US Securities and Exchange Commission (SEC)/PCAOB issues
- Leveraging the compliance effort
- Gearing up for year two
- Taking an enterprise risk management approach
- A balance between application controls and general controls
- Documenting new processes and capturing enterprise change management
- Remediating deficiencies and resolving weaknesses

Prerequisites:

The participant should have an understanding of controls and how they fit into an overall control framework for the enterprise.

October 12-13 – Washington, DC

For registration information, please visit the ISACA website or click [here](#).

ISACA Conferences

CISA and CISM Review Workshops at the November Computer Security Institute (CSI) Conference

CISA® Exam Prep Course

The CISA Exam Prep Course is a two-day workshop designed to assist and enhance the study process of Certified Information System Auditor™ (CISA) candidates in preparation for the December 2006 CISA exam.

The course will address IS audit practices, issues and concepts and will follow the newly defined CISA job areas, task statements and knowledge statements.

The participant will learn about:

- The CISA exam study process
- IS audit practices defined in the CISA job practice
- Related practices, topics, issues and concepts
- The structure of CISA exam items via use of practice questions

Note: This workshop is a supplement to an intensive, multiple week ISACA chapter review program.

CISM® Exam Prep Course

This two-day workshop is a review course designed to assist and enhance the study process of Certified Information Security Manager® (CISM) candidates in preparation for the 2006 CISM exam.

The course will address information security management practices, issues and approaches and will follow the CISM job areas, task and knowledge statements. Workshop participants will receive extensive handout material including ISACA's CISM Review Manual 2006, as well as complimentary material developed by the presenter.

The participant will learn more about:

- The CISM exam study process
- Information security practices defined in the CISM job practice
- Related practices, topics, issues and concepts
- The structure of CISM exam items via use of practice questions

Note: This workshop is a supplement to an intensive, multiple week ISACA chapter review program.

November 9-10 – Orlando, FL

For registration information, please visit the CSI Conference website or click [here](#).

ISACA New England Sponsors

| | | | |
|-----------------------|---|------------------------|---|
| Deloitte & Touche LLP | http://www.us.deloitte.com/ | CaseWare IDEA Inc. | http://www.caseware-idea.com/ |
| KPMG | http://www.us.kpmg.com/ | MIS Training Institute | http://www.misti.com/ |
| Ernst & Young | http://www.ey.com/ | Wolf & Company | http://www.wolfandco.com/ |
| ACL Services Ltd | http://www.acl.com/ | | |

Job Resources

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

Job positions may be advertised in our e-newsletter or through our World Wide Web page. Fees are \$50 for a ¼ page, \$100 for a ½ page and \$200 for a full page (8 1/2 by 11 inch) for either the newsletter or the web page. (Thus, a full size page on both the newsletter and the web would cost \$400.)

Job Ad Posting Process

Create an ad in MS Word, formatted as you wish, including hypertext links. Newsletter ads will run in the next month's emailing and web ads will be posted within a week and stay up until September 1 or until requested to be taken down. To place an advertisement in the ISACA New England Chapter (ISACANE) **home page** please email position information to webmaster@isacane.org. To place an advertisement in the ISACA New England Chapter (ISACANE) **e-newsletter** please email information to Heather Fowles at hfowles@rcn.com.

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, at hfowles@rcn.com.