ENGAGEMENT OF CHIEF INFORMATION & SECURITY OFFICER (CISO) ON CONTRACT BASIS

National Insurance Company Limited, a Government of India Undertaking is India's oldest General Insurance Company offering a wide range of insurance services to its customers, invites applications for the post of **Chief Information Security Officer (CISO) on contractual basis**. Candidates fulfilling required eligibility criteria may send their application / testimonial(s) to ciso_recruitment@nic.co.in on or before 28th November, 2025.

Start date of receiving of application — **29th October, 2025**

Last date of receiving of application — **28th November, 2025**

Post	Vacancy	Age (as on 01-10-2025)	Contract period	Place of Posting
Chief Information Security Officer (CISO)	1 (One) – Unreserved	Minimum 45 years ; Maximum 55 years	03 (Three) years, which may be extended for a further period of 02 (Two) years based on satisfactory performance	Head Office, Kolkata

1. Eligibility Criteria:

(i) Nationality: Candidate must be a citizen of India

(ii) Qualification:

Essential:

a. Educational qualifications: An Engineering Graduate/ Post-Graduate Engineer or MCA.
b. At least one of the below certifications:
   i. Certified Information Systems Security Professional (CISSP)
   ii. Certified Information Security Manager (CISM)
   iii. Certified Chief Information Security Officer (CCISO)
   iv. Certified Information Systems Auditor (CISA)
c. Cloud security certified professional e.g., Certified cloud security professionals (CCSP).

Desirable

a. Should be a Certified Ethical Hacker (CEH).
b. Experience in the financial services sector in India.
c. Familiarity with IRDAI IT security regulations, DPDP2023 Act, ISO 27001 standards
d. Having proven leadership capabilities in Information Security.

(iii) Experience: 20 years in Technology functions, with at least 15 years of demonstrable experience in network and cybersecurity domains as on 01.10.2025. Of this, a mandatory minimum of 10 years must be in Leadership Roles encompassing SOC transformation, enterprise-wide cybersecurity strategy execution, and BFSI/public sector digital security transformation. This must include key functions such as Security Solution Architecture covering Information Security Governance, Risk and Compliance Management, and Security Operations—all of which should have been held at a Senior Management level within the respective organization. While minor variation in total experience may be considered for the right candidate with proven BFSI/PSU impact, demonstrated hands-on expertise and leadership in SOC transformation remains non-negotiable.

2. Job Profile:

i. Cybersecurity Vision, Plan, and Architecture for Core Insurance and its secure upgrades; dovetailing this into CTO's technology transformation roadmap for NICL
ii. Ownership of the Cybersecurity Vision of National Insurance Co. Ltd. – secure digital transformation and paperless office, being part of the technology transformation roadmap for NICL.
iii. Studying the threat environment, ensuring secure innovation, and rolling out new secure products/initiatives.
iv. Working with CTO, conceptualizing and executing strategic planning for secure Core Insurance upgrades/replacements to deliver on the Cybersecurity Vision.
v. Managing and supervising secure development of applications for IT operations and business requirements.
vi. Making secure new software applications or modifications available with least turnaround time.
vii. Focused attention on secure integration of internal and external applications with Core Insurance, compliant with DPDP data sharing rules.
viii. Ensuring uninterrupted secure availability of IT Hardware and Software for Core Insurance.
ix. Keeping IT infrastructure in a contemporary secure state (user end to data centre end) by adopting latest protections.
x. Accounting and reconciliation of cybersecurity projects.
xi. Handling customer complaints related to data breaches/security and their resolution.
xii. Collaborating with business teams, IT partners, and consultants on secure practices.
xiii. Maintaining a secure IT environment per ISMS Policies, Procedures, Guidelines, IRDAI, DPDP, and CERT-In.

Activities:

i. Deliver on the Cybersecurity Vision, update the Cybersecurity Policy document for the next 5 years, incorporating DPDP and IRDAI updates, along with changes in regulatory, government requirements as and when applicable.
ii. Contribute to technology vision and business by influencing secure strategies and monitoring major security initiatives.
iii. Analyze solution requirements; facilitate secure development projects from requirements to implementation for business continuity.
iv. Review, refine, and modify prevalent security architecture to meet Core Insurance needs, upgrades, and market competitiveness.
v. Help adopt the latest, cost-effective, efficient security initiatives.
vi. Ensure optimal secure utilization of IT resources.
vii. Defining success criteria for security projects, including scope, time, cost, technical parameters.
viii. Developing and executing cybersecurity strategy aligned with business, redefining security vertical for improved operations and analytics.
ix. Ensuring future demand is factored into secure capacity plans.
x. Validating monitoring technologies for alignment with security metrics, alerts, and operations.
xi. Overall monitoring of applications aiming at zero security incidents/downtime.

xii. Forecasting and procuring secure IT infrastructure.
xiii. Onboarding vendors for security support (System Integrators).
xiv. Supervise and monitor security testing functions (e.g., penetration testing, vulnerability assessments).
xv. Creating a Security Analysis layer for business departments.
xvi. Collaborating with stakeholders (internal/external) on security, guiding processes, maintaining security plans.
xvii. Team-based style to improve performance via negotiations, persuasion – with employees, Management, Departments, Vendors, ensuring effective secure dialogue.
xviii. Supervising teams in evaluating, deploying, managing secure IT systems to improve efficiency, optimize delivery, lower risks.
xix. Work with CTO, collaborating with Corporate Management so they embrace secure technology for innovation and advantage.
xx. Provide in-depth cybersecurity expertise to Management.
xxi. Ensure standards for governance, regulatory compliance (DPDP, IRDAI, CERT-In).
xxii. Any other activities assigned by CTO, Corporate Management.

Company Expectations from the CISO

Short Term:

i. The CISO should be an adequately experienced professional from the industry who will lead the cybersecurity transformation process at National Insurance Co. Ltd., starting with conducting a comprehensive security assessment of the Core Insurance Solution and implementing immediate enhancements to address vulnerabilities, ensure compliance with IRDAI's 6-hour cyber incident reporting mandate, and stabilize incident response protocols.
ii. The CISO shall work with the CTO, plan the roadmap as a part of the CTO's technology transformation roadmap for NICL and design the security architecture for the company's technology transformation to Cloud, SAS, digitalization and paperless office, incorporating upgrades/replacements of applications and databases in the Core Insurance Stack, with a focus on integrating security-by-design using microservices, AI/ML for threat detection, RPA, Big Data analytics for anomaly detection, Cloud security postures, Blockchain for data integrity, and other emerging technologies to mitigate risks and ensure compliance with DPDP Act requirements for data minimization, consent management, and breach notifications.
iii. As part of this exercise, the CISO would be responsible for working with the CTO in identifying cybersecurity opportunities and risks in the transformation roadmap, including assessment of competitive threats, innovation in secure product offerings, marketplace obstacles like regulatory hurdles, and technical challenges such as data localization under DPDP and cross-border transfer restrictions.
iv. Evaluate and identify appropriate security platforms (including secure web application frameworks, encryption standards, and deployment stacks) for delivering the company's services, with emphasis on Indian-specific requirements like CERT-In logging mandates (180 days retention) and IRDAI's enhanced monitoring.

v. Analyze and assess new technologies like Big Data, Stream Analytics, Cloud, IoT, AI/ML, RPA, Blockchain, and Mobility for potential vulnerabilities, and develop innovative, user-friendly secure products and services for customers, agents, and partners.
vi. Evaluate the cost efficiency of emerging security technologies and assess their applicability to the transformation, ensuring alignment with DPDP's security safeguards and IRDAI's resilience frameworks.
vii. Design high-level security architecture, modules, and components, including database security strategies, access controls, and encryption protocols.
viii. Design training programs and coordinate cybersecurity awareness training across the organization
ix. Advise CTO, Corporate Management and the Board on key decisions through Cybersecurity Risk Analysis, Technology Risk Analysis, establishing governance processes for direction and control to manage risks appropriately, particularly in ongoing technology transformation and data privacy compliance.

Long Term:

i. The CISO should be a cybersecurity strategist with a strong business focus, meeting the following expectations:
ii. In partnership with the CTO and Information Security & Network Team, deliver on the company's secure technology transformation to digitization and paperless office. Explore and identify cybersecurity trends, evolving threat landscapes (e.g., AI-generated attacks, ransomware-as-a-service), and social behaviours that may support or impede business success.
iii. Identify new opportunities in secure digital operations and create strategies to implement them for the company, its agents, customers, and partners.
iv. Drive initiatives to create flexible, secure IT architecture that enables faster speed to market for new products and services while maintaining zero-trust principles.
v. Ensure new software applications or modifications are securely available to the business with minimal turnaround time.
vi. Keep IT infrastructure (software, hardware, and data) in a contemporary, future-ready state by adopting latest security technologies.
vii. Adopt systemic security management methodologies in all IT projects, leveraging the existing IT talent pool.
viii. Take initiative in thought leadership, innovation, and creativity in cybersecurity.
ix. Participate as a member of the Corporate Management team to collaborate with departments in assessing and recommending secure technologies that support organizational needs.
x. Maintain a secure IT environment per established ISMS Policies, Network Policies, Procedures, and Guidelines, while ensuring compliance with DPDP Act, IRDAI guidelines, MeITY guidelines and other regulatory standards for data privacy and cyber resilience.

3. Terms of Appointment:

No.	Particulars	Terms & Conditions
(i)	Nature of appointment	Appointment of CISO will be contractual in nature in the cadre of Deputy General Manager
(ii)	Remuneration	Rs. 35 Lakhs per annum (all inclusive). However, remuneration will not be a limiting factor for the right candidate
(iii)	Leave	12 days of Casual Leave (CL) for every calendar year. However, if the contractual period starts mid of a calendar year, proportionate CL shall be accordingly granted. Un-availed leaves, if any, shall not be carried forward
(iv)	Other facilities for official purposes	TA/DA, mobile and laptop facility as per entitlement for DGM Scale officer. Rail/Air travel entitlement as applicable for DGM Scale officer
(v)	Termination of contract	The contract may be terminated by either party by giving to the other three months' notice
(vi)	Superannuation benefits	No superannuation benefit shall be applicable
(viii)	Confidentiality & Non-Disclosure	The appointee shall furnish a confidentiality & non-disclosure undertaking in the prescribed format on the stamp paper of requisite value at the time of joining

4. Selection Procedure:

The selection process will comprise of:

- Preliminary screening and shortlisting based on the eligibility criteria, candidate's qualifications, experience, etc. submitted with the application.
- Shortlisted candidates shall be called for an interview.

The candidature is purely provisional subject to verification of documents / testimonials.

Candidates serving in Government/ Quasi Govt. Offices/ Public Sector Undertakings (including Nationalized Banks and Financial Institutions) are required to produce a "No Objection Certificate" from their employer at the time of interview, in the absence of which their candidature will not be considered.

Mere eligibility, shortlisting and appearance in interview does not imply that the NICL is satisfied beyond doubt about the candidate's eligibility and it shall not vest any right in a candidate for selection. NICL would be free to reject the candidature of any candidate at any stage of recruitment process, if he/ she is found to be ineligible and/ or furnished incorrect or false information/ testimonials/ documents or has suppressed any material fact. If appointed, the contract of such a candidate may be terminated.

The interview date and venue, along with the list of documents to be produced, of the shortlisted candidates shall be informed in due course. Candidates are advised to check NICLs official website https://nationalinsurance.nic.co.in for details.

5. How to apply:

Candidates are required to send their application comprising their detailed CV/ Resume and testimonials to **ciso_recruitment@nic.co.in** mentioning the **"Application for the post of CISO"** in the subject line.

Candidates should ensure that recent photograph and signature is present in application.

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.

6. General Instructions:

(i) Before submitting the application form, the candidates must ensure that they fulfil all the eligibility criteria with respect to age, qualifications, experience, etc. as stated in this advertisement. If the candidate qualifies in the selection process and subsequently it is found that he/ she does not fulfil the eligibility criteria, his/ her candidature will be cancelled and if appointed, services would be terminated without any notice or compensation.
(ii) Not more than one application should be submitted by any candidate. In case of multiple applications only the last (complete) application will be considered.
(iii) NICL reserves the right to modify or amend or reverse or cancel any or all of the provisions of the engagement process including eligibility criteria.
(iv) NICL may at its sole discretion, re-hold interview, if deemed necessary.
(v) Any resultant dispute arising out of this advertisement and the selection process shall be subject to the sole jurisdiction of the Court(s) situated in Kolkata only.
(vi) Decisions of NICL in all matters regarding eligibility, conduct of Interviews and selection would be final and binding on all candidates.

4. General Terms:

- Cut-off date for eligibility criteria is October 01st, 2025.
- Before applying, candidates should ensure that they fulfil the eligibility as on the cut-off date. Admission to Personal Interview (PI), will be purely provisional without verification of documents. Candidature will be subject to verification of details / documents with the originals when the candidate reports for PI, if called.
- National Insurance Company Limited reserves the right to place the selected candidates in any of the functional areas of the corporation other than those advertised, if found suitable for the same.
- Candidates are advised to check Careers Page on NICL's website https://nationalinsurance.nic.co.in for all further announcements / details. Any revision / corrigenda will be provided / hosted on NICL's website only. Only Candidates willing to serve anywhere in India, should apply.

GENERAL MANAGER
NICL HEAD OFFICE, KOLKATA
28TH OCTOBER 2025.