



INVITATION FOR REQUEST FOR PROPOSAL FOR DEVELOPMENT OF DATA, REPORTING AND ANALYTICS SOLUTIONS FOR LIFE INSURANCE CORPORATION OF INDIA

(Ref No. LIC/CO/IT/DT/2024/RFP/01 Dated 14.05.2024)

Corrigendum 4

S.No	Addition / Deletion / Modification	RFP Clause No. / Annexure No. & Page No.	Old Requirement / Condition / Annexure	New Requirement / Condition / Annexure
1	Modification	1.8 Appendix to RFP: Tender Information Summary (TIS) Critical Dates (ITB-clauses 2.6; 2.7; 2.8; 2.9 and 2.10); Page 3 Corrigendum 3, Point 2 Page 2	Bid Submission Closing Date & Time: Monday, 12.08.2024 till 3:30 PM Bid Opening (techno-commercial Proposal) Date & Time: Monday, 12.08.2024 at 4:00 PM	Bid Submission Closing Date & Time: Friday, 23.08.2024 till 3:30 PM Bid Opening (techno-commercial Proposal) Date & Time: Friday, 23.08.2024 at 4:00 PM
2	Modification	Form T-13: Manufacturer's Authorization Form (MAF)		Please refer to Form T-13: Manufacturer's Authorization Form (MAF) (Revised) for the revised form.
3	Modification	Form T-17: Checklist for consumption of OEM Tools/Core & Other Enterprise Systems		Please refer to Form T-17: Checklist for consumption of OEM Tools/Core & Other Enterprise Systems (Revised) for the revised form.
4	Modification	Table 6: Data security requirements, Point 1, page 237	Data encryption: Encryption of Data at rest & data in-transit as per LIC's InfoSec policy. Sensitive and personal identification data on data lake / lakehouse should be encrypted. Data encryption applies to the following data on data lake / lakehouse: <ul style="list-style-type: none"> • Data at rest • Data in motion • Data available over an API to external sources / applications • Data at end users • Data from source system during ingestion 	Data encryption: Tokenization of sensitive and PII data at rest & TLS Encryption of data in-transit as per LIC's InfoSec policy (Required certificates will be provided by LIC). Disk/data-file level encryption is required for structured data store(s). The bidder is not required to procure/integrate with HSM.

S.No	Addition / Deletion / Modification	RFP Clause No. / Annexure No. & Page No.	Old Requirement / Condition / Annexure	New Requirement / Condition / Annexure
			<ul style="list-style-type: none"> Data in use <p>Standard encryption/decryption techniques / policies should be implemented for this activity.</p> <p>Encryption should be possible at both overall database level and at finer-grained column / parameter level. This should be easily defined and implemented.</p> <p>Decryption should be allowed only to selective users/roles by complying the global standards like AES256, DES, SKC, PKC, 3DES, MD5 cryptographic hash, etc</p>	

Additional clarifications

1. The Backup strategy should exclude Object Storage. However, Backup shall include all Structured Data and RDBMS data store(s).
2. The Hot and Warm layered data requirements shall not be applicable for Object Storage.
3. The following Application Performance and Monitoring (APM) stack is available for reuse –

Category	
Logging, audit trail capture and application / database / host monitoring	ELK stack
Dashboards	Grafana
Infrastructure monitoring	Nagios XI Enterprise Edition + Prometheus
Event based alerting	ELK stack

Note: All other terms and conditions, forms of the RFP document remain unchanged. In case of any ambiguity, the RFP document will stand.

Date: 8th August 2024

Place: Mumbai

**Executive Director
(IT & Digital Transformation)**