



# The Disk Patch



Volume 18 Issue No. 2

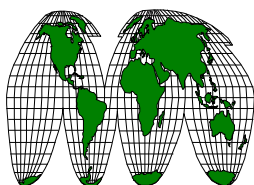
*Newsletter of the Winnipeg Chapter of the  
Information Systems Audit and Control Association*

April, 2001

*Continue your education with ISACA by  
visiting our Internet Resource Centre*

<http://www.isaca-wpg.org/>

Discount on COBIT® (Control Objectives for Information and related Technology) 2nd Edition © (includes Executive Summary, Framework, Control Objectives, Audit Guidelines, Implementation Tool Set and fully searchable CD-ROM). Discounts on CISA® Examination fee and materials. Discounts on leading-edge technical and managerial conferences and workshops. Discounts on co-sponsored events. Subscription to the bi-monthly Information Systems Control Journal, which features articles on current and future practices and technology, and *Global Communiqué*, a member publication. Access to the latest IT research and to ISACA Bookstore publications. Leadership and networking opportunities through participation on ISACA boards/committees that are making a positive impact on the IT profession.



## *Answering the Membership Value Question*

**“Why should I belong?”  
“What's in it for me?”**

**become better** at your job as a result of access to  
**leading-edge research**

**increase** your value to your employer by expanding  
your warehouse of **skills**

**pay less** for publications of **value** to you  
expand your **network** of business contacts

**International ISACA web site:**

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

earn **global** credentials in the **IS audit** profession  
with **CISA accreditation**

prepare yourself for **management** responsibility

**leadership opportunities** through participation on  
**ISACA boards and committees**

### *Inside This Issue:*

2000/2001 Board of 2

From the Editor's 3

Spotlight on 4

Your Board 5

ISACF Research 5

Bits & Bytes 7

2000/2001 Program 8



**Information Systems Audit and Control Association  
Board of Directors  
2000-2001**

<u>Position</u>	<u>Name</u>	<u>Voice</u>	<u>Fax</u>	<u>Email</u>
President	Gord Glessman	945-3790	945-2169	gglesman@pao.mb.ca
Vice President/ Program Chair	Roger Yost	945-3277	948-3860	ryost@gov.mb.ca
Assistant Program Chair	Alan Gellatly	926-2400	944-1020	alan.m.gellatly@ca.pwcglobal.com
Treasurer	Fred Horbaty	926-2411	944-1020	Fred.j.horbaty@ca.pwcglobal.com
Assistant Treasurer	Barry Saunders	945-4106	945-2169	bsaunders@pao.mb.ca
Secretary	Mike Rogers	474-6691	474-7638	rogers@ms.umanitoba.ca
Director - Newsletter	Jeff Thomas	944-3639	947-9390	jefthomas@deloitte.ca
Director - Membership & CISA	Les Hansen	946-7918	946-8478	les.hansen@gwl.ca
Director - Marketing				
Director - Program	Stewart Bidinosti	986-8274	986-4134	sbidinos@city.winnipeg.mb.ca
Director - Program	Mike Rogers	474-6691	474-7638	rogers@ms.umanitoba.ca
Director - Program	John Graeb	632-2194	633-6489	jgraeb@rrc.mb.ca
Director - Program	Jeff Murray	933-0264	956-0138	jeff.murray@ca.eyi.com
Director - Program	Lawrence Elkow	474-8430		cyberjet@icenter.net
Director - Program	Jeff Butler	667-5535	663-0308	jbutler@wilsonautoelectric.com
Director - Program	Pat McCarthy	956-8188		pat.mccarthy@investorsgroup.com
Director - Program Email	Ken Fitzpatrick	949-3648	727-7761	kfitzpatrick@westmangroup.com
Director - Research & Library	Dan Swanson	956-8625	942-1880	dan.swanson@investorsgroup.com
Director - Security	Dave Abesamis	956-8782	942-1880	ABESAD1@investorsgroup.com
Event Registrar	Cheryl Devaney	945-4130	948-3021	Cdevaney@fin.gov.mb.ca
Past President	Barry Safiniuk	933-0230	956-0138	barry.safiniuk@ca.eyi.com
Webmaster/Program Fax	Michael Li	947-6912		mike@ingen.mb.ca

If you have any comments, questions or ideas about the chapter activities, publications, seminars, membership, C.I.S.A. designation, library books or would like other information about the ISACA, please contact one of the above persons.

## From the Editor's Desk:

Spring is in the air and at the Winnipeg Chapter of ISACA we are winding up our activity program for the year. I don't know about you but my brain is going to enjoy a brief rest after soaking up this year's development program.

The "almost" final event of the year will be a luncheon on Thursday May 17, 2001. Join us at the Royal Crown Conference Centre for "**Enabling Security, Integrity, and Trust for Your E-business Initiatives**".

The guest speaker will be Robert Reimer. Robert is the national leader of the Technology Risk Services group of PricewaterhouseCoopers LLP (PricewaterhouseCoopers) *Global Risk Management Solutions* practice.

Robert will discuss the challenge of ensuring that security is woven into all aspects of an organization's digital enterprise.

Why is this the "almost" final event? Plans for a **CISA Review** course are in the works. If you are planning on taking the exam this year and interested in a top quality review course at a bottom dollar price then be sure to stay in touch with Les Hansen, Membership and CISA Director (946-7918)

If you are taking your family to North America CACS in Lake Buena Vista Florida, April 29 to May 4, you may want to check out the Disney web site at [http://disney.go.com/disneyworld/rm\\_resource/resorts/contemporary.html](http://disney.go.com/disneyworld/rm_resource/resorts/contemporary.html)

Send me a postcard!

Soon, planning for the 2002 development year will begin. Think about what training you would like to see in Winnipeg next year (*my vote is for PKI, VMS and O/S 390 audit*), and let your board know.

**Jeff Thomas, CA, CIA, CISA, CMC**



*Write to Disk Patch at:*

J.W.G. (Jeff) Thomas, CA, CIA, CISA, CMC  
 c/o Deloitte & Touche LLP  
 Enterprise Risk Services  
 360 Main Street, Suite 2300  
 Winnipeg, Manitoba R3C 3Z3  
 email: [jefthomas@deloitte.ca](mailto:jefthomas@deloitte.ca)  
 facsimile: (204) 947-9390  
 Or call...  
 telephone: (204) 944-3639

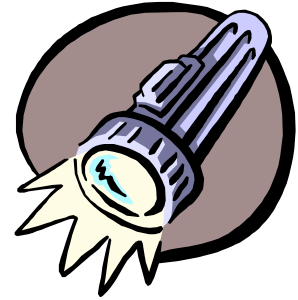
### ISACA International Internet Addresses

**Home Page:** <http://www.isaca.org>

**E-Mail:** [membership@isaca.org](mailto:membership@isaca.org)  
[certification@isaca.org](mailto:certification@isaca.org)  
[conference@isaca.org](mailto:conference@isaca.org)  
[education@isaca.org](mailto:education@isaca.org)

[publication@isaca.org](mailto:publication@isaca.org)  
[research@isaca.org](mailto:research@isaca.org)  
[exec@isaca.org](mailto:exec@isaca.org)

# Spotlight On



## CA SysTrust™

The reliance that businesses place upon information systems is increasing, hastened by the rapid development of e-Business and the spread of the Internet. Information systems are becoming more and more pervasive within an organization, running not just the financial systems but in many instances a significant proportion of the business' operational systems. As a result stakeholders are having to place greater reliance upon the *availability, security, integrity and maintainability* of these systems.

SysTrust™ is an assurance service jointly developed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) to provide stakeholders with trust in the information systems upon which their businesses and organizations rely.

In the SysTrust™ model, a system consists of:

1. **Infrastructure** – The physical and hardware components of a system, including facilities, mainframes, servers, networks, and related components
2. **Software** – The programs and operating software of a system, including operating systems, utilities, business applications software such as Enterprise Resource Planning (ERP), and financial systems
3. **People** – The personnel involved in the operation and use of a system, including information technology (IT) personnel such as programmers and operators, users of the system, and management
4. **Procedures** – The programmed and manual procedures involved in the operation of a system, including IT procedures such as back-up and maintenance, and user-based procedures such as data entry
5. **Data** – The information used and supported by a system, including transaction streams, files, databases, and tables

The components of the system are evaluated against the four essential principles using specific criteria. The criteria are designed to be complete, relevant, objective, and measurable and to address all of the system components and the relationships among them. The criteria address the following features that contribute to system reliability:

1. **The definition and documentation of an entity's performance objectives, policies, and standards as they relate to system performance expectations and entity commitments, and their communication to applicable personnel.**
2. **The procedures an entity implements for all system components to achieve its performance objectives in accordance with its established policies and standards.**
3. **System monitoring activities and monitoring of the surrounding environment to enable an entity to identify potential impairments to system reliability and to take appropriate action to achieve compliance with objectives, policies, and standards.**

SysTrust™ includes 58 specific criteria. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) believe that all 58 of these criteria must be met in order to provide reasonable assurance that the system is reliable. These criteria are consistent with the leading information technology control frameworks such as the Information Systems Audit and Control Foundations' *Control Objectives for Information and related Technology* (COBIT) and the CICA's *Information Technology Control Guidelines*.

This article was prepared by  
Jeff Thomas, CA, CIA, CISA, CMC  
Senior Manager, Enterprise Risk Services  
Deloitte & Touche LLP

Based upon AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability Version 2.0

**Jeff Murray, CA, Program Director**

Jeff is a Manager in the Information Technology Risk Management Solutions practice in the Winnipeg Office of Ernst & Young. Jeff has six years experience in external audit and specializes in the performance of control analysis specific to information systems. Jeff also performs data analysis using tools such as ACL (Audit Command Language). Jeff spends his leisure time playing hockey and golf. He also enjoys spending time with family and friends at the cottage with his wife Nicole.

**Ken Fitzpatrick, CISA, Program Director**

Ken just recently became the I.S. Manager for WGI. WGI is a steel manufacturing company that contains Behlen Industries and Westman Steel and Culvert. He came from Liberty Tax Services after 2 years as the I.S. Manager and had prior experience of 14 years with Meyers Norris & Penny designing business solutions both internally and for clients.

Ken obtained his CISA designation in 1999 and shortly there after joined ISACA.



## Your Winnipeg Chapter Board Members

### ISACF Research News

**Security and Risk Management in ERP Project**

ERP systems are now pervasive globally in medium to large enterprises and in the public sector. Application security and technical infrastructure considerations will be covered for each ERP offering in a technical reference guide. The first in this series will be SAP, which is strong in manufacturing and has its own project management methodology, ASAP (accelerated SAP). The SAP technical reference guide will focus on business process controls for the inventory and revenue cycles and project management. Internet and wireless implications also will be addressed. Project completion is scheduled in the third quarter of 2001.

**Wireless Communication Project**

This project will provide both a technical and functional assessment, written from a business and risk management perspective. Because wireless communications transcend traditional and regulatory boundaries, they pose significant technical issues and even greater challenges in the areas of control, security and audit. Users expect the same features they enjoy on their home network when they take communications devices with them on their travels and roam onto foreign networks. Work is targeted for completion in third quarter 2001.

**Oracle Database Security, Control and Audit Project**

Work has begun to update the ISACA Monograph Series book *Security and Controls in an Oracle Environment*. The revision will include a recommended plan for addressing issues that have changed in Oracle environments since the original publication. Availability is expected late in third quarter 2001.

**Enterprise Information Integrity Project**

In an increasingly dynamic global environment, IT organizations must address complex solutions and operating environments to provide assurance of the dependability and trustwor-

thiness of information across the enterprise. The purpose of this project is to define the key elements of enterprise information integrity, identify associated benefits criteria and present a framework and process for management. The Centre for IS Assurance will conduct this project for ISACF, with funding from Unitech Systems Inc. Completion is projected for third quarter 2001.

**Customer Relationship Management (CRM) Project**

CRM provides organizations with increased functionality by providing e-business facilitation, field sales representative support, sales compensation determination, mobile field service, and management of accounts, contacts, opportunities, pipeline, forecasts, campaigns, events and telephony. The research project will address a number of issues, including: CRM application functionality, technical architecture, operational and strategic risk management opportunities, as well as security and control criteria within the CRM IT environment. Completion is scheduled for fourth quarter 2001.

**OS/390 Security, Control and Audit Project**

This research project will cover recent updates to the legacy functions of the operating system; will outline system components and their interaction; and will cover system initialization, security functions, audit tools and methods. It also will provide detailed descriptions of new components and functions in the above areas and recently added functions, mainly those that permit the use of Internet and UNIX functions in the OS/390 environment, i.e., the OS/390 core functions. Targeted completion is first quarter 2002.

**COBIT 3<sup>rd</sup> Edition**

COBIT 3<sup>rd</sup> Edition can be ordered through the Bookstore at [www.isaca.org/pubs1.htm](http://www.isaca.org/pubs1.htm). Sixteen new detailed control objectives and an update of over 40 others have been added. It also reflects a review of seven new or updated international

(Continued on page 7)

# Bits & Bytes

All the news that's fit to print. From ISACA International, members, and anywhere else we can find it.

010011010011000101101001001110101110100110110110100100101101000110011

## The Seven Top Management Errors That Lead to Computer Security Vulnerabilities

(Source: SANS Institute Resources; [www.sans.org](http://www.sans.org))

### Error #7:

Pretending the problem will go away if you ignore it.

### Error #6:

Authorizing reactive, short-term fixes so problems re-emerge rapidly.

### Error #5:

Failing to realize how much money the organization's information and reputation are worth.

### Error #4:

Relying primarily on a firewall.

### Error #3:

Failing to deal with the operational aspects of security (making a few fixes and then not allowing the follow-through necessary to ensure the problems stay fixed).

### Error #2:

Failing to understand the relationship of information security to the business problem. You understand physical security, but do not see the consequences to poor information security.

### Error #1:

Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to do the job.

(Ed. Does SANS have a list of the Seven Top Security Administrator Errors that Lead to Computer Security Vulnerabilities?)

## Sleeping With the Enemy

Steve Pozgaj, CIO of Mackenzie Financial is the subject of an article titled "Sleeping With The Enemy" in the January 2001 edition of CIO Canada. Steve talks about the challenges of building effective e-business connections with customers and suppliers without undermining more traditional relationships. What's the Winnipeg connection? Investors Group recently offered to purchase Mackenzie. If the offer is accepted, I wonder how it will impact the challenges Steve is facing?

(Sleeping with the Enemy, Pat Atkinson, CIO Canada, January 2001)

## Maximize Return, Minimize Risk

The Treasury Board of Canada Secretariat has issued an Enhanced Management Framework for IM/IT. The framework is designed to aid managers in maximizing their department's information management and information technology (IM/IT) investments and minimizing risks.

The website ([http://www.cio-dpi.gc.ca/emf/EMFIndex\\_e.html](http://www.cio-dpi.gc.ca/emf/EMFIndex_e.html)) contains information on how you can reap the benefits of implementing best practices including:

- Savings between \$4-\$6 for every \$1 invested.
- Increased productivity by 10-100%
- Reduced schedule delays by 50-70%
- Reduced rework by 25-40%
- Improved quality by 45-70%

## Board with Security?

In Volume 1, 2001 Information Systems Control Journal, Michael P. Cangemi discusses the Role of the Board in Information Security. Information Security fits nicely within the board's governance responsibilities and many of us involved with audit committees have noticed that boards are increasingly interested in information systems controls.

The Institute of Internal Auditors, National Association of Corporate Directors, American Institute of Certified Public Accountants, and Information Systems Audit and Control Association have jointly prepared a package called "**Information Security Management and Assurance: A Call to Action for Corporate Governance**". The package includes 26 questions for board members to ask about information security.

(see <http://www.theiia.org/> for further information)

## Enough With The Passwords!

(Continued on page 7)

(Continued from page 6)

Steven J. Ross makes an impassioned plea for getting rid of passwords entirely in "Why Passwords Matter", Volume 1, 2001, Information Systems Control Journal.

What is the answer? Certificates. According to Steven, "we all have to get in with certificates or we will all be left out. It is a new way of doing things, a new order."

### **Wanted: CISA Question Writers**

Work has already begun on the 2002 CISA exam study materials. While many ISACA members have already committed to assisting in the review and updating of the *CISA Review Manual* (CRM), additional volunteers are needed to write questions for the *Questions, Answers & Explanations Manual, 2002 Supplement*. In addition to earning continuing education (CE) hours, question writer volunteers will earn US \$50 for each question accepted for publication. Encourage chapter members interesting in volunteering to contact Elia Fernández at [efernandez@isaca.org](mailto:efernandez@isaca.org) or at +1.847.253.1545, ext. 484.

### **New Audit Programs Available in the GIR**

Chapter members are encouraged to review the new audit programs available in ISACA's Global Information Repository (GIR) at [www.isaca.org/gir/girMenu.cfm](http://www.isaca.org/gir/girMenu.cfm), or through the member-only section of the web site. Programs on Business Continuity Planning, Change Control and UNIX were reviewed and approved for inclusion by ISACA's Education Board. Additional programs will be added on a regular basis.

## **PUBLICATIONS FROM ISACF**

### **Technical Reference Guide: Trading Partner Identification, Registration and Enrollment—A Reference for the IS Auditor when Dealing with e-Business Transactions**

This technical reference guide is part of the third phase of the e-commerce project currently being conducted by ISACF™ in partnership with Deloitte & Touche. This publication's focus is the establishment of the relationship, on "new account" time, and it documents the process of recognizing and establishing the authenticity of a new trading partner and deciding whether to do business. Auditors will find it useful in deciding whether to audit an e-commerce application and when planning or conducting such an audit. They may also find it helpful when examining or making judgments about any new account process automation. This portion of the audit process is becoming increasingly critical with the rapid growth of e-trading exchanges. For purchase information contact the

ISACA Bookstore at [www.isaca.org/bk\\_ints.htm#trs-1](http://www.isaca.org/bk_ints.htm#trs-1). (This publication is also available through amazon.com.)

### **PKI**

This technical reference guide is another part of the third phase of the e-commerce research project being conducted by ISACF in partnership with Deloitte & Touche. In a very real sense, this project is not about securing information, but about the infrastructure that makes security efficient, manageable and effective in the real world of commerce and competition, easy for the implementer and transparent (or nearly so) for the user. This publication will address public key infrastructure (PKI), including digital signatures, certificates and certificate authorities. The project is based on the understanding that the primary tool that has been developed to protect information and transactions on the Internet is cryptography, the art and science of "secret writing" involving codes, ciphers and the ability to conceal data and information from non-authorized persons. However, modern cryptography can do far more, if there is an infrastructure in place to make the use of cryptography possible. Target availability is early in the second quarter of 2001. This book will be available through the ISACA Bookstore and amazon.com.

### **Virtual Private Network—New Issues for Network Security**

This new ISACF publication provides security, audit and control professionals with an overview of the architecture behind Internet VPN, as well as commonly used security algorithms. Consistent with COBIT® and CONCT® (*Control Objectives for Net Centric Technologies*), the publication addresses implementation and supplies general audit suggestions. Target availability date is the beginning of the second

---

### **ISACF Research News**

(Continued from page 5)

references. COBIT 3<sup>rd</sup> Edition includes the *Management Guidelines*, with key performance indicators, critical success factors, key goal indicators and a maturity model for COBIT high-level control objectives. The *Management Guidelines* (and most of the other sections of COBIT) are an open standard and are available now for download on the ISACA web site, [www.isaca.org/cobit.htm](http://www.isaca.org/cobit.htm). The 2<sup>nd</sup> Edition is now available in French, German, Japanese, Korean and Spanish. Work is in progress for the translation to Dutch, Estonian and Norwegian. See "What's New with COBIT" at [www.isaca.org/cobit.htm](http://www.isaca.org/cobit.htm) for download sources and for regular addition of new information concerning implementations of COBIT within enterprises, governmental adoptions of COBIT and use of COBIT as a

---

### 2000/2001 Program & Events

The *Information Systems Audit and Control Association (ISACA)* is devoted to the development and support of professionals involved in the audit and control of computer-based systems. The 2000-2001 professional development program covers management issues and control practices facing professionals involved with information technology (IT) and audit.

Date	Topic	Speaker	Event Director(s)	Advance Registration
<b>September 20, 2000</b> Luncheon	<b>E-Commerce Security</b>	Jan Wolynski	Mike Rogers 474-6691	
<b>November 30 &amp; December 1, 2000</b> 2 day event	<b>Hands on Unix Security</b> (Hands on lab at U of M Downtown with individual computers)	Randy Marchany, Virginia Tech	Dave Abesamis 956-8782	
<b>December 13, 2000</b> Wednesday Luncheon	<b>Information Security - A Balanced Approach</b>	Marc Rogers	Pat McCarthy 956-8188	
<b>January 16, 17 &amp; 18, 2001</b> Tuesday, Wednesday & Thursday 3 day event	<b>Fraud Detection &amp; Investigation (2 days)</b> <b>Fraud Awareness for Managers (1 day)</b> (Joint session with CFE & IIA)	Courtney Thompson Courtney Thompson & Associates, Dallas Texas	Mike Rogers 474-6691 Brian Brown (IIA) 944-5660 George Anderson (CFE)	January 12, 2001
<b>February 7, 2001</b> Wednesday 1 day event	<b>SAP Audit</b> (Joint session with CGA & IIA)	Graham Larson, Deloitte & Touche	Stewart Bidinosti 986-8274	
<b>March 1 &amp; 2, 2001</b> Thursday & Friday 2 day event	<b>Oracle Security Audit and Control Issues</b>	Betty Dorsey, MIS Training Institute	John Graeb 632-2194 Lawrence Elkow 474-8430	
<b>April 9, 10 &amp; 11, 2001</b> Monday, Tuesday, & Wednesday	<b>Intermediate IT Audit and Security</b>	Stuart B. Holoman, MIS Training Institute	Jeff Murray 933-0264	
<b>May 17, 2001</b> Thursday Luncheon	<b>Enabling Security, Integrity, and Trust for Your E-business Initiatives</b>	Robert Reimer, PricewaterhouseCoopers	Alan Gellatly 926-2400	