isaca@mumbai

www.isacamumbai.org Issue No. XXXVIII October 2009-April 2010

Message From The President

Dear Fellow Members,

It gives me immense pleasure to address you on behalf of ISACA Mumbai Chapter as the Chapter President. At the outset my sincere thanks to all of you for coming forward and supporting the present Management committee.

My sincere apologies for not being able to address you earlier, as your chapter was amidst a lot of hectic activities focused around holding an international conference-ASIA CACS 2010 which came to Mumbai after a decade.

As usual your chapter has been a trend setter at ISACA and at the recently concluded ASIA CACS 2010 conference, we had a record number of participants which crossed 275 + and we broke our own earlier record of year 2000. The Conference and the Pre-Conference Workshops were both sold out much before the dates of the conference. The participants included delegates from nearly 18 countries of the Asia Pacific Region. We could successful achieve many of the goals that ISACA HO had set for us and the same was well appreciated by ISACA HO

The Asia CACS 2010 conference was preceded by an Asia Leadership Conference where Chapter Leaders from across the Asia Pacific attended and the concerns of the local chapters in the Asian region was also addressed by ISACA HO. I am also delighted to inform you that K Wayne Snipes Award for the best Very Large Chapter in Asia for the year 2009 was presented to the Chapter at the Asia Leadership Conference by Mr. Robert Stroud, International Vice President of ISACA

As on date our membership stands at 1785. One of the key concerns which has been bothering us is the growth in the membership figures at the same time involvement of members. This is also a reminder time for a lot of members to renew their membership and continue with their membership benefits.

We are actively seeking a Feedback from our members, seeking suggestions and ideas for improvement in our services. This will surely help us to understand your needs better and help us to serve you better. Those who have not yet sent in your feedback forms, we sincerely request your feedbacks at the earliest. We have also embarked upon a volunteer scheme which has received a fairly good response

As usual we are coming up with increasing number of chapter meetings and programs with more focus being given to hands-on / practical oriented training workshops to give the delegates a flair of actual working environment. Your suggestions to help us improve these workshops / training programs will be greatly appreciated

There is one area which I personally would like to focus is the **Trainee System Auditor Scheme**, which has been framed in response to requests from newly passed members to help them gain the requisite Experience and attain ISACA's Valued Certification. I sincerely request our Senior Members to come forward in large numbers as Trainers, Mentors and Counselors' and help their younger brethren to gain the valuable experience.

We also look forward to your continued support in the days to come as we continue our Mission for the year – **Educate, Enrich and Excel**

With Best wishes and regards,

Anand P. Shenoy

Editorial

Dear Friends,

It gives me great pleasure to address all of you through the news letter after a along gap of more than 3 years. My sincere apologies to all of you for not having been able to release the newsletter as scheduled in January 2010.we have had an hectic time in the last couple of months especially we had to launch an international event Asia CACS which came to us in the month of February after a gap of 10 years.

On the regulatory front, we are happy to inform you that SEBI vide its circular has asked for an audit of mutual Fund once every two years. The IS audit has to be conducted by a CISA/CISM or equivalent professional. This is a very healthy step in terms of involving CISA professionals.

One of the key events was the launch of Windows 7 and Windows 2008 R2. Unlike the launch of Vista which was held with much fanfare, the launch of this two products did not catch the eye of the media as it was a low profile event.

ISACA Mumbai chapter jointly with Microsoft is in the process of releasing the Microsoft Security Handbook 2010 ,which will be shared with the community shortly. I have been instrumental in the content management of this book and would look forward to valuable suggestions in improving the value delivery of the content.

COBIT is also undergoing a major change to COBIT 5. Request all of you to closely watch the ISACA website for further developments on this front.

There has been hectic activity at the ISACA end. They are working on the new look and feel and efficiency enhancements on the website.

We are now having a new logo and a new certification has been introduced and request members to avail of the benefit of the same.

As the examinations are round the corner, we wish all the CISA/CISM/CGEIT aspirants best of luck.

Regards,

Nanda Mohan Shenoy D

ATM security

Automated Teller Machines (ATMs) has become a very Important delivery channel for banking transactions in India. All banks have been deploying ATMs to increase their reach within the masses. Indians are now using the automated teller machines (ATM) for various banking needs. According to a recent survey, 95% people now prefer this modern channel of banking.

Different value added services, provided on the ATMs along-with it primary cash dispensing services makes it more popular. Customers use ATMs to recharge their mobile phones, pay utility bills and other related services.

This electronic access to banking needs has also given rise to financial frauds carried out through the ATM channel. These frauds are very sophisticated requiring both technical and human expertise to embezzle the confidential customer data including crispy notes available in ATM chests. These kinds of frauds are widespread in foreign countries. Such frauds are also now on rise in India too.

Different physical and logical security controls need to be implemented around the ATM service provided to the customers. There should be a well defined defense-in-depth program placed around the ATM channel to address security vulnerabilities and covering all aspects including personnel, technology and operations.

Physical security controls like installing CCTV cameras at the ATM site capturing the photos of people using ATMs and capturing the ATM site including the drop-boxes are very common. Regular review of the camera logs should be in place to identify fraudulent activities. Round- the-clock guard at the ATM site to keep a check on the skeptical visitors must be in place. Installation of privacy panels to avoid shoulder surfing to customer's confidential data. Educating customers using security signage placed in and around the ATM vicinity.

Logical controls have to be in place prevent leakage to confidential data using complete encryption of channel and messages (TDES and AES), encryption of hardware and software. Installing ATMs with industry accepted encrypted PIN Pads, which will encrypt data directly behind the PIN pads. Using industry accepted ATM switches which follow ISO8583, ISO 9564, ANSI X9.8 and Payment Application Data Security Standard (PA-DSS) industry standards to protect customer confidential data.

In US, ATM frauds are covered by various regulations. There is no regulation governing ATMs in India. They are treated as a general criminal act governed by the Indian Penal Code. In the current scenario, industry best practices like PCI DSS, ISO 27001, COBIT and VISA PIN Security have to be implemented to ensure all required IT controls are in place to protect customer confidential data.

Sachin M Bhosle
CISM, CISSP, ISSAP
Head – Audit and Compliance
Euronet Services India Pvt.Ltd.

Achievements Galore

Mumbai Chapter wins the Gold Level Award for the Best Website for the Year 2009

ISACA Mumbai Chapter wins the K Wayne Snipes Award for 2009 for Best Very Large Chapter in Asia

Memento received on account of Hosting the Asia CACS

Local News Round up

CISA/CISM/CGEIT News

CISA,CISM & CGEIT Exams
The examination was conducted Thakur engineering college Kandivali and at SBOA School @ Nerul

CISA,CISM Review Classes
The review classes and crash course for CISA was conducted as usual at Welingkar and CISM review classes were also conducted at Welingkar.
The normal classes were preceded by Awareness session on 26th July for Dec 2009 Batch on 17th January 2010 for Jun 2010

	CISA		CISM
	Normal Course	Crash Course	
June-2009	60	26	10
Dec-2009	76	20	16
June-2010	68	NA	16

CISA and CISM Felicitation was held at Welingkars for Dec 2008 and June 2009 passers on 6th Feb 2010

CISA Mock Test for all CISA Aspirants Scheduled on 30th May and for all CISM aspirants on 23rd May.
Please contact chapter office for further details
CISA crash course scheduled on two weekends (15th and 16th May,22nd and 23rd May)

Programme By ISACA,Mumbai October 2009-March 2010

Sr	Dates	Days	Workshop	Organisation	Partici-pants	CPE Hrs
1	7-8/11/09	2	Application Security & OWASP	MIEL	10	*140*
2	14-15/11/09	2	ITIL ver 3.0	Vinsys	1	*14*
3	28-29/11/09	2	BCM Workshop	NII Consulting	9	*126*
4	18-19/12/09	2	Application Security & OWASP	MIEL	10	*140*
5	23-24/12/09	2	Application Security & OWASP	MIEL	6	*84*
6	22-24/1/2010	3	Banking System Audit Seminar	ISACA	37	*777*
7	13/2/2010	1	ACL-Audit Workshop	SSPL	14	*98*
8	10-11/3/2010	2	Application Security & OWASP	MIEL	9	*126*
9	20-24/3/2010	5	ISMS Lead Auditor	SAI Global	11	*385*
10	30-31/3/2010	2	Application Security & OWASP	MIEL	4	*56*
11	21/1/2010	1	GRC Seminar	Oracle	50	*350*
12	13/3/2010	1	Windows 7 Security	Microsoft	14	*98*

Forthcoming Programmes

Sr	Date	Days	Proposed Programme	In association with	Venue
1.	17/4/2010-18/4/2010	2	Database Security Audit	NII Consulting	The Avenue
2.	1/5-2/5/2010	2	Computer Forensic	NII Consulting	The Avenue
3.	8/5/2010-9/5/2010	2	SAP Audit Workshop	Apiruh Consulting	Hotel Athithi
4.	Yet to be decided	2	COBIT Workshop	A Rafeq & Associates	
5.	26/6/2010	1	BI & Datawarehouse – Part I	Chandan Banerjee	WIM

The programs are based on tentative schedules received. ISACA Mumbai chapter reserves the right to cancel and /or modify the program schedule based on the number of participants or the availability of the Faculty. Members are advised to contact the Chapter Office for further details

International News Round up

	ISACA Unveils a new Logo Effective 1st January 2010 with a new Tag line **'Trust In, and value from, Information Systems**
	New Certification Launched ISACA is proud to announce its newest certification, Certified in Risk and Information Systems Control™ (CRISC™)(pronounced "see-risk"). This certification is designed for IT professionals who identify and manage risks through the development and implementation of appropriate Information systems controls to help enterprises accomplish business objectives. The certification is intended for individuals who have a minimum of three to five years of experience performing tasks related to the following subject areas (domains): • Risk identification, assessment and evaluation • Risk response • Risk monitoring • IS control design and implementation • IS control monitoring and maintenance A grandfathering program, through which professionals who are highly experienced in the CRISC job practice can apply for the CRISC certification without taking the exam, will be available beginning in April 2010. The first CRISC exam will be administered in the second half of 2011. • More information can be found at *www.isaca.org/crisc*.
	ASIA CACS comes to Mumbai after a decade The ASIA CACS Conference was held a Hyatt Regency on 22nd and 23rd February 2010 and was well attended by delegates across asia pacific and the registration crossed 250. The Next Year CACS will be held in Dubai in Feb 2011
	Exposure Drafts The most important framework COBIT 4 is under revision and the exposure drafts are available at the website. Request all members to give their valuable input on the exposure draft and contribute and at the same time earn CPE hours for the comments. Please visit ISACA website for further details
	CISA and CISM Review Manual goes online: As a part of the e- initiative the CISA and CISM Review Manual is now available online to all the members. As on the date of this news letter 2010 Chapter is available and others are in the process of being added. They can also be downloaded, with certain restrictions Members can access the e-library under Bookstore. In addition there are a huge number of resources available under the e-library

Know your ISACA

1.	How many Members of ISACA is present worldwide as on 1st Feb2010?
(a)	96,528
(b)	65,389
(c)	72,899
(d)	89,112
2.	How many Chapters of ISACA is present worldwide as on 1st Feb2010?
(a)	203
(b)	186
(c)	175
(d)	152
3.	ISACA worldwide is organized into how many regions
(a)	4
(b)	5
(c)	3
(d)	6
4.	Which of the following is not a Geographic region of ISACA
(a)	Oceania
(b)	Latin America
(c)	Asia Pacific
(d)	North America
5.	How many Chapters of ISACA do we have in India?
(a)	6
(b)	8
(c)	10
(d)	12
6.	How many certified CISA's worldwide as on 1/2/2010
(a)	57,272
(b)	45,363
(c)	65,278
(d)	25,786
7.	What percentage of CISA's are in Asia region?
(a)	15
(b)	27
(c)	10
(d)	35
8.	Vijayawada in India has a local ISACA Chapter
(a)	True
(b)	False
9.	ISACA was formerly known as
(a)	EDP association
(b)	EDP Auditors Association
(c)	ISACA itself, no change in the name
(d)	Information Technology Audit association
10.	ANSI has accredited CISA and CISM under which standard
(a)	ISO 17024:2003
(b)	ISO 9001:2008
(c)	ISO 27000:2005
11.	One can be Certified CISA and need not be a member of ISACA worldwide
(a)	True
(b)	False

Answer To Case Study of the Previous Issue

The case study reflects a potent environment and presents the dilemma of business, social interaction and security.

Security beings with a framework, policies, practices, procedures and ends with effective deployment of technology.

It is no doubt essential for an organization, not only to have a business focus but also have a human approach in its working. However, it is often the human element and people issues that prove significant in information security.

In the instant case the framework, policies and their deployment are found to be of a very high order and the employees are not only aware and tuned, but also have a human touch.

However, as can be seen from some of the issues that present themselves during the round that Ravi takes, on this first day in office, it is sometimes the human trusting approach that can expose an organization to serious social engineering threats including loss of trade secrets and design ideas to competitors.

Issue-1: Ravi who is without the smart card is let into the facility by an attendant, using his own card – An imposter can gain unauthorized access.

Issue-2: Ravi is accepted, on his first day – (he is obviously a stranger to Sanjay) as an employee without his smart card, (probably on the basis that he is already inside the factory unit) and shown and allowed to handle sensitive design department desktop.

Issue-3: Ravi is allowed internet and email access by Sanjay – an employee by using his (Sanjay's) own access credentials.

Issue-4: Ravi's password is telephonically reset for him by the help desk without sufficient identification.

Issue -5: Waste paper is being allowed to be removed by outside unknown scavengers (rag - pickers), instead of being securely destroyed and disposed off – a case of dumpster diving.

Issue -6: A rank outsider (pregnant lady) is allowed access into the office to use the toilet without identification and authorization – a perfect setting for a social engineering intrusion /attack.

Thus, apparently innocuous actions of staff, albeit on humanitarian grounds, trusting the outsider, can and do lead to severe compromise of the best security systems.

Answers To eQuiz of last Issue:

1. A - Metasearch engines are programs that automatically submit your search request to several search engines simultaneously.

2. B - Keyword search. In a keyword search, you enter a keyword or phrase (like "Marty Robbins" drummer 1965) reflecting the information you want.

3. A – Code. The last part of the domain name following the dot is the domain code.

4. D – E-learning. E-learning is a rapidly emerging Web application where it is possible to take classes online on almost any subject.

Case Study By Dr. Vishnu Kanhere

'Piping Pizzazz' is a renowned chain of over one hundred pizza and burger outlets that also serve softy ice creams spread across three continents, twenty countries and sixty cities.

The chain prides itself in providing toppings and flavors that the customers desire and has implemented data warehousing and data mining solutions to capture, understand analyze, process and use customer information, customer preferences and choices for decisions on toppings, flavors, products, pricing and marketing strategies. It is an expensive decision support system that has given a strategic advantage to the company over its competitors by enabling mass customization and competitive pricing.

The company's outlets have computer terminals connected to the central server to capture point of sale data as well as managing supplies, inventories and for accounting and control.

Strict instructions have been given to all outlets to follow proper procedure and ensure that supplies food preparation and sales happen only on recording in the online system.

This requires that the online central server is always available 24x7 and there is a robust BCP / DRP in place to enable prompt recovery in case of a disaster event.

The company has recently appointed you as a specialist to take care of BCP / DRP in the company. You visit the data centre as well as the disaster recovery site and after making a study of the existing system discover the following:

1.The BCP – DRP plan was last documented around three years back. The changes if any thereafter have not been documented.

2. On discussion with the IT department you discover that the server at the DR site has a capacity equal to 25% of the central server. You are not sure if this is adequate to provide the required processing capability in the event of a disaster.

3.The head of the IT team feels that given the customized nature of the solution the recovery point objective needs to be short, and given the complex nature of the data the recovery time objective also needs to be short.

4.The BCD/DRP plan has been tested once after it was developed but the IT manager is not happy with the results as he thinks that in a real emergency it may not work.

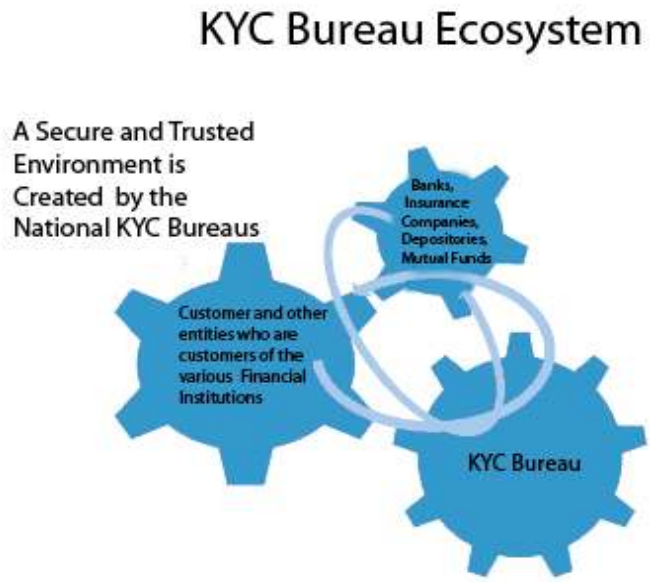
5.The board in its last meeting has suggested redeployment of certain IT staff currently dealing with data backups and recovery to data processing, as there has been a general downturn in the market. They feel for a food outlet chain, information systems and their recovery in times of disaster may be a bit of a luxury in these trying times.

You are requested to give your comments and suggestions
Email your answers to the case study to vkanhere@gmail.com your solutions will be given and a suggested solution will be published in the next issue.

A Solution for Centralized National KYC Bureaus in India

L.S.Subramanian

Summary:
This article examines the need for Centralized National KYC Bureaus in India and proposes an outline for their operations and regulations and deliverable. It also recommends that the Government of India bring KYC Bureaus into operation .It is also proposed to mandate use of two fingerprints for Biometric identification.



Background to KYC:
Knowing your customer – KYC- has become a strong focus of attention in recent years within the Banking and Financial services space, as the Indian Government and Financial organization being to view KYC as a critical, proactive measure against financial crime rather than just another compliance burden.
KYC compliance regulation has been proactive in making it mandatory for KYC norms for various financial transactions including Banking, Insurance, Mutual Funds, Depositories, Stock Market Intermediaries, Pension Fund Managers and host of other Financial Institutions.

Why KYC:
The various terrorist attacks in India and elsewhere in the world has revealed that there are sinister forces at work and that terrorist activities are funded with laundered money, the proceeds of illicit activities such as narcotics and human trafficking ,fraud and organized crime. The combating of terrorist financing has become a priority of Indian and rest of the world. Hence the financial services provider "Knowing your customer" was no longer a suggested course of action since Know Your Customer (KYC) compliance mandates were created by the Indian Government to combat

What is KYC?
Know Your Customer or KYC refers to the regulatory compliance mandate imposed on financial service providers to implement a Customer Identification Program and perform due diligence checks before doing business with a person or entity. KYC fulfills a risk mitigation function and one of its key requirements are checking that a prospective customer is not listed on any government lists for wanted money launders known fraudsters or terrorists.
Beyond customer identification checks, the ongoing monitoring of transfers and financial transactions against a range of risk variables forms an integral part of the KYC mandate.
money laundering and the funding of terrorist activities.

Origins of KYC Compliance:

The arrival of the new millennium was marred by a spate of terrorist attacks and corporate scandals that unmasked the darker features of globalization. These events highlighted the role of money laundering in cross-border crime and terrorism, and underlined the need to clamp down on the exploitation of financial systems worldwide.

KYC legislation was principally not absent prior to this era, regulated financial service providers for a long time have been required to conduct due diligence and customer identification checks in order to mitigate their own operation risks, and to ensure a consistent and acceptable level of service.

In essence, the new KYC Laws are not so much a radical departure from self regulated industry practices as it was a firmer and more rigorous regulation of a greater range of financial services providers, and expanded the authority of the law enforcement agencies and regulators in the fighting of terrorism and other anti social activities in India and globally.

KYC Compliance and Cost Implications for Business:

The KYC compliance mandate, for all its positive outcomes, has burdened companies and organizations with a substantial administrative obligation. Additionally, KYC compliance

Increasingly entails the creation of auditable proof of due diligence activities, in addition to the need for customer identification.

In order to meet KYC compliance requirements, financial institutions must:

1. Verify that customers are not or have not been involved in illegal activities such as fraud, money laundering or organized crime.
2. Verify a prospective client's identity.
3. Maintain proof of the steps taken to identify their identity.
4. Establish whether a prospective customer is listed on any sanctions lists in connection with suspected terrorist activities, money laundering, fraud or other crimes.

The KYC verification rules place a big financial burden on Banks, Insurance Companies, Mutual Funds due to costs involved on doing a KYC Verification. The centralized

KYC

Bureau will reduce the transactional costs for the KYC verification.

Stricter customer due diligence laws have forced financial institutions to increase compliance

Efforts in this area –leading to escalating compliance expenses at a time when the sector can least afford these additional costs.

Stricter customer due diligence laws have forced financial institutions to increase compliance efforts in this area - leading to escalating compliance expenses at a time when the sector can least afford these additional costs.

There is a real business need for Centralized and Automated National KYC Bureaus with current information technology that can drive cost savings while ensuring best practice . We are confident that the Finance Ministry of the Government of India will take the lead in ensuring that KYC Bureaus are operational at the Earliest. The KYC Bureau will also be effective in preventing identity theft fraud, money laundering and terrorist financing.

Approach:

The setting up of a KYC Bureau will allow a customer to be registered and screened by the KYC Bureau only once, thus reducing the burden on the customer to go through the KYC Process multiple times.

Validation of the norms can be done once in five years after registration unless there is a change in the customer like death, migration, address change, change in marital status, and change of income, change of employer or any criminal charges.

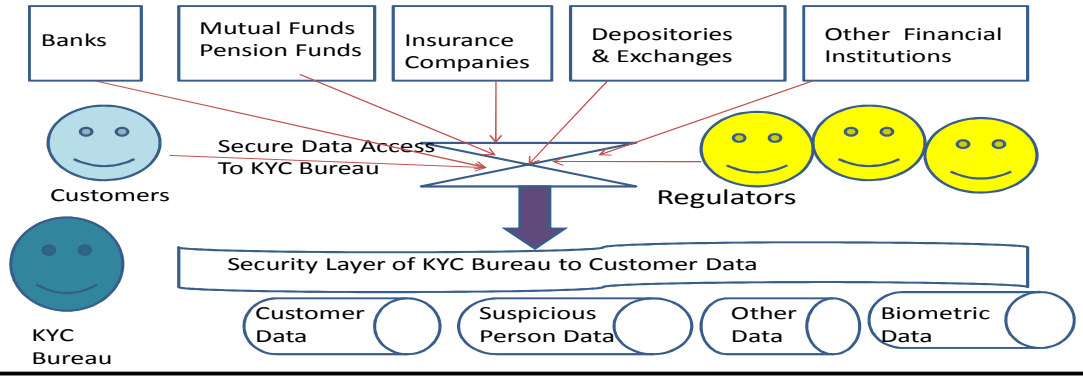
Process:

Once the KYC Bureau has a customer registered it will give the customer a unique Customer Identification Number (CIN) and also a KYC Smart Card with his name, address and other key details like date of Birth and biometric details in the smart card. The detail profile of the customer can be accessed by the participating bank/financial services company with access to data for the KYC verification required by its regulator.

The KYC Bureaus will conduct the KYC verification and will also retain the personal data of the customer Including biometric information. The KYC Bureau will maintain all ensure data required by various regulators of the Banking Sector, Financial Services Sector like Insurance, Financial Markets Mutual Funds and Pension Funds are addressed at the time of collecting Customer Data.

Participating companies can pay the Bureau on a transaction based model or fixed cost model for verifying the KYC requirements of the customer, the tariffs can be decided by the Regulator.

KYC Bureau Architecture

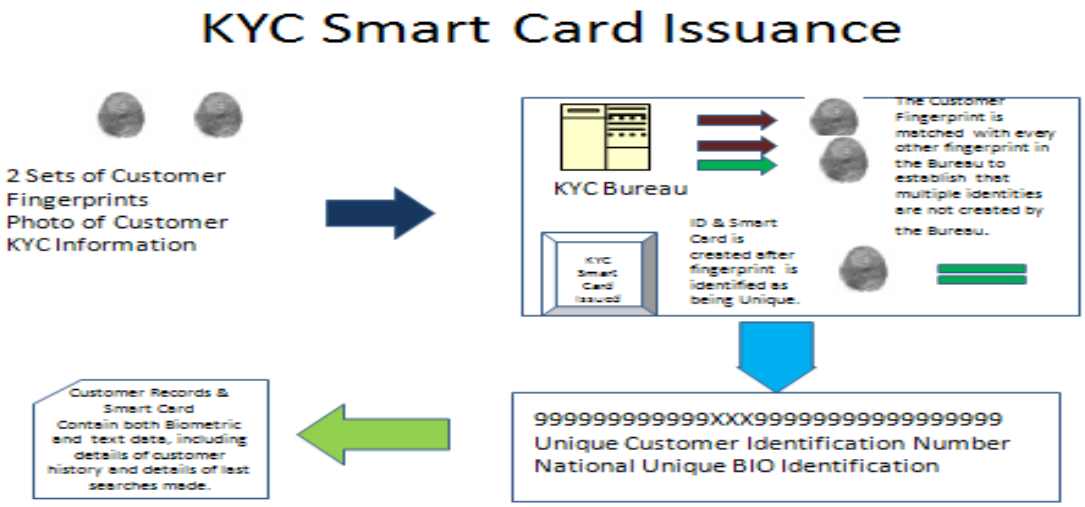


Information Technology in a Centralized National Credit Bureaus

Information Technology will be the key driver for a cost effective, secure and reliable solution for national KYC Bureaus. The Information technology driven solutions will reduce the look-up times, eliminate the need for analysts to manage multiple data sources and will enable smarter risk-rating so that the riskiest customers get the most attention.

Financial institutions of all sizes are seeking these features in their efforts to hold down the resource-consuming processes entailed in KYC - from Customer Identification Programs (CIP) to ongoing Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) which are all required to make KYC effective. Many institutions are still bogged down with manual and error-prone processes, while large firms face inefficiencies caused by the sheer volume of searches required, incompatible software in different lines of business, and redundant or duplicative tasks. Today's Information Technology driven solutions will help in overcoming these hurdles for cost effective, reliable and secure KYC verification. This will translate into saving time and improving risk controls. KYC process driven by Information technology solutions will allow innovation and streamline in regulatory risk to help financial institutions improve productivity and protect hundreds of millions of customer accounts from money laundering, terrorist financing, and other financial crimes

The challenges to complying with KYC are numerous:
Multiple data sources are needed for the solution, including internal and external information that is both structured and unstructured. Both automated and manual methods of collection of information are required.
Potentially complex risk scoring algorithms must be highly customizable
KYC requirements change frequently, due both to internal policy changes and external mandates.
Filing Suspicious Activity Reports (SAR) is one of the most difficult, complex compliance responsibilities financial institutions have. A KYC Bureau will be able to deal with this in a more effective and efficient manner and provide unbiased and independent reports.
A technology solution to these identified problems is a single centralized national system that stores all biometric and associated biographic data that is needed for customer identification. Biometric data and associated biographic data are used by the KYC Bureau to conduct background checks, facilitate smart card production, and accurately identify individuals.
The systems will capture biometric data from individuals to facilitate three key operational functions:Creating a "for life: unique bio-identification number; Conducting fingerprint-based background checks; Verifying an individual's identity; and Producing identity cards/documents.



The centralized national KYC bureau will operate a secure data center which will offer centralized storage and management area for customer information provided by various financial institutions and governmental agencies. The KYC bureau will host customer information including but not limited to customer fingerprints, photos and KYC information. In certain instances data concerning financial institutions and customer lending amounts will also be stored. Information relating to suspicious individuals will be accumulated centrally and then shared across the financial platform as batch info to banks and real-time identification information to Banks and other related lending institutions and credit bureaus.
Information in this system will be safeguarded in accordance with applicable laws and policies, including the information technology Act security policies. All records are will be protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards will include restricting access to only authorized personnel who have a need-to-know, using locks, and password protection features. The system will be protected through a multi-layer security approach.
The protective strategies will be physical, technical, administrative and environmental in nature, which provide access control to sensitive data, physical access control to the storage facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.
The KYC bureaus will possess a comprehensive and complete system, including hardware and software as well as a complete team of system experts to manage and assist in populating the database. A management transactional fee is applicable for every transaction been performed and is negotiable on an end user specific basis as authorized by the Regulator.
KYC Bureaus will also provide the current count of participants in the Indian Financial Markets because of the unique Customer Identification Number as against the multiple counting done today by the industry of the same customer.

KYC Bureaus will be an excellent Repository of Customer and with the right data mining tools it will assist Regulators and Law Enforcers by providing a unified view of various participants in the financial markets.
Sanction and Deployment of the KYC Bureau will have a positive impact on the India's Country Rating by Global Rating Agencies, thus giving the country an opportunity to raise funds at lower costs.
The Biometric identity in the Smart Card will help the financial services business user to quickly verify the customers KYC status and also review the audit log of financial transactions if required.
KYC Bureaus will be cost effective solution for Businesses to Comply with the various Government and Industry Regulatory Requirements..
KYC Bureaus will reduce the risk and opportunities of fraud and money laundering
Improved efficiency and speed of KYC verification will be delivered via automation
Decreased cost of KYC compliance will allow Businesses to focus on their Core Competence.

About the Author: Shri. L S Subramanian is a Senior Business and Technology Professional in the Financial Services Industry and is a Managing Committee Member of ISACA Mumbai chapter and be contacted on his email: subramianls@niseindia.com.

Asia Leadership Awards
L-R: Mr. Robert Stroud-International Vice President-ISACA, Mr. Anand P Shenoy-President-ISACA Mumbai Chapter, Mr. Ravikiran Mankikar-Immediate Past President-ISACA Mumbai Chapter, Mr.Pramod R Nayak- Hon.Secratary-ISACA Mumbai Chapter

Asia CACS-2010 Update

Asia CACS is one of the most prestigious events of ISACA held in this region. The last years conference was held in Kyoto and this year Mumbai had the privilege of hosting the same.
The planning activity begins almost a year back. Kyoto conference had a luke warm response of around 100 participants. The senior management was debating whether to continue or discontinue the same.
The Mumbai chapter was consulted on their views on holding the same. We vehemently argued that ,if at all the same was brought to India it should be an international conference at Indian prices.
Our plea was finally heard and the pricing was very competitive. Finally we got the same after a gap of 10 years, the last Asia CACS was held in Mumbai way back in 2000.
Even though the same was allotted to Mumbai the response in the initial stages was not up to the expectations of ISACA HQ. It is at this juncture the local chapter got into the scene.
It was an all round effort of the entire Management Committee, ably supported by a volunteer group, to make this event a grand success and a memorable one in the days to come.
The Mumbai chapter did a lot of out of the box thinking and convinced ISACA HQ to attempt things which was not attempted before. One such activity was local registration and receiving conference fees in Indian Rupees. We received not less than 50 local registrations out of the total 265 + paid registrations. In fact HQ had to reject request due to the paucity of the space in the Hotel. We surpassed our own record of 2000.Had it not been for the lack of hotel face we were confident of crossing 300+.
The conference was held on 22nd and 23rd February at Hyatt Regency with two tracks on both days and a pre conference workshop on 21st February.
The conference was inaugurated by Mr. Shyamal Ghosh, who was the keynote speaker.
Both days had useful power packed presentations and gave lot of opportunity for networking across the continent.
As usual the Asia Leadership Conference was held on 20th and 21st February ,prior to the Asia CACS .the Asia leadership conference is a very important platform where the ISACA HQ communicates their strategies and vision for the future and the past performance.
The regional awards are also distributed in this event. We also shared our concerns and all the Indian Chapters equivocally stressed the need for a dual pricing mechanism based on the per capita income of the country. The membership director assured us that he would look into the same. On 20th Feb night a dinner was hosted at ITC Grand Maratha for all the Asia Leadership conference delegates.

The next year's Asia CACS will be held in Dubai. We all look forward to this event

ISO NEWS

ISO unveils a new standard ISO 31000:2009 for Risk Management
ISO 31000:2009 provides principles and generic guidelines on risk management.
ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.
ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.
Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.
It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.
ISO 31000:2009 is not intended for the purpose of certification.

Photo Gallery

CISA-CISM Felicitation

Nerul Chapter Meeting

WIM Chapter Meeting

Nerul Chapter Meeting

CISA-CISM Felicitation

ISACA@MUMBAI IS PUBLISHED BY INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION, MUMBAI CHAPTER

C/o Welingkar Institute of Management Development & Research
Room No.317,3rd Flr.,
Lakhamsi Napoo Road,
Opp.Matunga Gymkhana,Matunga C.R.,
Mumbai-400 019

3701,Algonquin Road, Suit 1010
Rolling Meadows, Illinois 6008,USA

Telephone: +91-22-65527187
Website: www.isacamumbai.org
Email: isaca@vsnl.com
isaca@isacamumbai.org