



**Do you need CPE by year-end?**

**Are there topics or issues you would like to discuss with an industry expert and your peers?**

**Join us for a *Free* Breakfast Roundtable Discussion!**

This roundtable is scheduled for Thursday December 3rd from 8:30 to 10:30 AM at Navigant Credit Union in Smithfield, RI.

The only cost is the submission of one question with your registration. To get the most value of the roundtable, all questions will be emailed in advance to all attendees.

Industry expertise will be provided by Javed Ikbal. Javed is a co-founder and principal at zSquad, an Information Security and IT Audit consulting company. Javed specializes in building or re-engineering information security programs, IT auditing and application security issues. Javed holds the CISSP, CISM and CISA certifications

The session will be moderated by our chapter Past President, Camille Rigney. Please see our website for additional details and registration. ***Hurry – registration is limited to the first 20 registrants!***

**CONTENTS**

President’s Message.....1

Certification Corner.....2

ISACA Global News.....2

Article: The Adoption of Data Mining..... 3

ISACA Research–Shopping on the Job.....4

ISACA-RI’s 2009-2011 Board.....5

**PRESIDENT’S MESSAGE**

Dear Colleagues:

Two of our board members are on the move! Nitesh Kumar and Salomon Frangeigh have accepted opportunities in other countries. Serving on our Programming Committee, Nitesh played a valuable role in selecting speakers for topics that our members have requested. Nitesh also presented to the membership on Auditing SQL Server. Salomon had recently joined our board serving as our Audit Chair. On behalf of our members and board, I would like to sincerely thank them for their contributions and wish them well.

Our first two training events of the year were well attended and received. Attendees received valuable and timely information on IT Governance, privacy, and PCI compliance.

We are excited to offer another free breakfast roundtable on December 3rd. The discussion will be based on questions submitted by registrants. Along with your peers, Javed Ikbal of zSquad will be available to provide his expertise. **Sign up now - attendance is limited to the first 20 registrants.** Our Programming Committee is continuing to work on plans for 2010 events. Mark your calendars for a full day session on Integrated Auditing scheduled for February 23, 2010. Mitch Levine, CISA, founder of Audit Serve, Inc. will be our presenter. We are planning a joint meeting with the PMI’s Ocean State Chapter in April. Additional events are being planned and will be announced soon – keep checking our website for up-to-date information. As always, we welcome your suggestions on future topics and speakers. Please forward them to [info@isaca-ri.com](mailto:info@isaca-ri.com).

I had the honor of attending the Presidents Council Meeting for Eastern Region chapters of ISACA in October. The meeting provides an opportunity to network and exchange ideas with board members of other chapters. As a new chapter, we have the great fortune of learning from experiences of established chapters. Two representatives from ISACA International - Megan Moritz, ISACA Lead Chapter Relations Coordinator, and Patricia Goh, Chapter Support Committee - provided the attendees with an update on International’s new strategy, organizational structure, and the upcoming web site redesign!

The holiday season is upon us. Will you or your staff be shopping on-line for the holiday season? Read the results of ISACA’s® research of on-line shopping in the workplace.

On behalf of the entire board, I wish you a safe and happy holiday season!

Pauline G. Lamantia, CISA  
ISACA-RI President, 2009-2011

***ISACA-RI would like to acknowledge the following organizations for having provided free seminar and meeting space—AMICA, Citizens Bank, FM Global, and Navigant Credit Union. The chapter appreciates their support.***

**CONTACT INFORMATION**

RI Chapter website: [www.isaca-ri.org](http://www.isaca-ri.org)  
RI Chapter President: [president@isaca-ri.org](mailto:president@isaca-ri.org)  
RI Chapter General Information: [info@isaca-ri.org](mailto:info@isaca-ri.org)  
ISACA Global website: [www.isaca.org](http://www.isaca.org)

## CERTIFICATION CORNER

Registration for the December 2009 exams is now closed. If you have registered and do not receive an admission ticket by December 1<sup>st</sup>, notify [certifications@isaca.org](mailto:certifications@isaca.org). Best of luck to our members who will be sitting for an exam!

Exam preparation materials offered through ISACA International at [www.isaca.org](http://www.isaca.org) :

### CISA

- The CISA® on-line review course provides a choice of six modules covering the scope of information systems audit and review activity. The modules can be purchased separately or as a bundle. ISACA members receive a discount. Additionally, by specifying the code ISACA197, you will earn an additional 30 days on your course subscription length.
- CISA® Review Manual
- CISA® Review Questions, Answers & Explanations Manual
- A full list of CISA publications is available at [www.isaca.org/cisabooks](http://www.isaca.org/cisabooks).

### CISM

- CISM® Review Manual is a comprehensive reference guide. The 2009 edition has been developed to help the candidate understand essential concepts and is organized to facilitate study by job practice areas.
- CISM® Review Questions, Answers & Explanation Manual 2009 edition.
- CISM® Practice Question Database v9.
- A full list of CISM publications is available at [www.isaca.org/cismbooks](http://www.isaca.org/cismbooks).

### CGEIT

- Reference material for the CGEIT exam may be obtained at [www.isaca.org/cgeitbooks](http://www.isaca.org/cgeitbooks) and [www.isaca.org/cgeitreferences](http://www.isaca.org/cgeitreferences).

Riebeek Stevens, CISA, CISM, CGEIT in collaboration with Interactive Security Training and Imperva, will offer **FREE Refresher Webinars to cover the December 2009 CISA, CISM and CGEIT exams.**

CISA Nov 22 at 11:00 AM EST:

<https://www2.gotomeeting.com/register/764350931>

CISM Nov 22 at 3:00 PM:

<https://www2.gotomeeting.com/register/790029835>

CGEIT Nov 30 at 11:00 AM:

<https://www2.gotomeeting.com/register/546517890>

For questions concerning any of ISACA's certifications, please send an email to [info@isaca-ri.org](mailto:info@isaca-ri.org)

## ISACA GLOBAL NEWS

### Cloud Computing Benefits and Risks Detailed in New ISACA Guidance

**Rolling Meadows, IL, USA (29 October 2009)**—Cloud computing is rapidly becoming a business information technology (IT) buzz word, but there is still much debate on what exactly it is and how it benefits enterprises. A new white paper from ISACA, a nonprofit association of 86,000 global information technology professionals, clearly describes how enterprises can achieve greater efficiencies and mitigate new risks associated with cloud computing. The white paper, *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives*, is available as a free download from [www.isaca.org/cloud](http://www.isaca.org/cloud).

Cloud computing offers enterprises the ability to reduce IT infrastructure costs through a model of paying for service on demand. This requires less upfront capital expenditure and allows businesses to benefit from the ability to efficiently ramp up and power down based on current needs, as well as the flexibility to introduce new IT services.

“One way of describing cloud computing is to compare it to a utility,” said Jeff Spivey, trustee for the IT Governance Institute, which is affiliated with ISACA, and director of Security Risk Management, Inc. “In the same way businesses pay for the amount of electricity, gas and water that they use, there is now the ability to pay for IT services based on how much is consumed.”

As with any new advancement, though, there are many facets to consider.

“The benefits of cloud computing are tremendous, but it also creates new risks and security concerns,” added Spivey. “Through cloud computing, IT services can be contracted through an external provider, so new governance and control approaches are needed to ensure flexibility, resilience and security.”

According to the white paper, in addition to the financial savings involved with cloud computing, one of this model's strengths is for enterprises to streamline processes and increase innovation. This can translate into more reliable backup, more satisfied customers, increased scalability and possibly even higher margins.

While the risks associated with cloud computing may be similar to business IT risks already addressed, enterprises may need to adjust their policies and procedures to focus on the new dynamic environment. The white paper also delivers effective strategies for mitigating risks and addressing assurance issues related to cloud computing.

“The cloud represents a major change in the way computing resources will be utilized,” said Spivey. “By addressing many of these issues in advance, and with the involvement of a broad range of stakeholders, enterprises can gain significant advantage with appropriate control.”

In recognition of new risks around this emergent technology, ISACA has become an affiliate of the Cloud Security Alliance, which collaborated on this paper and will be involved in joint projects with ISACA in the future ([www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)).

## **The Adoption of Data Mining Not That Kind of Mining - How Data Mining Raises the Bar in Assurance**

**By Patrick S. King, CISA, Senior IT Assurance  
Consultant, Wolf & Company, P.C.**

This current regulatory environment continues to evolve into one of the most formidable ever seen. Requirements of corporate governance are at an all-time high as audit committees, boards of directors and executives require more assurance on the operating effectiveness of their controls from their internal auditors, external auditors and accounting departments. While these requirements will lead to improved success against fraud and financial misrepresentation, community financial institutions are likely to be challenged as there may be fewer people and less money available to complete the activities. A technique gaining momentum to affirm assurances to senior management and bolster risk management practices while keeping costs low is data mining. Essentially, the process is extracting and analyzing large volumes of data from computer applications in a manner that detects obscure facts, trends, or inconsistencies. The techniques allow the user to perform testing on 100% of a population to identify all of the discrepancies rather than choosing a sample and testing only a limited piece. Initially, the ability to report on particular measures and statistics directly helps to manage and consolidate data, providing the opportunity to maximize audit effectiveness. Looking down the road a bit, the operations can be improved as 100% of data is tested for veracity, suspicious transactions are found, and requirements of Sarbanes-Oxley and similar regulations are met.

### **Don't be an easy target**

When you have disparate systems, it makes it difficult to monitor data and identify potential fraud, and you could become an easy target for thieves. Data mining allows institutions to proactively extract electronic information, developing knowledge of trends and standard practices. Utilizing that information, it is easier to detect irregular behavior before an institution experiences a financial loss or reputation damage.

All institutions maintain financial data electronically, including general ledger transactions, customer information, customer transactions, and vendor information. This data is used to manage and operate the day-to-day activities of the institution to record income, prepare statements, process transactions, and pay vendor invoices. Applying data mining techniques to this data could identify high risk and possibly suspicious transactions including:

- Matching dollar journal entries recurring at similar frequencies (e.g. quarter-end);
- Duplicate invoice numbers from the same vendor;

- Unusually high or even-dollar payments to vendors;
- Loans over and under specified lending limits, terms, or rates;
- Deposit accounts with a change of address and reversal transactions performed within a given period.

### **The Road to Acceptance**

Historically, one of the biggest hurdles to the implementation of data mining is the belief within the institution that this type of testing activity is for organizations in larger asset or revenue ranges. Even the single-branch community bank will have thousands of transactions running through the systems on a regular basis, many of which cross over multiple systems. It would not be physically possible to monitor 100% of the transactional activity by reading through the paper reports kept at the institution. Not to mention what the cost would be for employee time and the paper resources used in this endeavor. In fact, the majority of systems running in institutions today have been designed by their creators with the ability to produce the necessary reports and export data in a usable format.

When conducting due diligence, the institution needs to define what data it will be interested in testing and what information will be needed in order to perform the tests. Additionally, there should be research conducted to determine where the data is coming from and in what format, so that the output will be usable to the data mining tools. Within the systems, there exist numerous options for export. Each system can be run on a number of databases and can have any number of reporting capabilities and formats, so evaluate each system on a case-by-case basis to determine the best method for obtaining the data. Once implementation is completed, the benefits of continuous testing quickly become apparent as standard tests can be performed at any time by utilizing updated information. As use of data mining grows within the institution, the techniques will lend themselves for developing new tests on additional data systems.

The regulatory environment is redefining how institutions are required to mitigate risk and provide assurance. The ever-increasing regulatory pressure on management to properly protect customer information and allow auditors to provide assurance of financial statements and operational controls is pushing the industry to find more effective and efficient methods of testing. Most technology systems in use today were endowed with the basic function to pull data into a usable format. Taking advantage of this capability, institutions can evolve their traditional means of testing and raise the bar on their assurance and risk management practices.

*Reprinted with permission from Wolf & Company, P.C.*



### **Survey: Employees Plan to Spend Nearly Two Full Work Days Shopping for the Holidays Using Work Computers**

*ISACA research reveals major gap between employee's online behaviors and business expectations*

#### **Rolling Meadows, IL, USA (21 October 2009)—**

Employees plan to spend nearly two full working days (14.4 hours) on average shopping online from a work computer this holiday season, according to a survey conducted on behalf of ISACA, a nonprofit association of 86,000 information technology (IT) professionals. One in 10 plans to spend at least 30 hours shopping online at work. Convenience (34%) and boredom (23%) are the biggest motivators, according to those polled.

Despite an economy expected to show flat or declining holiday retail sales, the second annual "Shopping on the Job: Online Holiday Shopping and Workplace Internet Safety" survey found that fully half of those surveyed plan to shop online for the holidays using a work computer. Less surprising is a growing uncertainty—the number of employees who are unsure about whether they will spend more or less time shopping online compared to a year ago has doubled.

The potential danger of shopping online is that it can open the door to viruses, spam and phishing attacks that invade the workplace and cost enterprises thousands per employee in lost productivity and potentially millions in destruction or compromise of corporate data.

Employees who shop online using a work computer are also likely to engage in other high-risk behaviors. Survey participants also bank online (51%), click on e-mail links redirecting them to shopping sites (40%) and click on links from social network sites (15%). Yet nearly one in five says they are not concerned that their online shopping habits may affect the safety of their organization's IT infrastructure.

"With the Internet now available to almost any employee in the workplace, it's unrealistic to think that companies can completely stop the use of work computers for online shopping," said Robert Stroud, international vice president of ISACA and vice president of IT service management and governance for the service management business unit at CA Inc. "What companies can and should do is educate employees about the risks of online shopping and remind them of their company's security policy. This is especially important this year, when the convenience of shopping

online may be very appealing to employees whose workloads have doubled or tripled because of downsizing."

#### **Upwardly Mobile Shopping**

This survey also found that more than one in 10 Americans who use a mobile work device such as a BlackBerry or iPhone plan to use it for holiday shopping. The increasing use of mobile work devices for personal business such as shopping can lead to additional security issues and exposure to data loss for a company.

"The lines between work and personal data are becoming more and more blurred as a growing number of people check work e-mail from their own phone or PDA, or use a work-supplied mobile device to shop or update their Facebook page. As our mobility increases, so does the risk to our corporate IT systems," said John Pironti, a member of ISACA's Certification Task Force and chief information risk strategist for Archer Technologies.

A significant percentage of those surveyed do not actively manage their work computer's security. Thirty percent report that they leave security up to their company's IT department. Of those who connect via a wireless connection, 30% don't or don't know how to check the security of wireless settings and just 21% personally check their work computer for the most recent security patches.

#### **Reality Gap Between Employees and the IT Department**

A separate ISACA survey of more than 1,500 IT professionals, who are ISACA members in nine countries, conducted during the same time period shows a major gap between what the IT department believes and what the employees are planning when it comes to online holiday shopping. Close to half (48%) of those in IT believe employees will spend just over one work day, or nine hours, shopping online from a work computer—yet ISACA's consumer survey shows that employees will average closer to two work days, or 14.4 hours.

IT professionals are realistic about the potentially staggering costs of shopping online for the holidays from workplace computers. One in four estimates that their company will lose US \$15,000 or more per employee in productivity during this year's holiday season.

"The reality gap between the IT department's perceptions and the online shopping behaviors of the rest of the company actually represents an important opportunity for IT," said Paul Williams, a member of ISACA's Governance Advisory Council and a past president of the association. "By educating employees and communicating common-sense online policies, IT can better protect one of the most critical assets a company has—its IT systems."

#### **5 Tips for Safe Shopping From the Office Computer**

ISACA recommends that employees and IT departments take the following steps to reduce the risk of spam, viruses and accidental downloading of backdoor "agents" that can hijack corporate data.

For online shoppers:

- 1) Use your desktop PC, not your mobile device, to shop, because your desktop browser is likely to be more secure.
- 2) Protect sensitive information, like credit card numbers, by password-protecting both your mobile device and its memory card.
- 3) Make sure you update your anti-virus and anti-malware programs continually.
- 4) Treat social networking sites with the same caution as other web sites—social sites are a growing target for fraudsters and virus writers.
- 5) Be cautious of special offers. If it looks too good to be true, it probably is. Fake online offers and coupons may lead to harmful sites, so be suspicious.

For the IT department:

- 1) Educate employees. Blocking sites can do more harm than good, causing employees to seek out less secure ways to get around your blockade. Education works better.
- 2) Get employees on board with learning by teaching them how to protect both their work computers and their home computers.

- 3) Reinforce what you teach by having employees sign an acceptable-use policy every year.
- 4) Offer a “safe zone” for holiday shopping—create an online sandbox that can be taken down after the holidays.
- 5) Don’t wait until Cyber Monday to step up security. Think of “Cyber Season” as the time from September to January and be extra-diligent throughout that time.

### About the ISACA Shopping on the Job Survey

The second annual “Shopping on the Job: Online Holiday Shopping and Workplace Internet Safety” survey is based on online polling in September 2009 of 1,210 US consumers and 1,513 IT professionals. The IT portion of the study provides the business/IT department’s perspective, polling members of ISACA in nine countries: the US, Canada, Mexico, the UK, France, Germany, Hong Kong, India and Australia. The study, which was designed to capture insights about online holiday shopping at work and employee compliance with workplace policies governing online shopping, was conducted by M/A/R/C Research and ISACA, respectively. The M/A/R/C study results contain a margin of error of 3.9% at the 95% confidence level.

## ISACA-RI’s 2009-2011 Board

<i>NAME</i>	<i>BOARD POSITION</i>
<b>Pauline G. Lamantia</b>	<b>President</b>
<b>Kevan Riley</b>	<b>Vice President</b>
<b>William C. Soares</b>	<b>Treasurer</b>
<b>Ronald J. Roy</b>	<b>Secretary</b>
<b>Colleen Sullivan</b>	<b>Programs &amp; Education Co-Director</b>
<b>William Nowik</b>	<b>Programs &amp; Education Co-Director</b>
<b>Susan Baumes</b>	<b>Programs &amp; Education Co-Director</b>
<b>Tom Laliberte</b>	<b>Programs &amp; Education Co-Director</b>
<b>Donald Borsay</b>	<b>Marketing &amp; Communications Director</b>
<b>Barbara Norris</b>	<b>Academic Relations Director</b>
<b>Susan Strakosch</b>	<b>Standards, Bylaws, &amp; Research Chair</b>
<b>Deepika Chandarana</b>	<b>Membership Director</b>
<b>Tim Schmutzler</b>	<b>Web Master</b>
<b>Camille R. Rigney</b>	<b>Past President</b>

## FREE CPEs

You can easily earn up to **62 FREE CPEs** each year to satisfy your certification requirements. Consider:

- As an ISACA® member you can earn 3 CPE credits for participating in ISACA’s® e-Symposia in their entirety and completing and passing a short 10 question quiz at the end of the session. A new e-Symposium is available each month. The past 12 events are archived and available for viewing on demand. For more information please visit [www.isaca.org/elearning](http://www.isaca.org/elearning).
- Earn 1 CPE for each of the 6 ISACA® Journals by completing the Journal quizzes.
- Earn 10 CPE by volunteering to serve your chapter. Send an email to [president@isaca-ri.org](mailto:president@isaca-ri.org).
- As of December 1, 2009 you can earn up to 10 CPEs for mentoring efforts related to coaching, reviewing, or assisting an individual with CISA, CISM, or CGEIT exam preparation.
- Write an article for the ISACA® Journal

For more details – [ISACA.ORG/CPE](http://ISACA.ORG/CPE)