

Inside this issue:

- **Full day ACL workshop conducted by ISACA Muscat Chapter** 1
- **Seminar on “Maximizing the Audit Effectiveness using ACL Data Analysis** 1
- **IT Governance Domains— Strategic Alignment** 3
- **SQL Injection Vulnerability** 4
- **Await Next Program!** 4
- **News Briefs** 5
- **About us** 6
- **CISA, CISM— Employ certified IT Professionals** 6



Full day ACL Workshop conducted by ISACA Muscat chapter

Muscat Chapter conducted a full day ACL workshop at the IT lab of the Oman Tourism College at Seeb on Thursday, April 12, 2007.

Ms. Gretel de Paepe, Certified ACL trainer from the ACL Associates conducted the training. Though the program was announced at short notice the registration got over immediately.



Gretel began with a brief introduction of ACL and its worldwide use in data analytics. Participants worked around on a case study which highlighted the controls in the payment cycle. Control objectives were identified following which the risks were listed one by one. Against each risks the controls that were instituted were applied.

These are the common scenarios one faces like overpayment due to duplicate invoices being introduced into the system, purchase



order authorization by an employee whose authorization level is inadequate, segregation of duties etc

(Continued on page 2)

Seminar on “Maximizing the Audit Effectiveness using ACL Data Analysis

ISACA Muscat Chapter conducted a seminar on “Maximizing the Audit Effectiveness using ACL Data Analysis on April 11, 2007 at the Sohar Hall of the Ruwi Hotel. The presentation was given by Ms. Gretel de Paepe, Certified ACL Trainer.

The highlight of the presentation was the challenges faced by auditors when they have to review the reliability and integrity of



financial and operating information. On one side there is severe limitations of time and staff resources and on the other side greater

responsibility is thrust on them due to high profile scams and corporate failures that have time and again surfaced all over the world.



There are great risks in relying on data without analyzing it. Gretel explained the major challenges in data analysis. Some of them are that data in a company resides in diverse data sources. The data volumes are large. Further, due to the complexity of IT infrastructure the challenges are not easy.

(Continued on page 2)

Full day ACL Workshop conducted by ISACA Muscat chapter (Contd..)

(Continued from page 1)

Gretel showed that each control objectives are to be tested by reviewing the supporting



documents to identify its control parameters, define tests for identifying control exceptions if any, determine the data sources to use for the specific tests and document the

test results and report findings after conducting the test.



At the end of the workshop, certificates were distributed. Participants earned 12 CPE hours. The feedback from the participants had one point in common that there should be more workshops of this nature.

Some feedback on the workshop

"It was worth the time and money. We request the chapter to organize more sessions on Audit tools especially IT Audit tools"

"We could have similar such workshops where practical training is available. Excellent support and facilities provided by the chapter"

"Well organized. ISACA Muscat chapter has taken lot of strain. Congrats!"

"An interesting session with clarity on the issues addressed"

"Gretel's presentations were great. A follow up workshop after a month or so to cover advanced aspects not covered today would be welcome"

April e-Symposium to Feature Compliance

The ISACA e-Symposium for April will focus on compliance issues, with key industry leaders presenting on using capability maturity models, the challenges of IT outsourcing, and ISO 20000 audits and assessments. To register for the 17 April 2007 e-Symposium and take the first step to three free continuing professional education (CPE) credits, please visit www.isaca.e-symposium.com. All of the live e-symposia have been archived and are available for viewing on demand. To view an archived event and have an opportunity to earn free CPE credits, please register at www.isaca.org/webcasts where additional information on these valuable educational opportunities is also available.



Seminar on "Maximizing the Audit Effectiveness using ACL Data Analysis (Contd..)

(Continued from page 1)

Against all this there is a fear of bad data. If such data were relied for business decision making, the business is exposed to serious risks.

Gretel explained that for analyzing data, ACL is clearly the most preferred software tool. It can extract data, analyse, detect conditions where fraud could exist and provide fraud detection and continuous monitoring. Searching for a needle in a haystack is impossible and venturing to do so is foolish. However, when it comes to ACL this is the opposite as the software can do searching effortlessly.

She said that huge volumes of data can be accessed in any format—whether they be in flat files, relational databases, spread sheets

and even print files. All this can be done without changing the raw data. ACL could locate errors, duplicates, missing transactions thereby highlighting potential areas of concern. She went on to say that data is growing exponentially. She then practically demonstrate how easy some of the functions could be used and the software always left a faithful and accurate audit trail.

While MS Excel and MS Access also could provide some of the functionalities, however, ACL processes data without altering it. There is no risk of data being lost. Imagine deleting a column by mistake! Imagine when data rows exceed the maximum allowed by Excel!. These are no limitations for ACL The Question and Answer session that followed eloquently showed the interest of the audience.



IT Governance Domains -Strategic Alignment

Seem to be quite busy with your new IT responsibilities?" said I, to this friend of mine, over the phone. It has been about a year since we met last. Gone are the days when we used to meet regularly over a cup of coffee by the beach side.

As a senior member in the management team, he had been entrusted with the responsibility of managing IT. "C'mon" he replied in a tired voice "We have invested lots of time, money and efforts into this IT project. I am struggling to put this new software into production. I had to skip my last vacation and hardly get to spend quality time with the family".

In the next half hour he poured his heart out. They had invested on this new software without proper research and the project team was now finding it difficult to meet the user requirements and gain their acceptance.

"I am sure you consulted with the business functions before the purchase" I quipped. "I am afraid not. We thought we could tailor the software according to our requirements later" he replied.

"So what's the problem now?" I asked him in a nonplussed voice. "We have bought a pair of shoes - one size smaller and are trying to cut our feet to fit into the shoes" was his response before he hung up.

Not a very unfamiliar situation though. This is not the first time one gets to hear about such situations. I keep wondering - when humans can build the tallest towers and tallest bridges on earth with meticulous planning - why do IT projects flounder?

A recent report from the UK based Butler group states that **lack of effective information technology (IT) governance in the majority of organizations is perpetuating the chronic failure rate of IT-enabled**

business projects, and seriously impairing the achievement of business value. The research indicated that **IT governance initiatives were most often deployed solely within the IT department, and did not take into account the broader requirements of alignment with business objectives.**

As a consequence, there is a lack of coordination between the IT-led elements of projects and management of the associated business change.

A whitepaper released by the ITGI institute titled "IT Alignment: Who is in charge?" discusses the subject in length. The paper highlights the fact that majority of the organizations do not have a formalized IT Governance structure and process in place to ensure IT and business alignment. The responsibility of developing an IT strategy is often entrusted with the management teams below the board. Board members and business units are hardly engaged in the process of setting an IT strategy.

I have tried to present here some important discussion points from the paper; however I shall encourage readers to download the document from the ISACA website for a detailed reading. The paper is available as a complimentary download for ISACA members from the following links.

http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=633

<http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=30981>

Highlights

1. Surveys indicate that alignment of IT with business was one of the biggest enterprise issues.
2. Proper governance over the achievement of IT alignment requires

leadership and commitment from the highest levels of the enterprise.

3. Proactive engagement of the CEO and board is required to ensure that IT strategy is aligned with business strategy and delivers the expected results.

4. Lack of strategic alignment and the associated issues shall result in erosion of stakeholder value over time.

5. Responsibility of setting and implementing the IT strategy should rest with the business leadership.

6. Senior business management should become IT literate and ensure that IT planning becomes embedded into the enterprise strategic plans.

7. IT should be on the board meeting agenda regularly. The CIO shall present to the board a periodic update on the IT capabilities, current issues and emerging technologies which might open new opportunities for the business.

8. An **IT Strategy Committee** headed by a board member should advise and assist the board in the formulation of IT strategy.

9. An **IT Steering Committee** shall engage and assist in the delivery of the strategy.

Additionally an **IT Procurement committee** could approve and review the portfolio of IT projects and investments at regular intervals.

In conclusion the paper suggests that seamless communication and mutual understanding between IT and business functions are the essential ingredients in enhancing the value delivery of IT investments.

D Balasubramaniam, works for the ITA. Bala is the Education Chairperson on the ISACA Muscat Chapter Board.

SQL Injection Vulnerability

SQL Vulnerability is one of the most common exploits that a lot of web developers overlook. This vulnerability is a common exploit that hackers take advantage of. In this article we will cover some of the key points about this vulnerability and how it can be prevented.

SQL injection is a technique for exploiting web applications using user-entered data in SQL queries. There are a number of systems on the Internet that are vulnerable to such an attack and in this brief article we will try and understand some of the challenges that websites face due to weak coding.

When designing a dynamic database driven website, a good programmer must take utmost care to ensure that correct mechanisms are deployed to protect against SQL injection attacks and input validation problems. The way in which coding is done must take into account that any malicious command entered in the URL is handled seamlessly.

This means that when the malicious command is entered, the program must redirect the user to a well defined error page that informs the users that a wrong action is being performed.

The program must not reveal the error on the page since this will pro-

vide enough input for the hacker to find vulnerabilities in the website code.

According to an informal study by Michael Sutton of SPI Dynamics, it was demonstrated that 80 out of 708 tested web sites were susceptible to SQL injection attacks. In order to limit the test to sites that used a database, a Google search was done to find sites with URLs containing "id=10". The assumption was that any site using a name=number pattern in the query string was most likely doing a database lookup. Using this, 1000 sites were selected.

After removing duplicates and non-functional sites, Michael Sutton was left with a pool of 708 candidate sites. By altering the query string, he found that 80 sites were returning error messages that suggested they were vulnerable to SQL injection attacks.

In Jan 2006, a 17-year-old high-school student in Taiwan used SQL injection to break into the site of a Taiwanese information security magazine and stole customer's information. While study may not be formal enough for an academic paper, it does suggest that SQL vulnerabilities are a wide-spread problem among websites.

To be continued

Sachin Ravindra Toprani works for Omani E-Commerce LLC. He is also the webmaster for the ISACA Muscat website. This article is the first of a three part series.

Certification Update: June 2007 Exam Registration

Registration for the June 2007 Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) exams continues. The final registration deadline is 11 April 2007. Candidates will find additional exam details in the CISA or CISM Bulletin of Information for the June 2007 exams, which are available at www.isaca.org/cisaboi and www.isaca.org/cismboi.

June 2007 Exam Cancellations

The last day to request an exam cancellation for the June 2007 exam and receive a refund is 20 April.

The request form is available online at www.isaca.org/examdefer. Any questions should be directed to the certification department by e-mail at certification@isaca.org or by phone at +1.847.253.1545, ext 772

June 2007 Exam Deferrals

Candidates unable to take the exam can request a deferral of their registration fees to the next exam date. Requests received on or before 2 May 2007 will be charged a US \$50 processing fee. From 3 May 2007 through 1 June 2007, a processing fee of US \$100 will be charged. Deferral requests will not be accepted after 1 June 2007. For the convenience of ISACA members, a deferral can now be requested online at www.isaca.org/examdefer. Any questions regarding cancellations or deferrals should be directed to the certification department

Await Next CPE Program

The next CPE program would be on "Data Warehousing and Business Intelligence". The presentation would be made by Mr. Lalit Kumar Jain, Sr. Manager-IT, OTE.

Highlights of the presentation

- Data Warehousing concepts
 - Building the Data warehouse
 - Extraction and Transformation Loader (ETL)
 - End User reporting
- Availability of tools for the 3 phases
- Data Marts / Mining concepts
- Practical examples using one of the products

Details would be announced soon by mail. Visit our website for more details at www.isacamuscat.org

To contact ISACA...

Voice.....+1.847.253.1545
Fax.....+1.847.253.1443
Web www.isaca.org
E-mail ...info@isaca.org

News Briefs

IT Training & Awareness initiative

Muscat. The Information Technology Authority of Oman (ITA), the agency responsible for implementing the Sultanate's Digital Oman strategy, has launched a digital literacy-training pilot for 400 civil service employees.

This pilot is part of ITA's National IT Training and Awareness Initiative. The project aims to provide IT training opportunities to government and community citizens in Oman to build IT literacy amongst Omani citizens and equip them with required skills for sustaining the knowledge society of Oman.

IT is continuing to play a growing and

significant part in our lives, and it is important that citizens of Oman are ready for the digital age. Private and public sector employees will become increasingly dependent on information technology to deliver services. At the same time the community will also require fundamental technology skills in order to be a part of the growing digital society. A component of the *e-Oman* strategy aims to equip the citizens of Oman with the necessary IT skills and knowledge.

The first phase of government pilot training Digital Literacy will involve training the trainers, who in turn will train other users.

International Conference 22-25 July 2007



Singapore: ISACA is pleased to present its 35th annual International Conference and Annual Meeting of the Membership, which will be held in Singapore. The International Conference attracts more than 250 professionals from around the globe and has long been recognized throughout the world for providing in-depth coverage of the leading-edge technical and managerial issues facing IT audit, control, security, assurance and governance professionals. World-class presenters will bring together a wealth of experience and knowledge on best practices, system security, audit tools and processes, and other topics that impact not only those in a given geographic area, but all IT professionals worldwide. Educational streams will focus on managerial and business issues of IT audit, control, security and assurance. For more information and to register, please visit www.isaca.org/international.

Bookstore Update

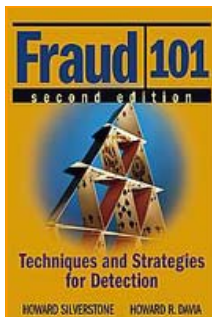
New ISACA Bookstore offerings include:

- COBIT 4.1
- COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition
- IT Assurance Guide: Using COBIT
- IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition
- Fraud 101: Techniques and Strategies for Detection, 2nd Edition

- Securing Converged IP Networks
- The Little Black Book of Computer Security



- Manager's Guide to Compliance: Best Practices and Case Studies



For descriptions and ordering, see the *Information Systems Control Journal* Bookstore insert, or contact the Bookstore at bookstore@isaca.org, www.isaca.org/bookstore or +1.847.253.1545, ext. 401 or 478. □ j

Journal Update

The *Information Systems Control Journal* is seeking articles for volume 5, 2007, to be issued in September 2007. The copy deadline for drafts for volume 5 is 24 May 2007, and the theme is **Value and Performance in IT**. For more information, please view the 2007 editorial calendar at www.isaca.org/journal or e-mail jhajigeorgiou@isaca.org. □ j

Distance Learning Update

The ISACA e-Symposium for April will focus on compliance issues with key industry leaders presenting on using capability maturity models, the challenges of IT outsourcing, and ISO 20000 audits and assessments. To register for the 17 April 2007 e-Symposium and take the first step to three free CPE credits, please visit www.isaca.esymposium.com. All of the live e-symposia have been archived and are available for viewing on demand. To view an archived event and have an opportunity to earn free CPE credits, please register at www.isaca.org/webcasts, where additional information on these valuable educational opportunities is also available

Information Systems Control Journal

This journal is a bimonthly publication of ISACA. This journal is read by professionals in over 140 countries around the world. Recent Journal articles are reserved for members. Articles more than one year old are available to the public.

Contact us

P.O Box No: 397,
Medinat Sultan Qaboos, PC -115, Oman,
E-mail: isaca_muscat@yahoo.com

President: A Subramaniam, 9931 8597
Vice President: Hamza Moosa Baqer, 9922 4410
Vice President: Ramamoorthy S, 9926 0391
Secretary: Itticheria P Joshua, 9938 9583
Treasurer: Nachiappan Thiagarajan, 9947 7891
Membership: Badri Narayan Subhudi, 9981 2050
CISA Coordinator: Gokul Krishnan, 9933 9637
CISM Coordinator: Abraham Kuruvilla, 9926 2459
Programs: Gopakumar C, 9932 0595
Education: Balasubramaniam D, 9523 4135
Newsletter & Website: Sachin Toprani, 9288 3116
Research Liaison: Sangeetha Sridhar, 9909 1600
Corporate Relations: Nabil Abdullah Al-Raisi, 99332985

Additional Directors

Treasury: Kishor Rabi, 9923 8067
CISA Co-ordination: Ernest Rodrigues, 24704457-351
CISM Co-ordination: Biju V.S., 9936 8459
Education: Venugopal Hari, 99215701
Programmes: Sandeep Menon, 9288 9027
Programmes: Ciby Mathew, 9292 6427
Membership: Hitendra Dutia, 9906 4960
Newsletter & Website: Mohd Moosa, 9933 1363
Research Liaison: Mohd Nayaz, 9942 9679

Immediate Past President: Antony Isaac, 9921 3008

About us..

Muscat chapter is one among more than 170 chapters of ISACA established in 60 countries worldwide. ISACA, as an international body has been in existence since 1969. ISACA with a worldwide membership of over 50,000 members is characterized by its striking diversity. Members live and work in more than 140 countries. They work in nearly all industries including financial and banking, audit and consultancy firms, government bodies and educational institutions. This rich diversity enables members to interact with each other. One of the strongest strengths of ISACA is the enormous resources it provides to its members through its website, regular regional and international conferences, free delivery of its technical journal -the *Information Systems Control Journal*, free access to *K-NET* an internet based compendium of reference materials and a bookstore covering the latest developments in the fields of IS assurance, control, security and governance.

Muscat chapter was established in 2000 under the sponsorship of the College of Banking and Financial Studies (CBFS) which is affiliated to the Central Bank of Oman. The chapter has a membership of more than 200 members. The chapter membership also mirrors the diversity of its parent body. The chapter's mission is to promote education for the CISA and CISM certifications, spread awareness of IS audit and controls, provide a framework for regular meetings and interaction amongst local IS audit and control professionals, thereby helping in raising standards and promoting best practices to manage Information technology effectively in their organizations.

CISA, CISM – Employ certified IT Professionals



CISA (Certified Information Systems Auditor) is ISACA's cornerstone certification. Since 1978, the CISA exam has measured excellence in IS auditing, control and security. CISA has grown to be globally recognized and adopted worldwide as a symbol of achievement. The CISA certification has been earned by more than 40,000 professionals since inception. The technical skills and practices that CISA promotes and evaluates are the building blocks of success in the field. Possessing the CISA designation demonstrates proficiency and is the basis for measurement in the profession. With a growing demand for professionals possessing IS audit, control and security skills, CISA has become a preferred certification program by individuals and organizations around the world.



Retaining CISA's and CISM's ensures success for any organization. Corporate governance and Accountability have stronger meaning when these efforts are powered by the presence of these qualified personnel.



If you have not joined ISACA, then join today. Visit www.isaca.org or www.isacamuscat.org for details....



CISM (Certified Information Security Manager) is ISACA's groundbreaking credential earned by over 5,200 professionals in its first two years. It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security.

The program is developed specifically for experienced information security managers and those who have information security management responsibilities.

The certification is for the individual who manages, designs, oversees and/or assesses an enterprise's information security (IS). Individuals earning the CISM certification become part of an elite peer network, attaining a one-of-a-kind credential.