

Control Bits & Audit Bytes

Western Michigan *INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION* Newsletter

JANUARY 2001 NEWSLETTER

OFFICERS

PRESIDENT

Rick Cummings, CISA
Jackson National Life Insurance Co.
One Corporate Way
Mailstop S38
Lansing, MI 48951
517 / 367-4301
FAX: 517 / 394-1795
rick.cummings@jnli.com

VICE PRESIDENT

James Green, CISA
Arthur Andersen
Technology Risk Consulting
Suite 700
171 Monroe Avenue NW
Grand Rapids, Michigan 49503
(616) 653-8364
FAX: (616) 653-6305
james.a.green@us.arthurandersen.com

SECRETARY

John Blair, CISA
Steelcase, Inc. CH-3E-18
P.O. Box 1967
Grand Rapids, MI 49501-1967
616 / 246-4730
FAX: 616 / 248-7550
jblair2@steelcase.com

TREASURER

Pam Bradford, CISA
National City, K-A16-C7
One National City Pkwy
Kalamazoo, MI 49009-8002
616 / 376-7523
FAX: 616 / 376-4408
Pam.bradford@national-city.com

BOARD OF DIRECTORS

CISA COORDINATOR

Michael Sekoni, CISA
Accident Fund of Michigan
P.O. Box 40790
Lansing, MI 48901-7998
517 / 342-4200 ext. 721
FAX: 517 / 342-4299
michaels@accidentfund.com

NEWSLETTER EDITOR

Rick Cummings, CISA
Jackson National Life Insurance Co.
5901 Executive Drive S52
Lansing, MI 48911-5389
517 / 367-4301
FAX: 517 / 394-1795
rick.cummings@jnli.com

PAST PRESIDENT

John Arens, CPA
Meijer, Inc. MC 985/4
2929 Walker Avenue NW
Grand Rapids, MI 49544-9428
616 / 791-3521
FAX: 616 / 791-5341
arensj@meijer.com

DIRECTOR AT LARGE

Kim Coyer
Independent Bank Corporation
623 Washington Ave
Bay City, MI 48708
(517) 892-3511
kcoyer@ibcp.com

February Dinner Meeting

ENTERPRISE SECURITY MANAGEMENT

By Ed van Essen, Senior Manager, Secure e-Business, Deloitte

February 21, 2001

Sheraton Lansing @ I496 and Crytes Rd.

The traditional relationships between corporations and their employees, customers, suppliers, and business partners are changing rapidly under the influence of the Internet and the World Wide Web. The Web enables delivery and access of more information and new types of services, while the once clear line between corporate information technology and public resources is getting fuzzy. The corporate IT environment must now support instant access to a large number of services and resources, from employee support applications to integrated supply chains to interactive, on-line customer services, while maintaining an environment where the right information reaches only the right people. This presentation will focus on the security issues that are a result of these seemingly contradictory requirements. From a technical perspective, we will highlight the capabilities of some of the software solutions that are specifically built to address these issues and that are available from major vendors like IBM and Novell today

Speaker BIO

Ed van Essen has been with Deloitte since 1998 and is a Senior Manager in our Secure e-Business group in Detroit. He has over 15 years experience in information and communication technology. Since joining the Firm he worked within the group that specializes in security solutions for complex network environments including secure e-business solutions. Ed is a network system engineer (MCSE), specializing in secure Windows NT based solutions in large heterogeneous networks, e-Business technology architecture, information systems control and security.

Please make your reservation now!

Call John Blair and make your reservation today!! **(616) 246-4730**

OR e-mail John at jblair2@steelcase.com

Costs - \$25 Non Members / \$22 Members

4:00 5:00 Board Meeting

5:00 5:30 Social Hour / Registration

5:30 6:30 Presentation

6:30 7:30 Dinner

Presidents Message

Happy New Year to all Western Michigan Members,

Let me begin with a special note on the February Dinner Meeting. The date has changed from February 14th (Valentines Day) to February 21st. Please remember to note this on your calendar.

The chapter has certainly had its challenges the past few months in securing speakers that can provide valuable topics in the short time frame required for a dinner meeting. In the past two newsletters, the chapter has been begging for membership input to the future of the presentation quality, format, timing, etc. The Western Michigan chapter is here for the members, and it is up to the member to help the board in directing the chapter activities. I must say that the suggestions and input from the membership body is less than desirable.

PLEASE, HELP US IN PROVIDING YOU, THE MEMBERSHIP, THE QUALITY PROGRAMS AND SUPPORT YOU DESIRE FROM YOUR CHAPTER. Any suggestion and or comments on how we can improve the chapters' activities, we ask that you please share your ideas with any of the Officers noted on the front of this newsletter.

Speaking of chapter improvements, Volunteering is a great way to make a difference in your chapter!!

We are beginning to seek nominations for Chapter Board Position for the 2001/2002 season. Everyone is encouraged to submit nominations (including yourself) for any one of the Officer positions on the Board. All positions are for a one-year tenure. The Officer positions are elected positions, and the Directors are volunteers which are appointed by the board. Positions that we are looking for nominations are President, Vice President, Treasurer and Secretary. Volunteers are also needed for the Board appointed positions of 'Director at Large' and 'CISA Coordinator'. Here is a chance to have a direct influence on how your board serves its membership!! We will be providing a list of duties for each position in the next newsletter or separate mailing. If you are interested in helping the chapter (and receiving extra CEU for certification), please send your nominations to the Official Election Officer, Mike Grinwis at Michael.Grinwis@jnli.com. Please support your local chapter by nominating a fellow member or volunteering your own services.

The March meeting, IT Governance, will also be held in Lansing at the Sheraton. The date is March 14th, so mark your calendars!!

Seminar – We are continuing to develop the Spring Seminar. We are currently looking at two excellent presentations on "Privacy". Once we select who will present the seminar, we will further define the detail content and objectives of the seminar. The following information has been determined:

Where – National City, Kalamazoo Michigan (Same as last year)

When – April 19 and 20

We will be providing additional information as it becomes available

Welcome to the New Year and we look forward to seeing you at the next meeting.

Rick Cummings

Internal Audit "Helpers" Newsletter from Audit Services

Some more ideas to "help" you, the professional internal auditor! If you have any difficulties accessing the web pages directly from this email, the newsletter is also posted on our web site at: www.auditservices.com/helpers.html

Let us know if we can be of any help.

XX

AUDITING THE INTERNET, E - BUSINESS/COMMERCE

Going to audit firewalls? For some ideas when auditing firewalls (evaluating functions, criteria used in selecting, classes of firewalls used, etc.), go to our web page, <http://www.auditservices.com/itfwall.html>

XX

AUDIT REPORTS

Required: accurate and timely reporting! However, it is also important to remember that reporting should reflect the thinking, attitude and competence of the auditor and understanding of the audience. For some ideas on how to better understand your audience go to <http://www.auditservices.com/arptcust.html>

XX

SAMPLING

Statistical sampling is either going to be an "attributes" or a "variables" test. Know when to use an attributes test? Remember the different types of attribute sampling models? For a "refresher", go to <http://www.auditservices.com/ssatt.html>

Also, go to <http://www.auditservices.com/ssindex.html> for an outline of our one day Sampling Seminar.

XX

INTERNAL CONTROLS

What is meant by "soft controls"? Have you ever audited soft controls? For some ideas on reviewing soft internal controls, <http://www.auditservices.com/icsoft.html>

XX

AUDIT PROGRAMS

Audit programs need to be adjusted/designed for each engagement. The success or failure of an audit engagement can depend upon an audit program that is properly designed and focused. For more, <http://www.auditservices.com/aprog.html>

XX

ASSESSING RISK

Trying to quantify business risks? Determine the significance of the potential risks and resulting consequences identified, without considering controls. For some ideas go to <http://www.auditservices.com/rquant.html>

XX

CERTIFIED INTERNAL AUDITOR (CIA) EXAM

Go to <http://www.auditservices.com/ciasch.html> for a list of our CIA Exam Review Course sites. Additional CIA related information, including a list of some test-taking techniques can be found at <http://www.auditservices.com/cia.html>

XX

Have a nice day,

Roger

www.auditservices.com

615-790-9858

The “Write” Stuff???

By M. B. Grinwis, CISA, CDP

Are you ***REALLY*** watching what you write?

Or are you just letting your spelling and grammar-checker do the work for you?

When you write a report, opinion, or other business communication, what are you ***really*** trying to do? You’re trying to persuade the recipient(s) to see your viewpoint and/or implement those actions which you are recommending. To accomplish this, you meticulously craft your words and phrases in order to convince the reader(s) that it is in their best interest to make those changes you recommend. At least, that’s what you think (hope) you’re doing . . .

Unfortunately, many of our best written efforts are being circumvented by the automated tools we’ve implemented to help ensure their success. How many times have you agonized over the wording of a draft document, only to unknowingly have the intent of those well thought-out words and phrases tossed asunder by blindly accepting the first suggested correction your automated spelling and grammar checking software lists? None, you say? Think again.

All automated spelling and grammar checking systems use a base “dictionary” of ***commonly used*** words and/or phrases. How extensive that “dictionary” is, is dependent upon the system. Many also include a “custom dictionary”, which is a separate file in which you can add words specific to you, your work, your profession, etc. (Ever tried spell-checking “auditee” or “workpaper”?) The “checking process” compares what you’ve written to these “dictionaries”. Any word or phrase that doesn’t match causes the system to stop and display a list of “suggested corrections” — those words or phrases in these “dictionaries” which come the closest to matching your text. The caveat to this process is that the first “suggested correction” is *not* necessarily the correction you want. Unfortunately, we too often blindly accept that first offering as correct, replacing a misspelled word with a correctly-spelled word that radically alters the intent of our message.

The following is a reproduction of the beginning of an actual letter I received from a Grand Rapids mortgage company:

DEAR, FUTURE CLIENT

Do to research by our professionals we have found that most people with your position may not need a stack of credit saving proposals sent to you weekly, but we also no that saving you more money write now is wonderful!! Please take a look at three of the benefits our company offers to you.

So, how many errors did you find? I typed this using both Microsoft® Word® 97 and Word® 2000, and both of these spelling and grammar checkers said that there are NO errors. But is it ***really*** correct? NO WAY!!!

The late Malcolm Forbes wrote an excellent article on business writing. In it, he said the best communications are direct. Tell the reader exactly what you want, why you want it, and express it in terms that they can easily understand. Don’t embellish it with “fluff” — don’t waste their time. When you’re done, set it down and leave it for awhile. Then come back later and read it anew. Is it still clear? Concise? Does it communicate what you really want to say?

Good communications are like anything else of quality — it takes time and effort. You’ve started the process by writing the document. Complete it by ***consciously reviewing*** what you’ve wrote.



SECURITY PERSPECTIVES

*THE ORANGE BOOK IS DEAD, LONG LIVE THE COMMON CRITERIA?

By Ben Rothke

A wake was held at the Computer Security Applications Conference in December, but don't think it was a gloomy event, as music played and spirits flowed. It was not for a person; rather, this send off was for the Orange Book, a security standard that was recently pronounced dead (though some would argue it had been lifeless since conception).

The Orange Book, officially titled the Trusted Computer Standards Evaluation Criteria (TCSEC), was the most noteworthy part of the Rainbow Series (<http://www.radium.ncsc.mil/tpep/library/rainbow>) of security standards developed by the U.S. Department of Defense in the early 1980s. It defined seven security levels for trusted hardware, software and data components of a system, namely:

1. Verified design, which demands the highest level.
2. Formal security verification methods to ensure that security controls can protect classified and other sensitive information
3. Mandatory protection, specifying that the Trusted Computer Base (TCB) protection systems should be mandatory, not discretionary.
4. Discretionary protection, which applies to the TCB with optional object (e.g. file, directory, devices) protection.
5. Minimal protection, reserved for systems that have been evaluated, but have failed to meet the requirements for a higher evaluation class (operating systems such as MS-DOS and Windows 95/98 fall into this category).

The Orange Book's noble goal was to provide a level of measurement and guidance in designing secure systems. So why did corporate America turn a blind eye to it? Some of the reasons include:

--Information security standards are inherently difficult to create. Imagine thousands of companies from scores of different sectors, all with different needs, attempting to formulate a common security framework.

--It was designed for government installations, not corporate networks. The security threats, vulnerabilities and requirements of the government and military are radically different from those of corporate America.

--It's based on the 1973 Bell-LaPadula model, which was the first mathematical model of a multilevel secure computer system. Such formal systems simply don't scale well in corporate environments because they don't really address many day-to-day security concerns outside the military sphere. The most significant flaw is the omission of a solidly defined initial secure state and problems with the concept of what exactly constitutes a user.

--The Orange Book, expressly designed for standalone systems, was doomed by the advent of client-server computing. With today's systems connecting users to varied intranets, extranets and the Internet, a standalone host in today's world offers a lot of security, but little functionality.

Seeing the deficiencies in the Rainbow Series (and the fact that most government facilities failed to implement them), the DoD made several attempts over the years to update the standards, but they never got beyond an initial draft. At that point, the designers forgot W.C. Fields' adage "If at first you don't succeed, quit. There's no use being a damn fool about it." Ignoring this pearl of wisdom, the National Institute of Standards and Technology (NIST) joined forces with their counterparts at the European Commission (http://europa.eu.int/comm/index_en.htm) and entered into the Common Criteria (CC) Initiative (<http://www.commoncriteria.org>) in 1993.

The CC is collectively an ISO, based on the Europe Information Technology Security Evaluation Criteria. Officially started in 1993, the CC was designed to bring security standardization efforts together into a single international standard. Providing a general model of assessment by defining general concepts and principles of security evaluation, it also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. Despite all of the interest that the CC is garnering in the government sector, corporate America is still ignoring it.

What does the CC offer that the Orange Book didn't? In truth, not much--certainly nothing that is persuading corporate America to embrace it. The CC, like the Orange Book, is heavy on generalities, but light on specifics. If you want to know how to securely deploy H.323 applications on a Cisco PIX, or how to configure a Microsoft proxy server to interoperate with Check Point's FW-1, don't look to the CC.

The fault doesn't lie within the CC; rather, it reflects the reality that any attempt to both quantify and standardize present-day information security is a digital violation of the Heisenberg uncertainty principle in quantum mechanics. Just as the position and momentum of an electron can't be measured simultaneously, neither can information security be both codified and standardized. Unfortunately, infosec changes far too quickly to be etched in stone. In this dynamic environment, it's only a matter of time before we ask, "When shall we hold a wake for the Common Criteria?"

BEN ROTHKE, CCO, CISSP (ben.rothke@baltimore.com), is a senior security consultant with Baltimore Technologies.

Job Market

Hello- my name is David James, I am the president of David James Search. We are a search firm who for the past ten years has been dedicated to the advancement and placement of Internal Audit professionals. In the year 2001, there was a calculated decision made that the focus would be on and in the area of Information Technology and I.T. audit related search.

Unlike most recruiters, I have decided not to post an erroneous position that does not exist in an attempt to get you to send me a resume. However, what I do want is to invite you to initiate a relationship. If you need or want a better position, for any reason, please call me or email me at david@davidjamessearch.com .

Or- If you are in need of a person for your department, please feel free to contact me as well.

Most respectfully,

David L James

909-719-1484

Opportunities

InfoSec World Conference and Expo/2001

"Topics geared to changing technologies and the changing needs of infosec professionals"
February 26–28, 2001 — Disney's Coronado Springs Resort, Orlando, Florida
Contact: MIS Training Institute — www.misti.com, E-Z Access # OS01

INTERNET PAYMENTS

"How to Drive Profitability, Increase Market Share and Improve Customer Relationships
March 13–14, 2001 — The Sunburst Resort, Scottsdale, AZ
By Implementing an Effective Internet Payment System"
Contact: eBillXchange — www.ebillx.com

RSA Conference 2000

"The Industry's premier data security and cryptography event"
April 8–12, 2001 — Moscone Center, San Francisco
Contact: RSA Security, Inc. — 1-425-544-9306

Electronic Commerce World 2001 Conference & Exhibit

May 29 – June 1, 2001 — Santa Clara Convention Center, Santa Clara, CA

Contact: Electronic Commerce World — www.ecmediagroup.com

Final Words

**Don't Forget.....
February Dinner Meeting**

**DATE CHANGED TO FEBRUARY 21, 2001
Lansing Sheraton @ I496 & Crytes Rd.**

Control Bits and Audit Bytes is a publication of the Western Michigan Chapter of the *Information Systems Audit and Control Association (ISACA)*. The purpose of this publication is to disseminate useful and timely information on automated systems control and security issues to Chapter members and selected practitioners of computer systems audit and security. Articles, submissions, and advertisements are the responsibility of the submitter, and do not reflect the opinions, beliefs, or practices of the Western Michigan Chapter.

Materials submitted for publication in *Control Bits and Audit Bytes* must be received by the Newsletter Editor no later than the submission deadline published in the newsletter. If no submission deadline is published, the default deadline is approximately three weeks prior to the next scheduled meeting of the Western Michigan Chapter of the *Information Systems Audit and Control Association*.



*Information Systems
Audit and Control
Association*