REVISED ANNEXURE S1: Technical Compliance - Patch 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	Proposed patch management solution must offer all the patching, application/ software delivery, license metering and asset inventory management capabilities, for Windows and non-windows operating system. The OS may be all the flavours of Windows client OS(Windows 7 and above and all future versions), all flavours of Windows Server OS, all flavours of Linux Server OS, Guest OS in VMs (Using any hypervisor like VMware / Nutanix AHV etc.). All critical application/software must also be patched as soon as patch/upgrade is available. Solution must support Intel and AMD CPUs both x86 and x64 architecture.		
2	Proposed solution should do granular filtering of software patches based on environment requirements		
3	Proposed solution should identify, schedule, deliver and track operating system and automate patch delivery.		
4	Proposed solution should provide automated OS and application patch management.		
5	The proposed solution should be capable of deploying security patches and enforcing security policies on target systems to remediate the detected vulnerabilities		
6	Proposed solution should schedule periodic scans to identify missing patches		
7	Proposed solution should identify and download missing patches from vendors' websites		
8	Proposed solution should download required patches and create tasks to schedule patch deployments		
9	Proposed solution should be supported for deployment of patches at end-points and servers		
10	Proposed solution should facilitate integrated remediation of non-compliance		
11	Proposed solution should have bundled reporting software so no third party tools would be required to customize reports		
12	Proposed solution should be able to provide audit reports.		
13	Proposed solution should be capable of providing Asset Management List with details of all the Hardware and/ or software installed on LIC's network as and when required by the LIC		
14	Proposed solution should be capable of integrating with one or more Active Directory structures whenever required		
15	Proposed solution should have the ability to throttle bandwidth, either statically or dynamically. The throttling capability must support up and down stream throttling for both the server and		

#	Revised	Compliance (Yes/No)	Remark
	agents		
16	Proposed solution should support centralized architecture.		
17	Proposed solution should support decentralized architecture also.		
18	Proposed solution should be able to deploy patch management agent as well as the patches with the help of IP addresses / host name.		
19	Proposed solution should have the ability to do centralized patch management for PCs, Servers, mobile device like Laptops and Surface Device		
20	Proposed solution should be able to install package through following mechanisms: Push, Pull, User Self Service		
21	Proposed solution should support virtualized environment		
22	Proposed solution should provide remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory or Local Administrator Authentication for deploying agents to remote computers		
23	Proposed solution should provide easy to use in-place upgrade procedures for all components through the console		
24	Proposed solution should have native support for high level of encrypted communications without any dependency on additional software, hardware, third party certificates or Certificate Authority		
25	Proposed solution should support the IPv4 & IPv6		
26	Proposed solution should support centralized administration, role-based access control and administration without much load on the network		
27	Latest fixes/ updates should automatically be downloaded to the patch management server on the same day that the patch is made available on software vendors' websites.		
28	All the patches downloaded must be applied to the endpoints (all devices like servers, laptops and PCs) after successful testing to avoid any disruption in services		
29	There should be a UAT set-up where every patch is to be tested before actual installations at endpoints or servers.		
30	If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from internet, then the integrity of all such content must be verified by the proposed solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the downloaded file is intact and unchanged		
31	Proposed solution should be able to determine if a patch has already been installed on a node, even though it is assigned manually. Proposed solution should have the capability to analyse appropriate patches of the OS/ applications for the Desktop/ server in comparison to the latest available patches/ updates released by respective OEMs		
32	Proposed solution should be able to detect the required patches according to individual node’s configuration		
33	Proposed solution should allow users to postpone the deployment of a patch for a period of time determined by the administrator		

#	Revised	Compliance (Yes/No)	Remark
34	Proposed solution should support event-driven remediation i.e. automatically initiate the process on receipt of a critical patch		
35	Proposed solution should support rollback of patches and service packs applied		
36	Proposed solution should have the capability for remediation i.e. continuously deploy, monitor, detect and enforce patch management policies		
37	Proposed solution should support easy integration with enterprise Wide area Network (WAN).		
38	Proposed solution should be able to deploy any software/ files through the patch management solution		
39	Proposed solution should have the capability to generate report specific to one group of servers/endpoints or should be capable of generating reports with an enterprise view		
40	Proposed solution should be able to verify if the patches on desktop are correctly installed by confirming that the vulnerability has been remediated		
41	Proposed solution should come along with standard reports and should generate customized reports as per business requirement		
42	Proposed solution should support various reporting formats i.e. reports can be downloaded easily and or exported		
43	Proposed solution should have the ability to consolidate scan data and to produce a single report for the entire network		
44	Proposed solution should support regulatory specific reports		
45	Proposed solution should be able to manually group computers together for deployment of patches. Proposed solution should provide the ability to dynamically group computers based on asset and software information		
46	Proposed solution should support the grouping of patches into a ‘baseline’ which can take the form of monthly patch bundle e.g. ‘Critical Patches’		
47	Proposed solution should be able to re-deploy the patch on a computer automatically if the initial deployment is not successful and even if the deployed patch is un-installed by the user		
48	Proposed solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc		
49	Proposed solution should come along with all operational technical manuals along with other related documents		
50	Proposed solution should be able to identify the computers that have installed the patch that is to be rolled back on need basis and rollback updated patches on need basis.		
51	Proposed solution should be able to provide real-time (within minutes) patch deployment status monitoring		
52	Proposed solution should allow console operator to deploy patches to all computers via a central console without intervention from the users or allow console operator to target which computers to deploy the patches to		
53	Proposed solution should allow console operators to spread the patch deployment over a pre-defined period of time to reduce overall impact to network bandwidth		

#	Revised	Compliance (Yes/No)	Remark
54	Proposed solution should be capable of generating reports on patches deployed, when, by whom, to which endpoints, etc.		
55	Proposed solution should be able to identify systems with non-patched vulnerability conditions		
56	Proposed solution should allow the console user to deploy actions to remediate against the vulnerabilities identified		
57	Proposed solution should have the dashboard to drill down to show details for both compliant and non-compliant systems, including but not limited to, non-compliant controls, component name, category, identifier and type		
58	In the proposed solution, information reported should not be more than 1-7 days old for devices that are active on the network		
59	The reporting module should contain, but not limited to, the following reports: (i) Progress of all patches applied (ii)Patch Compliance report for selected month /System (iii)Patch Compliance report for single patch (iv) Total number of computers managed and the distribution of these computers;		
60	Proposed solution should allow console operators to export report in CSV, PDF,XLS & HTML format		
61	Proposed solution should allow console operators to customize and save the reports without the use of third party reporting tools		
62	Proposed solution should allow console operators to drill-down from the report to the specific computers		
63	Proposed solution should allow console operator to trigger alerts when user defined conditions are met		
64	Proposed solution should generate both pre-packaged and custom, wizard generated reports like compliance reports can be generated for one month patches or one particular patch on all system or on one system		
65	Proposed solution should be capable of software distribution and installation e.g. Chrome patches, MS Office patches		
66	Proposed solution should have automatic patch management and deploy patches for various platforms including Windows, Linux, Unix as per RFP		
67	In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals		
68	In the proposed solution, reports should be viewed online		
69	In the proposed solution, reports should be downloaded in CSV, PDF, TXT and XML formats		
70	In the proposed solution, reports should be sent through emails		
71	The proposed solution should support proper business continuity plan		
72	Vendor should provide interface to integrate to multiple monitoring and reporting tools.		
73	The proposed solutions should conform to best practices to ensure minimum 98% service availability		
74	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		

#	Revised	Compliance (Yes/No)	Remark
	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.		
75	The bidder should submit the future roadmap of at least 3 years of the respective OEM regarding development and support of proposed solutions/ products.		
76	The successful bidder shall handle all matters including the configuration, implementation, operation, monitoring, management and maintenance of the proposed solution.		
77	Bidder must have valid licenses and ATS contract with the OEM for all the Software used to implement the proposed solution		
78	The software supplied by the vendor should be of latest versions.		
79	Bidder should provide updates, patches, rollups for all software supplied including operating system and should update the same immediately after its release. Back to back OEM support for all Software and updates to current Version is required to be provided. OEM authorization, partner status and back to back support document is to be submitted as part of eligibility bid.		
80	All critical patches for all software supplied should be applied to end points within 15 days or as per the recommended timeline (whichever is lower) mentioned by OSD/OEM of release of critical patches		
81	The proposed solution should be scalable to handle additional 50% of the above current requirement.		
82	The proposed Patch 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 patch compliance and tracking during user or ownership changes.		
83	The Patch Management solution should integrate with the Vulnerability Management Solution to provide remediation for identified vulnerabilities through patch deployments and configuration updates.		
84	The solution must provide software inventory capabilities to detect and report all installed applications across endpoints, and assess their compliance from a security perspective — including version status, patch availability, and vendor support lifecycle. It should also help identify unauthorized or unsupported software that may violate internal policies or pose security risks		
85	Proposed Solution must support Agent for Windows & Linux OS (Redhat, CentOS, Ubuntu, SUSE) Operating Systems		
86	Proposed Solution must support Role-based access control to allows administrators to restrict actions to users based on the devices associated with their user role, Solution must be able to work with networking customization such as routing tables and subnet access control list and Solution must support Real-time LDAP or Active Directory integration with incorporating of LDAP groups for labels		
87	Proposed solution should support Bandwidth throttling and		

#	Revised	Compliance (Yes/No)	Remark
	synchronization to minimize network impact		
88	Proposed Solution must provide Wake-on-LAN capabilities for device for after-hours maintenance regardless of location either using remote agent or from central console , Solution must provide One-click software upgrades and Solution must be able to Integrate with remote access software to control computer clients remotely to allow administrators to shut down, restart, hibernate, lock computers		
89	Solution should provide comprehensive reporting of all modules with several format like HTML, CSV, TXT, XLS, PDF		
90	Solution must provide authentication, permissions and administrative rights management through role-based management with read, write and hidden access including integration with Single Sign on Platform.		
91	The proposed solution is required to meticulously verify the patch metadata generated by each content source. It should rigorously validate both patch installation and uninstallation processes, ensuring that the deployment does not compromise the stability of the targeted operating systems and applications. The OEM of the proposed solution is expected to conduct thorough testing and verification of patches against the following parameters before making them available for download to the central site. The criteria include: a. Confirming the deployability of the patch package. b. Ensuring the suppress-reboot functionality operates as intended. c. Validating the uninstallation functionality. d. Verifying that on-demand package caching is functional and can be triggered from endpoints. e. Confirming the effectiveness of automatic deployment scheduling. f. Utilizing SHA1 and MD5 checksums to ensure the integrity of the patch package. g. Eliminating false positives in the detection of the digital fingerprint. h. Verifying that patch content aligns with mandatory baselines. i. Displaying vulnerabilities accurately in the Update Server, ensuring correct representation. This rigorous pre-download testing approach is intended to ensure the delivery of safe patches, subsequently saving time in User Acceptance Testing (UAT) and verification processes		
92	The solution must facilitate secure external communication between the client and server connections, permitting LIC to exclusively expose agent traffic either publicly or via the DMZ Zone		
93	The Proposed solution should support TLS 1.3 & SSL Certificate to validate the integrity of the connection , Communication between the Agent and the server should be over a tunnel which is encrypted using the TLS 1.3 protocol & provide Traffic Control for bandwidth at each client		
94	The solution should provide wizard-based or silent, deployment		

#	Revised	Compliance (Yes/No)	Remark
	or removal of software installed on inventory systems without the use of 3rd party software.		
95	The solution shall support corporate, VPN, and internet-connected users. There should not be the need to purchase additional software/hardware to support users not connected to the corporate network.		
96	Single Client License should allow Solution to Capture all the VM's running on Hypervisors like VMware or Hyper-V to get details of VM's Inventory		
97	Solution should provide Windows Client Agent with Defender integration to allow administrators to quickly review the current state & perform actions to scan, update signatures in one-click from Central Console for any Client machines		
98	The proposed solution must be able to continuously assess and remediate while on or off the network related to patch management		
99	Solution should have inbuilt reporting without third party tools to customize reports, should allow console operators to export report in CSV,PDF,XLS & HTML format. Also ready report to identify Windows 11 Readiness among the inventory of devices		
100	The solution should be capable to capture audit logs like (UI User authentication, SAML authentication, SSH/console login, Mail logs, FTP logs, Inventory MIA) etc, and should be able to forward logs to remote syslog server		