

# **CONTROL BITS**

**AND**

# **AUDIT BYTES**

The Newsletter of the Western Michigan Chapter

*INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION*

E MEETING ANNOUNCEMENT ]

## **DATA WAREHOUSING**

What every enterprise feels they need! But,...what about who is looking at the data stored? what kind of data is being presented to the enterprise? Is there any real Business benefit? How is it different from reporting and archiving? Meta Data...????????????????

Mr. Bob Savage will attempt to answer these questions in the upcoming November Chapter Meeting. Bob's presentation will be organized to conform to the Chapters Program Guidelines and will cover the following areas:

✓ Risks (what can go wrong); ✓ Mitigation (what keeps bad things from happening; ✓ Steps to test controls (how do we check the process for controls); ✓ How-to or fixes (process for developing controls); and ✓ Question/Answer (discussion of how we do it and what works or does not work)

### **SPEAKERS BIO**

Bob Savage is a frequent presenter on the topic of data warehousing. He has 20 years of IT experience embracing a variety of responsibilities including database administration, data warehousing, systems programming and project management. In his current position at Steelcase, he provides technical leadership for a team of 10 database administrators, and has "data management" architectural responsibility.

As an accomplished ToastMaster, Bob participated in the "International Serious Speech" competition placing among the top ten speakers in the country. Bob is also active in a number of user groups and is a recent past President of the West Michigan Oracle User Group.

When: Wednesday, November 17th, 1999

Where: Duba's Restaurant — I-96 & East Beltline, Grand Rapids

Cost: Members, AITP, IIA: \$ 22.00 — Non-members: \$ 25.00

**R.S.V.P. John Blair @ (616) 246-4730** — NO LATER THAN Monday November 15<sup>th</sup>  
at High Noon! (or else Pardner)

Be sure to tell him whether you're a member, and what your meal preference is!

---

**REGISTER NOW!!! SPACE IS LIMITED!!!**

---



## Upcoming Events

- Chapter Meeting ..... Wednesday, November 17, 1999  
Topic: Data Warehousing ..... Duba's Restaurant, I-96 & East Beltline, Grand Rapids
- Detroit ISACA Chapter - ..... November 16, 1999  
Auditing E-Commerce Applications (pre-Dinner)  
Auditing the Corporate Intranet (post-Dinner)
- Detroit ISACA Chapter - .....December 13, 1999  
Joint Meeting w/ IIA) World Headquarters, Dearborn  
TBA (provided by IIA) (pre-Dinner)  
Hackers & How to Fight Back (post-Dinner)

---

## Bits & Pieces

by Michael Grinwis

It's an unfortunate fact of life that we tend to receive far more too many newspapers, magazines, e-mail, flyers, Post-It® notes, etc. covering more topics than Mr. Wrigley ever envisioned flavors. And so, we tend to miss many a good piece of information just from being overwhelmed by the mass of communication that regularly lands in our laps. Several such articles have come this way in the past couple of weeks, which you should be aware of:

### E-Commerce Security

(www.infosecnews.com)

SC INFOSECURITYNEWS MAGAZINE

November, 1999, pp. 18-20

- Providing proper controls over e-commerce is quite a challenge. This article addresses the current top crop of automated tools (i.e. virus checkers, scanners, etc.) designed to protect your e-commerce site. At first the article looks like it's focused on one product, but it goes on to flesh out other products and the experiences of current user.

### Internet Professional Services

(www.thestandard.com)

THE INDUSTRY STANDARD

November, 1999, pp. 87-164

- **Everybody** has to have a web site these days, and business is looking for the quickest, fastest, cheapest, you-know-the-drill, means to get it. *The Industry Standard* has published a special report on who's doing it, how they're doing it, what to watch out for, and a boat-load of other good info. This one will take some serious coffee time, so plan accordingly. Definitely worth the read!

### ERP SYSTEMS FAILURES

(www.computerworld.com)

COMPUTERWORLD

November 1, 1999 & November 8, 1999

- In the 11/1 issue, Hershey Foods Corp., and W. L. Gore & Associates, Inc. failed new systems get highlighted in these separate front page articles. Hershey's installation of SAP R/3 during one of it's busiest shipping seasons has allegedly caused a 19% drop in 3Q99 profits, a 12% sales decline, and a 29% increase in year-to-year inventory costs. W. L. Gore, a.k.a. GoreTex's manufacturer is suing Peoplesoft Inc. and Deloitte & Touche over an allegedly bungled software installation. And in the 11/8 issue, Whirlpool Corp's disastrous Labor Day roll-out of SAP R/3 is highlighted. Do you *still* believe it can be fixed *after* the fact ???



# ***INTERNATIONAL NEWS***

A Recap of ISACA events from the *ISACA WEB site*

## **CISA CERTIFICATION UPDATE**

2000 CISA Examination Bulletin of Information

**Examination Date: Saturday, 10 June 2000**

For additional Information

<http://www.isaca.org/exam2.htm>

or

[certification@isaca.org](mailto:certification@isaca.org).

---

## ***Previously Approved IS Auditing Guidelines***

---

**Effective 1 September 1999**

- ✓ Audit Charter (Newly Developed)
- ✓ Audit Documentation (Previously issued SISAS 6)
- ✓ Due Professional Care (Previously issued SISAS 4)
- ✓ Materiality Concepts for Auditing Information Systems (Newly Developed)
- ✓ Outsourcing of IS Activities to Other Organisations (Newly Developed)
- ✓ Standards for Information Systems Control Professionals (Newly Developed)

The following guidelines were issued as exposure drafts in May or September 1998. At the end of the exposure period, they were revised as necessary to reflect the comments received during exposure, and are now issued as final versions.

**Effective from 1 March 2000**

- ✓ Audit Considerations for Irregularities (Previously Issued SISAS 8)
- ✓ Audit Sampling (Newly Developed)
- ✓ Effect of Involvement in the Development, Acquisition, Implementation or Maintenance
- ✓ Process on the IS Auditor's Independence (Previously Issued SISAS 2)
- ✓ Effect of Pervasive IS Controls (Newly Developed)

for additional information

<http://www.isaca.org/standard/guidelne.htm>

---

## ***Professional Seminar Series (PSS) Course Offerings:***

---

- ✓ Auditing Client/Server System
- ✓ Auditing Oracle
- ✓ Auditing Project Management & Change Control
- ✓ Auditing UNIX Systems
- ✓ Enterprise-Wide Security Management Tools
- ✓ Fundamentals of Information Systems Auditing
- ✓ The Internet - Security, Audit and Control Concerns
- ✓ Network Penetration Prevention Tools and Techniques
- ✓ Novell Netware: Security, Audit & Control
- ✓ Penetrating Windows NT Server 4.0
- ✓ Telecommunications Security
- ✓ Windows NT: Security, Audit & Control

For a brochure and complete packet of information on the Professional Seminar Series program, including detailed descriptions of each course offered, please contact the ISACA Education Department.

---

## ***Software Development is Risky Business -- is Audit Ready?***

---

by George R. Comrie, P.Eng., CDP, CMC

The ability to create and modify information systems quickly and reliably is critical to maintaining a company's competitive edge. The demands on software development departments are enormous. They must deliver higher volumes of feature-rich, error-free application software in shorter time frames and using fewer resources. This kind of pressure can easily lead to errors in the introduction of system changes and in the applications themselves. There are several steps, though, that can be taken to minimize the chance of mistakes and to protect an organization.

First of all, auditors should ask some basic questions. Can the organization afford a service outage due to a planned software change gone bad? Does the development environment have the tools and processes to ensure the best possible quality control? How can auditors enforce standards and not impede turnaround times? What about the cost to do this?

Establishing and following a good software configuration management (SCM) process is the starting point for error avoidance. This process should take into consideration the entire life cycle of software applications, not just their development. Managing an application's components as each new release is created, packaged, distributed, installed and obsoleted is important. Particular attention should be given to security, division of responsibilities, approvals and audit trails. Once the desired process has been established, SCM software can be implemented to ensure process compliance, provide audit trails, automate manual tasks and guarantee the reproducibility of the applications. From management's perspective, an SCM system provides assurance that a company's mission critical applications are not exposed to potential failure due to human error, staff turnover or sabotage.

In the development stage, version control is critical. Developers must work with "official" versions of sources and document the changes they make using the "check-out" and "check-in" facilities of the SCM tool. This ensures the proper audit trail for each change (who, what, when, etc.) is recorded in a secure system. As one would expect, this discipline adds some overhead to an otherwise uncontrolled development process; however it facilitates location of the correct component versions and their change histories.

Gerben Wieringa, senior consultant in the information technology center/user services group of ING Bank in the Netherlands, says, "An SCM system helps enforce the organization of the development and maintenance process. At first it is seen as difficult and inflexible, but eventually it becomes the way things should be done, because it reduces mistakes and improves the quality of the application. In using an SCM system, we relatively quickly got accustomed to fewer errors in the applications, and forgot how cumbersome the old situation sometimes could be. At the same time, the introduction of SCM didn't come without some trouble."

As software components are compiled and packaged into turnover packages or releases, the value of the SCM software becomes most evident. The ability to "lock" all components and their dependencies to a release is critical

to the guaranteed reproducibility of an application. Changes to a component must be done using a new version, and must not override any [dependent] component that needs to be kept intact as part of the application. One problem is that most dependencies are not obvious because their references are hidden in the source files. Without an SCM tool that knows every dependency and locks them into the release, it is almost impossible to know if a source change is "safe" or not.

"SCM software is essential in managing our Tandem-based trading systems," said Chris Fojut, Andersen Consulting, who is in charge of change management for the trading and information systems at the London Stock Exchange. "The software we use is RMS - Revision Management System. We know with certainty, information on how a release was put together and which components went in. With so many custom applications, it would be impractical to do this without the system."

It is important to understand the range of SCM software available and to recognize the limitations of some tools. Vendors with "source control" software sometimes claim to provide an "SCM solution". To the unaware auditor or management group, using a "source version control" tool for mission-critical applications can be detrimental to the application up-time if a disaster hits. This is because component dependencies are not typically tracked with "source" tools, and critical components may not be found when needed during an application failure. Critical components often are modified to accommodate new features and bug fixes, which may make it impossible to reproduce the release in its original form. A good SCM system will follow the chain of references and protect them from being changed by forcing the creation of a new version using proper security, with appropriate approvals and an audit trail. If reproducibility of a release is not guaranteed, additional downtime results while one tries to locate or repair the parts. This is even before any analysis can take place to fix the original problem.

Auditors should insist on having a separation of duties and an automated audit trail of software migration through each environment. As software migrates from development to test/QA to production, the security and access rules may have to change. A migration audit trail is an important feature, particularly for financial institutions, so that complete records are available when an external or internal audit is done. Gerben Wieringa says, "One of the main reasons we purchased SCM software was to obtain a separation of duties and of our environments."

While software migration takes place, it also is convenient for management to have an audit trail of approvals. This traditionally has been done with paper; however many SCM systems support electronic approvals, thereby improving efficiency and accuracy. When preparing a cost analysis of SCM solutions, the main factor to consider is the cost to the organization of not having a system in place. Just look at the numerous application failures found in the news lately (and the many not reported) for justification. These examples include hours of downtime for on-line brokers, bank ATM networks, telephone company networks, retail point-of-sale networks and many other mission-critical business operations. Application outages can't always be prevented, but at least with a good SCM solution an organization can have the best chance to recover from an unsuccessful change.

*George Comrie is a graduate and former academic staff member of the University of Toronto's Department of Industrial Engineering, where he specialized in information systems. His extensive IT industry experience includes management of an operational police information center with strict uptime and security requirements, as well as several years of management consulting. For the past 10 years, he has focused on configuration management as president of Data Design Systems Inc., a Toronto-based supplier of enterprise SCM tools and services.*

President

John Arens, CPA  
Meijer, Inc.  
arensj@meijer.com

Vice President & Program Chair

Rick Cummings, CISA  
Jackson National Life Ins.  
rick.cummings@jnli.com

Secretary

John Blair  
Steelcase, Inc.  
jblair2@steelcase.com

Treasurer

Pam Bradford, CISA, CPA  
National City  
pam\_1\_bradford@national-city.com

Cisa Coordinator / Webmeister

Michael Sekoni, CISA  
Accident Fund Company  
casa-2@rain.net

Member At Large

Jamie Depuydt, CISA, CBA  
Steelcase, Inc.  
jdepuydt@steelcase.com

Past President

Bernie Powers  
Steelcase, Inc.  
bpowers@steelcase.com

Newsletter Editor

Bernie Powers  
Steelcase, Inc.  
bpowers@steelcase.com

— *THE FINE PRINT* —

*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*.

**The deadline for submissions for the next Newsletter is Friday, November, 24<sup>th</sup> 1999!**



*Information Systems  
Audit and Control  
Association*