Information Technology/SD – Central Office, 'Yogakshema', Jeevan Bima Marg, P. B. No. 19953, Mumbai - 400021

CORRIGENDUM-1

Ref : LIC-CO/IT-DT/RFP/2026-2027/DE dated 02.06.2026_Corrigendum_1 **Date:25/06/2026**

Request for Proposal for Onboarding System Integrator (SI) for supplying, commissioning, configuration and maintenance of Database Encryption Solution

Reference: LIC-CO/IT-DT/RFP/2026-2027/DE dated 02.06.2026

This corrigendum is issued to amend the Request for Proposal (RFP) **LIC-CO/IT-DT/RFP/2026-2027/DE dated 02.06.2026**. The following changes will be made in the original RFP document. All other terms and conditions of the RFP remain unchanged unless explicitly modified herein.

Amendments to the RFP

1. **Section A - Sub-section 3 Activity Schedule Table items 9 & 10**

Existing clause:

Last date & time for submission of bids	07.07.2026, latest by 03:00 PM
Bid opening date & time (Eligibility & Technical)	07.07.2026, 03:30 PM

Revised clause:

Last date & time for submission of bids	14.07.2026, latest by 03:00 PM
Bid opening date & time (Eligibility & Technical)	14.07.2026, 03:30 PM

2. **Number of database instances under various database types.**

Database	**Number of Instances**
HANA DB	14
MongoDb	23
MySQL	795
Oracle	48
PostgreSQL	143
Teradata	17
Vertica	45
Total	**1085**

3. **Bidders may use the Bank account details of LIC for submitting the EMD as Bank guarantee.**

Bank Name	KOTAK MAHINDRA BANK
BANK ADDRESS	5 C/II, GROUND FLOOR, MITTAL COURT, 224, NARIMAN POINT, MUMBAI-400021
TITLE OF BANK A/C	LIFE INSURANCE CORPORATION OF INDIA
TYPE OF BANK A/C	CURRENT
BANK ACCOUNT NO.	7311115782
IFSC	KKBK0000958
MICR CODE	400485002
SWIFT CODE	KKBKINBBCPC

4. **RFP Section -B - Clause -6. Eligibility criteria -- Page no-17 -18. & Annexure-C -Eligibility criteria Page no-128 Sr no-2**

Sr no	Existing Clause	Revised Clause
2	The Bidder must have an annual turnover of minimum Rs. 100 Crores per annum during the last 03 (three) years preceding the date of this RFP For MSME bidders, the turnover requirement will be as follows: • the MSME bidder must have an average turnover of Rs. 15 Crores in the last three financial years (i.e., 2022-2023, 2023 2024, 2024-2025), instead of the minimum turnover of Rs. 100 Crores as stipulated for other bidders. • Furthermore, MSME bidders must have made a profit (before tax) in each of the last three financial years (i.e., 2022-2023, 2023 2024, 2024-2025). • The MSME bidder must submit a valid MSME registration certificate along with the necessary financial documents to support the above criteria	The Bidder must have an annual turnover of minimum Rs. 100 Crores per annum during the last 03 (three) years preceding the date of this RFP For MSME bidders, the turnover requirement will be as follows: • the MSME bidder must have an average turnover of Rs. 15 Crores in the last three financial years (i.e., 2022-2023, 2023 2024, 2024-2025), instead of the minimum turnover of Rs. 100 Crores as stipulated for other bidders. • Furthermore, MSME bidders must have made a profit (before tax) in each of the last three financial years (i.e., 2022-2023, 2023 2024, 2024-2025). • The MSME bidder must submit a valid MSME registration certificate along with the

		necessary financial documents to support the above criteria. In case the audited/published financial statements for FY 2025-26 are available, bidders may submit financial statements for FY 2023-24, FY 2024-25, and FY 2025-26, provided the financial statements for FY 2025-26 have been duly finalized, approved, and published/audited as on the bid submission date. In case the audited/published financial statements for FY 2025-26 are not available as on the bid submission date, the evaluation shall be based on FY 2022-23, FY 2023-24, and FY 2024-25 as specified in the RFP. The bidder shall adopt only one of the above approaches consistently for all financial eligibility criteria requiring assessment of turnover and profitability. All other terms and conditions of the RFP shall remain unchanged.

Accordingly, Annexure-B stands revised as follows:

Annexure B: Bidder's Profile

Sub: Life Insurance Corporation of India – RFP/Tender for Onboarding System Integrator (SI) for supplying, commissioning, configuration and maintenance of Database Encryption Solution

Ref: LIC-CO/IT-DT/RFP/2026-2027/DE dated 02.06.2026

S No	Details	Bidder Response	
1	**Company Background**		
	Name of the Firm/ Company		
	Year of Incorporation if India		
	Type of the Company [Govt/PSU/Pub.Ltd/Pvt ltd/ JV/LLP etc.]		
2	**Address**		
	Corporate Office (HQ)		
	Local Office in Mumbai		
	GST registration number and date of registration		
	PAN card number		
3	**Authorized Contact person**		
	a) Name and Designation		
	b) Telephone number/ Mobile No.		
	c) E-mail ID		
4	**Financial Parameters**		
	Business Results (last three years)	Annual Turnover (Rs. In Crores)	PBT (Rs. In Crores)
	2024-25 or 2025-26		
	2023-24 or 2024-25		
	2022-23 or 2023-24		
	(Only company figures need to be mentioned. Not to include group/ subsidiary company figures)	(Mention the above amount in INR only)	

Note: Enclose copies of Audited Balance Sheet along with enclosures.

Authorized Signatory of the bidder
Name:
Designation:
Date:
Place:
Seal of the company

5. **Section-C -Clause-11-Opening of bids – point (d)**

Existing provision:

"(d) The passwords of password-protected files shall be called for from Bidders during the Bid evaluation stage."

Revised provision:

Point (d) of Clause 11 under Section C stands deleted.

6. **RFP – Annexure -F – KMS/HSM related specifications Page no –133, 134**

Srno	Existing specification	Revised Specification
11	Support symmetric cryptographic algorithms including AES, ARIA, SEED, RC2, RC4, RC5, CAST and GCM.	Support symmetric cryptographic algorithms including AES (128/192/256-bit),Triple DES (for legacy compatibility),GCM mode for authenticated encryption. Legacy algorithms such as DES or RC-series algorithms to be supported only for backward compatibility where required
39	Solution should detect compromises or unauthorized modifications and send alerts (through email and SMS Gateway)	Solution should detect compromises or unauthorized modifications and generate alerts through email and support integration with enterprise monitoring/notification systems including syslog, SNMP, SIEM, APIs, and SMS Gateway for notification delivery.
41	Provide proactive notifications before key expiry, rotation or lifecycle events via email and SMS.	Provide proactive notifications before key expiry, key rotation, or other key lifecycle events through email or integration with enterprise monitoring, SIEM, ITSM, notification platforms, or other supported alerting mechanisms.
47	OEM should have warehouse in India for hardware replacement.	OEM/Bidder should have warehouse in India for hardware replacement.

Annexure-F -Page 135--2. Encryption Software / Encryption Agent Specifications

16	The solution should continuously perform integrity checks to detect unauthorized modifications –	The solution shall continuously detect unauthorized modifications, including ransomware-induced changes,

	including ransomware attacks – and promptly revert data to its secure state	and shall provide mechanisms, either natively or through integrated components, to restore/recover affected data to a secure and trusted state.

The following specifications have been added in Annexure-F

- The KMS shall support quantum-safe communication between KMS clients and KMS servers using Hybrid PQC TLS with NIST-standardized post-quantum cryptographic algorithms (e.g., ML-KEM and ML-DSA), aligned with Government of India quantum-safe migration guidelines for Critical Information Infrastructure (CII), and shall provide cryptographic agility with support for future migration to full PQC operation.
- All proposed hardware appliances including HSM, KMS and other security appliances shall support Fibre connectivity for integration with existing environment

** Revised Annexure-F is provided in Appendix-1

Appendix-1:

Annexure F: Technical Compliance

Sub: Life Insurance Corporation of India – RFP/Tender for Onboarding System Integrator (SI) for supplying, commissioning, configuration and maintenance of Database Encryption Solution

Ref: LIC-CO/IT-DT/RFP/2026-2027/DE dated 02.06.2026

Technical Specifications for proposed DE Tool

1. KMS / HSM Related Specifications

#	Specification	Complied (Y/N)
1	The Key Management Software and HSM should be from the same vendor for seamless integration and Root of Trust.	
2	Central dashboard for Key Management Solution to maintain all the encryption keys.	
3	Should have built-in secret management without any extra license cost.	

4	The HSM solution should be a tamperproof hardware box supporting operating systems such as Windows and Linux.	
5	Host interface should support minimum 3 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6.	
6	Proposed HSM should have FIPS 140-3 Level 3 certified cryptographic boundary to store cryptographic keys in tamper-evident FIPS 140-3 boundary. The FIPS certification of the HSM should be in the name of OEM and listed on NIST website.	
7	Minimum 100 partitions with isolation using user ID/password and memory isolation as per CCA IVG guidelines.	
8	Random number generation compliant with AIS 20/31 8 DRG.4 using hardware-based entropy source.	
9	Support cryptographic APIs including PKCS#11, Java (JCA/JCE), Microsoft CAPI/CNG, Rest API, and OpenSSL	
10	Support asymmetric cryptographic algorithms including RSA (1024–4096 bits), DSA, ECDSA, ECDH and ECC.	
11	Support symmetric cryptographic algorithms including AES (128/192/256-bit),Triple DES (for legacy compatibility),GCM mode for authenticated encryption. Legacy algorithms such as DES or RC-series algorithms to be supported only for backward compatibility where required	
12	HSM should support built-in clustering with Active-Active configuration.	
13	HSM Should support minimum 2000 Transaction(Signing) per Second @ RSA 2048 bits and expandable up to 10000 Transaction (Signing) per Second @ RSA 2048 bits and storage of at least 10000 keys in FIPS validated boundary.	
14	Built-in controls to detect and respond against tampering attempts.	

15	Support public key algorithms including RSA encryption/decryption, RSA sign/verify and ECC cryptography.	
16	Should provide a web based solution for administration, monitoring, and provisioning	
17	Full Suite B implementation with ECC including ECDSA and ECDH with named, user-defined and Brainpool curves.	
18	Keys must remain securely within the HSM FIPS 140-3 Level 3 cryptographic boundary throughout their lifecycle.	
19	API support including REST (JWT), KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C, Java APIs and OpenSSL.	
20	HSM must support onboard key generation and secure storage of minimum 10000 keys within the FIPS boundary of the HSM.	
21	Architecture should support failover, high availability, load balancing and scalability across devices/chassis.	
22	System shall support key caching, key rotation and key versioning without downtime.	
23	System shall support secure key destruction ensuring keys cannot be recovered.	
24	Support Key Management Interoperability Protocol (KMIP) version 2.0 or above.	
25	KMIP profiles covering client/server cryptography and storage arrays with self-encrypting drives.	
26	Support KMIP for tape libraries and symmetric/asymmetric key lifecycle management.	
27	Support key caching, key rotation and versioning without downtime.	
28	Support secure key destruction ensuring keys cannot be recovered.	

29	Support secure key backup with same level of protection and backward/forward compatibility during restoration.	
30	Support recovery of lost or corrupted keys with secure multi-admin backup and restoration process.	
31	Discover, create, renew and manage keys across heterogeneous and geographically distributed environments.	
32	Ensure secure delivery of keys to integrated source systems with integrity protection.	
33	Support automated key expiry management.	
34	Provide secure vault for key storage with integration capability for third-party vaults.	
35	Provide comprehensive APIs for communication with third-party systems.	
36	Support BYOK/BYOE for cloud platforms such as AWS, Azure, Salesforce and Oracle.	
37	KMS should support multiple partitions mapped to separate HSM partitions, each KMS partition master key should be stored in separate/unique partition of HSM	
38	EKMS should support different roles and RBAC.	
39	Solution should detect compromises or unauthorized modifications and generate alerts through email and support integration with enterprise monitoring/notification systems including syslog, SNMP, SIEM, APIs, and SMS Gateway for notification delivery.	
40	Support multiparty control and key splitting mechanisms.	
41	Provide proactive notifications before key expiry, key rotation, or other key lifecycle events through email or integration with enterprise monitoring, SIEM, ITSM, notification platforms, or other supported alerting mechanisms.	
42	Provide holistic view of keys across the enterprise environment.	

43	Provide automated real-time event alert mechanisms.	
44	Generate system logs/events including login activity and system changes.	
45	Provide 5-year onsite comprehensive warranty.	
46	OEM should have support center in India.	
47	OEM/Bidder should have warehouse in India for hardware replacement.	
48	The Key Management System (KMS) shall utilize cryptographic modules validated to FIPS 140-2 or FIPS 140-3 and shall operate in FIPS-approved mode. The KMS shall integrate with a dedicated Hardware Security Module (HSM) that is validated to FIPS 140-3 Level 3 or higher and listed on the NIST CMVP database with a valid and active certificate.	
49	The solution should provide a unified web interface to manage all KMS and integrated HSMs across different locations, support versatile Key and Secret Vaults with a decentralized security model so that data can be protected in line with differing local security policies and comply with regulatory mandates	
50	The proposed HSM should be scalable and field upgradable in future without changing the hardware.	
51	There should not be any limit on no. of Keys to be protected by HSM in accordance with FIPS 140-3 and CCA guidelines.	
52	The HSM should be scalable to support multi tenant architecture on the same device without the need of changing the hardware.	
53	The HSM must support multiple and multi-level administration with Two factor authentication using smart cards/tokens on the same device without changing the hardware.	

54	The HSM shall support scalable integration with multiple client systems (including KMS instances, databases, and applications) across data centers without restrictive per-client licensing limits.	
55	The proposed HSM and KMS solution should support or be upgradeable to support NIST-standardized Post Quantum Cryptographic(PQC) algorithms such as ML-KEM & ML-DSA.	
56	The KMS should support crypto-agility architecture enabling migration of cryptographic algorithms, protocols and keys without application redesign	
57	The solution should support Post-Quantum Cryptography (PQC) ready architecture with support for hybrid cryptographic models combining classical and post-quantum algorithms.	
58	The KMS should support cryptographic attestation for validating integrity of cryptographic modules and keys	
59	The KMS shall support quantum-safe communication between KMS clients and KMS servers using Hybrid PQC TLS with NIST-standardized post-quantum cryptographic algorithms (e.g., ML-KEM and ML-DSA), aligned with Government of India quantum-safe migration guidelines for Critical Information Infrastructure (CII), and shall provide cryptographic agility with support for future migration to full PQC operation.	
60	All proposed hardware appliances including HSM, KMS and other security appliances shall support Fibre connectivity for integration with existing environment	

2. Encryption Software / Encryption Agent Specifications

#	Specification	Complied (Y/N)

1	Check for encryption key algorithm and strength used by encryption software.	
2	Support encryption software for operating systems like RHEL, Linux on IBM-Z, CentOS , Oracle Enterprise Linux , Suse Linux , Windows servers.	
3	Support encryption software for Windows Server.	
4	The encryption solution shall support data-at-rest encryption for heterogeneous database platforms including MongoDB, MySQL, Oracle Database, and PostgreSQL through native integration mechanisms such as KMIP, PKCS#11, or database-specific key management interfaces. Where native integration is not available or limited (e.g., SAP HANA, Teradata, Vertica), the solution shall support alternative approaches including agent-based or agentless encryption while ensuring integration with the centralized KMS for key management. Preference shall be given to native database encryption mechanisms where supported.	
5	Central dashboard to maintain and manage server encryption health status.	
6	Support scheduled and automatic key rotation for encrypted databases and folders with minimal downtime.	
7	Support ACL-based encryption policies where users see only ciphertext or have restricted access.	
8	Support ACL-based decryption policies for authorized users to view plaintext.	
9	The solution should support an agent or agentless file encryption approach.	

10	The solution should secure structured and semi-structured data stored in databases across on-premises, cloud, hybrid, and multi-cloud environments. The solution should support encryption of data at rest and, where applicable, data in transit and data in use for enterprise database platforms.	
11	Easy integration with existing applications and data workflows	
12	The solution shall continuously detect unauthorized modifications, including ransomware-induced changes, and shall provide mechanisms, either natively or through integrated components, to restore/recover affected data to a secure and trusted state.	
13	The Database Transparent Encryption software should be fully compatible with Oracle Exadata engineered systems and support Oracle Real Application Clusters (RAC) architecture and **Oracle Automatic Storage Management (ASM) file system/storage architecture.	
14	The encryption solution should be fully compliant with the architecture of supported databases and should not introduce performance degradation, operational incompatibilities, or require any modifications to database binaries, database processes, or native database operations.	
15	The encryption solution shall support native database-aware encryption for supported databases and should not rely solely on file system or storage layer encryption mechanisms.	
16	The encryption solution should introduce minimal performance overhead and should not significantly impact database throughput, latency, or system performance under normal workloads. The bidder shall provide benchmark results or reference implementations demonstrating performance impact.	
17	The encryption solution shall not require modification of database binaries, database kernel components, or application code.	
18	The encryption solution should be fully compatible with native backup, restore, replication, and recovery utilities of supported	

	databases and should allow such operations to be performed without requiring decryption of the protected data or impacting database availability and performance.	

7. Section-E Scope of Work. Page no-79

Existing clause

Cryptographic Capabilities

The HSM shall support:

- RSA (2048–4096 bits; support for 1024 bits only for legacy compatibility)
- Elliptic Curve Cryptography (ECC) including ECDSA and ECDH
- DSA (where required for legacy compatibility)

The HSM shall support modern cryptographic algorithms aligned with NIST and industry standards.

Symmetric cryptography support shall include:

- AES (128/192/256-bit)
- Triple DES (for legacy compatibility)
- ARIA
- SEED
- CAST
- GCM mode for authenticated encryption

Legacy algorithms such as DES or RC-series algorithms may be supported only for backward compatibility where required.

Revised Clause

Cryptographic Capabilities

The HSM shall support:

- RSA (2048–4096 bits; support for 1024 bits only for legacy compatibility)
- Elliptic Curve Cryptography (ECC) including ECDSA and ECDH
- DSA (where required for legacy compatibility)

The HSM shall support modern cryptographic algorithms aligned with NIST and industry standards.

Symmetric cryptography support shall include:

- AES (128/192/256-bit)
- Triple DES (for legacy compatibility)
- GCM mode for authenticated encryption

Legacy algorithms such as DES or RC-series algorithms may be supported only for backward compatibility where required.

8. Section G: Payment Terms & Conditions

Page 118

Existing Payment schedule

Sr. No.	Items	Milestone	Percentage
1	Hardware	Delivery of the all-hardware items, rack-mounting, power on and submission of the invoice with proof of delivery and other documents (after due inspection). Submission of Undertaking -B, Undertaking-C and Declaration-A	60%
		Successful installation and acceptance of the hardware (after due inspection) including DR	20%
		One month after Go-LIVE	20%
2	Software	Delivery of respective software & its related components as per actual supply (after due diligence)	60%
		Successful installation, configuration, completion of customization and acceptance of systems for respective applications	20%
		One month after Go-LIVE	20%
3	Implementation Cost	On Successful Go Live including successful DR execution	100%
4	MySQL native encryption costs	On completion of successful implementation of Native encryption on all MySQL databases	100%

5	AMC/ATS	The AMC/ATS shall commence on completion of warranty period.	Quarterly in arrears
6	Training Cost	On Completion	100%
6	Facility Management Service	Quarterly arrears based on submission of error free invoice	Quarterly in arrears

Revised Payment schedule

Sr. No.	Items	Milestone	Percentage
1	Hardware	Delivery of the all-hardware items, rack-mounting, power on and submission of the invoice with proof of delivery and other documents (after due inspection). Submission of Undertaking -B, Undertaking-C and Declaration-A	70%
		Successful installation and acceptance of the hardware (after due inspection) including DR	20%
		One month after Go-LIVE	10%
2	Software	Delivery of respective software & its related components as per actual supply (after due diligence)	65%
		Successful installation, configuration, completion of customization and acceptance of systems for respective applications	20%
		One month after Go-LIVE	15%
3	Implementation Cost	On Successful Go Live including successful DR execution	100%
4	MySQL native encryption costs	On completion of successful implementation of Native encryption on all MySQL databases	100%
5	AMC/ATS	The AMC/ATS shall commence on completion of warranty period.	Quarterly in arrears
6	Training Cost	On Completion	100%

6	Facility Management Service	Quarterly arrears based on submission of error free invoice	Quarterly in arrears

All other payment terms & conditions remain unchanged.

These Corrigendum/Modifications to Request for Proposal for Onboarding System Integrator (SI) for supplying, commissioning, configuration and maintenance of Database Encryption Solution are issued with the approval of Secretary (IT/DT).

Secretary (IT/DT)