

May 2008



Newsletter

Serving IT Governance Professionals

Utah Chapter

Our Mission: Provide our members opportunities for career development and networking with peers. Advance and promote the profession by creating awareness of the skills and abilities of IT audit and security Professionals.

President's Message

Hello Utah ISACA members. We will be holding our one-day Spring seminar on May 22nd at Thanksgiving Point. Our speaker will be Steven Fox, and he will be presenting on the topic, "Developing and Implementing an Organizational Risk Assessment Process." This will be some great training at a great price. We hope to see you there.

"Developing and Implementing an Organizational Risk Assessment Process"

Speaker: Steven F. Fox

When: May 22, 2008

Time: 8:30 - 4:30

Where: Thanksgiving Point - Amber Room

(The amber room is located on the second floor above the North American Museum of Ancient Life)

Cost: \$250 for ISACA members

\$300 for non-ISACA members

*Member prices are also given to ISSA, IIA, and Students

Register: Go to <http://www.isaca-ut.org/utahevents.html> and follow instructions.

You must register by May 19th, so we can have an accurate count of how many people will be attending.

Speaker Bio:

Steven F. Fox has over 18 years experience consulting for educational institutions, nonprofit organizations, Big Three Motor Companies, and training providers. He is a published author and speaker addressing information security within the enterprise. He is the principal consultant and founder of secureLexicon LLC, a company specializing in vulnerability and risk analysis. He serves on the board of the Detroit ISSA chapter and works closely with the SE Michigan Information Security Regional Skills Alliance. Mr. Fox holds a Masters in Business Information Technology from Walsh College; an NSA designated Center of Excellence.

Have a great month,

Mark Murdock

Monthly Professional Training

Please see the above President's message on page 1.

Our next monthly luncheon will be held on Thursday, June 19th at the Lion House. This will be our Annual General Meeting. Come and enjoy a free lunch.

Earning CPE

ISACA e-Symposium

If you are in need of CPE credits, an easy way to earn them is by participating in an ISACA e-Symposium. These are free online web casts and you can earn 3 CPE credits. For further details, go to: www.isaca.org/webcasts

I found out from ISACA that there is no limit to the number of e-Symposiums or on-line quizzes that you can take to help fulfill your CPE requirements. If you have any questions concerning CPE credits please email the following:

certification@isaca.org and they will answer your questions.

International Training

More information is available at the following link: <http://www.isaca-ut.org/training.html>

From ISACA

ISACA has just released the new **IT Assurance Framework (ITAF)** as its latest member benefit. To meet the need for clear guidance for IT controls, ISACA has created this comprehensive assurance model incorporating standards and best practices. ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports. The framework also:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments;
- Defines terms and concepts specific to IT assurance; and
- Establishes standards, guidelines, and tools and techniques that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct and reporting requirements.

The current version of ITAF incorporates ISACA's IS Auditing Standards and Guidelines and allows for new guidance to be properly indexed as it is developed and issued. It is designed to be a living document to enable relevant tools, techniques, white papers and publications to be placed with the framework.

ITAF is applicable to any formal audit or assessment engagement. Its design recognizes that IT assurance professionals are faced with different requirements and different types of audit and assurance assignments—ranging from leading an IT-focused audit to contributing to a financial or operational audit.

ISACA is pleased to be able to offer ITAF to ISACA members as a complimentary PDF download from the ISACA web site. It can be purchased by nonmembers for US \$45.

For further information or to download the publications, visit www.isaca.org/itaf.

Failing an Audit

It is time to face the music when many of us must confront our executive team with the news that our organization failed an IT security audit. It is a moment of extreme embarrassment. But it is an event that is not that uncommon. Greater entities than ours suffer from security breaches. We would rather have the auditors find them than suffer headlines like these from www.Slashdot.com on April 15, 2008:

Apparently the folks at the Department of Corrections of Oklahoma just forgot to use common sense when they created the state's Sexual and Violent Offender Registry. By putting SQL queries in the URLs, they not only leaked the personal data of tens of thousands of people, but enabled literally anyone with basic SQL knowledge to put his neighbor/boss/enemies on the sexual offender list. Fortunately, after the author of the blog The Daily WTF notified the department about the issue, the site went down for 'routine maintenance' on April 13 2008."

Even major federal government organizations like the Department of Homeland Security (please note the position of the name of "security" in the name) earned a "D" in 2007 for their lack of IT security. Money-handlers are common targets for intrusions looking for phishing and vulnerabilities attacking the users of EBay and PayPal. Coding vulnerabilities are frequently found in Microsoft, and Oracle applications where there were based on earlier versions.

"Oracle has quite a few vulnerabilities, so they're now on a quarterly patch update process," said Ted Julian, vice president of marketing and strategy at Application Security, Inc., a leading provider of database security solutions. "Attackers have gone pro, and they're focusing on databases because that's where they can find data of value en masse." "Databases stand out as an obvious part of the infrastructure to highlight and include in the auditing process," Julian said.

So in reality that is the case for almost all systems organizations should simply plan on a security assessment discovering issues that affect business operations. Address them in a priority fashion by dedicating the necessary resources.

-List the vulnerabilities discovered by the audit. Design a plan to address them in priority manner. The audit will provide a significant amount of data. Decide the criticality of the vulnerabilities and which can wait. Determine the level of acceptable risk. Also determine ownership for the project and the deadlines for the project. Allocation for scant resources is essential.

-Determine the role of each task and assign each task to the appropriate manager or team. Be certain to follow up and set deadlines for completion. If necessary make certain to include SDLC and Change Controls if applicable. Additionally, make certain that resources are within bounds of budgetary and employee resources for each project.

-Set milestones for completion and when completed make certain the steps are made toward the goal have been made. Set report dates for status reports so delays are not issues.

-Once repairs to the systems have been started any reconfigurations and testing have been done make sure these are in line with policies. If your organization doesn't have the expertise to test the repairs to the systems, then hire the expertise and by all means make certain these professionals are indeed professionals.

Business systems are constantly developing and changing consequently security audits must be seen as a regular part of the business process. Once you repair a discovered security issues another is likely to arise, but as long as you are auditing regular assessments organizations can continuously improve their operations.

Alan B. Sternecker, CISA, CISM, CFE, CISSP is a consultant and is the author of Critical Incident Management, ISBN: 084930010X, published by CRC Press, www.crcpress.com. He has written numerous articles and regularly lectures regarding fraud and computer systems security auditing. He can be reached at absterneckert@yahoo.co

Journal Update

The Information Systems Control Journal is seeking articles for volume 1, 2008, to be issued in January 2008. The copy deadline for volume 1 is 24 September 2007, and the theme is **Dysfunctional Operations in IT**. For more information, please view the 2008 editorial calendar at www.isaca.org/journal or e-mail jblader@isaca.org.

Board of Directors and Officers

President

Mark Murdock
LDS Church
murdockma@ldschurch.org

Vice President

Julie Park
Weber State University
jpark@weber.edu

Treasurer

Brandon Brown
Deloitte & Touche LLP
brandonbrown@deloitte.com

Secretary

Kyle Finlayson
Intermountain Health Care
kyle.finlayson@intermountainmail.org

Newsletter/Publicity

David Gibson
Legislative Auditor General's Office
dgibson@utah.gov

CISA Coordinator

Jordan Fuller
Amedica Corporation
jfuller@amediacorp.com

Membership Director

Dan Anderson
IHC / GE Healthcare
daniel.anderson@intermountainmail.org

CISM Coordinator

Sod Chuluunbaatar
Deloitte & Touche LLP
schuluunbaatar@deloitte.com

Seminar/Education Chair

Kyle Chugg
America First Credit Union
Kyle.Chugg@questar.com

Academic Relations Chair

Jeff Davis
Weber State University
jtdavis@weber.edu

Research Chair

Angela Duff
Fiducian
aduff@fiducian.us

Webmaster

Ben West
Protiviti
ben.west@protiviti.com

The views and opinions contained in this publication are solely those of the authors, and do not necessarily represent or reflect the view or opinions of the Utah Chapter. In the event you have any questions concerning an article, you may wish to contact the author directly.