THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

ICSI House, 22, Institutional Area, Lodi Road, New Delhi –110003
Phone : 011-45341036/92 email : hr.dept@icsi.edu Website : www.icsi.edu

CAREER OPPORTUNITIES

The Institute of Company Secretaries of India (ICSI) is a statutory body set up under an act of Parliament, the Company Secretaries Act, 1980, to regulate and develop the profession of Company Secretaries in India. The ICSI invites applications for the following posts at its Headquarters at New Delhi/ Noida :-

Name of the Post	**Pay Level as per 7thCPC Pay Matrix (Rs.)**	**Gross Salary per Annum (Rs. in Lakhs)**	**Max. Age (as on 01.01.2024)**	**No. of Posts**
Information Security Officer	Level 12 (78800-209200)	17.62	50 years	01
IT Security Manager	Level 10 (56100-177500)	12.90	40 years	01

Interested candidates must **apply only through electronic application form (Online**) by clicking on the hyperlink provided at the end of this page.

The link shall be active from **31st January, 2024 to 20th February, 2024 (20th February, 2024 is the last date for applying Online.)**

Please use Windows Explorer (6.x, 7.x, 8.x, 9.x, 10.x and 11.x only) or Google Chrome and ensure that JavaScript is enabled for viewing this advertisement. Do not use Mozilla Firefox, Netscape Navigator or any other explorer.

In case you want to take a printout of the application form for your reference, please ensure that your printer is attached to your computer.

Please Note:

(i) Before applying for the above post(s) the candidates should satisfy themselves regarding eligibility criteria required for the said post(s).

(ii) Candidates interviewed for any particular post in the past one year (i.e. on or after 31.01.2023).

- **Will not be eligible** to apply for the same post or for a post at a higher pay scale than the post he/she was interviewed for.

- **Will be eligible** to apply for a different post at the same pay scale or for a post at a lower pay scale than the post he/she was interviewed for.

(iii) **The Cut Off date for all purposes (including Age, Qualifications & Experience etc.) for the posts mentioned below is 01.01.2024.**

(1)	**INFORMATION SECURITY OFFICER** **No. of posts : 1** (for New Delhi/ Noida) **Pay Level as per 7th CPC Pay Matrix** : Level 12 (78800-209200) (Gross Salary per annum – Rs. 17.62 lakhs approx.) **Maximum Age:** (as on 01.01.2024) 50 years **QUALIFICATION** MCA or B.Tech (Computer Science/IT/Electronics) or equivalent with 1st or 2nd Division from recognized Institute / University. **CERTIFICATION:** CISSP / CISA / CISM / PMP **EXPERIENCE** 13 year experience out of which 5 years experience in Senior Executive position **JOB CONTENTS (indicative)** • Professional security management certification. • Minimum of 8 years of experience in a combination of risk management, information security and IT jobs. • Knowledge of common information security management frameworks, such as ISO/IEC 27001, and NIST. • Responsible for establishing and maintaining a corporate-wide information security management program and ISMS to ensure that information assets are adequately protected and will have ownership and overall control of ITC process. • Responsible for discussing the control weaknesses noted from the Information Security audits to local and/or senior management and developing recommendations to address them. • Responsible for maintaining Information Security policies and controls, in addition to application, infrastructure and network security reviews of operations to ensure the security of all Information Security assets. • Responsible for prevention, identification and detection of IT and information security risks over the entire business environment supporting the company's operations and key processes. • Excellent written and verbal communication skills and high level of personal integrity. • Innovative thinking and leadership with an ability to lead and motivate cross-functional, interdisciplinary teams. • Experience with contract and vendor negotiations and management including managed services. • Experience with Cloud computing/Elastic computing across virtualized environments. • Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management program. • Work directly with the business units to facilitate risk assessment and risk management processes. • Develop and enhance an information security management framework.

	• Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services. • Provide leadership to the enterprise's information security organization. • Partner with business stakeholders across the company to raise awareness of risk management concerns. • Assist with the overall business technology planning, providing a current knowledge and future vision of technology and systems. • Strong ability to manage multiple projects with managing time and commitments effectively. • Information Security Management System (ISMS). • Execute audits efficiently including analysis of business data, IT systems and Data Center. • Assist the Head of IT Operations, Infrastructure Manager and the Head of Risk with the planning and scoping of audits. • Complete assigned tasks within specified times and provide concise and timely updates to the management. • Support, manage and enhance the ISMS system including scheduling of audits, reviews and management of documentation. • Carry out a continual improvement process with risk assessments in both methodology and scope by testing and evaluating operational & IT processes and the effectiveness of existing controls (encompassing policies, procedures, and standards). • Identify and clearly define control issues, including root causes. Review and evaluate the adequacy of internal controls and compliance with IT security policies and procedures. • Develop and review policies, controls, and standards where appropriate. • Develop and monitor the Information Security audit schedule. • Regularly interact and communicate with management to discuss the present audit results, gain acceptance and provide advice to remedy the audit issues or weaknesses discovered. • Standardise the reporting format so audit results are communicated to senior management in a consistent fashion. • Develop and maintain professional, credible relationships with key stakeholders (IT, Business & Risk) including relevant third parties and strategic suppliers. • Complete security audits on third parties. • Analyse and correlate information security events to identify appropriate event handling actions. • Assess operational and implementation costs and evaluate them against the potential business impact if the policies and controls are not implemented. • Assess the effectiveness of the measures against security risk management plan. • Develop IT security policy and operational procedures based on information collected. • Develop a documented action plan containing policies, practices and procedures that mitigate the identified risks. • Document information related to IT security attacks, threats, risks and controls. • Establish a standard methodology for performing security tests in accordance with security requirements. • Establish review procedures based on organisation's security risk management plan. • Evaluate effectiveness of current incident response plan against industry good practices.

	• Evaluate response plans periodically to ensure relevance. • Identify threats and risks that are relevant to organisation's operations and systems. • Monitor the effectiveness of action plans in addressing information risks. • Obtain corporate management's endorsement of security policies, standards and procedures by articulating cost and benefits. • Perform comparative analysis of security service performance level parameters against security information sources. • Prepare information security performance report based on results from analysis and correlation of information security events. • Rate and categorise potential security incidents. • Recommend suitable enhancements to improve information security performance. • Review business and security environment to identify existing requirements. • Review security policies, standards, and procedures by considering the threats identified and other information collected. • Test incident response plans periodically to ensure response times and executed procedures are acceptable. (**Note :** Training experience forming a part of the curriculum of any Degree / Diploma will not be counted towards the total experience.)
(2)	**<u>IT SECURITY MANAGER</u>** **No. of posts : 1** (for New Delhi/ Noida) **Pay Level as per 7th CPC Pay Matrix** : Level 10 (56100-177500) (Gross Salary per annum – Rs. 12.90 lakhs approx.) **Maximum Age:** (as on 01.01.2024) 40 years **QUALIFICATION** MCA or B.Tech (Computer Science/IT/Electronics) or equivalent with 1st or 2nd Division from recognized Institute / University. **CERTIFICATION:** CEH/ECSA/OSCP & CCNA/CCNP/MCSE/RHEL **EXPERIENCE** 7 year experience **JOB CONTENTS (indicative)** • Degree in business administration or a technology-related field required. • Implement ISO 27001 framework and Information Security Management System (ISMS). • Develop a complete set of corporate Information Security policies and standards and continually monitoring the information security controls, KRIs/KPIs and technical landscape. • Lead on compliance reviews, certifications and accreditations (e.g. ISO27001, Cyber Essentials, GDPR etc.). • Implement effective and appropriate GRC controls and measures to protect systems and data. • Identify, communicate and manage current and emerging security threats with relevant stakeholders.

	• Develop Information security compliance frameworks, security policies and procedures, where necessary. • Work with business, internal IT and 3rd party vendor teams to promote and adopt security best practices. • Validate IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable. • Work with Security partners, Managed Security Service Provider (MSSP) to conduct and review regular security assessments (Pen tests, Vulnerability scans etc) of vendors and solutions (SaaS, IaaS providers and MSSP). • Comprehensive understanding of Information Security Frameworks (e.g. ISO 27001 and Cyber Essentials). • Monitoring and reporting on compliance with security and data protection policies, as well as the enforcement of policies. • Working knowledge of Security Architecture and potential security issues related to them PaaS, IaaS, SaaS and understanding of IAM, and Data Loss Prevention in a Microsoft Azure, AWS etc. environment. • Knowledge of security technologies such as IDS/IPS, vulnerability testing and Firewalls. • Familiar with HMG Security Policy Framework requirements and Government Security Classifications. • Knowledge of security tools, technologies and best practices. Experience in Information Security domain that include Vulnerability Assessment, Penetration Testing off IT Infrastructure and application used • Experience of carrying out System and network wide Vulnerability Assessment to assess the security level of systems and network devices at client's networks. • Experience of Manual configuration review of Security Devices (Firewall, IDS, IPS etc.), Network Devices (Router, Switches), Servers and Systems • Experience of carrying out Penetration Testing of System and network devices accessible from the internet or configured with Public IP Addresses at client's networks. • Knowledge of Web/Mobile / cloud-based Application Security Testing based on OWASP Guidelines manually as well as using automated tools. • Knowledge of Client Server based Application Security Testing • Knowledge of understanding the security report with recommendations to mitigate the reported Vulnerabilities. • Hands on in application security tools like Burp Suite, Acunetix, IBM App Scan etc. • Experience of Source Code review (Manual /Automated tools) will be added advantage. • Strong ability to manage multiple projects with managing time and commitments effectively. • At least Level 3 ability on Linux and Windows Operating Systems • SIEM tools. AlienVault SIEM experience ideal, but any other similar SIEM tools also considered (McAfee SIEM, Splunk, OSSIM, ARCsight, etc.) • Security Operations Center, Network Support center, or Incident Response center experience. • Experience with advanced security solutions: Antivirus, firewall, IPS, VPN, and other security related devices i.e. (Endpoint security suites from McAfee, Symantec, ESET, etc). • Experience in Vulnerability Management and scanning. • Knowledge in virtualization and hosted environments. • Experience with routing protocols, switching, encryption, DNS and content delivery solutions.

	• Must be comfortable working with and troubleshooting in a heterogeneous operating environment. • Excellent oral and written communication skills, including the ability to interact effectively with executives, engineers, sales, vendors and peers. (**Note :** Training experience forming a part of the curriculum of any Degree / Diploma will not be counted towards the total experience.)

CLOSING DATE FOR SUBMISSION OF ONLINE APPLICATION : 20th February, 2024

1	**Before applying for the above post(s) the candidates should satisfy themselves regarding ELIGIBILITY CRITERIA required for the said post(s).** In case it is found at any stage of recruitment that an applicant does not fulfill Eligibility Criteria and/ or that he has furnished any incorrect / false information / certificate(s)/ documents or has suppressed any material fact(s), his/her candidature will stand cancelled. Even if any of these shortcomings is/ are detected after appointment his/her services are liable to be terminated. **Applicants must fill the online Form very carefully.** Applications which are incomplete or vague (i.e. details relating to qualifications / experience etc.) or applications not in the prescribed format will be rejected summarily, hence candidates are advised to ensure that all the relevant fields mentioned in the on-line Resume Form are duly completed in all respects.
2	**Candidates should have a valid e-mail address and are advised to check their mail regularly for any information regarding test /interview**. In case, a candidate does not have a valid personal email address, he/she should create his/her new email address before applying Online. "ICSI" reserves the right to communicate with the applicant through e-mail and not by post.
3	All candidates are requested to take a printout of their online forms and keep it with them for future reference. However, they are requested **not to send the hard copy of their online application Form/ CV's /Certificates to the Institute. The original documents would be required for verification only at the time of Interview.** Candidates may take out the print out in token of acceptance of on-line applications & no separate acknowledgement to the effect would be sent.
4	The percentage obtained in various degrees/ diplomas should be rounded off to the lower whole number. For eg. 49.3% or 49.8% should be entered as 49% & not as 50%. In case grades are awarded, they should be converted to numerical equivalent percentages.
5	**While Filling the Online Resume Form :-** 1. Don't enter Special Characters like " "/ ' '/ & etc. 2. Enter minimum Words /Characters while filling up the University Name/ Specializations/ Major Responsibilities/ Address / Board & School Name / etc. 3. Upload a resume file which does not exceed 100 KB.

GENERAL CONDITIONS

1	**Candidates who are working in a Central/State Government/ Autonomous/ Statutory Body/PSU would be required to produce a 'No Objection Certificate' from their present employer for verification at the time of interview failing which they will not be allowed to appear for the interview.**
2	All educational qualifications must have been obtained from recognized universities / Institutions in India or abroad. The courses offered by autonomous Institutions should be equivalent to the relevant courses approved/ recognized by Association of Indian Universities (AIU)/UGC/AICTE.

3	Mere submission of application / fulfilment of eligibility conditions will not confer any right on the candidate to be shortlisted / called for written test/ interview. The “ICSI” reserves the right to call for written test/ interview only those candidates who in its opinion are most suitable for the post. The “ICSI” also reserves the right to reject any or all the applications without assigning any reason thereof. The decision of The “ICSI” in all matters regarding Eligibility, shortlisting of candidates, conduct of interview and selection will be final and binding on the applicants and no correspondence will be entertained in this regard.
4	Reservation policy will be applicable as adopted by the “ICSI” in its Service Rules.
5	The “ICSI” reserves the right to fix minimum eligibility standard/bench mark and restrict the number of candidates to be called for interview taking into account various factors like number of vacancies, performance of the candidates etc., and decide to determine the qualifying marks for selecting candidates for interview. The “ICSI” also reserves the right to raise the eligibility criteria to restrict the number of candidates to be called for written test/ interview. The decision of the “ICSI” in this regard shall be final and binding and no correspondence in this regard would be entertained with the candidates.
6	The “ICSI” reserves the right to increase/decrease the number of vacancies for any post, as advertised as per its requirement or not to fill up any posts as per its requirement or even cancel the whole process of recruitment without assigning any reason.
7	The “ICSI” also reserves the right to alter / modify / relax any of the aforesaid eligibility criteria / conditions for deserving candidates.
8	The “ICSI” reserves the right to offer or appoint the candidate on the post/grade lower than the post / grade advertised or applied by the candidate.
9	The candidates cannot have any right or preference for posting in any particular State/ city of his choice as the selection and posting is on All India basis. The Institute’s decision would be final in all these cases and the candidates are liable to be posted or transferred anywhere in India.
10	Proficiency in Computer Applications is essential for all the above post(s).
11	For attending the interview to & fro train fare will be reimbursed by the shortest route to the outstation candidates, as per rules of the “ICSI”. However no Travel Allowance shall be reimbursed for attending the written test.
12	The “ICSI” takes no responsibility for any delay in receipt or loss in postal transit of any applications or communication.
13	Canvassing in any form will straightway disqualify the candidature.
14	Internal candidates should forward their application through their respective Heads of Departments after meeting the criteria as laid down in the ICSI Service Rules.
15	Any resultant dispute arising out of this advertisement shall be subject of the sole discretion of the courts situated at New Delhi.

FOR APPLYING ONLINE, click on the link below
OR
Copy, Paste and Enter the link on the address bar of the internet Explorer / Google Chrome

https://www.icsi.in/recruitment/

(Note : Please use Windows Explorer (6.x, 7.x, 8.x, 9.x, 10.x and 11.x only) or Google Chrome and ensure that JavaScript is enabled for viewing this advertisement. Do not use Mozilla Firefox, Netscape Navigator or any other explorer)

In case of any query please email at the below mentioned email address :

The HR Directorate
The Institute of Company Secretaries of India
New Delhi
Email : hr.dept@icsi.edu
website : www.icsi.edu.