REVISED ANNEXURE S2: Technical Compliance – Vulnerability Management

Other than the mandatory technical requirements specified in Annexure R, the following Technical Compliances are desired in the proposed solution.

#	Revised	Compliance (Yes/No)	Remark
1	On-premises vulnerability management platform designed to provide visibility into LIC's security posture and manage cyber risk by identifying, prioritizing, and remediating vulnerabilities across an entire IT infrastructure.		
2	The proposed solution should detect vulnerabilities, and should be capable of integrating with patch management to deploy patches on target systems to remediate the detected vulnerabilities		
3	Proposed solution should provide industry recognized vulnerability scanning and reporting for the purposes of integrated remediation of non-compliance		
4	The reporting module should contain, but not limited to, the following reports: (i) Number of vulnerabilities detected by month; (ii) Total number of computers managed and the distribution of these computers;		
5	The proposed Vulnerability Management solution should support logical grouping and assignment of assets for operational management, including grouping by user (single or multiple), project, department, and location. It should also support bulk asset grouping, as well as asset reassignment workflows to ensure continued compliance and tracking during user or ownership changes.		
6	Centralized Vulnerability Assessment across on-prem, cloud, VMs, containers		
7	Agent-based and agentless scanning support		
8	Comprehensive asset discovery and inventory		
9	Support for authenticated (credentialed) and unauthenticated scans		
10	Support for active and passive scanning		
11	CVSS v3.x scoring integration for prioritization		
12	Built-in threat intelligence integration		
13	Ability to correlate vulnerabilities with exploitability data		
14	Integration with patch management systems		
15	Role-based access control (RBAC) for different security teams		
16	Real-time dashboards with customizable visualizations		
17	Regulatory compliance reporting (PCI-DSS, ISO 27001, NIST, RBI-CSF, IRDAI guidelines etc.)		
18	Historical vulnerability trend tracking		
19	Integration with SIEM tools		
20	API support for automation and orchestration		
21	Asset tagging and grouping for targeted scan policies		
22	Scheduled scans with flexible recurrence rules		

#	Revised	Compliance (Yes/No)	Remark
23	Zero-day vulnerability detection and plugin updates		
24	Configuration compliance checks against CIS Benchmarks		
25	Risk scoring per asset and per vulnerability		
26	Executive summary and operational dashboards for different user personas		
27	Integration with ticketing systems for remediation tracking		
28	Support for cloud environments		
29	Vulnerability lifecycle management (identification → remediation → verification)		
30	Scan throttling and bandwidth control features to avoid system disruptions		
31	The Solution should be fully on-premises with no dependency on the cloud and shall not rely on component /service hosted outside the LIC's premise for any feature functionality or product capability. The solution should be sized to scale as per LIC's requirements.		
32	The Solution should have inbuilt dashboarding and reporting capability with an option of customization as per the customers requirement.		
33	The passive and active scanners as well as the agents should be fully controlled from the central console deployed on-prem without any dependency on the internet/external connectivity.		
34	The Solution should support different platforms of standard and non-standard OS, DB, and network devices firmware		
35	Tool should have the capability to conduct VA of entire IT infrastructure from the centralized VM tool.		
36	The product must support multiple geographically distributed scanning engines managed by a central on-prem console.		
37	The solution should allow the Organisation to create multiple profiles based on department, asset type, platforms, users, geographies, network zones, applications etc.		
38	The product must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.		
39	The product must allow administrators to define job functions and appropriate levels of access to functionality for user.		
40	The above profiling should ensure that the vulnerabilities, dashboards, reports, queries, data etc. should be accessible only to respective asset owner and his organization unit. There should be complete flexibility to customize it as per the Organisation's requirements.		
41	The solution must have capability to perform active and passive asset discovery scan, network VA, database VA etc, without additional licenses.		
42	The solution should be capable of scan-less vulnerability and host discovery on real time.		
43	The solution should be capable to perform unauthenticated or authenticated i.e. credential and non-credential based VA of all		

#	Revised	Compliance (Yes/No)	Remark
	entire IT Infrastructure.		
44	The solution should provide views of active and mitigated vulnerabilities with automatic migration of vulnerabilities from active to mitigated, flag re-opened vulnerabilities.		
45	The solution should provide remediation views that are automatically prioritized and streamlined for providing insight to management and application owners		
46	The solution should provide an option of uploading the custom audit policies to meet LIC's requirement. It should be possible to run this custom audits both on agents as well as agentless scanning methods.		
47	The solution should be capable to provide automated verification of Organisation's compliance policy		
48	The solution should ensure scan tool is suitably configured and fine-tuned to limit the amount of false positives in the scan results.		
49	The product must include an integrated active/passive vulnerability detection capability for full visibility of vulnerability and configuration. The passively identified detections should be forwarded to the centralized reporting and management console.		
50	The solution should provide centralized and fully automate updates of vulnerability and threat intelligence feeds from the vendor on a real time basis.		
51	The product must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and vendor best practice standards such as CIS, STIG, PCI etc.		
52	Tool should provide unique Vulnerability Priority Prediction apart from CVSS framework based on current Threat Intelligence Information.		
53	Vulnerability Prediction should not be a static rating and should change based on current Threat landscape		
54	The Solution should generate scanned reports in PDF and CSV formats. The solution should provide the customizable pdf reports as per Organisation's requirement.		
55	The solution should provide an option to encrypt and password-protect PDF reports generated		
56	The solution should have the capability of auto sending of reports via email to concerned.		
57	The solution should be capable of real time alerting mechanism.		
58	The solution should be able be able to automatically calculate Asset Criticality value and assign the same which can later be modified to reflect customers asset criticality value as recorded in any other source e.g. risk register		
59	The solution should be able to enable the user for creating variety of reports and dashboards out of vulnerability scan results for further analysis.		
60	The solution should be able to track mitigation for the reporting findings of scanning and assessment activities, maintain		

#	Revised	Compliance (Yes/No)	Remark
	comprehensive dashboard of the same.		
61	The product must fully integrate scanning and compliance to include combined licensing and consolidation of data, analysis, and querying.		
62	Dashboard elements must be fully customizable by filtering to display data based on asset list, vulnerability or compliance checks, time, key word search, IP address, etc.		
63	The product must provide the ability to generate reports directly from dashboards that include the same visual elements and results.		
64	The product must provide customizable trending of scan results in dashboards using filtered results to define multiple trend lines in a single graph.		
65	The server must provide a comprehensive API for automated scripting of scanning and exports of security data.		
66	The product must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and vendor best practice standards.		
67	The proposed solutions should conform to best practices to ensure minimum 98% service availability		
68	The Bidder should have support arrangements with the respective OEM. The successful bidder should have back to back agreement with the OEM for troubleshooting, patching, support through call centre or customer web portal and any other services which LIC is entitled to obtain from the OEM. The Bidder and LIC should be able to log a call with the OEM directly.		
69	The bidder should submit the future roadmap of at least 3 years of the respective OEM regarding development and support of proposed solutions/ products.		
70	The proposed solution should be scalable to handle additional 50% above the current requirement.		