

Get Recognized as an Expert in Your Profession!

ISACA certifications are globally accepted and recognized. Certification proves to employers that you have what it takes to add value to their enterprise. In fact, many organizations and governmental agencies around the world require or recognize ISACA's certifications.

Independent studies consistently rate ISACA's designations among the highest paying IT and impactful certifications that an IT professional can earn.

Get started today by [registering](#) for an exam.

FREE CPE!!!

eSymposium: A Holistic Approach to Identity and Access Management

When: October 25, 2011
11:00 - 2:00 pm EDT

Summary: Identity and access management continues to be an area of concern within enterprises. Our industry experts will be discussing a variety of issues ranging from identity theft, identity and access management in the cloud, automation of access authority, and the next generation of identity systems. Don't miss your opportunity to join the discussion and have your questions answered live at our next ISACA eSymposium on Tuesday, 25 October 2011.

Click [HERE](#) to register!

IN THIS ISSUE:

- A Note from the President P.1
- Certification Update & eSymposium P.1
- ISACA Updates P.2
- Information Security in Health Care Organizations P.3
- BR Chapter Info & Announcements 2011 - 2012 P.4



A Note from the President...

It is that time of year to renew your membership with ISACA. Our members are very important to us and we strive to provide service and guidance to you. I would like to also encourage you to consider serving on our ISACA Baton Rouge Chapter Board. Our final newsletter for 2011 will contain more details.

Most important for you; ISACA membership sets you apart from other IT professionals by signifying that you are:

- * *Dedicated to best practices and successful results*
- * *Committed to professional growth and advancement*
- * *Helping to advance your profession*
- * *A seeker of professional knowledge and a problem solver*
- * *Serious about continuing education*
- * *Connected with a highly regarded organization*
- * *Part of a global network of peers*

We do have one last chapter meeting for the year, CISA training and we are planning out our calendar for 2012. As always, if you have a topic of interest, needed training please reach out to any of our officers.

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 UPDATES

Ever Changing IT Risk and Emerging Technologies

By Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA

One of the advantages of the IT environment is the constant improvements being made to technology. Along with the good that these changes bring comes a fast-paced set of changes to IT that can also bring difficulties. In particular, when such changes and others are initially introduced, there is often a new technology that is so different from the prior one, if one existed, that IT auditing, controls and security for the new technology have to be developed almost from scratch.

The danger, or maybe excitement, of being in the IT profession is this changing world in which we live. In most cases, the changes are announced beforehand, gradually becoming a part of day-to-day IT operations, and thus, the IT auditor and IT professional know the new technology is coming.

So, it is beneficial to the IT auditor to try to keep abreast of these changes in order to be prepared to handle auditing, controls and security issues and to just answer questions appropriately about these new technologies for respective stakeholders. Therefore, IT auditors need to find authoritative ways to keep informed on emerging technologies. Professional publications (e.g., ISACA Journal), trade magazines, [IT conferences \(e.g., Computer Audit, Control and Security \[CACCS\] Conference\)](#), and even dedicated cable channels are some of the outlets that provide this information.

A look at history shows that the IT auditing profession was fortunate to have a number of “pioneers” in its beginning (1954-1964). These pioneers were the ones who developed procedures, concepts, training and other resources to perform adequate IT audits (known as electronic data processing [EDP] audits at the time). They accomplished these feats by learning all they could about emerging technologies; paying close attention to them with hands-on experience; and using their judgment, expertise and intelligence to develop tools and techniques. In the case of IT, that need for pioneers who will produce tools and techniques will continue because of the ever-changing IT world, driven by emerging technologies and associated IT risks.

Today, most understand that the emerging technologies with the greatest auditability, controls and security concerns are social networks, cloud computing and mobile computing. It is also obvious that these three technologies are growing by leaps and bounds. The surveys in [my recent column](#) substantiate this fact about these technologies. Also, see the [2011 ISACA IT Risk/Reward Barometer Survey](#) for more on these technologies and risks.

How Much Negotiation Skills Is Required for an IS Professional?

By Sivarama Subramanian Kailasam, CISM

Recently, I concluded a security assessment for a mobile-based web application. It is a hybrid mobile application that can be invoked from a web browser and from a mobile phone as a native application. At the end of the assessment, I reported 2 high, 7 medium and 14 low-rated vulnerabilities.

All is well so far except that there is no agreement on the severity levels of 2 of the high vulnerabilities reported to the project team. The project team is not ready to accept the vulnerabilities unless I demonstrate how the actual attack will happen. Simply put, the project team wants me to do a penetration test in the place of vulnerability assessment. I had a hard time convincing the team that a vulnerability assessment is different from penetration testing.

This brought up an important issue for the information systems (IS) professional—whether an IS auditor or IS implementer. The project team and the IS professional need to agree on the findings and address the issue(s) as quickly as possible; otherwise, the applications can be rolled out to production without fixing the vulnerabilities. As per the security policies of most customers, unless the application passes the security assessment without any high/medium vulnerabilities, it will not be eligible for production rollout. So, the tussle is about acceptance of the ranking of severities.

We have amicably resolved the previously mentioned situation with a review call and explained the business benefits of fixing the vulnerabilities. I also suggested multiple ways to handle the vulnerabilities in the code as well as in the security policies. It became a win-win situation for both the security tester as well as the project team.

As IS professionals, we must have good negotiation skills to resolve conflicts when there is disagreement about findings. We do not need to be masters of negotiations, but we need to practice these skills by communicating the business objectives, being more helpful and presenting the findings as a tool for improvement, not a fault-finding mission. The lesson is: With a little more empathy, both sides can reach an agreement quickly to better protect the information assets of the organization.

Read Sivarama Subramanian Kailasam’s recent Journal article: [“Measure and Monitor Application Security,”](#) ISACA Journal, volume 4, 2011



Feature News: An Introduction to Information Security Management in Health Care Organizations

While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information.

ISO/IEC 27002 is already being used extensively for health informatics IT security management. ISO/IEC 27002 provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security. ISO/IEC 27002 is a broad and complex standard, and its advice is not tailored specifically to health care. ISO 27799 allows for the implementation of ISO/IEC 27002 within health environments, in a consistent fashion and with particular attention to the unique challenges that the health sector poses.

Information Security Governance Within Clinical Governance

Until recently, the focus of protection has been on the IT systems that process and store the vast majority of information rather than the information itself. But, this approach is too narrow to accomplish the level of integration, process assurance and overall security that is now required. Information security takes a larger view that the content, information and knowledge based on it must be adequately protected, regardless of how it is handled, processed, transported or stored.

Health Information to Be Protected

There are several types of health information whose confidentiality, integrity and availability need to be protected:

1. Personal health information
2. Pseudonymized data derived from personal health information via some methodology for pseudonymous identification
3. Statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data
4. Clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g., data on adverse drug reactions)
5. Data on health professionals, staff and volunteers
6. Information related to public health surveillance
7. Audit trail data produced by health information systems that contain personal health information or pseudonymous data derived from personal health information, or that contain data about the actions of users with regard to personal health information
8. System security data for health information systems, including access control data and other security-related system configuration data for health information systems

The extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put and the risks to which it is exposed. Risk assessment can properly determine the level of effort needed to protect confidentiality, integrity and availability.

Health-informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. At the same time, the data they contain are confidential and their integrity must be preserved. Because of these critical requirements, and regardless of their size, location and model of service delivery, all health care organizations need to have stringent controls in place to protect the health information entrusted to them.

ISO 27799:2008 and ISO/IEC 27002 taken together define what is required in terms of information security in health care; they do not define how these requirements are to be met. That is, to the fullest extent possible, ISO 27799:2008 is technology-neutral. Neutrality with respect to implementing technologies is an important feature.

In the health context, information about individuals needs to be collected, stored and processed for many purposes, the main being:

- * Direct delivery of care, e.g., patient records
- * Administrative processes, e.g., booking appointments
- * Clinical research
- * Statistics

Data protection laws in many countries require that the data controller implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing of the personal data.

Application of best practices proposed by the international industry standard ISO 27799:2008 is no guarantee of compliance with legal obligations, but it may offer health care organizations a good starting point on the road to addressing international legal requirements for security in health.

ISACA® recently released:

- * [Geolocation: Risk, Issues and Strategies](#)—
Geolocation data, which reveal an individual's physical location, are obtained using tracking technologies such as global positioning system devices, Internet Protocol (IP) geolocation databases, and financial transaction information. This white paper explains how geolocation works and presents the business benefits and the risk, security and privacy concerns. The white paper also discusses the governance and assurance of applications using geolocation.

- * [COBIT® Mapping: Overview of International IT Guidance, 3rd Edition](#)—
This is an updated overview of the series of detailed COBIT® mapping publications, including mappings with Capability Maturity Model Integration for Development, Version 1.2; the US Federal Financial Institutions Examination Council; ISO/IEC 17799 and 20000; ITIL Version 3; US National Institute of Standards and Technology Special Publication 800-53 Revision 1; the Project Management Body of Knowledge; and The Open Group Architecture Framework 8.1.

- * [Audit/assurance programs](#)—
Business Continuity Management Audit/ Assurance Program and Microsoft® Windows File Server Audit/Assurance Program

Information on current research projects is posted on the [Current Projects](#) page.

Baton Rouge Chapter Information:

UPCOMING EVENTS:

November 16, 2011 @ 11:30am—Chapter Meeting on Advanced Persistent Threats (APT). Speaker: Srinivas Uppugonduri. Location: TBD

Additional information regarding location and registration will be coming soon!

Get to know a Member!

Michelle R. Seeling, ISACA Baton Rouge Chapter President

Q How did you get involved with your chapter board?

A *My boss at the time, Dana Dugas-Tarver was Vice President of the Baton Rouge Chapter and she highly encouraged serving on the board. I have been hooked ever since. And it has been the best career decision I have ever made.*

Q How many years have you been an ISACA Member?

A *I am approaching my 5th year! I finally get an award to showcase on my desk.*

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

A *We are in touch with the latest and greatest information which really sets you apart from the everyday IT organization. We are a dynamic field and this is VERY important.*

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

A *I was a student athletic trainer at Texas Tech University for football, baseball and track. And I love NHRA.*

Membership Announcements / Information:

- * *Anyone who joins ISACA on or after August 1, 2011 receives membership for the remainder of 2011 and for all of 2012. Individuals can learn more about and sign up to become members on the [Membership](#) page of the ISACA web site.*
- * *Baton Rouge Chapter Dues for 2012 - 2013 will be \$35*
- * *You may earn up to 20 continuing professional education (CPE) hours per year for working on ISACA® boards/committees—including active participation as an ISACA chapter officer. The CPE hours can be applied to each ISACA certification held. For details, please visit the [CPE](#) page of the ISACA web site.*