



# The Disk Patch



Volume 19 Issue No. 2

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

April, 2002

## Message From The President



Your 2002/2003 Winnipeg ISACA chapter board is listed in this issue of the ISACA newsletter. Many thanks to the remaining board members - and a big welcome to our two new board members - Anne Thompson, who is taking over secretary duties from Mike Rogers (thanks to Mike for the good work he has put in as our Secretary) and Marc Rogers who is joining the board as a Program Director.



After many years of service to ISACA, Dan Swanson is stepping down from the Winnipeg board. The board and I wish to thank Dan for his services to the chapter in promoting ISACA events and supplying us with fresh ideas for seminars and courses. Dan, it is people such as yourself that help to make our association flourish.

### *Inside This Issue:*

2001/2002 Board of Directors	2
From the Editor's Desk	3
Spotlight on "Improving Your Incident Response"	4
IT GOVERNANCE More Than A Specialized Concern	6
The Essentials of IT Project Management	10
2002/2003 Board of Directors	12
Bits & Bytes	13

Speaking of flourishing, our chapter roster now stands at 100 members!! Omena Babalola, from Western Canada Lotteries Corporation, is our official 100th member.

In the next few weeks we will be sending you the annual member survey. Please take the time to complete this survey as it is through your input that the program committee determines the courses and seminars to offer to you over the next year.

Roger Yost  
President



**Information Systems Audit and Control Association  
Board of Directors  
2001-2002**

<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	gglesmann@pao.mb.ca
Lawrence Elkow	University of Manitoba	1st Vice President/ Program Chair	cyberjet@icenter.net
Mike Rogers	University of Manitoba	Secretary	rogers@Ms.Umanitoba.CA
Fred Horbaty	PricewaterhouseCoopers	Treasurer	Fred.j.horbaty@ca.pwcglobal.com
Barry Saunders	Provincial Auditor's Office	Asst Treasurer	bsaunders@pao.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@pao.mb.ca
Jeff Murray	Ernst & Young LLP	Director Marketing	jeff.murray@ca.eyi.com
Dan Swanson	Investors Group	Director Research	dan.swanson@investorsgroup.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
Brian Mansky	City of Winnipeg	Audit Director - Program	bmansky@city.winnipeg.mb.ca
Cheryl Devaney	Internal Audit, Province	Event Registrar	Cdevaney@gov.mb.ca



## From the Editor's Desk:

For those of you with projects in mind check out **The Essentials of IT Project Management - Best Practices** with Neal Whitten, The Neal Whitten Group.

This two day event on **Monday & Tuesday, June 17 & 18, 2002** promises to be an insightful, no-nonsense, knowledge-rich, educational experience that can have an immediate and positive impact on your current or next project.

There is a breakfast event the following morning on June 19, 2002, titled **The #1 Reason Why Project Managers Fail - Being Too Soft!**

For more information and to register for these outstanding educational opportunities check out our web site at <http://www.isaca-wpg.org/>

The project management sessions were originally scheduled for May 6 and 7 with the breakfast on May 8. Those sessions filled up so fast that we had to schedule another round for June. If you are thinking about attending then register soon because the June spots are also filling up quickly.

See you there!

That's it for this year's ISACA program schedule. Thanks for making it one of our most successful ever.

And thanks to everyone who contributed information for the Disk patch. Like most good things (eg., TEAM CANADA HOCKEY!!), it is a team effort.

## 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](mailto:JWThomas@kpmg.ca)  
facsimile: (204) 957-0808

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

## The Loonie Challenge

You may recall from the last issue of Disk Patch that a challenge was issued to all readers. I flip a coin and make a bet with Roger Yost. For each toss that comes up heads I give a dollar to Roger and if it comes up tails Roger gives a dollar to me. I make a simultaneous bet with Mike Rogers so that Mike gives me a dollar when the coin comes up heads and I give Mike a dollar when it comes up tails. Finally, Roger, Mike and I agree to flip the coin five times.

Alan Gellatly received a loonie (which he promptly donated to the charity of his choice) by sending me an email describing what this illustrates about risk and control. I won't repeat what Alan said in this family rated newsletter, however I will point out that nobody picked up on the key concept I was looking for.

Risks are things that get in the way of objectives. Controls are those things that help to achieve objectives. The coin toss was a red herring because without an understanding of the objectives it is impossible to tell what is a risk and what is a control.

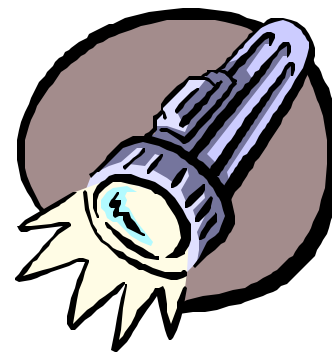
In the example, it is easy to assume that the goal of the coin toss could have been to make money or pass the time or perhaps watch Roger and Mike get worked up about winning and losing money (a few loonies goes a long way when parking the car). The fact is, as auditors, we can't afford to assume that we know what the organization's objectives are. We have to clearly understand them. What was my objective? To give a buck to a worthy charity.

Written by Jeff Thomas, the Loonie Challenger



# Spotlight On

## Executive Security Briefing: Improving Your Incident Response Management Capabilities



When a security incident occurs in your organization do you know how to **REACT**, **RESPOND**, and **RECOVER**? This was the topic of **Quarterstone Communications, Inc.**'s presentation at the Security Management conference hosted by the Winnipeg Chapter of the Institute of Internal Auditors in October 2001. The following article provides a high level summary of this in-depth presentation.

### **REACT**

Review policy and procedures  
Evaluate the situation  
Avoid panic  
Collect information  
Take appropriate action

### **RESPOND**

Request information  
Evaluate the situation  
Stop the "attack" and secure the "crime scene"  
Preserve evidence  
Organize forensic examination  
Note findings  
Determine causes

### **RECOVER**

Raise security Expectations  
Evaluate current security posture  
Create implementation plan  
Order it to be done  
Validate the implementation  
Expect the unexpected  
**RECOVER** on a regular basis

*An incident response team is critical to REACT, RESPOND and RECOVER*

### **What are the main elements of an incident response team?**

1. Director  
A person from senior management who has the authority to carry out incident response activities.
2. Lead Investigator  
Makes sure the incident response activities are followed in the correct order.
3. Forensic Technician  
Carries out incident response tasks under direction of lead investigator. The Forensic Technician must be an expert in that system. It is likely that more than one such expert will be required because different systems require different expertise.
4. Response Handler  
This person is usually the first one on the scene and is responsible for securing the crime scene and collecting evidence.
5. Evidence Handler  
The Evidence Handler Protects all evidence gathered during the course of the incident. This person also ensures the evidence is properly tagged and checked in and out of protective custody. A strict chain of custody is required.
6. Legal Advisor  
Providing guidance on all applicable laws, the Legal Advisor helps the organization decide whether to pursue any kind of legal action.
7. Dispatcher  
Available around the clock, the dispatcher receives the client's distress call and connects the client with the incident response team.

### **Anomaly**

something different, abnormal, or peculiar.

### **TERMS**

#### **Incident Response**

The timely marshalling of appropriate resources in response to a reported incident or anomaly.

### **Forensics**

The application of scientific knowledge to legal problems.

#### **Incident**

An anomaly that violates an organization's security policy.

#### **Computer Forensics**

The application of scientific knowledge to legal problems involving computer related evidence.

(Continued from page 4)

## ***So you are being attacked...***

### **REACT**

Review the IR policy and follow the procedures. It is not technically an incident until it the incident has shown to be breaking a policy.

Evaluate. Is it over? What are the assets involved? Damage?

*Follow the scientific methodology for REACT.*

1. OBSERVE
2. Hypothesize
3. Predict
4. Test
5. Expected Result
6. Provisional Acceptance
7. Report

Avoid panic. Don't let people log onto machine to figure out the problem. Don't trash the crime scene. Know your limitations.

Collect information. Start a log book. Safeguard evidence. Gather the latest configuration details.

Take appropriate action. Decide what kind of response is appropriate. If you're not sure, get expert advice and consider the legal ramifications.

### **RESPOND**

Request information. Be sure to get lots of details on the person making the notification. Find out if law enforcement is involved. Get a description of the problem and the support needs of the client.

Evaluate the situation. Determine the source of the problem. Estimate the level of effort required and identify if and when subject matter experts will be required.

Stop the attack. Take temporary measures such as disconnecting machines, changing network addresses, changing firewall rules. Be sure to secure the crime scene.

Preserve evidence. The criminal always takes something from the scene and always leaves something behind. Preserve scene. Collect all available evidence. Remember that there may be booby traps. Use digital signatures and checksums to ensure evidence is protected.

Organize the forensic examination. Follow proper evidence pre-processing to get evidence into the analysis environment without impacting integrity.

Analysis. Use a non-destructive process and remember, this evidence must stand up in a court of law. Use certifiable tools

widely used in the field by practitioners. You will need independently verifiable and repeatable results. Always question the validity of information and don't eliminate a hypothesis just because it doesn't have any supporting evidence.

Note findings and determine causes. Apply the scientific method to build timelines and rule out accidental causes. Generate a report and brief the client.

### **RECOVER**

Raise security expectations in your organization. You must have a security budget for tools, training, and user awareness. Develop baseline security configurations for all servers so that if one is hacked you know how to respond to all of them. Use security audits to assess your security profile. Ensure you have established long-term staffing requirements with committed resources and management support.

Evaluate your current security posture. Determine and document your current configurations and conduct a risk assessment.

Create an implementation plan. Revise policy and procedures. Reload system from trusted media. Apply known and proven patches. Are backups good? Create a disk image of workstations and baseline for all machines.

Order it to be done and validate the implementation. Get a status report. Does it meet all the requirements? Hold people accountable.

Expect the unexpected. Your systems will become vulnerable again with configuration changes, staff moving in and out, company policies and goals changing, so remain vigilant!

RECOVER often. Go through this process whenever anything changes and at least once a year.

## ***What are some of the keys to success?***

*Locate policy - create it if needed  
Have templates for servers and workstations  
Detection is the key*

Written by Jeff Thomas, CA, CIA, CISA, CMC  
Senior Manager, Information Risk Management  
KPMG LLP

This article is the second in a series based on presentations delivered at the IIA Security Conference in Winnipeg, October 16 to 19, 2001. The articles are intended to summarize the key thoughts of the presenter and should not be considered an alternative to conference attendance. While an attempt has been made to capture the significant elements of the presentation the reader should be aware that errors and omissions may exist and the content is highly summarized. This article was based on notes taken during the presentation as well as handouts available to conference attendees.

## **IT GOVERNANCE**

### **More Than A Specialized Concern**

#### Survey of Public Sector Board Members Has Implications for IT Governance

*By Jon Singleton, CISA, CA and Maria Capozzi, MPA, BA*

Copyright 2002. Reproduced with permission from the Information Systems Audit and Control Association® (ISACA™), Rolling Meadows, IL, USA 60008.

Governance is an issue that is currently receiving a great deal of attention in Canada, both in the private and public sectors. Recent private sector board scandals have made headlines, causing Canadians to question once again whether our current approaches to corporate governance are as effective as desired. It is important to note that the public sector is not immune to such failures in its governance practices.

There has been a general recognition in Canada that effective governance in public sector organizations is an important contributor to the well being of our communities. At the Provincial Auditor's Office, we believe that effective governance in public sector organizations can contribute a great deal to organizational effectiveness and stronger accountability processes; key components in ensuring that citizens are well served by their public institutions.

Our Office has long recognized the importance of IT to the success of enterprises, and, conversely, the threat that poorly managed IT strategies pose for organizations. In this article, we will share some thoughts on how the learning we have gleaned from board members and senior managers can be considered in the context of IT governance.

Consistent with our Office vision of contributing to greater public trust and confidence in the institutions of government, we began a dialogue on improving governance by producing a series of reports to our Legislative Assembly<sup>1</sup> that examined the board governance practices of various public sector boards within the government reporting entity. These studies surveyed board members and Chief Executive Officers (CEOs) of public boards on a variety of issues related to corporate governance. Our purpose in conducting these studies was to gain an improved understanding of the state of board governance and to foster a dialogue around improving public sector board governance practices. The interest and ongoing discussion generated by these reports confirm that our citizens have a strong interest in issues of governance.

#### **What Is Governance?**

Governance is a process of transformation, with people working together in specified relationships to enable effective

decision-making. With its focus on the responsibilities and actions of governing bodies, governance involves:

- **Setting Direction:** the aim towards which a board steers itself and its organization;
- **People:** board members exercising and expressing their attitudes, beliefs, and values on matters pertaining to the mandate of the organization;
- **Structure and Processes:** the formal means used to achieve the aim, and to direct and manage an organization's operations and activities.

A review of leading research, perspectives and practices of board governance reveals a number of models and approaches, each of which build upon the four pillars of good governance:

1. **Stewardship:** As stewards, boards act for others, have authority over their organization, and are trustees of their organization's mandate as well as its resources. A board therefore is sovereign and has ultimate authority for its organization. As a result of this stewardship, public sector boards must honor the trust citizens have placed in it.
2. **Leadership:** Governance fulfills a leadership function for society. As leaders, boards are expected to reflect the value system and priorities of the community from which they are drawn. Through the board, individuals accept the challenge to develop positive relationships, ensure respect between parties, and build a sense of belonging in the group. Leadership is about the relationship between the governors and those governed.
3. **Responsibility:** Having a fiduciary responsibility, boards are expected to manage the resources of the organization efficiently and effectively to accomplish the desired aim. Board members are expected to be reliable, and to allow appropriate factors to affect their judgement, including consideration of the effect of their choices on others. They are also expected to devote the personal time and energy to ensure that governance is appropriate and adequate.
4. **Accountability:** Boards are ultimately accountable for the actions of their organization. Accountability is the obligation to answer for the discharge of responsibilities conferred and that affect others in important ways. It requires that boards understand who is responsible for what, what performance is to be achieved, and what information needs to be shared to ensure appropriate decision-making.

<sup>1</sup>An Examination of Governance in Manitoba's Crown Organizations, 1998 and An Examination of School Board Governance in Manitoba, 2000; Office of the Provincial Auditor of Manitoba. Copies available at [www.pao.mb.ca](http://www.pao.mb.ca)

### More Than A Specialized Concern

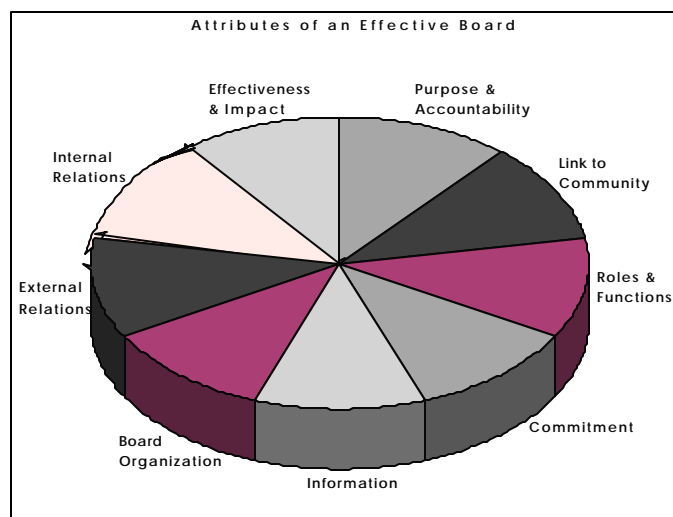
Survey of Public Sector Board Members Has Implications for IT Governance

(Continued from page 6)

Within these four pillars, there is a core perspective on what it is that a board should do. Drawing on this, our Office developed a Model for Governance (Figure 1) which operationalizes each of these four pillars, incorporating both a structural and behavioural perspective to board governance. The Model represents the attributes of an effective board, which should:

- Be accountable for the effectiveness of the organization in achieving a set of agreed-upon priorities that are based upon clearly understood goals;
- Be clear on who the board represents;
- Be clear on the role of the board and its responsibilities;
- Have members on the board who are committed to the organization;
- Have the appropriate information to make decisions;
- Be organized as a board with appropriate structures and processes;
- Maintain appropriate linkages with external organizations and stakeholders;
- Define clear relations with the Chief Executive Officer and staff;
- Make policy decisions for the organization and, as necessary, change recommendations made to the board by the administration.

We believe that, in general, the more a board fulfils each of these attributes, the more effective it is.



### How Does This Relate to IT Governance?

The above discussion of governance has focused on board governance generally. However, it can be broadened to incorporate the definition of IT governance put forward by the IT Governance Institute:

*IT governance, like other governance subjects, is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organization structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.*<sup>2</sup>

Our Model of Governance incorporates this IT perspective within its attributes and highlights that information is an important and key component of board effectiveness. IT system reliability is critical to board decision-making and ultimately, the success of the organization.

### KEY SURVEY FINDINGS AND THEIR IMPLICATION FOR IT GOVERNANCE

#### Board Purpose and Accountability

A shared aim is vital for effective governance. By holding a purpose in common, a set of individuals coalesces into a group, a team – the board. Given that formal goals are often vague, debating the goals and identifying shared priorities are two of the key activities that help a board add meaning to the shared aim. Effective governance requires significant time and attention be paid to organizational vision, mission, goals and priorities. The board has a responsibility to then be accountable for what is accomplished relative to those strategic goals and priorities. Being responsible for direction and accountable for actions situates the board as the ultimate authority for an organization.

Our studies found that while public sector board members and CEOs understand the goals of their organization and accept that the board is accountable, the responsibility for governance is perceived to be shared with government and other stakeholders. Our reports raised the question of how to reconcile a board's ultimate accountability with this perception of shared governance.

From an IT governance perspective, there needs to be compatibility and alignment between the strategic priorities of the enterprise and the strategic goals of IT. In fact, for many organizations, the pervasive use of technology has created a critical dependency on IT. IT success is therefore integral to

(Continued on page 8)

<sup>2</sup>Board Briefing on IT Governance, IT Governance Institute, 2001. Copy available at [www.ITgovernance.org](http://www.ITgovernance.org)

## **More Than A Specialized Concern**

Survey of Public Sector Board Members Has Implications for IT Governance

*(Continued from page 7)*

the success of the organization. The key question is whether an organization's IT investment is in harmony with its strategic objectives and thus building the capabilities necessary to deliver business value. The value that IT adds to the organization is a function of the degree to which IT is aligned and integrated with the organization's strategies and whether it meets the expectations of the organization. Further, it is appropriate for the board to give thought as to who is accountable for IT strategy. A review of best practices indicates an integrated approach where the board is involved in IT strategy and IT is involved in overall organizational strategy may best ensure the board's ultimate accountability for IT governance is fulfilled.

### **Board Functions and Performance**

The board job is comprised of a set of roles and associated functions. In addition to the role of ultimate authority, the board is also expected to act as a constructive critic of, and advocate for, the organization. Each of these three board roles has different expectations associated with it: when one is an advocate, one is celebrating the contributions of the organization to the community; when one is a constructive critic, one is examining that which the organization has actually accomplished or is proposing to accomplish; and as discussed previously, when one is the ultimate authority, one is concerned with mandate and accountability. These roles can require quite different mindsets and behaviours. As what is required in one role may conflict with another, it is important for a board to be clear on which role is being performed at any given time.

Our studies found that board members and CEOs accept these roles, but self-identify a performance gap between the desired and actual performance of their board on particular functions. Our reports raise the question of whether this results in less effective governance than is desirable and what measures can be taken to improve the board's functional performance.

From an IT governance perspective, the board's function and responsibilities as it relates to IT are not often clearly understood. Yet, ultimate responsibility for IT risk management and control rests with the board. Therefore, it may no longer be sufficient to relegate IT strategy and responsibility to a department "out there". As IT system reliability is an important element of governance, boards should reflect upon how to improve their performance in relation to IT functions. One option to ensure that IT risks are transparent and appropriately mitigated to a level deemed acceptable by the board may be for the board to create a specialized IT Committee of the board. The Chief Information Officer, reporting directly to the CEO, could work closely with this board committee in assisting the board in fulfilling

its IT governance responsibilities.

### **Board Information for Decision-Making**

Information is a key contributor to effective board decision-making. Board members have a duty to demand and expect quality information on a timely basis. In addition, as board members have only a limited amount of time to devote to board duties, the production, management and distribution of information is extremely important. While it is often assumed that board members will give to their board all the time and energy needed for good governance, this assumption is not consistent with the part-time nature of most board positions. Moreover it does not recognize the collective nature of boards, in which members do not necessarily devote equal levels of commitment to board duties and may in fact leave the actual work of governance to others. For this reason, pertinent and timely management information must be presented to board members to best ensure effective governance. In most organizations today, the quality of such management information depends greatly on the IT system and its reliability.

Our studies found that while board members perceive the management information available to their boards to be appropriate and useful for decision-making, it was not always timely or adequately presented. Further, there was a high reliance on management as the single source of information.

From an IT governance perspective, IT systems are a critical component in ensuring the quality and timeliness of information received by board members. Utilizing IT to optimize the information that is available to board members can have a considerable impact on the decision-making capabilities of the board. Further, the more efficiently the information flow to board members can occur, the more effective the utilization of board members' limited time and energy. Once again, the creation of a specialized IT Committee of the board may be an effective strategy to harness the power of IT to its best possible advantage. The provision of quality information to the board in a timely manner can perhaps be the most important catalyst in improving the board's decision-making and overall performance, and ultimately, its impact on the organization.

### **Board Membership**

Board legitimacy comes, in part, from it being comprised of individuals who represent appropriate communities and stakeholders. Clarity as to whom board members represent and on whose behalf they act is a fundamental component of effective board governance. Further, to do its job effectively, a board needs to build a team in which the members have the appropriate mix of knowledge and expertise, and in which the members feel free to participate and contribute.

Our studies found board members and CEOs agreed that the representation of certain board member skills and

*(Continued on page 9)*

## **More Than A Specialized Concern**

Survey of Public Sector Board Members Has Implications for IT Governance

*(Continued from page 8)*

characteristics on their boards is not as strong as they would like. They also noted that the board member recruitment process was not adequately managed by the board. Our reports raise this as an area which warrants further examination by boards in order to ensure they have the necessary skills, expertise and characteristics required.

Some of the more common skills or knowledge found on boards of directors include accounting, law, and general management. In specialized sectors, insurance companies may see the need to have actuarial expertise represented on their boards, and utilities may wish to have engineering skills represented. It is our belief that board's should give greater recognition to the need to have appropriate strategic IT skills represented at the board table. We believe that this flows logically and inexorably from any consideration of the importance of IT to enterprise success in both the private and public sectors.

### **Board Impact**

Determining the effectiveness of a board has been the subject of much research. As no objective indicators of effectiveness have been developed, the standard approach is to ask board members to self-assess their board's effectiveness. The limitation with this approach is that it is strictly a value-judgement made by those directly involved and research studies indicate that people, in making such value-judgements of their own effectiveness, are largely over-confident.

To move beyond such self-assessments, our studies consider how a board actually impacts, or makes a difference to, the organization for which it is responsible. While some board evaluations look to policy generation as a measure of impact, this indicator is not a unique activity upon which to assess board effectiveness, as many different parts of an organization are involved in the development of policy. Boards do however, specifically make decisions. Thus, our studies defined the board's service to its organization, or it's output, as its decisions. The impact of those decisions on the organization was deemed to be the desired outcome of the board.

Our studies found that board members self-assess their performance to be effective. However, many board members noted that they do not conduct board evaluations nor take the time to review and assess their performance on a regular basis. Further, while decision-making is perceived to be efficient, the impact of those decisions is somewhat more limited, as about a quarter of board members indicated a concern that their board acts as a "rubber stamp" for decisions reached by management. While board members agreed that the board should make changes, as necessary, to the policy

recommendations of management, few perceived that such changes actually occurred.

It is often the case that boards believe they are effective if their organization is successful. However, it is our belief that board effectiveness can be differentiated from organizational effectiveness. It should not be assumed that a board is effective when its organization achieves success, nor conversely, that a board is ineffective if its organization experiences difficulties. Distinguishing board effectiveness from organizational performance necessitates that a board clarify its desired outcomes and that it establish objective measures to evaluate its achievement of those outcomes. From an IT governance perspective, the board must clarify its desired outcomes with respect to IT governance and reflect on how IT has contributed overall to the board's effectiveness. The utilization of the balanced scorecard with respect to IT governance can be a useful tool in measuring IT performance and demonstrating the value that IT delivers to the organization. When linked to the overall business balanced scorecard, it can provide for the board the most complete picture of strategic alignment and performance.

### **Concluding Thoughts**

Effective governance in any organization takes hard work and sustained effort. The intriguing thing about governance is that, as with most human enterprises, it can always be improved.

However, there is no "one size fits all" solution for effective governance. Our Model of Governance outlines a number of attributes for effective governance, which can be further broadened to incorporate the key components of IT governance. This article is simply a starting point for board discussions around best practices and practical solutions that will suit each board's unique situation. The issues raised with respect to IT governance will hopefully provide a basis for a vibrant dialogue among board members, senior executives, IT specialists and auditors on enhancing both enterprise and IT governance practices.

---

#### **Jon Singleton, CISA, CA**

Was appointed to the IT Governance Board in 2001. In 1995/96, he was international president of the Information Systems Audit and Control Association, having previously served as vice president of certification. He was also a founding member of ISACA's Winnipeg Chapter in 1981. Currently, Singleton is the Provincial Auditor of Manitoba.

#### **Maria Capozzi, MPA, BA**

Is the manager of governance services, Office of the Provincial Auditor of Manitoba (Canada). Governance services provides assessments and advice on issues related to board governance practices of various public sector and government-funded entities.

# The Essentials of IT Project Management: Best Practices

## Monday & Tuesday

## June 17 18, 2002

Royal Crown Conference Center (Winnipeg, Manitoba)

7:45 AM – 4:30 PM

Presented (Jointly) By:

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

&

THE MANITOBA CHAPTER OF THE  
PROJECT MANAGEMENT INSTITUTE (PMI)

**For further information contact**

*Dan Swanson, Seminar Co-Chair (ISACA) - (204) 956-8625*

*Brenda Nylund, Seminar Co-chair (PMI) - (204) 788-2517*

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

## **Course Description**

### **Overview**

An insightful, no-nonsense, knowledge-rich, educational experience that can have an immediate and positive impact on your current or next project. This workshop cuts to the quick and reveals the essentials in practicing effective software project management-the first time. Based largely on two of Neal's books, [The EnterPrize Organization: Organizing Software Projects for Accountability and Success](#) and [Managing Software Development Projects: Formula for Success](#), this workshop identifies the most common "big ticket" project management problems plaguing software development projects — and shows you how to effectively deal with them.

As the need to focus on schedules, costs and quality continues to increase across the industry, it is more important than ever to understand and overcome the major inhibitors to achieving competitiveness. [Prepare to learn more than just conventional project management, prepare to learn about yourself and how to make things happen to achieve success.](#)

### **Who Should Attend**

This workshop is for Project Managers, MIS and Functional Managers, Team Leaders, Quality Assurance Personnel including IT Auditors, and anyone and everyone involved in the software development cycle: Planners, Developers, Testers, Writers, and Support Personnel. [Great refresher/booster for Seasoned Project Managers.](#)

---

## Your Workshop Experience Will Cover

- Identify and correct the most common "big ticket" project management problems for software development projects.
- Employ many proven practices that speed product development.
- Define and implement a software development process.
- Implement effective scheduling, tracking, and problem management.
- Improve vendor/contractor relationships.
- Examine project management problems that attendees are now experiencing and discuss their potential solutions.
- Bring about positive change in your team or project through leadership and motivation.

## Workshop Outline

- I. Introduction
- II. The Project Manager — and Other Project Roles
- III. Defining a Software Development Process
- IV. Project Planning
- V. Project Tracking and Problem Management
- VI. Softskills: Attributes of Successful Project Leaders
- VII. Project Reviews
- VIII. Earned Value
- IX. Vendor and Contractor Relationships
- X. Lessons Learned
- XI. Other Project Management Topics
- XII. People Communications
- XIII. Promoting Project Success

## The Essentials of IT Project Management: Best Practices

**Monday & Tuesday**  
**June 17 18, 2002**  
**Royal Crown Conference Center**  
**(Winnipeg, Manitoba)**  
**7:45 AM – 4:30 PM**

The workshop material is largely derived from two of Neal's books, [The EnterPrize Organization: Organizing Software Projects for Accountability and Success](#), and [Managing Software Development Projects: Formula for Success](#). [The workshop materials include both books \(a \\$95 U.S. Value\) and a notebook containing viewcharts, exercises and supplementary reading materials.](#)

Event costs: Member \$675 Non-Member \$775 Student \$675 GST included

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

## Registration

Cheryl Devaney, phone: 945-4130 or fax: 948-3021 or email: [Cdevaney@gov.mb.ca](mailto:Cdevaney@gov.mb.ca)  
Download registration form (MS Word format) 52 K

**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@pao.mb.ca
Lawrence Elkow	University of Manitoba	1st Vice President/ Program Chair	cyberjet@icenter.net
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	bsaunders@pao.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@pao.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	Deloitte & Touche	Program Director	mkr@escape.ca
Brian Mansky	City of Winnipeg	Audit Director - Program	bmansky@city.winnipeg.mb.ca
Cheryl Devaney	Internal Audit, Province	Event Registrar	Cdevaney@gov.mb.ca

Welcome new  
board members  
Anne Thompson  
and Marc Rogers



---

---

# Bits & Bytes

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

010011010011000101101001001110101110100110110110100100101101000110011011000110101

## **Award Winning Winnipeg Chapter!**

Our chapter web site at <http://www.isaca-wpg.org> has just won a silver award in the **2002 ISACA 'Best Web Site' Awards**. This is the first year for these awards. The awards recognise chapters with outstanding web sites.

Congratulations to our webmasters, Michael Li and Howard Yip for their excellent work on our web site.

## **Certification 2002 CISA Exam**

Registration for the 2002 CISA® examination continues on a record pace. Candidates are reminded that the final registration deadline is 3 April 2002.

A PDF of the *2002 CISA Bulletin of Information* is available at [www.isaca.org/exam1.htm](http://www.isaca.org/exam1.htm).

## **New CISA Status Approved**

The CISA Certification Board recently approved the implementation of a new CISA status, the CISA Non-practicing status. Effective 1 January 2002, the CISA Non-practicing status replaces the former CISA Inactive status.

CISAs currently in the Inactive status were informed of this change via e-mail. If any chapter members are currently holding an Inactive status please review the email sent out and take the appropriate action. Also, if you anticipate leaving the field but wish to retain your CISA, please contact the certification department at [certification@isaca.org](mailto:certification@isaca.org) to request further information on the Non-practicing status.

## **Credentialing Task Force Update**

The Credentialing Task Force has recently completed the development of a draft job analysis for a new information security credential, designed to provide executive management with assurance that those earning this designation have the required knowledge to provide effective security management and consulting. It will be business oriented and focused

on information risk management while addressing management, design and technical security issues at a conceptual level. This credential will be directed at information security management, which differentiates it from CISSP and other IT security credentials oriented toward testing specialist-based skills.

The draft job analysis was distributed to a select group of subject matter experts, and the results will be reviewed by the Credentialing Task Force. Once the job analysis is finalized, it will be distributed to a sample of information security professionals for further review and domain weighting. Members who are practicing as information security professionals and wish to participate in this review should contact Terry Trsar at [ttrsar@isaca.org](mailto:ttrsar@isaca.org).

## **ISACA International HQ Computer System Update**

The implementation of the new computer system at International Headquarters has entered a system fit analysis stage. Staff is identifying and specifying needs and reviewing potential system modifications in cases where the standard system does not meet business requirements. All proposed modifications are evaluated to ensure the integrity of the upgrade path is maintained. This phase will continue through early April, at which time the new software will be presented for testing and review.

The transition to the new system is scheduled to take place in June. Web applications will be implemented through the second half of 2002. For more information on the computer system, visit the FAQ document posted at [www.isaca.org/computer.faq.htm](http://www.isaca.org/computer.faq.htm).

## **International Conference**

(7-10 July 2002; New York City, New York, USA)  
This year's International Conference will address the most critical issues facing management today. Tracks will include: IT Governance and Control, IT Security Issues, IT Audit Issues and IT Business Issues. Visit the ISACA web site, [www.isaca.org/conf1.htm](http://www.isaca.org/conf1.htm), for more information as the conference draws nearer.

(Continued on page 14)

---

---

# Bits & Bytes

(Continued from page 13)

## Education

### Education Board Project

ISACA's Education Board has recently initiated a project to collect, summarize and report on the tasks and responsibilities of information systems (IS) auditors and the ways in which they are trained to perform their duties. The first phase of the project will focus on IS auditors who have just entered the field (with no prior audit experience), and subsequent phases will focus on different levels of IS auditors up to those individuals who have reached an IS audit manager status.

At this time, the Education Board is asking ISACA members and chapters to assist in this project by collecting and providing the following information as it pertains to their organizations:

- Copies of IS auditor job descriptions
- General IS auditor training schedules that include:

- General subject matter covered (not internal operations specific training)
- When in the experience cycle, or at which audit level, information is covered
- How it is presented (on the job, at internal training, at external training)
  - Estimates of average number of years until an IS auditor attains:
    - Senior auditor level
    - Supervisor auditor level
    - Manager auditor level

Members willing to share such information for use in this project should send it to Terry Trsar, chief professional development officer of ISACA, at: 3701 Algonquin Road, Suite 1010; Rolling Meadows, Illinois USA 60008; Phone: +1.847.590.7451; Fax: +1.847.253.1443; and e-mail: [ttrsar@isaca.org](mailto:ttrsar@isaca.org).

## Research Projects in Progress

### Electronic/Digital Signature Legislation Project

This publication will use UN and EU regulations as a basis for comparison of country laws around the globe. It will provide an analysis of what the assurance and control professional should look for when addressing electronic/digital signatures. Project completion is planned for the first quarter of 2002.

### Creating the Privacy-compliant Organization

The ISACF Research Board is developing a management guide to address the complex issues of privacy. The guide will include sample policies, a 10-step methodology, work plans, questionnaires and templates to guide the organization through the process of meeting legislative, regulatory and marketplace expectations of and demands for personal information privacy. Look for availability in the first quarter of 2002.

### Security and Risk Management in an SAP Environment

There has been a need for a series of definitive audit guides, including details on testing techniques within specific ERP products and their execution, for some time. The project will deliver a technical reference guide that will cover application security risk, audit and technical infrastructure considerations over SAP. The purpose of this research is to document current best practices in SAP risk and control issues and to provide a comprehensive reference guide for assurance and control professionals. This project will be completed in the first quarter of 2002.

### Security Provisioning in the New Economy

"Turning up" and "turning down" access privileges are not quite as simple as flicking a switch. Provisioning encompasses much more than assigning user passwords. It requires companies to determine roles based on

predefined business policies and standards, and then assign the appropriate roles to the appropriate users. The objective of this research is to present to senior management, CIOs, COOs and CISOs the concept of resource provisioning management solutions in the current business arena and explain why companies should move toward establishing a single authoritative system for tracking and granting access to resources within the organization. Project completion is expected in the first quarter 2002.

### Wireless Communication Project

Because wireless communications transcend traditional and regulatory boundaries, they pose significant technical challenges, as well as greater challenges in the areas of control, security and audit. Wireless users expect the same features they enjoy on their home network when they roam onto foreign networks and expect to use their communications devices wherever they travel. This project will provide both a technical

(Continued on page 15)

---

# Bits & Bytes

(Continued from page 14)

and functional assessment and will be written from a business and risk management perspective. The project is targeted for completion in first quarter 2002 beginning with several articles, a white paper posted to the ISACA web site and ending with a full publication.

## Oracle Database Project

Work has begun on an update to *Security and Controls in an Oracle Environment*, a part of the ISACA Monograph Series. The revised edition will include the issues that have changed in subsequent Oracle environments, resulting in the addition or removal of topics from the book, and a recommended plan for addressing the changes. Project completion is expected in second quarter 2002.

## OS/390 (Z/OS) Project

This research will include updates to the recent revisions of the legacy functions of the operating system and outline the system components and their interaction. The project's focus will include: system initialization; security functions; audit tools and methods; detailed descriptions of new components and functions in the above areas; recently added functions, mainly those that permit the use of the Internet; and UNIX functions in the OS/390 environment. Project completion is targeted for second quarter 2002.

## Net Markets Project

ISACF, in cooperation with the Canadian Institute of Chartered Accountants (CICA), is about to embark on a research project to identify the various business, risk, governance, assurance and control issues raised by the existence of net markets and procurement. The research is intended to define these issues, focus on the business issues at hand, provide guidance to those operating or reviewing net markets and address how this environment can be effectively controlled, given the known risks. Project completion is expected in the third quarter 2002.

## 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 trustworthiness of information across the enterprise. The purpose of this project is to define

the key elements of enterprise information integrity, as well as benefits criteria associated with them, and to present a framework and process for management. The Centre for IS Assurance is conducting this project for ISACF.

## Adding a Dimension to COBIT®

COBIT welcomes a new family member—the *IT Control Practices Statements*. Recently the COBIT Steering Committee celebrated the 10<sup>th</sup> anniversary of the birth of the concepts underlying COBIT. Ten years and so much hard work later, COBIT has gained international acceptance and has become *the* reference for IT control and governance. Many use COBIT as a reference work, some have succeeded to COBIT-ize processes in their organizations, but few have labeled COBIT as easy to implement. Indeed, numerous are the requests for more detail, added guidelines for implementation and verification of compliance, and clarifications of the rationale of some of the controls suggested by COBIT.

And that is where the *IT Control Practice Statements* come into play. IT control practices expand the capabilities of COBIT by providing the practitioner with an additional level of detail. The current COBIT IT processes, business requirements and detailed control objectives define what needs to be done to implement an effective control structure. The IT control practices provide the more detailed *how* and *why* needed by management, service providers, end users and control professionals to implement highly specific controls based on an analysis of operational and IT risks. The COBIT conceptual framework is thus extended with a more specific implementation focus that is further presented in the control practices.

The IT Governance Institute has published the first control practice statement. The control practice statement for PO-9 “Manage Risks” is available to members for download at [www.isaca.org/@member](http://www.isaca.org/@member). Please test the document and provide any and all comments (a questionnaire is attached to the document and posted at [www.isaca.org/cpsq.htm](http://www.isaca.org/cpsq.htm)).

COBIT 3<sup>rd</sup> Edition® can be ordered through the bookstore at [www.isaca.org/bookstore.htm](http://www.isaca.org/bookstore.htm). Please also review the COBIT home page to see how many organizations around the world are using COBIT. The COBIT Steering Committee is looking into future enhancements to the COBIT family of products. Some of these ideas include a benchmark tool to enhance the maturity models and a version of COBIT for small- to medium-sized enterprises

---

---

**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

---