

Calgary Chapter

April 2007
Volume 1, Issue 1

Information Systems Audit and Control Association

HIGHLIGHTS

Monthly ISACA Luncheon Dates	1
President's Message	1
Article: Promoting IT Governance	2
Article: Preparing for the Security Audit	5
Article: E-Commerce Security	8
Code of Ethics	9
e-Symposia Archive	9
Education News	10
ISACA International News	11
Call for Articles	12
Reader Survey	12
Naming Contest	12

CHAPTER OFFICERS & DIRECTORS

Greg Winters, President
Sanjeev Saha, Vice President
Barbara Clay, Treasurer
Andy Heale, Secretary
Leanne Roberts, Education Director
Kishore Iyer, Program Director
Jagruiti Sampat, Membership Director
Jarka Winters, Communications Director
Brian Sorrell, Corporate Relations Director
Alvaro Janikian, Technology Director
Kimberly Greenizan, Academic Advocate
Beata Biel, Webmaster
Linda Chan, Newsletter Editor



Website: www.isaca-calgary.ca
Email: vpres01@isaca-calgary.ca

Monthly ISACA Luncheon Dates

Date & Time: April 17, 2007
from 11:30AM to 1:00PM

Topic: Critical Infrastructure Control Systems – SCADA

Speaker: Vincent Chiew, City of Calgary

Location: Palliser Hotel, 133 - 9th Avenue SW

Date & Time: May 15, 2007
from 11:30AM to 1:00PM

Topic: Making a Business Case for Information Security

Speaker: Elaine Wong & Leonard Wiens, KPMG

Location: Palliser Hotel, 133 - 9th Avenue SW

Date & Time: June 21, 2007
from 11:30AM to 1:00PM

Topic: TBD

Speaker: TBD

Location: Palliser Hotel, 133 - 9th Avenue SW

- Members: \$35.00 (in advance)
- Non-members: \$40.00 (in advance)
- At the Door: \$40.00 (Subject to availability, a meal is not guaranteed)

President's Message

Dear Members,

I am very pleased to be writing you this message in the new ISACA Calgary Chapter newsletter! Since September 2006, the new board has been working hard to identify opportunities to improve our services and benefits to the members, and we're very excited to launch this newsletter after several months of preparation. We intend to publish the newsletter quarterly beginning with this issue.

Our aim is to put interesting information into your hands about what's happening in the world of IT Governance, Risk and Control, along with things that are going on right here in Calgary that will provide value to you and your organizations in a practical way. Look for articles about IS auditing in the oil & gas sector, interviews with local IS/IT leaders, and information on how leading companies in Calgary are addressing issues related to IT governance, including achieving compliance with

internal control legislation.

My personal thanks go out to our Newsletter Editor, Ms. Linda Chan, for her hard work and dedication to making this newsletter possible, and to Ms. Jarka Winters for her leadership as Communications Director.

As this is the first issue, we welcome your comments and suggestions on how we might make this a better newsletter. Please send your feedback to news01@isaca-calgary.ca - and don't hesitate to contribute articles or to contact us if you would like to help out!

I look forward to seeing you at one of our upcoming events.

Sincerely,
Greg Winters
President, ISACA Calgary



What Our Readers Can Expect

We have designed the newsletter around the CISA® job practice areas, and plan to feature articles on one or more of the following in each issue:

- IT Governance;
- IS Audit Process;
- Protection of Information Assets;
- Systems and Infrastructure Lifecycle Management;
- IT Service Delivery; and
- Business Continuity and Disaster Recovery Planning.

As we move forward, we also hope to add interviews and homegrown articles into the mix so that we can feature more local content for you, our members.

The next issue will be published in July 2007 so watch out for it in your email and on our website!

Promoting IT Governance at the CEO Level

Crossing the language divide between senior executives and internal auditors is important to ensure audit reports are understood and IT governance becomes a business priority.

By Jackie Bassett, CEO
BT INDUSTRIALS INC.

Many internal auditors use compliance with different laws and industry regulations, such as Europe's Risk Management Basel II Accord and the U.S. Sarbanes-Oxley Act of 2002, as a way to make IT governance a priority among senior managers and executive boards. Unfortunately, getting the attention of executives may not be as easy as it seems. It's not that internal auditors and executives don't want the same results — they do. Auditors and executives simply express their goals differently.

One of the main objectives of [IT governance](#) is the adoption of standards and best practices that ensure business success and continuity — this is where both auditors and corporate executives talk the same language. However, from here, they usually go their separate ways. Getting the attention of executives happens fastest when the behavioral delta is smallest. Therefore, internal auditors need to communicate audit results in a language senior executives know and understand for IT governance to be a priority.

IT GOVERNANCE AS A KEY BUSINESS OBJECTIVE

Today's chief executive officers (CEOs) must deal with equally compelling priorities simultaneously. For instance, a CEO's primary focus might be to drive innovation in an increasingly competitive global economy, while simultaneously growing new sources of revenue and maintaining existing profit margins in rapidly maturing markets. Consequently, although IT governance might be a business priority, it may not be at the top of the CEO's list. The fastest way for IT governance to become a priority is for CEOs to understand the added value of IT governance and its key role in other business priorities.

Internal auditors are in the perfect position to promote the significance of IT governance due to their knowledge of governance and compliance best

practices. The challenge for auditors is to align report recommendations with strategic goals and objectives. Doing so will help ensure the implementation of audit report recommendations and help CEOs see the value of IT governance as a top business priority.

Often times, internal auditors believe they've laid out an action plan in their IT audit reports as part of their recommendations. The problem lies when CEOs don't fully grasp these recommendations — many senior executives simply may not have the IT knowledge needed to translate recommendations into a plan of action that aligns with company-wide initiatives. For example, CEOs, who speak in terms of gross margins and EBITDA (i.e., earnings before interest, taxes, depreciation, and amortization), may not understand how compliance with the IT components of Basel II or Sarbanes-Oxley can help the company's bottom line (e.g., higher sales and stock prices).

To help CEOs cross this language barrier, internal auditors need to translate audit reports into information CEOs will find useful. Otherwise, recommendations will continue to get lost in translation and IT governance efforts will continue to take a back seat. Questions pertaining to IT governance internal auditors should keep in mind when drafting audit reports include:

- What is the business value of IT governance?
- How can IT governance directly contribute to revenues, profitability, and shareholder value?
- What is the relevance and perceived value of audit recommendations to a CEO?

While addressing these questions, auditors should present the information in a way that enables CEOs to take action. Doing so will help bring IT governance to the forefront and become more than a cost of doing business or a checkmark in a CEO's agenda.

Auditors also should remember that the ultimate goal of IT governance goes far beyond writing an audit report — auditors need to provide recommendations that are implemented effectively and efficiently for IT governance to succeed. Unless executives



What's New?

We're pleased to announce that the Calgary chapter of ISACA is now officially the third largest in Canada with 326 members (and counting)! We recently surpassed the Vancouver and Ottawa Valley chapters in size.

Also, ISACA Calgary has partnered with **Nonfiction Studios Inc.** to release a new chapter website. The newly designed website is set to be released in early summer.

Chapter members and non-members can look forward to a new look and feel to the website including the addition of new functionality.

More detailed information will follow in the coming months.

Continued from page 2

understand the recommendations provided in the audit report, and the negative consequences associated with maintaining the status quo, audit results will not get the level of attention they deserve.

IMPROVING THE VALUE OF IT GOVERNANCE TO CEOs

Internal auditors know the importance of companywide adoption of standards and best practices. Employing proper information systems, resources, and controls maximizes business processes and minimizes risk.

Successfully reaching the CEO requires the description of relatable scenarios that are specific to the audited company. These scenarios should be part of the report, thus enabling CEOs to incorporate audit recommendations into companywide goals and objectives. The following three scenarios will help illustrate how auditors can best communicate recommendations to make IT governance a top business priority.

Scenario 1: An audit report from a publicly traded company indicated that some of its quality assurance (QA) reporting systems have critical interoperability failures — several critical application controls were missing, which pose a serious security risk to the company's customer service activities. These missing controls were the result of faulty programming code during the software development phase. In this scenario, how does the adoption of compliance standards translate into CEO items for immediate action, such as profit margins and stock price?

Auditors can answer this question by indicating how the implementation of effective IT controls and monitoring mechanisms enable companies to have the necessary QA controls needed to identify programming errors earlier in the product's lifecycle. This would result in a higher quality application that helps the company bring in expected sales revenues. In addition, the potential impact of implementing sound QA controls can help internal auditors bring IT governance best practices to the forefront and allow the CEO to understand how implementing effective IT controls benefits the company's profit margin and stock price.

Auditors also can point out the negative consequences of not implementing audit recommendations. Using the same example above, auditors could let CEOs know what

would happen if sound QA controls are not established. For instance, disregarding report recommendations to fix QA control deficiencies can make it easier for a security breach to occur, thus compromising the integrity of sensitive customer information. The negative effects of a security breach could be catastrophic for a company, potentially leading to lower customer and stockholder confidence, and a decrease in sales and stock value.

Although the knowledge that IT controls improve quality is intuitive to internal auditors, a CEO reading an audit report may not be able to make this connection if the report does not specify how IT governance best practices can improve the company's bottom line. A language CEOs can understand and that provides real or hypothetical examples executives can relate to can give CEOs enough incentive to take action on audit recommendations.

Scenario 2: The company is developing a database application that will enhance the way data is captured and used. How can compliance with IT best practices in data management ensure that the product is innovative and its launch is successful? Innovation is a primary focus of many companies in today's increasingly competitive global economy. However, innovation demands great discipline. IT governance best practices allow companies to have the IT infrastructure necessary to support a well-disciplined process or, in this case, a product launch. Suppose an IT audit report finds that the company has poor internal processes in customer data capture, including a lack of input consistency and extensive delays in the reporting of customer purchasing activity. An effective audit report states what is wrong and makes the appropriate recommendations.

To ensure a successful implementation of recommendations, auditors should align their suggestions for IT infrastructure improvements directly with the company's business goal of driving innovation. Audit recommendations need to be stated in terms of the potential for improved margins and inventory as the result of having more relevant information available in a shorter period of time. For instance, a faulty product design might lead the executive team to make innovative product strategy decisions based on erroneous customer information from the database application. Following audit report recommendations will enable CEOs to make decisions based on the most



To Contact ISACA Global
 Voice.....+1.847.253.1545
 Fax.....+1.847.253.1443
 Web www.isaca.org
 E-mail info@isaca.org

CISA® and CISM® Scoring Change

The CISA® and CISM® certification boards recently approved changing the way exams are scored. To alleviate confusion found with the previous scoring method and to provide greater clarity, ISACA will use a 200-800 point scale with a passing point of 450 beginning with the June 2007 exams. Using a 200-800 scale will increase the range of scores and eliminate the perception that the score is a percentage. This scoring method is used by several testing organizations, including the well-respected SAT and GRE exams.

Continued from page 3

accurate, relevant data, thus maximizing corporate data assets and resources.

Scenario 3: A final example of how to reach CEOs successfully can be seen in today's mergers and acquisition environment. Interfaces are key controls, such as feeds from a company's central billing system into its general ledger and financial reporting packages. Most IT infrastructures support thousands of company reports that are part of their financial reporting processes. Standards and best practices in system configuration, change management, and data management all impact the accuracy of those reports.

Offentimes, internal auditors recommend the implementation of IT best practices and controls to improve the accuracy of financial reports. If the CEO waits until the merger or acquisition is near to implement IT audit report recommendations, important valuation numbers are the least likely to be accurate, potentially putting the CEO in a less favorable negotiating position. Thus, auditors could point out the negative consequences of a cost undervaluation. As every CEO knows, whoever goes into a merger and acquisitions negotiation with the most accurate data stands the best chance of winning the best deal.

WHAT NEEDS TO CHANGE?

Whether the company is a financial institution looking to identify potential money-laundering operations, a manufacturer looking to IT to improve processes that will recapture contract revenues, or a telecommunications company that uses technology to maximize its billing operations for voice over Internet protocol services, IT governance needs to be seen as a business priority. Auditors can and should take a leadership role in making that happen. Offentimes, CEOs simply don't have the time to take that initial first step.

For CEOs to give IT governance best practices the attention they deserve, the language and focus of audit reports need to change. The core of the problem is the language in which reports are written. Reports need to evolve from being seen as a simple index of the company's compliance level to a business intelligence tool. Therefore, for audit results to be implemented and IT governance to become a priority, reports need to provide an action plan that uses clear business language.

The most effective way to cross the chasm between auditors and corporate executives is to detail specific business process improvement solutions in terms that proactively drive executive decisions everyday. The end game isn't compliance; it's business process improvement. Therefore, chief audit executives and internal audit managers should be willing to leverage compliance data proactively from audit reports, and value the importance placed by the CEO on operational efficiency and profitability when writing the report. Furthermore, auditors who don't have a finance background should become familiar with acronyms and terms, such as EBITDA, gross margins, and shareholder value, and relate audit results as much as possible to them. This would enable CEOs to measure audit recommendations in terms of profits and savings. Although getting CEOs to pay more attention to audit reports may not happen overnight in some companies, it is up to auditors to drive this change.■

Originally published in *IT Audit*, Vol. 9, July 10, 2006, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit

Upcoming CISA® and CISM® Exams

Registration for the June 2007 Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) exams continues. Candidates may view or print a copy of the CISA® or CISM® Bulletin of Information for the June 2007 exams at www.isaca.org/cisaboi and www.isaca.org/cismboi

ISACA offers both the CISA® and CISM® exams twice a year – June and December.

June 2007 Exam

Registration Deadline: April 11

Exam Date: June 9

December 2007 Exam

Early Registration Deadline: August 15

Registration Deadline: September 26

Exam Date: December 8

Preparing for the Security Audit – Recommendations for Beginner IT Auditors

Identifying risks and vulnerabilities and evaluating the effectiveness of perimeter security efforts are some of the steps beginner IT auditors need to understand to conduct more effective reviews of security controls.

By Lakshmana Rao Vemuri, CISA, Senior Security Consultant, Paladion Networks

Organizations make different assumptions about the security levels needed to protect their information systems and assets. Although companies may differ on their ideas about IT security, the role of internal auditors is the same: Review the existing security environment and identify the effectiveness of internal controls. Unfortunately, beginner IT auditors have their work cut out for them. Many companies have poorly configured firewalls and intrusion detection systems (IDS), lack monitoring systems to detect noncompliance with IT policies and procedures, use antivirus systems with outdated definitions, and wait too long to patch systems when vulnerabilities are detected. Each of these issues can be a challenge for the seasoned auditor, so those just entering the field have to be up and running quickly. Furthermore, beginner auditors need to understand the complexities of often-disparate computer networks, operating systems, software programs, and hardware. Thus, even experienced auditors must "do their homework" prior to the audit to maximize the review process.

BEFORE THE AUDIT

To conduct successful reviews of security controls, beginner IT auditors must learn what to expect during the audit process. In addition, first-time auditors should understand the appropriate ways to identify security risks and vulnerabilities, evaluate the effectiveness of perimeter security efforts, and work with senior management effectively. The main issues beginner auditors should keep in mind before a security audit takes place are determining existing risks and vulnerabilities, as well as the organization's level of IT governance and compliance landscape.

Once an auditor is tasked with reviewing a company's IT security environment, he or she will have to evaluate the different security levels of all IT assets and how each asset is protected. The auditor also is expected to provide recommendations to improve the organization's IT security and certify whether adequate internal controls are in place to secure all IT assets. To make appropriate recommendations and understand which controls are needed, auditors should identify existing security vulnerabilities and risks in partnership with IT and senior management staff.

One way to identify security risks and vulnerabilities prior to the audit is by recommending that the organization conducts a risk assessment. Besides helping auditors determine which controls would be most effective based on the organization's security needs, a risk assessment can help dissipate resistance to audit results by allowing management to have an accurate picture of the current security landscape before the audit takes place. If the client has not completed a risk assessment, the auditor should conduct a basic risk assessment to identify any weak areas, which in turn will help demonstrate the need for a given control. IT governance is based on high-quality, well-defined, and repeatable processes, which must be documented and communicated properly, and requires the involvement and commitment from senior management, IT, security, and assurance professionals. One way to review whether a company has an effective IT governance program is by ascertaining that senior management has set clear goals, policies, and procedures and IT management is based on the use of effective frameworks, tools, or best practices. Many frameworks and best practices exist that can help companies in their IT management efforts. Some of the most popular models are the UK's Office of Government Commerce [II Infrastructure Library](#), ISACA's [Control Objectives for Information and related Technology](#), and the International Organization for Standardization's [17799: 2000 Standard](#).

Furthermore, when evaluating the effectiveness of existing IT governance practices, auditors should be on the lookout for the following red flags: absence of enterprise-wide internal



Did You Know...

That ISACA has Online Discussion Forums?

ISACA and ITGI have established several listservs to enable interested parties to find the group most suited to their professional interests. Each listserv offers excellent opportunities to share advice, seek assistance and raise pertinent questions.

Available discussion forums:

- [Sarbanes-Oxley](#)
- [IT Governance](#)
- [COBIT](#)
- [Information Security Manager](#)
- [General Audit, Control & Security Topics](#)

Continued from page 5

controls or a formal risk management program, and ineffective IT financial reporting and disclosure preparation processes. IT auditors also should note the executive board's or audit committee's level of knowledge about the organization's current IT security landscape and whether the IT department is unable to determine if the information stored in a system has been altered or if the data retention period has been executed properly. Although these indicators are not the only ones internal auditors should consider, they represent some of the main problems faced by organizations lacking an effective IT governance program.

IDENTIFYING SECURITY RISKS AND VULNERABILITIES

Given the current security landscape, beginner IT auditors should make every effort to understand the different security threats that may affect an organization's IT assets. When reviewing a company's security environment, auditors will likely come across one of the following:

- Scenario 1 — IT security controls properly address risks and vulnerabilities to IT assets. Minor modifications may be necessary to enhance the efficiency of existing controls.
- Scenario 2 — The company lacks a proper security infrastructure. Therefore, because any recommendations will be implemented for the first time, organizations may not feel they are reinventing the wheel or spending additional money to recreate already-established controls.
- Scenario 3 — The auditor comes across an existing security infrastructure that does not protect IT assets adequately due to poor configuration, monitoring, or management. The auditor then has to identify current risk levels, their possible impact, and provide recommendations. Thus, the organization has to spend additional time and resources to comply with the audit's recommendations.

Scenarios 2 and 3 usually provide beginner auditors with the most difficulty, because of the level of knowledge required to provide effective security recommendations. When encountering a company that lacks a properly established security infrastructure (i.e., scenario 2), the auditor may use the following plan of action to explain the security landscape and justify investment in a proper infrastructure:

- Recommend a risk assessment be completed to determine the value of IT

assets. This will give senior management an understanding of the various security threats that may affect or are affecting the business.

- Recommend that the IT department installs passive network tools to demonstrate the frequency of remote access attempts and external probes. This will help managers gain a thorough understanding of the network's topology (i.e., what services are available, what operating systems are in use, and what vulnerabilities may be exposed on the network).
- Explain to top managers how security threats may affect the organization's reputation and financial stability.
- Explain the legal ramifications of a security breach due to poor internal controls and the consequences of noncompliance with specific data laws and regulations.
- Provide executives with information on the latest cyber crime statistics and how they have affected similar organizations. This will help instill a sense of urgency for securing IT systems.
- Talk to executives about the possibility of insider threats by listing the different data assets and systems that could be affected. The auditor could do this by performing a data classification exercise and informing executives of the results. This will help point out how much money the organization is losing due to its lack of proper security controls and any losses of bandwidth due to unproductive use of network resources.

When auditing organizations with a security infrastructure that does not protect IT assets adequately (i.e., scenario 3), auditors can recommend that the IT department:

- Runs a vulnerability scanning tool on the network from outside the firewall's [demilitarized zone](#) (DMZ) to identify any security vulnerabilities.
- Conducts a network vulnerability assessment and submits the report to executive managers. The report should explain all IT security threats and their impacts, as well as expose any security gaps and weaknesses in the IT infrastructure.

If the organization does not have the skill set to perform a vulnerability test, it should hire an expert or use scanning tools to detect any system vulnerabilities. However, IT staff using these tools must have a thorough



Certification Renewals

Don't forget to renew and report CPE hours as soon as possible to avoid revocation. For reference regarding qualifying activities and the calculation formula, the CPE policy is available at www.isaca.org/cisacpepolicy or www.isaca.org/cismcpepolicy. The renewal process can be completed online by logging into www.isaca.org.

Quicklinks

- Canadian Securities Administrators (CSA) NOTICE 52-317 – *Timing of Proposed National Instrument 52-109 Certification of Disclosure in Issuers' Annual and Interim Filings*. Go to www.osc.gov.on.ca and search for "52-317" to download the notice.
- Public Company Accounting Oversight Board (PCAOB) : *Proposed Auditing Standard – An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements*. Go to www.pcaob.org/Rules/Document_021 to download the proposed standard.

Continued from page 6

understanding of how to use them to obtain the best results.

WHAT'S NEXT — AUDITING PERIMETER SECURITY IMPLEMENTATION

Senior management is more likely to accept audit recommendations if auditors document the organization's need to enhance IT security efforts first. However, documenting the effectiveness of perimeter security measures is also important to ensure audit recommendations are established properly. Because many organizations use perimeter security as their main line of defense against external threats, beginner IT auditors need to become familiar with how to identify common problems during and after the perimeter security implementation process.

According to the [SANS Institute](#), a security training and research organization, the following are some of the most common problems companies encounter during the perimeter security implementation process:

- Management and IT staff believe that once a firewall is in place, they have sufficient security and no further checks and controls are needed on the internal network.
- Analog lines and modems are provided to connect to an Internet service provider or have dial-in access to the desktop system, thus bypassing perimeter security measures.
- Internal host network services are passed through security perimeter control points unsecured.
- Firewalls, hosts, or routers accept connections from multiple hosts on the internal network and from hosts on the DMZ network.
- The organization allows incorrect configuration of access lists, which results in allowing unknown and dangerous services to pass through the network freely.
- The details of logged user activities are not reviewed regularly or are insufficient, thus deteriorating the effectiveness of the monitoring system.
- Hosts on the DMZ or those running firewall software also are using unnecessary services.
- Support personnel use unencrypted protocols to manage firewalls and other DMZ devices.

- Employees are allowed to run encrypted tunnels through the organization's perimeter device without fully validating the tunnel's end-point security.

- The company uses unsecured or unsupported wireless network applications.

Beginner auditors who identify any of the risk areas above should recommend that organizations purchase security tools to help evaluate the IT network's strength and detect network vulnerabilities and risk areas. Some of the tools available for different activities include host-based audit software, network traffic analysis and intrusion detection system tools, security management and improvement programs, and network-based audit and encryption software. ■

Originally published in *IT Audit*, Vol. 9, April 10, 2006, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

Editor's Note: This is an abridged article. To view the article in its entirety, please refer to the above website.

E-Commerce Security – Components Which Make It Safe

By Maha Mahadevan, CA, CISA, CISSP, CIA

POSSIBLE E-COMMERCE RISKS

From the wealth of information which proliferates on the topics of the Internet, or e-commerce specifically, there is a consensus on basic risks. Any transaction or message, financial or otherwise, would be subject to the following risks. In an ordinary commerce environment, plenty of avenues are available to address these risks through formal signatures and other mechanisms which would ensure secure transactions. The major risks facing e-commerce environments are summarized below:

- Identity or authenticity of the person--Who sent the message? Does the sender have the authority to bind the organisation he or she represents?
- Data Integrity - Is the message complete; has it been altered en route; can I prove that my copy of the message has not been altered?
- Denial of service - launch of an attack which would bring down the service.
- Non Repudiation - Proving up the message in court, ensuring that the sender cannot falsely deny sending the message, ensuring that the sender cannot falsely deny the contents of the message.
- Confidentiality - Ensuring that information is not disclosed to unauthorized parties.

CRYPTOGRAPHY

This is an encryption technique that dates back to the times of Julius Caesar who is accredited with using cryptographic techniques to convey messages to his military generals (www.entrust.com white paper "An Introduction to Cryptography", December 1997, Ian Curry). Encryption is a technique to alter a message (data, information) to an unrecognizable form so that an unintended recipient cannot decipher the message. Decryption is the technique of bringing back the message to its original form. Messages are encrypted and decrypted using a key. A key can be defined as a numerical value used by an algorithm to alter information or the vice versa. Key management has been critical and at times, a problem throughout. The greatest challenge is to keep the key secure.

Let us see if a school-aged person were to encrypt the message "Meet me at the candy store at evening four tomorrow." He would probably use a key, let's say "K" and the message would look like

kMkekekt kmke kakt ktkhke kckaknkdky ksktkokrke kakt kekvkknkknkg kfkokukr ktkokmkokrkrkokwk.

His friend would decrypt the message striking the "k" and read the message. This is a rudimentary example. In actual life, encryption and decryption take place differently.

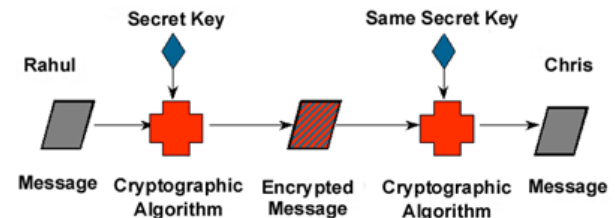
There are two systems of cryptography:

- a) Symmetric Key Cryptography
- b) Public Key Encryption

SYMMETRIC KEY CRYPTOGRAPHY

A rudimentary example: In many ways this system operates like a vault where two parties use the same key. Let's say two friends share a common locker and use the same key to open and close the vault. The friends would have a duplicate key for each to operate the vault.

In a real life situation when messages are sent, the same key; also called as secret key, single key or private key is used for both encrypting and decrypting a message. The problem lies in safely sending the key to the receiver and if they are geographically apart, the management and security of the key is always a concern.



In the example both Rahul and Chris share the same key secret key. Popular single key algorithms are generated using Digital Encryption Standards (DES), International Data Encryption Algorithm (IDEA).

While a private key system may be good for a small circle of people exchanging messages, it would be an onerous task to manage the keys and maintain confidentiality should the circle expand to a large corporation. Let us say an organization has 200 users. Then, it would require maintaining close to 20,000 keys between users. Management of keys would be unwieldy, should the user population increase.

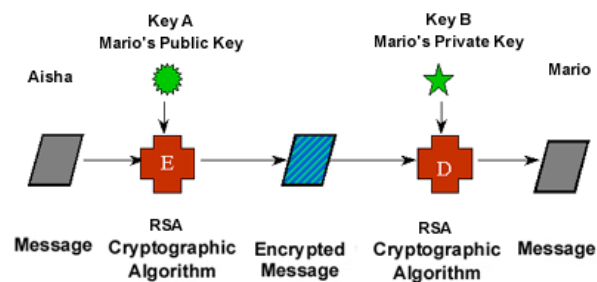
PUBLIC KEY CRYPTOGRAPHY

A rudimentary example: This system is similar to a company or an individual who wants to receive messages without disclosing his or her identity. For example: an advertisement for a response is placed giving the post box address of PO Number 5674. This information of PO Box address is the public key. Any interested party who wishes to correspond would use this PO number and the advertiser would have the

physical key to operate the post box, which is the private key. The private key is in the custody of the advertiser and the public key to the post box number is public.

Public key cryptography came as a remedy to do away with the private key system and the management of the keys. Mathematicians at MIT first developed public key in the 1970s, where each participant creates two unique keys: the public key, which is published in a directory available to all, and a private key, which is kept secret. The private key can decrypt the data encrypted by the public key and keys are always a pair. The key pairs are mathematically related, but cannot be calculated even if one or the other is known. Either key can encrypt but only one will decrypt.

Keys exist as a series of electronic signals stored on the disk drives of personal computers or transmitted as blips of data over phone lines as specified in the industry standards. The real hard work - complex math of encrypting and decrypting messages - is handled by the computer. One does not have to bother with any of the complexities. [Source: *The Keys to Safe Shopping*- www.visa.com]



Aisha uses the public key of Mario to send messages to Mario, and Mario uses his private key to decrypt the messages.

The public key mitigates risks to a large extent but a few issues which the users must address are:

- What happens if I loose my keys? Can I still decrypt?
- What is the proof that the keys used have not been tampered with and are trustworthy? Or, is some one masquerading or pretending to be the owner?
- I want to encrypt a file only once for the same message to be sent across networks to different people.

Digital signatures may remedy these concerns and have come to be accepted as a safe mechanism of communication between user groups. ■ ©2001 Information Systems Audit and Control Association. All rights reserved. Reprinted by permission.

Editor's Note: This is an abridged article. To view the article in its entirety, please go to www.isaca.org and search for the author's surname.

Code of Professional Ethics

ISACA® sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

e-Symposia Archive

Earn 3 Free CPEs for each symposium! The first time you participate in an ISACA e-Symposium®, you will need to register at www.isaca.e-symposium.com. The user id and password requested are specifically for the e-Symposium. The credentials are NOT the same as your ISACA username and password.

Date	Topic	CPE Hours
20 Mar '07	Auditing Operating Systems	3
27 Feb'07	Securing Access Management	3
30 Jan'07	COBIT: The Update	3
12 Dec'06	Identity and Access Management	3
21 Nov'06	Back to Basics: Tool and Techniques to Improve the Audit Process	3

Education News

Writing the CISA® Exam in June 2007?

Come join us for the Spring 2007 CISA® Review Course, May 4 – 6, 2007!

The course will provide an overview of the Certified Information Systems Auditor (CISA®) curriculum. The review course is designed to follow the 2007 CISA® Review Manual. The following areas will be addressed:

- IS Audit Process
- IT Governance
- Systems and Infrastructure Lifecycle
- IT Service Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

Watch your email for more details and registration information.

Calgary Chapter 2007 Education Week

The ISACA Calgary Chapter Education Week will be taking place in October this year. More details will follow in the July newsletter.

Questions may be directed to your local chapter representative - Leanne Roberts, Education Director at educ01@isaca-calgary.ca

What is the Value of Becoming a Certified Information Systems Auditor (CISA®)?



As the information systems audit, control and security profession evolves, experienced practitioners are seeking ways to promote their hard-earned knowledge and expertise to the business world. Professional certification attests to the knowledge and skills that professionals have earned in their chosen field. The CISA® designation, administered by

ISACA, demonstrates an individual's ability to effectively apply IS audit, control and security principles and practices. Employers worldwide look for the CISA® designation when hiring IS audit and control professionals, and CISA® certified professionals often receive higher compensation. According to the Foote Partners LLC, an independent IT consultancy, the CISA designation is the highest-paying technical certification. The CISA designation was recently accredited by the American National Standards Institute, indicating that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus and due process.

Information about the CISA® designation is available at www.isaca.org/cisa

Information Security Management Designation Provides Career Value



As information technology continues to grow in importance to all areas of an enterprise, professionals with IT security expertise are assuming greater responsibility and ascending to higher levels of management. A combination of strong business and technical knowledge is needed for managers to lead effective departments across entire organizations.

Until recently, it was difficult for senior business executives to ensure their IT security managers and directors had the expertise to mitigate IT-related risk and protect their enterprises. To address this need, ISACA offers the globally recognized Certified Information Security Manager (CISM®) designation.

IT security threats are becoming increasingly complex. The CISM® certification helps provide senior executives with the assurance that those certified have the expertise to offer effective security management and consulting. CISM® is a management-level business designation for advanced

professionals who manage an organization's information security and possess the knowledge and experience to set up, implement and direct a security structure to manage risks and add value.

Information about the CISM® designation is available at www.isaca.org/cism

Congratulations to the following Successful CISA® Exam Writers in 2006

Adebiyi Adeniran
 Brian Sorrell
 Deanne Stene
 Dylan Jackson
 Eric Bjarnason
 Evelyn Otte
 Frank Ogeh
 Geoffrey Milos
 Gordon Greenham
 Grace Rengifo
 Ibukun Aruleba
 Jagruti Sampat
 James Hennig
 Jamil Thobani
 Jarka Winters
 Joanne Molesky
 Linda Chan
 Lindo Petiot
 Marianne Wolters
 Neeraj Kumar
 Ofuya Eberchukwu
 Paola Odorico
 Rajesh Ghosh
 Randall Dyck
 Raveendran Madappattu
 Roberto Parales
 Ross Screation
 Susan Worthington
 Thomas Feltham
 Veronica Suarez
 Viana Cesar
 Vyacheslav Sklyarenko
 Wai Lee Chan

Congratulations to the following Successful CISM® Exam Writers in 2006

Coral Edington
 Ian Jones
 James Balkwill
 Lawal Olasupo
 Philip Fodchuk

ISACA International News

North America CACS



[North America CACS](#)
22–26 April 2007
Grapevine, Texas, USA

27–30 April 2008
Las Vegas, Nevada, USA
(Information Coming Soon!)

Presented by ISACA®, North America CACS (computer audit, control and security) is well known as the leading conference for IT audit, assurance, control, security and governance professionals. ISACA works together with industry leaders to develop a conference program that focuses on the complex needs of today's professional and provides solutions that address these needs from a practical perspective.

The 2007 conference promises to be better than ever. Thomas Ray, chief auditor for the PCAOB, will present the keynote address. Attendees will have more than 70 sessions to choose from that are sure to meet a wide range of technical and professional needs. Whether you have been managing or practicing for many years, or are relatively new to the profession, North America CACS will provide you with knowledge, tools and techniques that you can put to work immediately.

Register early to guarantee your place at the conference! For the past two years, the North America CACS event has sold out with more than 1,000 attendees. Plan now to join your peers at the one conference you can not afford to miss. And do not forget to sign up for an optional preconference or postconference workshop or two. These are great ways to explore a topic in full and to earn some additional CPE hours. To register, go to www.isaca.org/nacacs



[Oceania CACS](#)
9–12 September 2007
Auckland, New Zealand



[Latin America CACS](#)
21–24 October 2007
Monterrey, Mexico



[Asia-Pacific CACS](#)
The [International Conference](#) is coming to Asia-Pacific in 2007—in place of the Asia-Pacific CACS event—which will return in 2008.

ISACA® Training Week



Presented by ISACA®, Training Week provides a unique educational experience.

The Training Week courses use a combination of lecture, case study, class discussion and group exercises to explore all the nuances and subtleties of the named topics. Training Week participants will learn about proven strategies and techniques based upon best practices and lessons learned from the ISACA community.

Training Week courses will provide participants with:

- In-depth coverage of the topics important to you;
- Interactive format;
- Full range of technical programs;
- World-class presenters;
- Networking opportunities; and
- Valuable continuing professional education (CPE) credits.

Details will be posted as information is made available for these upcoming Training Week events:

- [7–11 May 2007 — Denver, CO USA](#)
- [11–15 June 2007 — Amsterdam, The Netherlands](#)
- [11–15 June 2007 — Seattle, WA USA](#)
- [8–12 October 2007 — Athens, Greece](#)
- [15–19 October 2007 — Montreal, Quebec, Canada](#)
- [5–9 November 2007 — San Antonio, TX USA](#)
- [3–7 December 2007 — Scottsdale, AZ USA](#)

K-NET, a Global Knowledge Network

As a member of ISACA you have immediate access to a compendium of Internet-based knowledge that has been sought, identified and peer reviewed, then organized into logical categories of interest and concern, reducing the necessary time to research answers to your professional questions.

K-NET contains:

- 12 subject areas
- over 90 topic areas
- more than 1000 knowledge references

Go to www.isaca.org/knet for more information.

Call for Articles

We are always looking for technical articles that fall into one of the following areas of interest. (These are also the six CISA® job practice areas.) The objective of each is noted below.

1. IT Governance
 - To provide assurance that the organization has the structure, policies, accountability, mechanisms, and monitoring practices in place to achieve the requirements of corporate governance of IT.
2. IS Audit Process
 - To provide IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the organization in ensuring that its information technology and business systems are protected and controlled.
3. Protection of Information Assets
 - To provide assurance that the security architecture (policies, standards, procedures, and controls) ensures the confidentiality, integrity, and availability of information assets.
4. Systems and Infrastructure Lifecycle Management
 - To provide assurance that the management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the organization's objectives.
5. IT Service Delivery and Support
 - To provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the organization's objectives.
6. Business Continuity and Disaster Recovery
 - To provide assurance that in the event of a disruption the business continuity and disaster recovery processes will ensure the timely resumption of IT services while minimizing the business impact.

Article submissions can be original articles or reprints from another publication or source. Interested individuals should contact the editor at news01@isaca-calgary.ca for a copy of the 'Writers Guidelines.' Please note that only articles that meet the minimum requirements as set out in the Guidelines will be considered for publishing.

Thank you for your interest.

Reader Feedback Survey

We welcome your suggestions and feedback on this issue of our e-Newsletter. Please take the time to send us your survey responses so that we can continue to add value to your membership with ISACA.

Just email your responses to us at news01@isaca-calgary.ca and you will be eligible to win a \$25.00 gift card from Starbucks (or any coffee shop of your choice)!

Survey Questions:

1. Are the technical articles helpful to you? Please explain.
2. Is the overall image, layout and design effective in capturing the reader's attention and enhancing readability?
3. What topics would you like to see us cover in future issues?

The deadline for survey responses is **May 14th**. A random draw will be made that week. Good luck!

Naming Contest

Test your creativity by submitting a name for the new Calgary ISACA e-Newsletter. Please email your entry to news01@isaca-calgary.ca. You may submit as many entries as you would like by the deadline of **June 4th**. The Board will select the most suitable choice among all entries received.

If your entry is selected, you could win a \$50.00 gift card to *McNally Robinson Books*!

We're on the Web!



See us at: www.isaca-calgary.ca