THE NEW INDIA ASSURANCE COMPANY LTD

(A Govt. of India Undertaking)

Regd. & Head Office: New India Assurance Building, 87, M.G. Road, Fort, Mumbai 400001

Appointment of full-time Chief Information Security Officer (CISO) on contractual basis

The New India Assurance Company Ltd., a leading Public Sector General Insurance Company, invites applications from eligible candidates for the appointment of Chief Information Security Officer (CISO) on Contract basis.

1. Details of POST / VACANCY:

Name of the post	Chief Information Security Officer
Type	Contractual on full-time basis
No. of posts	01 (Unreserved)*
Period of Contract	3 years initially. Can be extended by 2 years based on performance
Place of posting	Head Office, Mumbai

*Candidates belonging to reserved category (including PwBD), for whom no reservation has been mentioned, can also apply if they fulfil all the eligibility criteria for respective position.

- *Candidates should apply through **email to ciso.recruitment@newindia.co.in only**. Please refer to How to apply section of the advertisement for further details. No other means/mode of application will be accepted. Please keep referring to Recruitment section of our website https://newindia.co.in regularly for all further announcements/details.*

- *Before applying, candidates should ensure that they fulfil the eligibility criteria for the advertised post as on the cut-off date. If at any stage, it is found that any information furnished in the application is false/ incorrect or the candidate does not satisfy the eligibility criteria for the post, his/ her candidature will be cancelled and he/she will not be allowed to appear for interview / joining and can have their contract terminated without notice if he/she has already joined the Company.*

Please note the important dates:

Start date for receipt of Application	1st December 2025
Last date for receipt of Application	16th December 2025
Cut- off date for determining Eligibility Criteria with regard to Age, Qualification & Experience	01st January 2025

2. Eligibility Criteria

i. Nationality/ Citizenship
(a) a citizen of India, or (b) a subject of Nepal, or (c) a subject of Bhutan, or (d) a Tibetan refugee who came over to India before 1st January, 1962 with the intention of permanently settling in India, or (e) a person of Indian origin who has migrated from Pakistan, Burma, Sri Lanka, East African Countries of Kenya, Uganda, the United Republic of Tanzania, Zambia, Malawi, Zaire, Ethiopia and Vietnam with the intention of permanently settling in India.

ii. Age (as on 01.01.2025)

Minimum Age: 40 years and Maximum Age: 55 years

iii. Educational qualifications (as on 01.01.2025)

Mandatory:

- Full-time Master's or bachelor's degree in Engineering disciplines namely Electronics/ Computer/ Computer Science/ Information Technology from a recognized university.

And

- Professional Certifications (valid as on date of application):

CISSP (Certified Information Systems Security Professional) and CISA (Certified Information Systems Auditor)

Desirable:

Educational qualifications:

- Master's degree in Information Security/ Cyber Security/ Network Security/Information Systems/ Technology Management/ Risk Management from a recognize university.

Any (one or more) of the following professional certifications (valid as on date of application):
- CISM (Certified Information Security Manager)
- CCISO (Certified Chief Information Security Officer)
- CGEIT (Certified in Governance of Enterprise IT)
- ISO Lead Auditor (27001, 22301 etc.)
- CRISC (Certified in Risk and Information Systems Control)
- CGRC (Certified Governance, Risk and Compliance)
- CCSK / CCSP (Cloud Security certifications)
- Other globally recognized cyber security or risk certifications.

iv. Experience (as on 01.01.2025)

Mandatory:

- Minimum 15+ years of experience in IT/ Information Security, with at least 5 years in a senior leadership role (CISO / Deputy CISO / Head of Information Security).

Desirable:

- Prior experience in BFSI/Insurance sector is preferred.

v. Knowledge & Competence Areas

The candidate should demonstrate expertise and leadership-level understanding in the following domains:

Governance, Risk & Compliance:

- IT Act, Digital Personal Data Protection (DPDP) Act and associated rules thereunder, IRDAI and other Regulatory Guidelines, CERT-In cyber security circulars.
- International standards and frameworks: ISO/IEC 27001, NIST CSF (National Institute of Standards and Technologies Cyber Security Framework), COBIT (Control Objectives for Information and Related Technologies) etc.
- Cyber Risk Management

Cyber Risk Management:

- Information Security Risk Management, Third-Party Risk, Supply Chain Security, Cyber Insurance, Risk Quantification.

Security Operations Oversight:

- SIEM, SOC operations, Incident Response, EDR, Threat Intelligence.

Identity & Access Security:

- IAM, PAM, NAC, Zero Trust Architecture (ZTA).

Cloud, Application & Infrastructure Security:

- Cloud Security, Virtualization, Networking, Secure SDLC, DevSecOps, API Security.

Data Protection & Resilience:

- Data Security, DLP (Data Loss Prevention), Security Testing, DR & BCP, Crisis Management.

Emerging Security Practices:

- AI/ML in threat detection, Security Automation, Advanced Threat Hunting.

3. Job Profile

The role and responsibilities of the CISO will include, but are not limited to, the following:

A. Strategic Responsibilities

- Articulate, update, and enforce policies to protect the Company's information assets.
- Define and oversee the implementation of the Information & Cyber Security Assurance Programme, including governance frameworks, policies, procedures, and guidelines.
- Establish and manage the multi-year security roadmap and technology vision, ensuring deep integration with the Company's digital transformation, cloud strategy, and overall risk appetite.

- Continuously evaluate, pilot, and implement emerging cybersecurity solutions and industry frameworks
- Define and oversee the enterprise-wide Information Security Risk Management framework aligned with the Company's Enterprise Risk Management (ERM).
- Develop and maintain the Cyber Crisis Management Plan and conduct periodic stress testing to mitigate risks arising from cyber-attacks.
- Integrate security-by-design principles in emerging technologies like AI/ML.
- Ensure secure software development lifecycle (SDLC), integration of DevSecOps practices, and adoption of Cloud Security standards.
- Foster a culture of security awareness across the Company through continuous campaigns, training, and engagement.

B. Regulatory and Compliance Responsibilities

- Coordinate with regulatory and intelligence agencies including IRDAI, RBI, NCIIPC, and CERT-In for information sharing and compliance.
- Ensure compliance with the IT Act, Digital Personal Data Protection (DPDP) Act, IRDAI Cybersecurity Guidelines, and other domestic and international standards.
- Liaise with the Company's Legal and Compliance teams to interpret regulatory updates and ensure timely security control alignment.
- Lead the development and maintenance of the organizational Data Governance framework, policies, and standards related to data classification, retention, and access controls.
- Oversee the resolution of audit observations and inspection findings from regulators, statutory auditors, and internal/external agencies.
- Manage the Company's external IT Security certification processes such as ISO 27001 (Information Security Management Systems), and achieving other industry-specific certifications {e.g., ISO 22301 (International Standard for Business Continuity Management Systems (BCMS)} as dictated by evolving business needs.
- Stay informed about global regulatory requirements, standards, and best practices in information and cyber security, and ensure their adoption within the Company.

C. Operational Responsibilities

- Oversee day-to-day operations of the Security Operations Centre (SOC), including proactive threat monitoring, detection, and incident response.
- Conduct regular information and cyber security assurance audits, vulnerability assessments (VA), penetration testing (PT), and red-team/blue-team exercises.
- Oversee Threat Intelligence functions – monitoring dark web activity, geopolitical threats, and supply chain vulnerabilities.
- Ensure identity and access management (IAM), privileged access management (PAM), and endpoint security controls are enforced across the Company.
- Develop, test, and update Business Continuity and Disaster Recovery protocols.
- Review and recommend on application and infrastructure change requests to ensure secure design and deployment.
- Conduct investigations and digital forensics in case of incidents or breaches.
- Collaborate with IT, business departments, and regional offices to identify and manage cyber security risks, and oversee proof-of-concept (PoC) of new security initiatives.
- Supervise Third-Party and Supply Chain Security Management across all vendors, contractors, and business partners.

D. Advisory and Reporting Responsibilities

- Oversee the design and delivery of information security awareness and training programs for employees, vendors, and senior management, ensuring relevance, effectiveness, and compliance with regulatory requirements.
- Regularly brief top management, Risk Management Committee and the Board Risk/IT Committee on cyber security posture, risks, compliance, and initiatives.
- Oversee the development and ensure presentation of executive dashboards and key metrics on risk, compliance, incident management, and overall security posture to senior management and the Board.
- Represent the Company in industry forums, regulatory committees, and technical conferences on information and cyber security.
- Advise leadership on emerging global threats, vulnerabilities, and recommended actions to strengthen the Company's resilience.
- Ensure transparent communication with stakeholders (internal and external) during cyber incidents as per crisis communication protocols.

E. Residual Clause

Perform any other related responsibilities assigned by the Company in the area of information and cyber security.

4. Terms of Appointment

Period of contract	Contractual basis for initial tenure of three (3) years, subject to annual performance review at the end of each year, extendable by another 2 years based on performance review and organizational requirements
Nature of appointment	Contractual on full-time basis
Remuneration	Rs. 50 lakhs (all inclusive) with annual increment up to 5% based on annual performance review However, remuneration can be negotiable for the right candidate
Termination of contract	Either party may terminate the contract by giving 3 months' notice or on grounds of misconduct
Service rules	The contract is subject to satisfactory completion of all pre-recruitment formalities including medical examination, background checks, verification of testimonials etc. No statutory benefits or Company contributions towards P.F., NPS, etc shall be applicable No superannuation benefits shall be applicable
Place of posting	Mumbai
Accommodation	The applicants shall make own arrangements for his/her stay and it shall not be incumbent on the Company to provide any residential accommodation.
Leave Entitlements	Casual Leave: 12 days/ year Sick Leave 12 days/ year Maternity/Paternity Leave: As applicable Absence beyond 15 days would result in termination of the contract, unless approved by the Competent Authority
Undertaking	The appointee shall furnish a notarized contract as in the prescribed format on the stamp paper of requisite value at the time of joining.

5. Selection process

The selection process will comprise of:

Preliminary screening and shortlisting: Conducted on basis of the eligibility criteria, candidate's qualifications, suitability, experience, etc. submitted with the applications through email.
Shortlisted candidates shall be called for an interview.
After screening of the documents, if the candidate is found ineligible, his/her candidature will stand cancelled.

Personal Interview: Depending on the number of shortlisted candidates, they will be called for one or more rounds of interview to be conducted by the Company.
The interview date and venue, along with the list of documents to be produced, shall be informed to the shortlisted candidates in due course.

6. How to apply

Eligible candidates may send their Application form (as per format enclosed in Annexure – A) in pdf format duly signed by the candidate and affixed with a recent passport size photograph along with the relevant supporting certified and self-attested documents by email mentioning the "Application for the post of CISO 2025" in the subject line to **ciso.recruitment@newindia.co.in**.

Last date for Receiving Application: The completed application form (with signature and photograph) with all relevant certified documents in support of eligibility in respect of Age, Educational Qualifications, Certifications, Current Employment, Past experience (whether meets the standards mentioned in the eligibility criteria of this advertisement), copy of Identity card for e.g. Aadhar Card, PAN Card, passport etc., any other relevant documents in pdf format must be received by NIACL at the above email ID **on or before December 16 2025**. Applications received beyond the due date will be rejected and no communication will be sent to the candidate in this regard. NIACL shall not be responsible for non-receipt of application for whatsoever reason. Further, no request / representation for extension in last date of submission of application will be entertained by NIACL.
No other means/mode of application will be acceptable. An application which has not been signed by the candidate or incomplete in any respect will not be entertained and will be treated as rejected.

Any information submitted by a candidate in his/ her application shall be binding on the candidate personally and he/ she shall be liable for prosecution/ civil consequences in case the information/ details furnished by him/ her are found to be false at a later stage.

7. General Instructions

i. Company does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of any reason whatsoever.
ii. Candidates must necessarily produce the relevant documents in original and a self-attested photocopy in support of their identity and eligibility pertaining to nationality, age, educational qualifications, qualifications/certifications, post academic professional experience etc. as indicated by them in the application form at the time of interview. Please note that no change of application data will be permitted at any stage after submission of application. Merely applying for the post and being shortlisted in the online examination and/ or in the subsequent interview and/ or subsequent processes does not imply that a candidate will necessarily be selected in the Company.

iii. All correspondence will be made through Email / website. Therefore, all the candidates are advised to provide correct e-mail address and check their e-mails / Company website regularly for any updates from the Company.

iv. Candidates serving in Government / Quasi Government Offices, Public Sector undertakings including Nationalised Banks and financial institutions will be required to submit 'No Objection Certificate' from their employer at the time of Interview, failing which their candidature may not be considered and travelling expenses, if any, otherwise admissible, will not be paid. Candidates who are selected are required to submit discharge letter / relieving letter from their employer (Govt/Public sector / Private) at the time of joining the company, without which they will not be allowed to join.

v. Decisions of the Company in all matters regarding eligibility, conduct of interview and selection would be final and binding on all candidates. No representation or correspondence will be entertained by the Company in this regard.

vi. NIACL reserves the right to modify or amend or reverse or cancel any or all the provisions of the recruitment process including eligibility criteria.

vii. Candidates who merely meet the eligibility criteria shall not reserve right to be shortlisted and called for further process of recruitment. Decision of the Company shall be final in this regard.

viii. The candidates called for interview shall be entitled for to & fro economy air fare by shortest route, from their place of residence, on production of evidence of travel.

ix. The Company, may at its sole discretion, re-hold the Personal Interview or additional round/s of Personal Interview, wherever necessary.

x. The Company reserves the right to raise/relax criteria depending on the applications received.

xi. The selected candidate shall have no right or claim for regular employment in the organization.

xii. Any legal proceedings in respect of any matter of claim or dispute arising out of this advertisement and/ or an application in responses thereto can be instituted only in Mumbai. Courts/ Tribunals/Forums at Mumbai only shall have sole and exclusive jurisdiction to try any cause/dispute

xiii. The Company reserves the right to cancel the above Recruitment Exercise at any stage of the process without assigning any reason thereof.

xiv. Instances for providing incorrect information and/or process violation by a candidate detected at any stage of the selection process will lead to disqualification of the candidate from the selection process and he/she may not be allowed to appear in any of the Recruitment Process in the future. If such instances go undetected during the current selection process but are detected subsequently, such disqualification will take place with retrospective effect.

xv. Not more than one application should be submitted by any candidate. In case of multiple applications only the latest valid (completed) application will be considered.

xvi. At the time of interview, the candidate will be required to provide details regarding criminal cases(s), vigilance cases pending against him/ her, if any. The Company may also conduct independent verification, inter alia, including verification of police records etc. NIACL reserves the right to deny the selection/appointment depending upon such disclosures and/ or independent verification.

xvii. Canvassing or bringing any undue influence in any form will result in disqualification.

xviii. Any notice/communication meant for the candidates displayed on the Company's website or conveyed to the email id mentioned in the application, shall be deemed to be sufficient service of communication upon the candidate, for all purposes.

General Manager (P)

REF NO: RECTT/CISO/2025
01.12.2025