

February 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 having our regular monthly luncheon at the Lion House on Thursday, February 21st. Todd Brown from BYU Internal Audit will be speaking on COBIT. We hope to see everyone there. Just go to our Web site at <http://www.isaca-ut.org/utahevents.html> and sign up.

Our next monthly luncheon will be held on Thursday, March 20th. Also, we are planning on holding our Spring seminar in April. More information on these events will be coming.

As mentioned previously, our chapter is sponsoring the IT Summit conference held on April 16th in the Salt Palace Convention Center. As a sponsor, our chapter members can attend this conference for free. See more information about this conference on our Web site.

The next CISA and CISM exams will be held on June 14, 2008. If anyone is interested in our chapter setting up a review course for these exams, please contact Jordan Fuller (jordan.fuller@gmail.com) for the CISA exam or Sod Chuluunbaatar (schuluunbaatar@deloitte.com) for the CISM exam. We need about 7 people to show an interest before setting up the course. Please contact Jordan or Sod by March 15th.

Have a great month,

Mark Murdock

Monthly Professional Training

Date: Thursday, February 21

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Todd Brown, BYU

Topic: COBIT

Cost: Members- \$15, Students - \$15, Non-members - \$18

Please sign up via our web site: <http://www.isaca-ut.org/utahevents.html>

Menu

Sarah Salad

Lemon Thyme Chicken

German Chocolate Cake

Training Opportunities

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

Another way to earn CPE credits is by taking the Information Systems Control Journal CPE Quizzes that are online at:

http://www.isaca.org/Template.cfm?Section=CISA_Certification&CONTENTID=16839&TEMPLATE=/TaggedPage/TaggedPageDisplay.cfm&TPLID=58

Each quiz passed with at least 75% earns 1 CPE credit. There is no cost, which is hard to beat!

IT SUMMIT

For those interested, here is the information on the IT Summit:

“The IT Summit is the executive technology conference series coming to the Salt Palace on **April 16th, 2008**. The purpose of the conference series is to support the proliferation of information technology. Each conference features a full day of presentations, networking, and exhibits. We support certain non-profit IT organizations at no cost.

We propose to provide ISACA with complimentary admission for your members, promotion on the conference website, print work, marketing materials, and conference guide in exchange for promoting the event to your people. We hope you use The IT Summit as a membership drive vehicle.

Below, please see details from our annual Denver conference which took place on May 30th. I have included Denver details as an example because each of our programs is very similar. We welcomed 400 attendees in Denver.

More information is available at the following web link: <http://www.theitsummit.com>

International Training

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

Attention

If you did not receive your CPE certificate from the fall 2007 seminar, please contact Kyle Chugg at kchugg@americafirst.com and he will get it to you. Thanks

Here is a note for those who took the December CISA or CISM exam:

“ISACA is pleased to announce that the results from the December 2007 world-wide CISA and CISM exam administrations will be communicated shortly. Any candidate who previously opted for an email communication and does not have a balance due on their exam fee will receive this email notification by mid February. To ensure the confidentiality of scores, exam results will not be reported by telephone, fax or email other than the one-time pass/fail status and score notification email. The hard copy result letters will be sent out the week of 4 February 2008. Delivery outside of the USA can take as many as 21 business days.”

Training in Oklahoma:

Spring Seminars – March 31 – April 3, 2008
Information Risk Management and
Network Security Essentials
Oklahoma State University / Oklahoma City
Please see the attached pdf file in your email.

IT Auditing State of the Art

Having been a baseball fan/player for most of my life, the “I Ching” of IT auditing theory is summed up best by one of my favorite baseball diamond philosophers Yogi Berra when he said, “In theory, there is no difference between theory and practice. IT auditors serve stakeholders, executives, and managers that are seeking to assess and manage their risks. They select specialists in the form of IT auditors for their knowledge, skills and competence. These same entities are motivated by profit, boards of directors, customary practices, and legislation.

It is a fact of life that accounting practices for the most part have mandated audits of finances by auditors for the better part of two hundred years. However, in recent years we are seeing legislation requiring specialized professionals in the form of IT auditors to review and assess risks to computer systems. Auditing standards often are manifested in the form of ISO17799, COBIT GASSP while individual certifications are derived from ISACA, IIA, ISC2 or similarly recognized organizations.

As in the financial audit-world, IT auditors are usually deployed in spheres divided by external and internal worlds both tasked to provide a formal opinion about the state of the organization’s computer risks. IT auditors are primarily concerned with the integrity of the organization’s financial and accounting systems and to a lesser degree in supporting systems and related controls as a general rule.

Internal auditors are employed examining and commenting on the controls and processes present in the organization on an ongoing basis. Their review usually extends beyond the financial processes encompassing governance and controls. However, both have a common interest in the financial and related systems as well as the internal controls. The internal auditors will be the more likely of the two to review the attendant systems. Like it or not, external auditors are influenced by the work done by the internal auditors. However, it is the external auditors that answer the question, “who audits the auditors.”

Closely related to the field of IT auditing is information security as it is a field containing the areas of risk and controls relating to computer systems. Consequently, IT auditors must have a knowledge of computer, network, and telecommunications systems. Being immersed in IT-based risks, security controls and their related governance matters generally lends credibility to IT auditors. It is incumbent on auditors to obtain formal education and formal qualifications such as the CISA certification. But softer skills are also a distinct advantage in the form of interviewing skills. Many lack prowess in this area. They have advantages in understanding technical risks but fail when they meet actual personalities and are unable to conduct meaningful interviews.

For the most part, IT audits follow this process:

-Audit schedule. The organization decides which parts of the organization is subject to an audit, planning, when the audit is going to be scheduled and the rules of the audit. The timeframe is set, resources are allocated and scope of audit is enumerated.

-Scope and pre-audit survey. Auditors determine the areas of focus and form of risk based assessment is performed. Information sources, documentation reviewed (previous audits) and at times subjective impressions explored. Rules of engagement are crafted.

-Audit Planning and Preparation. Audit scope is divided into levels for audit team detailing audit work plan, checklist, risk control matrices, etc.

-Fieldwork. Evidence gathered by audit staff members, reviewing documents, data and observation. Computer Aided Audit Techniques might be deployed here.

-Analyses of collected evidence collected. Knowledge base and audit decision techniques may be used at this step.

-Reporting audit process. Often the reporting process is given preliminarily during the audit process, but this is part of the rules of engagement. This report is delivered orally and followed by a readable written report. Findings are succinct. If there are any suspicious activity this is reported immediately to authorities.

-Closure. Disclosure of work papers and notes. All work papers and note are organized and deposited with the stakeholder as documentation. Determine if stakeholders request follow-up audit and determine if stakeholders are satisfied with work product actively seeking response to work product.

Auditors must be able to be observant in the identification of actual and potential risks associated with systems, development, installations and applications. And more often than not, auditors must be able to articulate whether these risks are actual or not and potential for these risks impact for these risks and correctly identify which systems/applications are affected. For the auditor this competency means she must be able to reach between the two worlds of technology and business processes. More importantly it translates to words that the IT auditor must express to the stakeholders. Then armed with this understanding, the stakeholders should prioritize the auditors' findings and take remedial action. This is the burden of the auditor. If found to be flawed the fault belongs to the auditors not the process.

Alan B. Sternecker, CISSP, CISA, CISM, CFE 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.com

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
América 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
kchugg@americafirst.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.