NATIONAL SECURITY DATABASE

Empanelment for NSD Certified Penetration Tester Certification (NCPT)

EXAM OUTLINE

Information Guide

Non-Discrimination

The National Security Database, managed by Information Sharing and Analysis Center is restricted to Indian Citizens. ISAC does not discriminate against candidates based on the basis of religion, race, ethnicity, sexual orientation, age or disability. Please contact ISAC if you need further information on the non-discrimination policy.

Contents

About National Security Database

National Security Database (NSD) is a prestigious certification program from Information Sharing and Analysis Center (ISAC), a Public Private Partner (PPP) with National Critical Information Infrastructure Protection Center (NCIIPC), under Prime Minister's Office, Government of India. NSD is awarded to credible & trustworthy Information security experts with proven skills to protect the National Critical Infrastructure & economy of the country.

About Information Sharing and Analysis Center

A non-for-profit body, Information Sharing and Analysis Center (ISAC) is India's leading non-profit foundation committed to securing the cyber space of the nation by providing credible platforms for Information Sharing & capacity development.

Why join the National Security Database

With 300,000 plus jobs available in India alone, it is increasingly becoming difficult for companies to find good cyber security professionals. Organizations no longer want to trust professionals who become "ethical hackers" by simply passing an online objective based exam, as they seldom have the real world perspective and confidence to execute the job once given. Professionals with incomplete knowledge are not only putting their organization at risk, but also their Nation, as they handle sensitive projects impacting the economy of the country.

The National Security Database is the only not-for-profit program, well recognized and respected by various Corporate and Government organizations for its stringent process and hands-on lab exams for assessing the credibility of a professional.

When you pass the rigorous lab exams from National Security Database, you not only prove your credibility and skills, but also enter the elite database of chosen professionals in India who are the first preference by the law enforcement, corporate and multiple Government organizations for cyber security jobs and sensitive positions.

The domain requirements have been carefully chosen after extensive survey of the business need and reflect the latest skills needed by the Corporate Industry.

Power of Clean Exit

Professionals who become part of the National Security Database undertake an oath for "Clean Exit", attesting to the truth of their assertions regarding professional experience, academic background and legally committing to the adherence of the ISAC code of Ethics at all times.

Professionals who violate the code of ethics have the risk of getting their empanelment revoked permanently by National Security Database, in addition to having their profile marked in a central database shared in the Industry. This will mean increased difficulty in getting another job!

Benefits of Professionals

1. Gain recognition for your skills from the National Security Database
2. Exclusive access to Priority Job reference Network
3. Up to 3 Job Interviews on passing NSD Lab exams
4. Get connected with local law enforcement and Intelligence agencies to support them in various Cybercrime and related cases

5. Qualify to participate in exclusive cyber security projects open only for National Security Database professionals by various Government of India organizations
6. Network with elite cyber security professionals and hackers in India
7. Special benefits for entrepreneurs for start-ups in Information Security domain

Benefits for Employers

1. Hands-on proven skills recognized by National Security Database mean less time in training and faster "business ready" professionals
2. Hire with Confidence - Minimize your risks as you always hire the right people with right skills
3. Clean Exit Program empowers your business and ensures peace of mind as candidates will not risk violating the code of ethics
4. Provides increased credibility for your organization when working with vendors, contractors and government organizations
5. Guaranteed discounts on Training and security events across India for your IT staff, supported by ISAC

About the Domain

Penetration testing domain from NSD is a recognized empanelment program for information security professionals with hands-on proven experience in vulnerability analysis and penetration testing. The domains test a candidate’s skill, approach and knowledge that can provide an organization with a reliable workforce for detection and mitigation of cyber security threats in a timely manner.

The program is a **foundation** for many other job roles including Security Information and Event Management (SIEM), Computer Forensics, Web Application Security, ISO 27001 Compliance, PCI-DSS, Internal IT Security Audit etc.

Domains Covered

1. Ethics and Culture
2. Enterprise Security Challenges
3. Information Gathering
4. Introduction to Social Engineering
5. Systems Security
6. Password Hacking
7. Viruses and Trojans
8. Network and Web Application Security
9. Exploiting Approaches

The NCPT certification is constantly updated with new techniques and approaches.

Ethics and Culture

Understanding the ethics and culture behind the motivation and behaviour of hackers and security researchers is essential to gain the right perspective in not only handling and anticipating security incidents but also respecting the effort of hackers in modernising and securing much of today's technology. The domain tests a candidate's knowledge on the current trend of hacker ethics and beliefs.

The candidate is expected to research on various hacker groups, their language, lingo used, broad activities etc. and understand their motivation. Depending on the exam paper, you may be asked to write a short essay of 300 words during the exam on this subject.

1.1 Ethics and Culture

- 1.1.1 Overview of hacking history - Understand the evolution of hacking
- 1.1.2 Hacker Culture - Understand how hacker culture has evolved over time
- 1.1.3 Open Source - Understand difference between open source and closed source

1.2 Moral debate: Ethics

- 1.2.1 Social and political impact - Understand social and political impact of disclosures by hackers and discuss ethics
- 1.2.2 The need of hacking - Question and understand the need of hacking and its value towards technology progress and security
- 1.2.3 Research emerging trends in Hacker Ethics

1.3 Defining a system

- 1.3.1 Understanding Workflow - Understand how a given organization and a business workflow in it functions
- 1.3.2 People, Process and Technology - Understand key concepts of how people, process and technology impact a system
- 1.3.3 Knowing your enemy - Evaluate and identify various factors in a system that can compromise security

Enterprise Security Challenges

Running a business is not easy. With high capital costs, manpower costs and maintenance, most organizations focus on ensuring they are able to market and sell their services and products in a profitable manner. With thin profit margins, Information security and its associated costs is always the last aspect of investment.

Even as organizations do invest in Information security, there are multiple internal challenges of skilled manpower, limitations of resources, time consuming processes and funds. There is always an opportunity to make mistakes that can compromise the organization network and it's sensitive information by a persistent attacker.

The objective of this domain to make the candidate realise that it is always possible to hack any organization, no matter how big or small.

The exam may cover questions pertaining to planning of budget for securing an office, planning resource allocation and their time schedule across a week or month and approach in handling senior management with security policies.

2.1 Enterprise Security Challenges

- 2.1.1 What happens in a real company? - Understand budget constraints and investment challenges for organizations in security
- 2.1.2 Myth of people-ready business - Understand the challenges of skilled manpower in business
- 2.1.3 Skilled professionals – are they watching? - Understand utilization of skilled resources in security, priority activities of business
- 2.1.4 Products – who pushes them? - Understand general sales process, decision making of CIOs and role of Managed services provider
- 2.1.5 Running on a Scaffold! - Understand financial challenges in sustaining a business or a project and its impact on security

2.2 Management Challenges

- 2.2.1 Users Vs Administrators - Understand basic psychology and approach of users vs administrators for security in a company
- 2.2.2 Technology Vs Management - Understand management perspective on investment in technology for business
- Security budget across different verticals - Understand key perspectives of management on provisioning security budget for different business verticals in an organization
- 2.2.3 Who's got that access now? - Discuss and understand how security policies are implemented for various users, departments, branches, vendors etc in an organization
- 2.2.4 Watching for patterns and activities - Discuss how security activities are handled by an organization depending on security budget, skilled manpower, vendor guidance, new hires, incident response and patch deployment etc

2.3 Security concerns

- 2.3.1 Insider trading - Understand risks of Insider Trading
- 2.3.2 Employee attrition - Key challenges faced by organizations when employees leave the company with critical knowledge and data
- 2.3.3 End Point security - Impact of end point security in data leaks

- 2.3.4 Enterprise wide monitoring - Understand SIEM technologies and its role in detecting and preventing security incidents

2.4 Evolution and Adaption

- 2.4.1 Evolution of business needs - Understand security concerns as business evolves and scales
- 2.4.2 Adapting to change - How challenges faced by companies to adapting practices, implementation, training and processes for security as threats evolve rapidly
- 2.4.3 Why is it always possible to hack? - Understand how even the best and well equipped organizations with latest security technologies can be prone to attacks

Information Gathering

One of the most important skills for a penetration tester, detailed information gathering can often give insight and leads for hard-to-find deployed systems.

This domain, in the context of the examination focuses on candidate’s skill to plan and collect information about a target organization or its assets for effective use in further vulnerability analysis and penetration testing.

The candidate is tested on their knowledge for effectively using search engines such as BING, Google, Shodan etc and documenting their findings for further use.

3.1 Information Gathering

- 3.1.1 Creating a plan - Knowledge of various mind mapping and planning tools to assist in making a plan
- 3.1.2 Designing attack strategy - Creating an approach towards identifying vulnerabilities for a system or a network of an organization
- 3.1.3 Forensic Footprint - Planning an footprint strategy to avoid trace-back and detection by digital forensics

3.2 Information Gathering

- 3.2.1 Footprinting - Footprinting techniques
- 3.2.2 Scanning - Scanning approaches
- 3.2.3 Identifying vulnerabilities
- 3.2.4 Enumerating your target - Enumerating approaches

Proficiency expected with:

- Google and Google Hacking
- Email Harvesting
- NetCraft
- Whois
- Recon-ng
- DNS Enumeration
- Port scanning with NMAP
- NMAP Scripting Engine (NSE)
- SMB Enumeration
- SMTP Enumeration
- SNMP Enumeration

Social Engineering

From making a phone call to an unsuspecting employee for gathering sensitive information to sending a legitimate looking email to hack accounts, Social Engineering is one of the most successful techniques used by the attackers against their targets.

We look at how hackers exploit love, faith, belief, trust, anger, hatred, generosity etc. for their gains and advantage by social engineering.

Some of the questions expected in the lab exam include drafting an email to a target for gaining trust, crafting a phishing mail, approaches for using social media to gain credibility or proving their story to a possible victim etc.

4.1 Introduction to Social Engineering

- 4.1.1 Understanding your targets - Basic approach in understanding your targets
- 4.1.2 Character analysis - various approaches of character analysis
- 4.1.3 Body language - basic body language techniques
- ‘4.1.4 Blink’ factor - discussion on instinct and judgement on your targets

4.2 Using SMS, Facebook and Online Chat for effectively gaining trust

- 4.2.1 How SMS, Facebook and has taken over our lives - discussion on impact of various social communications
- 4.2.2 How to craft an emotion - Using words, spaces and dots for effective emotional exploitation
- 4.2.3 Finding the right words - Using online dictionaries for communicating with right words
- 4.2.4 Chat addiction - Making a person attached to you on chat
- 4.2.5 Exploiting targets - Using the art effectively for gaining information
- 4.2.6 Possible Psychological damage - Discussion on possible psychological damage and concerns
- 4.2.7 Not crossing the line - discussion on what not to say or discuss

4.3 Scripting in daily life

- 4.3.1 Games people play - Suggested reading of the book "Games people play"
- 4.3.2 Transactional Analysis - How can it help in networking and information gathering
- 4.3.3 Introduction to Reality Hacking - Concept of reality hacking

4.4 Reality Hacking

- 4.4.1 Understanding reality hacking - Introduction and larger concept application
- 4.4.2 Weakest link in security - exploiting people
- 4.4.3 Application in real life - how "everything" around you can be used for hacking

4.5 Exploiting Religion and Occult Science

- 4.5.1 People and belief - Discussion on what is god, belief and religion
- 4.5.2 How religion plays a big role - Importance of religion in peoples lives
- 4.5.3 Understanding occult science - Brief introduction to occult science and what people believe
- 4.5.4 Astrology and daily life - How astrology impacts daily lives of people and their decisions
- 4.5.5 Faith - How to exploit faith for hacking
- 4.5.6 How to get personal information - Getting personal information in the name of god
- 4.5.7 Bluff master: How to be a palmist - effectively and instantly getting the secrets of people in your first meeting
- 4.5.8 Playing with the mind - How to induce self-fulfilling prophecies
- 4.5.9 Respecting the science - How not to cross the line

4.6 Into the Mind: Inflicting damage

- 4.6.1 Introducing hope - exploiting greed and success and fun and profit
- 4.6.2 Attachment in Adults - exploiting relationships for fun and profit
- 4.6.3 Turning people against each other - exploiting the weakest link
- 4.6.4 Phishing god - Using phishing and spam based on information gathered
- 4.6.5 Knowing your target - Crafting mails and messages to lure people

Systems Security

Finding vulnerabilities in systems and compromising them is a key skill for a successful penetration tester. This can be done best by professionals who understand the systems and their workings in detail. The domain focusses on various offensive attacks to bypass systems security.

From the context examination, the candidate will be tested for technical competencies on using various offensive tools and their approach to compromise a system. Information Security professionals must constantly upgrade their knowledge in this domain.

5.1 Systems Security

- 5.1.1 Introduction to systems
- 5.1.2 Group Discussion: Windows vs Linux vs Mac
- 5.1.3 Assignment: Active Directory Fundamentals
- 5.1.4 Hiding Data – NTFS streaming

5.2 Offensive attacks

- 5.2.1 Gaining root access
- 5.2.2 Privilege Escalation
- 5.2.3 Man in the Middle attacks
- 5.2.4 Finding Vulnerabilities
- 5.2.5 Using Exploits

5.3 Wireless security

- 5.3.1 The 802.11 network
- 5.3.2 Wireless security standards
- 5.3.3 WEP and inherent vulnerabilities
- 5.3.4 Sniffing Wireless networks
- 5.3.5 Breaking WEP
- 5.3.6 Breaking WPA
- 5.3.7 Wireless security – Best practices

Proficiency expected with:

- Vulnerability scanning with Nmap
- The OpenVAS Vulnerability scanner
- Fuzzing basics
- Buffer overflows
- Privilege escalation tools
- Wireless hacking tools

Password Hacking

Passwords are the basic form of protection used by network devices and systems for allowing access to resources. Each system or technology may employ a different approach for using and managing passwords for access control and hence a strong knowledge of various password hacking techniques is crucial for security professional conducting an assessment.

Some of the areas covered in this domain include use of steganography, rainbow tables, decrypting password hashes, using brute force techniques etc. The candidate may be assessed for their skills in using the right approach to gain passwords for a system in a limited time.

6.1 Password Hacking

- 6.1.1 Secret of passwords
- 6.1.2 Group Discussion: Do you use the same passwords everywhere?
- 6.1.3 Case study: Most common passwords used
- 6.1.4 Team activity: Using online hash crackers
- 6.1.5 Attacking Windows system password
- 6.1.6 Attacking a Windows Server Domain Controller Password
- 6.1.7 Attacking Linux system password
- 6.1.8 Attacking Application passwords

6.2 Other approaches

- 6.2.1 Using Brute Force Tools
- 6.2.2 Steganalysis concepts
- 6.2.3 Using Rainbow Tables
- 6.2.4 Default Passwords of devices
- 6.2.5 Using Key loggers
- 6.2.6 Case study: Impact of default passwords on security
- 6.2.7 Team activity: Password recovery tools

Proficiency expected with:

- Brute force tools
- Using dictionary files
- Pwdump
- Fgdump
- Hydra
- Medusa
- Ncrack
- John the ripper
- Rainbow tables
- Keyloggers

Malwares

Malwares are the most prized weapons of attackers as they provide extraordinary capabilities in accessing infected systems and networks. With over a million new malware variants released every six months on the internet and a few dozen anti-virus companies to defend against them, the battle among the enterprise and the attackers is constantly increasing in complexity.

A good understanding of various malwares such as viruses, Trojans, worms, rootkits, botnets etc is essential to allow a professional in handling a compromised system. While use of malwares in a penetration testing assignment is unconventional, it should not be prohibited as it is the only way to test the effectiveness of deployed anti-measures.

The examination involves testing a candidate's skill and knowledge of handling a malware and using them for effectively compromising systems.

7.1 Viruses and Trojans

- 7.1.1 Group Discussion: How would you define a malware?
- 7.1.2 Introduction to malwares
- 7.1.3 Team activity: List the features will you look in a malware if you have to use it
- 7.1.4 What are Malwares?
- 7.1.5 Building a Trojan
- 7.1.6 Binding a Trojan to another file
- 7.1.7 Approaches for deploying a Trojan
- 7.1.8 Using Bit-torrent to spread Trojans
- 7.1.9 Targeting Victims by Games and movies

7.2 Worms

- 7.2.1 Anatomy of a worm
- 7.2.2 Worm propagation process in a network
- 7.2.3 Defense against worms
- 7.2.4 Worm Propagation possibilities in IPv6!

7.3 Rootkits and Botnets

- 7.3.1 Target Harvesting
- 7.3.2 Rootkits and Botnets
- 7.3.3 Case study: How botnets work?
- 7.3.4 Team activity: Find most popular malwares impacting the mobile platforms.
- 7.3.5 Rootkits infection techniques
- 7.3.6 Task: Analysis of a Malware.

Network, Web Application and Social Media Security

Denial of service attack is the most common form of network attack used by attackers to voice their protest or take down an organization. As a penetration tester, it is important to test how vulnerable an asset or a network is from this attack. From the context of examination, a candidate may be tested for their knowledge of such attacks and countermeasures commonly used.

This domain also covers Web application security and the candidate is expected to be well versed with OWASP Top 10 attacks with hands-on experience. The examination includes detailed testing of skills in web application hacking and security.

8.1 Network and Web Application Security

- 8.1.1 Conduction Basic DOS Attack
- 8.1.2 DDoS Attacks
- 8.1.3 Group discussion: DoS attacks impacting organizations
- 8.1.4 Targeting Firewalls and Routers
- 8.1.5 Defense - Clustering and NLB

8.2 Honeypots, Sniffing and Session Hijacking

- 8.2.1 Honeypots Overview
- 8.2.2 Deploying Honeypots
- 8.2.3 Sniffing Networks
- 8.2.4 Encryption - overview
- 8.2.5 Session Hijacking tools

8.3 Web Security

- 8.3.1 Using data from Information gathering activity for attacks
- 8.3.2 Attacking web applications
- 8.3.3 Team Activity: Setting up Wordpress on localhost
- 8.3.4 Group discussion: what mistakes can affect web application security?
- 8.3.5 Web server Security
- 8.3.6 Top 10 threats to Web Applications
- 8.3.7 Basic Authentication Attacks
- 8.3.8 SQL Injection & Cross site scripting
- 8.3.9 LFI / RFI
- 8.3.10 Advanced Google search techniques

8.4 Social Media, Politics and Hacking

- 8.4.1 Use of Social Media for news and updates
- 8.4.2 Importance of Social Media in opinion formation

- 8.4.3 Case Study: Politics and use of social media
- 8.4.4 Misleading people using Social Media
- 8.4.5 Manipulating search engine rankings

Proficiency expected with:

- Cross site scripting (XSS)
- File Inclusion Vulnerabilities
- MySQL SQL Injection
- Automated SQL Injection Tools
- OWASP Top 10
- Using Honeypots
- DDOS Attacks
- Session Hijacking tools

Exploiting Approaches

This is the most advanced and important domain in examination. From using a remote exploit to a local exploit, the skill mostly allows the attacker to gain administrative access to the targeted system.

The examination includes testing of pivoting skills, using metasploit, compiling and running exploits, using zero days etc. The approach of the candidate in their choice of exploit and use is also ranked.

9.1 Exploiting Approaches

- 9.1.1 Introduction to Shellcodes
- 9.1.2 Using exploit-db effectively
- 9.1.3 Metasploit - The Big Daddy
- 9.1.4 Introduction to msfencode/msfpayload
- 9.1.5 Manual Shellcode Writing and Automatic Shellcode Generation

9.2 Advanced Exploitation

- 9.2.1 Client Side Exploitation Techniques
- 9.2.2 Concept of tunneling and techniques
- 9.2.3 Evading Firewalls by hopping through the tunnels using proxy servers
- 9.2.4 smb fun – windows and linux
- 9.2.5 Anti Virus Evasion

Proficiency expected with:

- Port forwarding / redirection
- SSH Tunneling
- Proxychains
- Using Metasploit
- Metasploit payloads
- Building custom MSF modules
- Evading anti virus

NSD Exam Format

The total time for all National Security Database Examinations are eight hours, including scheduled and unscheduled breaks. For your understanding, the following general schedule is provided:

Start Time	End Time	Activity	Information
10:00	12:30	Written Exam (300 Credits)	This exam is also known as the Associate level and consists of approximately 100 questions on concepts, theory and fundamentals of the related domain.
12:30	13:00	Viva (100 Credits)	A personal interview testing your confidence, language skills, approach to technical challenges and analytic abilities.
13:00	14:00	Lunch Break	Candidate must have lunch / food within the exam premises
14:00	17:00	Lab Exam (600 Credits)	Capture the flag styled lab exam where you are required to finish various real-world security challenges in a time-bound manner.
17:00	18:00	Report Submission	You may be required to submit reports or answers in specific report formats. This hour can be utilized by you for completing the same.

The candidate has to submit minimum 300 CPEs every year to maintain their professional empanelment in National Security Database.Please check the official website on various ways to earn CPE Credits.

Sample Exam Questions

Theory (Written Exam) Sample

1. Submit a one page write-up (300 words maximum) on your view of Aaron Swartz case, hacker culture and its importance.
2. Is Security a cost Center? Provide Justification for your views. (Maximum 300 words)
3. What are the drawbacks of ISO 27001? Provide your top 3 points in brief. (Maximum 300 words)

Lab (Hands-on Exam) Sample

1. Provide a detailed vulnerability analysis report (no automated tools allowed) for the IP address 10.7.4.2
2. For the web application hosted on 10.7.4.8, find all the possible ways to exploit it successfully. Document your findings.
3. Conduct a detailed security assessment for the smart TV provided using only open source tools. Provide a detailed report for your approach and findings.

Viva (Personal Interview)

1. You have caught an employee downloading movies using bit torrent. How will you deal with the incident?
2. Your team member is quitting the company and has just informed you that he has copied sensitive data for his personal use. What will you do?
3. You are giving a closing presentation of your web application vulnerability analysis report to the company board and CISO. What will you NOT share or avoid stating during the presentation?

Registering for the Exam

This section describes the process for registration of NSD Examinations. The exam is conducted at the official exam centers located and can be booked online from the website www.isac.io

Step 1: Register for the examination at www.isac.io

Step 2: Select the most convenient exam center

Step 3: Select an appointment time and date for exam

Step 4: Pay the exam fees online

Step 5: Receive a confirmation mail from ISAC with the appointment details, test center location and relevant instructions, if any.

Fees

Please visit the National Security Database website www.isac.io for the most current examination registration fees.

Rescheduling or cancellation of a testing appointment

If you wish to reschedule or cancel your exam appointment, you must contact the National Security Database helpline 72 hours before the exam date or by writing an email to support@isac.io with your request.

Rescheduling charges are INR 3000 and there are no refunds for cancellation of appointment.

Late Arrivals and No shows

If the candidate does not arrive within 30 minutes of the scheduled exam staring timing, the candidate's exam fee will be forfeited.

What to bring to the exam center

Proper Identification

The following Photo Identification documents are accepted:

1. PAN Card (must be same as submitted during exam registration)
2. Aadhar Card
3. Passport

Please note that the ID should match with the exact name given during exam registration. All documents presented at the exam center must be original. Candidates whose names do not match or who fail to proper valid identification may be asked to leave the exam center and their exam fees will be forfeited.

Day of the Exam

Plan to arrive at the exam testing center at least 30 minutes before the scheduled testing time. If you arrive more than 30 minutes late to your scheduled appointment, you may lose your examination appointment.

For checking-in:

1. You will be required to present an acceptable form of identification.
2. You will be asked to have your photograph taken.
3. You will be required to leave your personal belongings outside the testing room. Secure storage will be provided. Storage space is small, so candidates should plan appropriately. The exam center or the staff do not assume any responsibility for candidates' personal belongings.
4. The Exam Moderator (EM) will escort you to a computer terminal. You must remain in your seat during the examination, except when authorized to leave by test center staff.
5. You may not change your computer terminal unless an exam moderator directs you to do so.
6. Raise your hand to notify the EM if you
   a. Believe you have a problem with your computer.
   b. Need to take a break.
   c. Need the administrator for any reason.
7. Total examination time includes any unscheduled breaks you may take. All breaks count against your testing time. You must leave the testing room during your break, but you may not leave the building or access any personal belongings unless absolutely necessary (e.g. for retrieving medication).

Technical Issues

If technical issues arise due to unforeseen circumstances on the day of exam, requiring a reschedule of a candidate's examination, the candidate has an option to reschedule an appointment without an additional fee.

When the exam is finished

Submit your exam answer sheets (if applicable) and provide all associated exam reports on completion of your exam to the Exam moderator. You may be additionally asked to submit the same to a specific email ID or upload the results to a website.

Results Reporting

All NSD Examination results are announced after 15 days from the date of completion of exam.

Retake Policy

Candidates who do not pass the exam in the first attempt will be able to retest after a gap of 30 days. There are no maximum limits on the number of retests.

Recertification by Examination

- Candidates may recertify by examination for the following reasons ONLY;
- The candidate has become decertified due to reaching the expiration of the time limit for empanelment.
- The member has become decertified for not meeting the number of required continuing professional education credits.

Questions?

Please contact us on support@isac.io for any further queries.

Corporate Office:

Information Sharing and Analysis Center

319A, Logix Technova, Sector 132, Noida

Delhi / NCR – 201301

End