



ENGAGEMENT OF CHIEF TECHNICAL OFFICER (CTO), CHIEF DIGITAL OFFICER (CDO), CHIEF INFORMATION SECURITY OFFICER (CISO) in LIC of India on Contract Basis

Last date for submission of Application : 10.10.2022 (Online)

VACANCIES & OTHER DETAILS (AGE, QUALIFICATION, EXPERIENCE) ARE DETAILED BELOW:

Post No.	Post Name / Posting Place	Vacancy	Age as on 01.01.2023	Contract Period	Annual Cost to Company
A	Chief Technical Officer/ Central Office Mumbai	1 (UR)@	Should not be more than 58 Years	Three years initially, renewable yearly at the sole discretion of LIC.	Would comprise of fixed and variable components but not a limiting factor for a suitable candidate
B	Chief Digital Officer/ Central Office Mumbai	1 (UR)@	Should not be more than 58 Years	Three years initially, renewable yearly at the sole discretion of LIC.	Would comprise of fixed and variable components but not a limiting factor for a suitable candidate
C	Chief Information Security Officer/ Central Office Mumbai	1 (UR)@	Should not be more than 58 Years	Three years initially, renewable yearly at the sole discretion of LIC.	Would comprise of fixed and variable components but not a limiting factor for a suitable candidate

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

Educational, Professional Qualification and Post qualification Experience should be reckoned **as on 01.09.2022** and as per **Annexure-1** given below:

Annexure- 1

	Post No. A (CTO)	Post No. B (CDO)	Post no. C (CISO)
Qualification	Engineering Graduate or MCA or equivalent qualification from a recognized University/Institution.	Bachelors/ Master's degree preferably a combination of Business/ Technology/Computer Science/Digital Marketing or related fields.	Graduate from a reputed University, preferably with credible certifications in information security or an Engineer from a reputed University.
Experience	<ul style="list-style-type: none"> Technology Leader with minimum 15 years of experience in Banking / Insurance/ IT Services with FS domain /projects of 	<ul style="list-style-type: none"> Minimum of 15 years experience. Domain expertise in driving Digital initiatives, preferably in broader financial 	<ul style="list-style-type: none"> Total of 15 plus years of experience with 5 years in information and cyber security, particularly in the areas of governance, risk management,

	Post No. A (CTO)	Post No. B (CDO)	Post no. C (CISO)
	<p>which 5 years should be at senior management level/managing or implementing large IT projects in Insurance/Banks or FI</p> <ul style="list-style-type: none"> • Domain expertise, preferably in broader financial services (Insurance, Banking, Other Financial services Institutions) • Someone with experience in a large, complex environment with strong stakeholder management experience 	<p>services (Insurance, Banking, FinTech, other Financial services or FS aligned Institutions).</p> <ul style="list-style-type: none"> • Strong people / team management experience with strong commercial orientation. • Experience in creating customer centric environments. 	<p>compliance, policy formulation, third party risk management, security awareness, external assessments etc.</p> <ul style="list-style-type: none"> • Should have played a leadership role either as a Leader of IS or at N minus 1 level • Experience of working in a large scale business / team is important • Preferable to have experience in IT Systems administration or security tools configuration. • Track record of navigating highly regulated, customer focused, compliance-oriented environments of similar scale and complexity.
Other qualities	<ul style="list-style-type: none"> • Strong people / team management –led large teams of IT professionals. • Familiar with cutting edge technologies. 	<ul style="list-style-type: none"> • A digital expert recognized by his/her industry peers, with a holistic view and deep understanding of existing and emerging digital disciplines. • Smart, curious leader who is effective working in a collaborative environment both internally and externally. 	<ul style="list-style-type: none"> • The role requires solid analytical and problem-solving abilities to identify and fix security risks Compliance. • Keep abreast of latest security related regulations, legislations and advisories affecting the organization.

JOB PROFILE:

Post No. A (CTO) : The Chief Technical Officer will report to Executive Director(IT)

Purpose: Technology will play critical role across LIC and will be integral to all aspects of the business. The expectation from the Chief Technical Officer (CTO) will be to create a framework and strategy that ensures technological service level excellence. It will be a unique opportunity to lead significant



transformation across the organization and create capabilities that supports and builds the future growth agenda of the company.

Role: Providing technology vision and IT architecture for LIC, Creating and owning the long term strategy for LIC. Assisting, managing and collaborating with the Executive Directors in IT to drive innovation, automation & change. Ensure future readiness by adopting latest options in technology hardware, software & solutions. Managing vendors and key outsourcing relationships. Lead IT projects for their completion in time. To conceptualize and operationalize integration efforts across multiple technologies, infrastructure and application ecosystems will be critical.

Core set of responsibilities:

- Outlining the Corporation's Technology vision, IT architecture roadmap & policy document including applications, infrastructure
- Reviewing, modifying and refining the technology architecture prevalent in the Corporation for meeting its projected needs and remaining competitive in the market.
- Be able to build and lead a team of technical professionals, including software architects, software developers and engineers.
- Drive initiatives to re-imagine how technology delivers to the business, leveraging existing and emerging technologies to support LIC's employees & stakeholders
- Helping adopt latest, cost effective and efficient new technology initiatives, with a strong focus on automation
- Oversee initiatives to replace legacy technology with cutting-edge platforms that leverage emerging technology trends; optimizing and managing existing information technology network in a manner it delivers high efficiency with sufficient resilience and yet managing the cost effectively.
- Recommend and prioritize IT Investments that align with the business objectives and budgetary commitments
- Manage Key outsourcing relationships/ technology vendors, to ensure high quality and timely delivery for Corporation at competitive pricing. Thereby developing consistent, repeatable project management / delivery methodologies.

Other day- to- day responsibilities:

- Supervising and monitoring progress of various IT projects for their on-time delivery.
- Oversee the development of enterprise technology standards, governance processes and performance metrics to ensure that IT delivers value to the organization.
- Ensure systems performance, availability and satisfy service level requirements. Ensure that there is no failure in business operations and appropriate business recovery plans are in place and regularly tested for readiness for unforeseen and unexpected events which can impact business continuity.
- Ensure that all IT assets achieve full life time cycle value.
- Conceptualize and execute strategic planning of IT facilities
- Providing in depth technical expertise to top management of the Corporation.



- Ensuring future readiness by adopting latest options in technology Hardware, Software & solutions.
- Enhance digital value proposition of the Corporation to internal users, customers, and to ensure faster product launches, richer set of features, greater flexibility, etc.
- Keeping IT environment secure as per Corporation's IT/ IS Policies.
- Ensure un-interrupted availability (24*7) of IT Hardware and software applications of the Corporation for business purposes.
- Develop IT for Rural/Micro/Group Insurance and support other government initiatives e.g. PMJJY, DBT schemes through systems changes.
- Ensure implementation of proper standards for governance as well as regulatory compliance.
- Be responsible for risk management and compliance to IT Security policies as well as regulatory prescriptions.
- Any other responsibility assigned by the Competent Authority from time to time.

Post No. B (CDO) : The Chief Digital Officer will report to Executive Director(IT).

Purpose: Driving & leading a Digital First data driven business philosophy in LIC in India, focusing on implementation of digital initiatives across the enterprise & ecosystem covering clients, vendors, customers amongst others. Put a special focus on creating new value through the smart use of digital tools, platforms, technologies, services, and processes.

The CDO will act as the organization's central leader and integrator in the digital transformation process, serving as an intermediary between all other companies, executives and functions in the rollout of digital initiatives and capabilities, fully integrating business and technology. Champion the use of digital initiatives and practices to enable a digital mindset from the top down. Be seen as a digital thought leader both internally and externally by balancing build, buy and third party partnerships in order to drive accelerated growth, profitability, customer experience, brand power and digital footprint.

Role: She /he will shape LIC's vision for digital, co-create and define, develop, and drive a digital framework and strategy to help ensure of its short and long term priorities. Develop a clearly-defined and compelling digital strategy for LIC's future, ensuring collaboration and knowledge sharing among employees across departments to build, manage and continue to grow digital innovation ecosystem; managing digital channels for customer journey, competition benchmarking, customer adoption and usage; leading digital transformation projects for their completion in time and providing technical expertise to the top management of the Corporation.

Core set of responsibilities: The responsibilities of Chief Digital Officer include but are not restricted to the following

- Build a coherent digital strategy and pipeline of value creating innovation
- Responsible for working closely with key business stakeholders. Technology



Partners, NPCI, e-commerce partners/merchants and regulatory partners and ensure maximum up-time for all digital channels.

- Support implementations of new Digital products and enhancement for the existing digital channels based on local and global trends to improve service offerings to our customers.
- Build and own Analytics / modeling team
- Build Digital First as a culture in the company
- Build outcomes, products, services and solution plans for the digital business
- Define budgets and measurable goals for the digital vision
- Implement best in class Digital processes and technologies
- Ensure all digital programs to clearly defined metrics to evaluate success and continuous measurable improvement
- Identify Business and Business Improvement opportunity and report complaints which require special attention and recommend preventive measures
- Drive and embed the firm's overall digital culture transformation
- Design effective and efficient digital customer journey to ensure delivery of excellent customer experience through website, mobile app, web etc as a result to ensure a robust and ambitious growth in digital usage.
- Work in unison with a wide range of stakeholders including product owners, technology, compliance and external vendors and agencies to construct and deliver efficient and quality service.
- Liaise with the Zonal Offices/ Divisional Offices/ Branches/ Satellite Offices/ customer Zones or any such offices and centres for digital registrations.

Other day-to-day responsibilities:

- Monitor competition and keep abreast of the channel offerings and service developments.
- Monitor daily operations of delivery channels and identify improvement areas for re-engineering to ensure delivery of efficient and high quality service to customers.
- Ensure timely and accurate MIS and Dashboard reporting to drive digital activations.
- Conduct researches on the best and evolving market practices to define the most efficient and customer friendly UI throughout the entire customer journey.
- Plan and implement increase in Digital Transactions in the Corporation.
- Manage digital channels process notes and operating instructions, with configuration management to ensure easy retrieval and safe keeping.
- Managing and on-boarding prospective and new customers on all fronts.
- Reviewing Complaints and ensuring resolutions of the same on digital channels.



- Assisting in framing policies and procedures for the implementation of digitalization in various reformatory initiatives
- Plan, execute, own and monitor Digital Marketing Campaign for incremental revenue to the Corporation.
- Any other responsibility assigned by the Competent Authority from time to time.

Post No. C (CISO) : The Chief Information Security Officer will report to Chief Risk Officer

Purpose: To develop the vision and technical roadmap for cyber security across an enterprise, prioritized cyber concerns and risks accordingly and centralized cyber processes and tools. The CISO will be expected to set and deliver an innovative and effective strategy to manage threats and satisfy regulatory expectations while maintaining operational efficiency.

Role: Managing & monitoring SOC & drive information security related projects, Supporting risk management process by analyzing threats to the computing environment, overseeing all information security processes & serve as focal point for all information security issues, Assist the Chief Risk Officer (CRO) by managing Core Cyber Security programs and handling strategic planning of Cyber security.

Responsibilities: The responsibilities of Chief Digital Officer include but are not restricted to the following

- Responsible for articulating, implementing and monitoring of information security system at the organization in accordance with the relevant security standards and applicable guidelines
- Build and lead the information security team with appropriate resource strength, competencies and attitude to deliver the information security program
- Collaboratively engage with other functions and business representatives to facilitate a standardized approach and governance structure to information security and risk.
- Help manage information security budgets and monitor them for variances
- Lead the second line of defense in reviewing the control effectiveness through control checks, access reviews and risk assessments.
- Drive risk assessment to identify important security risks to the enterprise and identify the mitigation plan for the same.
- Promote user awareness initiatives within the organization. Coordinate with Zones/Divisional offices to facilitate security risk assessment and risk management processes and assist stakeholders in identifying acceptable level of residual risk.
- Liaise with Enterprise Technology teams to ensure that appropriate information security architecture standards, policies, and procedures are available and implemented consistently across all infrastructure and application development projects and programs. This includes review of as-is state as well as engagement in future initiatives.
- Develop Business Continuity, Disaster Recovery and Security Incident Response policies and procedures and ensure appropriate plans are in place to facilitate recovery of critical business functions and systems.



- Implementation, management and monitoring of Security Operation Centre (SOC) and drive cyber security related projects.
- Maintain and update a threat landscape for the organization and preparedness of the Organization on risk mitigation and all these aspects and discuss with the management, Board and other IT subcommittees on a regular basis.
- Ensuring that periodic tests are conducted to evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks as well as after any major incident.
- To ensure that , whatever exception/deviations/non-adherence to the IS security are proposed by the Application Owner, the risk assessment process is completed and appropriate recommendations are put up to Managing Director and CIO
- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong security posture.
- Develop and maintain an incident response program to address security incidents, respond to policy violations, interfacing with internal or external stakeholders as required.
- Liaison among the Information Security team and corporate compliance, Oversight, audit, legal and HR management teams as required
- To define security violations and support investigative processes
- To direct Information Security incident Response Mechanism
- To represent the Organization in the area of Information security at industry standards committee, technical conferences and regulatory bodies as decided by CRO.
- Ensure that the team is highly engaged and committed to deliver the outcomes. Resolve any team engagement issues.
- Ensure compliance to IS guidelines from Regulatory bodies or statutory agencies
- Any other matter as may be entrusted by the Corporation from time to time.

1. **SELECTION PROCEDURE:**

- (I) Initial Screening.
- (II) Candidates will be short-listed for personal interview, based on their qualification, experience and overall suitability.
- (III) Selection will be based on personal interview/ interactions.

2. **NATURE OF ENGAGEMENT: CONTRACTUAL**

Contract will be for a period of 3 years renewable yearly or for a lesser period subject to satisfactory performance at the discretion of the Corporation. The contract can be terminated at one month's notice on either side.

3. **REMUNERATION:** The compensation package would comprise of fixed and variable components but not a limiting factor for a suitable candidate.



4. **APPLICATION FEES** including intimation Fees (Non Refundable): Rs.1,000/-(One thousand only) plus GST as applicable.
For SC/ST/PwBD candidates, there is no application fee, however they have to pay Rs.100/- (One hundred only) plus GST as applicable.
Transaction Charges are to be borne by the candidate. Payment has to be done through on-line only. Application Fee once paid will not be refunded on any account.
5. **HOW TO APPLY/GUIDELINES FOR FILLING ON LINE APPLICATION:**

Candidates can apply online only from 10.09.2022 to 10.10.2022 and no other mode of application will be accepted.

IMPORTANT POINTS TO BE NOTED BEFORE REGISTRATION

Before applying online, candidates should-

- (i) scan their :
- photograph (4.5cm × 3.5cm)
 - signature (with black ink)
 - brief resume
- Ensuring that the all these scanned documents adhere to the required specifications as
- (ii) Signature in CAPITAL LETTERS will NOT be accepted.
- (iii) Keep the necessary details/documents ready to make Online Payment of the requisite application fee/ intimation charges
- (iv) Have a valid personal email ID and mobile no., which should be kept active till the completion of this Recruitment Process. LIC may send intimation to the registered e-mail ID. In case a candidate does not have a valid personal e-mail ID, he/she should create his/her new e-mail ID and mobile no. before applying on-line and must maintain that email account and mobile number.

APPLICATION FEES/ INTIMATION CHARGES (NON REFUNDABLE) PAYMENT OF FEE ONLINE: 10.09.2022 to 10.10.2022

Bank Transaction charges for Online Payment of application fees/intimation charges will have to be borne by the candidate.

(a) Application Registration

1. Candidates to go to <https://licindia.in/Bottom-Links/careers> and select "SpecializedpositionsInIT".
2. Candidates have to click on the option "APPLY ONLINE" which will open a new screen.
3. To register application, choose the tab "Click here for New Registration" and enter Name, Contact details and Email-id. A Provisional Registration Number and Password will be generated by the system and displayed on the screen. Candidate should note down the Provisional Registration Number and Password. An Email & SMS indicating the Provisional Registration number and Password will also be sent.
4. In case the candidate is unable to complete the application form in one go, he / she can save the data already entered by choosing "SAVE AND NEXT" tab. Prior to submission of the online application candidates are advised to use the "SAVE AND NEXT" facility to verify the details in the online application form and modify the same if required. Visually Impaired



- candidates should fill the application form carefully and verify/ get the details verified to ensure that the same are correct prior to final submission.
5. Candidates are advised to carefully fill and verify the details filled in the online application themselves as no change will be possible/ entertained after clicking the COMPLETE REGISTRATION BUTTON.
 6. The Name of the candidate or his /her Father/ Husband etc. should be spelt correctly in the application as it appears in the Certificates/ Mark sheets/Identity proof. Any change/alteration found may disqualify the candidature.
 7. Validate your details and Save your application by clicking the 'Validate your details' and 'Save & Next' button.
 8. Candidates can proceed to upload Photo & Signature as per the specifications given in the Guidelines for Scanning and Upload of Photograph and Signature detailed under point "C".
 9. Candidates can proceed to fill other details of the Application Form.
 10. Click on the Preview Tab to preview and verify the entire application form before COMPLETE REGISTRATION.
 11. Modify details, if required, and click on 'COMPLETE REGISTRATION' ONLY after verifying and ensuring that the photograph, signature & Brief Resume uploaded and other details filled by you are correct.
 12. Click on 'Payment' Tab and proceed for payment.
 13. Click on 'Submit' button.

(b) PAYMENT OF FEES

ONLINE MODE

1. The application form is integrated with the payment gateway and the payment process can be completed by following the instructions.
2. The payment can be made by using Debit Cards (RuPay/Visa/MasterCard/Maestro), Credit Cards, Internet Banking, Cash Cards/ Mobile Wallets.
3. After submitting your payment information in the online application form, PLEASE WAIT FOR THE INTIMATION FROM THE SERVER. DO NOT PRESS BACK OR REFRESH BUTTON IN ORDER TO AVOID DOUBLE CHARGE
4. On successful completion of the transaction, an e-Receipt will be generated.
5. Non-generation of 'E-Receipt' indicates PAYMENT FAILURE. On failure of payment, Candidates are advised to login again using their Provisional Registration Number and Password and repeat the process of payment.
6. Candidates are required to take **a printout of the e-Receipt** and online Application Form containing fee details. **Please note that if the same cannot be generated, online transaction may not have been successful.**
7. For Credit Card users: All charges are listed in Indian Rupee. If you use a non-Indian credit card, your bank will convert to your local currency based on prevailing exchange rates.
8. To ensure the security of your data, please close the browser window once your transaction is completed.
9. **There is facility to print application form containing fee details after payment of fees.**

(c) GUIDELINES FOR SCANNING AND UPLOAD OF DOCUMENTS



Before applying online a candidate will be required to have a scanned (digital) image of his/her photograph, signature as per the specifications given below.

Photograph Image: (4.5cm × 3.5cm)

- Photograph must be a recent passport style colour picture.
- Make sure that the picture is in colour, taken against a light-colored, preferably white, background.
- Look straight at the camera with a relaxed face
- If the picture is taken on a sunny day, have the sun behind you, or place yourself in the shade, so that you are not squinting and there are no harsh shadows
- If you have to use flash, ensure there's no "red-eye"
- If you wear glasses make sure that there are no reflections and your eyes can be clearly seen.
- Caps, hats and dark glasses are not acceptable. Religious headwear is allowed but it must not cover your face.
- Dimensions 200 x 230 pixels (preferred)
- Size of file should be between 20kb–50 kb
- Ensure that the size of the scanned image is not more than 50kb. If the size of the file is more than 50 kb, then adjust the settings of the scanner such as the DPI resolution, no. of colours etc., during the process of scanning.

Signature Image:

- The applicant has to sign on white paper with Black Ink pen.
 - Dimensions 140 x 60 pixels (preferred)
 - Size of file should be between 10kb – 20kb for signature
 - Ensure that the size of the scanned image is not more than 20kb
- The signature should be of the applicant and not by any other person.
- Signature in CAPITAL LETTERS shall NOT be accepted.

Brief Resume Image:

- Document Min size > 0 KB and Max Size <= 500 KB

Scanning the documents:

- Set the scanner resolution to a minimum of 200 dpi (dots per inch)
- Set Colour to True Colour
- File Size as specified above
- Crop the image in the scanner to the edge of the photograph/signature, then use the upload editor to crop the image to the final size (as specified above).
- The image file should be JPG or JPEG format. An example file name is: image01.jpg or image01.jpeg. Image dimensions can be checked by listing the folder files or moving the mouse over the file image icon.
- Candidates using MS Windows/MOOffice can easily obtain documents in .jpeg format by using MS Paint or MOOffice Picture Manager. Scanned documents in any format can



be saved in .jpg / .jpeg format by using 'Save As' option in the File menu. Size can be adjusted by using crop and then resize option.

Procedure for uploading the documents

- While filling in the Online Application Form the candidate will be provided with separate links for uploading Photograph, signature & Brief Resume.
- Click on the respective link "Upload Photograph / signature/ Brief Resume "
- Browse and Select the location where the Scanned Photograph / signature / Brief Resume file has been saved.
- Select the file by clicking on it
- Click the 'Open/Upload'
- If the file size and format are not as prescribed, an error message will be displayed.
- Preview of the uploaded image will help to see the quality of the image. In case of unclear / smudged, the same may be re-uploaded to the expected clarity /quality.

Your Online Application will not be registered unless you upload your Photograph, signature & Brief Resume as specified.

Note:

- (1) In case the face in the photograph, signature or Brief Resume is unclear / smudged the candidate's application may be rejected.
- (2) After uploading the Photograph / signature / Brief Resume in the online application form candidates should check that the images are clear and have been uploaded correctly. In case the photograph, signature & Brief Resume is not prominently visible, the candidate may edit his/ her application and re-upload his/ her photograph, signature & Brief Resume prior to submitting the form.
- (3) Candidate should also ensure that photo, signature & Brief Resume are uploaded at the appropriate places.
- (4) After registering online candidates are advised to take a printout of their system generated online application forms.
- (5) Candidates should take utmost care to furnish the correct details while filling in on-line application.
- (6) After applying on-line, the candidate should take a print out of the system generated on-line application form and retain it along with Registration Number & Password safely for future reference. The print out of the on-line application will have to be invariably submitted at the time of Interaction.
- (7) Candidates are advised in their own interest to apply on-line much before the closing date and not to wait till the last date for depositing the fees to avoid the possibility of disconnection/ inability/failure to log on to the LIC's website on account of heavy load on internet/website jam.
- (8) The LIC does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of the aforesaid reasons or for any other reason beyond the control of the LIC.
- (9) Please note that the above procedure is the only valid procedure for applying. No other mode of application or incomplete steps would be accepted and any such incomplete/incorrect applications would be rejected.
- (10) The Candidate should note/remember the password for future reference and use.



(11) The candidate must ensure that the filled in information is correct and no correction will be accepted at subsequent stage in any field.

6. GENERAL INFORMATION:

- (I) Appointment of selected candidates is subject to his/her being declared medically fit as per the requirement of the Corporation. Such appointment will also be subject to the "Terms & Conditions of LIC's Policy on Fixed Term Engagement on Contract Basis."
- (II) Decision of Corporation in all matter regarding eligibility, selection etc. would be final and binding on the candidates. No representation or correspondence will be entertained by the Corporation in this regard.
- (III) LIC reserves the right to cancel the above recruitment process at any stage of the process without assigning any reason thereof.
- (IV) Any legal proceedings in respect of any matter of claim or dispute arising out of this advertisement and/ or an application in response thereto can be instituted only in Mumbai and courts/ tribunals/ forums at Mumbai only shall have sole and exclusive jurisdiction to try any cause/ dispute.
- (V) CANVASSING IN ANY FORM WILL LEAD TO DISQUALIFICATION OF CANDIDATURE.

Mumbai:

Date: 10.09.2022

Executive Director (Personnel)