Message from the President

Felix Ramirez
Chapter President
ISACA® NY Metro Chapter

Dear Friends,

We are truly happy to have each of you as a member of the ISACA® NY Metropolitan Chapter.

Over the past few months, we have been working hard to ensure that the chapter can deliver all the benefits ISACA® has to offer its members. The current market conditions have placed an extra burden on all of us, yet, somehow, every member, Board member and each of our committees has made an extra push to get things done. It’s been challenging but very rewarding.

As we approach the latter part of our Chapter year ending in June 2010, I’d like to remind everyone that in addition to training classes and membership meetings, the NY Metro Chapter also has several important events coming up. These events include the Board elections, the Wasserman Award selection, the Annual General Meeting, academic relations meetings and certification classes. I ask you to get involved in these activities by supporting them, actively volunteering to help, and by contributing your knowledge and expertise.

We are all busy with work, family and other activities; time is a very scarce resource and we need to manage it efficiently. Some of us can contribute more time than others. However, we encourage you to volunteer in any way, no matter how small your time commitment may be. The important thing is that we all contribute something because in that way we are not only helping our chapter, but also our profession, our peers and ourselves. In many instances, this chapter has helped its members with a key connection, a job interview, passing an exam, creating an opportunity or just becoming a better person. Your volunteer activities benefit us all.

I thank you again for being a member and hope to see you at our next function.

---

Calendar of Events

CGEIT® Review Course
APRIL 10 AND 17, 2010; 8AM – 5PM;
INSTRUCTOR – JAY RANADE
$700 MEMBERS; $900 NON-MEMBERS
LOCATION – ST. JOHN’S UNIVERSITY, 101 MURRAY ST., NY, NY

IT Boot Camp for CISA® Exam
APRIL 24, 2010; 8AM – 5PM; INSTRUCTOR – JAY RANADE
$500 MEMBERS; $700 NON-MEMBERS
LOCATION – ST. JOHN’S UNIVERSITY, 101 MURRAY ST., NY, NY

Cloud Computing – Technology, Risks, and Controls
APRIL 26 -27, 2010; INSTRUCTOR – RAM ENGIRA, SVP OF CITIGROUP
$550 MEMBERS; $750 NON-MEMBERS
LOCATION – AXA EQUITABLE LIFE INSURANCE COMPANY, 1290 AVENUE OF THE AMERICAS, NY, NY 10021 (6™ & 52™)

CISA® Review Course
MAY 1 / 8 / 15 / 22, 2010; 8AM – 5PM (4 CONSECUTIVE SATURDAYS); INSTRUCTOR – JAY RANADE
$500 MEMBERS; $700 NON-MEMBERS
LOCATION – ST. JOHN’S UNIVERSITY, 101 MURRAY ST., NY, NY

Auditing Active Directory
MAY 13, 2010 (1 DAY COURSE); INSTRUCTOR – FARID ABDELKADER, MSCE, CISA®
$200 MEMBERS; $300 NON-MEMBERS
LOCATION – TBD (NYC)

To register for the events above visit
WWW.ISACANY.NET
Membership Highlights

Featured Chapter Member

Barry Ko – Senior Manager at a Big 4 Accounting Firm

Jenny Urena
Metro Line Staff Writer
ISACA® New York Metro Chapter

The Metro Line spoke with Barry Ko, a Senior Manager in Enterprise Risk Services at a global accounting firm. Barry specializes in the Banking and Securities industries and has over 12 years of experience in IT external auditing. Read below to find out more about Barry Ko.

Metro Line: Which college or university did you attend? What did you study while there?
Barry Ko: I graduated with a Bachelor of Science in Accounting and a minor in Computer Science from Miami University in Ohio.

ML: Describe your career path. How did you get into IT audit?
BK: After graduating from MU, I received an offer from my current organization to work in Audit and later transfer to the Control Assurance Services practice. I am currently in the Enterprise Risk Services group as a Senior Manager. My area of focus is in the banking and securities industries, where I work with many international banks.

ML: What is a typical day on the job like for you?
BK: I spend 70% of my time in meetings with clients, performing audits, and working to understand the client’s environment. The remaining 30% is spent reviewing work papers and performing administrative activities, such as recruiting, etc.

ML: What changes or trends have you seen in the IT audit profession?
BK: From an external auditor’s perspective, I have seen how the role of an IT auditor has been limited since the implementation of the Sarbanes-Oxley Act. Before SOX, there was more liberty to audit whatever was necessary. Now, external audits are limited to audit controls related to financial reporting only.

ML: What are some of the key IT risk area(s) you’ve seen in your work?
BK: Security is still the number one IT risk area I have seen in my work. In recent years, I have noticed an even greater risk, which is the outsourcing of the IT security function overseas. Companies are taking huge risks by outsourcing security functions outside our borders where legislation and regulations around data protection and privacy are governed by the jurisdiction of other countries.

ML: What do you feel are the in-demand skill sets for an individual in the IT audit industry?
BK: Integrity and ethical values are important skill sets in the IT and external audit industries. Additionally, communication skills are necessary to share findings with your team and management. Technical skills are also in-demand skill sets for an IT auditor.

ML: In your opinion, what are the critical success factors of an IT audit department?
BK: In my opinion, the critical success factor of an IT audit department is to increase awareness of the IT Department function in regard to change management and IT security. Other critical success factors are following up on any issues on hand and reporting any findings.

ML: What type of training has been most impactful throughout your career?
BK: My most impactful training experiences have been security and UNIX trainings taught by former hackers from the hacker’s perspective. The depth of the hacker’s perspective is valuable to IT auditors because it provides insight into security related vulnerabilities.

ML: Do you hold any certifications? What are the benefits of holding each?
BK: Yes, I am a Certified Information Systems Auditor and I am currently working to obtain the CPA certification. The benefit of holding the CISA® is the accessibility to resources such as COBIT® and ISACA® books. Also, as a CISA® you are part of a large group of professionals to network with.

ML: What are some of your hobbies outside the office?
BK: My interest outside of the office is photography. I like to go out and take pictures.
Membership Highlights

Chapter Membership Update

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

Academic Relations

Congratulations to Raisa Serebrenik our new Academic Relations Chair. Raisa will be leading our initiatives to educate students about information technology, ISACA®, and frameworks such as COBIT®. The chapter will be presenting to students at Pace University and St. Francis College within the next month. If you would like to volunteer to speak to students, attend job fairs or design new pamphlets and handouts, please email Raisa.Serebrenik@isacany.org and copy volunteer@isacany.org

Membership

As of March 9th, 2,423 members are realizing the value of their membership to the New York Metropolitan Chapter of ISACA®. According to our records with we have 21 student members, 7 Academic Advocates, 3 Lifetime Members, 3 retired members, 23 members who have passed one of our exams but haven’t joined the chapter and 2,360 active members. If you think this number is inaccurate, please log in to ISACA.org and update your profile. In the next year we will be sending out special targeted emails based on information listed in your member profile. Also follow us on Twitter for event details and updates. Our next membership meeting will be held at Computer Associates in Islandia, Long Island on April 14. Also, save the dates of June 17th for our June Gala / Annual Membership Meeting. Location and details will be forthcoming.

Featured Member Benefits

Academic Research Area

ISACA® dedicates an area of its web site to providing its members with an opportunity to support potentially groundbreaking research. Each research project will also result in the addition of professional content to the site, such as white papers and articles. ISACA® encourages its members and chapters to participate in those projects they find of special interest or pertinence. Please visit www.isaca.org/academicresearch to learn more.

Complimentary Access to ISACA® Publications

Certain ISACA® publications are available at no charge to ISACA® members exclusively. For example, the new The Risk IT Practitioner Guide can be downloaded at www.isaca.org/riskit. Risk IT: Based on COBIT® is a framework based on a set of guiding principles for effective management of IT risk. Find other ISACA-published work at www.isaca.org/deliverables.

The Member Benefits above were featured in ExpressLine, a monthly newsletter for the leadership of ISACA®.
Chapter News

Chapter Bylaws Update

Patricia Martin
Board of Directors
ISACA® New York Metro Chapter

Bylaws are the foundation of effective governance, and in the latter part of 2009, the ISACA® New York Metropolitan Chapter Board undertook an effort to strengthen the Bylaws to improve controls, clarity, and consistency. To incorporate best practice, the Bylaws were benchmarked against the ISACA® model bylaws, the bylaws of many other large chapters in the United States, and several third-party compliance organizations.

The proposed Bylaws revisions were submitted to ISACA® International Headquarters for review and approval by the ISACA® Membership Board in Fall 2009. Members then made their voice heard when they approved the proposed Bylaws, which became effective on December 14, 2009.

Some highlights of the Bylaws changes are:

Chapter Board Members
More stringent qualifications were introduced for Chapter Board Directors and Officers to ensure that the Chapter leadership is comprised of qualified individuals that are fully committed to promoting the education, knowledge, and skills of the membership as well as building on the continued success of the Chapter.

Chapter Board members are required to meet certain standards relating to general fitness to serve. Board members must be dues-paying members, in good standing with both ISACA® and the New York Metropolitan Chapter for a minimum of one year by December 31 prior to the upcoming election and throughout their entire term of office. The requirement for the President, 1st Vice President, 2nd Vice President, and Treasurer is three years; plus, these officers must have served on the Chapter Board as a Chapter Board Director for a minimum of two years. 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
Greater flexibility in establishing Chapter committees and appointing members enables the Chapter Board to leverage talent and focus resources to best serve the needs of the membership.

The Nominating Committee process was improved by specifying a more comprehensive timeframe that begins in November and ends in April prior to the election in May. Nominations can be accepted in writing only from current Chapter members in good standing up to and including February 15 prior to the election.

Candidates must be properly screened and qualified for the Chapter Board positions for which they have been nominated. They are required to consent in writing to be nominated and to serve if elected for the specific position for which they are being put forth, and they must have completed, signed, and submitted a “Willingness to Serve Agreement” and the “Conflict of Interest Form” by March prior to the election. In addition, any candidate for a Chapter Officer position is required to be interviewed by the Nominating Committee.

The Nominating Committee process to conduct its screenings, document its findings, and report the results of the election to the Chapter Board is now more rigorous and comprehensive.

Other Changes
Other changes include provisions in the Bylaws relating to:

- Specific language that reinforces that Chapter Board and Committee members are not paid any compensation for their services, and only legitimate and reasonable expenses related to Chapter Board activities may be reimbursed.
- Conduct of Chapter Board meetings, including the ability to call a special or emergency Board meeting.
- Removal of a Chapter Board member if required.
- More definitive language about the election process.

The Chapter Board encourages you to visit the Chapter website and review the new Bylaws in their entirety. We are committed to serving the membership of the ISACA® New York Metropolitan Chapter in the best possible way, and we welcome your valued suggestions, comments, questions, and most importantly, your active participation in building on the continued success of our Chapter.
Get to Know Your Board Member

Danielle Henry
Metro Line Editor-in-Chief
ISACA® New York Metro Chapter

Metro Line recently interviewed Norman Levine, the ISACA® New York Metro Chapter Treasurer. Norman is currently the IT Compliance Manager at HBO. Read below to find out more about Norman Levine.

Metro Line: Which college or university did you attend? What did you study while there?
Norman Levine: I attended Southern Illinois University and Pace College, where I majored in general business studies.

ML: Describe your career path. How did you get into the field you are in now?
NL: I started in the IT industry in the early 80s working in Boston. I was originally in sales and marketing consulting for IT companies. I worked with Digital Equipment, Texas Instruments, Fujitsu, and Epson when IT was becoming more of a consumer oriented product. My first IT position was in the mid-90s as a consultant working with Reed Elsevier as a consultant hired to build a website for two advertising books. After consulting at Reed Elsevier, I went to work for a dot com for a time as the Director of Distance Learning until about 2000 / 2001. Following the dot com, I worked for KPMG for 3 ½ years in the back office as the go-to-guy for telecommunications and networking for outside offices. After KPMG, I started consulting on my own in IT auditing focusing on the Sarbanes Oxley Act. For 7 months I worked at Fannie Mae in Virginia on the assurance side of auditing. Then I relocated back to New York to do more auditing and consulted at 1-800-Flowers, followed by an accounting firm in Connecticut. Before I landed at HBO, I worked at CIGNA in IT audit. I joined HBO in November 2006 and am currently the IT Compliance Manager.

ML: How did you get involved with ISACA?
NL: While at CIGNA, I was a member of the Hartford, Connecticut chapter of ISACA®. They had a basic website when I joined, so I volunteered to build a new site for them and became part of the Board of Directors there as a result. When I joined HBO I was still on the Board of Directors in Hartford, but switched to New York shortly thereafter. Bob May, a previous NY Metro Chapter President, invited me as a guest to an ISACA® function in New York City. Shortly thereafter, I was nominated and elected to the Board of Directors in New York. My previous connections helped me get settled in the New York Metro Chapter.

ML: What are you responsible for on the chapter board of directors?
NL: As the Chapter Treasurer, I handle the expense processing for everyone that needs to be reimbursed for chapter related purchases. At every board meeting, approximately once a month, I report on where we are financially as a chapter. It is crucial to keep the Board up to date so they know how much money we have available to invest in classes. There is never a shortage of things to do on a Board of Directors and there are significant opportunities for new people to come on board to assist. We would like to see more individuals step up as members of the Board.

ML: What do you feel are the in-demand skill sets for an individual in the information systems audit and control field?
NL: A person in the IS audit and control field needs to be a good listener and be able to ask appropriate questions of system owners to ensure all the bases are covered with regard to the controls being implemented, trust what they say but verify. It is also important for an IT auditor to have some sense of understanding the technical aspects when it comes to computer systems. Continuing education is necessary to be able to understand systems. Two years ago I took a 5-day course in Chicago on Oracle R12 that provided a great baseline foundation, which is the start to really understanding the systems you audit. It is necessary to become familiar with systems you are auditing and to stay current on technology.

ML: Do you hold any certifications?
NL: I hold the CISA® and CGEIT® certifications. With SOX being what it is, it was clear to me that in order to be hired as an IT auditor I needed to have the CISA® certification. The certification says something about who you are and what you’re doing. Almost all of the companies at which I’ve consulted required the CISA® for IT auditors.

ML: What are some of your hobbies and/or interests outside the office?
I own three horses and am a passionate equestrian. My fiancé is the farm manager of an equine rescue so we try to include horses on all of our vacations. Last year we worked on a ranch in Soda Springs, Idaho and had a blast! As the weather gets warmer I am looking forward to begin Fox Hunting with my fiancé. And don’t worry, the fox isn’t killed! Also, I would like to put together an equestrian tour right here in Central Park for those members who might be interested. There is a stable that can provide up to twelve horses. It may cost about $150 to $175 per person for a 90 minute ride and lunch. And no…CPE credits are not included.
Chapter News

Job Postings on the ISACA® NY Metro Chapter Website
www.isacany.net

Current job postings in the NY – Metro area include:

**Senior SAP Information Systems Auditor – Ann Taylor**

*Job Description*

- Auditing the SAP environment to insure:
  - The design and operating effectiveness of SAP system internal controls
  - System functionality is optimized by utilizing SAP system based controls
- Participating in SAP implementation projects to insure the effective design and implementation of internal controls as well as the overall effectiveness of project management
- Planning and conducting reviews of non-SAP (legacy) systems to assess the adequacy of internal controls and compliance with Company and departmental goals, objectives and standards
- Effectively planning and executing the company’s SOX 404 IT general controls audit program

More information about this position can be found at the “Job Opportunities” section of www.isacany.net.

**Senior Attack and Penetration Consultant – Protiviti**

*Job Description*

Execute internal and external Network Attack and Penetration, and Vulnerability Assessments. This entails simulating an external attacker profiling and exploiting Client target networks. Senior must be familiar with leading penetration testing tools and techniques, be able to identify vulnerabilities within Client systems, identify or develop appropriate exploit code, and launch successful exploits to obtain access to target systems. Testing activity will be closely coordinated with Clients to minimize potential adverse affects to Client systems and network. Internal pentest activity involves simulating a motivated attacker to obtain physical access to client facilities (social engineering), identifying internal information assets, assessing threats and exploiting vulnerabilities via the use of manual techniques and automated testing tools such as native Operating System, network maintenance and troubleshooting commands as well as automated scanning software, e.g., NMap port scanner and Nessus vulnerability scanner.

Perform Web Applications Penetration Tests and Vulnerability Assessments utilizing software tools such as WebInspect and Nikto, and manual techniques to exploit vulnerabilities in the OWASP top 10 including but not limited to cross-site scripting, SQL injections, session hi-jacking and buffer overflows to obtain controlled access to target systems;

More information about this position can be found at the “Job Opportunities” section of www.isacany.net.

**Senior SharePoint Developer – Large Non-Profit Organization**

*Job Description*

A large non-profit organization, headquartered in NYC, is seeking a Senior SharePoint Developer reporting to the Chief Information Officer. This job will be located in Brentwood, Long Island (close to Hauppauge) and requires a strong development background in SharePoint, SQL database, and web development technologies. This position will provide technical expertise to the business utilizing a structured business analysis approach to software development and will maintain the organization’s intranet and external websites. They will also contribute to the decision making process in areas regarding the development and deployment of software architecture and technologies throughout the organization.

More information about this position can be found at the “Job Opportunities” section of www.isacany.net.

If your company is looking to fill an opening in IT audit, security, management, or operations we would be glad to list it on the ISACA® NY Metro chapter website for free!

To submit a job posting please email the job description and contact information to Membership@isacany.org. The opening will be posted on our site for 30 days unless otherwise directed. This service can only be seen by those logged into our website www.isacany.net.
Chapter News

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.

Joseph J. Wasserman Award Nominations

Chapter members are invited to submit nominations for the Joseph J. Wasserman Award via e-mail to Wasserman@isacany.org.

Each nomination should include contact information for the nominee and a description of their leadership, visibility, and contributions to the field of Information Systems Audit and Security and to ISACA®.

Every year the Chapter grants the Joseph J. Wasserman Award to an individual in recognition of their outstanding achievements and contributions to the field of Information Systems Audit and Security. Joe Wasserman was one of the founding members of the Chapter and was a pioneer in the field of Information Systems Audit and especially in the area of audit software.

When, in 1978, the Chapter created the Award, it was the first in our profession and it is regarded as the most prestigious.

Membership Meeting Photo Ops!

Left: Emil D’Angelo, ISACA® International President, presenting on the topic of ISACA®’s Strategy and Status at the October 2009 Membership Meeting held at HBO in Manhattan.

Above: Members of the Chapter Board of Directors participating in a panel discussion at the October 2009 Membership Meeting.
Myths and Realities of Data Security and Compliance

Ulf Mattsson | Michael Boldizar, CISSP
CTO |Founder
Protegrity | Knight Information Security Consulting

Today, perhaps more than ever, information security is capturing the attention of the CIO. Many companies have enhanced their perimeter and network security infrastructures. Yet, we still see a large number of security breaches and legislation being passed to encourage companies to increase security defenses. So what’s lacking in the current information security arsenal? What are the major driving factors behind these phenomena? How can companies evaluate information security and what are some of the remedies to address these issues?

One of the primary driving forces behind increased data security is data breaches. Unlike the stereotypical “hacker” of fifteen years ago who was interested only in defacing web sites for notoriety, today’s hacker seeks to steal information for profit.

“...In 2008, this [criminal activity] was accomplished by targeting points of data concentration or aggregation and acquiring more valuable sets of consumer information. The big money is now in stealing personal identification number (PIN) information together with associated credit and debit accounts...”

In a testament to the effectiveness of today's hackers, Verizon reports that the average breach resulted in approximately 38,000 records breached by external attacks, while internal attacks resulted in approximately 100,000 records breached. Using the Ponemon study's calculations an average breach resulted in a financial loss of $202 per record and an external compromise resulted, on average, a cost of over $7.5 million. It should be noted that the difference between the number of records compromised varied greatly between internal and external attacks. External attacks can be compared to “black-box” vulnerability assessments, where the actual target – in this case, points of data concentration – is unknown. Similarly, the location of the data, as well as the defenses protecting this data, are unknown to the attacker. Therefore, the attacker must carefully seek out data which would yield the largest payoff and how best to attack that data. Conversely, the internal attacker is acting in a manner similar to a “white-box” vulnerability assessment, in which the entire information technology landscape is often known. In this case, the attacker knows what data is valuable, where it is located, and, how those points of data concentration are defended. For example, take the case in January 2008 involving Societe Generale, in which Jerome Kerviel was able to execute unauthorized trades as a result of his knowledge of the control procedures of the bank.

Among the supporting documentation in the Verizon report was a table detailing the various compromised assets by percentage of breaches and records. While the Point of Sale (POS) system has the highest percentage of breaches, accounting for 32%, it only resulted in 6% of the total number of records compromised. In second place according to frequency of breaches was the database server, which experienced 30% of the breaches, yet resulted in 75% of the total number of records compromised.

Third on the list was the application server, with 12% of the breaches and 19% of the total records compromised. File servers accounted for 8% of the breaches, yielding 0.1% of the records breached. Although somewhat counter-intuitive, the web server was involved in 10% of the breaches, yielding only 0.004% of the records breached. The remaining assets were far lower on the list of both percentage of breaches and records compromised. With today's technology, databases typically are the central point of data concentration, followed by the application and file servers.

Breaches, while a strong factor, usually only result in changes to security after the breach has occurred and the company has lost a considerable amount of money. Fortunately for security, it is not the only driving factor. Government regulations and industry standards have been driving forces in developing security standards. Regulations and standards seek to set

2 Ibid.
minimun baselines across a particular industry segment, such as financial services or the medical field. Among the more commonly referenced laws are the California Security Breach Notification Act, (SB 1386), the first law specifically addressing data breaches, and the Massachusetts Privacy Law (201 CMR 17.00), the most recent law which only took effect in March 2010. Both laws have further defined requirements for notifying victims of a breach of personally identifiable information (PII). The Massachusetts law is especially groundbreaking, since it specifically states if any person or entity stores personally identifiable information of a Massachusetts resident, that person or entity must take reasonable steps to protect that information. This includes a wide variety of security controls, including a written security policy, as well as implementing technical and physical controls as necessary to protect PII. At a minimum, regardless of standard or law, PII is typically considered to include the following: (a) name; (b) social security number; (c) address; and (d) some form of account number. For the both of these laws, driver’s licenses and other information are also considered to be included as PII.  

In addition to state law, there are many industry-specific regulations to which companies and service providers must adhere to. While all of these regulations cover the entire spectrum of information security controls that must be followed, we will limit this article specifically to data protection references. For the health care profession, HIPAA regulations must be considered. HIPAA regulations add medical conditions to the list of PII that must be protected. While stopping short of mandating the use of encryption to protect electronically stored health information, HIPAA strongly encourages the use of a mechanism to encrypt and decrypt electronic protected health information. The HITEC act, which took effect in February 2010, expands the HIPAA regulations to apply to associate service providers rather than just the primary care providers. Under this act, the US Department of Health and Human Services (HSS) and the Federal Trade Commission (FTC) have both been given a role to play under the law, potentially levying punishments and fines on organizations that fail to adequately protect personal health information. For anyone involved in processing credit card information, PCI DSS Standards Requirement 3, Protect Stored Cardholder Data, suggests the use of encryption to protect information that it considers sensitive, which includes full magnetic stripe information, full Primary Account Number (PAN), and Card Verification Value (CVV). Entities regulated by Board of Governors of the Federal Reserve System, Federal Deposit Insurance Company (FDIC) and other entities fall under the Federal Financial Institutions Examination Council (FFIEC) guidelines. These guidelines suggest that sensitive data in transit should also be encrypted. In addition, both the PCI and FFIEC recommend encrypting data both in motion and at rest. Obviously, protecting data at rest, when it is merely stored somewhere, is important so that someone cannot simply compromise the native database files themselves. But it is also important to protect data in motion, as it traverses the network, because, under the right conditions, that information can be read (or “sniffed”) by someone using the proper utilities or programs.

Security best practices offer additional guidance regarding information security. As with the industry-specific guidelines and standards, the ISO 27001 and BS7799 standards cover the entire spectrum of information security controls that should be implemented by an organization. Specific to this article, both ISO27001 and BS7799 require sensitive information to be encrypted when either stored or transmitted.

An information security risk assessment essentially determines what needs to be protected by identifying and documenting: (a) threats, controls, and business impact; (b) gaps in relation to what is required by standards or best practices; (c) compensating controls or accepted risk; and (d) identify controls common to multiple standards. It should be noted that information security risk assessments use similar methodologies to document and evaluate all the major information security controls, not just controls pertaining to sensitive data.

It is now established that sensitive data must be protected, and encryption is one way of protecting that data. But the question now becomes, does everything need to be encrypted? As most of the regulations and standards have indicated, only sensitive information must be encrypted. But how do you identify what is sensitive and needs to be protected? As the FFIEC guidelines and best practices such as ISO 27001/BS7799 suggest, review the information security risk assessment and identify items and areas classified as requiring encryption.

To summarize, it has been established that the database, application, and file servers are typical points of data concentration that are often attacked by organized crime. These concentrated points of data contain large amounts of

6 http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf  
7 HIPAA §164.312(a)(2)(iv)  
8 https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml  
9 FFIEC Information Security IT Examination Handbook
sensitive data that must be protected in accordance with a vast array of legislation, standards, and guidelines. Encryption is one way of protecting sensitive data.

Encryption, while offering many advantages in protecting against data leakage and physical theft of the device on which the information resides, involves a number of considerations. First, in traditional encryption technologies such as asymmetric (public/private key pairs) and symmetric (private key) technologies, both the distribution of keys and the keys themselves must be heavily protected. Also, the wrong choice of configuration may lead to slow response times, additional disk space requirements, and impact upon legacy applications. Fortunately, there are newer technologies available today to help greatly minimize these potential issues.

Until recently, security experts believed the best way to defend data was to apply the strongest possible technological protections to all of the data, all of the time. While that plan may work perfectly in theory, this model creates unacceptable costs, performance and availability problems.

What works from both IT and management standpoints? Risk-adjusted data security. Protecting data according to risk enables organizations to determine the most significant security exposures, target budgets towards addressing the most critical issues, strengthen the security and compliance profile, and achieve the right balance between business needs and security demands.

Other issues that risk-adjusted security addresses are the unnecessary expenses, availability problems and system performance lags that result when data is over-protected. Cloud-based technologies, mobile devices and the distributed enterprise require a risk mitigation approach to security. This focuses on securing mission critical data, rather than the now-unachievable ‘protect all the data at all costs’ model of the past.

Risk-adjusted data security plans are cost effective. Among the typical benefits of a risk-adjusted plan is elimination of the common and costly ineffective triage security model. Replacing triage with a well thought-out logical plan that takes into account long-range costs and benefits enables enterprises to target their budgets toward addressing the most critical issues.

By switching focus to a holistic view rather than the common security silo methodology, an enterprise will naturally move away from deploying a series of point solutions at each protection point. Results in redundant costs, invariably leaves holes in the process, and introduces complexity that will ultimately cause significant and costly rework.

Additionally, understanding where data resides usually results in a project to reduce the number of places where sensitive data is stored. Once the number of protection points have been reduced, a project to encrypt the remaining sensitive data with a comprehensive data protection solution provides the best protection while also giving the business the flexibility it needs.

In conclusion, while encryption is not a “silver bullet”, it should be implemented as an integral part of a “defense-in-depth” strategy.

About Knight Information Security Consulting
Knight Information Security Consulting believes that all companies should strive for the appropriate level of security for their organization. Knight Information Security Consulting provides a wide range of information security services that can be customized to fit an organization's needs including: performing security risk assessments; gap analysis between information security standards (e.g., regulatory agency or parent company) and the organization's current environment; vulnerability assessments; creating or updating information security policies, procedures and work instructions; providing security awareness training; and computer forensics.

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 Education Update

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

We’re already off to a great start this year with our education program, with lots more on the way. We targeted our Spring course selection to align with many of the new technologies and hot topics that we, as IT Audit and security professionals, need to know.

We started 2010 with a class on Spreadsheets Risks – which was an immensely popular Webinar last year. Based off of that success, and your feedback on the type of classes you would like to see offered, the instructor prepared a ½ day, in-person seminar, which he delivered in January.

Since information security is always an in-demand skill, we held a course on the ISO 27001 Security Framework. This is already an industry-standard and the instructor, Jay Ranade from Technodyne University covered all the basics of what you really need to know.

Our March calendar featured two courses – “Monitoring for Fraud in an Electronic World” and “A Risk-based Approach to Information Security”. Judging from the turnout – both courses seem to be an extremely popular topic with our members. The former, was taught by Tony Reyes former NYPD electronic crimes detective, and the latter by Ulf Matson, CTO of Protegrity. I personally had the pleasure of working with Tony on a live case, back in 2002. He has since left the NYPD to become president of his own company, specializing in electronic crime investigations. Also, a big thanks to Ulf, who volunteered his time to teach the security class – allowing us to offer a free class to our members.

Coming up this spring, we have two other technical courses covering risks and audit approaches for Cloud Computing (April) and Windows Active Directory and Windows Server 2008 (May). We also have two Webinars in May – one on Software Asset Management and one featuring a Val-IT case study. Make sure you check our website, www.isacany.net, for details and registrations.

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!!
ISACA® Certification Update

Dustin Bradley
Board of Directors, Certification Coordinator
ISACA® NY Metro Chapter

CRISC® Certification

ISACA® is responding to market demand by introducing a new risk-related certification. The Certified in Risk and Information Systems Control (CRISC®) designation is for IT professionals who identify and manage risks through the development, implementation, and maintenance of information systems (IS) controls. These professionals help enterprises accomplish business objectives such as effective and efficient operations, reliable financial reporting, and compliance with regulatory requirements. A grandfathering program, through which experienced professionals can earn the certification without passing an exam, will open in April. The first CRISC® exam will be administered in 2011. Additional information about the CRISC® certification is available at www.isaca.org/crisc.

Certification Exam Review Courses

The ISACA® New York Metropolitan chapter will be offering four review courses to help individuals prepare for the ISACA® certification exams (including the “IT Boot Camp” course for non-IT professionals planning to take the CISA® exam). See below for the course listing. To register for a review course, visit www.isacany.net.

<table>
<thead>
<tr>
<th>Class</th>
<th>Date</th>
<th>Description</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGEIT® Review Course</td>
<td>April 10/17, 2010 (2 consecutive Saturdays)</td>
<td>2 Day Class (14 CPE) The purpose of this review course is to help prepare CGEIT® examination participants to successfully pass the ISACA® sponsored CGEIT® examination.</td>
<td>Jay Ranade</td>
</tr>
<tr>
<td>CISA® Review Course</td>
<td>May 1/8/15/22, 2010 (4 consecutive Saturdays)</td>
<td>4 Day Class (28 CPE) The purpose of this review course is to help prepare CISA® examination participants to successfully pass the ISACA® sponsored CISA® examination.</td>
<td>Jay Ranade</td>
</tr>
<tr>
<td>CISM® Review Course</td>
<td>May 8/15/22, 2010 (3 consecutive Saturdays)</td>
<td>3 Day Class (21 CPE) The purpose of this review course is to help prepare CISM® examination participants to successfully pass the ISACA® sponsored CISM® examination.</td>
<td>Jennifer Bayuk</td>
</tr>
<tr>
<td>IT Boot Camp for CISA® Exam</td>
<td>May 13</td>
<td>1 Day Class (7 CPE) The purpose of this review course is to help non-IT professionals/auditors prepare for the ISACA® sponsored CISA® examination. It is recommended as a prerequisite for attending the CISA® Review Course.</td>
<td>Jay Ranade</td>
</tr>
</tbody>
</table>

Remember, the deadline to register for a June 2010 CISA®, CISM®, or CGEIT® certification exam is April 7, 2010.
IT Frameworks

Doing More with Less: IT Framework Integration

George Spafford
Senior Manager, Cognizant Technology Solutions
ISACA® NY Metro Chapter Membership Meeting Presenter, December 2009

With the economic downturn organizations are pushing to drive down costs while improving quality. To shorten the learning curve and improve the likelihood of success, proven business and IT frameworks relating to quality and other disciplines are being reviewed for insights on how to improve effectiveness and efficiency. IT groups not familiar with the various frameworks and how they may integrate are apt to make wrong decisions or allow business management to make wrong decisions.

Given the plethora of frameworks that IT may be involved with, it only makes sense to review some of the most common ones at a very high-level and then discuss how they can work together. The following are common frameworks that IT may well encounter:

Control Objectives for Information and related Technologies (COBIT®) – This identifies controls that are used in process design to mitigate risks. Once an organization understands risks and wants to identify how to mitigate those risks, then COBIT® can help.

Information Technology Infrastructure Library (ITIL®) – This collection of five books codifies IT Service Management (ITSM®) and the associated lifecycle of IT services with supporting best practice processes. The ITIL® guidance begins with Service Strategy, then Service Design, Service Transition, Service Operation and Continuous Service Improvement.

ISO/IEC 20000:2005 – This is the international standard for ITSM. It is split into two parts: 20000-1 identifies the standard itself and what an organization must do to be accredited; 20000-2 is the code of practice that identifies opportunities for improvement. At this time, it is based on ITIL® v2 and whereas ITIL® does not have a certification associated with it, ISO 20000 does.

ISO/IEC 27000:2005 – This is the international standard for information security and at this time has two parts also and there are plans to add more in the future. 27001 outlines the requirements for the standard. The 27002 Code of Practice document gets into more details around the controls.

ISO 9000 – This generic name relates to a collection of standards that help define a quality management system. While it originated in manufacturing it can be found in many different types of organizations.

Lean Six Sigma (LSS) – This is a combined quality management approach that blends Lean’s desire to move faster and create value with Six Sigma’s approach to reduce defects and re-work. As a result, LSS addresses defects and time wasted as it seeks to increase overall speed while reducing cost.

Leveraging the Frameworks

In reviewing the above, we can make some broad groupings. ISO 9000 and LSS can be found in organizations around the world and are not IT centric. The others are specific to IT so let’s begin there:

COBIT® is used to mitigate controls and recommends what to do but doesn’t give details around how to design the control. In fact, controls need solid processes to be effective and then that raises the other frameworks. ITIL® provides very good guidance on IT Service Management processes. For perspectives on how to design processes that embody controls relating to the change management, release, incident management and other areas relating to service, ITIL® is very good.

Now, ISO 20000 and ITIL® do overlap. Right now, they are also a bit disparate because of ISO 20000’s grounding in ITIL® v2. Groups pursuing ISO 20000 may benefit from the additional guidance that can be found in ITIL® v3 but still must make sure they follow the requirements set forth in the standard in order to be certified. For groups looking to show their clients they are focused on providing quality services, an ISO 20000 certification is one way to do that.

To be clear, ITIL® is very much focused on improving the quality of services that IT provides. Its drawback is that it does not carry a certification. For example, when a tool claims to be “ITIL Compliant”, that is just a marketing term because no such certification exists. Likewise, a practitioner company can be assessed and receive objective recommendations on how to improve but there isn’t a certification like there is for ISO 20000.

continued on page 16
**Risk IT Framework and Practitioner Guide Overview**


Compiled by Michelle Syskrot

Metro Line Photo and Copy Editor

ISACA® New York Metro Chapter

What is Risk IT?
Risk IT is a new framework developed by a global team of industry experts that extends the COBIT® and Val IT® frameworks. Risk IT provides organizations with a guideline for synching IT-related risk management practices with company-wide risk management objectives. Risk IT was designed to help management implement IT governance, manage risk to achieve enterprise-wide goals, understand the opportunities of risks, and gain a greater return on investments. Risk IT provides guidance to help executives and management ask valuable questions to make better, more informed, risk-based decisions. The Risk IT framework is ideal for companies that current utilize the COBIT® as their IT governance framework.

IT Risk Categories
IT risk is business risk; specifically, it consists of IT-related events that could potentially impact the business. There are three high-level IT risk categories, detailed below.
- IT benefit/value enablement risk – risks regarding missed opportunities to use technology to improve efficiency of the business
- IT program and project delivery risk – risks regarding the contribution of IT projects to business solutions
- IT operations and service delivery risk – risks regarding performance of IT systems and services

There is a “downside” and an “upside” to each of the three risk categories. Enterprises must consider the exposure that may result if a risk is not addressed and also the benefit that may occur if the opportunity is taken.

Risk IT’s Three Domains
The Risk IT framework provides guidance on how to manage three major risk domains, listed below:
- Risk Governance – Understand the “risk culture” of the enterprise; define responsibility and accountability for IT risk management, develop a common risk view within the enterprise
- Risk Evaluation – Evaluate the risk scenarios and business impact
- Risk Response – Managing and reacting to risks, risk prioritization

What are the benefits of Risk IT?
- Risk IT allows an organization to obtain a high-level view of current and future IT-related events and how to manage IT-related risks
- Enterprises can increase information quality
- Organizations can gain an increased knowledge of how to take advantage of the investment made in an IT internal control system that is already in place

For more details on the Risk IT framework and Practitioner guide, refer to the ISACA® website. Both the Risk IT Framework and Risk IT Practitioner Guide are available as a free download to all ISACA® Members (www.isaca.org/riskit)
The ISACA® New York Metropolitan chapter continues to respond quickly to the market needs of establishing governance structure at all levels (e.g. corporate, government, regulatory). The chapter Education Committee actively supports ISACA®'s educational strategic objectives in three ways: 1) by providing high quality training to meet membership and market needs, 2) by promoting ISACA® as the recognized leader in IT Governance, and 3) by finding new technologies and better ways of delivering education to our membership.

In October 2009 ISACA® New York Metro chapter Education Committee organized a featured event about Enterprise Governance of IT. It was conducted by myself and a distinguished professor, Dr. Wim Van Grembergen, of the eminent University of Antwerp in Belgium. As a result of that successful event, we established an IT Governance roundtable group which has already held two sessions since then, on November 13th, 2009 and February 25th, 2010.

The topics for both sessions were selected based on the feedback and questions we have received from membership and during training sessions. During the recent roundtable session we had a renowned speaker, Brian Barnier, who brought a unique perspective to business-IT management. With a split career between “the business” and IT, he works to bridge two sets of needs to get greater business benefits from IT. He has a unique vantage point because of his experience in practical projects, best practices committees, research and teaching professional education across industries and countries. His research on “what works” in risk management with a co-author at MIT Sloan CISR has been published in several publications, most recently the ISACA® Journal. During the roundtable session he covered IT governance essentials for getting more value for the business. Roundtable participants learned the critical role of program/project management in managing change, learned about new techniques of overcoming the unit cost trap and became aware of new trends and improvement plans of COBIT®, Val IT™, and Risk IT.

A series of IT Governance training sessions will be offered by ISACA® to our members, including live sessions and webinars during the April - June 2010 period. Here are some of the highlights of IT Governance upcoming sessions:

**IT Governance Roundtable 3rd session** (moderated by Emma Arakelyan, guest speakers: Brian Barnier and TBD), Targeted for May 2010
Two hour meeting with one hour training session (1 CPE) and one hour open discussion. The meeting will take place at Ernst & Young, 5 Times Square New York City location. If you are interested in this session and/or if you have ideas on topics to be covered, please send an email to emma.arakelyan@isaca.org.

**Val IT™ Case Study 1 Hour Webinar** (by Bob Reinhold and Nikhil Lele)
*Date – TBD*
This one hour webinar (1CPE) will provide an overview of IT Value Management mentioning industry standards (such as the ISACA® Val IT™ methodology), including the processes, activities and tools that are required to control and maximize performance across each key phase of the IT investment value chain. The following phases of the value chain will be discussed in detail:
- Understanding value delivered by an IT project and quantifying the value delivered by an IT project
- Determine the value of an IT investment by understanding how Demand, Execution, Process Portfolio, and Value management can help

**Software Asset Management and IT Governance** (by Dan Stavola)
*Date – TBD*
This one hour webinar (1 CPE) provides an overview of Software Management and Governance activities to control these business-critical assets in order to maximize performance of both the software lifecycle and any direct or indirect costs related to the overall asset program.
- Introduction to Software Governance and Compliance through a SAM Program
- Industry Standards for SAM: ITIL® & ISO/IEC 19770-1 SAM Processes
- Cost Leadership Strategies: Cost Reduction & SAM

More details will follow on the content and dates for these sessions. We are very interested to hear from you on these currently proposed sessions and urge you to offer additional topics you would like the ISACA® New York Metro chapter to offer. Please send your comments or feedback to emma.arakelyan@isacany.org.
Editorial

What’s the Limiting Factor?

James Ambrosini
First Vice President
ISACA® New York Metro Chapter

Last year, I took up competitive cycling. While I was by no means the next Lance Armstrong, I did beat out a few younger, stronger and more experienced riders in the nine races I entered, including the US Grand Prix. So, being the competitive person I am, I decided to figure out just what I needed to do to take cycling to the next level. I spent countless hours calculating the efficiencies gained and power increases through lighter wheels, better tires, and changing my bike fit. If there was a website dedicated to cycling performance, I probably read it - at least twice.

So what did I learn from all this research? I discovered that for entry-level racers, even the lightest, fastest bike in the world won’t drastically improve race performance. The answer was the simplest thing to do – but also the toughest to put into practice: just train harder. As a novice racer, performance gains are made with a better “engine;” a more aerobically-adapted body that’s used to the demands of racing. The only way to get that better engine is to simply ride and train harder. All of the equipment upgrades I was considering weren’t affecting my endurance, which my coach determined was my “limiting factor.” Improving my endurance would offer the biggest performance gains on the bike.

I decided to apply the same reasoning to my work life. Through some introspection, I realized that over the years I had drifted away from some industry-specific business processes knowledge. This particular knowledge, while never really holding me back, now meant the difference between being able to deliver targeted solutions to new clients by understanding their pain-points, and getting by with what I already knew, and hoping that was enough. So, I’ve embarked on several self-study options to get what I need.

I believe that we all have a “limiting factor” that could be preventing us from getting the job or position we want, or getting to the next level. The gap may be very granular, like not knowing a particular technology/business process, or not having the right credentials to get you in the door. It could even be a softer skill, like experience with managing teams, multi-tasking, or communicating effectively.

I would encourage everyone to sort through this process themselves before you may have to do it unexpectedly. Think about the one thing, which if you possessed knowledge about, could open doors for you. You may want to ask people in your industry or career for advice on upcoming trends, or what they think it takes to succeed. I’ll give you a tip: a simple call with an experienced recruiter can be an eye-opener as to what companies are looking for, and what gets people hired. The answer may not be what you were hoping to hear, but overcoming the right limitation will surely mean a noticeable performance improvement for your career.

Doing More with Less: IT Framework Integration

 Returning to COBIT® and process guidance, if controls around information security are needed, then ISO 27000 can be used for additional guidance. For organizations that want to market their attention to information certification, becoming certified in ISO 27000 and identifying such is one approach.

ISO 9000, Lean, Six Sigma or LSS are all quality management frameworks the overall organization may be pursuing. Many business managers and executives have formal training and experience with these approaches to quality. What they do not have exposure to is ITIL®. If there is pressure to stop an ITIL® implementation because LSS is being pursued, for example, then it needs to be explained that ITIL® can provide reference practices for groups pursuing process improvement. If ITIL® is not used, then process improvement will be limited. For instance, it may be identified that the handling of incidents needs to be streamlined. Without referring to ITIL®, the stakeholders involved can only try to improve their approach based on what they know.

In closing, there are many frameworks in the world today; far more than the handful mentioned in this article. IT groups seeking to improve their processes would do well to understand what other groups are doing, both within the firm as well as in the industry, and the direction the overall organization is taking. IT can then plan how to best continuously improve the services that they provide to create and protect value for the organization.

This article was previously published at http://www.itsmwatch.com.
Spring Into Reading...New on the ISACA® Shelves

Faye Reece  
Metro Line Staff Writer  
ISACA® New York Metro Chapter

Vulnerability Management by Park Foreman  
This book focuses on being proactive to prevent the exploitation of IT security and weaknesses that exist particularly within a large organization.

IT Financial Management by Maxime Sottini  
This book covers the main financial concepts that managers need to be familiar with in order for IT to take its proper place as a contributor to the business.

Internal Controls Policies and Procedures by Rose Hightower  
This is a collection of documents that summarizes the regulations and rules which are part of corporate governance.

Information Technology Governance and Service Management: Frameworks and Adaptations by Alleen Cater-Steel  
This book provides an in-depth view into the critical contribution of IT service management to IT governance, and the strategic and tactical value provided by effective service management.

SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach by Dave Chennault and Chuck Strain  
This practical guide blends the needs of the deployment staff and audit teams with a comprehensive blueprint that puts business in charge.

COBIT® User Guide for Service Managers by IT Governance Institute  
This guide focuses on service managers, providing them a better understanding of the need for IT governance and how to apply good practices in their specific roles and responsibilities.

Fraud Analysis Techniques Using ACL by David Coderre  
This book / CD offers auditors and investigators an authoritative guidance on the use of computer-assisted audit tools and techniques in fraud detection.

PCI Compliance, 2nd Edition by Anton Chuvakin and Branden R. Williams  
This book is packed with help to develop and implement an effective security strategy to keep infrastructure compliant and secure using the new Payment Credit Card Industry Data Security Standard (PCI DSS)1.2.1

Security, Audit and Control Features Oracle Database, 3rd Edition****NEW EDITION**** by ISACA®  
This book provides a new perspective of security controls over Oracle, and is intended to guide the assessor through a comprehensive evaluation of security for an Oracle database based on business objectives and risks.

Security, Audit and Control Features SAP ERP, 3rd Edition****NEW EDITION**** by Deloitte Touche Tohmatsu Research Team and ISACA®  
The publication is based on SAP ERP [also known as SAP ERP Central Component (ECC)], the latest version of which is SAP ECC 6.0, and focuses on enabling assurance, security and risk professionals to evaluate risks and controls in existing ERP implementations.

Computer and Information Security Handbook by John Vacca  
This book presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats.

Cloud Computing: Implementation, Management, and Security by John W. Rittinghouse and James F. Ransome  
This guide provides an understanding of what cloud computing really means, explores how disruptive it may become in the future, and examines its advantages and disadvantages.

Go to WWW.ISACA.ORG/BOOKSTORE for more information!
ISACA® International Seminars & Conferences at a Glance
ISACA® Educational Events Happening Around the Globe

Michelle Syskrot
Metro Line Photo and Copy Editor
ISACA® New York Metro Chapter

Conferences

UNITED STATES - CHICAGO
North America Computer Audit, Control, and Security (CACS)
18-22 April, 2010
Get the knowledge you need to stay one step ahead of the competition and keep up with changing professional trends at ISACA®’s North America Computer Audit, Control and Security (North America CACS™) Conference. North America CACS is the must attend, hot-topic event for IT audit, security and governance professionals in North America. It attracts the best and brightest with its content-rich and thought-provoking sessions that delve into some of the biggest challenges facing IT audit and security professionals.

MEXICO - CANCUN
International Conference
6-9 June, 2010
Every year, the worldwide ISACA® community comes together at the International Conference, ISACA®’s leading educational and networking event. At this global forum, you will discuss and debate the most critical issues facing IT and business professionals, and discover the differing way similar problems are solved around the world. Attendees can earn up to 40 continuing professional education (CPE) credit hours. While you will see a high concentration of the traditional ISACA® topics of IT governance, IT audit, information security and risk management, you will also note a series of sessions on cloud computing and business continuity, as well as individual sessions on legal issues, leadership, controls and information management.

e-Learning

ISACA® eSymposia: The Next Generation of Data Privacy
23 March, 2010, 11:00 AM (EST)
With the emergence of new technologies, the state of privacy and information is constantly evolving. Today we see accelerated attention to systemic privacy risk and increased expectations of auditable privacy compliance, stemming not only from legislative and regulatory mandates, but also reflecting the business realities of our information-rich IT environments. This event will focus around how new laws are impacting IT governance and technical standards.

For a complete program overview and to register, please visit http://isaca.brighttalk.com.

Visit http://www.isaca.org/elearning for more Webcasts/e-Symposia learning opportunities.

ISACA® News

The “Plaid-ing” of Business and IT
Emil D’Angelo, CISA®, CISM®, 2009-2010 ISACA® International President

My daughter recently showed me a new clothing purchase and told me that “plaid is the new black.” When I looked blankly at her, she further explained that her phrase means that plaid—which has become the general term for cloth with crisscrossed lines of different colors—is now “cool” and has become a staple in her wardrobe.

Looking at her purchase made me think of how business objectives and IT objectives in the past often operated as parallel lines. IT was often considered as an afterthought and as separate from business strategy. Over the last years, though, this has changed dramatically. Business and IT objectives are now more like plaid—with many intersections and reliance on each other for the complete picture.

The material for plaid can be used anywhere that cloth is needed, just as the COBIT®, Val IT™: Based on COBIT® and Risk IT: Based on COBIT™ frameworks can be customized for any enterprise, regardless of size, industry, geographic location or other factors. ISACA® has long been a leader in this area, especially starting with the introduction of COBIT™ nearly 15 years ago.

As we continually revise and update all three frameworks, I would like to send a sincere thank you to the thousands of professionals around the world who have contributed to these frameworks and all of their related materials. I may never understand the inner workings of fashion, but I do know that ISACA® knows how to keep up with—and more often be a leader in—the “plaid-ing” of business and IT.

NOTE: This article was featured in the February 3rd, 2010 edition of @ISACA. For more articles featured in @ISACA visit www.isaca.org today!

ISACA® QUIZ – Test Your Knowledge!

1. How many members does ISACA® have, worldwide?
   (a) 33,000
   (b) 86,000
   (c) 113,000

2. What does “ISACA®” stand for?
   (a) Information Systems Association for Controls in Auditing
   (b) Information Systems Audit and Control Association
   (c) Information Systems Auditable and Controls Association

3. ISACA, started in 1969, was originally known as…
   (a) EDP Auditor’s Association
   (b) Technology Audit Controls Association (TACA)
   (c) Technology Auditing Group (TAG)

4. ISACA has more than _____ chapters in _____ countries.
   (a) 75 chapters in 60 countries
   (b) 100 chapters in 100 countries
   (c) 185 chapters in 75 countries

5. The Certified Information Systems Auditor certification has been earned by how many professionals to date?
   (a) 70,000
   (b) 93,000
   (c) 140,000

See page 20 for answers.
THANK YOU TO ALL THOSE WHO CONTRIBUTE TO
Metro Line!

Your efforts and support are greatly appreciated!

ISACA® Quiz - Answers
1. (b); 2. (b) 3. (a) 4. (c) 5. (a)

ISACA® New York Metropolitan Chapter Newsletter Committee

James Ambrosini
Board Newsletter Committee Chairman

Danielle Henry
Editor-In-Chief

Michelle Syskrot
Photo and Copy Editor

Debbie Morales
Staff Writer

Faye Reece
Staff Writer

Jenny Urena
Staff Writer

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

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

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

Norman Levine
Treasurer
Norman.Levine@isacany.org

James Powers
Corresponding Secretary
James.Powers@isacany.org

Nigel James
Recording Secretary
Nigel.James@isacany.org

2009-2010 Directors
Alexander Abramov
Manisha Agarwal
Emma Arakelyan
Dustin N. Bradley
Kevin Fuller
Patrick Grant*
Yonique Malbranche
David Kipin*
Patricia Martin
Robert May*
Andrew T. Robinson
Raisa Serebrenik
Kwongmei (May) To
Chris Westerman
Richard Ziegler

* Past President