

President's Column

Dear Readers,

I feel greatly privileged writing my first post to you after my assuming the office of the President of this glorious chapter.

Looking back, I am humbled by some of the greatest leaders in the past who have led this chapter and set new standards. I am conscious of the responsibility that lies ahead of my team!

Amongst our various initiatives, the chapter newsletter is a key initiative to enable our chapter members to connect more closely. With the rotational Editorial scheme, I hope you will find new energy and dynamism in every issue!

I take this opportunity to thank each of you for your confidence in me and look forward to your support in our journey to elevating our chapter as the globally best chapter!

Wishing you the very best!

D Namasivayam
ISACA, Chennai Chapter



D Namasivayam & team takes over

Change of Guard @ ISACA Chennai



The Annual General Meeting of ISACA Chennai was held on 27th July 2009 at Hotel Maris. Some of the highlights of the general body meeting included K B Sankaran presenting the Secretary's report enumerating the impressive happenings during the last two years, followed by C M Krishnaswamy detailing the financial performance and management of chapter funds.

The outgoing president NSN Pillai profusely thanked the members for their whole-hearted support to the activities of the chapter, after which the elections were conducted by veteran member P K Ramanan. The new team of Directors under the leadership of D Namasivayam was elected and took charge from the outgoing team, to hold office for the coming two years. Amongst the newcomers to the Board were Vijayalakshmi Sankar, who took charge as Director (Academic Relations) and M R Jambunaathan as CISA Co-ordinator. Jamuna Swamy, veteran and Past President of the chapter volunteered to lead as the Director (Programs).

In his takeover address to the members, Namasivayam was his usual modest self, recounting his initial humble steps at the chapter and assuring his best to keep up the good work done by the past leaders.

The meeting was well attended and ended with a networking dinner hosted by the chapter.

this issue

Change of Guard **P.1**

Happenings @ ISACA Chennai **P.2**

BCP Lessons from Pandemic **P.3**

It's time to start counting CPEs **P.4**

Meet your new Board !



President	- D Namasivayam
Vice-President	- K B Sankaran
Hon. Secretary	- Chitra Murali
Hon. Treasurer	- K Suresh Kumar
Director Membership	- M P Badrinath
Director Spl Int. Grp.	- C M Krishnaswamy
Director Research	- S C Sekar
Director Certification	- R Vittal Raj
CISA Co-ordinator	- M R Jambunaathan
Director Programs	- Jamuna Swamy
Director Acad. Rel.	- Vijayalakshmi Sankar
Director Marketing	- A Vijayakumar
Director Audit	- N R Murali
Imm. Past President	- NSN Pillai



CPE Events

BCM during pandemic outbreak

Half Day Seminar on **Business Continuity during Pandemic Outbreak** was held on August 24. In the background of the swine flu outbreak alert, SC Sekar & Jamuna Swamy eloquently elucidated on the vulnerabilities and various facets associated with business continuity measures that organizations need to take to effectively initiate early steps for protecting its people and countering business disruption arising therefrom.

Monthly Meetings

July 2009

Mrs. Vijayalakshmi Sankar, Consultant, Steria, spoke on **'Outsourcing Governance, Risk and Compliance'**.

The talk held at our chapter on 18th July, highlighted the risks underlying increasing tendency of organizations to outsource operations and management and highlighted the importance to continuously monitor the risk and value of any outsourced activity. The session also involved interesting discussions on practical aspects and problems faced by organizations in implementing such controls.

August 2009

On 15th August 2009, Mr. Gouri Shankar, Reachwell Software spoke on **'Software Asset Management'**, a much discussed topic. Besides highlighting the importance of managing software assets, he elaborated on the risks and practical limitations in enumeration, recording and managing of software assets. The risks underlying ineffective management software assets and solutions and tools therefor were also discussed.

September 2009

Defects and reworks costs are silent killers that can cause significant and sometimes irreversible damage to organizations..... At the monthly meeting of the Chapter on 24th September, 2009, a distinguished speaker on

the subject, Mr. Chandrakumar Raman, Programme Manager, Quality Operatiins, Hewlett Packard, emphasized on the need for structured Delivery Cost Optimization Programme that every quality conscious business needs to put in place to meet their quality missions and deliver operational excellence.

Certification Events

CISA Exam Review Course

The regular CISA Exam Review course of the chapter commenced on August 2, 2009 with overwhelming response. As usual, the opening session of the course was marked by the presence of most of the directors of the Chennai Chapter, who encouraged and inspired the members. Spread over about 14 sessions every Sunday, the Chennai Chapter's CISA Review course continues to be voted the best. The secret of success has been the energetic and enthusiastic but selfless volunteer support of the faculty members who come forward to share their knowledge and experience on the subject.

CISA Mock Exam

The chapter also conducted the first mock exam for the benefits of exam aspirants on 19th September 2009. The mock exam is open to CISA Review course candidates and to others for a fee.

Certification Meet

A certification meet was organized by the chapter on October 12, 2009 at the Chapter premises, with two sessions, the first focused on CISA certification requirements and the other session for CISM & CGEIT. Many delegates benefited from the discussion on various aspects of getting certified and clarifying their doubts.

ISACA – LIBA Partnership

The Diploma course in IS Security & Audit administered by LIBA, continues to grow with the dedicated faculty support provided by many of our board members. This time a new record was set with the enrolments reaching 26, which included senior professionals from the industry.

Upcoming CPE Events

One Day COBIT Event

October 24, 2009
IC & SR Centre,
IIT-M Campus



The one full day seminar will provide insights into the fundamentals of IT Governance and COBIT 4.1®, (Control Objectives for Information and related technology), the globally recognized standard on IT Governance from the IT Governance Institute, USA.

The seminar will discuss on:

- Why & What of IT Governance and its relevance in Corporate Governance
- Overview of COBIT 4.1® - Framework and its components
- How Audit & Assurance professionals can use COBIT components

Facilitator: R Vittal Raj

For more details visit the chapter website.

CISA Intensive Review Course

Four Day CISA Intensive Review Course

November 5 to 8, 2009

Limited Seats!

To register visit chapter website

Computer Security Day

Chennai Chapter Annual Conference

Theme:

Managing Value IT in uncertain times

When:

November 28, 2009

Where:

GRT Grand, T.Nagar

It's here! Be there!

BCP Lessons from a Pandemic Aftermath

SWINE FLU



Risk IT
BASED ON COBIT®

The Risk IT Framework

Risk IT is the ISACA's new kid on the bloc!

Risk is a natural part of the business landscape. If left unmanaged, the uncertainty can spread like weeds. If managed effectively, losses can be avoided and benefits obtained.

In business today, risk plays a critical role. Almost every business decision requires executives and managers to balance risk and reward. Effectively managing the business risks is essential to an enterprise's success.

Too often, IT risk (business risk related to the use of IT) is overlooked. Other business risks, such as market risks, credit risk and operational risks have long been incorporated into the corporate decision-making processes. IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same 'umbrella' risk category as other business risks: failure to achieve strategic objectives

Risk IT is a framework based on a set of guiding principles for effective management of IT risk. The framework complements COBIT®, a comprehensive framework for the governance and control of business-driven, IT-based solutions and services. While COBIT provides a set of controls to mitigate IT risk, Risk IT provides a framework for enterprises to identify, govern and manage IT risk. Simply put, COBIT provides the *means* of risk management; Risk IT provides the *ends*. Enterprises who have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

The Risk IT Framework fills the gap between generic risk management frameworks and detailed (primarily security-related) IT risk management frameworks. It provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues.

In summary, the framework will enable enterprises to understand and manage all significant IT risk types, building upon the existing risk related components within the current ISACA frameworks, i.e., COBIT and Val IT.

The Risk IT Framework describes a detailed process model for the management of IT-related risk. In this model, multiple references are made to risk analysis, scenario analysis, responsibilities, key risk indicators and many other risk-related terms. *The Risk IT Practitioner Guide* contains practical and more detailed guidance on how to accomplish some of the activities described in the process model.

The Risk IT Framework and its companion, *The Risk IT Practitioner Guide*, are currently in publication review and scheduled to be available in late November. However, you may download the exposure draft of the framework and an informative brochure for a sneak peak at ISACA's newest framework.

After SARS, Swine Flu (H1N1 Influenza Virus) was the next and this time it decided not the spare India! Probably for the first time, a pandemic seized the attention of the best of the industry, especially the IT & ITES companies, like never before. Numerous initiatives were taken by both the government and the industry associations in preparing the industry to contain the outbreak and minimize the risk of infection.

With the World Health Organisation (WHO), labelling H1N1 as a stage 6 pandemic outbreak, the worse may be yet far from over, but more than the pandemic containment measures, H1N1 exposed some hidden vulnerabilities in the most security conscious organisations, many of which were not only certified against some of the coveted standards such as the ISO 27001 but also boasted of the best security practices.

Amongst the vulnerabilities exposed included the following:

- While most organisations had included people as a key asset in their security risk assessment but the individuals, roles and positions vis-à-vis their criticality was not considered. Further IT organisation, roles and responsibilities were either not formally defined, lacked clarity or were not updated.
- The threats and vulnerability assessments did not include pandemic and the organisation's vulnerabilities thereof.
- More than the numbers actually affected by the pandemic, organisations experienced pangs of mass absenteeism due to the fear of infection.

- Instances of mass resignations or losing critical employees due to team/unit level outbreak of infection, more out of the fear and depression.
- Organisations discovered several single point of failure arising from critical dependence on a few critical staff, which included vulnerable positions such as customer account managers, network and system administrations, Unit heads etc.
- Exposed the lack of or weaknesses in knowledge management systems, which failed to capture people expertise and knowledge.
- Human Resource function not actively included/involved in the security forum, especially risk assessment exercises.
- Lack of updated documentation of processes, activities, roles and responsibilities.
- Incidence Response did not factor effective escalations for pandemic risks.
- Reputation impact arising from unwanted media publicity targeting organisations experiencing such exposures.
- Disaster Recovery drills did not include testing for pandemic risk scenarios.

The lessons highlighted the need for re-looking at the Business Continuity Management processes and remediating related vulnerabilities in the IT governance framework.

ISACA Member Benefit



Make
Employment
Connections

Visit ISACA Career Centre

It's time to start counting your CPEs!

It's going to be year end again, time to count your CPEs.

Whether you are a CISA, CISM or CGEIT, it is common knowledge that securing the required CPEs as per ISACA's CPE policy is a critical requirement to maintain your certification. It is critical to ensure compliance with CPE requirements to be able to maintain your certification!

Check out on the following:

Do you have a minimum 20 hours CPE for 2009? Else plan to make it up before December! It is advisable to clock 40 CPE hours per year.

If you are in your last year of the 3 year cycle, ensure that you will get atleast 120 CPE hours before December 2009?

Remember to pay your certification fee for 2009! You would already have received your mail from ISACA by now. If not don't worry, ISACA generally sends a reminder before year end.

How to check your CPEs – login to www.isaca.org using your login credentials and go to 'My profile → Certification Profile', you will find your CPEs that you have reported till 2008 or later for the 3-year cycle period.

Some of the ways to make up your CPEs:

- E-symposiums
- Professional meetings & conferences
- Information Systems Control Journal quiz

To know more about qualifying educational activities and other professional activities, read the Continuing Educational Policy applicable to your certification(s).

ISACA has the right to audit your CPEs claimed, hence it is highly recommended to ensure you maintain proper records of your CPEs. Some suggestions to keep your records

- Ensure the event for which you are claiming CPE, qualifies for CPE as per ISACA CPE Policy
- Maintain a copy of the invitation/brochure with programme schedule details
- Secure and maintain a certification of your participation in the event/part of event
- Maintain a CPE tracker to help you track your CPEs and keep the tracker updated.
- Update CPE Hrs in your ISACA profile as per the tracker maintained by you.

Latest @ ISACA Book Store

Security, Audit and Control Features SAP® ERP, 3rd Edition

Building the Business Case for COBIT® and Val IT™: Executive Briefing

Val IT™ Mapping: Mapping of Val IT™ 2.0 to MSP™, PRINCE2™ and ITIL® V3

COBIT and Application Controls: A Management Guide



Interesting Findings from Audit Reports

Finding: The company has implemented maker-checker controls for most significant controls except the maker and checker were not identified in most cases.

Finding: Access Controls have been implemented with well defined documentation of controls over application and system privileges, however we were unable to verify the implementation of such privileges in the system since the administrator password was reported to be known only to the personnel deployed by the service provider, who was not available and appears to have quit the services.

Finding: We were unable to review access controls in the sensitive technical help desk area since the physical access to this area is strictly restricted only to authorised personnel, however while reviewing the CCTV monitoring facility, we were able to pick up the passwords and line commands typed on secure terminals in this area by zooming in on the PC monitors using the surveillance cameras installed in the secure help desk area, ably assisted by the security personnel responsible for surveillance

CERT IN Risk Advisory on SMB v.2

The latest advisory from CERT-IN alerts on the SMB v.2 holes in Windows operating systems. SMB (Server Message Block) is a protocol used by Microsoft to share files, printers, serial ports, and also to communicate between computers using named pipes and mail slots. Even a casual hacker can crash a system by mounting a denial of service attack or even remotely execute arbitrary code using user/anonymous account. The solution is to ensure good firewall standards and apply the latest OS patch.

This newsletter is for circulation among members of ISACA Chennai. Not for sale.

Editorial Committee: NSN Pillai, K B Sankaran, M P Badrinath, R Vittal Raj, S C Sekar. Advisor to the Editorial Committee: Emani BSP Sarathy.

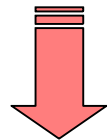
This issue is edited and published by R. Vittal Raj on behalf of the Editorial Committee of ISACA, Chennai.



from: ISACA Chennai



Next



@ Mumbai
Feb 2010

Send your comments and suggestions on this newsletter to the editor of this issue at rvittalraj@vsnl.com

