



# The Disk Patch



Volume 20 Issue No. 1

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

August, 2002

## Message From The President



And the survey Says.....

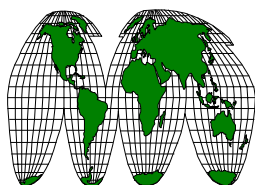
Thanks to the members that submitted their survey input this year. We had the highest member survey response to date with over twenty-five percent of members responding.

Congratulations to Raymond Lau and Larry Neufeld, winners in our member survey draw.

The survey results show we are on the right track – with 95% of members finding interest in the courses we offer. There was an even split on the question of adding more full-day or multi-day technical courses so we will continue for the coming year with an even mix of luncheon and full-day / multi-day technical courses.

The survey provided a wealth of event suggestions - with a high response for a Windows 2000 security technical session. We are planning on bringing in a MIS 2 day Controlling and Securing Windows 2000 seminar in April, 2003 to address that

*(Continued on page 3)*



### ***Inside This Issue:***

<b>2002/2003 Board of Directors</b>	<b>2</b>
<b>From the Editor's Desk</b>	<b>3</b>
<b>Spotlight On Information Systems Audit and Control Foundation and IT Governance Institute</b>	<b>4</b>
<b>Bits &amp; Bytes</b>	<b>5</b>
<b>Computer Investigations</b>	<b>7</b>

**Information Systems Audit and Control Association  
Board of Directors  
2002-2003**

<b>NAME</b>	<b>COMPANY</b>	<b>BOARD POSITION</b>	<b>EMAIL</b>
Roger Yost	Province of Manitoba	President	ryost@gov.mb.ca
Gord Glesmann	Provincial Auditor's Office	Past President & Assistant Marketing Director	gglesmann@oag.mb.ca
Lawrence Elkow	University of Manitoba	1st Vice President/ Program Chair	cyberaudit@msn.com
Anne Thompson	Air Canada	Secretary	anne.thompson@aircanada.ca
Fred Horbaty	PricewaterhouseCoopers	Treasurer	Fred.j.horbaty@ca.pwcglobal.com
Barry Saunders	Provincial Auditor's Office	Asst Treasurer	b Saunders@oag.mb.ca saunders@ilos.net
Jeff Thomas	KPMG LLP	Newsletter Editor	JWThomas@kpmg.ca
Michael Li	Direct Focus	Webmaster	mike@ingen.mb.ca
Howard Yip	Provincial Auditor's Office	Student Member / Webmaster	hyip@oag.mb.ca
Jeff Murray	Ernst & Young LLP	Director Marketing	jeff.murray@ca.eyi.com
Les Hansen	Great West Life	Director - Membership & CISA	les.hansen@gwl.ca
Stewart Bidinosti	City of Winnipeg Audit	Director - Program	sbidinos@city.winnipeg.mb.ca
John Graeb	Red River College	Director - Program	jgraeb@rrc.mb.ca
Patrick McCarthy	Investors Group	Director - Program	Pat.McCarthy@investorsgroup.com
Barry Safiniuk	Cangene Corp.	Director - Program	bsafiniuk@cangene.com
Alan Gellatly	PricewaterhouseCoopers	Director - Program	alan.m.gellatly@ca.pwcglobal.com
Marc Rogers	Manageworx	Program Director	mkr@mts.net
Brian Mansky	City of Winnipeg	Audit Director - Program	bmansky@city.winnipeg.mb.ca
Cheryl Devaney	Internal Audit, Province	Event Registrar	Cdevaney@gov.mb.ca

**International Office Contacts**

Information Systems Audit and  
Control Association / Foundation  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, Illinois 60008  
USA

Main Telephone: +1.847.253.1545  
Fax: +1.847.253.1443

Membership Info:  
Christen Gunning membership@isaca.org  
+1.847.253.1545 ext. 475

Chapter Info:  
Andy Jacoby ajacoby@isaca.org +1.847.590.7470

Conference Info:  
Sandy Arens conference@isaca.org +1.847.590.7454

Certification Info:  
Kim Fields certification@isaca.org +1.847.590.7474

Education Info:  
Karen Lamb klamb@isaca.org +1.847.590.7452

Research info:  
Linda Wogelius research@isaca.org +1.847.590.7462

## From the Editor's Desk:

While I am writing this, the weather is +30c. A beautiful warm sunny day. Funny how there doesn't seem to be anyone in the office today. In fact almost nobody in town except for the forever hard working ISACA board members.

Last I checked, the Program Committee was locked in an underground former bomb shelter. Roger Yost was outside the door pocketing the key and shouting through the steel doors "None of you are getting out until that program schedule is done!"

I hope you enjoy this summer issue of Disk Patch. If you print it off you can tuck it in your back pocket and take it on the golf course with you. If you're a lake person, consider having a read while you are waterskiing. Or do like me, take it to the beach and lay it over your eyes as you catch a few rays of sun on the sand.

Hope you have a great summer.

## Jeff Thomas, CA, CIA, CISA, CMC Newsletter



*Write to Disk Patch at:*

J.W.G. (Jeff) Thomas, CA, CIA, CISA, CMC  
c/o KPMG LLP  
Information Risk Management  
One Lombard Place, Suite 2000  
Winnipeg, Manitoba R3B 0X3  
email: JWThomas@kpmg.ca  
facsimile: (204) 957-0808

Or call...  
telephone:(204) 957-2291

# Message From The President

*(Continued from page 1)*

requirement. Other suggestions have resulted in planned seminars on eSecurity / Internet Security and Computer Investigations. We will keep the remaining suggestions for use in next year's planning. As a result of a survey suggestion, we hope to have a member e-vote in place on which topics to bring in for the 2003/2004 season.

The tentative event schedule for 2002-2003 will be up on your web site at <http://www.isaca-wpg.org> (hopefully by the time you get this!). This allows you to plan well in advance for events of interest to you (another survey suggestion). We will put up the detailed event information as soon as it is available – we hope that to be a minimum of 3 months before the event date.

We are again offering a free member luncheon event on October 9, 2002. We have **Brian Bowman** from Aikins, MacAulay & Thorvaldson presenting on how the new Privacy legislation WILL affect your business. Please register for this event using our new ONLINE member registration process. Thanks to board members **Howard Yip**, **Mike Li** and **Barry Saunders** for their hard work in getting the on-line registration process in place.

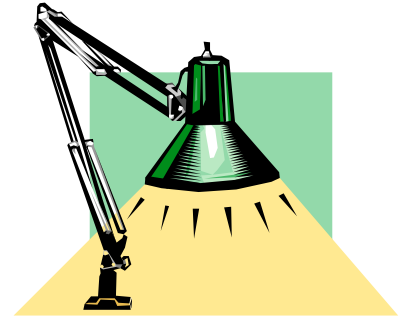
Well, it is time for summer holidays. I hope yours are safe and enjoyable.

Your program committee will be working over the summer to finalize the 2002/2003 events. We hope to see you at our September one day event on Computer Investigations with Dr. Marc Rogers of Manageworx.

Roger Yost  
President

# Spotlight On

## The Information Systems Audit and Control Foundation And IT Governance Institute



### Foundation and Research

The Information Systems Audit and Control Foundation (ISACF) was established in 1976 and today remains committed to the development of world-class research with the goal of being "the recognized global leader in IT governance, control and assurance."

Members and CISAs rely on ISACF's publications and advanced research for information on critical issues. They benefit from the foundation's pioneering work on controls for new or pervasive technologies and harmonized international control objectives. Recent examples of this advanced research include: *e-Commerce Security: A Global Status Report*, *e-Commerce Security: Enterprise Best Practices*, and *e-Commerce Security: Trading Partner Identification, Registration, and Enrollment*. ISACF, in collaboration with the IT Governance Institute, also released the revised and enhanced COBIT 3rd Edition, complete with the all-new *Management Guidelines*.

### Funding the Foundation

Research requires resources. For more than twenty-five years, ISACF has dedicated itself to global research programs that address pressing issues facing IT professionals. This research contributes significantly to the success and security of the enterprises in which those professionals serve. The research and projects of the foundation are funded solely through donations from individuals, chapters and corporations (check out <http://www.isaca.org/finfo2.htm>). Without the support of constituents, the research needed to advance the study and practice of IT would go undone.

### IT Governance Institute

The [IT Governance Institute](http://www.itgi.org/) (<http://www.itgi.org/>), established by the Information Systems Audit and Control Association (ISACA) and its affiliated foundation in 1998, exists to clarify and provide guidance on current and future issues pertaining to IT governance, control and assurance. Consisting of individuals who bring both business and IT expertise to the subjects at hand, the IT Governance Institute plans to undertake original research, convene symposia, conduct trend analysis and pursue other activities designed to benefit professionals and enterprises impacted by the effective control of information and related technologies.

### Available Resources:

[Board Briefing on IT Governance](http://www.itgovernance.org/boardbriefing.pdf) (<http://www.itgovernance.org/boardbriefing.pdf>)

June 2001

One of the first two publications from the IT Governance Institute, this book describes IT governance, outlines why it is important, defines the role of boards and executive management and offers tool kits and maturity models for implementing and measuring IT governance enterprise-wide.

(Continued on page 5)

(Continued from page 4)

[Information Security Governance: Guidance for Boards of Directors and Executive Management](http://www.itgovernance.org/infosecurity.pdf) (<http://www.itgovernance.org/infosecurity.pdf>)

June 2001

Another of the first two publications from the IT Governance Institute, this book discusses why information security governance is increasingly important and outlines questions to ask and steps to take to ensure an effective information security governance program within an enterprise.

[IT Governance \(IT\\_gov\\_books\\_member\\_PPt.ppt\)](#)

Revised June 2002

A PowerPoint presentation about IT governance and information security governance, based on the two new IT Governance Institute books. Provided to ISACA members only, this presentation will help members present the concepts of IT governance to management. Talking points are available upon request to [jseago@isaca.org](mailto:jseago@isaca.org).

[IT Governance and the IT Governance Institute \(ITGovChapPres.ppt\)](#)

July 2000

---

# Bits & Bytes

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

010011010011000101101001001110101110100110110110100110110110100100101101000110011011

## Certification Update

### **CISA® Results to Candidates**

Candidates who sat for the 2002 CISA examination will be mailed their exam results in early August. Those passing the exam receive an Application for Certification to become a CISA and will be granted certification after a completed application is received by ISACA™ and all work and educational experience has been verified. Those who failed the exam will receive their overall score, scores by each content and process area and an English-only copy of the 2003 *Bulletin of Information*.

### **Cycle-ending Reminder**

Recently all CISAs whose three-year certification cycle ends in 2002 were sent an e-mail reminding them about how many CPE hours are needed to be in compliance with the annual requirement and the three-year requirement. Included also were the number of CPE hours needed to comply with 2002 even if the individual already has met the three-year cycle requirement. Any CISA with questions about the hours required for 2002 should contact the certification department at +1.847.253.1545, ext. 471 or 474, or by e-mail at [certification@isaca.org](mailto:certification@isaca.org). ■

### **Certified Information Security Manager™ (CISM™)**

Progress continues on the Certified Information Security Manager (CISM) credential that is designed to provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective security management and consulting. The new credential will be business-oriented and focused on information risk management while also addressing management, design and technical security issues at a conceptual level.

To earn the CISM designation, information systems professionals will be required to:

- Successfully complete the CISM examination (to be offered first in 2003)
- Adhere to a code of ethics

Submit verified evidence of a minimum number of years of information security work experience, with a minimum number of these years in the job analysis domains.

## Standards

### **Newly Issued Guidance**

Five new documents effective

(Continued on page 6)

---

# Bits & Bytes

(Continued from page 5)

1 July 2002 are posted to the ISACA web site. The documents include three guidelines—*Irregularities and Illegal Acts*, *Effect of Nonaudit Role on the Auditor's Independence* (replacing the guideline *Effect of Involvement in the Development, Acquisition, Implementation or Maintenance Process on the IS Auditor's Independence*) and *IT Governance* (replacing *Corporate Governance of Information Systems*)—and two procedures—*IS Risk Assessment Measurement* and *Digital Signatures*.

A comprehensive standards PDF document containing all the standards, guidelines and procedures is in the process of being posted on the ISACA web site.

## New at the Bookstore

Two new research books are expected in July:

- *Security, Audit and Control Features SAP® R/3®*
- *e-Commerce Security—Business Continuity Planning*

In *Security, Audit and Control Features SAP R/3*, current best practices and future trends in ERP issues are documented in a practical how-to guide to enable auditors and risk professionals (IT and non-IT) to evaluate risks and controls in existing ERP implementations and to facilitate the design and building of better practice controls into system upgrades and enhancements. FAQs, audit programs, ICQs, references and tips for the assurance professional regarding SAP's Audit Information System and *mySAP.com* also are provided, making this publication a valuable resource in today's environment.

*e-Commerce Security—Business Continuity Planning* examines business continuity planning as adapted to encompass the dynamic requirements of doing business in today's e-commerce-enabled environment. The book provides assistance, hints and templates to the person charged with the task of implementing business continuity planning in an e-commerce environment. Included are audit programs, ICQs, recommendations for the assurance professional, as well as FAQs.

The latest research book from Information Systems Audit and Control Foundation is available now—*Security Provisioning: Managing Access in Extended Enterprises*. This is a new authoritative reference book about provisioning, a technology that automates the process of granting, changing and revoking user access to corporate resources and data using predetermined policies. Provisioning can help companies prevent cybersabotage, boost productivity and open the doors

to effective collaboration with other enterprises.

Fourteen new peer-reviewed books have been added to the ISACA Bookstore. Look for descriptions and ordering information in volume 3 of the *Information Systems Control Journal*. The newest additions include:

- *The E-Business Workplace: Discovering the Power of Enterprise Portals*
- *Internal Control: A Manager's Journey*
- *Management Skills for the IT Professional*
- *A Practical Guide to Security Engineering and Information Assurance*
- *Incident Response*
- *Virtual Private Networks: Technologies and Solutions*
- *Virus Revealed: Understand and Counter Malicious Software*
- *Voice and Data Security*
- *Accounting and Auditing Research: A Practical Guide, 5<sup>th</sup> Edition*
- *Auditing: A Risk Analysis Approach, 5<sup>th</sup> Edition*
- *Auditing and Assurance Services, 7<sup>th</sup> Edition*
- *Control Self Assessment, Leading Edge Thinking: Books, Articles and Tools*
- *Fraud Toolkit for ACL*
- *Meyor COBIT Autoevaluación de Controles*

For more information on these titles and other ISACF/ITGI books, visit the ISACA Bookstore at [www.isaca.org/bookstore](http://www.isaca.org/bookstore). ■

## News Briefs

### International HQ Computer Implementation Update

The implementation of the new computer system at International Headquarters has entered the training phase. The internal staff users who were identified as "early adopters" have received their training and have been using the system in test mode. The remainder of staff is scheduled to receive training in the new internal functions of the system in June.

By mid-June, the data files from the old system will be prepared for conversion onto the new system and physical inventory taken. The anticipated go-live date for the new system is 24 June, and the week thereafter is allocated to bringing the systems into alignment. By early July, the old system should be disbanded and all processing will be taking place on the new system.

The next phase of the implementation, the web applications, which will enable enhanced member and chapter online activity, more effective and timely e-mail confirmations, electronic commerce and more, is scheduled for the second half of 2002. For more information, visit the FAQ document posted in the member-only area of the ISACA web site, [www.isaca.org/computer/faq.htm](http://www.isaca.org/computer/faq.htm).

# Computer Investigations

Wednesday

September 18, 2002

Royal Crown Conference Center (Winnipeg, Manitoba)

7:45 AM – 4:30 PM

Presented By:

## THE WINNIPEG CHAPTER OF THE INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA)

### For further information contact

*Stewart Bidinosti Chair - (204) 986-4214*

*Or visit our web sites at [www.isaca-wpg.org](http://www.isaca-wpg.org)*

### Schedule Overview

Registration with continental breakfast 7:45 - 8:30

Presentation 8:30 - 10:15

Break 10:15 – 10:30

Presentation 10:30 – 12:00

Lunch 12:00 – 1:00 (Revolving Restaurant)

Presentation 1:00 – 2:30

Break 2:30 – 2:45

Presentation 2:45 – 4:00

Question and Answer Session 4:00 – 4:30

### Session Overview

The one day seminar will cover management issues and concepts related to incident response and evidence management. In today's technology dependent business environment, understanding how to react effectively and efficiently to a suspected network intrusion is extremely important. Knowing what to do and how to do it correctly can greatly reduce the impact that a information security incident can have on the organization. The seminar will also cover the management and handling of potential evidence in a forensic friendly manner that will assist, as oppose to hinder, any required computer forensic or law enforcement investigation.

### Speaker Information

**Dr. Marc Rogers, Ph. D. , CISSP**

Marc Rogers, Ph.D., CISSP, is the Director of Information Security Services at Manageworx Infosystems Inc. He also is a researcher and lecturer at the University of Manitoba, where he studies computer criminal behavior and cyber-terrorism. Dr. Rogers is an instructor for the international body that certifies information system security professionals (CISSP), a lecturer at the University of Winnipeg Continuing Education Department, and a former police detective who worked in the area of computer crime

---

investigations.

Dr. Rogers's consulting and seminar involvement includes work for major corporations, national and international financial institutions, governments, law enforcement agencies, small businesses, and professional associations. He has designed and taught numerous courses on information system security at various universities. Dr. Rogers also has authored several articles and book chapters in the area of information security and its interaction with society.

### Presentation Description

With business's increased reliance on technology, there is now a greater emphasis on the security, confidentiality, availability, and integrity of information systems and the data they contain. This seminar is designed to provide a strategic, conceptual, and pragmatic approach to incident response and dealing with possible forensic investigations. The seminar views incident response as a methodical process as opposed to a quick fix or vendor tools. The seminar will introduce the students to the phases of a commonly accepted methodology (PDCAERF). The phases include Preparation, Detection & Notification, Containment, Analysis & Tracking, Eradication, Recovery, Follow-up, and Legal considerations. Participants will also be introduced to proper evidence management & handling.

### Who Should Attend

Managers, internal auditors, CFOs, CTOs, CIOs and anyone involved in or who has direct or indirect responsibility for, the security of information systems, network infrastructures, and/or electronic information.

### Benefits

Upon completion of the seminar, participants should be able to:

- Understand the how incident response fits into the DRP/BCP model;
- Develop strategies to deal with challenges and difficulties surrounding the development of an effective incident response capability;
- Appreciate how incident response is related to the computer forensic process;
- Understand forensic friendly data management and handling processes;
- Use their knowledge to begin the process of developing a computer incident response team.
- 

### Program Outline

- 1) Information Security Basics
- 2) What is the true state of affairs
- 3) Who is targeting our systems & data, and why?
- 4) Regulated & Legislated Infosec Responsibilities
- 5) Formal Incident Response Management Methodology
- 6) Basic Computer Forensic Procedures and Liaising with "Authorities"
- 7) The Basics of Forming an Effective Computer Incident Response Capability
- 8) The Challenges and Legal Considerations

Event costs: Member \$130 Non-Member \$165 Group rate of 5 or more, \$145 per person all prices are GST included

**Note: If we must cancel a course for any reason liability is limited to the registration fee only.**

Register ONLINE or Download the registration form (MS Word format)

Our registrar is: Cheryl Devaney, phone: 945-4130 or fax: 948-3021

For ISACA membership information contact Les Hansen at 946-7918. For ISACA chapter information contact Roger Yost at 945-3277.

---

---

*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**

---