

Oct. 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 regular monthly luncheon at the Lion House on Thursday, October 16th. Dan See, from Microsoft, will be speaking on IT Security. We will also be holding our one-day Fall seminar on November 21<sup>st</sup> at Thanksgiving Point. Our speaker will be Ralph Bonnell, from FishNet, and he will be presenting on the topic, "Linux Security and Audit Fundamentals." This will be some great training. We hope to see you at both of these events.

## “Linux Security and Audit Fundamentals”

By FishNet Security  
(Utah ISACA 2008 Fall Seminar)

- Speaker:** Ralph Bonnell, CISSP  
**When:** November 21, 2008  
**Time:** 8:30 - 4:30 (7 CPE credits)  
**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, students, & affiliated chapters (ISSA, IIA)  
\$300 for non-ISACA members
- Register:** Go to <http://www.isaca-ut.org/utahevents.html#fallseminar>.  
**Payment:** Check, Visa, or MasterCard accepted  
(If paying by check please send to Dan Walker, Utah ISACA Treasurer • PO Box 11154 • SLC, Utah 84147-0154)

**Chapter Email:** RSVP to David Gibson at [utah.isaca.chapter@gmail.com](mailto:utah.isaca.chapter@gmail.com)

**Registration Deadline:** November 17th at Midnight MST

**Questions:** Email Kyle Chugg at [kyle.chugg@questar.com](mailto:kyle.chugg@questar.com)

**Register right away to hold your spot and to be eligible for great training and prizes!**

### Speaker Bio:

Ralph Bonnell is an instructor for FishNet Security and has over 10 years of experience in the computer networking industry. Mr. Bonnell holds over 20 industry-related certifications, including CISSP, CLPIC-2, and JNCI and has a proven track record with knowledge in a wide variety of technologies. He has built complete networks from the design stage to implementation, and his accomplishments have been noted in several publications. Mr. Bonnell continually works toward his depth of knowledge and skill base to insure he is always up-to-date in the information security industry.

Our next monthly luncheon after the Fall seminar will be held on Thursday, December 18<sup>th</sup> at the Lion House. More details will follow.

Have a great month,

Mark Murdock

## Monthly Professional Training

Date: Thursday, Oct. 16th  
Time: 11:30 – 1:15 pm.  
Place: Lion House  
Speaker: Dan See from Microsoft  
Topic: on IT Security  
Cost: \$15 for members and students, \$18 for all others  
CPE: 1 Credit

Email: [utah.isaca.chapter@gmail.com](mailto:utah.isaca.chapter@gmail.com)  
Include the first and last name with e-mail address for each attendee you are registering.  
Please **RSVP** to David Gibson by noon on 9/16/2008

### Menu

Sarah Salad  
Pork chop w/Mushroom Gravy  
Cherry Pie

## **Monthly Training Registration**

The cutoff time period to sign up for the professional lunch meeting is the Tuesday before the monthly Thursday meeting. If you sign up after noon on Tuesday, you may or may not have a guaranteed seat. Since the rooms at the Lion House are small we have to give them a hard count by Tuesday at noon to reserve a room. Thanks

## **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](http://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](mailto: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>

## **Other Training Opportunities**

Upcoming ACFE Anti-Fraud Course in Salt Lake City

Topic: Introduction to Digital Forensics

Date: Oct 27-28, 2008

Place:

Hilton Salt Lake City Center

255 S. West Temple

Salt Lake City, UT 84101

### **Cost:**

Member: \$795

Non-Member: \$945

Register by September 27 and SAVE \$95\*\*!

### **CPE Credit**

16

Course Details<<http://eweb.acfe.com/./eweb/DynamicPage.aspx?webcode=topicdesc&topkey=4ee0d451-82b5-4ef8-9fea-06008ef34c99>>

View the Course Outline <<http://www.acfe.com/training/IDFSchedule.asp>>

### **Course Level**

Basic

This two-day course will introduce the fraud examiner to basic concepts of computer forensic investigation and analysis. In this instructor-led course the attendee will learn basic techniques involved in gathering and analyzing digital evidence in fraud examinations, as well as the proper procedures for seizing and securing digital evidence. A software demonstration will also allow you to examine forensic artifacts. The speaker for the course will be James J. Butterworth<<http://www.acfe.com/about/bio-jbutterworth.asp>>.

# Internal IT Audit Charters

Often internal information technology (IT) audit units do not have charters or they have charters that were crafted so long ago they are out of date from their business functions. There are times in which the audit unit is not clear to whom they report their findings or exactly what their objectives are. The internal IT audit charter functions as a guide and as an informant upon which members and executives can rely.

Charters must be plainly written avoiding techno-speak, and jargon specific to the field. Acronyms must be clarified at every opportunity. Throughout there should be an attempt to use language that is explanatory and yet does not “speak down” to the reader.

When drafting charters is wise to include information from interviews of executives, audit committee members, steering committee members and various levels of users so they might include their thoughts about relevant topics as vulnerabilities and risks affecting the business organization, auditor qualifications, internal audit authority, audit frequency, ethics, and audit objectives.

Charters must include pattern language so auditors have degree of benchmarking. This level of benchmarking can be as simple as a survey conducted at the conclusion of their audit giving the auditors a metric of their performance. This quantitative measurement can then be compared with previous performance levels in other audits.

There are many patterns for audit charters, but none are sufficiently complete so they might be considered inclusive in business applications. Nevertheless here is some pattern language for a sample charter:

## **Introduction**

The purpose of this charter is to establish the Internal Audit position within My Business Organization, authorizing its access to systems, records, personnel and physical properties relevant to the performance of audits and define the scope of IT Internal Audit activities.

## **Objective of IT Internal Auditing**

The objective of IT Internal Auditing is to assist management and end users in the effective and efficient discharge of their responsibilities. To this end, the IT Internal Audit function furnishes management with analyses, appraisals, recommendations, and information concerning reviewed activities to promote effective control.

## **Authority of Internal Audit**

IT Internal Audit reports administratively to the Chief Information Security Officer (CISO), however it may report directly to the Chief Executive Officer of members of law enforcement depending upon circumstances.

In the performance of audits, IT Internal Auditors are granted access to all business activities, records, property and employees. IT Internal Auditors shall exercise discretion ensuring the safekeeping and confidentiality of relevant audit and business matters.

The IT Internal Audit is a distinct business staff function and as such has no direct responsibility for, or authority over, any of the activities reviewed.

Because performance of line responsibility may compromise objectivity, the IT Internal Audit shall not perform non-audit related work.

## **Responsibility of Internal Audit**

-The Internal Audit function has the following responsibilities:

-Review, analyze and evaluate the adequacy, efficiency and effectiveness of the organization's system of internal controls and the quality of performance.

-Review the reliability and integrity of computer, networking system and operating information and the means used to identify, measure, classify, and report such information. These systems include vulnerabilities, risks, attendant safeguards, and internal controls.

-Review the systems established to ensure compliance with statutory, regulatory and organizational policies, plans, procedures, laws, and regulations that could have impact on operations and reports, and determine whether the organization is in compliance.

-Serve on related committees as appointed or elected.

-Participate in or conduct evaluations, IT and management studies, special audits and fraud investigations as directed.

-Maintain technical competence through continuing education and active participation in professional activities.

## **Fraud/Abuse of Resources**

Internal auditors should have sufficient knowledge to be able to identify indicators that fraud and abuse may have occurred. If sufficient control weaknesses are detected, additional tests conducted by internal auditors should include tests to identify other indicators of fraud and abuse.

Internal auditors are not generally expected to have knowledge equivalent to a person whose primary responsibility is to detect and investigate fraud and abuse.

Internal Audit will assist in the investigation of fraud and abuse in order to:

-Determine if controls need to be implemented or strengthened.

-Design audit tests to help disclose the existence of similar frauds in the future.

A written report will be issued at the conclusion of each investigation. It will include all findings, conclusions, recommendations, and corrective action taken. Upon discovery of unlawful activity, specific reporting will be made to executives and a parallel report will be made to law enforcement authorities in a timely fashion.

# **IT Duties and Responsibilities**

## **General Responsibilities of the IT Internal Audit Function**

- Manage the IT Internal Audit function.
- Develop and obtain proper approval for goals, audit work schedules, staffing plans, and financial budgets for the IT Audit Unit.
- Perform individual audits according to the IS Auditing Guidelines issued by ISACA.
- Maintain audit staff proficiency by obtaining an adequate amount of continuing education.
- Supervise staff auditors by assigning which match their abilities, reviewing their work, and appraising their performance.
- Conduct scheduled and special audits making recommendations for improvement.
- Keep current on trends in IT technology, systems and auditing.
- At the conclusion of each audit the audited personnel will be required to complete a questionnaire determining measuring the effectiveness and efficiency of the audit. These data will be reviewed with appropriate executive levels.

## **Preparation for the Audit**

- Develop and discuss audit objectives with the CISO.
- Perform field surveys touring the facilities to provide exposure to the relevant business operations.
- Develop an audit program which will provide a thorough review of IT operations.
- Conduct an entrance conference with applicable audit staff to explain audit objectives and the areas to be audited.

## **Conduct of the Audit**

- Perform the audit in a professional manner and in accordance with the approved audit program.
- Revise audit programs as appropriate to make them apply to the audit to be performed.
- Demonstrate sound judgment and reasonableness in the application of audit principles and procedures.
- Develop specific audit techniques and procedures for assigned areas when necessary.
- Prepare neat, legible, and accurate work papers. Indicate the source of information and purpose of the work performed.

- Schedule contacts with the audited officials and employees on matters relative to audit assignments so they are not unnecessarily disrupted.
- Maintain an amicable yet professional relationship with audited personnel.
- Carefully handle department systems and records.
- Safeguard work papers and taking care not to disclose matters of a confidential nature.
- Discuss findings and recommendations with the CISO before the relevant audited managers.
- Keep audited personnel aware of audit findings and recommendations so required improvements might be started as soon as possible.

## **Completion of the Audit**

Prepare a draft audit report, review it with the CISO making desired changes and provide it to audited management for their review at least one week prior to the exit conference.

- Conduct the exit conference with the audited managers.
- Work with the CISO on the final draft of the audit report.
- Determine whether work papers are complete and ready for filing. This effort includes indexing and cross referencing final reports to the work papers. All work papers must be deposited at the audited business unit before the auditor's departure.

## **Qualifications**

Education:

A bachelor's degree is required, however advanced degrees and certifications are preferred such as CISM, CISA, CFE and CISSP.

Experience:

Five years experience at the in-charge auditor level or higher to be an audit manager.

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](http://www.crcpress.com). He has written numerous articles and regularly lectures regarding fraud and computer systems auditing. He can be reached at [absterneckert@yahoo.com](mailto: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](http://www.isaca.org/journal) or e-mail [jblader@isaca.org](mailto:jblader@isaca.org).

## Board of Directors and Officers

### President

Mark Murdock  
LDS Church  
[murdockma@ldschurch.org](mailto:murdockma@ldschurch.org)

### Vice President

Julie Park  
Weber State University  
[jpark@weber.edu](mailto:jpark@weber.edu)

### Treasurer

Dan Walker  
Deloitte & Touche LLP  
[danwalker@deloitte.com](mailto:danwalker@deloitte.com)

### Secretary

Kyle Finlayson  
Intermountain Health Care  
[kyle.finlayson@intermountainmail.org](mailto:kyle.finlayson@intermountainmail.org)

### Newsletter/Publicity

David Gibson  
Legislative Auditor General's Office  
[dgibson@utah.gov](mailto:dgibson@utah.gov)

### CISA Coordinator

Jordan Fuller  
Amedica Corporation  
[jfuller@amedicacorp.com](mailto:jfuller@amedicacorp.com)

### Membership Director

Chuck Sims  
BYU  
[Chuck@byu.edu](mailto:Chuck@byu.edu)

### CISM Coordinator

Sod Chuluunbaatar  
Deloitte & Touche LLP  
[schuluunbaatar@deloitte.com](mailto:schuluunbaatar@deloitte.com)

### Seminar/Education Chair

Kyle Chugg  
Questar  
[Kyle.Chugg@questar.com](mailto:Kyle.Chugg@questar.com)

### Academic Relations Chair

Jeff Davis  
Weber State University  
[jtdavis@weber.edu](mailto:jtdavis@weber.edu)

### Research Chair

Dan Anderson  
Intermountain Healthcare  
[Daniel.Anderson@imail.org](mailto:Daniel.Anderson@imail.org)

### Webmaster

Ben West  
Protiviti  
[ben.west@protiviti.com](mailto: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.