Responses to Pre-bid Queries received through mail and during thePre-bid meeting						
Sr.	**RFP**	**Sub-**	**Pg.No**	**RFP clause**	**Bidder query**	**LIC's Response**
1	Section E	Project Timelines 2	100	Delivery of all the equipment (Hardware and Software) as quoted in the bill of materials for the DE Solution. Date of delivery of last item shall be taken as date of delivery for all items. It is T+8 Weeks	Considering the vast scope of work and involvment of multiple OEMs Requested you to please make it T+12 Weeks	No Change.Please be guided by the terms and conditions in RFP
2	Section E	Project Timelines 3	100	Current State Assessment & Project Planning. Understanding of the current landscape of LIC, project plan creation, documentation, HLD creation, use case creation, collating list of users and applications to be integrated and any other activities as required as part of scope(Planning & Designing Phase). It is T+10 Weeks	Considering the vast scope of work and involvment of multiple OEMs Requested you to please make it T+14 Weeks	No Change.Please be guided by the terms and conditions in RFP
3	Section E	Project Timelines 4	100	Implementation of the DE solution (Date of integration of last database shall be taken as date of completion of implementation) (Implementation phase). It is T+24 Weeks	Considering the vast scope of work and involvment of multiple OEMs Requested you to please make it T+28 Weeks	No Change.Please be guided by the terms and conditions in RFP
4	Section E	Project Timelines 5	100	Policy fine-tuning for all the deployed policies during implementation phase (Pilot phase--where the installed system or solution is deployed in a limited, controlled environment to evaluate its performance, usability, and effectiveness before a full-scale rollout). It is T+28 Weeks	Considering the vast scope of work and involvment of multiple OEMs Requested you to please make it T+32 Weeks	No Change.Please be guided by the terms and conditions in RFP
5	Section E	Project Timelines 6	100	User Acceptance Testing (UAT) (UAT phase) T + 30 Weeks	Considering the vast scope of work and involvment of multiple OEMs Requested you to please make it T+34 Weeks	No Change.Please be guided by the terms and conditions in RFP
6	Section E	Rate Validity	105	The unit prices quoted by the successful bidder and finalized through the Online Reverse Auction (ORA) shall remain firm and valid for a period of five (5) years from the date of issuance of the first Purchase Order under this RFP	Considering the dollar fluctuation factor it is requested you to please keep the rate validity only for 180 days. Also, OEM does not provide the rate validity of 5 years.All the OEMs provide bid/price validity for maximum 180 days.	No change. Please be guided by the terms and conditions specified in RFP.

7	Section G	Annexure F: Technical Compliance 1	132	The Key Management Software and HSM should be from the same vendor for seamless integration and Root of Trust.	We request the Purchaser to modify this clause by removing the requirement that the Key Management Software (KMS) and HSM must be from the same vendor. The clause may instead state:"The proposed Key Management Software (KMS) shall seamlessly integrate with the proposed HSM and establish a secure root of trust." The requirement for KMS and HSM to be from the same OEM is technically unnecessary and restricts fair competition. Modern enterprise-grade KMS solutions support seamless integration with industry-standard HSMs from multiple OEMs through standard APIs and interfaces such as PKCS#11, KMIP, and JCE/JCA, while maintaining the required Root of Trust and security controls. Mandating the same vendor unnecessarily limits participation to a very small number of OEMs, reduces competition, and restricts the Purchaser's ability to evaluate best-of-breed solutions. Removing this OEM restriction while retaining the interoperability and security requirements will encourage wider bidder participation without compromising functionality,	No change.Please be guided by the terms and conditions in RFP
8	Annexure-W p.182 vs Section E p.74 / p.92	Annexure-W p.182 vs Section E p.74 / p.92	Annexure-W p.182 vs Section E p.74 / p.92	Annexure-W: size HW for 1,085 servers + 10% growth/yr over 5 yrs. Section E: initial procurement 'up to 10 DB instances'; KMS/HSM/HW qty 'decided after technical presentation'.	Please clarify the basis on which bidders must size and price HSM, KMS and associated hardware: for the initial 10 DE instances + MySQL native, or for the full 1,085-server estate. The two instructions imply very different Bills of Material.	Please refer to Annexure-W in RFP document. Sizing of the KMS and HSM infrastructure shall be based on the total number of database instances and the year-on-year growth projections specified in Annexure-W. Bidders are required to propose, as part of their Technical Bid, the solution deployment architecture and the corresponding Bill of Material (BoM) best suited to meet LIC's requirements.(Please refer to Section-C - Clause 12. Evaluation process for selection of bidder - sub-clause -g) Technical bid evaluation criteria--page-35 of RFP document) LIC intends to utilize native Data-at-Rest Encryption capabilities of database platforms wherever such capabilities are available, supported, and compatible with LIC's requirements. The procurement of ten (10) third-party Database Encryption licenses is intended for price discovery and for deployment in scenarios where native database encryption is not available, supported, or otherwise feasible.
9	Section E	Initial Phase table	p.92,	KMS, HSM and associated HW quantities = 'Will be decided after technical presentation by bidders'.	With HSM/KMS/associated-HW quantities open, how will commercial bids and the ORA be evaluated on a like-for-like basis across bidders? Will LIC	Please refer to RFP document -Section-C -page no-35 under Clause (g)Technical bid evaluation criteria
10	Annexure-W		p.182	1,085 servers given by Active/Passive/Read-Only and by location; database engines listed but not mapped to server counts.	Please provide the number of database instances/servers per engine type (Oracle Enterprise/Standard, PostgreSQL, MongoDB, SAP HANA, Teradata, Vertica, MySQL). OEM DE licensing depends on this split.	Please refer to corrigendum-1, Sr.No: 2

11	Section E		p.74-75	Third-party DE licensing model not specified.	Confirm the licensing metric for the third-party DE solution: per database instance, per host/server, or per CPU core. Confirm whether the 600 MySQL native instances are fully excluded from third-party DE licensing.	Please refer to Page 92 of RFP-Section-E-Clause-4.Phased Procurement and Rate Validity for Future Quantities. Number of MySQL databases instances are provided in Corrigendum-1,Sr.No: 2
12	Sec B Eligibility (Sr 5) ~p.19 vs Section E HSM p.78 & Annexure-F	Sec B Eligibility (Sr 5) ~p.19 vs Section E HSM p.78 & Annexure-F	Sec B Eligibility (Sr 5) ~p.19 vs Section E HSM p.78 & Annexure-F	Eligibility: HSM 'preferably FIPS 140-2 Level 3 or higher'. Section E / Annexure-F: HSM 'FIPS 140-3 Level 3 or higher certified'.	Please confirm the binding HSM requirement is FIPS 140-3 Level 3. The eligibility and technical-spec clauses are inconsistent.	The Eligibility Criteria specify the bidder qualification requirements with respect to prior experience in supply, installation, configuration, implementation, and maintenance of similar solutions. The technical requirements and features of the proposed solution are detailed separately in Annexure-F (Technical Compliance) and the Scope of Work section of the RFP. Bidders are required to comply with both the eligibility criteria and the technical specifications stipulated in the RFP.
13	Section E Annexure-W		p.75; p.182	Platform support listed includes AIX and Linux on IBM-Z.	Confirm whether host-based third-party DE agents are mandatorily required on AIX and Linux-on-IBM-Z, and for how many hosts. Third-party DE agent support on these platforms varies by OEM.	At present, LIC does not have any AIX systems in its environment. However, Linux on IBM-Z (Red Hat Enterprise Linux) is in use. Bidders shall support Linux on IBM-Z as per the requirements specified in the RFP.
14	Section D Annexure-W		p.69-71;	Current data-at-rest encryption state not specified.	Please specify the data-at-rest encryption currently enabled per database engine (e.g., native TDE, file/volume encryption, self-encrypting drives), if any.	Please refer to Scope of Work. Implementation of Native encryption on MySQL databases is part of scope of work of the bidder. Other databases are either already encrypted using native encryption or will be encrypted thru native encryption.
15	Section E		p.72-73	eFEAP MySQL: 150+ instances (~600 with replicas), v8.0.34 upgrading to 8.4.8, native encryption.	Confirm the MySQL keyring/component approach LIC intends (e.g., keyring_file vs KMIP-backed keyring) and that the proposed KMS/HSM must integrate via that mechanism, for both 8.0.34 and 8.4.8.	LIC has not mandated a specific MySQL keyring/component implementation (e.g., keyring_file, keyring_vault, KMIP-backed keyring, cloud-native keyring, or equivalent). The bidder shall implement native MySQL data-at-rest encryption and integrate with the proposed KMS/HSM through a supported MySQL key management mechanism. The bidder shall ensure compatibility and supportability for the proposed approach with MySQL 8.0.34 and MySQL 8.4.8.

16	Sec C Clause 28 (single product) vs Section E	Sec C Clause 28 (single product) vs Section E	Sec C Clause 28 (single product) vs Section E	Clause 28: propose only one product/solution per requirement. Section E mandates BOTH MySQL native encryption AND a third-party DE solution.	Confirm that proposing MySQL native encryption together with a single third-party DE product for non-MySQL databases does not violate the single-product-per-requirement rule.	Please refer to RFP Scope of Work. Implementation of Native encryption on MySQL databases is part of scope of work of bidder.
17	Section E		p.76-77	KMS must interoperate with KMIP-compliant systems / SEDs / encrypted storage arrays.	Please specify the storage platforms, SED models and encrypted arrays in scope for KMIP integration, with quantities.	Specific storage platforms, SED models, encrypted arrays, and quantities are not defined at this stage. Bidders shall confirm support for industry-standard KMIP interoperability and provide details of supported platforms and any associated limitations or prerequisites.
18	Section E		p.72, p.77	SIEM integration named variously as Splunk, QRadar, FortiSIEM.	Confirm the specific SIEM platform(s) in production for log/audit integration.	The SIEM platform(s) currently in production include Splunk. Bidders shall ensure compatibility and integration support with other industry-standard SIEM platforms like Qradar, FortiSIEM etc. for log and audit event forwarding.
19	Annexure-W		p.182	'Provision for DC, DR and UAT; systems in HA mode.'	Confirm the minimum number of HSM appliances expected per site (DC, DR, UAT) for HA, or confirm this is entirely bidder-proposed.	The minimum number of HSM appliances per site is not prescribed. Bidders shall propose the required HSM sizing and deployment architecture to meet the DC, DR, and UAT requirements, including High Availability (HA), resiliency, and performance requirements specified in the RFP. Please refer to RFP document Section- C - Clause 12. Evaluation process for selection of bidder - sub-clause-(g) Technical bid evaluation criteria
20	Annexure-W		p.182	'Beyond 6 months till 5 years logs moved to secondary storage / archival.'	Confirm whether the secondary/archival storage for logs is provided by LIC or must be sized, supplied and priced by the bidder.	Secondary/archival storage required for log retention shall be sized, supplied, implemented, configured, and supported by the bidder as part of the proposed solution to meet the retention requirements specified in the RFP.
21	Sec C Clause 27 (PBG)	Sec C Clause 27 (PBG)		PBG = 5% of 'total contract value'; procurement is phased with open-ended future quantities.	Confirm whether PBG is 5% of the initial purchase-order value or of an estimated total contract value, given phased/open-ended procurement.	The Performance Bank Guarantee (PBG) shall be submitted for 5% of the value of the Purchase Order(s) issued under the contract. For additional procurements thereafter during the contract period, the PBG requirement shall be based on the value of the respective Purchase Order(s) and not on any indicative or open-ended future quantities.
22	Section G (Warranty /AMC)			5-year comprehensive warranty + AMC/ATS.	Confirm whether the 5-year warranty/AMC clock starts at each item's delivery or at solution go-live, given a phased rollout across many servers.	Please refer to Section-C - Clause 58. Important time-limits Page-66 of RFP document

23	Annexure U (Make in India)			Make-in-India certificate + auditor certificate for value > Rs 10 Cr.	Confirm whether the foreign OEM (HSM manufacturer) must furnish a local-content certificate, or only the bidder, and confirm the prescribed format/issuing authority for the statutory/cost-auditor certificate.	As per Annexure-U of the RFP, the Make in India Certificate is required to be submitted by both the OEM and the bidder. In case the OEM's product does not contain any local content, the OEM may declare the applicable local content percentage, including zero (0%) local content, as per the provisions of the Public Procurement (Preference to Make in India) Order and amendments thereto. Where the total contract value exceeds ₹10 crore, the certificate shall be certified by the Statutory Auditor/Cost Auditor of the OEM and the bidder, as applicable.
24	Eligibility Criteria			Turnover for MSME Bidder	The eligibility criteria currently consider the average turnover of FY 2022-23, FY 2023-24, and FY 2024-25. We request that the latest financial year, FY 2025-26, also be considered and the average turnover be computed based on the latest three financial years, i.e., FY 2023-24, FY 2024-25, and FY 2025-26, as this would provide a more current assessment of bidders' financial strength. Further, since FY 2025-26 may not yet be audited	Please refer to the corrigendum-1, Sr.No: 4
25	Annexure F: Technical Compliance	1. KMS / HSM Related Specifications, Point No : 6	132	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.	We would request to add the below clause to the specification: The HSM board within the network chassis must be manufactured, engineered, and IP owned by the OEM, with full lifecycle responsibility and assurance retained. Rebranded, private label, or third party sourced cryptographic modules are not permitted.	No change.Please be guided by the terms and conditions in RFP
26	Annexure F: Technical Compliance	1. KMS / HSM Related Specifications, Pont No : 6	132	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.	We would request to add the below clause to the specification: Apart from the FIPS 140-3 Level 3 certification, the HSM should also have CC EAL4+ certification. The certification should be in the name of OEM.	No change.Please be guided by the terms and conditions in RFP
27	Annexure F: Technical Compliance	1. KMS / HSM Related Specifications, Point No : 13	132	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.	For a KMS solution, having an HSM with 2000 RSA 2048 signings/second as the TPS will be an overall. Ideally 500 TPS should suffice and more than enough. In case the business need arises in future, the HSM should be scalable to 10,000 TPS on the same device without changing the hardware. We request LIC to amend this clause accordingly.	No change.Please be guided by the terms and conditions in RFP

28	Annexure F: Technical Compliance	1. KMS / HSM Related Specifications, Point	134	OEM should have warehouse in India for hardware replacement.	Request you to please amend this clause to: OEM/Bidder should have warehouse in India for hardware replacement.	Please refer to the corrigendum-1 , Sr.No: 6
29	Annexure F: Technical Compliance	1. KMS / HSM Related Specifications, Point No : 48	134	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.	Since the core requirement is for Encryption and Key management, hence it's very required for the Key Management System to be at least FIPS 140-2 Level 1 certified with the FIPS 140-2 Level 1 certification in the name of OEM. We humbly requesting LIC to add this point to the clause.	The clause stands clarified that the proposed Key Management System (KMS) shall utilize cryptographic modules validated to FIPS 140-2 Level 1 or higher, or FIPS 140-3, and shall operate in FIPS-approved mode. The KMS shall integrate with a dedicated HSM validated to FIPS 140-3 Level 3 or higher with a valid and active NIST CMVP certification. No additional requirement for separate FIPS certification of the KMS product in the OEM's name is envisaged.
30	Annexure F: Technical Compliance	2. Encryption Software / Encryption Agent	135	Support encryption software for operating systems like RHEL, Linux on IBM-Z, CentOS , Oracle Enterprise Linux , Suse Linux , Windows servers.	We humbly requesting LIC to please remove Linux on IBM-Z, since it's not widely used. Most of the Linux distributions are RHEL, Oracle Linux, CentOS, SUSE.	The RFP requirement stands . The Operating system Linux on IBM-Z RedHat Enterprise is being used .
31	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 3	132	Should have built-in secret management without any extra license cost.	Kindly clarify the intended use case and requirement for the Secret Management solution as part of the proposed Database Encryption solution. Please provide details of the applications that are expected to integrate with the Secret Management solution, along with the total number of applications in scope. Additionally, Point No. 34 requires the KMS to support integration with third-party vaults for secure storage of keys. In view of this requirement, kindly clarify the technical rationale for a separate Secret Management solution and its intended use cases, particularly where a third-party vault is proposed to be used.	Built-in Secret Management is required as part of the solution to support secure management of application credentials, service accounts, API keys, tokens, certificates, and other sensitive secrets, in alignment with applicable regulatory and cybersecurity requirements. At this stage, the specific applications and quantities are not fixed. The solution should support integration with LIC's existing and future applications without requiring additional licensing costs for Secret Management capabilities. The requirement for third-party vault integration (Point 34) is distinct and relates to interoperability with external key management and vault solutions for cryptographic key storage and management. Secret Management and third-party vault integration serve different but complementary functions and are both required under the proposed solution.
32	Annexure F: Technical Compliance 1. KMS /	Point 5	132	Host interface should support minimum 3 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6.	Requesting LIC to change this requirement to "1 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6" as 1 Gigabit ethernet ports is widely used industry standrd and more than enough for this requirement.	No change.Please be guided by the terms and conditions in RFP

33	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 7	132	Minimum 100 partitions with isolation using user ID/password and memory isolation as per CCA IVG guidelines.	Partitions are primarily required when the HSM is shared across multiple applications or environments that require cryptographic isolation. In the current design, the HSM is dedicated to supporting CipherTrust as the Root of Trust only. Typically, only one partition is enough to serve the RoT use case. Increasing the partition count would not provide additional benefit for this architecture. The proposed HSM anyways comes with 5 partitions. Request LIC to revise the requirement to "Minimum 5 partitions with isolation using user ID/password and memory isolation as per CCA IVG guidelines"	No change.Please be guided by the terms and conditions in RFP
34	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 13	132	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.	The proposed HSM is intended to serve as the Root of Trust for the KMS, supporting secure key generation, storage, wrapping/unwrapping, and lifecycle management of encryption keys. As the HSM is not intended for high-volume cryptographic signing applications such as PKI Certificate Authorities, UPI payments, or digital signature services, the requirement of minimum 2000 RSA-2048 signing TPS expandable up to 10000 TPS appears significantly higher than the expected workload for the proposed use case. Requesting LIC to review and revise the requirement to a more appropriate performance benchmark, such as minimum 1000 RSA-2048 signing TPS which is more than enough for this requirement.	No change.Please be guided by the terms and conditions in RFP
35	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 16	132	Should provide a web based solution for administration, monitoring, and provisioning	Requesting LIC to update this requirement as "Should provide a web based solution for administration, monitoring, and provisioning of KMS solution". HSM being highly secure cryptographic devices, are typically administered and provisioned through secure CLI and dedicated security administration utilities rather than web-based interfaces.	The clause stands clarified. The proposed solution shall provide a web-based interface for administration, monitoring, and provisioning of the Key Management System (KMS). Administration and provisioning of the HSM may be through secure command-line interfaces, dedicated security administration utilities, or other OEM-recommended secure management mechanisms, provided all functional and security requirements specified in the RFP are met.

36	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 20	133	HSM must support onboard key generation and secure storage of minimum 10000 keys within the FIPS boundary of the HSM.	As the HSM is proposed to function as the Root of Trust for the KMS, with operational keys managed by the KMS, the requirement for storage of 10,000 keys within the HSM boundary appears excessive for the intended use case. Request LIC to revise the requirement to: "HSM must support onboard key generation and secure storage of a minimum of 1,000 cryptographic keys within the FIPS-validated boundary of the HSM, with support for future scalability."	The proposed HSM is intended to serve as the Root of Trust for the enterprise Key Management System (KMS) and must support LIC's current and future cryptographic key management requirements over the solution lifecycle. While operational keys may be managed through the KMS, the HSM is required to securely generate, store, and protect cryptographic keys within its FIPS-validated boundary, including master keys, key-encryption keys, application keys, signing keys, certificates, and other cryptographic objects associated with multiple applications, environments, integrations, and future expansion requirements. The requirement for secure storage of a minimum of 10,000 keys has been specified to ensure adequate scalability, operational flexibility, business continuity, and long-term growth without requiring hardware replacement or architectural changes. The requirement is aligned with LIC's anticipated enterprise-scale deployment and future onboarding of additional applications and services. Accordingly, the requirement shall remain as specified in the RFP
37	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 29	133	Support secure key backup with same level of protection and backward/forward compatibility during restoration.	Kindly clarify whether LIC expects cryptographic key backups to remain within a FIPS-validated cryptographic boundary throughout their lifecycle. If yes, request LIC to consider the requirement that secure key backup and restoration should be performed using a dedicated FIPS 140-3 Level 3 certified Backup HSM providing the same level of security assurance as the production HSM environment. Requesting to modify this point as "Support secure key backup using FIPS 140-3 level 3 certified hardware with same level of protection and backward/forward compatibility during restoration"	LIC expects key backup and restoration mechanisms to provide security controls equivalent to those applicable to production cryptographic keys and to support backward and forward compatibility during restoration. The specific method of implementing secure backup, including the use of dedicated backup HSMs or other secure mechanisms, is left to the bidder's proposed solution, provided the stated security objectives are met.
38	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 34	133	Provide secure vault for key storage with integration capability for third-party vaults.	Please confirm the use case of third-party vaults integeration and name of such vaults.	The requirement is intended to ensure interoperability and flexibility of the proposed solution with enterprise-grade third-party vault solutions that may be deployed currently or in the future within LIC's ecosystem. At this stage, LIC is not mandating integration with any specific third-party vault product. Bidders shall confirm that the proposed solution provides standard integration capabilities through industry-standard APIs, connectors, protocols, or SDKs to facilitate integration with third-party vault solutions, if required during the contract period.

39	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 39	133	Solution should detect compromises or unauthorized modifications and send alerts (through email and SMS Gateway)	KMS/HSM platforms typically generate alerts and security events through email notifications, syslog, SNMP, APIs, SIEM integrations, and enterprise monitoring systems. SMS notifications are generally delivered through external notification platforms or SMS gateways integrated with the organization's monitoring infrastructure. Please modify this clause as "Solution should detect compromises or unauthorized modifications and send alerts through email/syslog/SNMP/SIEM integerations or any other supported notification mechanisms.	The solution shall detect compromises or unauthorized modifications and generate security alerts/events. The solution shall support alert notification through email and integration with enterprise monitoring and notification mechanisms such as syslog, SNMP, APIs, SIEM platforms, and SMS gateways, wherever applicable. Accordingly, the requirement is revised as follows: "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." Please refer to Corrigendum-1, Sr.No: 6
40	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 41	134	Provide proactive notifications before key expiry, rotation or lifecycle events via email and SMS.	Enterprise KMS platforms typically generate key lifecycle alerts through email notifications, dashboards, syslog, SNMP, APIs, SIEM integrations, and enterprise monitoring systems. SMS notifications are generally implemented through external notification infrastructure and are not typically a native capability of KMS/HSM solutions. Request LIC to modify the requirement as follows: "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."	Please refer to corrigendum-1 , Sr.No: 6. The requirement stands modified as follows: "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."

41	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 49	134	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	The requirement references "versatile Key and Secret Vaults" and a "decentralized security model," which may be interpreted differently by bidders. Request LIC to clarify the meaning of "versatile Key and Secret Vaults" and "decentralized security model". Also, clarify the specific regulatory and compliance requirements intended under the phrase "differing local security policies and regulatory mandates," and whether support for logical segregation, RBAC, delegated administration, and independent security domains shall be considered compliant.	The requirement for "versatile Key and Secret Vaults" refers to the capability to securely store and manage various types of cryptographic keys, certificates, secrets, credentials, tokens, and other sensitive data with appropriate lifecycle and access controls. The "decentralized security model" refers to the ability to centrally monitor and manage the solution while supporting independent administration, policy enforcement, and security controls for different business units, locations, or security domains. The phrase "differing local security policies and regulatory mandates" is intended to ensure that the solution can accommodate varying organizational, geographical, and compliance requirements through appropriate segregation and governance mechanisms. Support for logical segregation, RBAC, delegated administration, independent security domains, and equivalent capabilities will be considered compliant with this requirement.
42	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 50	134	The proposed HSM should be scalable and field upgradable in future without changing the hardware.	Enterprise HSM solutions are typically designed to achieve scalability through clustering, high-availability groups, and the addition of HSM appliances rather than through in-place hardware upgrades. Request LIC to either remove this requirement or reconsider the requirement and permit scalability through a scale-out architecture without mandating future upgrades on the same hardware platform. Proposed requirement: "The proposed HSM should support future scalability through clustering, high-availability configurations, or addition of HSM appliances without impacting existing cryptographic operations."	The requirement is self-explanatory. The proposed HSM should be scalable and field upgradable in future without replacement of the deployed solution. Bidders may propose OEM-supported mechanisms to achieve scalability and field upgradability, subject to compliance with the RFP requirements.

43	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 51	134	There should not be any limit on no. of Keys to be protected by HSM in accordance with FIPS 140-3 and CCA guidelines.	The requirement states that keys must remain within the FIPS 140-3 Level 3 cryptographic boundary of the HSM throughout their lifecycle. As HSMs have finite secure storage capacity within the validated cryptographic boundary, the requirement of having no limit on the number of keys protected by the HSM appears inconsistent with the architectural constraints of FIPS-certified HSM platforms. Requesting LIC to remove this requirement.	LIC acknowledges that HSMs have finite physical storage and processing capacities. The intent of the requirement is that the proposed HSM/KMS solution should not impose arbitrary restrictions on the number of cryptographic keys that can be managed and protected in accordance with FIPS 140-3 and applicable regulatory guidelines. The solution should support scalable expansion through vendor-supported mechanisms, as required to meet LIC's operational requirements. Accordingly, the requirement remains unchanged.
44	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 53	134	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.	Requesting LIC to clarify whether equivalent administrator authentication mechanisms supported by the HSM, including strong password-based authentication, hardware tokens, smart cards, PED devices, or multi-factor authentication, shall be considered compliant. Proposed Modification: "The HSM must support multiple and multi-level administration with secure administrator authentication and separation of duties through one or more supported authentication mechanisms."	The intent of the requirement is to ensure support for multiple and multi-level administration with strong multi-factor administrator authentication and separation of duties on the same HSM platform without requiring hardware changes. Smart cards/tokens are cited as preferred mechanisms. Equivalent authentication mechanisms may be considered compliant, provided they offer security equivalent to or stronger than two-factor authentication using smart cards/tokens and support role-based administration and separation of duties. Accordingly, the requirement remains unchanged.
45	Annexure F: Technical Compliance 2. Encryption	Point 3	135	Support encryption software for operating systems like RHEL, Linux on IBM-Z, CentOS , Oracle Enterprise Linux , Suse Linux , Windows servers.	Request LIC to clarify whether Linux on IBM-Z, Oracle Enterprise Linux, and SUSE Linux are currently deployed within the databases and applications covered under this project. If these platforms are not part of the current scope, request LIC to remove them from the mandatory operating system support requirements.	The operating systems Linux on IBM-Z RedHat Enterprise , Oracle Enterprise Linux and SUSE Linux are currently in use.
46	Annexure F: Technical Compliance 2. Encryption	Point 13	135	The solution should support an agent or agentless file encryption approach.	Enterprise data protection capabilities typically available through agent-based encryption solutions. Requesting LIC to revise the requirement: The solution should support an agent based file encryption approach.	The intent of the requirement is to provide flexibility in deployment and implementation. The proposed solution may support either an agent-based or an agentless file encryption approach, provided it meets the functional, security, and operational requirements specified in the RFP.

47	Annexure F: Technical Compliance 2. Encryption Software / Encryption Agent Specifications	Point 16	136	The solution should continuously perform integrity checks to detect unauthorized modifications – including ransomware attacks – and promptly revert data to its secure state	The requirement combines encryption, integrity monitoring, ransomware detection, and automated data recovery capabilities, which are typically delivered through separate technology domains including encryption solutions, endpoint security platforms, file integrity monitoring solutions, and backup/recovery systems. Request LIC to modify the requirement as follows: "The Key Management Transparent Encryption solution should continuously monitor protected data and associated processes to detect unauthorized modifications, abnormal file activity, ransomware behavior, or malicious encryption attempts. The solution should provide trusted process enforcement and be capable of generating alerts and/or blocking unauthorized processes, applications, or ransomware activity attempting to access, modify, or encrypt protected data."	Please refer to Corrigendum-1, Sr.No: 6
48	Annexure F: Technical Compliance 2. Encryption Software / Encryption Agent Specifications	Point 19	136	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.	Request LIC to clarify the meaning of "native database-aware encryption" and the expected scope of compliance. Specifically, confirm whether solutions providing file-level encryption of database files with centralized key management and policy enforcement shall be considered compliant, provided the solution does not rely solely on storage, hypervisor, or infrastructure-level encryption mechanisms.	For the purpose of this RFP, "database-aware encryption" refers to encryption capabilities specifically designed to protect database data and database files with awareness of the database environment and database operations. The intent of this requirement is to distinguish such solutions from generic file system, volume, disk, storage, hypervisor, or other infrastructure-level encryption mechanisms. Compliance will be evaluated against the RFP requirement that the proposed solution provide database-aware encryption capabilities for the supported databases and does not rely solely on file system, storage, or infrastructure-level encryption mechanisms.
49	Section E: Scope of Services 1. Scope of work – Database Encryption	Point 4	72	Enablement of online (near zero-downtime) encryption and rekeying capabilities for seamless deployment and key rotation.	This point is mentioned in SOW section but missing in technical specification. Requesting LIC to add this point as "The proposed KMS solution must support non-disruptive encryption deployment with live data transformation, enabling in-place encryption and rekeying of active data without application downtime, service interruption, or data migration."	No change. Please be guided by the terms and conditions of RFP

50	Earnest Money deposit (EMD	Point 7	13	EMD exemption will be given for Micro and Small Enterprises as defined in MSME Procurement Policy issued by the Department of MSME or are registered with the Central Purchase Organization or the concerned Ministry or Department. Bidders should submit relevant MSME/NSIC certificate as mentioned in this RFP document.	Request you to provide exemption as we fall under Medium entperprise in MSME	No change. Please be guided by the terms and conditions of RFP
51	Section E – Scope of Work for Key Management Solution & HSM		76 onwards	Bidder to supply, install and configure KMS and HSM infrastructure	Kindly confirm whether LIC would accept a software-based Database Encryption solution integrated with a third-party FIPS 140-3 compliant HSM/KMS solution, instead of a single OEM providing the complete DE, KMS and HSM stack.	Software-based Database Encryption solution integrated with a FIPS 140-3 Level 3 certified HSM is required. The solution including KMS, and HSM components shall be offered as a complete integrated solution from a single OEM. Solutions comprising products from multiple OEMs will not be accepted.
52	Section E – KMS & HSM Requirements		76 onwards	Centralized key lifecycle management including generation, storage, rotation, archival, recovery and destruction	Kindly clarify whether the key lifecycle management functions may be fulfilled through an external enterprise KMS/HSM integrated with the proposed Database Encryption solution.	The key lifecycle management functions, including key generation, storage, rotation, archival, recovery, and destruction, may be fulfilled through an enterprise KMS/HSM integrated with the proposed Database Encryption solution
53	Section E – HSM Requirem		76 onwards	HSM deployment and integration requirements	Kindly confirm whether any industry-standard FIPS 140-3 compliant HSM from a third-party OEM can be proposed, provided all integration, support and SLA	Please be guided by the terms and conditions specified in RFP
54	Section E – Database		72 onwards	Database Encryption solution requirements	Kindly confirm whether the Database Encryption solution and KMS/HSM solution may be supplied by different OEMs under a single System Integrator-led	Please be guided by the terms and conditions specified in RFP
55	Section E – Integration		72-84	Integration with databases, applications, storage and other platforms	Kindly provide the indicative list of databases and versions currently in scope (Oracle, SQL Server, PostgreSQL, MySQL, etc.) to facilitate accurate sizing and solution design.	Please refer to RFP -Annexure-W for Databases in use . Database version cannot be provided due to security reasons
56	Section E – Cryptographic Compliance		Relevant clause mentioning FIPS 140-3	Solution to be built using FIPS 140-3 compliant cryptographic modules	Kindly clarify whether compliance through integration with FIPS 140-3 validated HSMs is acceptable, or whether every software component within the solution stack is required to hold independent FIPS 140-3 validation.	For the purpose of this RFP, the requirement is that the proposed encryption solution and KMS integrate with a FIPS 140-3 Level 3 compliant/validated HSM for protection and management of cryptographic keys and related cryptographic operations. LIC does not require every software component within the solution stack to hold an independent FIPS 140-3 validation. Compliance will be evaluated based on the bidder's proposed architecture and its integration with the required FIPS 140-3 Level 3 HSM in accordance with the RFP requirements.

57	Scope & Sizing		Annexure-W	Database Encryption sizing requirements	Kindly confirm whether the sizing provided in Annexure-W represents the final production scope or whether additional databases/workloads may be included during implementation.	The sizing provided in Annexure-W is as per current status. Additional databases/new type of database may get added in future
58	General Architecture		Scope of Services	Overall solution architecture	Kindly clarify whether LIC has any preferred or existing HSM vendors currently deployed in its environment that bidders should consider for interoperability and integration.	Currently , there are no HSMs or KMS deployed in LIC
59	Eligibility Criteria – Point 4		Eligibility Criteria	The bidder should have a minimum of three (3) years of experience in supply, installation, implementation and/or maintenance of enterprise-grade Data-at-Rest Encryption (DE) solution.	We request LIC to consider "Bidder or its OEM" experience whose solution is being offered under this RFP. Trust LIC would consider our request favourably.	No change. Please be guided by the terms and conditions of RFP
60	Eligibility Criteria – Point 5		Eligibility Criteria	Reference experience requirement for implementation/deployment of the proposed solution.	We request LIC to consider "Bidder or its OEM" experience whose solution is being offered under this RFP. Trust LIC would consider our request favourably.	No change. Please be guided by the terms and conditions of RFP
61	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 3	132	Should have built-in secret management without any extra license cost.	Kindly clarify the intended use case and requirement for the Secret Management solution as part of the proposed Database Encryption solution. Please provide details of the applications that are expected to integrate with the Secret Management solution, along with the total number of applications in scope. Additionally, Point No. 34 requires the KMS to support integration with third-party vaults for secure storage of keys. In view of this requirement, kindly clarify the technical rationale for a separate Secret Management solution and its intended use cases, particularly where a third-party vault is proposed to be used.	Built-in Secret Management is required as part of the solution to support secure management of application credentials, service accounts, API keys, tokens, certificates, and other sensitive secrets, in alignment with applicable regulatory and cybersecurity requirements. At this stage, the specific applications and quantities are not fixed. The solution should support integration with LIC's existing and future applications without requiring additional licensing costs for Secret Management capabilities. The requirement for third-party vault integration (Point 34) is distinct and relates to interoperability with external key management and vault solutions for cryptographic key storage and management. Secret Management and third-party vault integration serve different but complementary functions and are both required under the proposed solution.
62	Annexure F: Technical Compliance	Point 5	132	Host interface should support minimum 3 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6.	Requesting LIC to change this requirement to "1 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6" as 1 Gigabit ethernet ports is widely used industry standrd and more than enough for this requirement.	No change.Please be guided by the terms and conditions in RFP

63	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 7	132	Minimum 100 partitions with isolation using user ID/password and memory isolation as per CCA IVG guidelines.	Partitions are primarily required when the HSM is shared across multiple applications or environments that require cryptographic isolation. In the current design, the HSM is dedicated to supporting CipherTrust as the Root of Trust only. Typically, only one partition is enough to serve the RoT use case. Increasing the partition count would not provide additional benefit for this architecture. The proposed HSM anyways comes with 5 partitions. Request LIC to revise the requirement to "Minimum 5 partitions with isolation using user ID/password and memory isolation as per CCA IVG guidelines"	No change.Please be guided by the terms and conditions in RFP
64	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 13	132	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.	The proposed HSM is intended to serve as the Root of Trust for the KMS, supporting secure key generation, storage, wrapping/unwrapping, and lifecycle management of encryption keys. As the HSM is not intended for high-volume cryptographic signing applications such as PKI Certificate Authorities, UPI payments, or digital signature services, the requirement of minimum 2000 RSA-2048 signing TPS expandable up to 10000 TPS appears significantly higher than the expected workload for the proposed use case. Requesting LIC to review and revise the requirement to a more appropriate performance benchmark, such as minimum 1000 RSA-2048 signing TPS which is more than enough for this requirement.	No change. Please be guided by the terms and conditions in RFP
65	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 16	132	Should provide a web based solution for administration, monitoring, and provisioning	Requesting LIC to update this requirement as "Should provide a web based solution for administration, monitoring, and provisioning of KMS solution". HSM being highly secure cryptographic devices, are typically administered and provisioned through secure CLI and dedicated security administration utilities rather than web-based interfaces.	The clause stands clarified. The proposed solution shall provide a web-based interface for administration, monitoring, and provisioning of the Key Management System (KMS). Administration and provisioning of the HSM may be through secure command-line interfaces, dedicated security administration utilities, or other OEM-recommended secure management mechanisms, provided all functional and security requirements specified in the RFP are met.

66	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 20	133	HSM must support onboard key generation and secure storage of minimum 10000 keys within the FIPS boundary of the HSM.	As the HSM is proposed to function as the Root of Trust for the KMS, with operational keys managed by the KMS, the requirement for storage of 10,000 keys within the HSM boundary appears excessive for the intended use case. Request LIC to revise the requirement to: "HSM must support onboard key generation and secure storage of a minimum of 1,000 cryptographic keys within the FIPS-validated boundary of the HSM, with support for future scalability."	The proposed HSM is intended to serve as the Root of Trust for the enterprise Key Management System (KMS) and must support LIC's current and future cryptographic key management requirements over the solution lifecycle. While operational keys may be managed through the KMS, the HSM is required to securely generate, store, and protect cryptographic keys within its FIPS-validated boundary, including master keys, key-encryption keys, application keys, signing keys, certificates, and other cryptographic objects associated with multiple applications, environments, integrations, and future expansion requirements.The requirement for secure storage of a minimum of 10,000 keys has been specified to ensure adequate scalability, operational flexibility, business continuity, and long-term growth without requiring hardware replacement or architectural changes. The requirement is aligned with LIC's anticipated enterprise-scale deployment and future onboarding of additional applications and services.Accordingly, the requirement shall remain as specified in the RFP
67	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 29	133	Support secure key backup with same level of protection and backward/forward compatibility during restoration.	Kindly clarify whether LIC expects cryptographic key backups to remain within a FIPS-validated cryptographic boundary throughout their lifecycle. If yes, request LIC to consider the requirement that secure key backup and restoration should be performed using a dedicated FIPS 140-3 Level 3 certified Backup HSM providing the same level of security assurance as the production HSM environment. Requesting to modify this point as "Support secure key backup using FIPS 140-3 level 3 certified hardware with same level of protection and backward/forward compatibility during restoration"	LIC expects key backup and restoration mechanisms to provide security controls equivalent to those applicable to production cryptographic keys and to support backward and forward compatibility during restoration. The specific method of implementing secure backup, including the use of dedicated backup HSMs or other secure mechanisms, is left to the bidder's proposed solution, provided the stated security objectives are met.
68	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 34	133	Provide secure vault for key storage with integration capability for third-party vaults.	Please confirm the use case of third-party vaults integeration and name of such vaults.	The requirement is intended to ensure interoperability and flexibility of the proposed solution with enterprise-grade third-party vault solutions that may be deployed currently or in the future within LIC's ecosystem. At this stage, LIC is not mandating integration with any specific third-party vault product. Bidders shall confirm that the proposed solution provides standard integration capabilities through industry-standard APIs, connectors, protocols, or SDKs to facilitate integration with third-party vault solutions, if required during the contract period.

69	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 39	133	Solution should detect compromises or unauthorized modifications and send alerts (through email and SMS Gateway)	KMS/HSM platforms typically generate alerts and security events through email notifications, syslog, SNMP, APIs, SIEM integrations, and enterprise monitoring systems. SMS notifications are generally delivered through external notification platforms or SMS gateways integrated with the organization's monitoring infrastructure. Please modify this clause as "Solution should detect compromises or unauthorized modifications and send alerts through email/syslog/SNMP/SIEM integerations or any other supported notification mechanisms.	The solution shall detect compromises or unauthorized modifications and generate security alerts/events. The solution shall support alert notification through email and integration with enterprise monitoring and notification mechanisms such as syslog, SNMP, APIs, SIEM platforms, and SMS gateways, wherever applicable. Accordingly, the requirement is revised as follows: "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." Please refer to Corrigendum-1, Sr.No: 6
70	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 41	134	Provide proactive notifications before key expiry, rotation or lifecycle events via email and SMS.	Enterprise KMS platforms typically generate key lifecycle alerts through email notifications, dashboards, syslog, SNMP, APIs, SIEM integrations, and enterprise monitoring systems. SMS notifications are generally implemented through external notification infrastructure and are not typically a native capability of KMS/HSM solutions. Request LIC to modify the requirement as follows: "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."	Please refer to corrigendum-1,Sr.No: 6. The requirement stands modified as follows: "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."

71	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 49	134	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	The requirement references "versatile Key and Secret Vaults" and a "decentralized security model," which may be interpreted differently by bidders. Request LIC to clarify the meaning of "versatile Key and Secret Vaults" and "decentralized security model". Also, clarify the specific regulatory and compliance requirements intended under the phrase "differing local security policies and regulatory mandates," and whether support for logical segregation, RBAC, delegated administration, and independent security domains shall be considered compliant.	The requirement for "versatile Key and Secret Vaults" refers to the capability to securely store and manage various types of cryptographic keys, certificates, secrets, credentials, tokens, and other sensitive data with appropriate lifecycle and access controls. The "decentralized security model" refers to the ability to centrally monitor and manage the solution while supporting independent administration, policy enforcement, and security controls for different business units, locations, or security domains. The phrase "differing local security policies and regulatory mandates" is intended to ensure that the solution can accommodate varying organizational, geographical, and compliance requirements through appropriate segregation and governance mechanisms. Support for logical segregation, RBAC, delegated administration, independent security domains, and equivalent capabilities will be considered compliant with this requirement.
72	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 50	134	The proposed HSM should be scalable and field upgradable in future without changing the hardware.	Enterprise HSM solutions are typically designed to achieve scalability through clustering, high-availability groups, and the addition of HSM appliances rather than through in-place hardware upgrades. Request LIC to either remove this requirement or reconsider the requirement and permit scalability through a scale-out architecture without mandating future upgrades on the same hardware platform. Proposed requirement: "The proposed HSM should support future scalability through clustering, high-availability configurations, or addition of HSM appliances without impacting existing cryptographic operations."	The requirement is self-explanatory. The proposed HSM should be scalable and field upgradable in future without replacement of the deployed solution. Bidders may propose OEM-supported mechanisms to achieve scalability and field upgradability, subject to compliance with the RFP requirements.

73	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 51	134	There should not be any limit on no. of Keys to be protected by HSM in accordance with FIPS 140-3 and CCA guidelines.	The requirement states that keys must remain within the FIPS 140-3 Level 3 cryptographic boundary of the HSM throughout their lifecycle. As HSMs have finite secure storage capacity within the validated cryptographic boundary, the requirement of having no limit on the number of keys protected by the HSM appears inconsistent with the architectural constraints of FIPS-certified HSM platforms. Requesting LIC to remove this requirement.	LIC acknowledges that HSMs have finite physical storage and processing capacities. The intent of the requirement is that the proposed HSM/KMS solution should not impose arbitrary restrictions on the number of cryptographic keys that can be managed and protected in accordance with FIPS 140-3 and applicable regulatory guidelines. The solution should support scalable expansion through vendor-supported mechanisms, as required to meet LIC's operational requirements. Accordingly, the requirement remains unchanged.
74	Annexure F: Technical Compliance 1. KMS / HSM Related Specifications	Point 53	134	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.	Requesting LIC to clarify whether equivalent administrator authentication mechanisms supported by the HSM, including strong password-based authentication, hardware tokens, smart cards, PED devices, or multi-factor authentication, shall be considered compliant. Proposed Modification: "The HSM must support multiple and multi-level administration with secure administrator authentication and separation of duties through one or more supported authentication mechanisms."	The intent of the requirement is to ensure support for multiple and multi-level administration with strong multi-factor administrator authentication and separation of duties on the same HSM platform without requiring hardware changes. Smart cards/tokens are cited as preferred mechanisms. Equivalent authentication mechanisms may be considered compliant, provided they offer security equivalent to or stronger than two-factor authentication using smart cards/tokens and support role-based administration and separation of duties. Accordingly, the requirement remains unchanged.
75	Annexure F: Technical Compliance 2. Encryption	Point 3	135	Support encryption software for operating systems like RHEL, Linux on IBM-Z, CentOS , Oracle Enterprise Linux , Suse Linux , Windows servers.	Request LIC to clarify whether Linux on IBM-Z, Oracle Enterprise Linux, and SUSE Linux are currently deployed within the databases and applications covered under this project. If these platforms are not part of the current scope, request LIC to remove them from the mandatory operating system support requirements.	The operating systems Linux on IBM-Z RedHat Enterprise , Oracle Enterprise Linux and SUSE Linux are currently in use.
76	Annexure F: Technical Compliance 2. Encryption	Point 13	135	The solution should support an agent or agentless file encryption approach.	Enterprise data protection capabilities typically available through agent-based encryption solutions. Requesting LIC to revise the requirement: The solution should support an agent based file encryption approach.	The intent of the requirement is to provide flexibility in deployment and implementation. The proposed solution may support either an agent-based or an agentless file encryption approach, provided it meets the functional, security, and operational requirements specified in the RFP.

77	Annexure F: Technical Compliance 2. Encryption Software / Encryption Agent Specifications	Point 16	136	The solution should continuously perform integrity checks to detect unauthorized modifications – including ransomware attacks – and promptly revert data to its secure state	The requirement combines encryption, integrity monitoring, ransomware detection, and automated data recovery capabilities, which are typically delivered through separate technology domains including encryption solutions, endpoint security platforms, file integrity monitoring solutions, and backup/recovery systems. Request LIC to modify the requirement as follows: "The Key Management Transparent Encryption solution should continuously monitor protected data and associated processes to detect unauthorized modifications, abnormal file activity, ransomware behavior, or malicious encryption attempts. The solution should provide trusted process enforcement and be capable of generating alerts and/or blocking unauthorized processes, applications, or ransomware activity attempting to access, modify, or encrypt protected data."	Please refer to Corrigendum-1 Sr.No: 6
78	Annexure F: Technical Compliance 2. Encryption Software / Encryption Agent Specifications	Point 19	136	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.	Request LIC to clarify the meaning of "native database-aware encryption" and the expected scope of compliance. Specifically, confirm whether solutions providing file-level encryption of database files with centralized key management and policy enforcement shall be considered compliant, provided the solution does not rely solely on storage, hypervisor, or infrastructure-level encryption mechanisms.	For the purpose of this RFP, "native database-aware encryption" refers to encryption capabilities specifically designed to protect database data and database files with awareness of database workloads, processes, or data structures. The intent of this requirement is to distinguish such solutions from generic file system, volume, disk, storage, or infrastructure-level encryption mechanisms. Compliance will be evaluated against the stated requirement that the proposed encryption solution support native database-aware encryption for supported databases and does not rely solely on file system or storage layer encryption mechanisms.
79	Section E: Scope of Services 1. Scope of work – Database Encryption	Point 4	72	Enablement of online (near zero-downtime) encryption and rekeying capabilities for seamless deployment and key rotation.	This point is mentioned in SOW section but missing in technical specification. Requesting LIC to add this point as "The proposed KMS solution must support non-disruptive encryption deployment with live data transformation, enabling in-place encryption and rekeying of active data without application downtime, service interruption, or data migration."	No change. Please be guided by the terms and conditions of RFP

80	Section C	4.Commercial Bid	28	The spread of costs for ATS/AMC/Warranty needs to be provided in appropriately distributed manner. If bidder is found to make upfront loading of these charges / payments etc. to initial years, then bidder's bid may be rejected.	Need more clarity on the said point	The intent of the clause is to ensure that ATS/AMC/Warranty charges are distributed reasonably across the applicable contract period and are commensurate with the services to be provided during each year. Bidders should avoid disproportionate front-loading of such charges in the initial years of the contract. LIC reserves the right to seek justification for any pricing structure that appears significantly skewed towards the initial years and to evaluate the same in accordance with the RFP provisions.
81	Section C	11.Opening of Bids	33	d) The passwords of password protected files shall be called for from Bidders during the Bid evaluation stage.	One of the clause in the same section says Files not to be password protected.	Please refer to Corrigendum-1, Sr.No: 5
82	Section C	14.Commercial Bid Evaluation :	37	NPV Rule	Need Clarity on this point	The clause pertaining to Net Present Value (NPV) evaluation, including the basis of computation and discounting rate, is adequately defined in the RFP and stands unchanged. Bidders shall calculate NPV in accordance with the provisions specified therein. No further clarification is envisaged.
83	Section C	30.Period of Validity of Bids	49	a) Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. LIC shall reject a bid as non-responsive if the bid is submitted with a shorter validity period	Due to current Global disrupts in SCCM price validuty can not be hold for the bid validity Requested t reducce to bid validityh	No change. Please be guided by the terms and conditions specified in RFP.
84	Section C	60.Digital Personal DATA Protection Act, 2023	67	The Vendor shall comply with the provisions of the Digital Personal Data Protection Act, 2023, as amended from time to time, along with rules and applicable information security guidelines issued by the Insurance Regulatory and Development Authority of India (IRDAI).	Need clarity on this point.	The requirement is intended to ensure that the proposed solution and related services support compliance with applicable provisions of the Digital Personal Data Protection Act, 2023 and relevant IRDAI guidelines. This includes, inter alia, implementation of appropriate technical safeguards for protection of digital personal data, encryption of data at rest, secure cryptographic key management through KMS integrated with HSMs, access controls, audit trails, activity logging, and maintenance of confidentiality of LIC data handled under the contract. The clause otherwise stands unchanged.

85	Section G:	Payment Terms & Conditions	118	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%	Request for making this payment term to 80% instead of 60%	Please refer to Corrigendum-1
86	Section G:	Payment Terms & Conditions	118	Successful installation and acceptance of the hardware (after due inspection) including DR 20%	Request for making this payment term to 10% instead of 20%	Please refer to Corrigendum-1
87	Section G:	Payment Terms &	118	One month after Go-LIVE	Request for making this payment term to 10% instead of 20%	Please refer to Corrigendum-1
88	Section G:	Payment Terms & Conditions	118	Delivery of respective software & its related components as per actual supply (after due diligence) 60%	Request for making this payment term to 80% instead of 60%	Please refer to Corrigendum-1
89	Section G:	Payment Terms & Conditions	118	Successful installation, configuration, completion of customization and acceptance of systems for respective applications 20%	Request for making this payment term to 10% instead of 20%	Please refer to Corrigendum-1
90	Section G:	Payment Terms &	118	One month after Go-LIVE 20%	Request for making this payment term to 10% instead of 20%	Please refer to Corrigendum-1
91	Section G:	Payment Terms & Conditions	118	The AMC/ATS shall commence on completion of warranty period. Quarterly in arrears	Request for making it Yearly advance instead of Quarterly in arrears	Please be guided by the terms and conditions of RFP
92	Section E:	Section E: Scope of Services	99	1.Case Studies: Evidence of managing database estates of at least 100+ nodes or 500+ TB of total data in last 5 years and MySQL Database Administrator or equivalent Cloud Provider Database Specialist Certifications – L3	we would like to request a brief clarification to ensure our response perfectly aligns with your expectations.	The clause mentioned in RFP document is self-explanatory.
93	Section C: Instructions to Bidders (ITB)	1. Pre-bid meeting and Clarification/ Amendment of Bid Documents	25	The original Bid must be printed on 8.27" by 11.69" (A4 size) paper in indelible ink.	Since the bid submission is completely online, we did not understand this calsue? Request for your clarification	Please refer to Section-C of RFP Document -- Clause-2 - Submission of Bids. Bidders are required to prepare documents in A4-size format and, wherever signatures are required, such documents shall be signed by the authorized signatory in indelible ink before being scanned and uploaded to the portal. Digitally signed documents, wherever applicable as per the e-procurement process, shall also be acceptable. No physical submission of the bid documents is required, except for those documents specifically required under the RFP (such as EMD Bank Guarantee and Integrity Pact).

94	Consortiums or sub-contractor	55	63	No consortium bidding is allowed. LIC will not consider joint or collaborative proposals that require a contract with more than one prime Vendor. Bidders need to fulfil all the eligibility criteria and technical evaluation criteria in its individual capacity unless mentioned otherwise.	We kindly request for the relaxation as Bidders/OEM need to fulfil all the eligibility criteria and technical evaluation criteria in its individual capacity.	Please be guided by the terms and conditions of RFP
95	Eligibility Criteria	6	19	Bidders and the proposed OEM should have support centres in India with availability of 24 x 7 onsite, telephonic/ remote support	We kindly request LIC to keep it as either bidder or OEM should have support centers in India with availability of 24x7 onsite, telephonic/remote support.	No change. Please be guided by the terms and conditions of RFP
96	Scope of services	Section E: 1. Scope of work – Database Encryption	72	The bidder shall be responsible for the end-to-end implementation and 5-year maintenance of Encryption solution for securing data at rest across LIC's databases and server infrastructure.	We kindly request for the relaxation as Bidders/OEM shall be responsible for the end-to-end implementation and 5-year maintenance of Encryption solution for securing data at rest across LIC's databases and server infrastructure.	No change. Please be guided by the terms and conditions of RFP
97	Scope of services	Section E: 1. Scope of work – Database Encryption	75	The bidder shall provide a third-party enterprise encryption solution capable of integrating with proposed KMS and HSM and supporting encryption of data at rest for database environments where native encryption integration is not feasible.	We kindly request for the relaxation as Bidders/OEM shall provide a third-party enterprise encryption solution capable of integrating with proposed KMS and HSM and supporting encryption of data at rest for database environments where native encryption integration is not feasible.	No change. Please be guided by the terms and conditions of RFP
98	11. Service Level Agreements (SLAs)	General conditions	101	c) The bidder shall provide 24x7x365 support for all supplied solutions during the contract period.	We kindly request for the relaxation as Bidders/OEM shall provide 24x7x365 support for all supplied solutions during the contract period.	No change. Please be guided by the terms and conditions of RFP
99	12. Evaluation	g) Technical	35	A-Bidder expereience	We kindly request for the relaxation as Bidders/OEM in the Crietria	No change. Please be guided by the terms and conditions of RFP

100	Annexure F: Technical Compliance	132	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.	The Crypto Hub HSM platform is currently undergoing FIPS 140-3 Level 3 certification under the NIST Cryptographic Module Validation Program (CMVP). As confirmed by the accredited testing laboratory, the module has already completed submission to CMVP and has transitioned from the "Implementation Under Test (IUT)" phase to the "Modules In Process (MIP)" phase as part of the certification lifecycle. The certification is expected to be completed within this calendar year (December 2026). https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list In view of the above, we kindly request LIC to consider allowing bidders/OEM whose HSMs are currently in the Modules In Process (MIP) Phase to participate, with a provision that the OEM shall provide a valid FIPS 140-3 certification This approach preserves the long-term compliance objective while enabling maximum participation from OEMs actively undergoing certification. The time taken is due to	Please be guided by the terms and conditions of RFP
101	Annexure F: Technical Compliance	132	11	Support symmetric cryptographic algorithms including AES, ARIA, SEED, RC2, RC4, RC5, CAST and GCM.	ARIA, SEED, and CAST are primarily region-specific cryptographic algorithms used mainly in South Korea and certain North American implementations. These algorithms are not generally required for Indian banking and CTS environments, where AES and Triple DES are the commonly adopted industry standards. We kindly request to consider removing the requirements for ARIA, SEED, and CAST algorithms and change the clause to "Must support symmetric algorithms: AES and Triple DES."	Please refer to the Corrigendum issued

102	Annexure F: Technical Compliance	133	18	Keys must remain securely within the HSM FIPS 140-3 Level 3 cryptographic boundary throughout their lifecycle.	The Crypto Hub HSM platform is currently undergoing FIPS 140-3 Level 3 certification under the NIST Cryptographic Module Validation Program (CMVP).As confirmed by the accredited testing laboratory, the module has already completed submission to CMVP and has transitioned from the "Implementation Under Test (IUT)" phase to the "Modules In Process (MIP)" phase as part of the certification lifecycle. The certification is expected to be completed within this calendar year (December 2026).https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list In view of the above, we kindly request LIC to consider allowing bidders/OEM whose HSMs are currently in the Modules In Process (MIP) Phase to participate, with a provision that the OEM shall provide a valid FIPS 140-3 certification. This approach preserves the long- term compliance objective while enabling maximum participation from OEMs actively undergoing certification. The time taken is due to enhanced feature set, HSMs	Please be guided by the terms and conditions of RFP
103	Annexure F: Technical Compliance	134	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.	The Crypto Hub HSM platform is currently undergoing FIPS 140-3 Level 3 certification under the NIST Cryptographic Module Validation Program (CMVP).As confirmed by the accredited testing laboratory, the module has already completed submission to CMVP and has transitioned from the "Implementation Under Test (IUT)" phase to the "Modules In Process (MIP)" phase as part of the certification lifecycle. The certification is expected to be completed within this calendar year (December 2026). https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list. In view of the above, we kindly request LIC to consider allowing bidders/OEM whose HSMs are currently in the Modules In Process (MIP) Phase to participate, with a provision that the OEM shall provide a valid FIPS 140-3 certification. This approach preserves the long- term compliance objective while enabling maximum participation from OEMs actively undergoing certification. The time taken is due to enhanced feature set, HSMs	Please be guided by the terms and conditions of RFP

104	Annexure F: Technical Compliance	134	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.	The Crypto Hub HSM platform is currently undergoing FIPS 140-3 Level 3 certification under the NIST Cryptographic Module Validation Program (CMVP). As confirmed by the accredited testing laboratory, the module has already completed submission to CMVP and has transitioned from the "Implementation Under Test (IUT)" phase to the "Modules In Process (MIP)" phase as part of the certification lifecycle. The certification is expected to be completed within this calendar year (December 2026).https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list.In view of the above, we kindly request LIC to consider allowing bidders/OEM whose HSMs are currently in the Modules In Process (MIP) Phase to participate, with a provision that the OEM shall provide a valid FIPS 140-3 certification This approach preserves the long-term compliance objective while enabling maximum participation from OEMs actively undergoing certification. The time taken is due to enhanced feature set, HSMs which are providing more features	Please be guided by the terms and conditions of RFP
105	Eligibility Criteria	9	20	Power of Attorney/Board resolution or Authorization, duly authorizing the authorized signatory to act on behalf of the Bidder for all legal and financial matters pertaining to this Bid and the resulting contract, if any.	Kindly confirm whether submission of a Board Resolution (BR) alone duly authorizing the signatory for the above purposes would be sufficient to meet this requirement, or if a separate Power of Attorney / specific authorization document is also mandatory.	Please refer to RFP
106	Annexure C: Eligibility Criteria	4	129	The Bidder should have a minimum of three (3) years of experience in supply, installation, implementation and/or maintenance of enterprise-grade Data-at-Rest Encryption (DE) solutions, Key Management Systems (KMS), and Hardware Security Modules (HSMs) for Private Organizations in India with market capital of minimum 500 Crores or PSU/ Government/ Regulator/ Stock Exchanges/ BFSI Sector Firms in India or Globally.	We kindly request for the relaxation as Bidders/OEM in the Crietria and for a wider participation kindly requesting to change it to any one of the solutions from DE, KMS & HSM. We request LIC to consider the relaxation of this clause and allow qualification based on the credentials of either the Bidder or the OEM.	No change. Please be guided by the terms and conditions of RFP

107	Annexure C: Eligibility Criteria	5	129	The Bidder should have successfully supplied, installed , implemented and/or maintained during the seven (7) years preceding the date of this RFP: At least two (2) projects involving : . Enterprise-grade Data-at-Rest Encryption solutions (preferably beyond native database TDE), . Centralized Key Management Systems (KMS) with full key lifecycle management, and . Hardware Security Modules (HSMs) (preferably FIPS 140-2 Level 3 or higher), For: Private sector organizations in India with a minimum market capitalization of INR 500 Crores, OR PSUs / Government Organizations / Regulators / Stock Exchanges / BFSI sector firms in India or globally. It is not mandatory that all the above components (DE, KMS, and HSM) be implemented within a single project. However, the Bidder must demonstrate cumulative experience across all three areas through one or more eligible projects.	We kindly request for the relaxation as Bidders/OEM in the Crietria.	No change. Please be guided by the terms and conditions of RFP
108	Annexure N	Integrity pact	155	This pre-bid pre-contract Agreement	Looks like there is a mis-print here, as the pre contract agreement we generally make and submit along with the bid and not for pre-bid. Please clarify	No misprint is involved. The Integrity Pact is required to be executed and submitted along with the bid and is applicable during the pre-bid and pre-contract stages of the procurement process. The clause stands unchanged.
109	Annexure F: Technical Compliance	KMS / HSM Related Specifications	132	Host interface should support minimum 3 Gigabit Ethernet ports with port bonding and support IPv4 and IPv6.	From this statement, it depicts that LIC wants the On-premise solution and not the cloud solution. Please clarify that what can be deployment model On-prem only, cloud only or hybrid or can be multi-cloud	On-premise solution is required
110	Annexure F: Technical Compliance	KMS / HSM Related Specifications	132	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.	Is it mandatory that keys need to be backed by FIPS 140-3 Level 3 or is Level 2 sufficient	No change in requirement. The proposed HSM shall have a FIPS 140-3 Level 3 certified cryptographic boundary as specified in the RFP. Bidders shall propose a key backup mechanism supported by the OEM and compliant with the overall security requirements of the solution.
111	Annexure F: Technical Compliance	KMS / HSM Related Specifications	133	KMS should support multiple partitions mapped to separate HSM partitions, each KMS partition master key should be stored in separate/unique partition of HSM	How many HSM partitions are expected as part of the new HSM solution	Please refer to the Specifications mentioned in RFP-Annexure -F
112	Annexure F: Technical Compliance	KMS / HSM Related Specificati	132	HSM should support built-in clustering with Active-Active configuration	If HSM/KMS is totally down, what is other mechanism. Please confirm new solution to take care of regional failover as well	HSM should be deployed in HA mode and should be in Active-Active configuration. Bidder has to propose the deployment architecture

113	Annexure F: Technical Compliance	KMS / HSM Related Specifications	133	KMS should support multiple partitions mapped to separate HSM partitions, each KMS partition master key should be stored in separate/unique partition of HSM	For master key recovery, do you require multiple administrators to authorize the action	The solution should support industry-standard security controls for master key recovery, including dual control, split knowledge, separation of duties, and configurable M-of-N authorization mechanisms. No single administrator should be able to perform master key recovery independently. Bidders should describe the supported recovery authorization model and any configurable M-of-N capabilities.
114	Definitions r/w Section C r/w Annexure P : Contract Form,	Definitions, Agreement Section C.57. I Annexure P : Contract Form, Pt. 4(b	7 64 166	Pg. 7Agreement - The written contract signed between the LIC and the Selected vendor and all the attached documents with respect to any/all deliverables or services contemplated by this RFP. The "Agreement" includes the RFP all addenda/corrigenda issued by LIC, subsequent mutually agreed modifications to the RFP, response of the selected vendor to the RFP and the contract document itself. Pg. 64I. Variations proposed by LIC – LIC reserves the right to initiate any change in the scope of contract. LIC will request the Vendor in writing setting out the proposed variations. a) within 15 working days after receiving LIC's request or within another period mutually agreed, the Vendor must respond in writing to LIC specifying what impact those variations will have on: i. the Service Charges; the Services or Deliverables, including any Deliverable. ii. the Vendor's ability to perform its obligations	This RFP, all addenda / corrigenda issued by LIC, the Bid of the Successful Bidder consist part of the Agreement which will make the scope of the Agreement vast. Mutually executed MSA & SOW will constitute the entire Agreement. Also MSA should prevail over RFP. We propose to add "This Agreement, including the schedules attached hereto and all Statement of Works entered into pursuant to its terms, sets forth the entire agreement and understanding of the parties with respect to the subject matter hereof, and supersedes all prior oral and written agreements, understandings, representations, conditions and all other communications relating thereto. Should any inconsistency exist or arise between a provision of this Agreement and a provision of any exhibit, schedule, Statement of Work, or other incorporated writing, the provision of this Agreement shall prevail unless otherwise provided herein."	No change. Please be guided by the terms and conditions of RFP
115	18. Non-Disclosure Agreement (NDA) r/w annexure Q	NDA	42	Refer verbiage from RFP	1. Unlimited indemnity for breach of Confidential information which includes customer list & financial statements which falls under PII. 2. No CI duration mentioned, we propose to limit the confidentiality obligation for 5 years from the date of disclosure.	No change. Please be guided by the terms and conditions of RFP

116	Section C: Instructions to Bidders (ITB) & Section F: General Terms & Conditions	Pt. 25 - Patent Rights and other litigation costs Pt. 7 - Intellectual Property Rights	46 109 & 110	Pg 46 In the event of any claim asserted by a third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC's country, the successful Bidder will act expeditiously to extinguish such claim. If the successful Bidder fails to comply and LIC is required to pay compensation to a third party resulting from such infringement, the successful Bidder will be responsible for the compensation including all expenses (court costs and lawyer fees). LIC will give notice to the successful Bidder of such claim, if it is made, without delay as when received. In no event shall LIC be liable for any indirect, incidental or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against	Clause imposes broad, likely uncapped IPR indemnity on vendor Treats third-party ecosystem claims as direct damages, significantly increasing exposure Includes full litigation costs without safeguards Overrides protection offered in limitation of liability clause. We have added standard carve-outs to the IP indemnity clause to ensure the indemnity remains fair and commercially reasonable. These exclusions cover scenarios where infringement may arise due to factors outside our control—such as Client's specifications, third-party software used in accordance with its license, or modifications not made by us.IP- Right to reproduce, adapt, modify and communicate that Auxiliary Materials which are third-party materials is not acceptable. Third-party license will be granted as per the third-party licensing agreement terms. IP Indemnity; Reimbursement obligation; Absolute liability disclaimer for LIC We propose to add "Notwithstanding anything to the contrary in this	No change. Please be guided by the terms and conditions of RFP
117	Section C: Instructions to Bidders (ITB)	Pt. 39 - Indemnifying LIC	53 & 54	A. The successful bidder shall indemnify LIC: c) Against all third-party claims of infringement of patent, copyright, trademark etc. arising from use of the goods and services, software package or any other part thereof supplied by the vendor provided that this indemnity shall not apply to in the following cases: i) the modification of the Vendor 's deliverables provided hereunder by any person other than the Vendor or its personnel ii) LIC's failure to use of any modification to the Vendor's deliverables made available by Vendor where use of such modification would have avoided the infringement. iii) Information, materials instructions, or specifications that are themselves infringing which are provided by or on behalf of LIC or which LIC requests or requires Vendor to use. iv) the use of the Vendor 's deliverables in a manner not agreed to.	The clause imposes overly broad and one-sided indemnity obligations, extending beyond standard IP and fault-based risks, without defense control, mutuality, standard carve-outs, or cure rights, and exposes the vendor to expanded, potentially uncapped liability with no sole remedy protection or structured claim process, making the risk allocation commercially unbalanced. Bidder's uncapped liability for third-party claims due to simple negligence or any breach under the contract. We Propose to eliminate the clause entirely,	No change. Please be guided by the terms and conditions of RFP

118	Section E: Scope of Services	Pt. 6 (d) - Warranty & Annual Maintenance Contract	95	d) The proposed Database Encryption and KMS and HSM solution should be latest and not declared end-of-life within 5 (five) years from the date of submission of bid and it should be in support for a minimum period of seven years.	1. Total 7years warranty period. The proposed EDMS warranty substantially exceeds Infosys' standard position, which limits warranties to industry-standard services for 30 days post-delivery with remedies restricted to rectification, replacement, or refund. Given this deviation, Infosys can agree only subject to exceptional internal approvals.2. Trigger of rolling warranty- In the event of any replacement of defective system during the warranty period, the warranty for the replaced system shall be extended to a further period of 5 years. 3. We propose to add, " EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, BIDDER HEREBY DISCLAIMS ALL WARRANTIES (WHETHER IMPLIED, STATUTORY OR OTHERWISE) WITH RESPECT TO THE SERVICES PROVIDED UNDER THIS AGREEMENT ISSUED HEREUNDER, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.BIDDER DOES NOT REPRESENT OR WARRANT THAT SERVICES OR DELIVERABLES, INCLUDING BUT NOT LIMITED TO ANY SOFTWARE, WILL BE ERROR OR BUG FREE OR	No change. Please be guided by the terms and conditions of RFP
119	Annexure P: Contract Form	Pt 2 (d)- Project Duration, Scope of Work, and Timelines	166	d) The Vendor shall ensure the complete and timely delivery of all services, products, documentation, and other deliverables as detailed in the RFP and the Vendor's proposal, in accordance with the implementation timelines agreed between the Parties.	We propose deletion of this entire clause. In a contract having a 'time is of essence' clause, the slightest delay in performing even an insignificant obligation constitutes a material breach and such breach is deemed to be incurable. This gives the customer a very broad and 'hair trigger' right to claim LDs and also can terminate the Agreement. In such a case, Infosys may be required to refund all	No change. Please be guided by the terms and conditions of RFP
120	Section F: General Terms & Conditions	8. Termination Bidder's Right to Termination for non payment	112	Refer verbiage from RFP	i. Step in with cost to be paid by Bidder; ii. Bidder has no right to terminate the contract. Bidder cannot terminate the MSA for non-payment/ material breach. Proposed Clause: if Tenderer fails pay any invoice and remains in default not less than 7 days after being notified in writing to make such payment, then Bidder shall be entitled to: (i) suspend performance or reduce its rate of performance under any Statement of Work until such payment is made and Tenderer shall be liable for any costs of such suspension or reduction in rate of performance and Bidder shall be entitled to an extension of time; or (ii) terminate this Agreement with immediate effect. (iii)Each party has the right to terminate this Agreement if the other materially breaches any	No change. Please be guided by the terms and conditions of RFP

121	Section F: General Terms & Conditions	8. Termination, Business Continuity Beyond Contract Period 12. Bidder's Business Continuity Plan (BCP) readiness	114 116	Pg. 114 At the end of the contract period the vendor shall support takeover of the solution by LIC or a new vendor selected by LIC for business continuity. The vendor will provide an expert facility to obtain the data/knowledge in a usable format. The vendor shall render all reasonable assistance and help LIC and any new service provider engaged by LIC for smooth switch over and continuity of service. Pg. 116 The Bidder shall submit an executive summary of their own Business Continuity Plan (BCP) as part of the proposal. This submission must outline the Bidder's internal framework and preparedness to ensure continuity of services in the event of disruptions such as natural disasters, system failures, cyberattacks, or any other operational risks. The purpose of this requirement is to assess the Bidder's ability to maintain seamless service delivery throughout the duration of the contract, regardless of adverse conditions affecting their	1.No force majeure relief for delay/non-performance due to uncontrollable events. 2. No suspension right for affected services during disruption. 3. No 90-day termination right for prolonged force majeure event. 4. No remote-working flexibility or alternate delivery protection. 5. Stricter continuity expectation instead of reasonable-efforts standard. 6. Additional BCP submission obligation as part of bid. 7. Mandatory transition / takeover support to LIC or new vendor. 8. No cost allocation for extra continuity/security measures. LIC's position is broader than bidder standard as it mandates continuity, handover, and BCP readiness obligations but does not provide force majeure relief, suspension rights, or remote-working protections, resulting in unbalanced vendor risk.	No change. Please be guided by the terms and conditions of RFP
122	Section 36. Limitation of Liability, r/w Undertaking B: Undertaking by the bidder indemnifying the Life Insurance Corporation of India (LIC) against Violation of	Pt. 36 - Limitation of Liability Pt. 4 - Unlimited Liability Clause	51 191	Pg. 51 Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent, IPR, trademark, copy right or industrial design rights arising from use of the Solution or any part thereof in any of the services supplied by the vendor and used/consumed by LIC pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the vendor to pay liquidated damages to LIC; and the aggregate liability of the vendor to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment. The liability of the vendor arising out of violation of	1. Unlimited liability for Patent, trademark, copyright & IP breach (for both direct and indirect losses). 2. Capped to TCV liability of Infosys for any third party claims for any breach even due to simple negligence. 3. Uncapped (both direct and indirect) inter se and third party liability for IP claims- 4. Uncapped direct liability for cost of repairing or defective services - we Recommend to that it should be capped. Suggested clauses to be added: The total and aggregate liability of each party (including its Affiliates) to the other party (Affiliates including the service recipients) for any and all claims, arising out of or in connection with this Agreement and all Statements of Work, whether in contract, tort, indemnity (including negligence) or otherwise, shall be limited to twelve (12) times the Average Monthly Charges under the relevant Statement of Work.	No change. Please be guided by the terms and conditions of RFP

123	Section C: Instructions to Bidders (ITB)	Pt. 41 - Applicable Law	56	This RFP shall be governed by and construed in accordance with the laws of India, without giving effect to conflict of law rules. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts and hence, any legal dispute will come under the jurisdiction of Bombay High Court only.	The definition of Applicable Law is wide in nature. Bidder shall comply with the provision of all laws and regulations specifically applicable to CONTRACTOR's business activities. We propose to add the following to the definition: "Applicable Law" means all applicable laws including, but not limited to, treaties, statutes, decrees, edicts, codes, orders, instructions, judgements, rules, ordinances and regulations of any Governmental Authority and applicable to a party in the performance of its obligations under this Agreement and in the conduct of its respective line of business.	No change. Please be guided by the terms and conditions of RFP
124	Section E: Scope of Services r/w 3. General Scope: r/w 11. Service Level Agreements (SLAs) & Penalties	Phase 3: Post-Migration Optimization & Support 3. General Scope: - Pt.49 Availability SLA - Compliance Requirements	74 88 105	Pg. 88 In case of any changes in the guidelines on Software impacting the current solution, the vendor agrees to make necessary modifications to comply with the revised guidelines, after discussions with LIC Pg 105 o The bidder shall comply with LIC security policies, audit requirements and applicable regulatory guidelines during the contract period. o LIC or its authorized auditors may review SLA compliance records, logs and reports maintained by the bidder. o The bidder shall provide monthly SLA compliance reports covering uptime, incidents, resolution timelines, patch compliance and preventive maintenance activities.	1. Bidder will abide and comply with those regulations and guidelines which are informed by LIC to the Bidder in writing. 2. The successful Bidder is to abide by the job safety measures prevalent in India, which are applicable to Bidder's business activities and will undertake all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's Gross negligence. The successful Bidder will pay all indemnities arising from such incidents which are directly attributable by Bidder and will not hold LIC responsible or obligated.	No change. Please be guided by the terms and conditions of RFP

125	Section F: General Terms & Conditions	Pt. 4 - Transportation & Insurance	108	The successful Bidder should obtain insurance cover for the equipment if any supplied, for all risks up to date of delivery of the devices and acceptance by LIC. The cost for the same will be borne by the successful Bidder. Successful bidder has to submit a copy of the insurance document to LIC. Should any loss or damage occur, the vendor shall: Intimate and pursue claim with the Insurance Company till settlement and Promptly make arrangements for replacement of any damaged item/s (within fifteen days of detection of damages), irrespective of the settlement of claim by the Insurance Company.	1. No aggregate annual cap of insurance is present. We propose to mention **"2MUSD as capping on an annual aggregate basis"** 2. We do not provide Insurance policy documents evidencing the policies in existence. We can only provide a confirmatory letter from Insurance broker supporting the Insurance policy holding. 3. Term of the insurance should be for Contract Period i.e. 7years. 4. valid and enforceable insurance policies for all risks of loss or damage, public liability- making the list broader and open ended, Infosys obtain insurance under specific heads and procuring any different insurance for individual client is not possible. 5. LIC's clause is broader than Bidder standard as it places end-to-end insurance and replacement responsibility on the vendor until acceptance, instead of allocating shipping, handling, and insurance costs of customer materials to the customer.	No change. Please be guided by the terms and conditions of RFP
126	MISSING CLAUSE	AR Discounting			Suggested Clause: Customer hereby consents to Bidder assigning all or some of its Receivables under this Agreement to a third party ("Bank") and Bidder is hereby notifying Customer of such assignment. For the sake of clarity, the term "Receivables" is hereby defined as any amounts due from the Bidder under an invoice raised by Bidder for Services delivered under this Agreement. Further, Bank acknowledges that Bidder may share limited excerpts of this Agreement and other details directly relating to the Receivables on a "need to know" basis with the Bank, subject to appropriate confidentiality undertakings by the Bank.	No change. Please be guided by the terms and conditions of RFP
127	MISSING CLAUSE	NON SOLICITATION			Suggested Clause: Except as otherwise expressly agreed to by the Bidder in writing, during the period of their involvement with the provision of the Services and a further period of one (1) year thereafter, Bank agrees not to directly or indirectly or through third parties solicit or hire for employment any of Bidder's current or previous employees.	No change. Please be guided by the terms and conditions of RFP

128	MISSING CLAUSE	PAYMENT CLAUSE			In the event LIC's payments are not paid when due under this Agreement, such amounts shall bear interest at a rate equal to the lower of: (i) twelve percent (12%) per annum for the period commencing on the due date until the same are paid in full; and (ii) the maximum amount permitted by Applicable Law. Such interest shall be payable on demand.	No change. Please be guided by the terms and conditions of RFP
129	MISSING CLAUSE	COLA			For SERVICES rendered on a time-and-materials basis, the FEES shall be as set forth in the FORM OF AGREEMENT and INVOICES will be raised on a monthly basis (in arrears, unless otherwise stated in the AGREEMENT). The FEES in FORM OF AGREEMENT shall be valid for a period of one (1) year from the COMMENCEMENT DATE. The PARTIES agree to negotiate a rate revision at the latest by the first anniversary date from the date of last rate revision based on CPI of each country and if the PARTIES fail to negotiate a rate revision by the anniversary date, the rates shall be increased by three percent (3%) at onsite. The new rates shall be effective as of the first day of the first calendar month after the anniversary date.	No change. Please be guided by the terms and conditions of RFP
130		Security			We propose to add: "The LIC shall implement and maintain appropriate security measures, administrative and procedural safeguards to protects its systems and environment under its control in accordance with industry standard [ISO 27001]. LIC may also take appropriate steps for fixing any design or other gaps, vulnerability and weak processes pertaining to LIC controlled environment and systems that may be identified or highlighted by the Vendor, if any, as part of delivering services under the Agreement."	No change. Please be guided by the terms and conditions of RFP

131		IP Exclusions			Notwithstanding anything to the contrary in this Agreement or any statement of work, in no event shall Bidder be responsible for any failure to perform in accordance with the requirements of this Agreement or a Statement of Work to the extent such failure results from: (i) the acts or omissions of LIC or any agent, contractor or contractor of LIC ;(ii) hardware, software or system failures not attributable to Vendor's negligence; or (iii) LIC's specifications or (iv) any third party software or open-source software or (v) modification of the Deliverables unless made by Vendor, (vi) use or incorporation of the Deliverables in a manner for which they were not designed; or (vii) use or combination of the Deliverables with items not provided by Bidder.	No change. Please be guided by the terms and conditions of RFP
132	Section C: Instructions to Bidders (ITB)	Pt. 12 - Evaluation process for selection of bidder Bidder	35	Number of relevant implementation projects (design, supply, and implementation and / or maintenance) of Data-at-Rest Encryption (DE), KMS, and/or HSM solutions in BFSI/Govt/Pvt sector in last 5 years	Request for Modification: Number of relevant implementation projects (design, supply, and implementation and / or maintenance) of Data-at-Rest Encryption (DE), KMS, and/or HSM solutions in BFSI/Govt/Pvt sector in last **10 years**	No change. Please be guided by the terms and conditions of RFP
133	Section C: Instructions to Bidders (ITB)	Pt. 12 - Evaluation process for selection	35	Documentary proof (Work Order / Client) required	We have all solution modules requested in RFP successfully implemented in our large government engagements but it will not be specifically called out in the PO/WO.	No change. Please be guided by the terms and conditions of RFP
134	Section B: Invitation for Request for	Pt. 6 - Eligibility Criteria - Pt. 4 & Pt. 5	19	Copies of the Letter of acceptance (LoA)/ work order/ contract/ completion certificate confirming relevant experience.	We have all solution modules requested in RFP successfully implemented in our large government engagements but it will not be specifically called out in the PO/WO.	No change. Please be guided by the terms and conditions of RFP
135	Section E: Scope of Services	Clause 12	105	The unit prices quoted by the successful bidder and finalized through the Online Reverse Auction (ORA) shall remain firm and valid for a period of five (5) years from the date of issuance of the first Purchase Order under this RFP. 2. During the above validity period, LIC shall have the right to procure additional quantities of the items covered under this RFP, including but not limited to encryption solution licenses, Key Management System (KMS), Hardware Security Modules (HSM), and associated components and services	Bidder submit that price quoted shall be firm for entire contract period for BOQ submitted. Any additional quantity shall be subjected mutual agreement.	No change. Please be guided by the terms and conditions of RFP.

136	Section G: Payment Terms & Conditions	Milestone payment	118	Hardware 1. 60% on delivery 2. 20% on installation 3. 20% one month after go-live Software 1. 60% on delivery 2. 20% on installation 3. 20% one month after go-live	Biddere request to change payment milestone as below. Hardware 1. 80% on delivery 2. 20% on installation and Go-live Software 1. 80% on delivery 2. 20% on installation and Go-live	Please refer to Corrigendum-1
137	Section C : Instruction to Bidders	36 - Limitation of Liability	51	Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent, IPR, trademark, copy right or industrial design rights arising from use of the Solution or any part thereof in any of the services supplied by the vendor and used/consumed by LIC pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We would kindly request that all indirect damages be excluded because it is simply too remote to be assumed by the Bidder. We are however amenable to these grounds being uncapped (i.e. criminal negligence, wilful misconduct, IPR infringement). This clause is also unclear as the RFP does not define what "Conditions of Contract Clause" is. We would also request that the LOL apply to the cost of repairing or replacing defective equipment.	No change. Please be guided by the terms and conditions of RFP.
138	Section C : Instruction to Bidders	37 Force Majeure	52	b. Where the Vendor is the Affected Party, it will be entitled to payment for Services Accepted or work performed prior to the date of termination of the contract.	We would request minor amendments to be carried out to this clause as the vendor should be entitled to its due payments irrespective of who the affected party is and thereby the clause would read as: *" ~~Where~~ the Vendor ~~is the Affected Party, it~~ will be entitled to payment for Services Accepted or work performed prior to the date of termination of the contract."*	No change. Please be guided by the terms and conditions of RFP.

139	Section C : Instruction to Bidders	39- Indemnifying LIC	54	A. The successful bidder shall indemnify LIC: a) Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC. b) Against all losses on account of Vendor's negligence or wilful default in performance or non-performance under the contract. c) Against all third-party claims of infringement of patent, copyright, trademark etc. arising from use of the goods and services, software package or any other part thereof supplied by the vendor provided that this indemnity shall not apply to in the following cases: i) The modification of the Vendor's deliverables provided hereunder by any person other than the Vendor or its personnel ii) LIC's failure to use of any modification to the Vendor's deliverables made available by Vendor where use of such modification would have avoided the infringement. iii) Information, materials instructions, or	We would submit that the right remedy for breach of contract is damages and not indemnity. Additionally, LIC already has several other recourses including PBG, LDs, liabilities, etc. Hence, we would kindly request that the clause be amended as follows: *"A. The successful bidder shall indemnify LIC* ***for all third party direct claims*** *:* ~~*a) Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC.*~~ *b) Against all losses on account of Vendor's* ***gross*** *negligence or wilful default in performance or non-performance under the contract.c) Against all third-party claims of infringement of patent, copyright, trademark etc. arising from use of the goods and services, software package or any other part thereof supplied by the vendor provided that this indemnity shall not apply to in the following cases:i) The modification of the Vendor's deliverables provided hereunder by any person other than the Vendor or its personnel*	No change. Please be guided by the terms and conditions of RFP.
140	Section F: General Terms & Conditions	8- Termination	112	Termination by LIC for default	We would request clarity that the termination only takes place after 30 days of notice. Additionally, we would also request that the procurement of undelivered services be tied to an amount of the undelivered portion price paid by LIC. We would also request that the bidder have the right to terminate the contract in case of non-payment of more than 30 days for due payments by LIC.	No change. Please be guided by the terms and conditions of RFP.
141	Section F: General Terms &	8- Termination	113	Survival	We would submit that the right to audit is not a surviving right and is to be removed from the list.	No change. Please be guided by the terms and conditions of RFP.
142	Annexure Q			Non-Disclosure Agreement (NDA)	We would request that the indmenity be for **wilful** breaches of confidentiality and restricted to only direct losses.	No change. Please be guided by the terms and conditions of RFP.
143	Section E: Scope of Services	KMS & HSM Backup, Recovery and Provisioning	84	Loss of cryptographic keys shall be treated as a catastrophic risk, and the solution must guarantee recoverability under all failure scenarios.	Kindly clarify the acceptance criteria and validation methodology for demonstrating guaranteed key recoverability under all failure scenarios.	The requirement is for the solution to support secure backup and recovery of cryptographic keys for all supported failure scenarios within the proposed architecture. Bidders shall provide details of the available key recovery capabilities and mechanisms.
144	Section E: Scope of Services	3. General Scope – Clause 12	95	The bidder shall also provide a UAT setup for testing and validation of the proposed solution.	Kindly confirm whether LIC will provide infrastructure, operating systems and database environments for UAT, or whether the bidder is expected to provision the complete UAT environment.	Bidder has to provision UAT setup as per the scope of work mentioned in RFP

145	Section E: Scope of Services	4. Phased Procurement and Rate	92	Licenses to be provided in initial phase - Encryption licenses - Quantity 10	Kindly clarify the intended usage and deployment scope of the initial 10 encryption licenses.	Please refer to Section-E-Scope of Services -Clause-4.Phased Procurement and Rate Validity for Future Quantities - page 91 of RFP document
146	Section E: Scope of Services	4. Phased Procurement and Rate Validity for Future Quantities	93	The selected bidder shall be responsible for configuring, reconfiguring, and integrating the encryption solution, Key Management System (KMS), and Hardware Security Module (HSM) for all such existing, migrated, and newly introduced database environments during the contract period.	Kindly clarify whether any upper limit is envisaged for future onboarding, migration and reconfiguration activities covered under the no-additional-cost scope.	The requirement is prospective in nature. At present, it is not possible to estimate the number or extent of future onboarding, migration, or reconfiguration activities that may arise during the contract period. Bidders are required to provide the necessary capabilities and support for such activities as and when required.
147	Section E: Scope of Services	4. Phased Procurement and Rate Validity for Future Quantities	93	All installation, configuration, reconfiguration, integration, and related implementation activities shall be carried out by the bidder at no additional cost to LIC, within the overall scope of the contract.	Kindly clarify whether the no-additional-cost obligation shall be limited to the database growth assumptions specified in Annexure-W and the licenses procured under this RFP.	The requirement shall be governed by the overall scope of the contract and shall not be limited solely to the database growth assumptions specified in Annexure-W. All installation, configuration, reconfiguration, integration, and related implementation activities within the scope of the contract shall be carried out by the bidder at no additional cost to LIC.
148	Section E: Scope of Services	10. Project Timelines	100	Date of integration of last database shall be taken as date of completion of implementation	Kindly confirm that delays arising due to application owner dependencies, database owner dependencies, change approvals or third-party integrations shall be excluded from implementation delay calculations.	Please refer to Service Level Agreements (SLAs) & Penalties , page no 102 of RFP
149	Section E: Scope of Services	11. Service Level Agreements (SLAs) & Penalties – Security Patch & Update SLA	104	Critical security patches shall be provided within seven (7) calendar days from OEM release/advisory.	Kindly confirm that the seven-day timeline shall commence after LIC approval and availability of the approved maintenance window.	The requirement pertains to the availability of critical security patches from the OEM. The bidder shall ensure that such patches are made available and recommended for deployment within seven (7) calendar days of the OEM release/advisory. Deployment in the production environment shall be subject to LIC's approval and maintenance window requirements.
150	Annexure F: Technical Compliance	Encryption Software / Encryption Agent Specifications – Sr. No. 20	136	The encryption solution should introduce minimal performance overhead and should not significantly impact database throughput, latency, or system performance under normal workloads.	Kindly specify the acceptable performance overhead threshold that LIC will consider compliant for the proposed encryption solution.	No specific performance overhead threshold is prescribed under the RFP. Bidders shall ensure that the proposed solution introduces minimal performance impact and provide relevant performance benchmarks and sizing recommendations.
151	Annexure F: Technical Compliance	KMS / HSM Related Specifications – Sr. No. 39 &	134	send alerts (through email and SMS Gateway) and Provide proactive notifications before key expiry, rotation or lifecycle events via email and SMS.	Kindly confirm whether SMS Gateway infrastructure and integration APIs shall be provided by LIC.	LIC shall provide the available SMS Gateway infrastructure/API, if required. The bidder shall ensure integration of the proposed solution with the SMS Gateway for sending alerts and notifications.

152	Annexure G: Commercial Bid (Indicative Pricing)	Sr. No. 6	137	100 man days cost- for CRs	Kindly clarify the indicative scope of change requests expected to be covered under the 100 man-days provision.	The scope of change requests is prospective in nature and cannot be estimated at this stage. The 100 man-days provision is intended to cater to future requirements that may arise during the contract period within the scope of the contract.
153	Annexure G: Commercial Bid (Indicative Pricing)	Notes 7, 8, 9 & 10	138	LIC reserves the right to procure additional DE licenses at any time during the entire contract period... The unit rates for any additional DE licenses and associated implementation costs shall be the same as those discovered in the ORA.	Kindly clarify whether implementation, integration, migration and onboarding services associated with future license procurements shall be compensated separately or deemed included in the original contract scope.	For any additional Data Encryption licenses procured during the contract period, the applicable implementation, integration, migration, onboarding, and related service costs shall be as per the corresponding unit rates discovered in the ORA.
154	Section E: Scope of Services	11. Service Level Agreements (SLAs) & Penalties	105	Penalties arising from multiple SLA breaches during the same period shall be calculated separately and shall be cumulative in nature.	Kindly confirm whether cumulative penalties arising from multiple SLA categories during the same period shall remain subject to the overall penalty caps defined under clauses (i) and (j) of the SLA section.	Please refer to Clause-11.Service Level Agreements (SLAs) & Penalties
155	Annexure-W: Data for Sizing of the proposed DE Solution	Database Sizing Information	182	Total Number of Database Servers – 1085 and Total Number of Cores – 11097	Kindly provide current database size distribution (TB/PB) across the in-scope database platforms for accurate sizing of encryption, key management and backup infrastructure.	The database size distribution across the in-scope platforms cannot be disclosed due to security reasons. Bidders shall propose and size the solution based on the server/core details provided in the RFP and their OEM-recommended sizing practices.
156	Annexure-W: Data for Sizing of the proposed DE Solution	Database Sizing Information	183	Databases being used currently across various platforms (LIC may upgrade the versions of its Databases periodically) 1) HANA DB 2) MongoDB 3) MYSQL 4) Oracle Enterprise version & Standard version 5) PostgreSQL 6) Teradata 7) Vertica	Kindly provide database-wise distribution (number of databases/instances) across HANA, MongoDB, MySQL, Oracle Enterprise, Oracle Standard, PostgreSQL, Teradata and Vertica platforms.	Please refer to Corrigendum -1, Sr.No: 2
157	Annexure C: Eligibility Criteria	Criteria No 5	129	The Bidder should have successfully supplied, installed , implemented and/or maintained during the seven (7) years preceding the date of this RFP: At least two (2) projects involving : ? Enterprise-grade Data-at-Rest Encryption solutions (preferably beyond native database TDE), ? Centralized Key Management Systems (KMS) with full key lifecycle management, and ? Hardware Security Modules (HSMs) (preferably FIPS 140-2 Level 3 or higher),	Request LIC to modfiy the clause to below : The Bidder should have successfully supplied, installed, implemented and/or maintained during the seven (7) years preceding the date of this RFP: At least one (1) project involving : ? Enterprise-grade Data-at-Rest Encryption solutions (preferably beyond native database TDE), ? Centralized Key Management Systems (KMS) with full key lifecycle management, and ? Hardware Security Modules (HSMs) (preferably FIPS 140-2 Level 3 or higher). Bidder can also quote project where Implementation is under progress .	No change. Please be guided by the terms and conditions of RFP.

158	12. Evaluation process for selection of bidder	Technical bid evaluation criteria	35	Number of relevant implementation projects (design, supply, and implementation and / or maintenance) of Data-at-Rest Encryption (DE), KMS, and/or HSM solutions in BFSI/Govt/Pvt sector in last 5 years: • 10 marks for each implementation project • 5 marks for each maintenance-only engagement	Request LIC to modify clause as below : Number of relevant implementation projects (design, supply, and implementation and / or maintenance) of Data-at-Rest Encryption (DE), KMS, and/or HSM solutions in BFSI/Govt/Pvt sector in last 7 years: • 10 marks for each implementation project • 5 marks for each maintenance-only engagement	No change. Please be guided by the terms and conditions of RFP.
159	Section E: Scope of Services	Delivery & Implementation	102		Request overall penalty cap to 10% of Implementation Charges	No change. Please be guided by the terms and conditions of RFP.
160	Section E: Scope of	Availability SLA	102		Request overall penalty cap to 10% of TCO.	No change. Please be guided by the terms and conditions of RFP.
161	Section E: Scope of Services	2. Scope of work for Key Management Solution & HSM:	79	Symmetric cryptography support shall include:	**Query:** The requirement of ARIA,CAST, SEED algorithm is not generally applicable in the Indian procurement ecosystem and unnecessary for this	Please refer to corrigendum -1
				· AES (128/192/256-bit)		
				· Triple DES (for legacy compatibility)	**Suggested Change:** Symmetric cryptography support shall include:	
				· ARIA	· AES (128/192/256-bit)	
				· SEED	· Triple DES (for legacy compatibility)	
				· CAST	· GCM mode for authenticated encryption	
				· GCM mode for authenticated encryption	Legacy algorithms such as DES or RC-series algorithms may be supported only for backward	
				Legacy algorithms such as DES or RC-series algorithms may be supported only for backward compatibility where required.		
162	Annexure C: Eligibility Criteria	Point 4	**129**	The Bidder should have a minimum of three (3) years of experience in supply, installation, implementation and/or maintenance of enterprise-grade Data-at-Rest Encryption (DE) solutions, Key Management Systems (KMS), and Hardware Security Modules (HSMs for eligible organizations.	We request to amend the clause to include Bidder/OEM experience to enable wider participation. The clause may be revised as: "The Bidder/OEM should have a minimum of three (3) years of experience in supply, installation, implementation and/or maintenance of enterprise-grade Data-at-Rest Encryption (DE) solutions, Key Management Systems (KMS), and Hardware Security Modules (HSMs for eligible organizations."	No change. Please be guided by the terms and conditions of RFP.
163	Annexure C: Eligibility Criteria	Point 5	**129**	The Bidder should have successfully executed at least two (2) projects involving DE, KMS, and HSM solutions over the last seven (7) years.	We request to amend the clause to include Bidder/OEM experience. The clause may be revised as: "The Bidder/OEM should have successfully executed at least two (2) projects involving DE, KMS, and HSM solutions over the last seven (7) years."	No change. Please be guided by the terms and conditions of RFP.

164	2. Submission of Bid	Point 17	**26**	The bidder should not respond to this RFP in consortium with any other partner. All such consortium bids will be summarily rejected.	We request the authority to kindly allow consortium / partnership bidding, as such projects typically involve multiple specialized components (DE, KMS, HSM) that may be delivered through domain expert partners. Allowing consortium participation will enhance competition.	No change. Please be guided by the terms and conditions of RFP.
165	Section E	POC & Tuning	73		For the Proof of Concept (PoC) on a 2TB dataset, will LIC provide a representative dataset that mirrors the production data schema and query patterns to ensure the benchmark results are accurate and reliable?	LIC will provide representative data on LIC system for conducting POC.
166	Section F	KMS & HSM	76		The RFP mandates that the KMS and HSM should be from the same vendor for seamless integration. In a scenario where a HSM from one vendor and a KMS from another vendor could offer better security and functionality, would LIC be open to considering such a solution, provided the integration is KMIP-compliant and proven?	No change. Please be guided by the terms and conditions of RFP.
167	Section F	KMS & HSM	81		Is there Key Backup and Recovery cycle baselined from LIC, this will impact the HSM requriement.	No specific key backup and recovery cycle is prescribed. Bidders shall size and propose the solution, including HSM requirements, based on their recommended architecture and industry best practices.
168	E	Cloud Key managem net	82		for Bring Your Own Key (BYOK) for cloud platforms. As LIC's current environment is described as on-premises (DC, DR, Colo), can LIC share its cloud adoption roadmap and specify which Cloud Service Providers (CSPs) are in scope for this adaptation?	At present, the requirement is limited to on-premises database environments. The BYOK/BYOE requirement is intended to ensure future readiness. In the event LIC adopts cloud architecture during the contract period, the proposed solution should be capable of integrating with and supporting the applicable cloud platform(s) and associated BYOK/BYOE models.
169	E	UAT setup	85		For UAT setup for testing and validation. Will the UAT environment be a scaled-down replica of the production infrastructure, including dedicated HSMs and KMS clusters, or will it share non-production resources	LIC has not prescribed a specific UAT architecture. Bidders shall propose the UAT setup, including HSM/KMS requirements and sizing, as part of the overall solution architecture. The UAT environment shall be logically and physically segregated from the production environment. The final architecture and BoM shall be finalized by LIC after evaluation of the proposed architecture and technical presentations.

170	Section G	Payment Terms & Conditions	118	MySQL native encryption costsOn completion of successful implementation of Native encryption on all MySQL databases	Can it be made 50% adavnce and 50% on sucessful implementation instead of on completion of sucessful implementation	No change . Please be guided by terms and conditions of RFP
171	Section E	9.Resource Deployment 3.Evaluation Criteria for the	99	1.Case Studies: Evidence of managing database estates of at least 100+ nodes or 500+ TB of total data in last 5 years and MySQL Database Administrator or equivalent Cloud Provider Database Specialist Certifications – L3	We request you to kindly relax this term with no specificvalues mentioned like 100 plus nodes or 500 plus TB etc as its onetime activity and its responsibility of venodr to get it done. We request you to change it to resource should be expereience in scuh requirments.	The clause mentioned is self-explanatory.
172	Section E	9.Resource Deployment 3.Evaluation Criteria	100	Proposed engineers should ideally hold certifications MySQL Database Administrator or equivalent Cloud Provider Database Specialist certifications. – L2	Casestudy clause says equivalent Cloud Provider Database Specialist Certifications – L3, however Certification clause says equivalent Cloud Provider Database Specialist certifications. – L2 . So can we consider it L2 level. Kindly cofirm the same.	Both requirements are mutually exclusive
173					Can LIC will asked to conduct POC to all the OEM participating for the Database Encryption Solution asked for so that all the products will be compared in as aspects with reference to the solution asked for before starting the commercial evaluation. As it happens in most of the BFSI customer whiel they go for such similar solutions.	LIC reserves the right to conduct POC during the technical evaluation stage