Quality Māntrā Nov, 2023

A Newsletter of International Certification Services

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Quality Mantra Nov, 2023
A Newsletter of International Certification Services

DIGITAL WORLD HELPING MSME
(CMD)

Dr. Sundar Kataria

Today, we are in twenty first century in Global Village; technological advancement, competition, customer overgrowing demand for quality and safety of the Products & Services and Occupation Health & Environment are in priority. The organization need to be proactive that shall focus to have an effective and efficient management system to provide products and services at reasonable and affordable price. This will be possible for MSME unless they adopt to a robust management system and digital business operation. Further more MSME supports and provides products and services to the corporate world that means they need to follow modern management system and adopting to the digital operation.

The latest digital tools and techniques to help the MSME organization to prepare for any future challenges. It is time to priorities digital transformation "is most critical for businesses to remain in today's fast moving, constantly evolving market. The organization adopting to digital technologies, organization can become more efficient, customer-focused and agile, resulting into increased revenue and profitability. They can anticipate and navigate future challenges including disruptive event like supply chain, changing customer needs & behaviour.

Organization not adapting to digital transformation may fall prey to falling behind and losing market share including going out of business.

Digital business operation will help in Lean management; digital technologies systems are available to choose and / or can be tailored made.

Technologies available are:

- Block chain
- Social computing
- Financial control
- Online operation
- Cloud based storage and application services
- Data analytics
- Inventory control etc.
- Website and mobile app
- Multimedia

Let's embrace to new Digital technology to beat the global competition, continue and sustain your business.

Quality Mantra Nov, 2023

A Newsletter of International Certification Services

Mr. Nagaraju Etikala

Information Security Management System – ISO/IEC 27001:2022

Introduction:

ISO/IEC 27001:2022 Transition certification is the latest version of the widely recognized international standard for Information Security Management Systems (ISMS). The international standard ISO/IEC 27001 is an ISMS set of requirements for establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving a documented ISMS with respect to an organization's overall business risks and opportunities.

It belongs to a class of standards referred to as the Management System Standards (MSS), which includes standards such as ISO 9001(Quality Management System), ISO 14001 (Environmental Management System), ISO 22000 (Food Safety Management System), ISO/IEC 20000-1 (Service Management System) and ISO 22301 (Business Continuity Management System).

What is information Security?

- Securing information is a big challenge. This includes not only the protection of your personal information but also of organizations that store your personal information on their systems. We give organizations our consent to keep our information and they have the responsibility to protect it from getting into the wrong hands.
- In addition, an organization's information could be stolen by their competitors. Industries that are particularly vulnerable include the banking, automobile, aviation, software, and hardware industries.
- The type of information that you need to secure includes personal and organizational data.
- Personal information includes banking data like ATM card details, transaction details, information regarding banking passwords, and other personal details. Medical reports are also at risk of being stolen this can be in the form of electronic reports or hard copies.
- Organizational data, such as trade secrets, product designs and customer information, is also at risk and must be secured

ISMS stand on three main pillars, referred to as the CIA triad

Confidentiality: Confidentiality refers to protecting information from being accessed by unauthorized parties.

Integrity: Integrity refers to the consistency, accuracy, and trust worthiness of data over its entire lifecycle

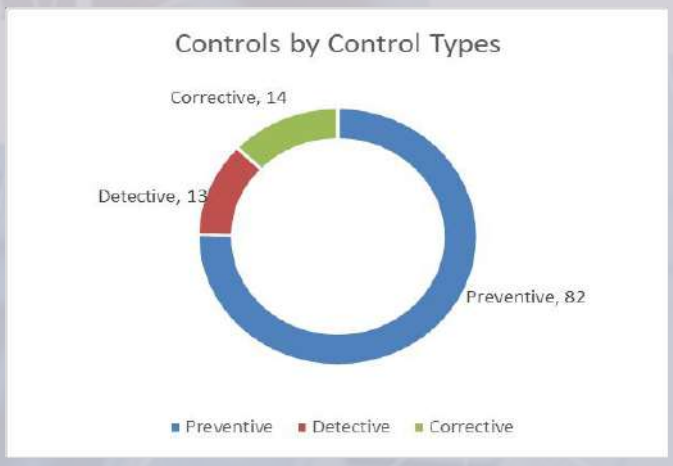
Availability: The availability of data is also very important. If the data is stored in a database, it is very important that the business or authorized user can access it when needed. The data should be readily available to authorized users. If the data is secured but not available when it's requested, this can be a big risk to the company.

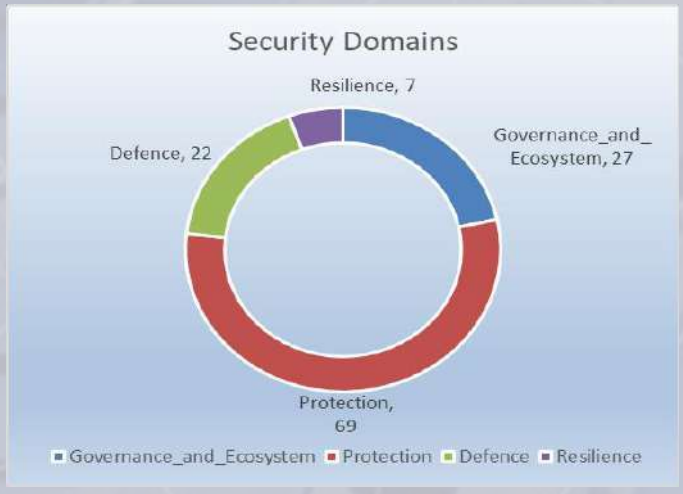
ISO 27001:2022 New requirements

- Requirements of interested parties to be addressed through the ISMS
- Planning of changes
- Establishing criteria for processes and implementing control for them
- MRM input: Changes in needs and expectations of interested parties

New Controls:

1.Threat Intelligence
2.Information security for use of cloud services
3.ICT readiness for business continuity
4.Physical security monitoring
5.Configuration management
6.Information deletion
7.Data Masking
8.Data leakage prevention
9.Monitoring activities
10.Web filtering
11.Secure Coding





Quality Mantra Nov, 2023

A Newsletter of International Certification Services

Sunki Saikumar

Third-party Security Risk Management (TPSRM)

What is TPSRM:

TPSRM is a form of risk management that involves identifying, assessing and managing information security risks associated with the use of third-parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers). The TPSRM gives organizations an understanding of how the third-parties are used, managed, monitored and the safeguards they have in place to protect client's data.

Need of TPSRM:

1.In today's interconnected business environment, organizations heavily depend on third-party vendors for various services, such as IT support, software, logistics, and marketing. In order to provide services, the third-parties require access to sensitive data, infrastructure, or critical systems; which brings the risks that must be managed effectively.

2.To minimize the issues related to third-parties such as security breaches, reputational damages, financial losses, legal and regulatory compliance violations.

Steps in TPSRM program:

1.Vendor Identification and Categorization: Organizations should maintain the list of all vendors utilized by them for various services. Organizations should categorize the vendors based on the risk level they pose to organization. The risk level can be identified by different parameters such as criticality of service, type of data handled by vendor, volume of data involved, level of data access, data exchange method etc. In general, the vendors are classified as critical, high, medium and low risk vendors.

2.Vendor Risk Assessment: The vendor risk assessment includes review of vendor security related documents, processes and identification of risks. The risk assessment process involves using questionnaires to gather information about the vendor's security practices and review of vendor security policies, procedures, security certifications (ISO 27001, ISO 22301, PCI DSS etc.), independent audit reports (SOC2, SOC1 etc.), vulnerability and penetration test reports, etc.

3.Risk Mitigation: Risk mitigation process involves implementation of controls to mitigate the risks identified in risk assessment. The risk mitigation could involve implementation of technical controls, implementation of security policies and procedures, conducting security awareness training to staff, etc.

4.Periodic Monitoring: TPSRM is an ongoing process. The organisation needs to continuously monitor the vendor's security practices and conduct regular security risk assessments. The vendor risk assessments are carried out periodically based on the classification of vendors. In general, for critical and high-risk vendors the risk assessments are conducted at least annually; For medium and low risk vendors the risk assessments are conducted for every two or three years.

5.Security Incident Management: The organizations should maintain agreements with its vendors related to security incident detection, response and management. The vendors should have proper incident response plan, defined roles and responsibilities, communication and notification protocols for various types of incidents.

Conclusion: The main goal of TPSRM is to identify the security risks posed by vendors and remediate them to protect organization's data and systems.

DR. V. MURALIDHAR

INFORMATION SECURITY

What is Information Security (Info Sec)?

Information security covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

The consequences of security incidents include theft of private information, data tampering, and data deletion. Attacks can disrupt work processes and damage a company's reputation, and also have a tangible cost.

Organizations must allocate funds for security and ensure that they are ready to detect, respond to, and probatively prevent, attacks such as phasing, malware, viruses, malicious insiders, and ram software.

The 3 Principles of Information Security?

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customs

The CIA Triad defines three key principles of data security

Information Security Policy

An Information Security Policy (ISP) is a set of rules that guide individuals when using IT assets. Companies can create information security policies to ensure that employees and other users follow security protocols and procedures. Security policies are intended to ensure that only authorized users can access sensitive systems and information.

Top Information Security Threats

There are hundreds of categories of information security threats and millions of known threat vectors. Below we cover some of the key threats that are a priority for security teams at modern enterprises.

Unsecure or Poorly Secured Systems

The speed and technological development often leads to compromises in security measures. In other cases, systems are developed without security in mind, and remain in operation at an organization as legacy systems. Organizations must identify these poorly secured systems, and mitigate the threat by securing or patching them, decommissioning them, or isolating them.

Social Media Attacks

Many people have social media accounts, where they often unintentionally share a lot of information about themselves. Attackers can launch attacks directly via social media, for example by spreading malware via social media messages, or indirectly, by using information obtained from these sites to analyze user and organizational vulnerabilities, and use them to design an attack.

Social Engineering

Social Engineering involves attackers sending emails and messages that trick users into performing actions that may compromise their security or divulge private information. Attackers manipulate users using psychological triggers like curiosity, urgency or fear.

Malware on Endpoints

Organizational users work with a large variety of endpoint devices, including desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the organization's control, and all of which connect regularly to the Internet.

Lack of Encryption

Encryption processes encode data so that it can only be decoded by users with secret keys. It is very effective in preventing data loss or corruption in case of equipment loss or theft, or in case organizational systems are compromised by attackers.

Security Mis-configuration

Modern organizations use a huge number of technological platforms and tools, in particular web applications, databases, and Software as a Service (SaaS) applications, or Infrastructure as a Service (IaaS) from providers like Amazon Web Services.

Active vs Passive Attacks

Information security is intended to protect organizations against malicious attacks. There are two primary types of attacks: active and passive. Active attacks are considered more difficult to prevent, and the focus is on detecting, mitigating and recovering from them. Passive attacks are easier to prevent with strong security measures.

Active Attack

An active attack involves intercepting a communication or message and altering it for malicious effect. There are three common variants of an active attacks:

- **Interruption**—the attacker interrupts the original communication and creates new, malicious messages, pretending to be one of the communicating parties.
- **Modification**—the attacker uses existing communications, and either replays them to fool one of the communicating parties, or modifies them to gain an advantage.
- **Fabrication**—creates fake, or synthetic, communications, typically with the aim of achieving denial of service (DoS). This prevents users from accessing systems or performing normal operations

Passive Attack

In a passive attack, an attacker monitors, monitors a system and illicitly copies information without altering it. They then use this information to disrupt networks or compromise target systems.
The attackers do not make any change to the communication or the target systems. This makes it more difficult to detect. However, encryption can help prevent passive attacks because it obfuscates the data, making it more difficult for attackers to make use of it..

Information Security and Data Protection Laws

Information security is in constant interaction with the laws and regulations of the places where an organization does business. Data protection regulations around the world focus on enhancing the privacy of personal data, and place restrictions on the way organizations can collect, store, and make use of customer data.

IT Act India.

It was introduced in the year 2000 with a wide range of principles.

Data Protection Laws in the European Union (EU): the GDPR

The most known privacy law in the EU is the GDPR. This regulation covers the collection, use, storage, security and transmission of data related to EU residents.

The GDPR applies to any organization doing business with EU citizens, regardless of whether the company itself is based inside or outside the European Union. Violation of the guidelines may result in fines of up to 4% of global sales or 20 million Euro.

The main goals of the GDPR are:

- Setting the privacy of personal data as a basic human right
- Implementing privacy criteria requirements
- Standardization of how privacy rules are applied
- Our comprehensive approach relies on multiple layers of protection, including:
- Database firewall—blocks SQL injection and other threats, while evaluating for known vulnerabilities.
- User rights management – monitors data access and activities of privileged users to identify excessive, inappropriate, and unused privileges.
- Data masking and encryption – aobfuscates sensitive data so it would be useless to the bad actor, even if somehow extracted.
- Data Loss prevention – inspects data in motion, at rest on servers, in cloud storage, or on endpoint devices.
- User behavior analytics – establishes baselines of data access behavior, uses machine learning to detect and alert on abnormal and potentially risky activity.
- Data discovery and classification – reveals the location, volume, and context of data on premises and in the cloud.
- Database activity monitoring—monitors relational databases, data warehouses, big data and mainframes to generate real-time alerts on policy violations.
- Alert prioritization – AI and machine learning technology to look across the stream of security events and prioritize the ones that matter most.

SO PROTECT YOUR DATA AND SAFE SECURITY OF ALL YOUR INFORMATION

Training Calendar - November-2023

Course Title	Date	Time	Fees	Class Type
IQA 13485	6th & 7th Nov 2023	10.00 am to 5.00pm	7000+18%GST	Offline
LA QMS	20th to 24th Nov 2023	10.00 am to 5.00pm	15000+18%GST	Online
IQA IMS	28th to 30th Nov 2023	10.00 am to 5.00pm	7000+18%GST	Online
LA 19443	24th to 30th Nov 2023	10.00 am to 5.00pm	14000+18%GST	Offline training at palghar

Riddles

1.Which is the twitter hashtag used for 'Swachh Bharat Mission'?

2.What is the full form of SBM?

3.Who composed the audio track 'Swachh Bharat kaIradaKarliya hum ne' which is specially prepared for 'Swachh Bharat Mission

4.Who designed the logo of 'Swachh Bharat Abhiyan'?

5.Who flagged the Swachh Bharat Run (SBR)?

6.Why did the spider get a job in I.T.?

7.What kind of coat is always wet when you put it on?

8.I have branches yet I have no leaves, no trunk and no fruit. What am I?

9. What belongs to you but other people use it more than you?

10.What is harder to catch the faster you run?

1.#MyCleanIndia, 2.Swachh Bharat Mission, 3.Prasoon Joshi, 4.Anant from Maharashtra, 5.President of India, 6.He was a great web designer, 7.A coat of paint, 8.A bank, 9.Your name, 10.Your breath

Horoscope Month of November - 2023

Aries

Arise should try to move ahead in their career in the month of October. There can be a balance between money, work and family. You may get praise and help from people senior to you in your work. People may be influenced by your style. This month, you will have to take great care of your stomach, otherwise, health problems related to the digestive system may arise.

Taurus

Taurus individuals will get opportunities to spend time with family and enjoy happiness this month. Luck may favour you in matters related to job and business. You may get happy opportunities. There will be a time of mixed experiences. It would be advisable to avoid making any big decisions under someone's influence. This month you may have to face some difficulties in the workplace. People associated with business may get positive results.

Gemini

This month will be normal for employed people. Workload will be less. There are chances of improvement in spoiled relations. You may get some good news. You may also get social respect. The decision of buying and selling land and buildings needs to be taken very thoughtfully. At the beginning of this month, you will see positive changes in your love relationships

Cancer

This month will be auspicious for Cancer individuals. People around you can be helpful to you to a great extent. You can also fulfill any wish of your spouse. Have faith in the decisions you make. Be calm. Be patient. Inclination towards material comforts may increase. There are also chances of solving personal problems.

Leo

This month will open paths to good fortune for Leo individuals. People can constantly try something new in business and jobs. This month has been filled with success. Old problems can be resolved. There are chances of resolution of job and family tensions. Move forward with hope and confidence. There are chances of achieving success. You may get a transfer and promotion in your job. Your married life will be good.

Virgo

This month will be full of turmoil for Virgo individuals. Someone may prove helpful to you in the future. Employed and working people can be successful in whatever they try. You will be able to take time out for yourself also. Think carefully before signing any contract.

Horoscope Month of November - 2023

Libra

This month will be beneficial for Libra individuals. You can start some beneficial work at the beginning of this month. There are chances of success in every kind of collective work. Whatever is in your mind, you will express it openly. There are chances of going somewhere with family. The process of meeting new people will begin. Employed people will bring something new to their work. People doing business will get their old money back. Complicated matters can also be resolved.

Scorpio

Scorpio individuals will be influential this month. You will take care of the needs and wishes of others. There may be opportunities for positive change in life. Your fears will go away. You will be happy with the progress of those around you. There are chances of making new plans in business.

Sagittarius

Sagittarius individuals may get good news this month. Work wisely in the office. Try to improve the atmosphere at home. Your workload in the office may increase to a great extent. Relations with friends can become better. Chances of meeting someone new are possible.

Capricorn

People of Capricorn may have to make a plan on important matters. You may also be given the task of conveying someone else's message to someone else. New plans may also come your way. Some planned tasks may also be completed. This month will be fine for you.

Aquarius

This month will be full of relief for Aquarius individuals. If you are thinking of doing some new things at work, then do it. There is hope of getting relief from problems. Your vision will remain broad and your planning will continue, keeping in mind the times to come. You will include new technology in your life also. You can get timely help from the people around you.

Pisces

Pisces individuals are going to get many auspicious opportunities this month. There is a need to work with patience. Maintain trust in yourself. If you want to do some special and good work, you will get a chance to do it. Try to understand the needs of others. You may also get help from some trusted people. Any old disease may also emerge.

Birthday's Month of November - 2023...

Sr. No.	Emp. Name	Station	Emp. Dob
1	Md Shahnawaz Hussain	ICS-IOCL Haldia Shutdown	01/Nov/1991
2	Raksitha Devadiga	ICS-Assure - Health	02/Nov/1994
3	Qureshi Muzamil Abdul Sattar	ICS-Assure - Health	03/Nov/1994
4	Ram Ashis Yadav	ECD-Gail Survey	03/Nov/1990
5	Ankit Anand	ICS-IGL New Delhi	03/Nov/2000
6	Simran Sumeet Kataria	Directors	03/Nov/2003
7	Adimulam Durga Venkata Prasad	ICS-IOCL Haldia Shutdown	04/Nov/1995
8	Manikandan S	ICS-Torrent Gas July 2022	04/Nov/1995
9	Adimulam Durga Venkata Prasad	ICS-IOCL Haldia Shutdown	04/Nov/1995
10	Shubham Dhaygude	ICS-MNGL-Pune	07/Nov/1995
11	Munish Kumar Chouhan	ICS-ONGC-WADU	08/Nov/1991
12	Ashok Lodhi	ICS-Torrent Gas July 2022	08/Nov/1992
13	Dilip Singh Negi	Mumbai-CO	08/Nov/1962
14	Akash Baid	Mumbai-Admin	09/Nov/1997
15	Dhaval Odhavji Bhanushali	Vapi	09/Nov/2002
16	Md Afroz Alam	ICS-Torrent Gas July 2022	09/Nov/1994
17	Wasim Golandaj	ICS-Reliance Ro Project	10/Nov/1988
18	Mihir Ramesh Ahirekar	ICS-Assure - Motor OD	10/Nov/2001
19	Hemant Sharma	ECD-BPCL BINA & KOTA	10/Nov/2000
20	Arjun Singh	ICS-ONGC-WADU	10/Nov/1993
21	Himanshukumar Dhobi	ICS-ONGC-WADU	11/Nov/1987
22	Bal Govind Maurya	ICS-Torrent Gas	11/Nov/1995
23	Nikul Suthar	ICS-ONGC-WADU	12/Nov/1988
24	Sandeep Kumar	ICS-IGL New Delhi	12/Nov/1986
25	Mohammad Sahil	ICS-Torrent Gas July 2022	14/Nov/1995
26	Manik Chavan	Mumbai-Admin	14/Nov/1989
27	Yasmita Shetty	ICS-Assure	14/Nov/1994
28	Gaurav Kumar .	ICS-IGL New Delhi	15/Nov/1996
29	Minal Balkrishna Posarekar	ICS-Assure - Forensic	15/Nov/1995
30	Narsaiah Seepathi	ECD-CORRAD	15/Nov/1969
31	Sunil Khanna	ICS-ONGC-Mehsana	15/Nov/1956
32	Vinnarasan G. .	ICS-Reliance Ro Project	15/Nov/1997
33	Alok Ranjan	ICS-IGL New Delhi	16/Nov/1992
34	Sunil Saini	Jaipur	19/Nov/1992
35	Naveen Rana	ECD-BPCL BINA & KOTA	19/Nov/1998
36	Prasanth M.	ICS-ONGC-Offshore	19/Nov/1995
37	Puneet Kumar Lal Bahadur Yadav	ICS-VENDOR	20/Nov/1996
38	Shifa Shaikh	Mumbai-HR	20/Nov/2002
39	Viraj Indulkar	ICS-Assure - Reconstruction	20/Nov/1992
40	Vijay Kumbhoje	ICS-ISRO Mumbai	23/Nov/1991
41	Ankur Semwal	ICS-IGL New Delhi	24/Nov/1999
42	Nitish Dwivedi	ICS-Torrent Gas July 2022	25/Nov/1997
43	Dr. Rohini Sakpal	ICS-Assure - Health	25/Nov/1981
44	Anand Mitkari	Mumbai-ECD	26/Nov/2001
45	Mohammad Aasim	ICS-Technology	26/Nov/1993
46	Pabitra Mallik	ICS-MNGL Nashik	26/Nov/1998
47	Avijit - Jha	ICS-ONGC-Ankleshwar	28/Nov/1982

ICS Ganpati Festival- 2023

CORCON- 2023


AMPP INDIA
2023


AMPP INDIA
AMPP


AMPP INDIA
2023


AMPP INDIA
CORCON
2023
ASIA'S LARGEST CORROSION
CONFERENCE IN INDIA
NACE


COATING SURVEY


CORCON
2023
WELCOME TO ASIA'S LARGEST
CONFERENCE & EXHIBITION ON CORROSION
CORCON 2023

Quality Mantra

Nov, 2023

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: 022-42200900, **Email:** info@icspl.org / **Web:** www.icspl.org

BRANCH OFFICE

*Ahmedabad*Bangalore *Belgaum*Chennai *Gandhidham *Hyderabad *Indore *Jaipur
*Ludhiana *Mumbai *Nasik *New Delhi *Pune *Udaipur *Vadodara *Vapi

OVERSEAS OFFICE

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

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

ICS Group Companies