

## ISACA 2012 Training Courses!

### Healthcare Information Technology

Up to 32 CPE's!

Los Angeles, February 6 - 9  
New York, August 20 - 23

ISACA and Deloitte & Touche LLP deliver a course that focuses on healthcare industry regulatory reform and healthcare information technology (IT). Hot topics include regulatory issues, trends and future reform, as well as how these affect the IT audit Professional.

For registration and additional information click [here](#).

### Information Security Essentials for IT Auditors

Up to 32 CPE's!

San Francisco, March 12 - 15  
New York, Oct 29 - Nov 1

ISACA and Deloitte & Touche LLP deliver strategies and tactics to address a range of information security issues in the workplace. Learn to identify and analyze the risk associated with security threats across network, operational and physical systems.

For registration and additional information click [here](#).

For a listing and information on all 2012 ISACA Training Courses, click [here](#).

## IN THIS ISSUE:

- A Note from the President & Events for 2012 P.1
- ISACA 2012 Training Courses P.1
- ISACA Updates P.2
- Get Involved in 2012! P.3
- BR Chapter & June 2012 Exam Information P.4
- Upcoming Webinar P.4



## A Note from the President...

*Wow! Where did the year go? What a victorious year for the LSU Tigers and New Orleans Saints! Your Baton Rouge Chapter had the honor of hosting a very successful CISA Review course for our fellow ISACA neighbors from near and far. We had participants from across Las Vegas to Canada! We are excited to show the ISACA Nation what the Baton Rouge Chapter can do. We are striving to bring you training that is in demand and convenient for you.*

*It is the end of 2011 and time to start planning out our 2012 calendar. We are sharing our wish list with you regarding trainings to bring to you in 2012. If you don't see what you need, please let us know. Help us help you.*

*Best wishes for your end of year work tasks, I am sure we have many activities to juggle. Stay sane and stay up to date with ISACA.*

*Sincerely,  
Michelle R. Seeling  
ISACA BR President*

### ISACA BR Events for 2012

#### Annual Chapter Meeting – February

Our annual update from ISACA National, Membership Appreciation and Nomination and Voting of your 2012-2013 Baton Rouge Chapter Board Members!

#### Membership Social – June

#### Trainings we are looking into...

- \* COBIT Foundation Course
- \* Part Two Forensics
- \* Network Security Essentials
- \* Implementing Control Self Assessment
- \* Information Risk Management

**If you have any training and or meeting suggestions you would like to see, please send them our way!**

# ISACA UPDATES

## 7 Common Threat Areas

By Leighton Johnson, CISA, CISM, CIFI, CISSP

One In the current Internet-based world, there are common threat areas to be aware of and plan for as we provide security services to our customers and clients. They are:

**Data breaches**—The current trend of stealing corporate data for financial or ideological reasons has led to wide-reaching political and economic fallout. There are multiple possible sources for these data thefts including, among others, compromised accounts, web attacks and insider threat realization. There are reports of large-scale data breaches appearing in the press with regularity. Both internal compromised accounts and external attacks against web sites and networks have been the source of these attacks. Always be on watch for potential exfiltration of corporate data as an indication of a potential data breach.

**Identity theft**—The current statistics on identity theft are somewhat staggering. The US government is reporting that there is an identity stolen every 3 seconds. The incredible ramifications of personal loss and stress cause many to experience a lack of guidance and policy in this area. The means for such attacks are usually phishing e-mail attachments being sent via personal and corporate e-mail accounts. The best way to handle all e-mail is to “distrust by default” all e-mail attachments, no matter where they come from or who sent them.

**Web 2.0 attacks**—The proliferation of embedded malware on legitimate web sites has led to computers being attacked by unknown assailants from normal web activity. The actual sites are infected by pictures or mashup actions wherein malware is installed via pictures, images, searches or scripts that then install them when these “pictures” are read by the unsuspecting browser.

**Messaging attacks**—E-mail and instant message still provide the largest spread of questionable content on the Internet. Standard spam accounts for more than 85% of all e-mails travelling the Internet on a daily basis and these messages provide attackers a way into personal and corporate servers. The incredible range of computing devices and models in the current world require the security professional to constantly be aware of the messaging methods for attack.

**Botnets and zombie computers**—The primary reason for computers being infected and the incredible increase in botnets is very simple: money. Given the current economic state globally, these programs allow the criminal element to obtain large sums of money with relative ease and low risk. Always be on the lookout for machines running when they should be off and communicating on new or different channels, which can indicate they are part of a botnet.

**Rootkits**—These programs are usually targeted attacks against a specific company or person, very technical in nature, extremely difficult to detect, and even harder to remove once detected.

These programs are designed to run below the operating system on the computer, while most security software runs at the operating system level; therefore, such security software will not detect these malicious programs running. One possible way to determine if a rootkit is running is to monitor the system processing channels while the machine is operating; however, the machine would most likely not reflect this activity if it was turned off.

**Logic bombs**—Logic bombs are pieces of code or scripts attached to legitimate code that operate in the normal computing environment, but have time-based triggers to cause detrimental or malicious effects. These are almost always loaded by insiders who are disgruntled or angry. Always watch the activity of soon-to-be ex employees or passed-over administrators for these types of activities.

Each area of your computing environments has the potential to be attacked and have a malicious or detrimental effect on you, your organization or a customer. So always be on guard as you provide security services for them and yourself .

## Using the ISACA Wiki to Build New Knowledge

Have you ever looked for an audit program only to discover that one is not available? If you could ask hundreds or even thousands of your colleagues to help create the audit program, would you? Using the collaboration tools on the ISACA web site allows you to do just that.

By creating a wiki and inviting others to provide input, you can benefit from the experience and expertise of other members. Wikis are available in all Knowledge Center topics. Just find the topic that matches the subject matter and then create your wiki.

For step-by-step instructions to create a wiki, please click [here](#).

## ISACA's World Congress: INSIGHTS 2012

June 25—27, 2012 | San Francisco, CA

Earn up to 18 CPE Hours!

Designed for progressive IT and business leaders like you, the conference addresses topics at a strategic level, giving you the insights needed to develop strategies for effective integration of business and technology.

For additional program information and registration, click [here](#).



## *Get Involved in 2012!*

*ISACA has been fortunate to have benefited from many exceptional volunteers throughout the association's history. Members are encouraged to accept the personal responsibility to carry on that tradition, and help ISACA excel now and in the future. Our nominations for the 2012-2013 year are coming up in February!*

**We invite you to familiarize yourself with the benefits of being an ISACA volunteer and the criteria for the volunteer bodies that support ISACA. Join us in shaping your profession, as well as your future, as an ISACA volunteer!**

### **Board positions at the Chapter Level:**

- \* Chapter President
- \* Chapter Vice President
- \* Treasurer
- \* CISA/CISM Coordinator
- \* Publicity Coordinator
- \* Membership Coordinator
- \* Secretary

Please email [president@isaca-br.org](mailto:president@isaca-br.org) for the responsibility descriptions.

Committee opportunities at the Chapter Level are also available if you would still like to be involved but not at the Board Level. Email your president at [president@isaca-br.org](mailto:president@isaca-br.org) for additional information regarding committee opportunities.

Participants in ISACA's volunteer bodies help ensure successful certification programs, comprehensive professional conferences, timely and relevant education programs, insightful research, thorough and appropriate online resources, representative professional standards, and financially sound infrastructures. In short, they ensure that members and constituents receive the high-quality resources they have come to expect from ISACA and ITGI.

Volunteers and their employers benefit from increased self-confidence, broadened professional expertise, enhanced leadership and decision-making skills, and an extensive international network of professional colleagues that come from this opportunity.

### **Positions at the National Level:**

#### **WHO IS ELIGIBLE TO PARTICIPATE?**

Individuals with expertise in the professional areas supported by ISACA should:

- \* Read the descriptions of the boards, committees and subcommittees, weigh your qualifications and expertise against the needs of the groups, and determine to which group(s) you can make the most meaningful contribution.
- \* Review the information on confidentiality, intellectual property (IP) and conflict of interest described within the ISACA participation agreements.

Please see the following web page for in depth details:

[Boards and Committees - Credentialing - Governance - Knowledge - Relations | ISACA](#)

***Finally, as participation represents a significant time commitment, consider your obligations, both professional and personal.***

## Upcoming Webinar!

### Mapping Application Security to Compliance

Thursday January 12, 2012  
@ 11am CST  
Duration 1 hour

Regulatory compliance activities, which have historically focused on network security as the primary means to protect data, are beginning to focus increasingly on application security. Why? Because insecure applications are the biggest threat to data—and the evidence supports this. Both Verizon Business and NIST reported that over 90% of data breaches occur at the application layer.

As a result, regulators and industry standards bodies have dutifully added explicit and implicit security requirements as they relate to application development practices. However, these requirements are often difficult to understand and the security activities that need to be introduced within the development process are not well known. This talk will present a practical approach towards mapping application security practices to compliance requirements.

Topics include:

- \* Aligning security and compliance policies with corporate requirements and translating these policies for application development and assessment teams.
- \* Aligning application development processes and practices with security and compliance policies.
- \* Creating an action plan that identifies and remediates gaps between current and best application security practices, and documents the use of the best practices for auditing purposes.

To register for this event, click [here](#).

# Baton Rouge Chapter Information:

## UPCOMING EVENTS:

**Annual General Meeting - February 2012:** Member Appreciation and Board Elections

*Additional information regarding location and registration will be coming soon!*

## Get to know a Member!

**Tome Frazier, ISACA Baton Rouge Chapter Vice President**

**Q** How did you get involved with your chapter board?

**A** I started off on the program's committee ( helping plan and organize the chapter's trainings and luncheons).

**Q** How many years have you been an ISACA Member?


**A** Five years.

**Q** What is the most important benefit you get from being an ISACA Member?


**A** Networking with other's in my field.

**Q** What is one thing your friends know about you that your ISACA colleagues do not?

**A** I do not like speaking in front of large crowds.



**CISA**  
Certified Information Systems Auditor  
An ISACA® Certification



**CISM**  
Certified Information Security Manager  
An ISACA® Certification

**Get Recognized As An Expert In Your Profession!**


Earn the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT) or Certified in Risk and Information Systems Control (CRISC) certification.

**June 2012 Exam Registration is Open**


Online early registrations received by February 8, 2012  
\$395 (Member) \$545 (Nonmember)

Online final registrations received by April 4, 2012  
\$445 (Member) \$595 (Nonmember)

**Exam - June 9, 2012**



**CGEIT**  
Certified in the Governance of Enterprise IT  
An ISACA® Certification



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

Newsletter created by:  
Connie Freeland

For comments/suggestions please contact:  
[publicity@isaca-br.org](mailto:publicity@isaca-br.org)