Quality Mantra April, 2025

A Newsletter of International Certification Services

Special Issue On

CYBER SECURITY

Mr. Sundar Kataria

ICS Assure One Decade of Successful Journey

CMD

The achievements and footprint of ICS Assure in penetrating India's vast insurance sector are truly remarkable. We take immense pride in what we have accomplished and continue to achieve, especially in the evolving landscape of the industry.

We warmly welcome all of you to this MRM-25 event and are pleased to see the growing strength of our team. Your contributions have played a key role in strengthening International Certification Services (ICS) Assure. Congratulations from the bottom of my heart on reaching the milestone of successfully completing a decade of operations.

ICS Assure has become a preferred investigation body in India, particularly within the private insurance sector. Our services have gained widespread recognition for being professional, efficient, and advanced. We are considered one of the most effective techno-forensic organizations in the country. Our strength lies in our highly skilled investigation team, which includes doctors, automobile engineers, forensic experts, fire and natural disaster specialists, and computer specialists.

We provide a wide range of services, including the examination of documented information, the detection of forgeries, digital and cyber forensics, DNA and serology analysis, and accident investigations using accident reconstruction. ICS Assure ensures in-depth investigations with a limited turnaround time, a crucial aspect of our services.

In today's fast-evolving world, technological advancements are rapidly shaping every aspect of life. Artificial intelligence (AI) is being adopted across industries, and its potential to enhance the effectiveness and efficiency of data analysis presents both challenges and opportunities. The manufacturing and services industries face a growing need for robust solutions to counter emerging threats, and ICS Assure is positioned to capitalize on this need by expanding our scope of services.

The IT and digital industries have undergone a major transformation with the rise of cloud computing, mobile devices, and social media. Cloud services like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud continue to capture significant market share by offering businesses flexibility and cost-effective IT infrastructure solutions. Smartphones, tablets, and mobile applications are now integral to meeting consumer demands, while platforms such as Facebook, Twitter, LinkedIn, and Instagram have become essential for marketing, customer engagement, and efficient communication.

The past few years have seen AI technology revolutionize the IT industry, offering both challenges and opportunities. As we move forward, it's crucial for us to adapt and equip ourselves with new services and tools to address the evolving landscape. Some of the key challenges and concerns we must address include:

- Cyber security
- Digital Transformation & Data Security
- Integration of IT & OT (Operational Technology)
- Real-time Operations
- Size and Scalability of Data Centers
- Environmental Considerations
- Selection of the Right Software (ERP and Applications)
- SDI (Serial Digital Interfaces
- AI Uncertainty and Its Impact

AI offers immense potential for improving operations, reducing costs, and increasing productivity. Over the next two days, we will delve into how advancements in the IT and digital worlds have transformed the manufacturing and services industries. We will explore how these changes present both opportunities and threats, and how we can prepare ourselves to navigate this evolving landscape.
Let's continue our journey toward success by embracing the challenges, maximizing opportunities, and staying at the forefront of technological innovation.


Mr. Sanjay Chauhan

Cyber Security: Safeguarding the Digital Future

General Manager - Hardware & Networking

In today's interconnected world, where technology underpins almost every aspect of our lives, cybersecurity has become an essential concern. With the growing volume of sensitive information stored and shared digitally, protecting this data from malicious threats has never been more crucial. Cybersecurity refers to the practice of defending systems, networks, and data from digital attacks, unauthorized access, and damage. It involves a combination of technologies, processes, and practices designed to safeguard digital infrastructure from a wide range of cyber threats.

The Importance of Cyber security

As more businesses and individuals move their operations online, cyber threats are becoming increasingly sophisticated. Cyberattacks such as data breaches, ransomware, phishing, and denial-of-service (DoS) attacks are on the rise, causing significant financial, reputational, and operational damage to organizations and individuals alike. These attacks often target personal information, financial data, intellectual property, and critical infrastructure. With the growing reliance on digital systems, the cost of these cyber incidents is escalating, both in terms of direct financial loss and long-term damage to trust and reputation.

Moreover, as more critical infrastructure such as healthcare, transportation, and utilities become reliant on digital systems, the impact of cybersecurity vulnerabilities can extend well beyond financial losses, potentially jeopardizing public safety and national security.

Types of Cyber security Threats

- **Malware:** Is malicious software designed to damage or disrupt systems, networks, and devices. It can take various forms, such as viruses, worms, Trojan horses, and ransomware. Ransomware, in particular, has gained attention due to its ability to encrypt victims' files and demand payment for their release.
- **Phishing:** Is a method of tricking individuals into revealing sensitive information, such as usernames, passwords, or financial details. This is often done by sending fraudulent emails or messages that appear to come from legitimate sources, such as banks or government agencies.
- **Data Breaches:** Data breaches occur when unauthorized individuals gain access to sensitive data, such as customer records, credit card numbers, or personal health information. These breaches can lead to identity theft, financial fraud, and other malicious activities.
- **Denial-of-Service (DoS) Attacks:** DoS attacks aim to overwhelm a system, network, or website with excessive traffic, rendering it unavailable to legitimate users. Distributed denial-of-service (DDoS) attacks involve multiple compromised systems targeting the same target, increasing the intensity of the disruption.

- **Man-in-the-Middle (MitM) Attacks:** In a MitM attack, an attacker intercepts and alters communication between two parties without their knowledge. This can be used to steal sensitive data, such as login credentials or financial transactions.
- **Insider Threats:** Insider threats involve employees, contractors, or other trusted individuals who intentionally or unintentionally compromise an organization's cyber security. These threats can range from employees accessing and leaking sensitive data to malicious acts aimed at sabotaging company operations.

The Key Elements of Cyber security

To protect against these diverse cyber threats, cyber security strategies generally focus on several key elements:

- **Network Security:** Network security involves protecting an organization's internal networks from external threats. This can be achieved by implementing firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other network defences.
- **Application Security:** Ensuring that software applications are designed and maintained with security in mind is crucial to preventing exploitation. Regular software updates, code reviews, and security patches are vital in addressing vulnerabilities.
- **Information Security:** Information security focuses on safeguarding data from unauthorized access or disclosure, ensuring data integrity, and protecting its availability. This involves encrypting sensitive data and restricting access to only authorized users.
- **Identity and Access Management (IAM):** IAM systems are designed to ensure that only authorized individuals can access certain systems or data. Multi-factor authentication (MFA) is one of the most common methods to enhance security by requiring users to provide multiple forms of identification.
- **Incident Response:** In the event of a cyberattack or breach, having a robust incident response plan is critical. This plan outlines the steps an organization should take to detect, respond to, and recover from cybersecurity incidents, minimizing damage and restoring operations as quickly as possible.
- **Cloud Security:** As more organizations migrate their operations to the cloud, ensuring the security of cloud-based systems is essential. This involves securing data, applications, and services hosted in cloud environments and ensuring compliance with regulatory standards.
- **End-User Education and Awareness:** Many successful cyber attacks begin with a single user clicking on a phishing email or downloading malicious software. Training employees and users on best practices, such as avoiding suspicious links and using strong passwords, is one of the most effective ways to reduce the risk of cyber threats.

Emerging Trends in Cyber security

The field of cyber security is constantly evolving, with new technologies and threats emerging regularly. Some of the latest trends in cyber security include:

- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML are playing an increasingly significant role in cyber security, both in terms of identifying and responding to threats. Machine learning algorithms can be used to analyze vast amounts of data for unusual patterns, helping to detect and mitigate cyberattacks in real-time.
- **Zero Trust Architecture:** Zero trust is a security model that assumes that no one, whether inside or outside the organization, can be trusted by default. Access to systems and data is only granted after strict verification and continuous monitoring. This approach minimizes the risk of insider and external threats.
- **Ransomware Defense:** With the rise of ransomware attacks, organizations are increasingly focusing on preventing and mitigating these types of incidents. This includes implementing regular backups, improving employee awareness, and using advanced threat detection tools to spot ransomware before it can spread.

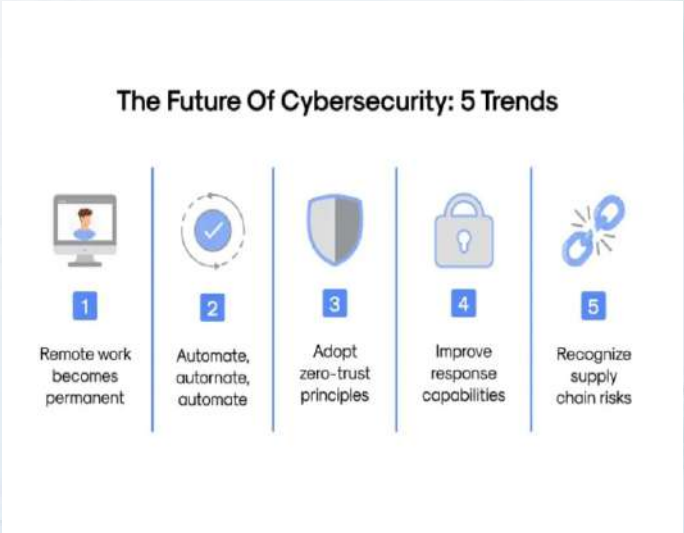
4.Quantum Computing: As quantum computing advances, it holds the potential to revolutionize cyber security, both positively and negatively. While quantum computers could be used to develop more secure encryption methods, they could also pose a threat by breaking current encryption techniques. Researchers are exploring quantum-safe cryptography to address these challenges.

The Future of Cyber security

The future of cyber security will be shaped by technological advancements, evolving threats, and increasing regulatory requirements. With the rise of the Internet of Things (IoT), 5G networks, and digital currencies, new vulnerabilities will emerge, and cyber defense strategies will need to evolve accordingly.

Governments, businesses, and individuals must work together to create a resilient cyber security ecosystem. Proactive measures, including adopting best practices, investing in cyber security technologies, and fostering a culture of cyber security awareness, will be key to staying ahead of emerging threats.

As the digital landscape continues to expand, the role of cyber security will only become more critical in ensuring a secure and trustworthy online environment.



Quality Mantra April, 2025
A Newsletter of International Certification Services

Mr. Parmesh Yadav

How to Develop a Secure Website

General Manager - Software

In today's digital landscape, website security is more critical than ever. Cyber threats such as SQL injection, cross-site scripting (XSS), and data breaches can compromise user data and damage your reputation.

Building a secure website requires a proactive approach—from secure coding practices to continuous monitoring. By implementing these best practices, you can protect user data, prevent breaches, and maintain trust in your web application.

To build a secure website, developers must follow best practices in coding, authentication, and data protection.

1. Use HTTPS with SSL/TLS Encryption

Always secure your website with **HTTPS** (Hypertext Transfer Protocol Secure) by installing an **SSL/TLS certificate.** This ensures encrypted communication between the server and users, preventing man-in-the-middle (MITM) attacks.

Obtain an SSL certificate from trusted providers like **Let's Encrypt, Digi Cert, or Comodo.**

Enforce HTTPS by redirecting all HTTP traffic.

Use **HSTS (HTTP Strict Transport Security)** to prevent downgrade attacks.

2. Protect Against SQL Injection (SQLi)

SQL injection occurs when attackers manipulate database queries through input fields. Prevent it by:

- Using **prepared statements** (parameterized queries) instead of dynamic SQL.
- Employing **ORM (Object-Relational Mapping)** frameworks like **Hibernate or Sequelize.**
- Validating and sanitizing all user inputs.

3. Prevent Cross-Site Scripting (XSS) Attacks

XSS attacks inject malicious scripts into web pages. Mitigate them by:

- **Escaping output** (convert special characters to HTML entities).
- Using **Content Security Policy (CSP)** headers to restrict script sources.
- Sanitizing user-generated content (e.g., comments, forms).

4. Implement Strong Authentication & Authorization

Weak authentication leads to unauthorized access. Secure login systems by:

- Enforcing **strong password** policies (min. 12 chars, multi-factor authentication).
- Using **bcrypt, Argon2, or PBKDF2** for password hashing (never store plaintext passwords).
- Implementing **role-based access control (RBAC)** to limit user permissions.

5. Secure File Uploads & Data Handling

File uploads can introduce malware. Protect your system by:

- Restricting file types (whitelist extensions like .jpg, .pdf).
- Scanning uploads with antivirus tools.
- Storing files outside the web root and renaming them to prevent execution.

6. Protect Against CSRF (Cross-Site Request Forgery)

CSRF tricks users into executing unwanted actions. Prevent it by:

- Using **anti-CSRF** tokens in forms.
- Enabling **Same Site cookies.**

7. Keep Software & Dependencies Updated

Outdated software is a major security risk.

- Regularly update **frameworks, and libraries, CMS (Word Press, Drupal).**
- Use tools like **Dependa bot or Snyk** to scan for vulnerabilities.

8. Use Security Headers

Add HTTP security headers to protect against common attacks

9. Backup & Disaster Recovery Plan

- Schedule **automated backups** of databases and files.
- Store backups in **secure, offsite locations.**

Mr. Ravi Gupta

Secure Code Environment of Web Development

Sr. Software manager

Introduction

Security is very important when building web applications, especially in **Web Development**. A secure coding environment helps protect against attacks like hacking, data theft, and unauthorized access.

1. Secure User Login

The first step in security is ensuring that only the right people can access your application.

2. Authentication: This checks if a user is real. Web allows different login methods like usernames and passwords, Google or Face book login, and Windows authentication.

3. Authorization: This controls what each user can do. Role-based access (RBAC) allows assigning different permissions to users, like ADMIN, SM ,Project Manager and regular users.

4. Strong Passwords: Always require users to use strong passwords and enable multi-factor authentication (MFA) for extra security.

Protecting Data

Keeping data safe is important to prevent leaks or unauthorized changes.

- **Encrypting Sensitive Data**: Store important data (like passwords) using encryption methods such as AES and hash passwords using BCrypt.
- **Using Secure Cookies**: Set cookies with security features (Secure, Http Only, Same Site) to protect user sessions.
- **Validating User Input**: Always check and clean user input to prevent attacks. Use Regular Expressions to allow only valid data.
- **Do Not Store Passwords in Code**: Keep secrets like API keys in **Azure Key Vault** or configuration files instead of writing them in the code.
- **Use HTTPS**: Always use HTTPS instead of HTTP to protect data sent between users and the server.
- **Error Handling**: Do not show detailed error messages to users, as hackers can use them to find weaknesses.
- **Use Security Headers**: Add headers like Content-Security-Policy (CSP) and X-Frame-Options to protect against web-based attacks.

Regular Security Checks

Checking security regularly helps keep your application safe.

- **Penetration Testing:** Test your application by trying to hack it and fix weaknesses before attackers find them.
- **Logging and Monitoring:** Keep logs of user activities using Application Insights to detect suspicious behaviour.
- **Keep Software Updated:** Regularly update .NET libraries and security patches to fix known issues.

Mr. Jayesh Gujar

Enhancing Security in Android and iOS Mobile Applications

Sr. Software Developer (Mobile Application)

In today's digital era, mobile applications play a vital role in our daily lives. However, with the increasing reliance on mobile apps, security threats have also risen significantly.
As a mobile application developer, ensuring the security of your Android and iOS applications is crucial to protect user data and prevent cyber threats. This article highlights key security practices to enhance the security of mobile applications.

1. Implement Secure Authentication
User authentication is the first line of defence. Always use strong authentication mechanisms such as OAuth, biometric authentication (Face ID, Touch ID), and multi-factor authentication (MFA). Avoid storing passwords in plaintext and use hashing algorithms like bcrypt or Argon2.

2. Use Secure Data Storage
Sensitive user data should never be stored in plain text. Use encrypted storage mechanisms such as Android's Encrypted Shared Preferences and iOS's Keychain. For database encryption, consider using SQL Cipher to protect SQLite databases.

3. Secure API Communication
APIs are a common attack vector for mobile applications. Always use HTTPS with TLS 1.2 or higher to encrypt network traffic. Implement API authentication using tokens (JWT, OAuth 2.0) and avoid exposing sensitive information in API responses

4. Minimize Permissions and Follow the Principle of Least Privilege
Request only the necessary permissions required for the app's functionality. Excessive permissions can increase security risks. Regularly audit permissions and remove unnecessary ones.

5. Protect Against Reverse Engineering and Code Tampering
Use code obfuscation tools such as ProGuard, R8 (Android), and Bitcode (iOS) to make it harder for attackers to decompile and analyze your code. Implement runtime integrity checks to detect tampering and modifications.

6. Implement Secure Session Management
Ensure secure session handling by setting appropriate session timeouts, using secure cookies, and
invalidating sessions after logout. For web-based authentication, consider implementing HTTP-only and secure cookies.

7. Regularly Update and Patch Vulnerabilities
Security threats evolve constantly. Keep your application and third-party libraries updated to fix
known vulnerabilities. Regular security audits and penetration testing can help identify potential security gaps.

8. Implement Runtime Security Measures
Detect and prevent attacks such as jail breaking (iOS) or rooting (Android) by implementing security
checks at runtime. Use frameworks like Google Play Protect and Apple's App Transport Security (ATS) for enhanced
protection.


Mr. Ramesh Prajapat

ASP.NET Application Security

Software Developer

ASP.NET is a widely used web development framework developed by Microsoft, designed to create dynamic web applications and services. As with any web-based platform, ensuring security is of paramount importance. ASP.NET provides a comprehensive set of tools, techniques, and built-in features to protect applications against common vulnerabilities and security threats.

1. Authentication and Authorization

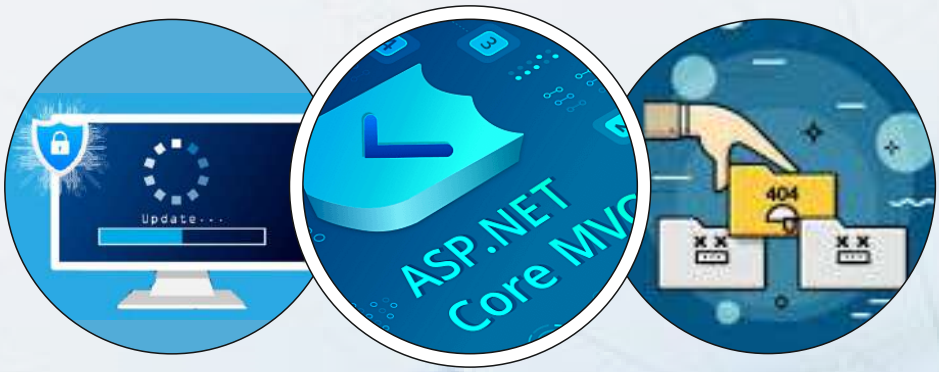
Authentication and authorization are foundational components of application security. Authentication verifies the identity of a user, while authorization determines what that authenticated user is allowed to do.

ASP.NET Identity: ASP.NET provides a robust Identity framework that supports various forms of authentication, including username/password, Open ID to Connect the social media, and external providers like Google, Facebook, and Microsoft.

Role-Based and Claims-Based Authorization: ASP.NET supports both role-based and claims-based access control, allowing fine-grained control over who can access specific resources or perform particular actions.

Data Protection and Encryption

Protecting sensitive data is essential to maintaining confidentiality and integrity.



2. HTTPS (SSL/TLS): ASP. NET applications should always use HTTPS to encrypt data in transit. This prevents attackers from intercepting or tampering with data between the client and server.

3. Data Encryption: Sensitive data stored in databases should be encrypted using secure algorithms. ASP.NET Core offers the Data Protection API, which simplifies encryption tasks.

4. Session Management

- **Session Timeout:** Configure session timeouts appropriately to prevent unauthorized access due to inactive sessions.
- **Cookie Security:** Use secure flags (HttpOnly, Secure, and SameSite) on cookies to enhance security. The HttpOnly flag prevents client-side scripts from accessing the cookie, and Secure ensures cookies are sent only over HTTPS.

5. Error Handling and Logging

Improper error handling can expose sensitive application details.

- **Custom Error Pages:** Configure custom error pages to avoid exposing stack traces or sensitive information.
- **Logging and Monitoring:** Use structured logging and centralized monitoring tools to detect unusual activity and diagnose potential security breaches.

6. Security Updates and Patching

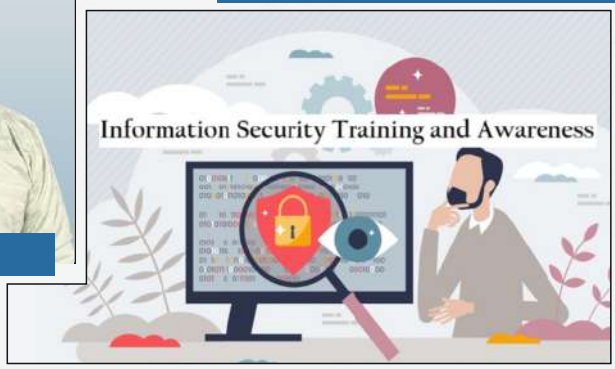
Regularly updating the framework, third-party libraries, and server environments ensures that known vulnerabilities are addressed promptly.

- **NuGet Package Management:** Monitor and update NuGet packages regularly to include the latest security fixes.
- **Patch Management:** Apply patches to the OS, web server (IIS), and other system components.

Mr. Arun Gaud

Network Secure & Network Security

Sr. Hardware and Networking Engineering



1. Network Security Measures:

- **Set up a firewall:** A firewall acts as a barrier, blocking unauthorized access to your network.
- **Enable network encryption:** Use encryption protocols like WPA2 or WPA3 for Wi-Fi networks to protect data transmission.
- **Consider a VPN:** If employees need to access the network remotely, a VPN can create a secure, encrypted connection.
- **Implement Intrusion Detection/Prevention Systems (IDS/IPS):** These systems monitor network traffic for malicious activity and can take action to block threats.
- **Segment your network:** Divide your network into different zones to isolate critical systems and limit the impact of a potential breach.

2.Strong Passwords and Authentication:

- **Enforce a strong password policy:** Require passwords to be long, complex, and unique for each account.
- **Enable multi-factor authentication (MFA):** Add an extra layer of security by requiring users to verify their identity with a second factor, such as a code from a mobile app.
- **Regularly update passwords:** Encourage employees to change their passwords periodically.

3. Software and Hardware Security:

- **Keep software up-to-date:** Regularly update operating systems, antivirus software, and other applications to patch security vulnerabilities.
- **Use antivirus and anti-malware software:** Install and regularly update antivirus and anti-malware software on all devices connected to the network.
- **Secure your router:** Change the default admin login credentials and update the router's firmware.
- **Physically secure your network hardware:** Ensure that routers, servers, and other network devices are in a secure location.

4. Employee Training and Awareness:

Train employees on cyber security best practices: Educate employees about phishing scams, password security, and other common threats.

Promote a culture of security awareness: Encourage employees to be vigilant and report suspicious activity.

5.Regular Security Monitoring:

- **Monitor network traffic for suspicious activity:** Use network monitoring tools to detect and respond to potential threats.

To monitor network traffic for suspicious activity, you can use tools like Wire shark, Net flows or Intrusion Detection Systems (IDS) to analyze traffic patterns, identify anomalies, and detect potential threats, such as malware or unauthorized access attempts)

Network Security

1. Use strong passwords.
2. Keep Patch updated.
3. Turn on encryption.
4. Use a VPN.
5. Use multiple firewall.
6. Rename routers and networks.
7. Turn off the WPS setting.
8. Make Data Backup Regularly

1.Use strong passwords: Ensure your passwords are complex (a mix of letters, numbers, and symbols) and long (at least 12-16 characters). Avoid using obvious information like birthdays or common words.

2.Keep everything updated: Regularly update your operating system, software, and apps to patch vulnerabilities and stay protected from the latest threats.

3.Turn on encryption: Use encryption protocols like SSL/TLS for websites and AES for files to keep your data secure from hackers. Encryption turns your data into an unreadable format that can only be decoded by someone with the correct decryption key.

4.Use a VPN: A VPN (Virtual Private Network) encrypts your internet connection and hides your IP address, making your online activity more secure and private, especially on public networks.

5.Use multiple firewalls: Firewalls can monitor incoming and outgoing network traffic. Having both hardware and software firewalls provides an extra layer of protection from unauthorized access.

6.Rename routers and networks: Change the default name (SSID) of your router and wireless networks to make it harder for attackers to target your devices.

7.Turn off the WPS setting: Wi-Fi Protected Setup (WPS) can be a vulnerability because it allows attackers to crack your Wi-Fi password through brute force. Disabling WPS can prevent this security risk.

8.Make data backup regularly: Regularly back up your important files and data to ensure you can recover from unexpected events like hardware failure or malware attacks. Use cloud storage, external drives, or automated backup solutions.

Up Coming Training Calendar- May - 2025

Training Name	Date	Time	Fees	Mode
LEAD AUDITOR TRAINING ISO 9001:2015	12TH TO 16TH MAY 2025	10.00 am to 5.00pm	17000 + 18% GST	Online
INTERNAL AUDITOR ISO 9001:2015	20TH & 21TH MAY 2025	10.00 am to 5.00pm	7000 + 18% GST	Online
INTERNAL AUDITOR ISO 45001	3OTH & 31ST MAY 2025	10.00 am to 5.00pm	7000 + 18% GST	Online

Word Search

G	G	C	O	A	R	A	N	H	I	A	S	W	M
E	B	Y	A	P	O	Y	O	R	A	R	T	G	A
P	Y	B	E	N	E	D	E	T	G	C	I	A	L
T	N	E	D	N	S	E	O	R	R	K	K	V	W
P	E	R	A	W	M	O	S	N	A	R	T	E	A
E	S	E	T	O	X	O	G	R	N	S	O	V	R
N	S	S	G	N	I	F	F	I	N	S	O	I	E
T	P	P	S	P	Y	W	A	R	E	N	R	R	W
E	O	I	W	H	I	T	E	L	I	S	T	U	G
S	N	O	T	O	G	N	I	F	O	O	P	S	G
T	I	N	S	P	H	I	S	H	I	N	G	S	F
I	S	A	N	D	B	O	X	I	N	G	C	I	A
N	N	G	S	P	E	N	A	J	O	R	T	G	I
G	P	E	R	O	K	E	Y	L	O	G	G	E	R

CYBERESPIONAGE
HACKER
ROOTKIT
TROJAN
SPYWARE
RANSOMWARE
SANDBOXING
SNIFFING
VIRUS
PEN-TESTING
SPOOFING
WHITELIST
MALWARE
KEYLOGGER
PHISHING

May Month Birthday's- 2025

Sr. No.	Emp. Name	Station	Emp. Dob
1	Ankur Mathur	Udaipur	01-May
2	Mohammad Rafi Ahmad	ICS-ONGC-Mehsana	01-May
3	Naim Zikare	Mumbai-CertCell	01-May
4	Sharique Ahmad	ICS-ONGC-Bokaro	02-May
5	Faisal Khan	ICS-VENDOR	02-May
6	Pabitra Debbarma	ICS-ONGC Tripura	02-May
7	Prakathees Kumar	ICS-ISRO Coimbatore	02-May
8	Prem Kumar Poddar	ICS-IGL New Delhi	02-May
9	Jugendra Singh	ECD-ADANI TCP RJ	03-May
10	Vidyadhar Sane	ICS-PNGRB	04-May
11	Vilas Krishna Patere	Mumbai-InspCell	04-May
12	Rajendra Kumar	ICS-ONGC-Rajahmundry	04-May
13	Shuvendu Bhusana Dash	Mumbai-ECD	04-May
14	Brijeshkumar Galoliya	ICS-ONGC-Mehsana	05-May
15	Sanchi Gamare	ICS-Assure - Reconstruction	05-May
16	Babu Ram .	ICS-IOCL Shutdown	06-May
17	Nileshkumar Prajapati	ICS-ONGC-Offshore	06-May
18	Rithiksha .	ICS-Assure - Reconstruction	06-May
19	Mohtashim Ali Sayyed	ICS-MGL Steel	06-May
20	Rajesh	Training centre	07-May
21	Mehulkumar Baldevbhai Patel	Ahmedabad	08-May
22	Mohammad Shahid	ICS-IGL New Delhi	08-May
23	Ajeet Singh	Mumbai-ECD	08-May
24	Pankaj Singh	ECD-HPCL-MDPL-Coating & Integrity Survey	10-May
25	Arvind Kumar	ICS-IGL New Delhi	10-May
26	Kunal Kumar	ICS-ONGC-Ankleshwar	10-May
27	P. Sakthi Thalavai	Mumbai-InspCell	10-May
28	Angad Yadav	ECD-Gail Survey	11-May

May Month Birthday's- 2025

Sr. No.	Emp. Name	Station	Emp. Dob
29	Kiran Jadhav	Mumbai-Finance	12-May
30	Harish Shinde	ICS-MNGL-Pune	12-May
31	Khilji Mahammadsafik	ICS-ONGC-Ankleshwar	14-May
32	Dinesh Chavan	ICS-Assure - Reconstruction	15-May
33	Sujit Roul	ICS-Reliance Ro Project	15-May
34	Dipali Kumbhare	ICS-Assure - Forensic	16-May
35	Matla Mohana Ramesh	ICS-IOCL RO South	16-May
36	Venkata Vijayaraju Gollapalli	ICS-ONGC-Rajahmundry	16-May
37	Kiran Vilas Bhanushali	ECD-MGL	16-May
38	Ashvi Valand	Gandhidham	18-May
39	Aanchal Sunil Chhabria	Mumbai-CO	19-May
40	Abhishek - Pathak	ICS-ONGC-WADU	19-May
41	Pratibha Nishad	Mumbai-Finance	19-May
42	Rajesh Kumar Prasad	ICS-Lakshya Powertech	20-May
43	Dinesh Kumar Yadav	ICS-Reliance Ro Project	20-May
44	Dipti Lakhe Chawade	Mumbai-CertCell	20-May
45	Sheetal Sundarlal Kataria	USA	23-May
46	Abishek Pushpa	Chennai	24-May
47	Makwana Chndrakant	ICS-ONGC-Mehsana	24-May
48	Mohd Khalid Khan	ICS-ONGC-Mehsana	25-May
49	Nikhil Adangale	Nasik	25-May
50	Prakash B. Agri	Mumbai-Admin	25-May
51	Som Dhanbir Thapa	Mumbai-Finance	25-May
52	Ajay Prakash Bhoir	ECD-Gail Survey	26-May
53	Arun R	ICS-ONGC-Offshore	26-May
54	Anik Deol	ECD-GAIL-HVJ-SURVEY	27-May
55	Rajendra Bhalerao	ICS-VENDOR	28-May
56	Kimaya Kadolkar	ICS-Assure - Property	29-May

Horoscope Month of April - 2025

Aries

Feel the energy surge and begin with your new efforts now. Your leadership side will be vastly emphasised, making this a good time for taking control of situations. Work upon self; some improvement needs to be done, fitness routines, or skill development. Be mindful not to cross the line between assertiveness and aggression. Direct this energy toward the right initiatives, and you will find that others will draw inspiration from you as you set out on your journey toward personal growth. Grab that opportunity now.

Taurus

It's the right time to delve deep into the subconscious mind, explore your dreams, and confront those hidden fears and anxieties that have been holding you back. You will feel a strong call to retreat and recharge; follow that call. Take some time to be alone and discover your inner self. Meditation, or connecting with nature, will also be beneficial during this time. It is an excellent time for closure and healing, so you may want to consider letting go of some past grievances. By the end of this month, aim to emerge refreshed and spiritually renewed, ready to face the world with a clear mind and heart.

Gemini

Gemini, shift your focus towards social ties and community involvement. It's the perfect time to broaden your horizons-gather within yourself with like-minded others or causes of inspiration; use this time to build your social network. You may be presented with opportunities that allow you to form significant connections with people who could be important later on. Boost cooperation and teamwork- your ideas can really gather steam through shared effort. Consider how hopes and dreams fit into a larger picture. This is a good time to reassess your goals and align them with social networking again.

Cancer

Career and public image take center stage this month. There is great potential for growth and recognition now, so take every opportunity to prove your skills and commitment. This month shines a spotlight on your career ambitions, so it's best to either stop and think through your long-term career goals logically or make some stronger present moves toward them. The presence of authority figures and mentors may be quite strong, so remember to be professional and receptive. It will also be talked about how your career coincides with your values; being real will be a major boost.

Leo

Leo, you carry the spirit of adventure and learning within you this month. It is beneficial for you to broaden your perspective through travel, education, or even the consideration of new philosophies. This is a great opportunity to go beyond what you normally do and experience the unfamiliar. Consider taking a course that piques your interest or planning a trip to a place you've always dreamed of visiting. Your quest for knowledge will lead you not only into new personal growth but also into new opportunities in life and work.

Virgo

Virgo, this month signals a time for transition and serious soul-searching. Here, you will experience some of the most interesting themes in the transformation of your life, including personal and intimate relationships, joint finances, and personal development. You may have to manage your partner's finances. It's a time for introspection and self-renewal. Reflect on what habits or fears need to be shed to move forward. This is a fine time to heal, making the most of the transformative energy to take those significant steps in personal growth.

Horoscope Month of April - - 2025

Libra

Libra, relationships and partnerships are in focus this month. Your ability to forge deep connections with others, both in business and personal matters, is enhanced during this month. It's a great time to solidify existing relationships and perhaps consider forging new ones. Communication is the key: be open, truthful, and strive to compromise for the sake of harmony. Take the time to first understand others and their needs before presenting your own. Legal or contractual matters may also be subject to examination during this period; therefore, proceed with extra caution and diligence.

Scorpio

The month is the most active time of the year for reflecting on and changing habits into more favorable and productive forms. Diet alterations, setting up a workout schedule, and cleaning your workspace may seem small, but they make a huge difference in achieving healthy living. It is possible to have opportunities to work more efficiently and develop skills. Take care of duties and health. As you surround yourself with discipline and mindfulness, you will attain new heights in both physical health and productivity at work.

Sagittarius

It's time for self-expression and indulging in activities you love. Art, romance, or leisure - it's time to unleash the child in you and let them jump and play. This is also a wonderful time for romance, where either new passions or rekindled old flames flourish again. Get involved in what excites you or try some new creative endeavor. This is also a great period for joyful fun with children or indulging in things that are typically child-like. Enjoy this playful phase, Sagittarius, enjoy the atmosphere for being light and bright, and you will attract equally bright experiences!

Capricorn

This month, attention shifts toward home and family, nurturing the other half of your life. During this period, you are offered the chance to strengthen ties with loved ones and attend to some household matters. Ensure that you work towards making your home feel comfortable and safe, which will enhance your overall well-being. Additionally, now is a great time for reflection on your roots and heritage, or the security you derive from your family ties. On the emotional side, this may involve any form of grounding, bringing insight and focus to any unresolved issues that may be buried within the family's tapestry.

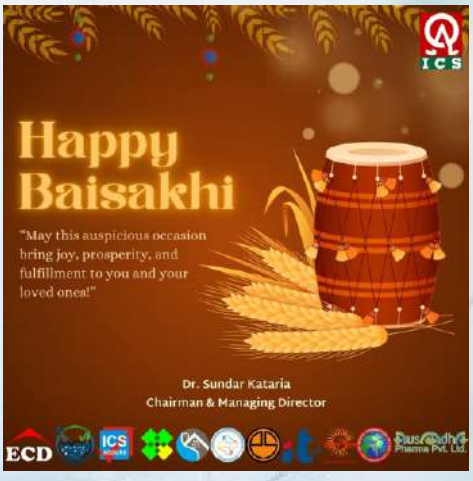
Aquarius

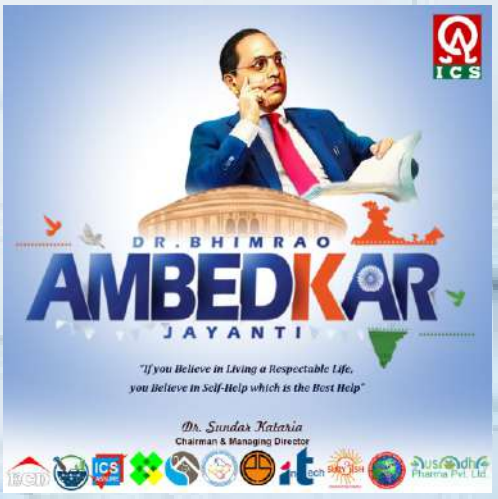
This month, Aquarius, communication is your forte! Therefore, expect a lot of interactivity, ranging from the buzz on social media to serious conversations with neighbours or siblings. It's a prime time for any learning, teaching, or sharing of knowledge. Participate freely in talks or take that short trip to kick your mind into gear and connect with others. Your mind might become carried away with picking up new hobbies or skills that enhance your perception of the world around you. Additionally, articulating thoughts comes easily at this time, making it an ideal period for writing, speaking, or any form of communication.

Pisces

The month will be about finances and personal values. The entire time corresponds to inventorying all resources, including income, savings, possessions that comfort and secure lives. This is an ideal approximation of your budget and financial plans for moving forward, ensuring they align with the current needs and future aspirations. You may even want to consider discovering new sources of income or managing your possessions more effectively. Consider what is truly important to you, not just in a material sense, but also in terms of personal satisfaction, and cultivate a sense of gratitude for what you have.

ICS Festival Greeting





suryaansh

Training & Convention Center (Residential), Palghar, Maharashtra.

About Us

Nestled near Mumbai, in the serene surroundings of Palghar, Suryaansh Training & Convention Center stands as an epitome of luxury and tranquility, offering an unparalleled experience that caters to your every need, whether you're seeking a serene getaway or planning a grand event.

At Suryaansh, we believe that every journey deserves a touch of luxury, every stay should be unforgettable, and every traveller deserves seamless experiences. We are your premier destination for hotel bookings, committed to transforming your travel dreams into reality. Established with a passion for hospitality and a commitment to excellence, Suryaansh is a leading name in the travel industry, with a team of dedicated professionals deeply passionate about curating exceptional travel experiences.








Vision:

"Our vision at Suryaansh is to be Your Gateway to Memorable Stays", where every journey is imbued with luxury, every stay is etched into memory, and every traveller experience seamless excellence. As your premier destination for hotel bookings, we are committed to transforming your travel dreams into reality. At Suryaansh Training & Convention Centre, we extend this vision to become the ultimate destination for events, training programs, and leisure getaways, setting new standards of excellence in hospitality and service."

Mission:

"Our mission at Suryaansh is simple yet ambitious: to redefine the way people travel by providing unforgettable experiences through world-class facilities, impeccable service, and a commitment to excellence in everything we do. We are dedicated to leveraging cutting-edge technology and innovative solutions to streamline the booking process, enhance convenience, and elevate the overall travel experience for our guests. With a relentless focus on customer satisfaction and continuous improvement, we strive to set new standards of excellence in the travel industry."

www.suryaansh.org

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