Life Insurance Corporation of India
Central Office, Mumbai

Corrigendum - 2 Ref: LIC/CO/IT/DT/2025-26/RFP/PM/C2 Date: 24.07.2025

Life Insurance Corporation of India – RFP for selection and onboarding of OEM / System Integrator (SI) for Supply, Implementation, and Management of Centralized and Automated Patch and Vulnerability Management Solution. Ref: LIC/CO/IT/DT/2025-26/RFP/PM Date: 14.07.2025

This is with reference to the RFP released by the Life Insurance Corporation of India captioned above.

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Modification Clause
1	7. Scope of Work	7.5 SERVICE LEVELE AGREEMENTS (SLAs) & PENALTIES	79	7.5 SERVICE LEVELE AGREEMENTS (SLAs) & PENALTIES	Kindly refer 7.5 Revised SERVICE LEVEL AGREEMENTS (SLAs) & PENALTIES
2	5. BID EVALUATION PROCESS	5.10 Award Criteria	30	Additional Clause	f. LIC reserves the right to evaluate and procure the Patch Management and Vulnerability assessment components of this RFP either jointly or independently, based on the technical and commercial submissions received. Accordingly: i) LIC may award the contract for both components (Patch Management and Vulnerability Assessment) to a single Bidder if it is deemed technically and commercially advantageous. ii) LIC also reserves the right to award the two components separately, to different Bidders or to the same Bidder, depending on the merit and compliance of each component independently. iii) LIC further reserves the right to procure only the Patch Management component and forego procurement of the Vulnerability

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Modification Clause
					Assessment component, particularly in cases where client references or technical submissions for the Vulnerability Assessment component are found inadequate. iv) No claim or compensation shall be entertained by any Bidder(s) if only one of the components is awarded, or if components are awarded to separate vendors. The decision of LIC in this regard shall be final and binding. v) Bidders must quote separately for each component in both the Technical and Financial bids and clearly confirm modularity in implementation and integration.
3	6. TERMS AND CONDITIONS	6.13 Payment Terms	42	Additional Clause	13) LIC reserves the right to evaluate and procure the Patch Management and Vulnerability assessment components of this RFP either jointly or independently, based on the technical and commercial submissions received. Accordingly: i) LIC may award the contract for both components (Patch Management and Vulnerability Assessment) to a single Bidder

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Modification Clause
					if it is deemed technically and commercially advantageous. ii) LIC also reserves the right to award the two components separately, to different Bidders or to the same Bidder, depending on the merit and compliance of each component independently. iii) LIC further reserves the right to procure only the Patch Management component and forego procurement of the Vulnerability Assessment component, particularly in cases where client references or technical submissions for the Vulnerability Assessment component are found inadequate. iv) No claim or compensation shall be entertained by any Bidder(s) if only one of the components is awarded, or if components are awarded to separate vendors. The decision of LIC in this regard shall be final and binding. v) Bidders must quote separately for each component in both the Technical and Financial bids and clearly confirm modularity in implementation and integration.

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Modification Clause
4	6. TERMS AND CONDITIONS	6.13 Payment Terms	42	11) Warranties: b) The offer must include comprehensive on-site warranty for five years from the date of installation and acceptance of the systems by LIC. The warranty will include supply and installation of all updates and subsequent releases of security solutions.	11) Warranties: b) The offer must include comprehensive on-site warranty for three years from the date of installation and acceptance of the systems by LIC. The warranty will include supply and installation of all updates and subsequent releases of security solutions.
5	7. Scope of Work	7.1 Detailed Scope of Work	72	1. General Requirements k. The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period.	1. General Requirements k. The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the three-year contract period.

7.5 REVISED SERVICE LEVEL AGREEMENTS (SLAs) & PENALTIES

Successful vendor(s) will have to agree to the defined SLA and Milestone schedule and non-compliance of which will result in application of penalties/liquidated damages as per penalty clauses given below. It will form part of the contract.

The penalty so calculated will either be adjusted with the payments or will be separately realized from the bidder.

Cumulative penalty during the contract period for breach of SLA mentioned above shall be capped at 10% of the contract value (TCO).

The liquidated damages (LD)/penalties shall be deducted / recovered by LIC from any money due or becoming due to the bidder under this purchase contract or may be recovered by invoking of Bank Guarantees or otherwise from bidder or from any other amount payable to the bidder in respect of other Purchase Orders issued under this contract, levying liquidated damages without prejudice to LIC's right to levy any other penalty were provided for under the contract.

All the above are independent of each other and are applicable separately and concurrently. LD/penalty is not applicable for the reasons attributable to LIC and Force Majeure.

The bidder has to ensure adherence to time-schedules given in this RFP. Non-adherence will attract penalties as given below:

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td>Implementation Phase</td><td>Target:
Complete rollout of patch and vulnerability management agents and controls on all eligible endpoints within the implementation timeline.</td><td>
<table>
<tr><th>Coverage Achieved</th><th>Penalty (% of Total Implementation Charges)</th></tr>
<tr><td>≥ 90%</td><td>Nil</td></tr>
<tr><td>85% - < 90%</td><td>2%</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>80% - < 85%</td><td>4%</td></tr>
<tr><td>75% - < 80%</td><td>6%</td></tr>
<tr><td>70% - < 75%</td><td>8%</td></tr>
<tr><td>< 70%</td><td>10% (Max) – Material Breach</td></tr>
</table>
Note: If coverage drops below 70%, it shall be treated as a material breach and LIC reserves the right to terminate the agreement and invoke performance security.

Cap on Penalties

Implementation Phase: Capped at 10% of total implementation charges</td></tr>
<tr><td>Sustenance and Operations Phase Post Implementation and Go Live.</td><td>Target:
Maintain ≥ 90% average patch and Vulnerability Assessment (VA) compliance across all managed endpoints on a monthly basis.</td><td>If the deployed agent coverage is below 90% of Base Count on a quarterly basis, a penalty of 5 % of quarterly FMS charges will be levied.

If the deployed agent coverage is below 80% of Base Count on a monthly basis, a penalty of 10% of quarterly FMS charges will be levied.

Note: If coverage drops below 70%, it shall be treated as a material breach and LIC reserves the right to terminate the agreement and invoke performance security.

Facility Management Services(FMS) is the Support cost for 5 Onsite Resource.</td></tr>
</table>

Service Area	Service Level	Penalty
		Sustained Non-Compliance: If compliance remains below **85% for more than two consecutive quarters**, LIC shall initiate a **contractual compliance review**. Continued failure may result in: ● Engagement of OEM for joint audit, ● Mandatory submission of a remediation plan, ● Withholding of further payments, or ● Partial/full contract termination. Quarterly Patch/ VA Compliance refers to the percentage of managed endpoints (servers, desktops, laptops, etc.) that are successfully patched/ VA completed within a given quarter (typically a 3-month period), according to defined security policies and patch baselines. Quarterly Patch/ VA Compliance = { Number of endpoints that received and successfully applied required patches/ VA) / Total number of endpoints in scope X 100] Measured over a fiscal quarter (e.g., April–June, July–September).

Service Area	Service Level	Penalty
		An endpoint is considered patch compliant if: All critical and security patches (as per your patch policy or CVE severity) applicable to that system have been: Deployed (pushed or made available),Installed successfully, and Verified (via agent reporting or compliance scan). An endpoint is considered Vulnerability Assessment compliant if Assessment is completed. It complies within the defined patching window . Non-Compliant Examples Endpoints may be non-compliant due to: Agent not installed or inactive System not reachable Patch deployment failed Patch reboot pending Unauthorized or rogue systems
System Uptime Requirement	The Centralised Patch and Vulnerability Management Solution (including dashboard,	

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr>
<td></td>
<td>agent console, and reporting components) shall maintain a minimum uptime of 98.0% on a quarterly basis.

The uptime calculation shall be based on 24x7 availability of the solution across the quarter.

Planned Maintenance Window:

● Scheduled downtime notified at least 24 hours in advance will be excluded from uptime calculations, subject to a maximum of 8 hours per month.

● All scheduled downtimes must occur during off-business hours (e.g., 10:00 PM to 6:00 AM IST).

Exclusions:</td>
<td>
<table>
<tr><th>Uptime Achieved (Quarterly)</th><th>Penalty (INR per quarter)</th></tr>
<tr><td>≥ 98.0%</td><td>No penalty</td></tr>
<tr><td>97.0% to < 98.0%</td><td>₹ 50,000</td></tr>
<tr><td>95.0% to < 97.0%</td><td>₹ 1,00,000</td></tr>
<tr><td>< 95.0%</td><td>₹ 2,50,000</td></tr>
</table>
</td>
</tr>
</table>

Service Area	Service Level	Penalty
	● Penalties will not apply for outages due to: ○ Force Majeure events ○ Issues attributable to LIC's infrastructure	
Facility Management Services(FMS) with 5 Onsite Resource.	The bidder has to provide experienced and certified manpower at LIC premises as per RFP. Any gap will attract penalties. The bidder has to replace the manpower if specially asked by the LIC within a period of one month. A delay beyond next Month billing cycle will attract the penalty	One day resource cost for each day of delay , till the replacement provided by the Bidder.

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td>Security Vulnerability Management:</td><td>All identified vulnerabilities to be patched as per respective OEM recommendations. Failure to close these within timelines will attract penalties based on criticality of calls.</td><td>SLA & Penalty Matrix
<table>
<tr><th>SLA Area</th><th>Description</th><th>Target SLA / Threshold</th><th>Penalty for Breach</th></tr>
<tr><td>Patch Discovery/ Vulnerability Detection/ Zero-day vulnerability detection</td><td>Detect new patches from OEMs / CERT-In</td><td>Within 1 working day</td><td>₹5,000/day delay</td></tr>
<tr><td>Patch Categorization/ Vulnerability Categorization</td><td>Classify as Critical/Important/Non-Critical</td><td>Within 1 day of detection</td><td>₹5,000/instance</td></tr>
<tr><td>Patch UAT Deployment</td><td>Deploy patch in UAT</td><td>3 days (Critical), 7 (Others)</td><td>₹10,000/week delay</td></tr>
<tr><td>Patch Production Deployment</td><td>OEM to production deployment</td><td>Critical: 7 days
Important: 15 days
Non-Critical: 30 days</td><td>₹25,000/week (Critical)
₹15,000/week (Important)
₹5,000/week (Non-Critical)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Vulnerability Scanning Frequency</td><td>Auto-scans across infra</td><td>Monthly</td><td>₹10,000/missed scan</td></tr>
<tr><td>Vulnerability Remediation</td><td>Fix high/critical CVEs</td><td>Within 7 working days</td><td>₹25,000/week delay</td></tr>
</table>
Penalty Cap: 10% of annual contract value for FMS.
Patch Deployment Timelines
<table>
<tr><td>Patch Category</td><td>Definition</td><td>Timeline for Deployment</td><td>Deployment Environment</td></tr>
<tr><td>Critical Patches</td><td>Includes patches fixing security vulnerabilities rated High (CVSS ≥ 8.0), CERT-In/IRDAI advisories, zero-day exploits.</td><td>Within 7 working days from OEM release</td><td>UAT testing followed by Production</td></tr>
<tr><td>Important Patches</td><td>Medium-risk security patches (CVSS 4.0–7.9), stability fixes.</td><td>Within 15 working days from OEM release</td><td>UAT then Production</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Non-Critical Patches</td><td>Cosmetic updates, enhancements, low-risk patches (CVSS < 4.0).</td><td>Within 30 working days from OEM release</td><td>UAT then Production</td></tr>
</table>
</td></tr>
<tr><td>Compliance of RBI/ CERT-IN Advisories/ other regulatory advisory</td><td>Compliance by end date, as notified in the advisory . Penalty by delay by each day.</td><td>Compliance by end date - No Penalty

By Delay of each day, 25000, per day .

Penalty Cap: 10% of annual contract value for FMS.</td></tr>
</table>

These amendments will form a part of the RFP for selection and onboarding of OEM / System Integrator (SI) for Supply, Implementation, and Management of Centralized and Automated Patch and Vulnerability Management Solution. Ref: LIC/CO/IT/DT/2025-26/RFP/PM Date: 14.07.2025. All the bidders are requested to take note of the amendments and respond accordingly.

Executive Director IT/DT