Quality Māntrā

May, 2021

A Newsletter of International Certification Services

INFORMATION TECHNOLOGY

Quality Māntrā May, 2021
A Newsletter of International Certification Services

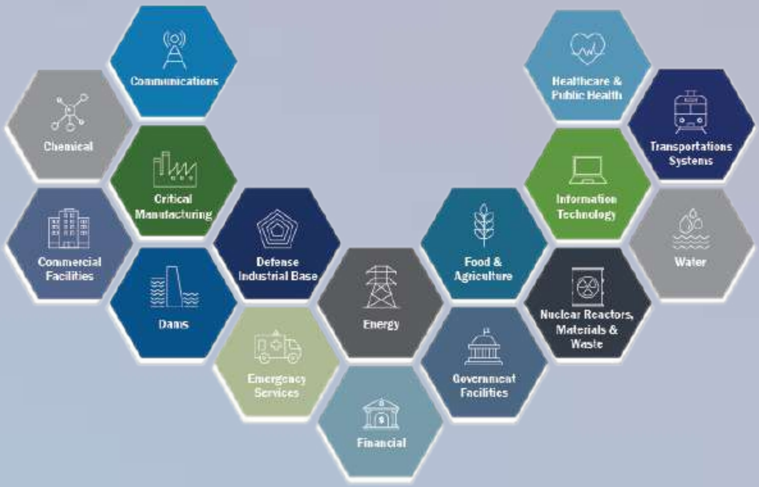
Information & Data Security, Cyber Security In Critical Infrastructure

(By Dr. Sundar Kataria, Chairman & Managing Director, International Certification Services)

Today we are living in Digital World where in from smallest organization to large corporate house it has become essential to have Robust Information Security System in place.

Did you know that there are 16 sectors identified for critical infrastructure cyber security?

1)The Energy Services
2) The dams
3) The Financial Services
4) The Nuclear Reactors, Materials and Waste
5)The Food and Agriculture
6) The Water and Waste Water System
7) The Health Care and Public Health
8) The Emergency Services
9) The Transportation
10) The Chemical
11) The Communications
12) The Information Technology
13) The Defense Industrial Base
14) The Critical Manufacturing
15) The Government Facilities
16) The Commercial Facilities



Does our IT Security Team secure our drive where our critical data & information is stored ? Who has access to it ? The key activities and steps in protecting secretive data includes automating visibility control of access policies and ongoing controls, monitoring to discover vulnerabilities and risk before they are compromised and get breached.

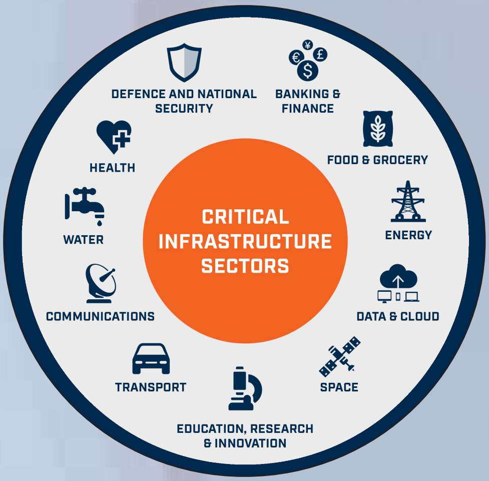
What are the information and data in various departments across the organization? The information related to customers, marketing, pricing policy, sales, complaints, legal and regulatory compliance, suppliers, vendors and contractors for purchase department, design and development, research and innovation, special processes and quality assurance / quality control and deliveries etc. Personal information, personnel data, production, performance, payments, intellectual properties and marketing intelligence, finance and internal and external issues, etc. are available on computers and servers including ipads, and mobile due to increase of the use of mobile apps.

Addressing the increasing number of legal regulations related to IT and privacy policy is it becoming difficult to keeping pace with reporting.

The smarter and adaptive approach is necessary to protect critical data bases, folders and more with IT platform security. A professional approach required to conduct comprehensive risk to know vulnerability. Get contractual insight and analyst and take immediate correction and corrective action to monitor, protect and mitigate action to prevent IT security failures.

We need to transform our information & data security and cyber security using available data security technologies and expertise. Furthermore we need to adhere with national / international legal and regulatory requirements towards IT Security and privacy policy that will help and enhance trust within the organization as well as stakeholders, thus standing out from the competition and business associates.

It is very vital to have latest enterprise solutions, data security strategy and program and critical hard wares in house and cloud storage strategy. We need to exercise full control of the organization's sensitive data which is accessed / stored and transmitted by other parties using various technologies and expertise from the IT Consultants.


CRITICAL INFRASTRUCTURE SECTORS
DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
HEALTH
FOOD & GROCERY
WATER
ENERGY
COMMUNICATIONS
DATA & CLOUD
TRANSPORT
SPACE
EDUCATION, RESEARCH & INNOVATION

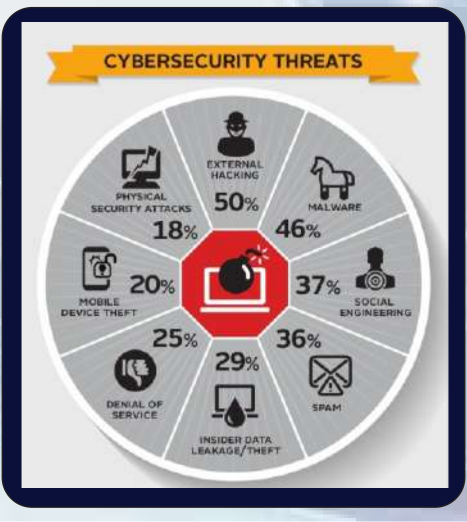
Our Nation depends on the resilience of implementing critical infrastructure cyber security. Evolving threats will continue to inspire a collective effort among both private and public-sector partners. User awareness and training is the cornerstone critical infrastructure cyber security. Users must learn about the security best practices to ensure the resiliency of our critical infrastructure in the future

Cyber Security Threats

(By Sumeet Kataria, Country Manager, International Certification Services)

The realm of technology is ever changing and the new technology advances have transformed the way people communicate. Technology has allowed people to keep in touch no matter the distance. One is able to communicate 24 hours around the clock. New Era of Information & Technology has changed everything in the modern society.. The internet data has completely replaced traditional paper base means of communication and information and data storage system. The electronic media of the computer networks in which online communication takes place and where individual can interact, exchange ideas, share information, provide social support, business, direct actions, create artistic media, play games, engage in social and political discussions, etc is a new way of communication.

The increase in use of internet and digital media has improved the communication and the way we communicate has been revolutionized by the advancement of new innovation in the telecommunication sector.But also there are piles of issues associated with using free WiFi, whether at an internet cafe or elsewhere. Thus the cyber risk and hazards have increased in many folds. This has been realized by the world and cyber security has been focus to prevent cyber crimes.



Cyber Security threats and crimes can be broadly classified as

1.Cyber Security & control crime against individual.
2.Cyber security & control crime against property
3.Cyber security & control crime against organization / government

The Information Security Management System provides you with effective and efficient management system. An international management system based on ISO 27001 given below is the brief description of the category of the cyber security risk, threats and crimes. It may be against person, property , organization, government, society and country at large.

1. Individual Cyber Security

A) Cyber Security Individual

This includes e-mail and internet frauds where personal information is stolen and used.Theft of financial or card payment data, spam mails or other forms of communication, are sent on masses with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for.

Harassment through letters, e-mail and multimedia messages are also the major issues. They could be boyfriend , ex- husband may emotionally black mailing and threatening them. Presently harassment is done through social media sites like Facebook, Orkut, Instagram, Twitter, Whats app,etc has been increasing day by day.

B) Cyber Stalking

Cyber Stalking may involve person's movement across the internet by posting messages including threatening notes using the chat room bombarding person with e-mails, etc

C) Dissemination of Obscene Materials / Indecent Exposure / Pornography

Miscreant may host / post on website containing prohibited material, pornography materials and obscene material ,etc. These obscene material may cause harm to the mind of adolescent to deprive and corrupt their mind.

D) Defamation

Virtual medium may be used to defame the person / persons in the society to cause him to be shunned or avoided or to expose him to hatred, contempt and / or ridicule

E) Hacking or Unauthorized Control

Computer hacking is common these days in friends and family circle to steal the information which is unauthorized without the knowledge of the person.

F) Email Spoofing

Email Spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust.

G)Fraud & Cheating

Online fraud and cheating has increased in many folds as it is most lucrative business specially credit / debit bank cards, documents and offering jobs.

2. Property Cyber Security

A)Intellectual property contribution of Pirated Software

Intellectual Property may include pirated software , infringement of copyright, trademark, patent, design and drawing , book mark / logo, service marks and computer service code,etc

B)Cyber Vandalism

Destroying and damaging property of another person / organization through physical harm done to the computer or computer system . This may include theft of a computer or some part like peripheral / hard drive and memory chips and RAMs.

C)Virus Transmitter

Spreading of virus or worm through the internet that attach to other file / other computer and circulate it themselves in other file / other computer or a network. The virus may attack and corrupt data on a computer either by altering or deleting it.

D)Cyber Squatting

The another person may claim for the same domain name either by closing that they have first registered and have right to use it before the other holder (original domain name holder).

E)Online Gambling

Online fraud and cheating has increased as its the most lucrative business . This may be related to credit / debit cards , contractual jobs ,etc.

F) ATM Frauds

False ATM Cards being clowned by criminals to withdraw money from the victim's bank account and this can cause monetary loss to the victims.

G)Financial Frauds

There is a rapid growth in the users of networking sites where culprits attack by sending bogus mails or messages through internet and password / OTP using bank credit cards.

F) Forgery

Deceiving large number of persons by sending threatening mails as online business transactions are increasing have become today's life cycle.

3.Organization / Government Cyber Security

A)Government Organizations - Terrorism

Cyber Terrorism has increased globally which has a national as well as international consequences. The common terrorism attacks on Internet is by distribution of denial of service attacks, hate websites, hate emails , attacks on sensitive Domestic / National computer networks, etc. Cyber security is to control pre mediated and disruptive activities conveying social, ideological,religious, political or for specific objectives like separatism , violation and disruption of services.

B) Trafficking

Trafficking of drugs, human beings , arms and weapons is another means of cyber security threat.

C) Cyber Security Warfare

Cyber warfare involves the actions by a nation-state or international organisation to attack and attempt to damage another nation's computers or information network through, for example, computer viruses or denial of service attacks .

ISMS Is a System of Managing Data Security

(By Ganesh Deherkar, Dy Manager- Marketing, International Certification Services)

The term "information" includes not just words, numbers and images, it also includes all kinds of ideas, concepts, and knowledge.

Imagine for a moment that you have a specific mobile phone that you use for work. On it, you've stored credit card information to help you pay for things, banking information so you can review your finances, the important details of the clients that you work for, login information for the services that you subscribe to, and lots of proprietary data pertaining to the innermost workings of your business.

If, like most people, you bring your cell phone everywhere with you, there's a chance it might be lost or stolen at some point. If that situation occurs, what happens to the information stored on the device? How do you protect your own privacy and information security? What about securing the information of your clients?

The answer to all of these questions is to establish an Information Security Management System (ISMS)—a set of policies, procedures, and protocols designed to secure sensitive information at your business and prevent it from either being destroyed or falling into the wrong hands.

What Is an ISMS?

An ISMS is a set of controls that an organization implements to protect its own informational assets and other information assets for which it is responsible. Organizations that design and implement their own ISMS will find ways to reduce the likelihood of a data breach occurring, ways to limit their liability when a data breach does occur, and other ways to mitigate the impact of any data security issues. Here are some of the key elements that make up an effective ISMS:

An established ISMS governs the policies, procedures, processes, and workflows that are chosen to help protect an organization's data security. Once the policies have been set by the organization, they must be implemented and operated throughout the organization to realize their benefits. The organization governs the policies with the PDCA (Plan, Do, Check, Act) cycle, regularly revisiting the procedures and adjusting them as needed.

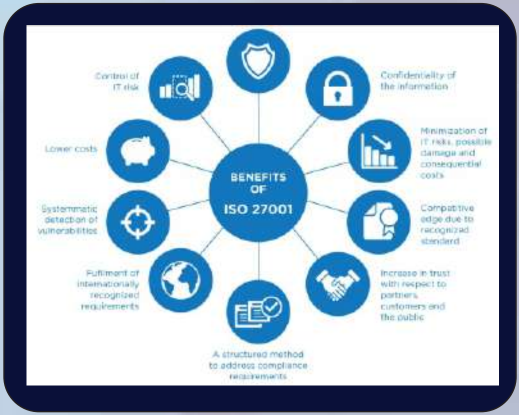
Not All Data Are Treated Equally by the ISMS

The ISMS describes how data should be protected by the organization, but it does not have to treat all organizational data the exact same way. Organizations create, record, and exchange many different types of data each day. We mentioned a few types above—financial records for the company, login details and information for services that the organization uses, client and customer profiles and information, and corporate credit cards and banking details. There are also emails, reports, inventory data, facilities data, service records for equipment, etc.

Not all organizational data has to be under the same level of security, and there are financial and productivity costs associated with protecting certain types of data. For example, if the organization requires two-factor authentication for email logins, an employee might lose an extra two minutes of productivity each time they check their email. Is it worth it? That's up to organization leaders to decide through their own risk assessments.

Quality Māntrā May, 2021

A Newsletter of International Certification Services

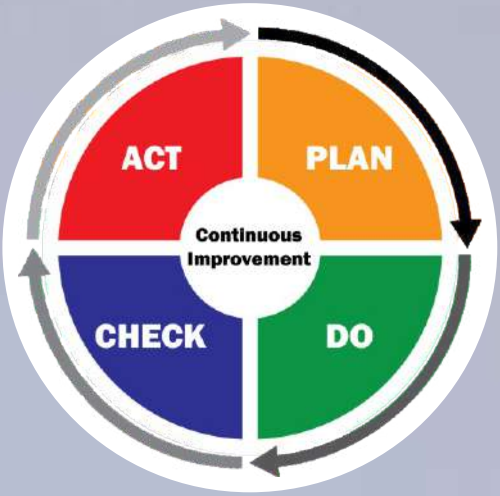

BENEFITS OF ISO 27001
Control of IT risk
Confidentiality of the information
Lower costs
Minimization of IT risks, possible damage and consequential costs
Systemmatic detection of vulnerabilities
Compatitive edge due to recognized standard
Fulfilment of internationally recognized requirements
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements

Compliance with ISMS Is Crucial for Successful Implementation

Creating an ISMS and storing it in a folder somewhere ultimately does nothing to improve information security at your organization—it is the effective implementation of the policies and the integration of information security into your organizational culture that protects you from data breaches. While the establishment and maintenance of the ISMS is an important first step, training employees on the ISMS and building compliance into daily processes and activities at your organization is a priority if you wish to adequately secure your data.

An ISMS Is Dynamic, Not Static

The ISMS is a living system that is constantly changing—it is dynamic, not static. In ISO 27001, an information security standard, the PDCA cycle is applied to ISMS systems. Companies should establish the ISMS (plan), implement and operate the ISMS (do), monitor and review the ISMS (check), and maintain and improve the ISMS (act). The ISMS should be reviewed and updated regularly to reflect a changing information security environment and new best practices for data security.



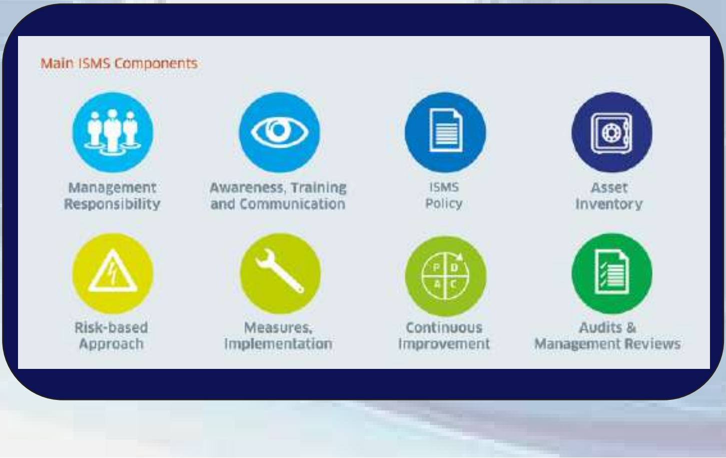
An Effective ISMS Is Risk-based

It is important to understand that protecting your organizational data from security breaches in an absolute sense is probably impossible. A thief or a hacker with enough time and resources will most likely eventually find a way to penetrate the security measures that you implement. A cyber attack against an unsophisticated security system might take a single person just a few hours to complete, while a heavily secured server might take weeks to access for a team of trained security experts.

Organizations must perform a risk assessment that determines which assets need to be most heavily protected, and effectively allocate resources towards the protection of those assets. A risk-based ISMS accounts for the relative risk of different types of informational assets when allocating resources towards asset

ISMS Helps You Manage Data Security at Scale

Returning to our original example of a business cell phone that could be lost or stolen, it would be relatively easy to protect a single device from falling into the wrong hands, but what happens when your organization has 100 employees with 85 desktop computers, 20 laptop computers, 40 mobile phones, a server room, and a cloud-based repository for all of your crucial documents? At this point, you need to manage information security at scale because there is a high volume of data and a big network. A single device with an improperly configured, out-of-date anti-virus program could become a vulnerability that compromises the network. An ISMS provides controls that help secure each endpoint against malicious attacks, protecting the system as a whole.



Cyber Security In Day to Day Life

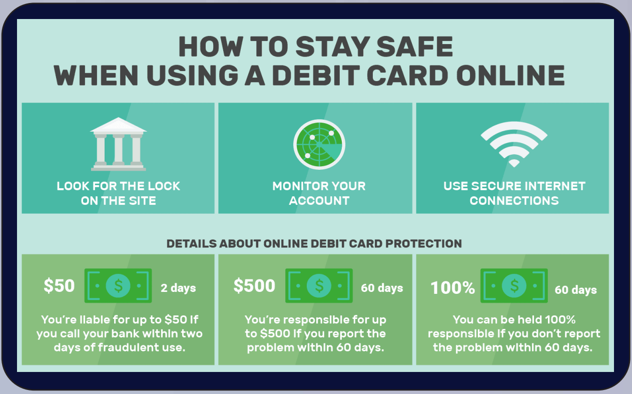
(By Nagaraju Etikala, Station Manager-Hyderabad)

The Internet is today's backbone for all kind of online services, and it has given rise to various features such as: Social Media, Online Shopping, Digital Payments, e-Education, e-Health etc.

Cyber Security is now a part of every individual's life. The more connected we get, safeguarding our digital identities becomes a shared responsibility. The more we share, the more we must care.

Online shopping

Online Don't Shop at Public Hotspots. Online shopping is convenient, but you shouldn't make it too convenient for someone to hack your account while you're shopping. So, avoid making online purchases when you are in a public place (coffee shop, restaurant, shopping mall) and using their free wireless Internet ("hotspot" or Wi-Fi)



HOW TO STAY SAFE
WHEN USING A DEBIT CARD ONLINE

LOOK FOR THE LOCK ON THE SITE
MONITOR YOUR ACCOUNT
USE SECURE INTERNET CONNECTIONS
DETAILS ABOUT ONLINE DEBIT CARD PROTECTION
$50
2 days
$500
60 days
100%
60 days

You're liable for up to $50 if you call your bank within two days of fraudulent use.

You're responsible for up to $500 if you report the problem within 60 days.

You can be held 100% responsible if you don't report the problem within 60 days.

Use Reputable and Secure Websites: Before you type your card details into a website, ensure 1) the website is trustworthy and 2) that the site is secure. When it comes to a site's security, look out for a small padlock symbol in the address bar (or elsewhere in your browser window) and a web address beginning with "https://" (the "s" stands for secure).

Use Strong Passwords: Most sites will have set up an account before you're able to make a purchase. This is a good idea, since it means you'll have a user name and a password and an account that is set up for you and only you. You will want to use a strong password, one that isn't easy for anyone to figure out and that you don't use for other online shopping sites

Websites, valid and trustworthy ones, may have one more layer of security for online credit and debit card purchases, to protect you. You might be asked for another password or piece of information. The Visa Card's "Verified by Visa" and MasterCard's "SecureCode" are examples of this.

Just about anytime you use a credit card, you will be asked for the 3- or 4- digit number that is on the back of your card. It's called your card's "security number" or more accurately, the "CVV2" code. CVV2 stands for "Card Verification Value 2," It is an important security feature for major credit cards and credit card transactions made on the Internet and over the phone. The code is located on the back of your card on or above your signature line.

Social Media:

Every person likes to be social and interactive in the world. In a web-based society, it is quite easy these days to engage. It is not tough to communicate with other people with the intervention of social media.

1) Use a strong password. The longer it is, the more secure it will be.
2) Use a different password for each of your social media accounts.
3) Set up your security answers. This option is available for most social media sites.
4) If you have social media apps on your phone, be sure to password protect your device.
5) Be selective with friend requests. If you don't know the person, don't accept their request. It could be a fake account.
6) Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not sound like something your friend would post.

7) Be careful about what you share. Don't reveal sensitive personal information ie: home address, financial information, phone number. The more you post the easier it is to have your identity stolen.
8) Become familiar with the privacy policies of the social media channels you use and customize your privacy settings to control who sees what.
9) Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system, and software are kept up to date.
10) Remember to log off when you're done.
11) more we must care.

Safer Tips – Digital Payments

1) Use a prepaid debit card for all your online transactions
2)Use a reputable and trusted digital payment provider
4)Beware of fraudulent apps.
6) Protect your phone with a screen-lock mechanism and use strong password protection for your phone and apps
7) Ensure the online Merchant is compliant
8) Sign up for payment transaction alert messages
9) Ask for a One Time Password (OTP) feature for any of your digital payment methods
10) Don't carry out digital/mobile banking using your app via a public Wi-Fi:
11) Don't click on links sent via SMS, emails, WhatsApp or other social networking sites claiming to be from your bank or financial institutions
12) Do not disclose information such as your digital wallet PIN, card or card's CVV number, mobile money PIN, Sim card PIN

e-Education

Online degrees are accepted by many companies and employers in India as long as it is accredited and approved by Distance Education Council (DEC) of India. Many of them are encouraging their employees for getting online education as well

1) Use a device that is secure, ensure that the gadget or device being used is optimized to load the current software that is not 'End of Life'. An upgrade to hardware to cater for the utility software should be made. Obsolescent hardware should be done away with.
2) Avoid use of those gadgets and devices that are used by elders or parents for secure transactions or work, for the purpose of online education of children.
3) Install a legitimate software, that is still supported by the OEM, or use those that has shelf-life remaining. 3) Install security software like anti-virus or firewall, etc
4) Use an account that is other than admin account while going online.
5) Remember to login to an online service with complete security turned on. Subsequently, on establishment of trust, the features can be allowed or disallowed on review.
6) Always start a session on the learning portal or application with the camera and microphone turned OFF. (subsequently the facility can be turned ON as per requirement)
7) Use passwords and multi-factor authentication

8) Update the operating system at the earliest.
9) Use a browser that is secure and access the same with all the privacy and security settings turned ON.
10) Update all software including applications that are being used while being online or those installed on the computer/ device.
11) Always install any required application downloaded from legitimate store or from authentic sites.
12) Verify all links received on email or from social media, before clicking on them.
13) Do not share sensitive information and those that are confidential unless the domain is trusted.
14) Ensure that the site and the browser is secure prior to passing sensitive information. Check for “https” protocols while performing financial transactions or while using login credentials.
15) Sharing of files on cloud services should be based on limited access or it should be done to those on locked Ids
16) Never open multiple tabs and also avoid concurrent opening of secure websites or pages related to finances, while on online mode of learning schemes.
17) Remember to logout any online classroom or application after you have finished with your online learning portal.
18) Avoid accessing emails or confidential websites when on online e-Learning mode/activity.
19) Always use a secure connection and a trusted broadband/WiFi connection. Avoid using public WiFi.

e_Health

eHealth is a broad term, and refers to the use of information and communications technologies in healthcare. eHealth covers a lot of territory, which is why digital health industry experts often contest exactly what the term means – and to add to the confusion, it's also frequently used as a synonym for Health IT.

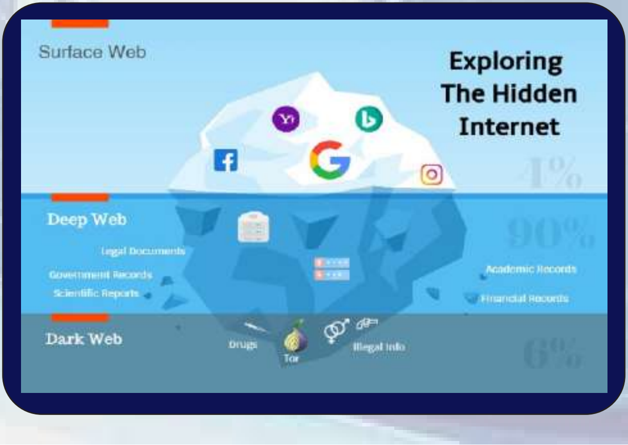
1) Perform Risk Assessments Regularly. Don't underestimate the value in performing routine Risk Assessments.
2) Perform Vulnerability Scans & Penetration Tests.
3) Utilize Encryption. 4)Perform Updates & Patch Your Systems. 5)Check Your Audit Logs.

Types Of Web Servers

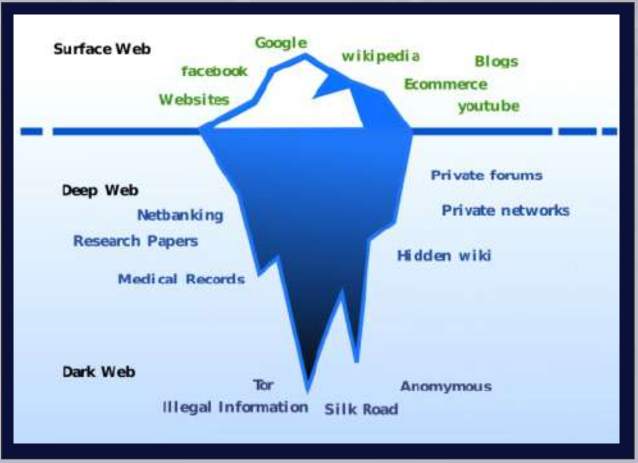
(By Murlidhar Vaity, Vice President (Business Continuity), International Certification Services.)

The Surface Web is what users access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft’s Internet Explorer or Edge, and Google Chrome.The section of the internet that is being indexed by search engines is known as the “Surface Web” or “Visible Web”.

Deep web is part of the World Wide Web whose contents are not indexed by standard web search engines for any reason. Some pages are part of the Deep Web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, so they are not indexed by search engines, while others explicitly block search engines from identifying them. The content of the deep web is hidden behind HTTP forms, and includes many common uses such as web mail, online banking, and services that users must pay for, and which is protected by a pay wall, such as video on demand, some online magazines and newspapers, and many more. Content of the deep web can be located and accessed by a direct URL or IP address, and may require password or other security access past the public website page.



Dark Web is defined as a layer of information and pages that you can only get access to through so-called "overlay networks", which run on top of the normal internet and obscure access. You need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously. The technology to create the Dark Web was initially created (and still funded) by US Military Researchers in the mid-1990s to allow spies and intelligence agencies to anonymously send and receive messages. Named "The Onion Router", it was quickly coined with the shorter "Tor" with its name coming from application layer encryption within a communication protocol stack; many layers representing the layers of an onion.



JOKES

"Agar 2-3 Din Baad Hi Reply Karna Ho Toh **"Kabutaar"** Hi Rakh Lo, **Whatsapp aur Facebook** Kyun Use Karte Ho?"

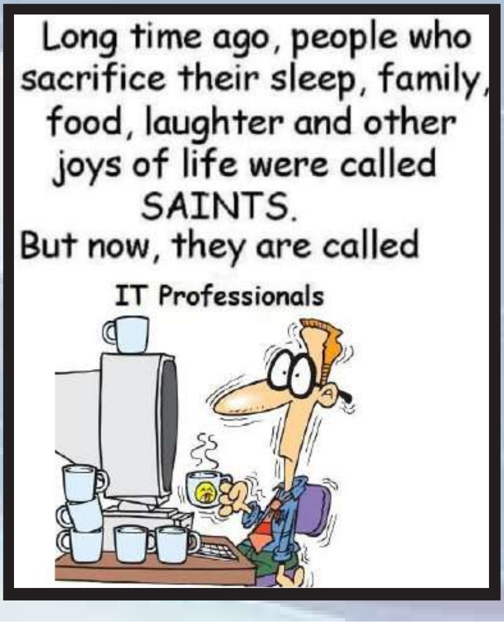
A Software engineer was smoking.
A lady nearby told him
can't you see the WARNING!
Smoking is injurious to health!

He replied:
"We are bothered about ERRORS, not Warnings...!

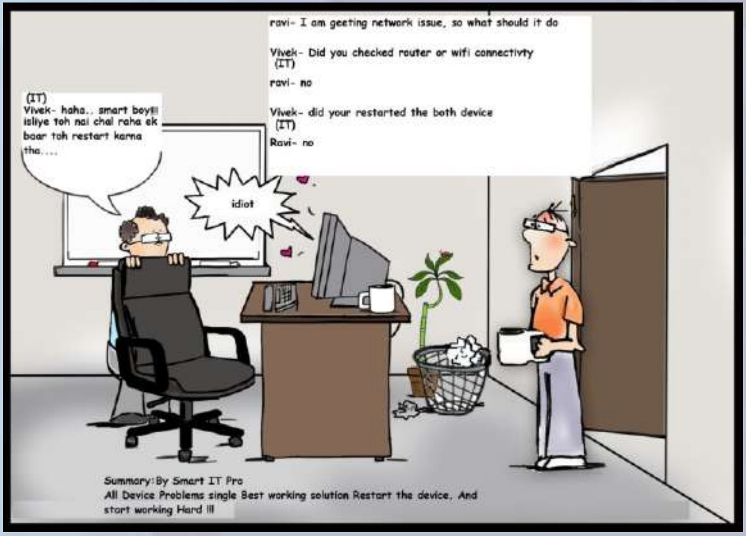
Wi-Fi went down for five minutes, so i had to talk to my family. They seem like nice people.

Never let your computers know that you are in a hurry

Computers can smell fear. They slow down if they know that you are running out of time.



Long time ago, people who sacrifice their sleep, family, food, laughter and other joys of life were called SAINTS.
But now, they are called
IT Professionals


ravi- I am geeting network issue, so what should it do
Vivek- Did you checked router or wifi connectivty (IT)
ravi- no
Vivek- did your restarted the both device (IT)
Ravi- no
(IT) Vivek- haha.. smart boy!!! isliye toh nai chal raha ek baar toh restart karna tha....
idiot
Summary: By Smart IT Pro
All Device Problems single Best working solution Restart the device. And start working Hard !!!

Horoscope Prediction For The Month Of May 2021

Aries (March 21-April19)

You will be focused on matters regarding your own health and appearance. The diet that you have started recently or gymnastics will finally give first results. Thanks to self-discipline, you can overcome all weaknesses and thanks to that there will be no problem that you will not be able to achieve.

Taurus(April 20-May20)

May will be the month when you want to think about deleting yourself. This does not mean, however, that you are about to stagnate. Act, but away from human sight. Pay more attention to home matters. Professional matters are important, but not the most important, the more that recently you neglected your family. You will become a diplomat in every inch.

Gemini (May 21-June20)

Get ready for some turbulence in your life. There will be a lot of stressful situations that will result from misunderstandings and misunderstandings. A certain person who previously seemed to you to be friendly and cordial will have many things to complain about and emphasize it in a proper way. You, however, defend yourself from this!

Cancer (June21-July22)

You will feel the irresistible need to get to know yourself and look deeper into your soul, to find out again the meaning of life and new truths about yourself. This need will be most noticeable in the first half of the month, so be careful that the trips to the mysterious corners of your soul are only constructive. This is a good period for trips. Therefore, plan a weekend trip and break away from the monotonous and gray reality.

Leo (July23-Aug22)

Finally, you'll prove to everyone what you can really do! Already the end of being in the shadow of others, now is the time for you and you will now be in the spotlight. If your relations with your partner have not been going well lately, then finally there will also be a time when fate will start favoring you in love.

Virgo (August23-September22)

In matters related to investments, finances, applying for promotion or an increase, it is recommended to slow down the pace. In May, pay more attention to your family, because it should be the most important thing for you, especially when it's not going well. Your intuition will be good to tell you. You will be able to find yourself in a good place and good time.

Libra (September23-October22)

In May you lived at high speed, and now you will feel it. Therefore, it is recommended to allocate May for rest, relaxation and recuperation. Focus on your inner world, dreams and fantasies. Listen to the voice and intuition. Then it is quite possible that you will quickly find answers to doubts that have been bothering you for a long time.

Scorpio (October23-November21)

Stop for a moment and give your thoughts. Soon, very much will happen in your life, so it's better to prepare for it. Therefore, save your strength and indulge in blissful relaxation in the company of those closest to you. An elderly lady will give you some valuable tips, listen to her and use all the advice that will prove very helpful in the future.

Sagittarius (November22-December21)

In May there will be no time to relax and rocking in the clouds. You have to start working hard from the beginning of the month. Start more realistically assess what is happening in your immediate environment and draw conclusions that will be a recipe for the future - especially in professional matters. Do not act too hastily, let your steps be carefully thought out

Capricorn (December22-January19)

There will be a good streak for professional matters. This month brings many possibilities. Many ideas that have so far been circulating in your head now have a chance to turn into reality. But be careful - do not make promises and commitments without coverage. If you feel that you can not do something, just say it openly. Some older person will give you some tips.

Aquarius (January20-February18)

At May, plan the end of all important matters that have been hanging in the air for a long time waiting for the finale. It is quite possible that they concern the end of education, writing a job or performing another task, such as business. You can be sure that you will be able to get it all this month. And it will be a source of satisfaction for you .

Pisces (February19-March20)

May will be a great month to implement your long-planned plans, to complete important projects that have been suspended or even to start your own business. Ideas in your head will multiply by the minute. Many people of this creativity and brilliance will start to envy you. In addition to the original ideas, you will have full freedom in their implementation.

Quality Māntrā

May, 2021

A Newsletter of International Certification Services

Please send us your valuable comments & suggestions on suggestions@icsasian.com. To subscrite for a free Subscription send us a mail with subject "Subscribe for QUALITYMANTRA"at suggestions@icsasian.com

Be a part of the Publication, Share your Ideas, thoughts, Vision and Knowledge, Join us in our mission of a Quality World. Please send your article in 300-500 words with your name and photograph to quality.mantra@icsasian.com.

This Edition Compiled and Presented by ICS Corporate Office Team

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, **Email:** info@icspl.org / **Web:** www.icspl.org

BRANCH OFFICE

*Ahmedabad * Bangalore* Baroda* Belgaum *Chennai*Gandhidham* Hyderabad *Indore* Jaipur*
*Kanpur * Ludhiana* Mumbai* Dombivali* Nagpur* Nasik* New Delhi* Pune*
Surat Udaipur* Vapi*

OVERSEAS OFFICE

*Dubai(UAE) *Nepal* Oman* Qatar* SriLanka* Uganda* USA*

Web : www.icsasian.com / www.icspl.org

Disclaimer: This e-Magazine / publication is for internal circulation only. While every effort has been made to ensure that informationis correct at the time of going to print International Certification Services Pvt. Ltd. cannot be held responsible for the outcome of anyaction or decision based on the information contained in this publication / website. The publishers do not give any warranty forarticle's written by various author's for the completeness or accuracy for their publication's content, explanation or opinion.

ICS TECHNOLOGIES