Quality Māntrā

May 2009

A Newsletter of International Certification Services

CODES & STANDARDS,DRAWINGS,

SPECIAL ISSUE ON

KNOWLEDGE

JAS-ANZ

ACC NO S1900799IM
ACC NO E2391101IM
ACC NO H43391105IM
ACC NO O2990704IM
ACC NO S1900799IM(MS)
Www.jas-anz.com.au/register

DATA PROCESSING/STORAGE

NABCB

QM0009
EM0003
www.qci.org/nabcb/index.php

HOSPITALS

ISMS

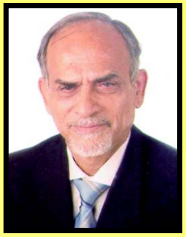
DATA DRIVES

COURTS

BOOKS

LAN,WAN,WI-FI

BANKS,CREDIT CARD



Message From
Sundar Kataria
CMD, ICS Pvt. Ltd.

INFORMATION SECURITY is one of the tenth most threat world is facing today because of availability of modern communication system. The communication system has been developed to enhance the safety, security and wellness of the human and world. The information and data, of any size and type of organization is most vital and critical to have continuity of business and ensure its growth in the development. Today leakage of vital information and data can lead to major problem and loss to the organization. If the vital information and data is misused by the other interested parties like business competitors and business associates.

Information and date are not limited / useful to the organization but to the Anti-social Elements and terrorists, if the information and date are not properly secured and prevented access to other interested parties.

Number of quality tools and management system are available to the present world to have proper and secure Information System. Thanks to IT that provides access to number of software to collect analysis and store the information and necessary data for the improvement of the security, safety and performance of the organization.

Message From
V. Muralidhar
Regional Manager
ICS, Mumbai

ISO 27001:2005 INFORMATION SECURITY MANAGEMENT SYSTEM

What is Information

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation"

What is ISO 27001?

It does not insist that you have a firewall, but it does say:
A.10.4.1 Controls against malicious code: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
It does not say that your system has to be the same as my system. It says:
It s essential that an organizations identifies its security requirements'

Security Breaches

- **60% of all companies have suffered a security breach;**
- **75% regarded the breach as 'serious' and had no contingency plans in place to deal with them;**
- **Over 50% of the breaches were perpetrated by staff;**
- **Management often fail to act when abuse occurs;**
- **Internal audit/management skills not keeping pace with:**

- **Increased dependence on IT**
- **Increased legislation**
- **Increased threats to information**

So please SECURE your Information today.

Message From:-
Sanjay Chauhan
IT Manager
ICS, Mumbai

MANAGEMENT SYSTEM

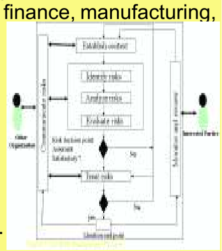
Some would define management as an art, while others would define it as a science. Whether management is an art or a science doesn't matter. Management is a process that is used to accomplish organizational goals; that is, a process that is used to achieve what an organization wants to achieve. An organization could be a business, a school, a city, a group of volunteers, or any governmental entity. Managers are the people to whom this management task is assigned, and it is generally thought that they achieve the desired goals through the key functions of (1) planning, (2) organizing, (3) directing, and (4) controlling. Some would include leading as a managing function, but for the purposes of this discussion, leading is included as a part of directing.

We focus on Information Security Management System(ISMS):-

- A management system describes the people, processes and technologies used to focus and manage the activities of an organization.
- Each organization builds a unique system that is supportive of the goals of that organization.
- Even though each organization builds a unique system, the management systems have several common elements, and are based around an improvement cycle.
- This cycle guides us as we plan the action of what needs to be done and how best to go about it, establish the controls that we need, monitor progression, and improve the system taking preventive and corrective actions and identifying areas for improvement and management review.
- In an ISMS the information protected includes not just that residing in electronic format on computer or network, but includes paper-based information and extends as far as intellectual property.
- A properly implemented ISMS can be effectively used by either small or large organizations and can be tailored to support the protection of information in diverse organizations including data processing centers, software development, e-commerce, health care organizations, finance, manufacturing, service organizations, non governmental organizations, colleges and not-for-profit organizations.

How does an ISMS support Information Security?

- Effective implementation of the framework ensures that a management team, committed to information security, provides appropriate resources to support the processes that the organizations need as to achieve appropriate information security.
- This inevitably includes processes related to the basic management of the system, and training and awareness.
- It emphasizes a risk management process that guides the choice of safeguards and that, coupled with the metrics necessary to ensure that the chosen controls are implemented correctly, ensures that the system evolves to manage the changing business and security environment, and that the resulting management system is, and continues to be effective.



• The key process identified for the effective management of information security is the risk management process, and the key role of this process should not be overlooked.

THE RISK MANAGEMENT PROCESS:

• The Risk Management Process describes the fundamental process. This has been recognized by the expert community ISO/IEC 27005 is planned to present a standardized risk management process.

• Such an approach does not preclude the adoption of the various specialized methods for risk assessment.

THE BENEFITS OF USING AN ISMS :

• By using an ISMS an organization can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs.

• If they draw from a standardized ISMS framework they can be sure that they are drawing from the experience of many others and that the system has been reviewed and reflects best practices.

• Such a framework is a tried and tested tool that helps management ensure that security-resource is spent on the most effective areas for the business.

• Is the money available to spend on information security better spent on a firewall and network security technology, conduct VA/ PT or would investing in training personnel bring more effective results?

The Certification Process, What assurance an organization or third party can draw from it?

• It is worth re-stating that the certification scheme in use does not allow for certification of compliance with the code of practice ISO/ IEC 17799. No formal scheme exists to assess compliance with ISO/IEC ISO/IEC 27002 (17799:2005). What is assessed is that the information security management system meets the requirements of the management system standard (ISO 27001).

• In order to ensure meaningful and repeatable assessments against the standard it is necessary to use an independent and accredited third party known as a "certifying body" or "CB".

• An accreditation body is responsible for ensuring that the certification bodies reach the necessary standards for consistently assessing that an ISMS implementation is meeting the ISO/IEC 27001 standard.

• There are several accreditation bodies what is important is that they must operate under agreement with the International Accreditation Forum (IAF), and use standards such as ISO/IEC 27006, ISO/IEC 17021 and EA7/03 in their accreditation activities.

**Message from :-
P. Subramanian**

A Journey in Business Excellence

"What needs to be improved needs to be Measured"
- Peter Drucker

ISO 27001:2005 ISMS provides us a platform to measure our business functioning as a Service Provider to Industrial clients . We have to break up our performance process & measure the following :-

1. Management Controls :-

□ Business Objectives
□ Management Reviews
□ Security Policy & Procedure
□ IT Policy
□ Business Continuity Plan
□ Security Improvement Plan

2. Business Process :-

□ Human Resource Process
□ SOA selection process
□ Risk Assessment & Risk Treatment

3. Operational Controls :-

□ Operational Procedure
□ Change Control
□ Problem Management
□ Capacity Management
□ Release Management
□ Backup
□ Secure Disposal
□ Data Management

First we confirmed the following :-

a) Relevance of controls through Risk Assessment
b) Define objectives, ensuring they map back to business
c) Use existing indicators SLAs or KPI
d) Identify controls within ISMS audit framework for continuous Monitoring
e) Agreements with third parties through SLA
F) Establish baseline against which future measurements can be Compared**.**

As a service provider , when we embarked on this quality improvement Journey we put an end to the grey area and built few systems so that a structured practice is in the work place. This brought about visibility, transparency, speed and customer confidence in transactions.

Benefits included ease of process monitoring, problem prevention, reduction of incidents, improved staff motivation, tangible evidence to auditors and top management.

The implementation of ISMS and the audit work has strengthened our clients' confidence in Online transactions using our solutions, they are sure that the transactions are secure, encrypted, stores and integrity is guaranteed. This ISO 27001:2005 ISMS certification has improved our clientele and business growth in last fiscal.

You will find we are enthusiastic and passionate about what we do. Security Survey Once optimum levels of protection have been determined, a security survey will reveal areas needing improvement, such as:-

- □ Backup Procedures
- □ Software Application Security
- □ System Architecture including Servers, Workstations, Routers,Firewalls, IDS, Modems, etc.
- □ Patch & Revision Level Control
- □ Laptop & Wireless Devices
- □ Personnel Issues
- □ Employee Training
- □ Physical Security
- □ Access Control
- □ Administrative Procedures - Policies, Management Practices, Configuration Controls

Policy & Procedure Plan Design

Policies are the blueprint for your information security activities. Effective policies must cover all relevant areas without limiting your business activities. They must be carefully tailored to your environment and reinforce, rather than weaken, your corporate culture. They must provide for reasonable expected growth, as well as current concerns. These policies and procedures must be periodically reviewed and updated.

Disaster Recovery Plans

Sixty percent of companies which suffer from natural or man-made disasters do not survive. For this reason, Disaster Recovery Planning which provides for timely restoration of vital business functions must be an integral part of your security program. These plans can take many forms and can be quite simple or very elaborate. We will work with you to design, implement and test plans to meet your business requirements.

Security Awareness Training

Security awareness training is as important as any of your technical safeguards, perhaps more so. Social engineering attacks are common and extremely effective. Your personnel are your first line of defense. They must be fully aware of your policies and procedures, and understand their importance. It is imperative they understand your objectives, enabling them to changing situations. We can provide customized, on-going training programs to prepare your people for the challenges they will face.

Vulnerability Assessment

This involves evaluating your company's information assets, the type and degree of risk to which you are subject, and establishing plans to protect those assets.

System Hardening

System hardening involves selecting and installing the optimum hardware and software products, then configuring them to established benchmarks to minimize the risk of intrusion, data loss or compromise. This sometimes involves evaluation of your software applications for vulnerabilities, as well as examining the systems on which they run . We can work with you to achieve the level of security you require.

Computer Forensics

A forensic examination is quite different than a casual look through a computer. It must be performed in a legally sound manner, so that the evidence will be admissible in court, if necessary. We follow a strict, carefully developed set of procedures addressing security, authenticity and chain-of-custody of the original media. Simply powering up a computer may result in many files being changed, thus endangering admissibility

Compliance

We help you meet the requirements of all the current and future federal and state information security regulations, and any newly proposed legislation which may apply to your business . Our programs include:

- □ Health Insurance Portability and Accountability Act (HIPAA) compliance
- □ Sarbanes-Oxley compliance (SOX)
- □ California SB1386 compliance
- □ Gramm-Leach-Bliley Act (GLB) compliance .

MESSAGE FROM
Manoj Tina
REDIFF BUSINESS SOLUTION

ISSUES IN E-MAIL SECURITY

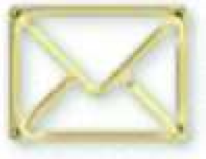
In today's electronic world, email is absolutely critical for any business to be competitive. In most cases it now forms the

Backbone of most organizations' day-to-day activities, and its use will continue to grow.

Thus as e-mailing becomes more & more prevalent in the market, the importance of email security is bound to gain in significance. In particular, the security implications associated with the management of email storage, policy enforcement, auditing, archiving, spam, viruses, support infrastructure, data recovery etc. Managing large, active stores of information takes time and effort in order to avoid failures failures that will impact the users and therefore the business, undoubtedly leading to lost productivity. For secure and effective storage management, organization must take a proactive approach and invest wisely in a comprehensive solution.

When considering a secure email storage management solution, a layered approach, combining both business processes and applications makes sense. By considering the service email provides to the business, email management can be broken down into a number of components: mail flow, storage, and user access both at the server and user levels. Whilst each one of these components should be addressed separately, they must be viewed as part of a total security agenda.

Mail flow covers many aspects of an email system. However, the security of mail flow is for the large part focused around the auditing and tracking of mails into and out of the organizations. Monitoring the content and ensuring that any email that has been sent and received complies with business policy is fundamental. Proving who has sent or received email is a lawful requirement for many industries and email can often be used as evidence in fraud and human resource court cases.



Another key aspect of the management of mail flow security is the protection of the business from malicious or unlawful attacks such as hacking, spam, viruses etc. It is at the gateway into the mail system where a business must protect itself via a variety of methods including hardware and software protection systems, such as spam filters and virus scanners.

Storing of the actual email data includes physical storage, logical storage, archiving systems as well as backup and recovery solutions. The biggest security threat to any email storage system is the potential for mail data to be lost. Most organizations see this threat as existing in the datacentre and spend many lakhs of rupees on securing it. In fact, the threat is most likely to come from lost or stolen hardware, such as laptops containing offline email files. When you consider that the number of employees working remotely is growing, including those who only work away from the office periodically, email security on laptops becomes more significant. Providing a managed method of archiving and controlling this data is therefore essential.

When it comes to archiving, organizations should take a two-pronged approach, to reduce the risk and protect valuable corporate knowledge. Users should be frequently educated about email retention policies. Administrators should be able to control, retain and backup the email files, by consolidating the information stored in email files whilst ensuring that users are prevented from simply creating new emails.

Organizations must plan for the inevitable request to recover data from backups and archives. For the most critical users, such as company executives, many administrators have turned to slow, expensive brick-level backups to provide quick restoration of data to a select few. However, with the onslaught of regulations dictating email retention policies, organizations need to have a comprehensive recovery plan for their entire organization. Faced with this challenge, the traditional method of restoring lorry loads of backup tapes to find all the communications that fit specific criteria is extremely time consuming, and not entirely accurate. An email recovery solution must allow for individual messages and attachments to be quickly restored from regular backups and information stores without setting up a dedicated recovery server.

A large risk to email data within the enterprise is unlawful access to highly sensitive mailbox information. Without a method to both secure and audit this access, there can be no guarantee that data is in fact secured. This can be any link in a lengthy chain, all the way from the administrator resetting, and therefore knowing, the CEO's password through to proving that some other party had access to his/her mail account. Authentication and mailbox data security are both constant battles that need to be monitored closely to ensure that the critical data contained within the email system is available only to those for whom it's intended.

However, creating any such secure email environment is not especially easy for organizations to be setup & managed on their own. Not only are the Costs(Hardware, Software, Manpower etc.) prohibitive but the time that it takes away from their Core Business Functions also has to be taken into account. This is where a proven specialist such as Rediff Business Solutions comes into the equation. Rediff Business Solutions offers Corporate E-Mail Services with premium level of security, no hassles and at a fraction of the spend associated with In-house mail management.

Such a Professional E-Mail setup managed by a specialist helps businesses focus on their productivety & profitability confident in the knowledge that the security of its email system is not being compromised.

We would like to hear from you. Please E-mail us at suggestions@icsasian.com

MESSAGE FROM :- SUSHMA

Information Security (IS) is one of the most crucial tasks facing organizations today. We are in an environment where information assets are threatened from a variety of external sources that simply did not exist a few years ago. Information Security is the way we protect the information entrusted to an organization by shareholders, customers and fellow employees. It is a collective set of policies, standards, processes and procedures that limits or controls access to and use of information to only those that are authorized. It is the protection of all information, regardless of format (electronic, paper-based, etc.), from unauthorized disclosure, use or modification. Organizations need to take every technical precaution to prevent these threats. IS ensures that work environments are adequately protected to prevent unauthorized access to "sensitive" information.Key components of IS management related to data protection are

- Secure E-mail
- Secure File Transfer
- Laptop Encryption
- Portable Media (USB/CD/DVD)
- File Share Encryption

The business workplace can easily be infiltrated. The compromise of information found here could severely impact customers and employees, constitute a breach in laws and regulations and negatively affect the reputation and financial stability of the Corporation. While technology is an effective tool for protecting information electronically, safeguards must also be put into place to accommodate the human factor.

Today, many organizations are moving towards the virtual work spaces for improved efficiency and greater employee flexibility. These alternative work arrangements heighten the need for proper information security precautions. Working on public, shared or home computers can pose additional risks to an organization's information. Every necessary step needs to be taken to ensure that this information remains secure. No matter where you're working – in a conventional office, a shared space, remotely at home or on the road – an employee needs to make sure that the necessary information security precautions are being taken. The organization has to ensure that it selects and implements adequate and proportionate security controls that protect confidentiality, integrity, and availability of its information assets from a wide range of threats (including but not limited to electronic eavesdropping, unauthorized access, data misuse, loss, and theft).

Message From :-
Sanjay K Baral.
Head IT/Information Security Manager.
TechTrek Technologies India Ltd.

Successful Implementation Of an ISMS

One of the major factors for a successful implementation of an ISMS is to know why you need it. The worst thing that can happen to you is that midway through the implementation you notice that an ISMS according to ISO 27001 is not what you wanted or you have failed to choose the appropriate controls for your organization which is too expensive or requires too many resources to operate.

First of all, try to reflect about why you need an ISMS at all. Depending on what role you occupy within your company, the reasons might be quite different. If you're responsible for (information/data) security, you might have been told to do so. Or you might want an ISMS on your own account in order to adequately protect the information you are responsible for. If the latter is the case, you must need the *top management support*. This is one of the most important factors for successful ISMS.

An important aspect of ISO 27001 (ref BS 7799□2:2002) is that of the Plan -Do -Check -Act (PDCA) model, which must be applied to the ISMS.

In the planning phase, the top management provides the overall guidance and direction by defining the *scope and boundaries of ISMS* and the *ISMS policy* in terms of the characteristics of the business, its location, assets and technology. Organization must identify the assets and their risks like threats, vulnerabilities, and impacts (i.e. loss of confidentiality, integrity and availability) by using *Risk assessment*. Selection of control is also very important, while ISO 27001 expects you to meet every requirement, it does allow you to exclude control objectives and controls if you can justify doing so.

Then comes Implement and operate ISMS phase. In this phase the organization implements controls selected during planning stage to meet the control objectives. Define the measure the effectiveness of the selected controls. Implement training and awareness programs and manage overall operation and resources for the ISMS. In Monitor and review phase, security process performance is measured against the ISMS policy and objectives. Security metrics are defined to measure the effectiveness of the implemented controls. The effectiveness of ISMS is then reviewed by the top management, taking into account the results of security audits, results from effectiveness measurements. Corrective and preventive action is then taken based on the findings in the check phase. Corrective action corresponds to those actions that are taken to eliminate the cause of the non-conformities, whereas, preventive action corresponds to the actions that are taken to eliminate the cause of potential non-conformities. Organizations can get certified as compliant with ISO/IEC 27001:2005 through any of the certification bodies.

Ten Top tips to keep your business critical information secure

1. Use strong passwords
2. Don't share passwords
3. Keep password protected documents secure
4. Be careful with memory sticks
5. Store electronic documents securely
6. Lock your screen
7. Lock your laptop
8. Actively support physical Security measures
9. Check email addressees
10. Careless talk

CORPORATE JOKES

Babies delivery at Corporate World

1) Project Manager is a person who thinks Nine women can deliver a baby in one month

2) Developer is a person who thinks it will take

18 months to deliver a baby.

3) Onsite Coordinator is one who thinks single woman can deliver nine babies in one month.

4) Client is the one who doesn't know why he wants a baby.

5) Marketing Manager is a person who thinks he can deliver a baby even if no man and woman are available.

6) Resource Optimization Team thinks they don't need a man or woman; They'll produce a child with zero resources.

7) Documentation Team thinks they don't care whether the child is delivered, they'll just document 9 months.

8) Quality Auditor is the person who is never happy with the PROCESS to produce a baby.

And lastly...

9) Tester is a person who always tells his wife that this is not the right baby.

ICS Welcome the below members in the ICS Family

Name of Employee	Designation	Station
Ravindra Kumar	Inspector	Delhi
Bipin Bagi	Dy. Manager	Belgaum
Kushal Mitra	Inspector	Kolkata
Kiran Patil	Inspector	Mumbai TPI
Jayeshkumar Rakholiya	Inspector	Surat
Sachin Tambat	Inspector	Mumbai TPI
Dhiraj Parmar	Inspector	Surat
B. Saravanan	Station Manager	Chennai
Chirag Prajapati	Inspector	Surat
Anees Shaikh Nazir	Jr. Office Executive	Mumbai TPI
Sunil Patel	Inspector	Surat
Dixon Davis	Inspector	Mumbai TPI
Waquar Anjum	Inspector	Delhi
Somil Keskar	Marketing Executive	Indore
Dilyog Sahotra	Inspector	Ludhiana
Rakesh Tiwari	Inspector	Ludhiana
Chandrakant Tambe	Inspector	Pune
Vinay N.	Inspector	Bangalore
Praveen Kumar	Inspector	Bangalore

ICS wishes the below a very Happy Birthday

Name of Employee	Date of Birth	Station
Shivanand Heggeri	01-May-79	Belgaum
Anil Kumar	03-May-83	Delhi
Vilas Patere	04-May-69	Mumbai Admin
Chand Kumar	16-May-85	Delhi
Aanchal Chhabria	19-May-74	Mumbai Admin
Sangeeta Chauhan	20-May-84	Mumbai TPI
Subhransu Nathsharma	20-May-84	Mumbai TPI
Sheetal Kataria	23-May-79	Mumbai CO
Vikram Jangam	23-May-79	Mumbai TPI
Som Bahadur	25-May-77	Mumbai Fin
Prakash Agari	25-May-86	Mumbai Admin
K. K. Pramod	27-May-69	Mumbai TPI
K. Ananda Kumar	28-May-76	Chennai
A. Rajamani	30-May-70	Chennai
Abhijit Patil	31-May-82	Mumbai FSMS

Horoscope For the Month Of May 2009

Based on Moon Sign

Aries : . The main or predominant trend is power position, pelf. That means you will be striving Hard and long for success and straining every sinew and muscle.. You should be careful of your health. There is a possibility of deception and theft, therefore be careful and verify matters before taking final decision, especially in financial and/or property matters.Your tremendous drive and determination with see you though.

Taurus: Power and project is the name of the game. 2008 should be taken in a spirit of enterprise and adventure for a maximum mileage. Your creativity will be at an all-time high. Sorrows and disappointments in matters of the heart *may* (not will) be possible. That's Real life.

Gemini: Good money will come your way in one way or the other. Domestic disturbances the health of parents and in-laws could cause concern/anxiety. Anything to do with house, home, office, shop, godown, land, building, constuction, buying and selling shopping and spending with be strong emphasised As a role model, I have cited Gemini L.N. Mittal, the world's second richest man! He is great and very sure of himself. The key for Geminis, very specially, is CONFIDENCE.

Cancer: A thwacking good year for cancerians. Marriage, journeys, fame, love, communications, the birth of children, a house or office move, and above all, the resolution of problems and posers. You have EARNED your place in the sun!

Leo: Money is the master key, thanks to URANUS, Hard work and gains are the legancey of Jupiter. Saturn advises caution in food and family matters. Ganesha says, the bonus will be spirituality and a higher level of consciousness, as Jupiter and Saturn are in fine positioning by Western astrology. 2008 is a milestone in your life that's for sure. It will help you to live life fully.

Virgo: Top drawer creativity, clear and powerful expression children, games of chance love hobbies make sure pleasure and profit. But you do need to take care of your health (a few of you are hypochondriacs, as are a few Scorpios) pray to Hanuman / Allah / Zoroaster / Jesus and burnish/ polish your image and be POSITIVE. Attitude helps. Belive me, you will fan out to people and places and be a WINNER!

Libra: Windows of opportunity, as the Americans says, open out for you on the home and domestic frontierS. Here's your chance, a RARE one, for PEACE and HARMONY, despite expences and worries. That's the beauty of life itself. Saturn will trouble you, but also help you in tradition, the welfare of others, Philanthropy, true spirituality and liberation from material bondage. You see, Saturn and Jupiter, the two stalwarts are in TRINE or Lucky Formation. 3 cheers!

Scorpio: This says Ganesha, could be a fine a year, for the both honey (love) and adventure. I include all types of intellectual, physical, mental pursuit and ventures. Clearly, a year to reach out to people and places. This is, believe me, a very apt cliché and even an irreplaceable one.

Sagittarius: it is all about MONEY and Honey! If power goes to your head, you will have a big fall. Health of family members, friends, well-wishers, will cause pain and tension. Charity is strongly suggested. Property matters are favoured.

Capricorn: The tallest tree in the world was 450 feet. You can compare yourself to the tallest tree in terms of stature, class, power! You can be all that you want to be, as the as the Americans say. You, Capricornians, have both will-power and executive ability. This is your year to utilize your considerable abilities for optimum results. Success and fame will RIDE with you! Be practical, but also be philanthropics. That would be ideal, says Ganesha!

Aquarius: Ganesha Confirms that 2009 is a mystical year. Planning ahead is good, but looking for Diving guidance is better. Sudden ups-and-downs are almost certain. Life could be a see-saw but you will enjoy the 'high' phases, and come terms with yourself. Ganesha claims that you will have much to do also with charities, ESP manifestation, strange lands and distant places, behind-the-scene activities (definitely so, is my finding), visits to hospitals and clinics most probably to nurse and help others. (Again, this, I can say, is true from personal experience.) The pleasures of the bed right sleeping like a curled up cosy cat, to violent and passionate sex, dreams and visions, telepathy and clairvoyance are also include under the umbrella (just like the nuclear umbrella) of this forecast.

Pisces : Friends, profit and promotion, children, hobbies, wish-fulfilment, socialising and all group activities (this very definitely) are a few of the goodies in store for you. But separations and law cases and parting of the ways for various reasons is also foretold. Ganesha says, that's life, "C' est la vie" as the French have it.

Quality Māntrā

May 2009

A Newsletter of International Certification Services

ICS gets Accredited for
ISO 27001:2005
Information Security
Management System
by JAS-ANZ

ICS ACHIEVMENTS

Yet Another Milestone Achieved

➧ ICS gets Accredited for ISO 27001:2005 by JAS-ANZ.

➧ International Certification Services is please to enhance launching of their ISO 27001:2005, Information Security Management System (ISMS) Accredited through the Joint Accreditation System of Australia And New Zealand, Australia. The ISMS, ISO 27001:2005 system is beyond quality tool like CMM and most beneficial to enhance the products and service performance and quality.

➧ ICS enters into Association with Rediff Business Solution For :

- Domain Registration / Mailing Solution
- Web Hosting

ICS Ventures New Avenues:-

NEW

● Software Services :

✐ Software Development

- *Application Software*
- *Client-Server Application*

✐ Web Based Solution

- *Static Websites*
- *Website Redesign and Migration Services*
- *Data Driven Web Application (Dynamic Websites)*

● Hardware Solution :

✐ *Sales & Services*

✐ *AMC*

✐ *Sales all kind of Computer Hardware & Peripherals*

Please send us your valuable comments & suggestions *on* " suggestions@icsasian.com*". To* subscrite *for* a free subscib*tion send us a mail with sub*ject *"* subscribe for "QUALITY MANTRA"" at suggestions@icsasian.com

**This Edition Compiled and Presented by IT Department ,
Sanjay Chauhan (IT Manager) , Vikas Sharma , Deepesh Aagri .**

International Certification Services Pvt. Ltd.

Corporate Office

22/23 Goodwill Premises, Swastik Estate, 178 CST Road, Kalina, Santacruz (E),
Mumbai- 400 098. Maharashtra, INDIA.
Tel : 022-26507777-82, 42200900, 30608900- 4, **Fax :** extn. 933, **Email :** info@icspl.org

Branch Offices

Ahmedabad 079 -26858687   Bangalore 080- 22384620   Baroda 0265-3202067   Belguam 09341370107
Chennai 044- 24719070 Goa 09322382887 Delhi 011- 22042107 Hyderabad 040-23713335 Indore 0731-4076365
Jaipur 0141-2610291   Kanpur 0512-2262648   Kolhapur 09373107108 Kolkata 033- 32542986
Ludhiana 0161- 3230461   Mumbai 022-26507777   Nagpur 09326175990   Nashik 0253- 3205994
Pune 020 25424204 Surat 09374658605 Shimla 09318671776 Udaipur 09314116813   Vapi 0260-3291135

Overseas Offices

Dubai +9714-3933343 / Nepal +9771-4258455 / Muscat +968-24499785 / Turkey +90-312-4471428
Doha +974-4670022 / Sri Lanka +94-112-433406 / Ukraine +380-633363468 / Romania +40-21-6652608
China +86-755-83038357 / USA +1-919-342-5772

Disclaimer
The article and information given by the authors / companies and ICS are based on their information and views; International Certification Services shall not be held responsible for the correctness of the data and information.

For Internal Circulation Only