CHAPTER NEWSLETTER

March 2009
Volume 3

ISACA®
Serving IT Governance Professionals
Rhode Island Chapter

TABLE OF CONTENTS

VOLUNTEER OPPORTUNITIES

Earn up to 10 ceu's annually by volunteering to serve your chapter, and benefit from the many opportunities for leadership growth and professional development that volunteerism offers. Send an email to ***info@isaca-ri.org*** if you are interested in serving on any of the following capacities:

Communications (newsletter)
Membership (e-bulletins)
Certification (liaison)

PRESIDENT'S MESSAGE

Dear Colleagues,
I hope that you'll be able to attend our next training session. On April 8, a daylong seminar on 2 highly pertinent topics—*Risk Assessment of Data Privacy* and *Certifying Information Security* (see Seminar Schedule sidebar)—is being presented jointly by ISACA-RI and ISACA-NE. Register at www.isaca-ri.org.

Additional reasonably priced, high value seminars are planned for May and June 2009, the latter being the ISACA-RI Chapter's Annual Meeting and Awards Luncheon. We'll advise you of upcoming seminars details as they evolve, to encourage you to save the dates and register to attend.

As a reminder—if you haven't already done so, be sure to renew your membership with ISACA International.

Regretfully, ISACA-RI was unable to administer local CISA training due to insufficient interest. Subsequently, Brookedge Technologies has partnered with ISACA-RI to provide a special rate to our members for CISA and CISM training that will be held in Rocky Hill, CT on three Saturdays in May. See "Certification Corner" for details.

Lastly, Will Nowik of Wolf and Company has generously provided the chapter with a timely article: *"Don't Let Your Information Technology Be A Game of Chance – Is your change management up to the test?"* (See page 3).

Best regards to you during the spring season.

Camille R. Rigney, CISA
ISACA-RI President, 2007-2009

SEMINAR SCHEDULE

2008-2009
REGISTER at www.isaca-ri.org

April 8, 2009
Four Points by Sheraton Norwood
Hotel & Conference Center
Norwood, Massachusetts
Full day seminar 6 CEUs
$100 members
$125 non-members
Co-hosted with ISACA-NE
8:30 - 9 am registration
RISK ASSESSMENT OF DATA PRIVACY
9 am – noon
Will Nowik & Matt Putvinksi,
Wolf and Company
CERTIFYING INFORMATION SECURITY
1 -3:30 pm
Don Borsay, FM Global
Breakfast, lunch, and breaks included in registration fee

May 2009
Topic & Location TBD
½ day seminar
Co-hosted with IIA Ocean State Chapter
Steve J. Ursillo, Jr.
Sparrow, Johnson, & Ursillo, Inc.

June 2009
ANNUAL BUSINESS MEETING & SEMINAR
RECOGNITION OF RECENT CERTIFICATIONS
Full day seminar
Topic, speaker, & location TBD

CERTIFICATION CORNER

CISA, CISM and CGEIT Certification

This spring, the ISACA-RI Chapter planned to sponsor a Certified Information Systems Auditor™ (CISA®) Examination Study Course in preparation for the June 13, 2009 examination.

However, due to minimum enrollment numbers not being met (8 persons); we were not able to hold the Study Course. We plan to re-evaluate this again in the fall in preparation of the December 2009 CISA examination.

Knowing the importance of preparing for these examinations; and our commitment to adding value to existing and prospective members; we are pleased to announce that ISACA-RI and BROOKEDGE Technologies have jointly organized CISA, CISM and CGEIT review courses. These classes will help students prepare for ISACA's CISA, CISM and CGEIT exams respectively. The CISA and CISM courses will be held on three Saturdays (May 9, 16, 30) in the greater Hartford area just south of the city at the Hartford Marriott Rocky Hill hotel.

The CGEIT course will be held on Monday and Tuesday (Jun 1 and 2) in the Boston metro area just west of the city at The Westin Waltham-Boston hotel. Each course starts at 8:30am and ends at 5:00pm with a 45 minutes to 1-hour lunch break and networking session.

Please check our ISACA-RI website for further information beginning in April 2009.

Certification training and reference material provided by ISACA International at www.isaca.org:

CISA Certification

- *CISA® Review Manual 2009* (available in English, French, Italian, Japanese and Spanish)
- *CISA® Review Questions, Answers & Explanations Manual 2009 Supplement* (100 questions; available in English, French, Italian, Japanese and Spanish)
- *CISA® Review Questions, Answers & Explanations Manual 2008* (600 questions; available in English, Italian, Japanese and Spanish)
- *CISA® Review Questions, Answers & Explanations Manual 2008 Supplement* (100 questions; available in English, French, Italian, Japanese and Spanish)
- CISA® Practice Question Database v9 (800 questions—CD-ROM or web download; available in English and Spanish)

CISM Certification

- *CISM® Review Manual 2009 (available in English, Japanese and Spanish)*
- *CISM® Review Questions, Answers & Explanations Manual 2009 (450 questions; available in English, Japanese and Spanish)*
- *CISM® Review Questions, Answers & Explanations Manual 2009 Supplement (100 questions; available in English, Japanese and Spanish)*
- *CISM® Practice Question Database v9 (550 questions—CD-ROM or web download; available in English only)*

CGEIT

Reference material for the 2009 CGEIT Exam may be obtained at www.isaca.org/cgeitbooks and www.isaca.org/cgeitreferences.

For questions concerning any of ISACA's certifications, feel free to contact:

William C. Soares, CISA, PMP
ISACA-RI Certification Director
bill.soares@cox.net
.

Don't Let Your Information Technology be a Game of Chance - Is your change management up to the test?

By Will Nowik, CISA, CISSP

At its core, a change management program serves to minimize disruption of your business. It includes assessing the impact of the change on connected systems, testing of the change before rolling it out enterprise-wide and obtaining authorization and approval from management. Even if there are procedures governing how IT changes are made, more often than not, critical systems and application outages are caused by unauthorized changes. Whether these unauthorized changes are business requirements, a quick patch to a problem, or poor internal practices, they make your organization vulnerable to:

- Operational Issues - Unplanned downtime of the organization's most critical systems and costs responding to errors rather than being utilized to improve business processes.
- Information Security Issues - Non-public data left unprotected and vulnerable to theft.
- Regulatory Compliance Issues - Noncompliance with the requirements dictated by the Gramm-Leach-Bliley, Sarbanes-Oxley, and HIPAA acts, as well as industry requirements such as the Payment Card Industry Data Security Standards (PCI DSS);
- Financial Reporting Issues - Increased opportunity that independent auditors will cite the organization for inadequacies in change management practices increasing board and regulatory scrutiny.

How are you doing?
Proactive assessment of your change management process can increase its effectiveness and give the organization faith that it is doing everything it can do to maintain a secure, compliant, and operational IT environment. Start with defining your key performance indicators (KPI), otherwise known as what the organization considers success. When determining the KPI's important to your organization ensure that each is SMART: Specific, Measurable, Achievable, Relevant, and Time-bound. Placing these limits around each KPI will help to break the issues into workable projects rather than one large problem that can seem overwhelming. A few examples of KPI's the SMART way:

KPI:
Review the number of authorized changes versus unauthorized changes

SMART KPI:
Review all changes having taken place in the past 12 months. Goal is to have 95% being authorized changes.

KPI:
Measure the number of disruptions of service caused by unauthorized data.

SMART KPI:
Measure the number of disruptions in the past month, noting the amount of downtime per each disruption.

Consistency is key.
All of the planning in the world won't be worth anything if you're not going back and reviewing the results. Once you have defined your KPI's, you should track the progress toward your goal. Analyzing the goals to actual outcomes will clarify where opportunities for improvement exist. The indicators important to each organization will vary but this consistent measuring will provide insight into areas that require enhancement and make sure that disruption is always trending downward. By performing such an activity, limited IT resources can be used proactively rather than reacting to a "fire-drill" situation.