

CALGARY CHAPTER

HIGHLIGHTS

President's Message	1
Luncheon Dates	1
High CISA Scores	1
Defining the Right to Audit Clause	2
ISACA, eh.	4
Canadian Tire COBIT Case Study	5
ISACA Certs Growing in Demand	8
2007 Calgary Conference	10
ISACA International News	11
How to Earn CISA CPE Hours	12
Chapter Membership Information	13

CHAPTERS OFFICERS & DIRECTORS

Greg Winters, President
Sanjeev Saha, Vice President
Barbara Clay, Treasurer
Andy Heale, Secretary
Jarka Winters, Communications Director
Jagruhi Sampat, Membership Director
Leanne Roberts, Education Director
Louis Fernandes, CISA/CISM Coordinator
Beata Biel, Webmaster
Linda Chan, Newsletter Editor

ISACA INSIDER

www.isaca-calgary.ca



A newsletter for Calgary Chapter members about ISACA news updates, events and articles of interest

Volume 2

July 2007

President's Message

The 2006-2007 ISACA year officially ended at the Calgary chapter's Annual General Meeting (AGM) and luncheon held at the Palliser hotel on June 21, 2007. As some of you pointed out to us, our meeting was held on the same day as the Institute of Internal Auditors' (IIA) AGM, and so some of you had to choose which meeting to attend. I apologize for any inconvenience, and we will work with the IIA to avoid this in the future. For those of you who were unable to attend, I'll recap here the major topics we discussed.

The past year has been one of fairly significant change for the chapter. We started last season with a largely new board of directors and a new set of bylaws and operating principles. Also, with 301 members, Calgary became the third largest ISACA chapter in Canada, surpassing Vancouver with 288, and behind Toronto with 1857, and Montreal with 406 members, respectively.

Unfortunately, four directors resigned their posts in 2007: Leanne Roberts, our Education Director, and Kishore Iyer, our Program Director, are leaving Calgary to pursue other career opportunities; Dr. Kimberly Greenizan, our Academic Advocate, is currently serving with the Cana-



Greg Winters, Calgary Chapter President, & Everett Johnson, ISACA International President, at the North American Leadership Conference

dian Armed Forces in Afghanistan; and Alvaro Janikian, our Technology Director, will be focusing on other professional development opportunities that require his time. On behalf of ISACA Calgary, I extend our sincere thanks for all their contributions to the chapter and our best wishes for their future endeavors.

On the financial front, Barb Clay, our Treasurer presented the 2006 financial statements to the membership.

Continued on page 2

Monthly ISACA Luncheon Dates

Upcoming Dates: September 11, October 18, November 20 and December 12. The December luncheon will be held jointly with the IIA Calgary Chapter.

Time: 11:30 AM to 1:00 PM

Location: Palliser Hotel, 133 - 9th Avenue SW, Calgary

Please note that dates and times are subject to change. Speakers and topics will be updated on the website as they are confirmed.



Members mingle at an ISACA Luncheon at the Palliser Hotel earlier this year

High CISA Scores from the

In a previous issue of this newsletter, we reported that Geoffrey Milos, CISA, IPA, SSCP, was a successful writer of the CISA exam in December 2006. Well, it turns out that he earned the *highest score in North America!* Worldwide, he earned the *third highest score*. Considering that 10,833 individuals wrote that exam worldwide, his accomplishment is extraordinary. Geoffrey is an Enterprise Business Architect at the Calgary Health Region. As well, another member of our chapter scored extremely well on the same exam. 'Biya Adeniran, CISA, PMP, earned the *second highest score in North America*. 'Biya is an IT Audit Manager at Westjet. Congratulations to both individuals!

In December, 3130 CISA candidates took the exam in North America and 1936 candidates passed. 637 CISM candidates took the exam in North America and 509 candidates passed. Worldwide, there were 10,833 CISA candidates in December and 5620 passed the exam. Worldwide, there were 782 candidates in December and 1280 passed the exam.

About ISACA

With more than 65,000 members in more than 140 countries, ISACA® (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 50,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 6,500 professionals since it was established in 2002.

“When the auditor invokes the right to audit, the vendor may claim that 30, 60 or 90 days notice is required.”



President's Message

Continued from Page 1

We ended the year with a sound financial position and a healthy balance sheet, with sufficient funding to ensure that we can continue to provide high-quality services and events at a very low cost to the membership.

With respect to services to our members, we forged ahead with some major initiatives last year, starting with this newsletter, the ISACA Insider. And, by the time you read this message, the new Calgary Chapter website should be up and running with a completely new look and feel. My thanks go out to Jarka Winters

and Beata Biel for their efforts in working with Non-Fiction Studios to get the website launched!

For next season, watch for new services through the website to make registering for luncheons and events easier; the introduction of a discounted season-pass for our monthly luncheons; and the availability of the entire ISACA bookstore library to our members through a new chapter library. We'll keep you posted as we work to get these projects off the ground.

We closed off the meeting with

the election of Sanjeev Saha, our Vice President, and of me as President to second terms. We thank you all for your continued confidence, and we will strive to do our very best on your behalf. Please be sure to send an email with any feedback, comments or suggestions you have, and don't hesitate to volunteer if you think you'd like to participate as a member of the board! I can be reached at president@isaca-calgary.ca.

Best wishes for a great summer, and we look forward to seeing you at the luncheon in September!

Defining the Right-to-Audit Clause

By Gordon Smith, President, Canaudit, Inc.

In this article I would like to address an issue that is often left out of vendor contract negotiations – the right to audit. My concern is that many of our clients fail to include right-to-audit clauses in critical contracts. Other clients have a simple clause that specifies the right to audit, but not the terms. Before I go any further, I have to state that I am not a lawyer. I am simply an auditor who has read and audited many contracts. All contracts regarding consulting services, software, outsourcing and other terms relating to processing your organizations transactions should be reviewed by an attorney who specializes in information technology. The items I have listed below should be used as a guideline for negotiating contracts.

CAREFULLY CRAFT THE RIGHT-TO-AUDIT CLAUSE

The right-to-audit clause should not be a single paragraph. Rather, it should include statements that ensure that a full audit can be conducted of vendors or trading partners. A common shortfall of

existing contracts is that the required notice period is not mentioned. When the auditor invokes the right to audit, the vendor may claim that 30, 60 or 90 days notice is required. This precludes the ability to perform a surprise audit, and the lengthy delay may disrupt the audit plan. Hours of work should be clearly defined. If you would like to conduct your audit in normal business hours, specify the timeframe. A vendor could claim that auditing must be performed in the evening or overnight hours, to ensure that normal processing is not affected.

Do not forget to include the business locations that can be audited. A vendor could state that the audit can only be performed at their headquarters. Their data centers or data storage facilities could be at other locations. If you can not visit those locations, then your right to audit is severely impeded.

DATA ACCESS AND AUDIT AUTOMATION

The right to audit may not include the right to access data or use

audit software. When using an application service provider (ASP) to process your data, it is essential to ensure that the data is accurate and that it balances. This will require the use of specialized data analytic software, such as Interactive Data Extraction and Analysis (IDEA) or Audit Command Language (ACL), to interrogate the data. It would also be useful to run other audit software tests to ensure that there are no unusual data, transactions or conditions. The right to use audit software and the software products that can be used should be clearly specified, along with the right to change the audit software. I prefer this wording: "The client has the right to use general audit software and other reporting tools against the data files and / or databases." This includes the use of IDEA or ACL. It should also leave the door open to use other ad hoc reporting tools, as your audit department may switch tools over the life of the contract

It is quite possible that your organization might have a contract clause that states that your data

Defining the Right-to-Audit Clause

will be segmented from other vendor client data. You may assume that it is physically separated. It is likely that this assumption is wrong. In most cases, the data is logically separated within a database or database instance. If the data is stored in a database that is logically separated, it is doubtful that the vendor will give you direct access to the database. Before signing the contract, the data storage issues should be addressed. Determine if the data is physically segmented in different files or storage partitions, or if it is logically separated within a database. Once this is determined, you can draft the required contract clause. It is best to keep your options open in case the vendor changes their segmentation methodology. If they currently physically segment, then you should include a clause that states that you will be given direct access to data if the databases are merged and segmented logically.

If the data is logically segmented, the vendor may not want to give your organization direct access to the database. Instead, they may offer to give you an extract that contains only your organization's data. I usually frown on this, as it compromises independence. As an alternative, I believe that the extract program or code should be reviewed by your organization's internal IT auditor, then run under the supervision of your auditor. This will need to be clearly stated in the right-to-audit section of the contract.

LET'S NOT FORGET DISASTER PREPAREDNESS, BUSINESS CONTINUANCE, BACKUPS AND OFFSITE STORAGE

We are very concerned about disaster preparedness and business continuance. If the vendor has an outage and services are not available, then their disaster becomes your disaster. The right to audit the vendor's disaster and business continuance plans are necessary to ensure that your organization will be protected in the event the vendor has a prolonged outage or full-scale disaster. If your organization is a major client of the vendor, try adding in a clause that enables your auditors to attend one of the disaster-readiness tests.

The right to audit backup and recovery procedures is essential. This right to audit should extend to the offsite records management facility and data transfer procedures to and from the facility. In the last year, there have been several examples of data lost during the transfer process. Also, with summer coming, the courier van should be climate controlled to ensure that the media is not damaged by excessive heat buildup in the vehicle.

Another issue is the ability to read the backups when they are needed. Recently, an employee of the State of Alaska inadvertently destroyed the primary files. The backup files could not be read. In the past, we suggested that the backup process be modified to include a "read after write" option. This ensures that the media can be read when it is needed. For the backup audit test, it would be a good idea to see if volumes containing your organization can be read.

SAS 70's DO NOT ENSURE THAT A THIRD-PARTY VENDOR IS SECURE

In an outsourced environment, the auditor usually relies on the SAS 70 reports. In my opinion, a SAS 70 does not give me any assurance that the required security is in place. If you are relying on a SAS-70, then additional testing is required to ensure that the network, servers, programs and data are properly protected. In an outsourced environment, the right to audit must include the right to conduct testing above and beyond the SAS 70 testing to ensure that your organization's information assets are properly protected.

There are several levels of testing that can provide that assurance. The first is a Security Baseline. This test is performed with the knowledge and the possible participation of the outsourcer and the IT Security staff. With many of the same tools used during a Penetration Test, the audit team documents the network, then runs a battery of security tests against the machines and software to identify and document vulnerabilities. At the end of the pro-

ject, the security status of the machines in the network is documented along with the specific remediation efforts required to enhance security. The baseline is re-performed in three months to quantify improvement and create metrics for measuring the remediation effort.

SURPRISE AUDIT AND PENETRATION TESTS

The ability to perform surprise audits and penetration tests is a necessity if your organization has outsourced processing and networks. Surprise audits are intended to test the controls in place during the normal business cycle. The vendor does not know when the test will be performed. Audit clients are often most careful during normal audits. Surprise tests are intended to measure how the client performs on a day-to-day basis. This technique is useful for testing physical security procedures and cash and application controls. It can include the surprise use of audit software to identify application errors or security patches on servers and workstations. We also suggest that

the vendor's network be tested to ensure that your data is properly encrypted when the data is transmitted. This can be done as part of the normal audit or as part of a Penetration Test.

A Network Penetration Test should also be performed on a surprise basis. This enables the audit team to test the Intrusion Detection and Response Procedures. The Penetration Test is required for outsourced IT operations and application outsourcing. The right to perform surprise penetration audits should be written into the contract. When we do penetration tests of our clients, they often ask us to do some testing of their outsourced vendor's site. We work closely with the client to obtain the required permission to do testing of the vendor's site. In most cases the vendor is very receptive as they get the test without paying for it. We have done Network Penetration Tests for several of our clients that



“Determine if the data is physically segmented in different files or storage partitions, or if it is logically separated within a database. Once this is determined, you can draft the required contract clause.”

Right-to-Audit Clause

Assistant Editor Needed!

The Chapter is in need of a volunteer to assist the Newsletter Editor in preparing, compiling and editing an e-newsletter, published each January, April, July and October.. Responsibilities include researching articles, compiling information on ISACA events and programs, and preparing the newsletter in Microsoft Publisher. For more information, please email Linda at newslettereditor@isacacalgary.ca.



ISACA International President Hands Out Award to the Vancouver Chapter.

ISACA, eh.

Canada Dominates the 2007 K. Wayne Snipes Awards

ISACA held its North American Leadership conference in April in Dallas, Texas. The conference was attended by over 100 delegates representing approximately 50 ISACA chapters across the US and Canada. At the annual event, ISACA International presents the K. Wayne Snipes award to the best small, medium, large and very large chap-

ters from the region. The award was established in 1989 and provides recognition to those chapters that meet or exceed special service goals by actively supporting local membership, and thus the IS audit and control profession.

Chapter performance is assessed on the following criteria:

- Chapter membership growth
- Member service projects
- Chapter-sponsored educational events
- Attendance at chapter meetings

- Involvement on association committees, or with association activities

- Involvement with other professional organizations

This year' winners for North America are:

Small—Victoria (Canada)

Medium—Winnipeg (Canada)

Large—Vancouver (Canada)

Victoria and Winnipeg also won Global award for Best Worldwide Chapter.

Congratulations!

Call for Articles

We are always looking for interesting technical articles from members of the Calgary Chapter.

Article submissions can be your original article or if it has been published in another publication or source and reprinting permission is obtained. 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.



Interview with Kees Jansen, President of the ISACA Vancouver Chapter

1. Did your chapter consciously pursue the award? If so, what did you do, and how did you do it?

We just moved from being a mid-size chapter to being a large chapter and it was a surprise for us as well that as new entrants in the large chapter group, we won the award. We have pursued the award successfully in the past but we did not consciously pursue the award this year. Typically what we do is look at the criteria that are used for the award and make sure we are meeting the requirements in different categories.

2. What are the most difficult challenges your chapter faced, and how did you overcome them?

There are many challenges; a continual key challenge is putting the luncheon program together for the year as that is a large part of the activities that is particularly visible to members. We have learned over the years to start planning early for the lunch sessions (half a year in advance) and target some key speakers. As an example, this year we were very successful to put a series together regarding IT governance and for the first time, did a panel discussion that included people from the industry (e.g. CIO's, IT directors).

3. What are the top five factors or characteristics that you believe made your chapter successful?

The award is based on what you let ISACA international know, so a key component is the completion of your annual report in a timely manner and ensuring that it reflects all the activities that you do. Some of those factors include:

- consistency in monthly lunch sessions that are covering assurance, governance and security top-

ics;

- running CISA and CISM course preparation programs;
- actively promoting the local chapter and demonstrating that by how marketing efforts are directed (e.g. attendance of student/university fairs, regular news briefings to members, providing grants to university students);
- coordination with other chapters (e.g. IIA and ISSA) and local universities (e.g. regarding accreditation of their programs); and,
- last but not least, the percentage of growth in the chapter is probably an important factor as well and is a result from the above activities.

4. How did your members contribute to the success of the chapter?

A variety of members obviously volunteer on the Board. Other than Board members, the biggest contribution of members is showing up for events and bringing along colleagues to events.

5. How did your Board contribute to the success of the chapter?

The Board members were a huge contribution. We have about 10 people on the board and by everyone doing his part, that makes it a success. In the last few of years, each area of responsibility has been doing a few activities very well instead of doing many things partially well. In addition, this year, each area of responsibility has introduced (at least) one new aspect. ■

COBIT and IT Governance Case Study: Providing Maximum Benefits and Strong IT Governance and Control at Canadian Tire Financial Services

ABSTRACT

Employing more than 1,700 people and financing and managing the Canadian Tire Options® MasterCard® for more than three million cardmembers, Canadian Tire Financial Services, Ltd. (CTFS) is an important entity in the financial services industry. After recognizing the need to implement a proactive IT governance program, CTFS implemented Control Objectives for Information and related Technology (COBIT). COBIT helped the organization communicate to IT and management why they needed to care about effective controls and provide a framework for implementation. COBIT's components were successfully used in many ways, such as building a strategic IT internal audit review plan, assessing process maturity and validating the accuracy of IT risk scoring.

BACKGROUND

As the financial services arm of Canadian Tire Corporation, Ltd., Canadian Tire Financial Services (CTFS) is primarily engaged in financing and managing the Canadian Tire Options MasterCard for more than three million cardmembers. The Options MasterCard is accepted at more than 24 million locations worldwide and offers the Canadian Tire "Money" On the Card loyalty program.

CTFS also markets a variety of insurance and warranty products to more than six million customers. In addition, its emergency roadside service, Canadian Tire Roadside Assistance™, provides peace-of-mind driving to many Canadians. CTFS's goal is to build lifelong relationships with Canadian Tire customers by providing products and services they truly value.

The company began in 1961 as Midland Shoppers Credit Limited, a small financial service company offering third-party credit processing for local retailers. During the 1960s, the company began adding Canadian Tire Associate Stores to its client list. By 1968, Midland was servicing Associate Stores across Ontario. It eventually became a subsidiary of Canadian Tire Corporation, Ltd. and was renamed Canadian Tire Acceptance Limited (CTAL).

CTFS, with Canadian Tire Bank, currently employs more than 1,700 people, with offices in Welland, St. Catharines and Burlington, Ontario, Canada. Contributing significantly to Canadian Tire Corporation's annual profits, CTFS is an important player in the financial services industry. The Service Quality Measurement Group Inc.

(SQM) has repeatedly recognized CTFS as the "Best Call Centre in North America" and as an organization whose overall customer satisfaction ratings are at the world-class level. This designation requires 80 percent or more of customers to rate their satisfaction at the very satisfied level, which is the highest score possible on the SQM ratings.

PROCESS

CTFS recognized the need to implement proactive IT governance initiatives in 2004 because the upcoming CEO/CFO Certification requirements meant that it had to have a formalized process to successfully implement the appropriate controls. The CEO/CFO Certification requirements were developed by the Canadian Securities Administrators (CSA) and the Ontario Securities Commission (OSC) in response to the U.S. Sarbanes-Oxley Act. This set of rules requires CEO and CFO certification of annual and quarterly reports (MI 52-109, Certification of Disclosure in Issuers' Annual and Interim Filings). The process was formalized and implemented in 2005 and 2006.

The next step was to pursue the support of senior management for the initiatives. Once it was determined and confirmed that there was a gap within the current process, the business plan was presented to the executive team and approval was obtained to move forward with the initial analysis required.

To successfully implement IT governance and CEO/CFO Certification activities, COBIT was recommended by an external audit consultant who had been working with CTFS Information Technology Product & Services (ITP&S), helping to determine the requirements for the CEO/CFO Certification scope. The COBIT framework came highly recommended as the appropriate framework for the division. Published by the IT Governance Institute, the COBIT guidance enabled CTFS to begin designing the implementation of a general computer controls model.

Reasons Behind CTFS's Selection of COBIT:

- COBIT is an internationally accepted standard for IT governance and control practices.
- It provides a means for benchmarking inter-

nal control compliance.

- It can be used by management, end users, and IT audit and security professionals, and it provides a common language.
- The driving force for introducing COBIT was ensuring that all of IT and management understood why they needed to care about effective controls. Getting them to realize that there are many important business reasons for this was the initial milestone to be successfully addressed.
- COBIT easily maps to other leading standards, including ISO 17799, ITIL and NIST.
- CTFS was able to gain agreement with the external and internal audit partners on the same framework and control objectives.
- The COBIT framework addresses three main audiences: ITP&S, management and auditors. The benefits of implementing COBIT as our governance framework included better alignment based on business focus. It makes management understand IT better. There is senior level clarity of ownership and responsibilities, based on process orientation.
- CTFS is subject to many regulations and audit requirements, including PCI, OSFI, Privacy, (ICOFR) Internal Control over Financial Reporting associated to CEO/CFO Certification, IT General Controls Sub-certification, and COBIT serves as the framework that enables the company to implement or fine tune the appropriate control compliance and governance activities while maintaining the business alignment and understanding of the required changes.

COBIT was also used to establish and improve IT governance. Once departmental owners were assigned to each domain and subdomain of COBIT, they detailed a business plan and obtained approval to form an IT Risk Governance department to manage the governance and compliance of the controls on an ongoing basis internally and with external vendor relationships.

CTFS realized many benefits from COBIT, including the following:



- COBIT enabled CTFS to build and prepare a strategic IT internal audit review plan based on the 34 COBIT process areas.
- COBIT enabled CTFS to assess process maturity using the COBIT capability maturity model.
- COBIT was used to evaluate the IT risk identification based on the COBIT control objectives and the risk assessment process.
- COBIT was used to validate the accuracy of IT risk scoring based on objective and risk mapping.
- COBIT was used to rationalize the requirement for an audit using the COBIT framework descriptions.
- CTFS IT was able to prepare a tactical internal audit plan based on the COBIT audit guidelines.
- COBIT was used to break down the scope of the audit review using COBIT key goal indicators (KGIs) and critical success factors (CSFs).
- COBIT was used to help develop the required testing to assess control effectiveness based on the COBIT control practices.

Continued on Page 7

Defining the Right-to-Audit Clause

Continued from Page 3

have outsourced IT operations. We found that the outsourcer is generally open to the testing; however, they may have to place some limitations on the test. As an example, they would not want our team to access another client's data, or they may exclude certain systems from testing as they are shared with other clients. These are acceptable exclusions.

VENDOR SUBCONTRACTING OR OUTSOURCING OF WORK

In the last three years, I have noticed an increase in vendors who outsource or offshore all or part of their operation. Our concern is that confidential information or proprietary software may be transferred to an offshore entity. There have been several published cases where confidential information has been harvested and sold to others. In one case, a contractor threatened to release confidential information if she was not paid. In my mind, it is important to know if any work is subcontracted to other vendors. In addition, it is necessary to know if any data has been off-shored.

Let's look at the subcontracting issue first. Many companies subcontract or outsource parts of their organizations. Helpdesk functions and network support are examples of functions that are outsourced. While your organization may outsource to a selected contractor, the contractor could in turn outsource their operation. It is essential to extend the Right-to-audit clause to all subcontractors. Note that the contract should also state that the contractor cannot subcontract the work out without your organization's prior written approval.

Many vendors have opened their own offices in other countries, in their continuing efforts to

export North American jobs and reduce costs. The offshore employees are of high quality and industrious. My concern is not with the employees, as it is with the data and the protection of that data. I strongly urge your audit department to consider the risk of data stored or viewable offshore. Controls must be in place in the overseas facility to ensure that the data is properly protected. When I talked to one vendor about offshore data, they insisted that the data was not offshore. It was securely located in a database in this country. They stated that the offshore employees can only view the data on their screens, that only the image is sent overseas. I suggest that the vendor did not consider screen scrapers or database queries that export the data to a printer or a file. I believe you should include in the contract the right to audit all locations where your data can be viewed or exported.

ENFORCING SALESPERSON PROMISES

If a salesperson promises something or says something is "no problem", make sure you include whatever that something is in the contract. Often the sales staff truly believes that a right-to-audit clause will not be an issue. When it is time to sign the contract, they find that their own Management does not want contract modifications. When in negotiations with the salesperson and they agree to a condition, I always double-check that they are willing to put the specific issue into the contract. I keep a list of the items and present it to them at the end of the meeting. When the contract is presented, I check it carefully to ensure that all promised items are included. If anything is missing, we send it back for revisions

along with copies of the salesperson's statements.

CONCLUSION

The right-to-audit clause is more complicated than most auditors or even lawyers realize. If a vendor wants to restrict your ability to find issues, they can deny access to your auditors if there is no right-to-audit clause. If there is a clause, then they can restrict your ability to audit unless your organization's rights are carefully documented in the contract. I also caution you to be realistic. Each vendor is different. Some will add some or all of the above items. Others will push back. We have assisted several clients in the contract negotiations, specifically on the right-to-audit clause. In each case, we have found that the vendor was willing to deal if your firm would not sign the contract until they did. The vendor wants the contract more than you need the vendor – remember that during the negotiation phase. ■

This article was reprinted with expressed permission from Canaudit. (www.canaudit.com)

Opinions expressed in the newsletter represent the views of the authors and advertisers and may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this newsletter. This newsletter does not attest to the originality of authors' content.

“The COBIT framework was a strong partner in the organization’s success.

By implementing COBIT, CTFS was able to analyze the key live blood areas of the company and the systems and applications associated with these business units. The management guidelines helped prioritize and monitor business processes by using KGIs, key performance indicators and maturity models. By addressing the COBIT control objectives and mapping them to the areas of defined risk, it helped to facilitate the system or process changes required to enhance the existing controls and the confidence of CTFS business managers that they can ensure that an adequate control system is provided for their IT environment. This allows them to continue to grow the business and focus on new business plans.

Board Involvement in IT Governance

CTFS believes that effective IT governance delivers the structured processes needed to meet business goals while defining the required regulation requirements and the controls associated with their shareholders and to ensure that the board’s objectives have been met and monitored. However, as the organization has learned, governance is only the first step toward improved IT decision making. The governance process begins with the board of directors and then funnels through the executive team and on to the operations staff. Through this approach, everyone can obtain the same goals and outcome.

The board is responsible for the review and approval of the strategic plans and direction of IT. Its members also ensure alignment between the needs of the business and the plans of IT. They will annually review the IT cost structure, and once every three years they review the results of a cost benchmark analyzing internal IT costs against a peer group of companies.

The benefits of technology are never doubted; however, to be a successful IT division the risks associated with implementing new technologies or changes to existing systems or applications have to be understood and managed. Fortunately, CTFS was introduced to COBIT early in its planning stages, and it was used to organize one of the most intensive process changes across all areas of IT. The COBIT framework was a strong partner in the organization’s success.

CONCLUSION

COBIT provides a clear, concise approach to aid the planning and implementation of IT general computing controls. It provides the ability to assign accountability across the domains, which has enabled CTFS to match up the owners of the functional area. CTFS looks forward to the ongoing value that using the COBIT framework will provide.

COBIT has enabled CTFS IT to provide managers, internal and external auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices used to ensure that the challenges of the CEO/CFO Certification regulatory requirements have been met. COBIT has been a valuable tool for maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in the company’s IT division.

As a successful organization, CTFS understands the benefits of information technology and uses this knowledge to drive shareholders’ value. The organization recognizes the critical dependence of many business processes on IT, the need to comply with increasing regulatory compliance demands and the benefits of managing risk. To enable the organization to successfully meet today’s business challenges; CTFS ITP&S will continue to utilize the IT Governance Institute’s COBIT framework. This framework will set the baseline for ongoing and new technology initiatives, including internal control requirements, allowing CTFS to provide a consistent approach to all ongoing work within IT. ■

This article was reprinted with expressed permission from the IT Governance Institute. Source: www.itgi.org (Go to [Home](#) > [ITGI](#)> [Case Studies/Best Practices](#) > Case Studies)

e-Symposia Archive

The ISACA e-Symposium on July 31, 2007, will focus on IT governance tools. To register for the July e-Symposium and take the first step toward earning three free CPE credits, please visit www.isaca.e-symposium.com. For more information, please visit www.isaca.org/webcasts.

Date	Topic	CPE Hours
July 31, 2007	IT Governance: The Tools of the Trade	3
June 19, 2007	Managing Enterprise Security Risk	3
May 29, 2007	Audit Risk Management	3
April 17, 2007	Compliance: Drama, Secrets & Silos	3

Online CISA Review Course in Development

Development is underway for an online CISA review course. ISACA will be working with VCampus (www.vcampus.com) to develop an interactive, web-based course that will provide members throughout the world with a consistent, efficient and cost-effective tool for exam preparation. The course will include interactive exercises, case studies, review sessions and practice exams. With this learning portal, ISACA will be able to implement an online training solution and expand its CISA exam preparation offerings. The new online course will complement the exam preparation trainings currently offered through the chapters.



And the Winner is...

Congratulations to Shemina Rashid for submitting "ISACA Insider" which the Board selected as the new name of this newsletter. Shemina was awarded with a \$50 gift certificate to *McNally Robinson Bookstore*.

Definition:

insider -noun

1. A person who is a member of a group, organization, society, etc.
2. A person belonging to a limited circle of persons who understand or share special knowledge

Congratulations to Mufazal Hassanali for participating in the Reader Feedback Survey. His entry was selected as the winner by the Board. Mufazal was awarded with a \$25 gift card to *Starbucks!*

ISACA Certs: Continuing to Grow in Demand and Importance

By Sarah Stone Wunder, Certification Magazine

With a new U.S. Department of Defense (DoD) program in May and the 50,000th certified professional earning the Certified Information Systems Auditor (CISA) certification in late September, 2006 has turned out to be a milestone year for the Information Systems Audit and Control Association (ISACA).

According to Kent Anderson, managing director of Network Risk Management and five-year ISACA member, ISACA reached 50,000 CISA certifications and 6,000 CISM certifications in 2006. He said the CISM milestone is especially impressive.

"That's just in the first three years that cert has been available," Anderson said. "Obviously, it is very popular."

Partially driving this popularity is a new program from the DoD, which was announced in May. Under the DoD's Information Assurance Workforce Improvement Program, both CISA and CISM have been named as approved certifications for the DoD's information assurance professionals. Under the DoD's directive, up to 80,000 professionals are required to earn one of 13 certifications offered by five organizations.

The DoD's information assurance professionals are classified into two categories — information assurance technical (IAT) and information assurance managerial (IAM) — that are each divided into three levels. CISA is among the four approved baseline certifications for professionals in IAT Level III, and CISM is among the three approved certifications for professionals in IAM Levels II and III.

In addition to these professionals, assistant examiners employed by

the U.S. Federal Reserve Banks must pass the CISA examination before they are eligible for commissioning; the National Stock Exchange of India has recognized CISA as a requirement to conduct systems audits; and in Singapore, CISA was accredited under the Critical IT Resource Program of the National Infocomm Competency Centre (NICC), the national body that oversees the accreditation of IT-related certifications. Additionally, CISM is a recognized credential in the Security Solutions Competency of Microsoft's Partner Program.

Since the DoD began the program, demand for CISA and CISM has continued to increase, Anderson said.

"We've seen continuous growth, and it's been a fairly steep climb," he said. "Requests for information about our certification and for registration for future testing, more and more people are signing up."

Anderson said this increased demand is a sign of the CISA and CISM's growing importance.

"The Department of Defense has made both the CISA and CISM one of the mandatory certifications, so both of those will grow significantly," Anderson said. "I think there are two things (increasing demand). Organizations like the DoD are beginning to require some level of certification. Also, there have been some studies. Foote Partners did an independent review and has labeled both CISA and CISM as some of the most-valued certifications. There is a strong desire among the individuals who seek these certifications to distinguish themselves."

Anderson said part of the reason the CISA and CISM certifications

are valuable is because they are experience-based.

"There are lots of certifications based on technical skill, where you can just sit for an exam and become certified," he said. "The value of both of these certifications is the experience requirement. It helps professionals become better prepared for the positions they hold."

ISACA's Beginnings

ISACA got its start in 1967, when a small group of individuals with similar jobs — auditing controls in the computer systems that were becoming increasingly critical to the operations of their organizations — sat down to discuss the need for a centralized source of information and guidance in the field.

In 1969, the group formalized, incorporating as the EDP Auditors Association. In 1976, the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

Today, ISACA's membership — more than 50,000 strong worldwide — is characterized by its diversity. Members live and work in more than 140 countries and cover a variety of professional IT-related positions, including information systems (IS) auditor, consultant, educator, security professional, regulator, chief information officer and internal auditor.



CISA

Since 1978, the CISA program has been a globally accepted standard

ISACA Certs: Continuing to Grow in Demand and Importance

of achievement among IS audit, control and security professionals.

To earn the CISA designation, candidates are required to:

- Successfully complete the CISA examination, which is offered twice annually at more than 200 locations.
- Adhere to ISACA's Code of Professional Ethics and agree to comply with a continuing professional education policy.
- Submit evidence of a minimum of five years of professional IS auditing, control or security work experience.

A 2003 survey of ISACA members revealed 70 percent of CISAs and members in the process of becoming CISAs think the certification helped advance their careers. When all ISACA members, CISA or not, were asked whether they thought gaining the CISA would help their careers, the positive response was even greater: 77 percent.

According to ISACA, more than 400 CISAs are employed in organizations as CEOs or CFOs. More than 900 CISAs serve as CIOs or IS security directors, more than 2,300 CISAs serve as audit directors or audit partners and more than 8,500 CISAs are employed in managerial or consulting positions in IT operations, security or auditing.

In addition to CISA's demand in U.S. government agencies, it also has reached international prominence.

In Hong Kong, ISACA members who have held a CISA certification for at least four years have the right to vote for the city's legislative counselors as representatives of the IT category among the functional constituencies.

CERT-IN, the Indian Computer Emergency Response Team, has recognized CISA as one of the requirements to conduct security audits.

In Romania, banks desiring to implement distance or electronic payment instruments are required by law to be certified by CISA-holding auditors.

CISM

The CISM certification program is developed specifically for experienced information security managers and those who have information security management responsibilities. The CISM certification is for the individual who manages, designs, oversees and/or assesses an enterprise's information security.

The CISM certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services.

To earn the CISM designation, candidates are required to:

- Pass the CISM examination.
- Adhere to ISACA's Code of Professional Ethics and agree to comply with a continuing professional education policy.
- Submit proof of five years of IS work experience with at least three years as an information security manager. A 2006 study by Foote Partners LLC named CISM one of the highest-paying IT certifications and a hot tech skill certification (indicating an annual growth of greater than 11 percent).



According to ISACA, more than 1,000 CISM serve as a chief information officer, chief executive officer or IS security director. More than 2,000 CISM serve as an information security manager or in a related information security position, and nearly 1,000 CISM are employed in security consulting or training positions.

Anderson said ISACA probably will see much of its growth within with CISM certification over the long term. "CISA is a fairly mature certification, and it's always under review. However, the CISM is probably where the highest future growth is," he said. "ISACA has been working with some of the other security bodies on studies on what security convergence is going to mean to the industry. In the long term, you are going to see the security certifications move in those directions. The CISM will probably be moving in that direction, as well." ■

This article was reprinted with expressed permission from Sarah Stone Wunder of Certification Magazine. (Go to www.certmag.com.) Originally published in November 2006.

Opinions expressed in the newsletter represent the views of the authors and advertisers and may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this newsletter. This newsletter does not attest to the originality of authors' content.

June 2007 Exam Result Notifications and Scoring

The pass/fail result letters for the June 2007 exam will be mailed during the first week of August. To ensure the confidentiality of scores, exam results are not reported by telephone or fax. For candidates who consented to item #25 on the registration form, a onetime pass/fail status and score notification will be sent by e-mail during the first week of August. To ensure receipt of these documents, please update your profile if any contact information has changed. To prevent the e-mail notification from being blocked or sent to a spam folder, candidates should add certification@isaca.org to their address book or safe-senders list. Candidates will also be able to view their exam score at www.isaca.org using their login credentials and password. Beginning with the June 2007 exam, ISACA will provide CISA and CISM exam scores according to a scale from 200-800, with the passing score set at 450. A scaled score is a method of reporting exam performance relative to other candidates taking the same exam. The process begins with the establishment of a passing score on an exam, the cut score. This cut score process establishes a passing point for the exam based on the review and input of numerous certified professionals from throughout the world who participate in several exercises and simulations. This pass point is not a percentage of correct answers. Once established, this passing score is placed on a scale. In the case of the CISA and CISM exam, the passing score has been established as a 450 scaled score. Regardless of the scale used for scoring, the same raw scores have the same results. No more, or fewer, candidates pass or fail the exam under any scale used.



2007 Calgary Conference

& Education Week

Come join us for an exciting week of IT Audit and Security information sharing and education! This year's conference features industry-expert speakers and focuses on how your IT audit, risk and control activities can deliver value and even reduce costs to your organization. Topics will include:

- **Practical and Cost Effective Implementation of COBIT, ITIL and ISO**
- **Enterprise Governance of Information Technology and the Role of Internal Audit**
 - **Implementing and Sustaining World Class IT Audit Practices**
 - **Tips for Managing Your Security Function**
 - **Optimizing Compliance Costs Related to IT Controls**
 - **The Pros and Cons of IT Risk and Control Spending**
 - **December 2007 CISA Exam Preparation**

Registration for this exciting event will begin very soon. Watch your email and our new website for details, including speakers, schedules and pricing!

OCTOBER 2007



Sun	Mon	Tue	Wed	Thu	Fri	Sat
7	8	9	10	11	12	13 CISA Review Course
14 CISA Review Course	15 CISA Review Course	16 CISA Review Course	17 Presentations & Resolver Sponsored Lunch	18 Presentations & Paisley Sponsored Lunch	19 Presentations & ACL Sponsored Lunch	20

December 2007 Exam Registration and BOI

Registration for the December 8, 2007 Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) exams is underway. To view additional details, please see the pertinent Bulletin of Information (BOI) at www.isaca.org/cisaboi or www.isaca.org/cismboi. Registration is available online at www.isaca.org/examreg. The early registration deadline is **August 15, 2007**. The final registration deadline is **September 26, 2007**.

ISACA International News

To contact ISACA International...

Voice.....+1.847.253.1545

Fax.....+1.847.253.1443

Webwww.isaca.org

E-mail ...info@isaca.org

ISACA to Offer New Credential

At the upcoming International Conference, ISACA will formally announce its newest credential program specifically developed for professionals who have responsibilities for managing and/or governing the IT-related contribution to an enterprise to achieve its business objectives. The certification, supported by the IT Governance Institute® (ITGI™) and built on its intellectual property, will promote the advancement of IT professionals who wish to be recognized for their governance-related experience and knowledge. The formal name of the certification is expected to be announced shortly, at which time an announcement will be available at www.isaca.org/news. The initial IT governance professional certification exam is expected to be administered in December 2008. A grandfathering program will be announced shortly, through which highly experienced IT governance professionals may apply for certification without taking the exam. More information will be available soon on the ISACA and ITGI web sites, www.isaca.org and www.itgi.org.

International Conferences



North America CACS
27 April—1 May 2008
Las Vegas, Nevada, USA



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



Canada
[15–19 October 2007 —
Montreal, Quebec](#)



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



2007 Sarbanes-Oxley Symposia
[23-24 August - Rosemont, IL](#)
[27-28 September - Washington, DC](#)



EuroCACS
9–12 March, 2008
Stockholm, Sweden



Paramount Energy Trust ("PET") is Canada's leading 100% natural gas royalty trust. Driven by a highly defined business plan, PET has stayed focused on maximizing distributions and creating Unitholder value.

Advertisement

PET is looking to fill a permanent SOX compliance role. This individual should be proficient in completing 404 documentation; evaluating and testing business process controls, ITGCs and entity-level controls; and full-cycle project management.

Qualifications include:

- one or more of the following designations: CMA/CA/CGA, CISA, or CIA
- a minimum of 2 years experience in documentation and testing
- a minimum of 1 year in project management
- experience in public practice an asset
- experience conducting internal audits an asset
- familiarity with SOX 302 requirements
- excellent interpersonal, communication and organizational skills

Total compensation includes a competitive salary and benefits package.

To apply, please email your resume and cover letter to gail.quartly@paramountenergy.com with the subject "Internal Control Analyst Position."

Correction

There was a mis-spelt name in the list of successful CISA exam writers in the April 2007 issue of the newsletter. The correct spelling is Paolo Odorico. We apologize for the error!

To Advertise

This newsletter is circulated to ISACA Calgary members and non-members who have voluntarily signed up for our mailing list.

For advertising inquiries, please contact the Editor at news01@isaca-calgary.ca.

CISA is a prestigious certification obtained by over 50,000 professionals. In order to maintain standards within the profession, the ISACA has put in place a Continuing Professional Education (CPE) Policy. "The goal of the CPE Policy is to ensure that all CISAs maintain an adequate level of current knowledge and proficiency in the field of information systems audit, control and security."

CISAs are required to attain CPE hours over an annual and three year certification period and comply with the following requirements:

- Each year attain and report a minimum of twenty (20) CPE hours for a three year reporting period.
- Submit CPE maintenance fees annually.
- Attain and report a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period.
- If selected for annual audit, respond and submit required documentation of CPE activities
- Comply with ISACA Code of Professional Ethics.



The CPE reporting period begins on January 1 each year and for newly certified CISAs, the CPE requirements commence in the year succeeding certification.

CISAs are not permitted to use the CISA logo on an individual basis, but can use the CISA acronym after their name.

A CISA must obtain and maintain documentation supporting reported CPE activities and is required to retain the documentation for twelve (12) months following the end of each three-year cycle. Failure to comply with the CISA CPE policy will result in the CISA credential being revoked and such individuals will no longer be allowed to present themselves as a CISA. There is an exemption for Retired CISA status and Non-practicing CISA status (for details refer www.isaca.org).

"Activities that qualify for CPE include technical and managerial training. This training must be directly applicable to the assessment of information systems or the improvement of audit, control, security or managerial skills (www.isaca.org/cisasicontentareas) to ensure a proper balance of professional development is attained."

CPE Activities comprise the following as summarized from the CPE Policy (for complete details refer the policy):

- ISACA professional education activities and meetings (no limit on the number of hours) which include ISACA conferences, seminars, workshops and related activities.
- Non-ISACA professional education activities and meetings (no limit on the number of hours) include in-house corporate training, university courses conferences seminars workshops and related activities (refer CPE Policy Calculating Continuing Professional Education Hours section)

- Self-study courses (no limit). These courses will only be accepted if the course provider issues a certificate of completion and the certificate contains the number of CPE hours earned for the course.
- Vendor sales/ marketing presentations (10-hour annual limitation)
- Teaching/ lecturing presentation (no limit): For presentations and courses (all types), CPE hours are earned at twice the presentation time or time estimated to take the course for the first delivery (e.g. a two hour presentation earns four CPE hours) and at the actual presentation time for the second delivery. CPE hours cannot be earned for subsequent presentations of the same material unless the content is substantially modified.
- Publication of articles, monographs and books (no limit): These activities include the publication and/ or review of material directly related to the information systems audit and control profession. Submissions must appear in a formal publication or website and a copy of the article or the website address must be available, if requested.

- Exam question development and review (no limit) of CISA or CISM (Certified Information Security Manager) examination or review material. One CPE hour is earned for each question accepted by an ISACA board or committee. Actual hours will be given for the formal item review process.

- Passing related professional examinations (no limit): This activity pertains to the pursuit of other related professional examinations. One CPE hour is earned for each examination hour when a passing score is achieved.
- Working on ISACA and ITGI Board/ Committees (10-hour annual limitation): These activities include active participation on an ISACA or ITGI board, committee, task force or active participation as an officer of an ISACA chapter. One CPE hour is earned for each hour of active participation. Active participation includes, but is not limited to, the development, implementation, and/ or maintenance of a chapter website.
- Contributions to the IS audit and control profession (10-hour annual limitation): These activities include work performed for ISACA that contributes to the IS audit and control profession (i.e. research development, certification review manual development, K-Net development).

Calculating CPE Hours: One CPE hour is earned for each fifty minutes of active participation (excluding lunches and breaks) in a professional education activity. CPE hours are only earned in full hour increments and rounding must be down.

ISACA Code of Professional Ethics: ISACA sets for this Code of Professional Ethics to guide the professional and personal conduct

How to Earn CISA Continuing Professional Education Hours

of members of the association and/ or its certification holders.

Members and ISACA certification holders shall:

- Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
- 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.
- 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.
- Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
- Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
- 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.

For more information on the CISA CPE Policy, refer to www.isaca.org/cisacepolicy. The renewal process can be completed online by logging into www.isaca.org.

Chapter Membership Information

Member Benefits

The Information Systems Control Journal is an authoritative, peer-reviewed publication that reports on topics such as Internet security, computer crime, e-commerce, information integrity, computer confidentiality issues and IT risk management. ISACA members receive a subscription to the print version of the Control Journal, which is published bimonthly. Members also have access to the online version, JOnline, which features additional articles not featured in the print version. Visit www.isaca.org/journal to view the latest Journal today.

Incentive Program

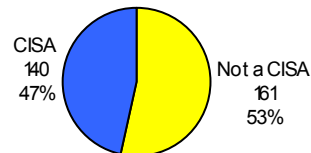
ISACA's midyear dues incentive program is again in place. Any new members joining between June 1 and August 6 will be charged only 50 percent of the association dues, plus the new member processing fee and chapter dues, for membership through 2007.

Social Event

The Chapter is planning an exciting social event for members and friends this Fall. Stay tuned as we will be sending out invitations via email.

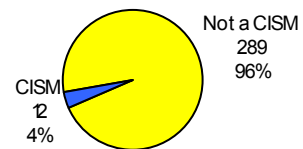
Percentage of Membership that are CISAs

As of June 28, 2007: Total Members = 301



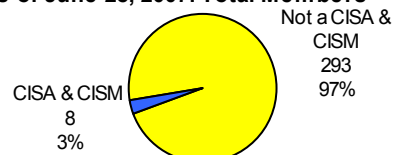
Percentage of Membership that are CISM's

As of June 28, 2007: Total Members = 301



Percentage of Membership that are CISAs & CISM's

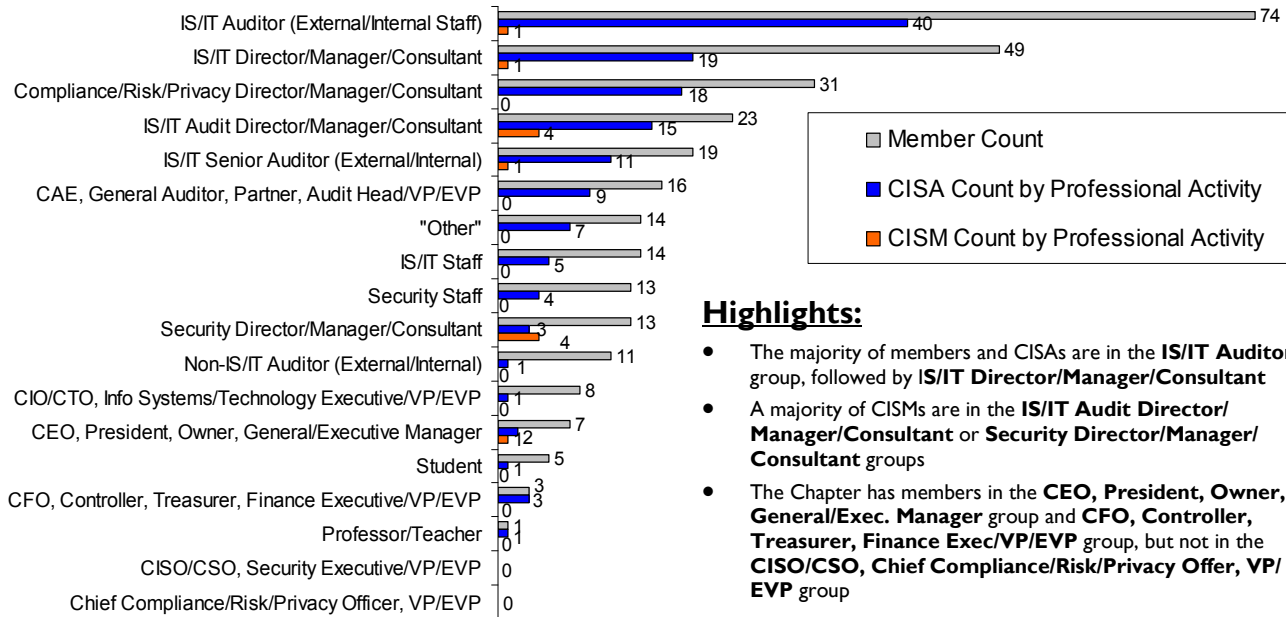
As of June 28, 2007: Total Members = 301



Chapter Membership Information

Members by "Professional Activity"

As of June 18, 2007: Total Members = 301, CISAs = 140, CISM = 12

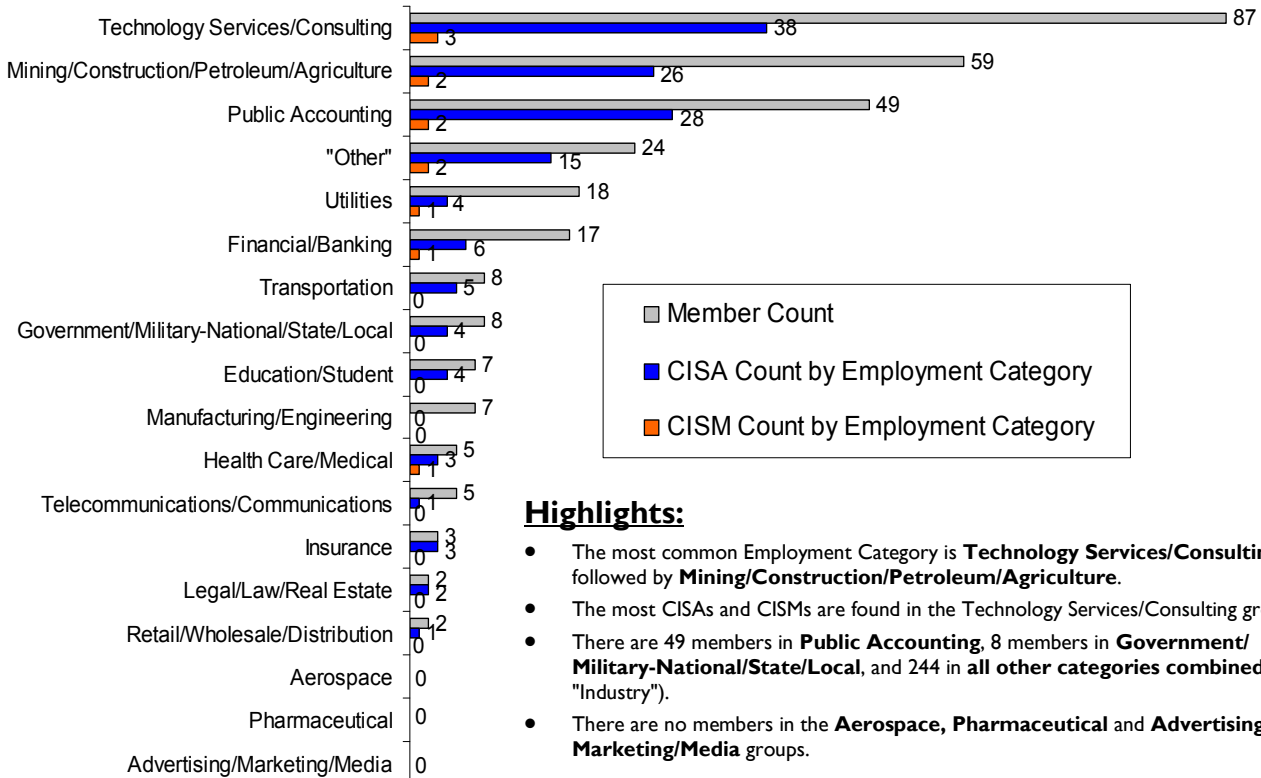


Highlights:

- The majority of members and CISAs are in the **IS/IT Auditor** group, followed by **IS/IT Director/Manager/Consultant**
- A majority of CISM are in the **IS/IT Audit Director/Manager/Consultant** or **Security Director/Manager/Consultant** groups
- The Chapter has members in the **CEO, President, Owner, General/Exec. Manager** group and **CFO, Controller, Treasurer, Finance Exec/VP/EVP** group, but not in the **CISO/CSO, Chief Compliance/Risk/Privacy Offer, VP/EVP** group

Members by "Employment Category"

As of June 18, 2007: Total Members = 301, CISAs = 140, CISM = 12



Highlights:

- The most common Employment Category is **Technology Services/Consulting** followed by **Mining/Construction/Petroleum/Agriculture**.
- The most CISAs and CISM are found in the **Technology Services/Consulting** group
- There are 49 members in **Public Accounting**, 8 members in **Government/Military-National/State/Local**, and 244 in **all other categories combined** (i.e. "Industry").
- There are no members in the **Aerospace, Pharmaceutical and Advertising/Marketing/Media** groups.