ISACA®
Trust in, and value from, information systems
New York Metro Chapter

Metro Line

Volume 2, Issue 6 October 2010

Message from the President

Felix Ramirez
Chapter President
ISACA® NY Metro Chapter

Thanks to Danielle and others on the chapter's Board of Directors, today we are publishing another delivery of the Chapter Newsletter. It continues to be an honor to communicate with you and inform you of the chapter's activities. I'd like to start by thanking you and the members of our Board for the support and dedication to implementing leading practices in managing the chapter.

Of particular importance in this issue, is revisions made this year to the chapter bylaws. ISACA requires that all chapters review their bylaws on an annual basis to incorporate changes that would allow the chapter to operate in a more effective and efficient manner. The changes to the bylaws have been reviewed and approved by the chapter board and by ISACA and the next step in the process is to have them approved by the membership. Please read the notes from Patricia Martin and the Bylaws Committee who are responsible for these annual revisions.

Despite all the challenges faced by organizations and individuals this year, our membership continues to grow steadily and I would like to welcome all our new and renewing members. The association is a path to continued professional development and networking. Much of the success of the chapter over the past few years has been possible because of the involvement of many members in supporting each individual activity by contributing ideas, time and hard work. We ask you to follow the example of many others and get involved in the life of the chapter to imprint your mark in everything we do.

Education and Certification are two other areas we need to mention as they are two of the channels we follow to deliver services to our members. Luckily for all of us, we have been able to continue to offer courses at very competitive prices and have managed to keep the quality of the classes at the highest possible level. Our certification review classes continue to produce higher passing rates than other chapters and all commercial vendors. These results speak very highly of the quality of the instructors and the volunteers who put the programs together.

I believe I am achieving the goals I had set initially when I was installed as the President of the Chapter. These goals were in the areas of chapter governance, learning management, certification and academic relations, networking opportunities and sound financial management. I continue to be open to receiving new ideas and putting them into practice for the benefit of all members. ■

Calendar of Events

How to Audit SAP Security
October 25 - 26, 2010; 9AM – 5PM;
Instructor – Harvey Berger
$500 members; $700 non-members
Location – Protiviti 1290 Avenue of the Americas, NY, NY

Introduction to Web Application Security
November 3, 2010; 9AM – 5PM;
Instructor – Tom Brennan - OWASP
$300 members; $500 non-members
Location – Protiviti 1290 Avenue of the Americas, NY, NY

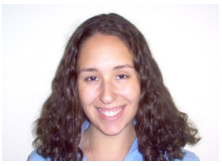
CISA® Exam Review Seminar
November 13, 20, 27 & December 4, 2010; 9AM – 5PM;
Instructor – Jay Ranade
$700 members; $900 non-members
Location – St. John's University, 101 Murray St., NY, NY

To register for the events above visit www.isacany.net

Inside This Issue

Membership Spotlight

Featured Chapter Member



Marguerite McCarthy

Danielle Henry
Metro Line Staff Writer
ISACA® New York Metro Chapter

The Metro Line spoke with Marguerite McCarthy, a professional in the IT audit field. Read below to find out more about Marguerite McCarthy.

MetroLine: Describe your career path.

Marguerite McCarthy: I started in administration at Ernst & Young and had the good fortune to work on several cutting edge technology implementations. Hooked on technology, I joined the Management Consulting Group to gain exposure to different industries and emerging technologies. Many of my consulting assignments were on special audit engagements for financial services clients. When the audit team needed IT yesterday, I knew the best software to use, where to find the fastest computers, and could guide a non-technical team through rapid data extraction and analysis.

Given an opportunity to join Bear Stearns' internal audit department, I jumped on it. My communication skills and ability to quickly learn new businesses and technology were perfect for pre-implementation reviews. Mentoring from my Director contributed greatly to my development as an IT auditor, and I quickly took charge of the application audit group and eventually attained the rank of Managing Director.

After many years of commuting to New York City, I wanted to develop roots in my home community so I switched careers and became a real estate broker. Over time, I added on appraising, construction inspections, and home renovation. I finally realized I was adding different work activities to fight boredom. I missed the thrill of a good pre-imp audit and collaborating with a team to make a positive impact.

I returned to IT audit in Citi's Audit & Risk Review department on the Project Risk Review team for Capital Markets. This experience enhanced my audit skills because of the focus on risk-based planning, SOX IT, risk-control self-assessment, continuous monitoring with quarterly reporting, and automated workpapers.

Shortly after leaving Citi, I took a family leave. Now I can return to full-time work and I'm looking forward to resuming my IT audit career.

ML: What changes or trends have you seen in the IT audit profession?

MM: The increasing velocity of change – regulations, standards, guidance, frameworks – the IT auditor needs to be in constant learning mode to keep up with rapid change in industry and technology. Also, a continuing trend is the constant evolution of IT security risks that accompanies changes and developments in technology.

Marguerite McCarthy

ML: What do you feel are the in-demand skill sets for an individual in the information systems audit and control industry?

MM: In my current job search, skill requirements I see most frequently include communications, relationship building, risk/controls assessment, compliance testing, project management, ACL. Qualifications typically include knowledge of industry, IT security, COBIT and other frameworks. CISA and other certifications are often required.

ML: How did you get involved with ISACA?

MM: I joined ISACA when I became interested in CISA certification. The *ISACA Journal*, and ISACA and ISACA NY websites are great knowledge resources, and the audit programs, white papers, COBIT and other frameworks are invaluable audit tools. Recently, I realized it is time to give back and I volunteered to work with the NY Metro Chapter's Education Committee.

continued on page 3

Membership Spotlight

Featured Chapter Member

continued from page 2

ML: Do you hold any certifications? What are the benefits of holding each?

MM: My certifications include CISA, CIDA (certified investments and derivatives auditor), and CAPM (PMI's certified associate in project management). I passed the CISM exam and am currently preparing for the LEED Green Associate exam. I see CISA as an important indicator of basic IT audit competency. My other certifications are in knowledge areas that are important to my IT audit practice. Aside from the credential value of a certification, preparing for an exam helps me identify and close knowledge gaps.

ML: What are some of your hobbies and interests?

MM: I enjoy a wide range of activities – gardening, cooking new recipes, rock concerts, sports (playing and watching) – and most of all sharing these activities with family and friends. My very expensive hobby is home renovation and this sparked my current interest in energy efficiency and sustainability. I recently completed a 12-week CleanTech QuickStart program designed to introduce experienced professionals to clean technology businesses and advanced energy concepts and I am continuing to study corporate sustainability, green data centers, and energy trading. ■

METRO LINE **FEATURES A CHAPTER MEMBER IN EACH EDITION! NOMINATE A CHAPTER MEMBER BY EMAILING METROLINE@ISACANY.ORG**

SUMMER DINNER CRUISE
ISACA® NEW YORK METROPOLITAN CHAPTER

On September 1st, we held a summer dinner cruise. About 25 chapter members set sail for an evening boat ride around Manhattan. The event was held on the Paddle Wheel Queen – a three-decker paddle boat which also featured an open bar and DJ. On top of that, the buffet dinner of Chicken Francese, Stuffed Shells, Eggplant Rollatini, and Vegetable Lasagna was sure to please any hungry seafarer (or IT auditor too). The tour was about three hours and there was networking and catching up among those who attended. A great way to kick off the end of summer, ISACA®-style!

Above Right: A photo of the Paddle Wheel Queen.

Above Left: James Ambrosini, Rochelle Brenner, Jose Ortiz, and Alexander Josephite.

Technical Corner

Data Breaches, Compliance and the New Frontier for Data Protection

Ulf Mattsson

Ulf Mattsson
CTO
Protegrity

Summary

Data security in today's business world is a classic Catch-22. We need to protect both data and the business processes that rely on that data, but in order to do so we need to move from a reactive, fear (or compliance) driven mode to a proactive data security plan. Meeting Payment Card Industry Data Security Standard (PCI DSS) compliance is important, but it is equally as important to understand that compliance does not equal security, as PCI DSS was intended to be the floor, not the ceiling. This article will discuss a newer method for protecting the entire data flow across systems in an enterprise while minimizing the need for cryptographic services.

Data Breaches

The Verizon Business RISK team, in cooperation with the United States Secret Service (USSS), has been conducting an annual Data Breach Investigations Report. [1] The purpose of the report is to study the common elements and characteristics that can be found in data breaches. In six years, the Verizon Business RISK team and USSS combined dataset now spans 900+ breaches and over 900 million compromised records.

As in previous years, the 2010 Report showed that nearly all data was breached from servers and online applications, with 98% of all data breaches coming from servers originating from hacking and malware. Financial Services, Hospitality, and Retail still comprised the "Big Three" industries, which were affected by 33%, 23%, and 15%, respectively. Targeting of financial organizations is hardly shocking, as financial records represent the nearest approximation to actual cash for the criminal. An astounding 94% of all compromised records in 2009 were attributed to Financial Services.

Financial firms hold large volumes of sensitive consumer data for long periods of time, and because of this, fall under more stringent regulation and reporting requirements. However, 79% of financial firms whose data had been breached had failed to meet PCI DSS compliance, the minimum security measure. Thus, organizations have been searching for a solution that protects the business from endpoint to endpoint, while easily meeting compliance.

Encryption vs. Tokenization

End-to-end encryption can encrypt sensitive data fields throughout most of its lifecycle, from capture to disposal, providing the strongest protection of individual data fields. Therefore, end-to-end encryption, and its next of kin - tokenization - are very practical approaches to protect data between specific parts of a solution that are in high risk areas. While there is no silver bullet to the data security and compliance woes of large enterprise organizations, all eyes are on tokenization right now.

Tokenization is different from encryption in that it is based on randomness, not on a mathematical formula. Encryption also requires compliance with key management, key rotation, selection of algorithm, etc. that are moot with tokens. Next generation tokenization offers a faster, more secure solution and uses less computing power than encryption. Also according to PCI DSS, encrypted data must be re-encrypted every year, while tokenized data can be left for a life time.

Currently there are two forms of tokenization available – first generation tokenization and next generation tokenization. First generation tokenization solutions are based on the simple concept of a large and dynamic table of token/credit card pairs. While this is an obvious and reasonable approach, it has its disadvantages and issues with respect to performance, scalability, and availability. The core obstacle with the traditional tokenization approach is that the token lookup table is so large and dynamic that it's hard to manage. Next generation tokenization, on the other hand, addresses all of these issues through scalability with multiple, parallel instances, dramatically increased performance, availability, centralized or distributed deployment, elimination of token collisions, and support of PCI, PHI and PII data.

When next generation tokenization is applied strategically to enterprise applications, confidential data management and PCI audit costs are reduced and the risk of a security breach is minimized. Security is immediately strengthened by the decrease of

[1] http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

continued on page 5

Technical Corner

Data Breaches, Compliance and the New Frontier for Data Protection *continued from page 4*

potential targets for would-be attackers, because authentic primary account numbers (PAN) is only required at authorization and settlement. Studies have shown annual audits average $225K per year for larger payment card acceptors, and next generation tokenization reduces audit costs dramatically by eliminating the need for encryption keys.

Given financial Institutions' need for high availability, high performance, scalability and quick response times with regards to data security, tokenization is a perfect solution for this sector. These companies need to protect data inside their firewalls and not just on the wire transport of data. Tokenizing sensitive data including PAN and social security numbers is a cost effective end-to-end solution that meets PCI compliance.

Unfortunately, the PCI Security Standards Council (SSC) has not yet developed standards for tokenization, nor will they include tokenization in PCI DSS 2.0. In attempt to fill this void, Visa published its "Best Practices for Tokenization" Version 1.0 on July 14[2]. However, this draft implies a "one-size-fits-all" architectural solution open enough for botched implementations, including encryption pretending to be tokenization and home-grown tokenization that lack security requirements, where random-based tokenization is the only true end-to-end solution.

Conclusion

With attacks coming in many different forms and from many different channels, consumers, merchants, and financial institutions must gain a better understanding of how criminals operate. Only then will they have a better chance of mitigating the risks and recognizing attacks before serious damage is done. Understanding the nature of both data theft and available protection options can help organizations of all types better anticipate where criminals may exploit the system, so they can put appropriate preventive measures in place.

A holistic solution for data security should be based on centralized data security management that protects sensitive information throughout the entire flow of data across the enterprise, from acquisition to deletion. While technologies such as tokenization and encryption cannot assure 100% security, they are proven to dramatically reduce the risk of credit card data loss and identity theft. Next generation tokenization, in particular, has the potential to help businesses protect sensitive data in a much more efficient and scalable manner, allowing them to lower the costs associated with compliance in ways never before imagined. ■

[2] http://usa.visa.com/download/merchants/tokenization_best_practices.pd

About Protegrity
Headquartered in Stamford, Connecticut, Protegrity delivers centralized data security management solutions that protect sensitive information from acquisition to deletion across the enterprise. Protegrity customers maintain complete protection over their data and business by employing software and solutions specifically designed to secure data, manage the data via a centralized policy, and generate detailed security reports.
Protegrity develops solutions that protect data. Protegrity employees are security technology specialists with deep expertise in data security techniques, encryption key management, and security policy in distributed environments. Maximize security with minimal business impact with the Protegrity Data Protection System, a high performance, transparent solution optimized for the dynamic enterprise. To learn more, visit **www.protegrity.com** or call 203.326.7200.

Chapter News

Chapter Bylaws Update

Patricia Martin
Board of Directors
ISACA® New York Metro Chapter

As required by the current Bylaws, the Chapter Board and the ISACA Association recently approved this year's Bylaws revisions, which will build on the success of the Bylaws improvements implemented last year.

In late 2009, we implemented a major upgrade to our Bylaws to provide effective governance and improve control, clarity, and consistency. Chapter Board Directors and Officers are now required to meet more stringent qualifications. Provisions for order of succession were also enhanced to ensure a smooth transition in the event of a vacancy in a Chapter Officer position. Chapter Committees were provided greater flexibility to leverage talent and focus resources to best serve the needs of the membership. The Nominating Committee process was refined to improve transparency and ensure that there was compliance with the qualification requirements of the Bylaws. There were also many other changes that improved the operations of the Chapter.

We are now asking for your support to approve this year's Bylaws revisions.

> By Thursday, October 7, 2010, an email notification of the upcoming Bylaws vote will be sent to the membership, and the proposed Bylaws and voting timeline will be posted on the Chapter website.
>
> **The voting period will be Monday, October 18, 2010 to Friday, November 12, 2010, and it is during this time that we ask for your active participation in voting for the Bylaws.**

The Chapter Board encourages you to visit the Chapter website and review the new Bylaws in their entirety.

The major substantive Bylaws revisions are as follows:

- **Composition of the Chapter Board**

  The number of Chapter Board members will remain the same at twenty-one (21). However, the composition is proposed to be changed to create additional opportunities for members to serve on the Chapter Board, introducing new talent and diversity of skills and opinions. Please see below:

  Six (6) Officers - No change.
  One (1) Immediate Past President - Previously there were three (3) Past Presidents.
  Fourteen (14) Directors - Previously there were twelve (12) Directors.

- **Finance Committee**

  A Finance Committee is proposed as a standing committee to prepare and submit a consolidated budget, provide financial reporting of actual results on a periodic basis, assist in the preparation and submission of required financial statement, tax, and audit information, and enhance segregation of duties and provide important checks and balances across the financial function.

We are committed to serving the membership of the ISACA New York Metropolitan Chapter in the best possible way and we thank you for your active participation in building on the continued success of our Chapter. ■

Chapter News

Get to Know Your Board Member

Julianne Wu

Metro Line recently interviewed Julianne Wu, an ISACA® New York Metro Chapter Board Director. Julianne is currently in the IT Audit Department at Morgan Stanley. Read below to find out more about Julianne Wu.

MetroLine: Which college or university did you attend? What did you study while there?

Julianne Wu: I attended Kean University where I was awarded a Bachelor's degree in Computer Science. I continued on to obtain a Masters in Computer Science from NJIT.

ML: Describe your career path. How did you get into the field you are in now?

JW: In my last year of college I interned with NBC in Manhattan and was retained as a full-time employee in the Olympic Division IT Department there after graduation. I worked in IT for a number of years in the general IT field in New York/New Jersey. After my years in IT, I chose to switch gears to the IT audit profession. My first job in IT audit was at a mid-sized consulting firm in Washington D.C. I moved back to New Jersey and joined the Bank of New York's Application Audit team. After that, I worked at AXA Equitable, also in IT audit. I now work for Morgan Stanley performing IT audits in relation to applications.

ML: What is a typical day on the job like for you?

JW: A typical day on the job for me is fast-paced, challenging in a positive way, and a learning experience. I am busy every minute of the day with my work. I walk away from every day knowing that learned something new and feeling accomplished. My days are very professional in nature, as the team I work with is very professional.

ML: What changes or trends have you seen in your profession?

JW: In the context of application audits, we are seeing more and more integration of IT into the business processes of an organization. IT testing is more and more tied back to business risks to make sure that controls are in place for risk mitigation. Technology is constantly evolving and with the introduction of web-based infrastructure and cloud computing, IT audit professionals need to educate themselves in these areas.

ML: How did you get involved with ISACA?

JW: I got involved with the ISACA NY Metropolitan Chapter by attending membership meetings and helping with training courses run by the chapter. Pat Grant, a past Chapter President, encouraged me to run for a position on the Board of Directors, which was a great piece of advice. As a board member I work on the Education Committee to help plan and execute the chapter's training and professional development initiatives.

ML: What do you feel are the in-demand skill sets for an individual in the Information Systems audit industry?

JW: It is important for individuals in IT audit to understand the business when performing integrated audits. It takes extra time and attention to get to know the business and how computer systems support that business. It is important to know the key functions and controls so that missing controls may be noted and communicated to management.

ML: What type of training has been most impactful throughout your career?

JW: On the job training has been the most useful for me throughout my career. On the job experiences force you to research, read, and seek further training so that you can apply the knowledge necessary to get the job done.

ML: Do you hold any certifications? What are the benefits of holding each?

JW: I hold the CISA certification. It helped me to transition between the IT Department and the IT audit field. I was able to obtain a working knowledge of the concepts related to IT audit, so that I could begin working in the field. I hope to pursue more certifications in the future.

ML: What are some of your hobbies outside the office?

JW: I like to ski and play badminton. Overall, I love being outdoors when I am not at the office. I volunteered at the Barclay's PGA Tournament in Jersey City last year, it was such an awesome experience and I can't wait to participate again next year! ■

Chapter News

Academic Relations and Research Update

Alexander Josephite
Second Vice President and Membership Committee Chairman
ISACA® New York Metro Chapter

Academic Relations

One of the Chapter's goals is to educate people about sound technology assurance, governance, and security practices. Especially important to the chapter is teaching these topics to future generations as students are increasingly exposed to technology at an early age.

Recognizing the need that educators are not always practitioners, ISACA has developed a model Curriculum based on COBIT. This year, ISACA will be utilizing the talent and expertise of Dr. Vincent Orrico to assist in revising and reviewing ISACA's Model Curriculum and specific curriculum used by professors in our area.

Each semester volunteers from our Academic Relations Committee, led by Raisa Serebrenik, meet with students to introduce them to ISACA, and the opportunities available as technology professionals. Our Chapter is teaming up with the New York Chapter of the Institute of Internal Auditors to spread our message to more Colleges and Universities. If you would like to volunteer to speak with students at a campus near you please email ***Raisa.Serebrenik@isacany.org***.

Research Update

Were you recently assigned to implement or review a new piece of technology at your company? What did you do? Are you are an assurance professional that just reviewed a cloud computing implementation or special audit for data leakage?

We're asking you to come forward and share your experiences with us. We would love to learn about your recent experiences, any potential issues and how they were avoided.

Please remember to cleanse proprietary information from any files you send to us.

In the mean time please visit **www.isaca.org** for the latest research/ audit programs on Information Security Management, Windows Active Directory, Crisis Management Audit, Cloud Computing Management, and Data Leak Prevention. Also keep an eye open for COBIT 5 in 2011. ■

PRESENTING…

THE ISACA® NEW YORK METROPOLITAN CHAPTER MENTORING PROGRAM

The Chapter is looking for participants who want to become mentors as well as candidates who want to be mentored. The one-on-one format of the Chapter Mentoring Program provides mentors and mentees the opportunity to spend individualized time-sharing ideas, challenges, and perspectives on specific areas of interest. If you would like to participate, please review the Roles and Responsibilities of Mentors and Mentees at **www.isacany.net** and submit your application to **membership@isacany.org** today!

Get Published in *Metro Line*!!

SHARE YOUR EXPERIENCES AND TECHNICAL KNOWLEDGE WITH OTHER ISACA® MEMBERS AND SUPPORT THE ONGOING DEVELOPMENT OF THE INFORMATION SYSTEMS FIELD. *METRO LINE* IS LOOKING FOR BOTH ONE-TIME ARTICLE SUBMISSIONS AND ONGOING VOLUNTEER REPORTERS. PUBLICATION IN *METRO LINE* PROVIDES NOT ONLY AN INCREASED EXPOSURE FOR YOUR COMPANY, BUT ALSO THE PROFESSIONAL RECOGNITION OF PEERS AND COLLEAGUES.

PLEASE SEND ALL SUBMISSIONS TO METROLINE@ISACANY.ORG

Education Update

Chapter Education Update

James Ambrosini
First Vice President and Education Committee Chairman
ISACA® New York Metro Chapter

We've organized our Fall education series to meet the demands of our profession and respond to your suggestions. We started off with a class on auditing UNIX because we found that an increasing number of companies are using this over Windows-based O/S. Coming up, we have a class on SAP segregation of duties lined-up for Oct 25/26th and a class on Windows Application Security, taught on November 3rd. Both of these are taught by industry-leaders in their respective domain, and are starting to fill up, so please register on our website: **www.isacany.net**.

We needed to postpone a class on ITIL until next semester. I would strongly encourage everyone to take this course. If you're not familiar with ITIL (Information Technology Infrastructure Library), it's the de facto standard for world-class IT processes. By taking this course, you will have a firm grasp of what it means to have sound processes within Service Support and Service Delivery – so you can 'talk the talk' with IT executives and get beyond just simply discussing controls. Two other benefits of this class are that it will prepare you for the new ITIL V3 certification exam and it's being taught by Jay Ranade of Technodyne – who's one of our most popular instructors, for good reason.

On a separate note – over the next few months, I'm going to be transitioning away from the role of Education Committee Chairman in order to assist our President with various strategic chapter initiatives. Membership Committee Chairman, Alex Josephite, will be taking the reins in December and I will continue to serve as an advisor to that committee.

I've always felt that our education offering is one of the best values around and was happy to serve our chapter in this capacity. Look for the Spring education schedule in December/January time-frame and don't forget to check out the SAP and Web security class this Fall. ■

ISACA® MAKES IT EASY FOR YOU TO EARN THE CPES YOU NEED TO MAINTAIN YOUR CERTIFICATIONS

ISACA® MEMBERS CAN EARN OVER 60 FREE CPES PER YEAR! HERE'S HOW:

- ✓ ISACA® Journal Quizzes – Earn 1 CPE credit for each of six journals per year (6 FREE CPEs per year)
- ✓ Monthly e-Symposia Quizzes – Earn 3 CPE credits for each of 12 e-Symposia per year (36 FREE CPEs per year)
- ✓ Local Chapter Volunteer Activities – Gain 1 CPE credit (up to 10 per year) for each hour of active participation in "Qualifying Educational Activities" as defined per ISACA® certification. Activities include participation as a chapter officer or member of an ISACA® or ITGI® board, committee, or task force. (10 FREE CPEs per year)
- ✓ Mentoring Efforts – Earn 1 CPE credit for each hour of mentoring directly related to coaching, reviewing or assisting an individual with CISA®/CISM®/CGEIT® exam preparation, or providing career guidance through the credentialing process. (10 FREE CPEs per year)

Total Possible Free CPEs for ISACA® Members: 62 FREE CPEs PER YEAR!!

Certification Update

ISACA® Certification Update

Kwongmei (May) To
Board of Directors, Certification Coordinator
ISACA® NY Metro Chapter

The fall season is here, which means it is time again to focus on how you can develop your career. I encourage you to take our signature CISA® Exam Review Seminar in preparation for the December 11, 2010 CISA® examination. This course is meant to help you pass the CISA® examination leading to a certification award. Act now and register for this wonderful course and be on your way to achieve your career aspirations.

CISA® Exam Review Seminar

Date: November 13 / 20 / 27 and December 4, 2010 (4 consecutive Saturdays)
Time: 9:00 AM - 5:00 PM
Location: St. John's University - Manhattan Campus, 101 Murray St., New York, NY 10007
Cost: Members: $700; Non-Members: $900
CPE: 28
Instructor: Jay Ranade
Registration End Date: November 8, 2010
Cancellation Date: November 8, 2010

Certification Deadline Reminder

Annual Revocations – Individuals whose Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) certifications were revoked are nearing the 60-day deadline for appeal. If your certifications have been revoked please contact the certification department at ***certification@isaca.org*** for assistance.

CRISC Grandfathering Deadline – Sunday October 31, 2010 ***www.isaca.org/criscgrandfathering***
The Certified in Risk and Information Systems Control™ certification (CRISC™, pronounced "see-risk") is designed for IT professionals who have hands-on experience with risk identification, assessment, and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance.

CRISC Certified in Risk and Information Systems Control
An ISACA® Certification

The CRISC designation will not only certify professionals who have knowledge and experience identifying and evaluating entity-specific risk, but also aid them in helping enterprises accomplish business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls. ■

Certification Update

Interview with Jay Ranade

Featured Certification Review Instructor

Kwongmei (May) To
Board of Directors, Certification Coordinator
ISACA® NY Metro Chapter

Kwongmei (May) To: How many years have you been involved with ISACA® as an instructor?

Jay Ranade: I have been teaching CISA® review classes for the ISACA® NY Metro chapter and other chapters in the USA since 2006. Felix Ramirez, who at that time was the CISA®/CISM® Coordinator for the NY Metro chapter, asked me to teach. Little did I realize that it would become an instantaneous success.

KT: What is the greatest achievement you have gained as the ISACA® NY chapter certification exam review class instructor?

JR: More than an achievement, it was a moment of pride for the NY Metro chapter that one of the students would drive 470 miles round trip every Saturday to attend our CISA® class last year. He is from Washington, DC.

KT: Do you hold any certifications? What are the benefits of holding each?

JR: I hold many certifications, but the most prominent ones are CISA®, CISM®, CISSP, ISSAP, and CBCP. For a control professional, these are the ideal certifications. ISACA®'s new certification CRISC® will be another prominent one.

KT: What are some of your hobbies outside the office?

JR: I am an active sports person and practice martial arts in my spare time. I am a 4 time world champion in arm wrestling and 2 time world champion in martial arts breaking (2002 and 2003). But it is just a hobby.

KT: What do you feel are the in-demand skill sets for an individual in the Information Systems audit industry?

JR: At any point in time, one is only two years away from obsolescence in our field. I plan to give a webinar on the topic of the 10 most wanted skills for a control professional that will be in demand over the next year. Stay tuned……

KT: In your opinion, how important is it for an individual to become a CRISC® certified?

JR: It is extremely important, but I wish certification bodies provide grandfathering-based certification for a 3 year only period, at which point a candidate has to pass the written exam to keep the certification.

KT: Describe your career path. How did you get into the field you are in now?

JR: I guess I believe that most of the career paths are opportunities that knock at the door and you just avail of them. From being an author of 37 books on IT with 7 million copies in print, it was easy for me to switch my career many times, and I did.

KT: In your opinion, what are the critical success factors of an Information Systems audit department?

JR: Understand business processes, use a risk based approach for audit planning, and help your staff grow by sending them to new educational

Editorials

The New Face of the Risk Manager

James Ambrosini
First Vice President
ISACA® New York Metro Chapter

When I was in graduate school in the mid-90's, during the proliferation of technology, one of my professors stated that since IT is changing the world, everyone needs to be an Information Manger. I didn't think much of it at the time, but what I've come to realize over the years is that he was absolutely right. Whether we realize it or not – how we learn to handle the vast amount of data we send and receive each day, has made us more adept and effective. We've become the quintessential 'Information Manager' – even though we use various tools and gadgets to help us.

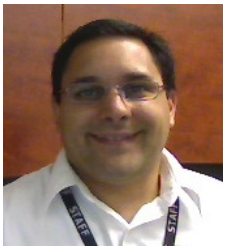
In the wake of the current business climate, and recent events over the last two years – I feel the exact same way about Risk: We all need to be Risk Managers. And I truly mean that in the literal sense of managing risk; not just pointing out where it is or trying to eliminate it. Risk is a pervasive force in business and growth cannot occur without it. We need to help our companies manage risk by tying it to strategic objectives and understanding (or perhaps even changing) the organization's risk tolerance. It's only when risk is taken into context with the strategic goals of a company that the company can fully appreciate the implications to their business.

During some research for an Enterprise Risk Management class I'm teaching at NYU this Fall – I learned that in as early as 2007, numerous economic reports pointed to a pending collapse in the housing market. These were presumably accessible to, if not actually read by, the banks who were making large profits off of the sub-prime lending in that sector. The ones who realized that this directly impacted their short and long-term strategy and who had the underlying risk tolerance level to change their course are better off today.

Often times I've felt that some of the day-to-day issues we uncover as IT audit and security professionals are not really resonating with companies. Perhaps, some of the reason is that many audits these days have been reduced to very specific, tactical and operational assessments (e.g. an operating system security review). That's fine. Every company needs those too. But we have an obligation to understand the bigger picture. We need to be the lamp bearer in the sea of risk our companies face. This requires a different mentality as much as it does a different focus. This may include auditing corporate strategy, spearheading or getting involved in a Corporate Risk Committee, or simply having periodic discussions with your Chief Risk Officer (if your company has one). Whatever the answer is, we owe it to ourselves, our companies, and our profession to bear this burden – even if it's uncomfortable or brings us to areas outside our domain of expertise. But in order to do this, we need to prepare ourselves by learning new skills; soft skills, business skills, new technologies etc. The landscape of business, and certainly how it relates to risk, is ever evolving – so we must evolve with it.

There is an old saying that goes, "Change is growth". If we can change how our companies deal with and understand strategic and enterprise risks, in all its forms, I think everyone would benefit. ■

The Value of IT Controls



Frank E. Roppelt, CISA
Director – IT Operations
ICON Central Laboratories

The need for IT auditors and IT Risk managers is on the rise. One of the top concerns of COO and CEO's today is the Risk of IT systems and the lack of controls within the IT environment. Whether your company is a highly regulated firm in markets such as Finance or Healthcare; or is a non-regulated firm, having IT Controls is key to running IT systems smoothly.

I have been an IT Professional for over 13 years in various management roles in Help Desk, Data Center, and Network Operations. Early in my career, I was somewhat ashamed to say that I thought controls were nothing more than paper trails and a waste of time. However, over the years, I have found that a lack of controls in an IT environment leads to issues with data integrity, system availability, unhappy users and ultimately a poor running IT environment. As businesses come to rely more on IT and the systems it supports, the needs for controls become much more important. The business these days is fed up with

continued on page 13

Editorials

The Value of IT Controls

continued from page 12

hearing that a system is down or not responding correctly because of a mistake made by the IT department. IT is all about control and maintaining stability with IT systems, networks, security, and the other aspects that IT departments are responsible for managing. The days of not having proper controls in your environment are gone and the level of acceptability for system outages is diminishing daily.

Managing IT is about establishing controls, providing value to the business by allowing it to be efficient, and lastly it is about technology. Note that technology is last on the list.

A Note on the CISA Certification Review Class

As an IT Professional, the CISA® (Certified Information Systems Auditor) is a great certification to obtain as it provides you with the knowledge of IT Controls, Risk, Security, Governance and the IS audit process. Having the certification opens your eyes to the number of controls that need to be in place in order to operate an effective IT department. By looking through the IT auditor's eyes, it is easy to see what controls are missing and what the risks are to the business due to the lack of controls. Obtaining the CISA® is no easy task and requires many hours of studying various materials in order to prepare for the test. Having recently passed my CISA® after over 200 hours of studying, the most effective training material that I leveraged was the CISA® Exam Prep Class provided by ISACA® and taught by Jay Ranade. This class not only provided me with the additional knowledge I needed to pass the test, it also provided me with concepts that can be used in the real world.

Taking the CISA® Exam Prep Class provides a deep dive into the six domains of the CISA® and provides you the extra boost to pass the test. I was astonished by what I learned in the CISA® Exam Prep Class. It helped me further understand the material provided in the CISA® Review Manual and also provided me with a level of confidence to pass the CISA®. Prior to taking the CISA® Exam Prep Class my pass rate was under 50% on the CISA® Exam Simulation CD. After completing the CISA® Exam Prep Class, my scores were well over 80%. I attribute the passing grade directly to the CISA® Exam Prep Class. I also feel that the CISA® Exam Prep Class works great for networking as well. I strongly suggest that the CISA® Exam Prep Class be part of your study aids for passing the CISA® December 2010 Exam. Good Luck! ■

2010 Joseph J. Wasserman Award Recipient

For the past thirty three years the Board of the New York Metropolitan Chapter of ISACA® has identified a person, each year, to receive this Award for their "Outstanding Achievement and Contribution to the Field of Information Systems Audit and Control". This was the first and is the most prestigious award created in our profession and it honors Joseph Wasserman who was one of the very early pioneers. He created one of the first audit software packages, which he called the Computer Audit Retrieval System. In recent years, the Board has extended the eligibility for this award to recognize those who have also contributed to the Information Security field.

In that context, the Board was pleased to announce Robert Clyde as the 2010 Recipient. Since the beginning of his career, Robert has been deeply involved in the development of software, which, while primarily designed to assist the Information Security function, is very useful to the IT auditor. He has always maintained a very close relationship with ISACA® by making many presentations at many conferences and Chapter meetings. His contributions have significantly helped to bring the Information Security and Audit professions closer together and he continues in the role today.

ISACA® News

New Online COBIT® Training

ISACA® has enhanced and restructured its online COBIT® training to meet the needs of ISACA®'s global membership. This web-based, self-paced course is designed to give foundation-level instruction on the COBIT® 4.1 framework and prepare you for the COBIT® exam.

The course is divided into five sections, or modules, each designed to educate you on the need for, and benefits of, an enterprise governance of IT framework. In module one, you will become familiar with the principles of governance of IT and be able to recognize the IT management issues that commonly affect enterprises. In module two, you will begin to identify COBIT® components and understand how COBIT® satisfies the requirements for a control framework. In module three, you will learn about the COBIT® IT processes and control objectives and the *IT Assurance Guide*. Module four explains how to apply the COBIT® framework in a practical situation by explaining the use of management guidelines, control objectives and control practices for key processes. Module five covers several different COBIT® resources that are available to users, including COBIT Online® and COBIT® Quickstart.

The new and improved Online COBIT® Foundation Course, complete with an updated case study, interactive activities and a practice test, is now available on the ISACA® e-Learning Campus. Visit the E-learning page of the ISACA® web site to register for the course; e-mail ***elearning@isaca.org*** for more information. ■

NOTE: THIS ARTICLE WAS FEATURED IN THE SEPTEMBER 29TH, 2010 EDITION OF @ISACA. FOR MORE ARTICLES FEATURED IN @ISACA VISIT **WWW.ISACA.ORG** TODAY!

International President: Going beyond "normal"

Computer and information systems managers earned an average salary of US $113,720 in 2009, a 44 percent gain (the third highest in the list) since 2000, according to a recent article in *Bloomberg Businessweek* (13 September 2010). Close behind, at number seven, accountants and auditors earned US $60,340, an increase of 39 percent during the same timeframe.

While this article brings some good news, those of us who work in these professions day-to-day know that salary ranges vary widely around the world—and from industry to industry—and that we and our colleagues have also felt the jarring effects of the global financial crunch.

While economic indicators point toward some semblance of a recovery, the overarching message seems to be that this is our "new normal." But my question is—as always—what is "normal?"

As a security executive, I am constantly challenged to be prepared for the unknown, the unexpected and sometimes even the unfathomable. The fact is, in our field, and in many others, there is no such thing as normal. There are incidents that reoccur, there are threats that are continually hovering above our heads and inside and outside of our perimeters, and there are precautions that we need to continually reassess and implement.

This is exactly why I frequently talk about the benefits of ISACA membership. Our association is a leader in delivering guidance and education to keep us abreast of, and often ahead of, the quickly changing business environment. Rather than focus on what is normal, ISACA helps its members and those who hold its certifications be better prepared for the new and ever-changing realities they face. Frankly, I feel that these opportunities for personal and professional growth are what keep our jobs fascinating and our challenges exciting.

Emil D'Angelo, CISA®, CISM®
International President, ISACA®
Senior Vice President, Bank of Tokyo Mitsubishi UFJ, USA

(Note: This news story is from www.isaca.org.)

ISACA® News

Fall Into Reading...New on the ISACA® Shelves

The newest titles include:

- ✓ ***GFI Network Security and PCI Compliance Power Tools***
- ✓ ***Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions***
- ✓ ***Effective Project Management, Traditional, Agile, Extreme, 5th Edition***
- ✓ ***Security, Audit and Control Features, Oracle E-Business Suite 3rd Edition****
- ✓ ***Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition***
- ✓ ***Network Security Bible, 2nd Edition***

(* Published by ISACA)

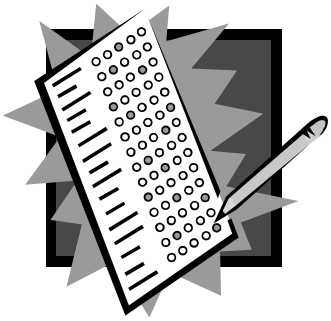
Visit the ISACA Bookstore at WWW.ISACA.ORG/BOOKSTORE or the New Books page, or see the *ISACA Journal* Bookstore insert, for additional information. Contact the Bookstore at bookstore@isaca.org or +1.847.660.5650 with any questions.

(The books above were featured in ExpressLine, a monthly newsletter for the leadership of ISACA®.)

ISACA® QUIZ – TEST YOUR KNOWLEDGE!

1. What does CACS® stand for?
(a) Continuous Audit and Control Structures
(b) Computer Auditing and Control Society
(c) Computer Audit, Control and Security

2. What year did ISACA® start?
(a) 1954
(b) 1969
(c) 1937



3. Which are the 3 largest ISACA® chapters worldwide? (as of April 30, 2010)
(a) Tokyo, Japan; China, Hong Kong; Washington D.C., USA
(b) Seoul, Korea; Tokyo, Japan; Moscow, Russia
(c) New York, USA; China, Hong Kong; Tokyo, Japan

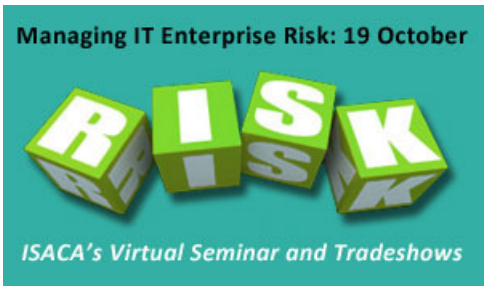
4. In how many languages is ISACA®'s CISA exam given?
(a) 20
(b) 12
(c) 8

5. What is the name of the ISACA® Linkedin Group?
(a) ISACA® Networking
(b) ISACA® Connections
(c) ISACA® Educational Events

See page 16 for answers.

THANK YOU TO ALL THOSE WHO CONTRIBUTE TO *METROLINE*!

YOUR EFFORTS AND SUPPORT ARE GREATLY APPRECIATED!



ISACA® NEW YORK METROPOLITAN CHAPTER NEWSLETTER COMMITTEE

James Ambrosini
Board Newsletter Committee Chairman

Danielle Henry
Editor-In-Chief

Christine Centola
Copy Editor

Madhu Mathew
Copy Editor

CONTACT THE NY METRO CHAPTER

ISACA® NY Metropolitan Chapter

954 Lexington Avenue #525

New York, NY 10021-5013 USA

Phone: 646.881.4696

www.isacany.net

Let us know your thoughts, comments and questions about our Chapter and Chapter activities. Send your messages to membership@isacany.org.

CONTACT ISACA® INTERNATIONAL

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545
Fax: +1.847.253.1443

www.isaca.org

ISACA® QUIZ - ANSWERS

1. (c); 2. (b) 3. (a) 4. (b) 5. (c)

VOLUNTEER OPPORTUNITIES AT THE ISACA® NEW YORK METRO CHAPTER

The chapter is always looking for volunteers to help with chapter activities, from organizing events to working with the different committees.

Email **volunteer@isacany.org** to get involved.

CHAPTER BOARD OF DIRECTORS

2009-2011 Officers

Felix Ramirez
Chapter President
Felix.Ramirez@isacany.org

James Ambrosini
First Vice President
James.Ambrosini@isacany.org

Alexander Josephite
Second Vice President
Alexander.Josephite@isacany.org

Dustin N. Bradley
Treasurer
Dustin.Bradley@isacany.org

James Powers
Corresponding Secretary
James.Powers@isacany.org

Nigel James
Recording Secretary
Nigel.James@isacany.org

2010-2011 Directors

Alexander Abramov
Emma Arakelyan
Kevin Fuller
Patrick Grant*
David Kipin*
Patricia Martin
Robert May*
Nancy Mendez
Andrew T. Robinson
Raisa Serebrenik
Kwongmei (May) To
Chris Westerman
Julianne Wu
Richard Ziegler

* Past President