Azadi Ka Amrit Mahotsav

राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

आज़ादी का अमृत महोत्सव

Corrigendum -I

RFP Reference No.: GEM/2026/B/7966910

RFP for Procurement and Implementation of IT Services Management Solutions.

The clauses amended in the RFP are as tabulated below:

S No	Clause	Earlier Clause	Revised Clause
1.	9.12 I. (a)	All the Bids must be accompanied by a refundable interest free security deposit of ₹2,00,000/- (Rs. Two Lakhs only), by way of an e-payment in favour of National using Bank.	All the Bids must be accompanied by a refundable interest free security deposit of ₹2,50,000/- (Rs. Two Lakh Fifty Thousand only), by way of an e-payment in favour of National using Bank.
2.	Technical Bids (Marks Distribution) S. No. 1	**Total number of implementations/supports of IT Services Management Solutions by bidder.** *(Only Work Completion Certificate (upto last 10 years) will be considered for award of points)*	**Total number of implementations/support of IT Services Management Solutions/NMS/UEM/Patch Management/similar services by bidder.** *(Only Work Completion Certificate (upto last 10 years) will be considered for award of points)*
3.	Technical Bids (Marks Distribution) S. No. 2	**Number of years of experience of the bidder in implementation/support of IT Services Management Solutions.**	**Number of years of experience of the bidder in implementation/support of IT Services Management Solutions/ NMS/UEM/Patch Management/ similar services.**
4.	Section 7 (8)	The successful bidder has to resolve any hardware, system software and integration issues with existing systems and application related problems during installation of the Total Solution	The successful bidder has to resolve any system software and integration issues with existing systems and application related problems during installation of the Total Solution

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि०
I. T. Deptt.
National Housing Bank, New Delhi

5.	Section 12.17.1	If not implemented within 40 days from the date of acceptance of work order, 0.5 % of the Total Solution & Implementation Cost /week subject to maximum of 10% of the Total Solution and Implementation Cost, will be levied as penalty.	If not implemented within 45 days from the date of acceptance of work order, 0.5 % of the Total Solution & Implementation Cost /week subject to maximum of 10% of the Total Solution and Implementation Cost, will be levied as penalty.
	Annexure XVIII-Section-A		
6.	Sr No. 2	Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	Ability to patch databases (RDBMS/NoSQL) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and third-party software (e.g. Adobe, Browsers, Microsoft Office Suite, .net framework etc.) natively - without a separate patching tool.
7.	Sr No. 4	The solution must support automated patch deployment for antivirus and security definition updates as a native task type.	The solution must support automated patch deployment for antivirus and security definition updates of Microsoft Defender as a native task type.
8.	Sr No. 22	Solution should enable Agents to dynamically connect to the next nearest Distribution point if the assigned Distribution point is not available.	Deleted
9.	Sr No. 32	The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status.	The solution must provide a centralised dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status.
10.	Sr No. 44	The Patch Management solution should support local distribution points through preferred servers and endpoints and also peer downloading. The Agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.	The Patch Management solution should support local distribution points through preferred servers and endpoints and also peer downloading.

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्रो०वि०
I. T. Deptt.
National Housing Bank, New Delhi

11.	Sr No. 49	All agent-server communication must be encrypted over HTTPS (TLS 1.2 or higher), with no unencrypted data exchange.	All agent-server communication must be encrypted over TLS 1.3 or higher, with no unencrypted data exchange.
12.	Sr No. 52	The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available.	The solution should support identification of published CVEs affecting managed endpoints, including CVEs for which the vendor has not yet released a patch, together with the vendor-published workaround or mitigation guidance and the severity, so that the Bank has visibility of unpatched exposure pending vendor release.
13.	Sr No. 54	The solution must support system quarantine policies isolating non-compliant or compromised endpoints from the network until remediation is confirmed.	Deleted
14.	Sr No. 57	The proposed solution should ensure that files are scanned for infections during both read and write operations.	Deleted
15.	Sr No. 59	Support periodic rotation of bitlocker keys.	Deleted
16.	Sr No. 60	The solution should support TPM and Non-TPM devices for Bitlocker encryption.	Deleted
17.	Sr No. 62	Support for patching standard desktop applications (e.g., Microsoft, Google Chrome, Mozilla etc) as well as VDI environments.	Support for patching standard desktop applications (e.g., Microsoft, Google Chrome, Mozilla etc).
18.	Sr No. 63	Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc)	Deleted
19.	Sr No. 75	The solution must support zero-touch OS deployment enabling new endpoints to be automatically imaged without administrator physical intervention, using PXE boot or equivalent mechanism.	Deleted
20.	Sr No. 76	The solution must support user profile migration as part of OS deployment, preserving user data,	Deleted

		desktop settings, and application preferences during OS refresh or upgrade cycles.	
21.	Sr No. 88	The management agent must support rebranding to display under the organisation's name and branding.	The management GUI must support rebranding to display under the organisation's name and branding.
22.	Sr No. 90	The solution must include a built-in credential manager for administrative credentials used in remote operations.	Continue
Annexure XVIII Section-B			
23.	Sr No. 2	The solution should have a unified console where all the key features of the solution as per the specifications are available in the form of a centralized dashboard for ease of access and monitoring.	Continue
24.	Sr No. 3	The access to the GUI console(s) should have proper authentication and authorization mechanisms including Multi-Factor Authentication, Role Based Access Control (RBAC) etc. This should be applicable for the centralized/unified solution dashboard as well as any GUI consoles that are part of the supplied solution.	The access to the GUI console(s) should have proper authentication and authorization mechanisms including Multi-Factor Authentication, Role Based Access Control (RBAC) etc.
Annexure XVIII Section-C			
25.	Sr No. 3	The Proposed Solution should support both Windows and Linux OS for deployment and should be 64-bit application to fully utilize the server resources on which it is installed.	The proposed solution should support deployment on either Windows or Linux operating systems and should be a 64-bit application to ensure efficient utilization of the available server resources.
26.	Sr No. 4	The proposed EMS solution must comply with the following standards: 27034-1 for application security, ISO 27001:2022 for information security management, GDPR or DPDP for data privacy, and SOC 2 Type 2	The proposed solution must comply with the following standards: ISO 27001:2022, DPDP requirements, SOC 2 Type 2 for service organization controls. This ensures robust security, regulatory compliance, and

		for service organization controls. This ensures robust security, regulatory compliance, and comprehensive data protection across all managed network operations. Valid supporting documents must be submitted with the bid.	comprehensive data protection across all managed network operations.
27.	Sr No. 9	The proposed solution should be able to accommodate network growth of up to 500 devices with any number of metrics (Ports, IP address etc.) on individual device.	The proposed solution should be able to accommodate network growth of up to 100 devices with any number of metrics (Ports, IP address etc.) on individual device.
28.	Sr No. 10	The proposed solution must provide central management of all components and administrative functions from a single web-based user interface.	The proposed solution shall provide centralized monitoring, administration, reporting, alerting, and user management through a unified web-based interface. Solutions comprising multiple integrated modules/components shall be acceptable, provided they offer seamless navigation, centralized authentication, role-based access control, and a unified operational experience.
29.	Sr No. 11	The proposed solution must be a natively unified observability platform, to seamlessly integrate full-stack monitoring, log analytics, application performance monitoring (APM), flow analytics, compliance tracking, netroute tracing, and telemetry correlation within a single cohesive system—without requiring any third-party plugins, tool-switching, or modular bolt-ons.	The proposed solution must be a unified observability design, to seamlessly integrate full stack monitoring, log analytics, application performance monitoring (APM), flow analytics, compliance tracking, netroute tracing, and telemetry correlation.
30.	Sr No. 19	The system must not use any open-source third-party relational or time-series databases for reporting data. It should use a native, proprietary-built reporting	Deleted

		database for high-speed, high-volume observability workloads and security constraints.	
31.	Sr No. 23	The proposed solution should allow the application of advanced statistical transformations and functions over selected KPIs, including but not limited to: Anomaly Detection Forecasting Moving Average Median Function Logarithmic Scale Transformation Delta/Derivative Functionality	The proposed solution should allow the application of advanced statistical transformations and functions over selected KPIs, including but not limited to: Anomaly Detection Forecasting Moving Average Median Function
32.	Sr No. 35	The proposed solution should offer a wide variety of intuitive widget visualizations to represent telemetry data effectively, including: Line Chart, Area Chart, Stacked Bar, Horizontal Bar, Vertical Bar, Pie, Donut, Top-N, Grid/Table, Sparkline, Treemap, Sankey, Bubble, Heatmap, Geo-Map, and Gauge	The proposed solution should offer a wide variety of intuitive widget visualizations to represent telemetry data effectively, including: Line Chart, Area Chart, Stacked Bar, Horizontal Bar, Vertical Bar, Pie, Donut, Top-N, Grid/Table, Treemap, Heatmap, Geo-Map, and Gauge
33.	Sr No. 35	The proposed NMS solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure.	The proposed NMS solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be able to set polling interval as low as 10 second with low overhead on target server infrastructure.
34.	Sr No. 37	The solution should support custom plugin development using Go and Python, allowing tailored data collection logic and protocol support extensions.	Deleted
35.	Sr No. 42	The system must support out-of-the-box CIS benchmarks tailored specifically for network devices.	The system must support CIS benchmarks configuration tailored specifically for network devices.
36.	Sr No. 58	The proposed solution must possess valid CIS Benchmarks Certification for Compliance Assessment, attesting its compliance with the security	Deleted

		configuration guidelines and best practices prescribed by the Center for Internet Security (CIS)	
37.	Sr No. 61	The proposal solution should support AI\ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspecious behaviour in network traffic, device performance and application metrics, Alets are triggered for deviations so Network team can respond to issues early.	Deleted
38.	Sr No. 67	Future Scalability - The system should be capable of supporting at least 15 thousand network flow per second on single server with capability to capture each unique traffic conversations	The system should be capable of supporting at least 15 thousand network flow per second with capability to capture each unique traffic conversations.
39.	Sr No. 74	The proposed solution should support agent-based auto-instrumentation for Java and .NET applications, including compatibility with a wide range of modern frameworks such as Spring Boot, ASP.NET and others without requiring code changes.	The proposed solution should support agent-based auto-instrumentation for Java and .NET applications, including compatibility with a wide range of modern frameworks such as Spring Boot, ASP.NET and others without requiring code changes. Additionally, it should allow for the manual insertion of JS snippets into the HTML header where automatic injection is not feasible.

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्रे०वि०
I. T. Deptt.
National Housing Bank, New Delhi

IT Department.
Dated 16-09-2026.

Annexure –IX - Commercial Bid Format (Revised)

Table 1 - Total Solution Cost

S.No	Description	Qty	Unit of Measurement	Total Cost excl. taxes	Applicable Taxes	Total Cost Inc. Taxes
1	License/Subscription cost of Enterprise Patch Management Solution with technical support & warranty for 3 years.	180 servers & 320 endpoints	No. of endpoints & servers			
2	License/Subscription cost of Active Directory Management and Audit Solution with technical support & warranty for 3 years.	500	No. of AD users			
3	License/Subscription cost of Unified Enterprise Management Solution with technical support & warranty for 3 years.	400 devices & 30 applications	No. of device and applications			
4	Annual Maintenance/Support Services for Existing ServiceDesk Plus Solution	1	Lot			
5	Additional ServiceDesk Plus Technician Licenses (Perpetual/Subscription as applicable)	3	No. of Technician License			
6	Operating System Licenses	To be mentioned by bidder	No. of licenses			
7	Database Licenses	To be mentioned by bidder	No. of licenses			
8	Any other Middleware / Application Server Licenses	To be mentioned by bidder	No. of licenses			
	Total Solution Cost					**I**

#For all the 3 years all software items should be under warranty and any cost for the same will be borne by the vendor.

Table 2 - Total Implementation Cost

S.No	Description	Total Cost excl. taxes	Applicable Taxes	Total Cost Inc. Taxes
1	One-time Implementation & Integration cost of Enterprise Patch Management Solution (Covering Implementation, Migration, Integration, Testing, Go-Live & Training)			
2	One-time Implementation & Integration cost of Active Directory Management and Audit Solution (Covering Implementation, Migration, Integration, Testing, Go-Live & Training)			
3	One-time Implementation & Integration cost of Unified Enterprise Management Solution (Covering Implementation, Migration, Integration, Testing, Go-Live & Training)			
Total Implementation Cost				**II**

राष्ट्रीय आवास बैंक, नई दिल्ली
सू०प्र०वि
I. T. Deptt.
National Housing Bank, New Delhi

Table 3 - Future/Optional Cost

S.No	Description	Total cost excl. taxes	Applicable Taxes	Total Cost Inc. Taxes
1	Enterprise Patch management Solution License cost of additional 10 servers			
2	Enterprise Patch management Solution License cost of additional 25 endpoints			
3	Active Directory Management and Audit Solution License cost of additional 10 users			
4	Unified Enterprise Management Solution License cost of additional 10 devices			
5	Unified Enterprise Management Solution License cost of additional 2 applications			
6	Manage Engine Service Desk Plus license cost of 1 Technician			
7	Implementation & License cost of DR instance of Enterprise Patch management Solution			
8	Implementation & License cost of DR instance of Active Directory Management and Audit Solution			
9	Implementation & License cost of DR instance of Active Directory Management and Audit Solution			
Future/Optional Cost				**III**

During the period of contract, the above rates remain same. In case of future requirement, Bank may procure any number of licenses as per the above-mentioned prices on pro-rata basis. Cost of licenses includes all the components mentioned in Total Solution Cost (I).

Table 4 - Financial Evaluation

S.No	Description	Total Cost Inc. Taxes
1	Total Cost of Ownership (TCO) = Total Solution Cost (I)+ Total Implementation Cost (II) + Total future cost (III)	(This price should be quoted in GeM)

Total Contract Value = Total Solution Cost (I) + Total Implementation Cost (II)

Total value be considered for Financial Evaluation (Y): Total Cost of Ownership (TCO) = Total Solution Cost (I)+ Total Implementation Cost (II) + Total future cost (III)

Final Bidder: Eligible and qualified bidder with minimum price quote (L1) will be marked as final bidder for this procurement.

Bidder 1				
	Sr No	Relevant Clause of RFP	Query / Request to the Authority	Bank Response
	1	General – Section A: Enterprise Patch Management Solution (Overall scope of Section A)	Section A of the RFP is titled "Enterprise Patch Management solution"; however, a significant number of specifications listed under this Section describe capabilities that belong to distinct and separately licensed product categories, and not to Patch Management: (a) Unified Endpoint Management / Client Management BIOS firmware and hardware driver patching (Sr. 3), zero-touch PXE OS provisioning and user profile migration (Sr. 75, 76), centralised printer management (Sr. 86), network drive mapping (Sr. 87), agent rebranding (Sr. 88) and Wi-Fi profile deployment (Sr. 91); (b) Endpoint Protection Platform / EDR – on-access antivirus scanning during read and write operations (Sr. 57) and network quarantine / isolation of endpoints (Sr. 54); (c) Encryption Management – BitLocker policy enforcement, recovery key escrow, key rotation and technician role restriction (Sr. 58 to 61); (d) Vulnerability Assessment / Security Configuration Management – zero-day identification (Sr. 52) and endpoint security misconfiguration scanning (Sr. 53). The simultaneous mandating of all four categories as native, single-console capabilities under a Patch Management tender is met natively by only one or two global OEM suites. The effect, whether or not intended, is that specialised and fully capable Enterprise Patch Management OEMs including OEMs that comply with the entirety of the core patch, software distribution, asset discovery, remote control and reporting requirements of this Section stand excluded at the technical evaluation stage on account of adjacent-category features that do not contribute to the Bank's patch and vulnerability remediation objective. Rule 144(i) of the General Financial Rules, 2017 requires that the subject matter of procurement be described in terms that are "objective, functional, generic and measurable" and that the description shall not indicate a requirement for a particular trade mark, trade name or brand. Rule 173(ix) further requires that specifications be broad-based to the extent feasible in order to attract a sufficient number of bidders. The Central Vigilance Commission's standing guidance on framing of tender specifications is to the same effect. We therefore request the authority, in the interest of fair and wider participation and of value for the Bank, to either (i) delete the specifications identified at (a) to (d) above from Section A, or (ii) reclassify them as "desirable / non-mandatory" specifications that are not scored and are not treated as grounds for technical disqualification. Clause-wise queries with the specific technical basis for each are submitted separately below.	Kindly refer corrigendum
	2	Section A - Enterprise Patch Management solution Sr. No. 2. Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	The clause prescribes an absolute catalogue threshold of "1000+ third party software" without publishing the list of applications actually deployed in the Bank's environment. A raw catalogue count is not an objective or measurable indicator of fitment for the following reasons: (i) Counting methodology is not standardised across OEMs some OEMs count each application once, others count every version, edition, language pack and 32-bit/64-bit architecture as a separate title, so that the same real-world coverage can be published as 400 or as 5,000 depending on the method of counting. (ii) A large catalogue number does not assure coverage of the specific OS, database, middleware and desktop applications in use at NHB, which is the only coverage that has value to the Bank. (iii) The figure as worded corresponds to the published catalogue claim of a single OEM, and therefore operates as a brand-linked qualifier rather than a functional requirement, contrary to Rule 144(i) of GFR 2017. We request the authority to publish, in the corrigendum, the list of business-critical operating systems, databases, middleware and third-party desktop applications deployed at NHB that are required to be patched, and to evaluate compliance on the basis of demonstrated coverage of that list, supported by the OEM's published patch catalogue and the ability to on-board any uncovered application through custom package/script deployment. We confirm our ability to patch the operating systems, databases and middleware expressly named in this clause.	Kindly refer corrigendum
	2	Section A - Enterprise Patch Management solution Sr. No. 3. The solution must support BIOS firmware and hardware driver patching from the central console as a native capability without requiring a separate driver management tool.	BIOS/UEFI firmware and hardware driver updates are not published through the vendor-neutral patch distribution channels that patch management platforms consume (Microsoft Update Catalogue / WSUS, and application vendors' public update repositories). They are released exclusively by the hardware OEM, in hardware-OEM-specific formats, and are distributed through that OEM's own client management utility for example Dell Command | Update and Dell Client Catalog, HP Image Assistant, Lenovo System Update / Thin Installer, and Intel Driver & Support Assistant. Any tool that offers "native" BIOS and driver patching does so through a proprietary, per-OEM integration built into a Unified Endpoint Management suite; it is therefore a UEM capability and not a Patch Management capability, and its availability is itself limited to the specific hardware makes for which that integration exists. We would also submit, for the Bank's consideration, that unattended fleet-wide automation of BIOS/firmware flashing is not regarded as good practice in a regulated banking environment: firmware updates are model-specific, are not reversible in the manner of an OS patch, carry a risk of rendering an endpoint unbootable if interrupted, and are ordinarily executed as change-controlled, model-wise campaigns by the hardware OEM's own utility. Accordingly, we request the authority to delete this clause from the scope of the Enterprise Patch Management solution. In the alternative, we request that compliance be accepted where BIOS firmware and driver updates are deployed through the proposed solution's native software / package / script deployment module, invoking the hardware OEM's own update utility which delivers the same operational outcome from the same	Please be guided by RFP
	3	Section A - Enterprise Patch Management solution Sr. No. 4. The solution must support automated patch deployment for antivirus and security definition updates as a native task type.	Antivirus and endpoint security OEMs distribute engine updates and virus/threat definition signatures exclusively through their own authenticated, proprietary update infrastructure for example Broadcom/Symantec LiveUpdate, Trend Micro ActiveUpdate, Sophos Central, and the vendor-controlled cloud tenants of CrowdStrike and SentinelOne. These OEMs deliberately do not expose signed definition repositories for consumption by third-party patch management tools; this is a security control enforced on the antivirus OEM's side, since an externally mediated signature channel would itself become an attack path into the endpoint protection stack. It is therefore not a limitation of any particular patch management product. Operationally, definition updates are released several times a day and are designed to apply continuously and automatically. Routing them through a patch management scan–approve–schedule–deploy workflow would introduce hours of latency into signature currency and would degrade, not improve, the Bank's endpoint protection posture. We request the authority to accept compliance where (i) Microsoft Defender security intelligence and Windows security definition updates are deployed natively by the proposed solution, (ii) third-party antivirus engine and definition updates continue to be delivered by the antivirus OEM's own native update mechanism, and (iii) the proposed solution reports antivirus presence, version and definition currency as part of endpoint	Kindly refer corrigendum
	4	Section A - Enterprise Patch Management solution Sr. No. 19. The Endpoint Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network and it should continue to enforce, while the device is disconnected from the network.	Two issues arise on this clause. First, the clause is drafted in terms of "Endpoint Management software", whereas the Section is titled and scoped as an "Enterprise Patch Management solution". We request the authority to align the terminology, so that bidders are evaluated against the product category actually being procured. Second, the requirement that the solution "continue to enforce while the device is disconnected from the network" is not technically achievable by any patch management product, because patch enforcement requires the patch binary itself. Where an endpoint is disconnected, the agent can and does continue to evaluate the locally cached patch baseline, maintain the compliance state offline, apply patch content already staged locally, and report and remediate on reconnection; it cannot, however, install a patch that has not been downloaded. A clause worded as an absolute enforcement obligation while offline is therefore not capable of being complied with, or of being objectively evaluated, by any bidder. Suggested Clause: "The Patch Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network, applying locally cached patch	Please be guided by RFP

	5	Section A - Enterprise Patch Management solution Sr. No. 52. The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available.	A patch management platform identifies vulnerabilities deterministically, by correlating the installed software and version inventory of each endpoint against published vulnerability intelligence NIST NVD CVE records and OEM security advisories. A zero-day vulnerability is, by definition, one for which no advisory, no CVE record and no vendor patch exists at the time of exploitation. It is consequently not discoverable by inventory-to-advisory correlation, and can only be surfaced by behavioural and heuristic detection, exploit-technique analytics or threat-intelligence telemetry — which are the functions of Endpoint Detection and Response, Extended Detection and Response and Threat Intelligence platforms, and are separately procured and separately operated by the Bank's information security function. Because no patch management product can demonstrate this capability, the clause cannot be objectively evaluated and cannot be complied with truthfully by any bidder; it can only be answered affirmatively by a bidder offering a bundled EDR/XDR module, which is outside the scope of this Section. We request the authority to delete this clause from Section A. In the alternative, we request that it be limited to the following, which is measurable and which we fully support: identification of published CVEs affecting managed endpoints, including CVEs for which the vendor has not yet released a patch, together with the vendor-published workaround or mitigation guidance and the CVSS severity, so that the Bank has visibility of unpatched exposure pending vendor release.	Kindly refer corrigendum
	6	Section A - Enterprise Patch Management solution Sr. No. 53. The solution must scan managed endpoints for security misconfigurations and enable remediation from the console.	Security configuration assessment the evaluation of operating system and application settings against CIS Benchmarks, SCAP or DISA STIG baselines is the function of a Security Configuration Management or Vulnerability Assessment product, and is a distinct discipline from patch remediation. In a bank of NHB's profile these controls are ordinarily already delivered through Active Directory Group Policy hardening baselines, the endpoint protection / EDR platform, and a dedicated vulnerability assessment tool. We would respectfully draw the authority's attention to Sr. No. 55 of this very Section, which requires the proposed solution to provide documented public REST APIs for integration with vulnerability tools, expressly naming Tenable, Rapid7 and CrowdStrike. The RFP therefore already contemplates that vulnerability assessment and endpoint security tooling are separately owned and separately deployed at the Bank. Requiring the Patch Management solution to additionally duplicate that scanning capability adds licence and operational cost without adding any control, while restricting eligibility to the small number of UEM suites that bundle a configuration-assessment module. We request the authority to delete this clause. In the alternative, we request that compliance be accepted through the documented API integration already required under Sr. No. 55, whereby misconfiguration and	Please be guided by RFP
	7	Section A - Enterprise Patch Management solution Sr. No. 54. The solution must support system quarantine policies isolating non-compliant or compromised endpoints from the network until remediation is confirmed.	Network quarantine and isolation are enforced at the network access control layer or at the host security layer by 802.1X / Network Access Control platforms such as Cisco ISE, Aruba ClearPass or Forescout, by EDR host-isolation, or by centrally managed host firewall policy. A patch management agent has no authority over switch port state, VLAN assignment, DHCP scope or session termination, and therefore cannot enforce quarantine; any product that claims this capability does so by bundling an EDR or host-firewall driver, which is a separate product category and a separate licence. We would also submit that in a regulated banking environment the automated disconnection of an endpoint from the network is a high-impact action with direct availability and business-continuity consequences, and is properly owned and authorised by the Bank's information security and network functions through its NAC/EDR controls, rather than triggered as a by-product of a patch compliance state. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the proposed solution continuously publishes endpoint patch-compliance posture through documented REST APIs and SIEM integration both already required under Sr. No. 55 and Sr. No. 94 enabling the Bank's existing NAC or EDR platform to enforce quarantine on that basis, which is the architecturally correct point of enforcement.	Kindly refere corrigendum
	8	Section A - Enterprise Patch Management solution Sr. No. 57. The proposed solution should ensure that files are scanned for infections during both read and write operations.	This clause is a description of real-time, on-access antivirus scanning implemented through a file-system filter driver. It is a core function of an Endpoint Protection Platform and has no relationship to patch identification, approval, distribution or remediation, which is the subject matter of this Section. NHB will, as a regulated entity, already have a licensed antivirus / EDR solution deployed across its endpoint estate. Introducing a second real-time on-access scanning engine on the same endpoints is not merely duplicative but is affirmatively undesirable: concurrent file-system filter drivers are a recognised cause of file-lock contention, I/O latency, application instability and mutual quarantine events, and antivirus OEMs expressly advise against running two real-time scanning engines on one host. Mandating this capability within a Patch Management tender would also restrict participation to OEMs offering a bundled antivirus engine. We request the authority to delete this clause from Section A, the capability being already provided by the Bank's existing endpoint protection solution.	Kindly refer corrigendum
	9	Section A - Enterprise Patch Management solution Sr. No. 58. The solution must support BitLocker encryption status monitoring, policy enforcement, and recovery key management for managed Windows endpoints.	BitLocker lifecycle management policy enforcement, recovery key escrow and key custody is a native Microsoft Windows capability, delivered without additional cost to an organisation already licensed for Windows Enterprise / Microsoft 365 through Active Directory Domain Services and Group Policy, and through Microsoft Intune or Microsoft Configuration Manager (which have succeeded MBAM as Microsoft's supported BitLocker administration route). It is an Encryption Management function, not a Patch Management function. Beyond the question of scope, we would submit that requiring BitLocker recovery keys to be escrowed inside a third-party operational management tool is a material expansion of the Bank's key-custody risk surface. The recovery key is the single credential that defeats full-disk encryption on every managed endpoint. Placing a second, non-Microsoft copy of that key store inside a patch management database creates an additional custodian, an additional access control boundary, an additional backup and retention obligation, and an additional audit scope under the Bank's cryptographic key management controls without any corresponding security benefit, since Active Directory already holds the authoritative escrow. We request the authority to delete Sr. No. 58 from Section A, the capability being natively available to the Bank through Active Directory / Group Policy and Microsoft Intune. In the alternative, we request that compliance be limited to read-only reporting of BitLocker encryption status as part of endpoint inventory and compliance reporting, with policy enforcement and recovery key custody remaining with Microsoft's native tooling.	This is required functionality. Please be guided by RFP.
	10	Section A - Enterprise Patch Management solution Sr. No. 59. Support periodic rotation of bitlocker keys.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds, namely that BitLocker key lifecycle management is an Encryption Management function outside the scope of an Enterprise Patch Management solution. We would add that periodic rotation of BitLocker recovery keys is itself a native Windows capability, available through the manage-bde command set and through Microsoft Intune's recovery key rotation policy, and can be invoked centrally by the Bank at no additional licence cost. A third-party rotation mechanism operating on the same keys introduces the risk of divergence between the key held in Active Directory and the key held by the third-party tool, which is precisely the failure mode that renders an encrypted endpoint unrecoverable.	Kindly refer corrigendum
	11	Section A - Enterprise Patch Management solution Sr. No. 60. The solution should support TPM and Non-TPM devices for Bitlocker encryption.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. We would further submit that whether BitLocker may be enabled on a device without a compatible TPM is determined entirely by a Windows operating system policy setting the Group Policy option "Require additional authentication at startup / Allow BitLocker without a compatible TPM" and by the corresponding startup authentication method (password or startup key). It is a Windows configuration state, not a differentiating capability of any management product, and no third-party tool can enable BitLocker on a non-TPM device except by setting that same Windows policy. We request the authority to delete this clause from Section A.	Kindly refer corrigendum
	12	Section A - Enterprise Patch Management solution Sr. No. 61. Restrict technician roles for BitLocker and recovery key access, enhancing security controls in enterprise environments.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. It presupposes that the Bank's BitLocker recovery keys are held within the proposed Patch Management solution, and requires role-based access control over that key store. If, as requested at Sr. No. 58, recovery key custody remains with Active Directory and Microsoft Intune, the corresponding access restriction is enforced by Active Directory delegation and Intune role-based access control, which are the Bank's authoritative and auditable controls for this purpose. We request the authority to delete this clause from Section A. We confirm that the proposed solution provides granular role-based access control and full audit logging over all administrative functions and data within its own scope.	Please be guided by RFP

	13	Section A - Enterprise Patch Management solution Sr. No. 75. The solution must support zero-touch OS deployment enabling new endpoints to be automatically imaged without administrator physical intervention, using PXE boot or equivalent mechanism.	We note that Sr. No. 73 and Sr. No. 74 of this Section already require OS image creation, capture, template-based customisation and deployment from the management console, and we are compliant with those requirements. Sr. No. 75 goes further and mandates zero-touch, PXE-boot-based bare-metal provisioning without any administrator intervention. We request reconsideration of this additional requirement for the following reasons: (i) PXE-based provisioning is an OS Deployment function delivered by Microsoft Deployment Toolkit, Windows Deployment Services, Microsoft Configuration Manager or Windows Autopilot, or by the hardware OEM's factory provisioning service. It is a build-and-provisioning discipline distinct from patch and vulnerability remediation. (ii) It is a one-time-per-device activity performed at the point of hardware induction or refresh, ordinarily by the Bank's desktop build team, and does not recur through the endpoint's operational life unlike patching, which is continuous. (iii) It requires enabling PXE/TFTP boot services and DHCP option changes (Options 66/67 or IP helper configuration) across the Bank's network segments. Unauthenticated network boot is a control the Bank's network security policy would normally restrict, and enabling it bank-wide is a network and security change well outside the scope of a patch management engagement. (iv) Mandating it as a native requirement narrows the eligible field to full Unified Endpoint Management suites.	Kindly refer corrigendum
	14	Section A - Enterprise Patch Management solution Sr. No. 76. The solution must support user profile migration as part of OS deployment, preserving user data, desktop settings, and application preferences during OS refresh or upgrade cycles.	User state migration is delivered by Microsoft's User State Migration Tool, which is supplied free of charge as part of the Windows Assessment and Deployment Kit, and in most enterprises is rendered largely unnecessary by OneDrive Known Folder Move, roaming user profiles or FSLogix profile containers, all of which are Microsoft entitlements the Bank is likely already to hold. Like PXE provisioning, profile migration is an episodic activity tied to hardware refresh and OS upgrade cycles, and is not part of the continuous patch and vulnerability remediation lifecycle that this Section is procuring. Its inclusion as a mandatory technical specification excludes otherwise fully capable Enterprise Patch Management platforms on a ground unconnected with the Bank's security objective. We request the authority to delete this clause from Section A, or in the alternative to reclassify it as a desirable, non-scored requirement.	Kindly refer corrigendum
	15	Section A - Enterprise Patch Management solution Sr. No. 86. The solution must support centralised printer management deploying and configuring network and local printers to Windows endpoints.	Centralised printer deployment and configuration on domain-joined Windows endpoints is a native Active Directory capability, delivered through the "Deployed Printers" Group Policy extension and Group Policy Preferences, and through Microsoft Universal Print for cloud-managed estates. It is available to the Bank at no incremental cost and is the standard, Microsoft-supported method in an Active Directory environment. It is a desktop administration and end-user configuration task that has no bearing on patch currency, vulnerability exposure or endpoint compliance, which are the objectives of this Section. Mandating it as a native Patch Management specification restricts participation to bundled Unified Endpoint Management suites without any corresponding benefit to the Bank. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where printer deployment and configuration are delivered through the proposed solution's native script and package deployment module, which achieves the identical outcome from the same central console.	Please be guided by RFP
	16	Section A - Enterprise Patch Management solution Sr. No. 87. The solution must support network drive mapping mapping network shares to specific drive letters on Windows endpoints.	This clause is submitted on the same grounds as our query on Sr. No. 86. Mapping network shares to drive letters is a native Active Directory function performed through Group Policy Preferences Drive Maps, or through logon scripts, in every domain environment. It is user-context desktop configuration, is dependent on the user's group membership and share permissions rather than on the endpoint's patch state, and bears no relationship to patch or vulnerability management. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where drive mapping is delivered through the proposed solution's native script deployment module.	Please be guided by RFP
	17	Section A - Enterprise Patch Management solution Sr. No. 88. The management agent must support rebranding to display under the organisation's name and branding.	White-labelling of an OEM's management agent is a cosmetic presentation feature offered by a limited number of OEMs. It delivers no security, operational, compliance or performance benefit to the Bank, and it does not relate in any way to the functional objective of patch and vulnerability remediation. Its inclusion as a mandatory technical specification is therefore restrictive of competition without a corresponding procurement rationale, and does not meet the test in Rule 144(i) of GFR 2017 that specifications be objective and functional. We would further submit that agent rebranding is affirmatively undesirable in a banking environment from a security operations standpoint. Concealing the true vendor identity of a privileged agent binary that runs with SYSTEM rights complicates antivirus and EDR allow-listing, weakens the Bank's ability to attribute a running process to a known vendor during incident triage and forensic review, and obscures the software inventory and SBOM record that the Bank is expected to maintain. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the end-user-facing elements of the agent self-service portal, end-user notifications and	Kindly refer corrigendum
	18	Section A - Enterprise Patch Management solution Sr. No. 89. The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.	We request the authority to confirm that compliance with this clause is satisfied where the proposed solution centrally creates, modifies and deletes Windows registry keys and values on targeted endpoints and endpoint groups through its native script / configuration deployment module, executed from the central console with scheduling, targeting, execution status and audit logging as distinct from requiring a separately named "registry management" module in the product's user interface. We confirm that we provide central set/reset of registry values on targeted Windows machines and seek this confirmation solely to ensure that all bidders are evaluated on the functional outcome rather than on the naming of a product module.	Registry value modification is required for various configurations. Please be guided by RFP
	19	Section A - Enterprise Patch Management solution Sr. No. 90. The solution must include a built-in credential manager for administrative credentials used in remote operations.	We seek the Bank's clarification on the intended architecture for this requirement, since the clause as drafted may sit in tension with the Bank's privileged access management controls. Under the RBI Cyber Security Framework and prevailing BFSI practice, privileged administrative credentials are expected to be vaulted, rotated and brokered centrally through a dedicated Privileged Access Management solution such as CyberArk, ARCON or BeyondTrust with check-out approval and session recording, precisely so that privileged secrets are not replicated into each operational management console. A requirement that a patch management tool maintain its own independent store of domain administrative credentials creates an additional privileged secret repository, an additional custodian and an additional audit scope. We accordingly request the authority to confirm: (i) whether NHB has an existing PAM platform with which the proposed solution is expected to integrate for credential brokering, and if so which platform and by what interface; (ii) that compliance will be accepted where administrative credentials are held in the solution's own encrypted credential store with role-based access control, audit logging and no plain-text retrieval, and/or are brokered from the Bank's PAM or Active Directory rather than stored in the tool; and (iii) whether the Bank requires credential rotation to be performed by the proposed solution or by its PAM platform.	This functionality is required for executing custom scripts without manually mention credentials in script. It is also required for remote troubleshooting, agent deployment etc. Please be guided by RFP
	20	Section A - Enterprise Patch Management solution Sr. No. 91. The solution must support Wi-Fi profile deployment to Windows endpoints.	Wireless profile provisioning on Windows endpoints is a native Active Directory capability, delivered through the "Wireless Network (IEEE 802.11) Policies" Group Policy extension, and through Microsoft Intune for mobile and cloud-managed estates. It is available to the Bank at no incremental cost. In a bank, enterprise wireless profiles carry 802.1X / EAP configuration and, commonly, machine or user certificates issued by the Bank's PKI. Their provisioning is therefore properly owned and controlled by the network and information security functions through the Bank's NAC and certificate infrastructure, and not distributed as a payload by a patch management tool. The requirement bears no relationship to patch currency or vulnerability remediation. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where Wi-Fi profiles are deployed through the proposed solution's native script or package	Please be guided by RFP

	21	Section A - Enterprise Patch Management solution Sr. No. 98. Solution is subject to regular penetration testing / vulnerability assessment exercise. Any vulnerability found in the solution will be patched by vendor as per defined timelines by NHB.	We accept in principle that the proposed solution will be subject to the Bank's periodic VAPT exercises and that the OEM will remediate vulnerabilities identified in its product. We seek the following clarifications and amendments, as the clause is presently not capable of being priced or accepted at bid stage: (i) Remediation timelines: the clause requires remediation "as per defined timelines by NHB", but no timelines are defined anywhere in the RFP. A product OEM operates a single, published, severity-based vulnerability remediation SLA applied uniformly across its global installed base, and cannot undertake customer-specific remediation timelines that are undefined at bid stage and to be fixed unilaterally after award. We request the authority to publish the intended remediation timelines by CVSS severity band (Critical / High / Medium / Low) in the RFP itself, so that bidders can evaluate, price and accept them. (ii) Scope of the OEM's remediation obligation: we request the authority to confirm that the obligation extends only to vulnerabilities in the OEM's own product-delivered code, packages, libraries and components, and expressly excludes the underlying operating system, database, web server, middleware and other customer-provisioned infrastructure on which the solution is installed, together with the hardware, hypervisor, network and endpoint estate. Patching, hardening and vulnerability remediation of the operating system and database layer remain the responsibility of the Bank or its system integrator, in accordance with standard software licensing practice. (iii) Third-party and OS-inherited findings: where a VAPT finding arises from a third-party or open-source component, the OEM's obligation should be to incorporate the upstream fix within its published SLA once that fix is released by the upstream maintainer, and to provide a documented mitigation or compensating control in the interim. (iv) Conduct of the exercise: we request confirmation that VAPT will be performed on the Bank's own instance in a non-production environment, under a mutual non-disclosure agreement, with findings and evidence shared with the OEM to enable validation and remediation, and that reverse engineering, decompilation and public disclosure of findings are excluded. (v) We request that the clause be amended to record that remediation is "as per the OEM's published vulnerability remediation SLA, or such timelines as are specified in the RFP", in place of timelines to be defined after award.	Kindly Refer Section 12.17 of RFP for timelines of closure of observations. Bidder has to to comply with observations pertaining to all supplied software components.
	22	Section C - Unified Enterprise Management Solution Sr. No. 7. The solution should support bi-directional CMDB sync along with auto-ticketing between the monitoring tool and ManageEngine ServiceDesk Plus.	The clause names a specific third-party OEM product as the mandatory integration target. As drafted, it is capable of being read as requiring a pre-built, product-specific connector to ManageEngine ServiceDesk Plus, which in practice is offered natively by that OEM's own monitoring products with the effect of favouring a single OEM's stack, contrary to the requirement in Rule 144(i) of GFR 2017 that specifications not indicate a requirement for a particular trade mark or trade name. Bi-directional CMDB synchronisation and automated ticket creation, update and closure are standard interoperability functions that any modern monitoring platform delivers through documented REST APIs and webhooks. We therefore request the authority to confirm: (i) that compliance will be accepted where bi-directional CMDB synchronisation and auto-ticketing are implemented through documented REST APIs and webhooks, and a pre-built ManageEngine-specific connector is not insisted upon; (ii) the edition, version and deployment model of the ManageEngine ServiceDesk Plus on-premise instance, and whether its REST API, CMDB / CI APIs and CI relationship APIs are licensed and enabled in that edition; (iii) the CI classes, attributes and relationship types to be synchronised, the direction of authority for each (which system is the master for each attribute), and the expected synchronisation frequency and volume; (iv) that the Bank will provide API access, authentication tokens, a test instance and the necessary support from its incumbent ManageEngine partner during integration and testing; and (v) that any configuration, licensing, customisation or professional-services effort required on the ManageEngine ServiceDesk Plus side sits with the Bank or its incumbent ITSM partner and is outside the bidder's scope and price. This information is necessary for all bidders to estimate integration effort accurately and to quote on a comparable basis.	Integration will be scope of bidder only. Bank will provide access of API of Service Desk Plus.
	23	Section C - Unified Enterprise Management Solution Sr. No. 33. The proposed solution should provide Network Detection and Response (NDR) capabilities to continuously monitor network traffic, detect anomalous or malicious activities, and enable rapid investigation and response to security incidents.	Network Detection and Response is a distinct security product category represented by platforms such as Darktrace, ExtraHop Reveal(x), Vectra AI and Cisco Secure Network Analytics and is not a function of an enterprise monitoring or observability platform. The two differ in three material respects: (i) Data plane: NDR requires full packet capture and deep packet inspection fed by SPAN, mirror or network TAP infrastructure, together with the associated capture appliances and storage. An enterprise management solution consumes flow telemetry (NetFlow, sFlow, J-Flow, IPFIX) and SNMP, which is metadata about conversations and is sufficient for performance, capacity and utilisation analytics but not for payload-level threat detection. (ii) Detection engine: NDR detection is built on attack-behaviour models, command-and-control and lateral-movement analytics and curated threat intelligence, maintained by a security research organisation. Monitoring platforms baseline performance behaviour, which is a different analytic objective. (iii) Response: the "Response" element of NDR requires enforcement authority over firewalls, NAC and EDR to block, isolate or terminate sessions. An enterprise monitoring platform neither holds nor should hold that authority, which in the Bank's architecture properly sits with its SOC, SIEM/SOAR and network security controls. Including NDR within the scope of a Unified Enterprise Management Solution therefore both mismatches the product category and materially narrows the eligible bidder set to the small number of OEMs that market a bundled NDR module, with a consequent effect on price discovery. We request the authority to delete this clause from Section C, the capability being properly procured and operated as part of the Bank's security stack. In the alternative, we request that compliance be accepted on the basis of flow-based traffic baselining and anomaly detection with alert forwarding to the Bank's SIEM/SOC for investigation and response — which is already required at Sr. No. 63 of this Section and which we fully	Kindly refer corrigendum
	24	Section C - Unified Enterprise Management Solution Sr. No. 75. The proposed solution should provide monitoring for SAP systems, including performance metrics, system health, and key operational parameters.	SAP environments are instrumented through interfaces controlled by SAP itself principally SAP Solution Manager and SAP Focused Run, and at the technical layer the CCMS / SAPControl web service, the /SDF/MON monitoring infrastructure and, on the Java stack, JMX. SAP does not permit byte-code instrumentation of the ABAP stack by third-party APM agents, and the installation of third-party agents on SAP application servers is governed by SAP's own support and certification policy, which can affect the customer's SAP support entitlement where unapproved agents are deployed. The extent to which any third-party solution can monitor SAP is therefore determined by the access the Bank's SAP landscape and SAP support agreement permit, and not by the capability of the monitoring product. To enable accurate and comparable responses from all bidders, we request the authority to confirm: (i) the SAP landscape in scope the products, the stack (ABAP, Java, HANA, S/4HANA) and the number of systems and instances; (ii) whether the Bank will enable and grant access to the SAPControl web service, CCMS and/or JMX interfaces, and provide a dedicated read-only monitoring service user with the necessary authorisations; (iii) whether the installation of a third-party monitoring or APM agent on SAP application servers is permitted under the Bank's SAP support and licensing agreement; and (iv) that where such access or agent installation is not permitted, compliance will be accepted on the basis of infrastructure-level monitoring of the SAP hosts operating system, database, availability, port and service response and resource utilisation or, failing that, that the clause be withdrawn from the mandatory specifications.	We are using SAP ECC 6 EHP 7 with SQL Server database. We are using two instances CI & DI.
	25	Section A - Enterprise Patch Management solution Sr. No. 32. The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status. [Read with Sr. No. 73: "...OS imaging and deployment of Windows operating systems from the cloud-connected management	Sr. No. 32 requires the compliance dashboard to be a "cloud dashboard", and Sr. No. 73 refers to a "cloud-connected management console". We seek clarification, as this wording appears inconsistent with the deployment posture that a regulated financial institution would ordinarily require, and with the balance of this Section which contemplates on-premise distribution points, air-gapped and closed-network patching (Sr. No. 6) and local content distribution. For a Housing Finance regulator and refinance institution, endpoint inventory, patch state and vulnerability posture constitute sensitive operational security data, and its residence in a vendor-operated cloud tenant raises data localisation, data residency and third-party risk considerations under the RBI framework, together with the corresponding outsourcing governance obligations. Mandating a cloud-hosted console also has the effect of excluding on-premise deployment models, which is restrictive without an evident functional rationale, since the substance of the requirement real-time compliance status, endpoint health classification and drill-down to device level is delivered identically by an on-premise centralised console. We request the authority to confirm whether the solution is to be deployed on-premise within the Bank's data centre, and accordingly to substitute the words "centralised cloud dashboard" at Sr. No. 32 with "centralised management dashboard", and "cloud-connected management console" at Sr. No. 73 with "centralised management console", retaining all functional requirements of both clauses unchanged. We confirm full	Kindly refer corrigendum

	26	Section C - Unified Enterprise Management Solution Sr. No. 66. ...must keep historical rate and Ip to Ip, Ip to protocol, protocol to protocol conversation data for a minimum of 3 months... maximum 15 minute window granularity. Sr. No. 67. Future Scalability – the system should be capable of supporting at least 15 thousand network flow per second on single server...	These clauses prescribe flow retention, granularity and throughput figures without stating the underlying environment parameters against which they are to be sized. Flow collector sizing, storage volume and licence quantum are a direct function of the sustained and peak flow rate, the number of exporters and monitored interfaces, and the retention and granularity policy applied at each tier. To enable all bidders to size the solution correctly and to quote on a uniform basis, we request the authority to confirm: (i) the number of flow-exporting devices and the total number of monitored interfaces from which flow is to be collected; (ii) the expected sustained and peak flows per second at the aggregate level, and whether the 15,000 flows per second at Sr. No. 67 is the sustained figure, the peak figure or a headroom requirement; (iii) whether the three-month retention at Sr. No. 66 is required at raw conversation granularity throughout, or whether rolled-up 15-minute aggregation is acceptable for the full three-month window raw and aggregated retention differ by an order of magnitude in storage; (iv) whether the storage required for the flow retention tier is to be provided by the Bank or is to be included in the bidder's scope, and if the latter, the storage type and protection level to be assumed; and (v) whether the "single server" requirement at Sr. No. 67 refers to a single flow collector node, and the server specification the Bank expects that figure to be achieved on. Absent these parameters, bids will not be comparable on a like-for-like basis.	Please refer section 5 of RFP for current infrastructure. Compute & Storage will be provided by bank. For rest, please be guided by RFP.
	27	Section C - Unified Enterprise Management Solution Sr. No. 61. The proposal solution should support AI/ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspicious behaviour in network traffic, device performance and application metrics. Alerts are triggered for deviations so Network team can respond to issues early.	We request the authority to confirm the intended scope of this clause, specifically that it is directed at operational anomaly detection for performance and availability management, and not at security threat detection, which is the subject of the Bank's SIEM and security stack and which we have separately queried at Sr. No. 33. We further request confirmation that compliance will be accepted where the solution provides machine-learning-based dynamic and adaptive thresholding on performance metrics, automatic baselining of normal behaviour with deviation alerting, forecasting and predictive analytics on capacity metrics, and baseline flow policies for detection of anomalous traffic behaviour as already required at Sr. No. 23, Sr. No. 24, Sr. No. 38, Sr. No. 39 and Sr. No. 63 of this Section without requiring a separately licensed security analytics or user-and-entity-behaviour-analytics engine. The word "suspicious" in the present drafting introduces a security connotation that overlaps with the NDR requirement at Sr. No. 33 and would, if read as a threat-detection requirement, restrict participation to OEMs bundling a security analytics module.	Kindly refer corrigendum
	31	Payment terms - After sign-off/go-live. Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. 80% of Total Solution Cost (as per commercial bid format) will be released. 100% of Total Implementation Cost (as per commercial bid format) will be released. This payment shall be released after the mentioned compliance has been met. At the end of every subsequent year (2nd year onwards) 10% of Total Solution Cost	We request the authority to to relax the payment terms as followed being software driven project and as per IT Industry norms :**After sign-off/go-live**.Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. **90% of Total Solution Cost** (as per commercial bid format) will be released. 100% of Total Implementation Cost (as per commercial bid format) will be released. The reamaining payment 10% shall be released against submission of Performance bank guarantee @ 10% for entire period of contract.	Please be guided by RFP
	Section B - Active Directory Management and Auditing			
	3	The solution should have a unified console where all the key features of the solution as per the specifications are available in the form of a centralized dashboard for ease of access and monitoring.	We request the authority to delete this clause so that maximum participation of leading OEM's can take place,No, Different consols as per the module.	Please be guided by RFP
	2	The access to the GUI console(s) should have proper authentication and authorization mechanisms including Multi-Factor Authentication, Role Based Access Control (RBAC) etc. This should be applicable for the centralized/unified solution dashboard as well as any GUI consoles that are part of the supplied solution.	We request the authority to delete this clause so that maximum participation of leading OEM's can take place. Pls. delete this clause as RBAC , MFA and other mechanism is thru individual module's console.	Please be guided by RFP
	6	Solution should have the feature to Audit Windows File servers, who, when, from where access the files.	We request the authority to add this clause as this Recommended to audit AD , Logon activity , AD Query & win file server. Request to add.	Please be guided by RFP
	50	The solution should provide comprehensive reporting, storage and retrieval of Active Directory logs from all domain controllers.	Solution should have Agent-based to (1) eliminate need native event logs, (2) allow for object protection, (3 optimized/configurable data transfer, and (4) real-time alerts , due to agent it can capture real time event at schema level not on log generation level . Request to incorporate this clause being industry mandate for BFSI vertical.	Please be guided by RFP
Bidder 2				
	Sr No	**Relevant Clause of RFP**	**Query / Request to the Authority**	**Bank Reply**

	1	General – Section A: Enterprise Patch Management Solution (Overall scope of Section A)	Section A of the RFP is titled "Enterprise Patch Management solution"; however, a significant number of specifications listed under this Section describe capabilities that belong to distinct and separately licensed product categories, and not to Patch Management: (a) Unified Endpoint Management / Client Management BIOS firmware and hardware driver patching (Sr. 3), zero-touch PXE OS provisioning and user profile migration (Sr. 75, 76), centralised printer management (Sr. 86), network drive mapping (Sr. 87), agent rebranding (Sr. 88) and Wi-Fi profile deployment (Sr. 91); (b) Endpoint Protection Platform / EDR – on-access antivirus scanning during read and write operations (Sr. 57) and network quarantine / isolation of endpoints (Sr. 54); (c) Encryption Management – BitLocker policy enforcement, recovery key escrow, key rotation and technician role restriction (Sr. 58 to 61); (d) Vulnerability Assessment / Security Configuration Management – zero-day identification (Sr. 52) and endpoint security misconfiguration scanning (Sr. 53). The simultaneous mandating of all four categories as native, single-console capabilities under a Patch Management tender is met natively by only one or two global OEM suites. The effect, whether or not intended, is that specialised and fully capable Enterprise Patch Management OEMs including OEMs that comply with the entirety of the core patch, software distribution, asset discovery, remote control and reporting requirements of this Section stand excluded at the technical evaluation stage on account of adjacent-category features that do not contribute to the Bank's patch and vulnerability remediation objective. Rule 144(i) of the General Financial Rules, 2017 requires that the subject matter of procurement be described in terms that are "objective, functional, generic and measurable" and that the description shall not indicate a requirement for a particular trade mark, trade name or brand. Rule 173(ix) further requires that specifications be broad-based to the extent feasible in order to attract a sufficient number of bidders. The Central Vigilance Commission's standing guidance on framing of tender specifications is to the same effect. **We therefore request the authority, in the interest of fair and wider participation and of value for the Bank, to either (i) delete the specifications identified at (a) to (d) above from Section A, or (ii) reclassify them as "desirable / non-mandatory" specifications that are not scored and are not treated as grounds for technical disqualification. Clause-wise queries with the specific technical basis for each are submitted separately below.**	Kindly refer corrigendum
	2	Section A - Enterprise Patch Management solution Sr. No. 2. Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	The clause prescribes an absolute catalogue threshold of "1000+ third party software" without publishing the list of applications actually deployed in the Bank's environment. A raw catalogue count is not an objective or measurable indicator of fitment for the following reasons: (i) Counting methodology is not standardised across OEMs some OEMs count each application once, others count every version, edition, language pack and 32-bit/64-bit architecture as a separate title, so that the same real-world coverage can be published as 400 or as 5,000 depending on the method of counting. (ii) A large catalogue number does not assure coverage of the specific OS, database, middleware and desktop applications in use at NHB, which is the only coverage that has value to the Bank. (iii) The figure as worded corresponds to the published catalogue claim of a single OEM, and therefore operates as a brand-linked qualifier rather than a functional requirement, contrary to Rule 144(i) of GFR 2017. **We request the authority to publish, in the corrigendum, the list of business-critical operating systems, databases, middleware and third-party desktop applications deployed at NHB that are required to be patched, and to evaluate compliance on the basis of demonstrated coverage of that list, supported by the OEM's published patch catalogue and the ability to on-board any uncovered application through custom package/script deployment. We confirm our ability to patch the operating systems, databases and middleware expressly named in this clause**.	Kindly refer corrigendum
	3	Section A - Enterprise Patch Management solution Sr. No. 3. The solution must support BIOS firmware and hardware driver patching from the central console as a native capability without requiring a separate driver management tool.	BIOS/UEFI firmware and hardware driver updates are not published through the vendor-neutral patch distribution channels that patch management platforms consume (Microsoft Update Catalogue / WSUS, and application vendors' public update repositories). They are released exclusively by the hardware OEM, in hardware-OEM-specific formats, and are distributed through that OEM's own client management utility for example Dell Command | Update and Dell Client Catalog, HP Image Assistant, Lenovo System Update / Thin Installer, and Intel Driver & Support Assistant. Any tool that offers "native" BIOS and driver patching does so through a proprietary, per-OEM integration built into a Unified Endpoint Management suite; it is therefore a UEM capability and not a Patch Management capability, and its availability is itself limited to the specific hardware makes for which that integration exists. We would also submit, for the Bank's consideration, that unattended fleet-wide automation of BIOS/firmware flashing is not regarded as good practice in a regulated banking environment: firmware updates are model-specific, are not reversible in the manner of an OS patch, carry a risk of rendering an endpoint unbootable if interrupted, and are ordinarily executed as change-controlled, model-wise campaigns by the hardware OEM's own utility. **Accordingly, we request the authority to delete this clause from the scope of the Enterprise Patch Management solution. In the alternative, we request that compliance be accepted where BIOS firmware and driver updates are deployed through the proposed solution's native software / package / script deployment module, invoking the hardware OEM's own update utility which delivers the same operational outcome from the**	Please be guided by RFP
	4	Section A - Enterprise Patch Management solution Sr. No. 4. The solution must support automated patch deployment for antivirus and security definition updates as a native task type.	Antivirus and endpoint security OEMs distribute engine updates and virus/threat definition signatures exclusively through their own authenticated, proprietary update infrastructure for example Broadcom/Symantec LiveUpdate, Trend Micro ActiveUpdate, Sophos Central, and the vendor-controlled cloud tenants of CrowdStrike and SentinelOne. These OEMs deliberately do not expose signed definition repositories for consumption by third-party patch management tools; this is a security control enforced on the antivirus OEM's side, since an externally mediated signature channel would itself become an attack path into the endpoint protection stack. It is therefore not a limitation of any particular patch management product. Operationally, definition updates are released several times a day and are designed to apply continuously and automatically. Routing them through a patch management scan–approve–schedule–deploy workflow would introduce hours of latency into signature currency and would degrade, not improve, the Bank's endpoint protection posture. **We request the authority to accept compliance where (i) Microsoft Defender security intelligence and Windows security definition updates are deployed natively by the proposed solution, (ii) third-party antivirus engine and definition updates continue to be delivered by the antivirus OEM's own native update mechanism, and (iii) the proposed solution reports antivirus presence, version and definition currency as part of**	Kindly refer corrigendum
	5	Section A - Enterprise Patch Management solution Sr. No. 19. The Endpoint Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network and it should continue to enforce, while the device is disconnected from the network.	Two issues arise on this clause. First, the clause is drafted in terms of "Endpoint Management software", whereas the Section is titled and scoped as an "Enterprise Patch Management solution". We request the authority to align the terminology, so that bidders are evaluated against the product category actually being procured. Second, the requirement that the solution "continue to enforce while the device is disconnected from the network" is not technically achievable by any patch management product, because patch enforcement requires the patch binary itself. Where an endpoint is disconnected, the agent can and does continue to evaluate the locally cached patch baseline, maintain the compliance state offline, apply patch content already staged locally, and report and remediate on reconnection; it cannot, however, install a patch that has not been downloaded. A clause worded as an absolute enforcement obligation while offline is therefore not capable of being complied with, or of being objectively evaluated, by any bidder. Suggested Clause: "The Patch Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network, applying locally cached patch	Please be guided by RFP
	6	Section A - Enterprise Patch Management solution Sr. No. 52. The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available.	A patch management platform identifies vulnerabilities deterministically, by correlating the installed software and version inventory of each endpoint against published vulnerability intelligence NIST NVD CVE records and OEM security advisories. A zero-day vulnerability is, by definition, one for which no advisory, no CVE record and no vendor patch exists at the time of exploitation. It is consequently not discoverable by inventory-to-advisory correlation, and can only be surfaced by behavioural and heuristic detection, exploit-technique analytics or threat-intelligence telemetry — which are the functions of Endpoint Detection and Response, Extended Detection and Response and Threat Intelligence platforms, and are separately procured and separately operated by the Bank's information security function. Because no patch management product can demonstrate this capability, the clause cannot be objectively evaluated and cannot be complied with truthfully by any bidder; it can only be answered affirmatively by a bidder offering a bundled EDR/XDR module, which is outside the scope of this Section. We request the authority to delete this clause from Section A. In the alternative, we request that it be limited to the following, which is measurable and which we fully support: identification of published CVEs affecting managed endpoints, including CVEs for which the vendor has not yet released a patch, together with the vendor-published workaround or mitigation guidance and the CVSS severity, so that the Bank has visibility of unpatched exposure pending vendor release.	Kindly refer corrigendum

	7	Section A - Enterprise Patch Management solution Sr. No. 53. The solution must scan managed endpoints for security misconfigurations and enable remediation from the console.	Security configuration assessment the evaluation of operating system and application settings against CIS Benchmarks, SCAP or DISA STIG baselines is the function of a Security Configuration Management or Vulnerability Assessment product, and is a distinct discipline from patch remediation. In a bank of NHB's profile these controls are ordinarily already delivered through Active Directory Group Policy hardening baselines, the endpoint protection / EDR platform, and a dedicated vulnerability assessment tool. We would respectfully draw the authority's attention to Sr. No. 55 of this very Section, which requires the proposed solution to provide documented public REST APIs for integration with vulnerability tools, expressly naming Tenable, Rapid7 and CrowdStrike. The RFP therefore already contemplates that vulnerability assessment and endpoint security tooling are separately owned and separately deployed at the Bank. Requiring the Patch Management solution to additionally duplicate that scanning capability adds licence and operational cost without adding any control, while restricting eligibility to the small number of UEM suites that bundle a configuration-assessment module. **We request the authority to delete this clause. In the alternative, we request that compliance be accepted through the documented API integration already required under Sr. No. 55, whereby misconfiguration and**	Please be guided by RFP
	8	Section A - Enterprise Patch Management solution Sr. No. 54. The solution must support system quarantine policies isolating non-compliant or compromised endpoints from the network until remediation is confirmed.	Network quarantine and isolation are enforced at the network access control layer or at the host security layer by 802.1X / Network Access Control platforms such as Cisco ISE, Aruba ClearPass or Forescout, by EDR host-isolation, or by centrally managed host firewall policy. A patch management agent has no authority over switch port state, VLAN assignment, DHCP scope or session termination, and therefore cannot enforce quarantine; any product that claims this capability does so by bundling an EDR or host-firewall driver, which is a separate product category and a separate licence. We would also submit that in a regulated banking environment the automated disconnection of an endpoint from the network is a high-impact action with direct availability and business-continuity consequences, and is properly owned and authorised by the Bank's information security and network functions through its NAC/EDR controls, rather than triggered as a by-product of a patch compliance state. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the proposed solution continuously publishes endpoint patch-compliance posture through documented REST APIs and SIEM integration both already required under Sr. No. 55 and Sr. No. 94 enabling the Bank's existing NAC or EDR platform to enforce quarantine on that basis, which is the architecturally correct point of enforcement.	Kindly refere corrigendum
	9	Section A - Enterprise Patch Management solution Sr. No. 57. The proposed solution should ensure that files are scanned for infections during both read and write operations.	This clause is a description of real-time, on-access antivirus scanning implemented through a file-system filter driver. It is a core function of an Endpoint Protection Platform and has no relationship to patch identification, approval, distribution or remediation, which is the subject matter of this Section. NHB will, as a regulated entity, already have a licensed antivirus / EDR solution deployed across its endpoint estate. Introducing a second real-time on-access scanning engine on the same endpoints is not merely duplicative but is affirmatively undesirable: concurrent file-system filter drivers are a recognised cause of file-lock contention, I/O latency, application instability and mutual quarantine events, and antivirus OEMs expressly advise against running two real-time scanning engines on one host. Mandating this capability within a Patch Management tender would also restrict participation to OEMs offering a bundled antivirus engine. We request the authority to delete this clause from Section A, the capability being already provided by the Bank's existing endpoint protection solution.	Kindly refer corrigendum
	10	Section A - Enterprise Patch Management solution Sr. No. 58. The solution must support BitLocker encryption status monitoring, policy enforcement, and recovery key management for managed Windows endpoints.	BitLocker lifecycle management policy enforcement, recovery key escrow and key custody is a native Microsoft Windows capability, delivered without additional cost to an organisation already licensed for Windows Enterprise / Microsoft 365 through Active Directory Domain Services and Group Policy, and through Microsoft Intune or Microsoft Configuration Manager (which have succeeded MBAM as Microsoft's supported BitLocker administration route). It is an Encryption Management function, not a Patch Management function. Beyond the question of scope, we would submit that requiring BitLocker recovery keys to be escrowed inside a third-party operational management tool is a material expansion of the Bank's key-custody risk surface. The recovery key is the single credential that defeats full-disk encryption on every managed endpoint. Placing a second, non-Microsoft copy of that key store inside a patch management database creates an additional custodian, an additional access control boundary, an additional backup and retention obligation, and an additional audit scope under the Bank's cryptographic key management controls without any corresponding security benefit, since Active Directory already holds the authoritative escrow. **We request the authority to delete Sr. No. 58 from Section A, the capability being natively available to the Bank through Active Directory / Group Policy and Microsoft Intune. In the alternative, we request that compliance be limited to read-only reporting of BitLocker encryption status as part of endpoint inventory and compliance reporting, with policy enforcement and recovery key custody remaining with Microsoft's**	This is required functionality. Please be guided by RFP.
	11	Section A - Enterprise Patch Management solution Sr. No. 59. Support periodic rotation of bitlocker keys.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds, namely that BitLocker key lifecycle management is an Encryption Management function outside the scope of an Enterprise Patch Management solution. We would add that periodic rotation of BitLocker recovery keys is itself a native Windows capability, available through the manage-bde command set and through Microsoft Intune's recovery key rotation policy, and can be invoked centrally by the Bank at no additional licence cost. A third-party rotation mechanism operating on the same keys introduces the risk of divergence between the key held in Active Directory and the key held by the third-party tool, which is precisely the failure mode that renders an encrypted endpoint unrecoverable.	Kindly refer corrigendum
	12	Section A - Enterprise Patch Management solution Sr. No. 60. The solution should support TPM and Non-TPM devices for Bitlocker encryption.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. We would further submit that whether BitLocker may be enabled on a device without a compatible TPM is determined entirely by a Windows operating system policy setting the Group Policy option "Require additional authentication at startup / Allow BitLocker without a compatible TPM" and by the corresponding startup authentication method (password or startup key). It is a Windows configuration state, not a differentiating capability of any management product, and no third-party tool can enable BitLocker on a non-TPM device except by setting that same Windows policy.	Kindly refer corrigendum
	13	Section A - Enterprise Patch Management solution Sr. No. 61. Restrict technician roles for BitLocker and recovery key access, enhancing security controls in enterprise environments.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. It presupposes that the Bank's BitLocker recovery keys are held within the proposed Patch Management solution, and requires role-based access control over that key store. If, as requested at Sr. No. 58, recovery key custody remains with Active Directory and Microsoft Intune, the corresponding access restriction is enforced by Active Directory delegation and Intune role-based access control, which are the Bank's authoritative and auditable controls for this purpose. **We request the authority to delete this clause from Section A. We confirm that the proposed solution provides granular role-based access control and full audit logging over all administrative functions and data within its own scope.**	Please be guided by RFP
	14	Section A - Enterprise Patch Management solution Sr. No. 75. The solution must support zero-touch OS deployment enabling new endpoints to be automatically imaged without administrator physical intervention, using PXE boot or equivalent mechanism.	We note that Sr. No. 73 and Sr. No. 74 of this Section already require OS image creation, capture, template-based customisation and deployment from the management console, and we are compliant with those requirements. Sr. No. 75 goes further and mandates zero-touch, PXE-boot-based bare-metal provisioning without any administrator intervention. We request reconsideration of this additional requirement for the following reasons: (i) PXE-based provisioning is an OS Deployment function delivered by Microsoft Deployment Toolkit, Windows Deployment Services, Microsoft Configuration Manager or Windows Autopilot, or by the hardware OEM's factory provisioning service. It is a build-and-provisioning discipline distinct from patch and vulnerability remediation. (ii) It is a one-time-per-device activity performed at the point of hardware induction or refresh, ordinarily by the Bank's desktop build team, and does not recur through the endpoint's operational life unlike patching, which is continuous. (iii) It requires enabling PXE/TFTP boot services and DHCP option changes (Options 66/67 or IP helper configuration) across the Bank's network segments. Unauthenticated network boot is a control the Bank's network security policy would normally restrict, and enabling it bank-wide is a network and security change well outside the scope of a patch management engagement. (iv) Mandating it as a native requirement narrows the eligible field to full Unified Endpoint Management suites.	Kindly refer corrigendum

	15	Section A - Enterprise Patch Management solution Sr. No. 76. The solution must support user profile migration as part of OS deployment, preserving user data, desktop settings, and application preferences during OS refresh or upgrade cycles.	User state migration is delivered by Microsoft's User State Migration Tool, which is supplied free of charge as part of the Windows Assessment and Deployment Kit, and in most enterprises is rendered largely unnecessary by OneDrive Known Folder Move, roaming user profiles or FSLogix profile containers, all of which are Microsoft entitlements the Bank is likely already to hold. Like PXE provisioning, profile migration is an episodic activity tied to hardware refresh and OS upgrade cycles, and is not part of the continuous patch and vulnerability remediation lifecycle that this Section is procuring. Its inclusion as a mandatory technical specification excludes otherwise fully capable Enterprise Patch Management platforms on a ground unconnected with the Bank's security objective. We request the authority to delete this clause from Section A, or in the alternative to reclassify it as a desirable, non-scored requirement.	Kindly refer corrigendum
	16	Section A - Enterprise Patch Management solution Sr. No. 86. The solution must support centralised printer management deploying and configuring network and local printers to Windows endpoints.	Centralised printer deployment and configuration on domain-joined Windows endpoints is a native Active Directory capability, delivered through the "Deployed Printers" Group Policy extension and Group Policy Preferences, and through Microsoft Universal Print for cloud-managed estates. It is available to the Bank at no incremental cost and is the standard, Microsoft-supported method in an Active Directory environment. It is a desktop administration and end-user configuration task that has no bearing on patch currency, vulnerability exposure or endpoint compliance, which are the objectives of this Section. Mandating it as a native Patch Management specification restricts participation to bundled Unified Endpoint Management suites without any corresponding benefit to the Bank. **We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where printer deployment and configuration are delivered through the proposed solution's native script and package deployment module, which achieves the identical outcome from the same central console.**	Please be guided by RFP
	17	Section A - Enterprise Patch Management solution Sr. No. 87. The solution must support network drive mapping mapping network shares to specific drive letters on Windows endpoints.	This clause is submitted on the same grounds as our query on Sr. No. 86. Mapping network shares to drive letters is a native Active Directory function performed through Group Policy Preferences Drive Maps, or through logon scripts, in every domain environment. It is user-context desktop configuration, is dependent on the user's group membership and share permissions rather than on the endpoint's patch state, and bears no relationship to patch or vulnerability management. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where drive mapping is delivered through the proposed solution's native script deployment module.	Please be guided by RFP
	18	Section A - Enterprise Patch Management solution Sr. No. 88. The management agent must support rebranding to display under the organisation's name and branding.	White-labelling of an OEM's management agent is a cosmetic presentation feature offered by a limited number of OEMs. It delivers no security, operational, compliance or performance benefit to the Bank, and it does not relate in any way to the functional objective of patch and vulnerability remediation. Its inclusion as a mandatory technical specification is therefore restrictive of competition without a corresponding procurement rationale, and does not meet the test in Rule 144(i) of GFR 2017 that specifications be objective and functional. We would further submit that agent rebranding is affirmatively undesirable in a banking environment from a security operations standpoint. Concealing the true vendor identity of a privileged agent binary that runs with SYSTEM rights complicates antivirus and EDR allow-listing, weakens the Bank's ability to attribute a running process to a known vendor during incident triage and forensic review, and obscures the software inventory and SBOM record that the Bank is expected to maintain. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the end-user-facing elements of the agent self-service portal, end-user notifications and	Kindly refer corrigendum
	19	Section A - Enterprise Patch Management solution Sr. No. 89. The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.	We request the authority to confirm that compliance with this clause is satisfied where the proposed solution centrally creates, modifies and deletes Windows registry keys and values on targeted endpoints and endpoint groups through its native script / configuration deployment module, executed from the central console with scheduling, targeting, execution status and audit logging as distinct from requiring a separately named "registry management" module in the product's user interface. **We confirm that we provide central set/reset of registry values on targeted Windows machines and seek this confirmation solely to ensure that all bidders are evaluated on the functional outcome rather than on the naming of a product module.**	Registry value modification is required for various configurations. Please be guided by RFP
	20	Section A - Enterprise Patch Management solution Sr. No. 90. The solution must include a built-in credential manager for administrative credentials used in remote operations.	We seek the Bank's clarification on the intended architecture for this requirement, since the clause as drafted may sit in tension with the Bank's privileged access management controls. Under the RBI Cyber Security Framework and prevailing BFSI practice, privileged administrative credentials are expected to be vaulted, rotated and brokered centrally through a dedicated Privileged Access Management solution such as CyberArk, ARCON or BeyondTrust with check-out approval and session recording, precisely so that privileged secrets are not replicated into each operational management console. A requirement that a patch management tool maintain its own independent store of domain administrative credentials creates an additional privileged secret repository, an additional custodian and an additional audit scope. **We accordingly request the authority to confirm:** **(i) whether NHB has an existing PAM platform with which the proposed solution is expected to integrate for credential brokering, and if so which platform and by what interface;** **(ii) that compliance will be accepted where administrative credentials are held in the solution's own encrypted credential store with role-based access control, audit logging and no plain-text retrieval, and/or are brokered from the Bank's PAM or Active Directory rather than stored in the tool; and** **(iii) whether the Bank requires credential rotation to be performed by the proposed solution or by its PAM platform.**	This functionality is required for executing custom scripts without manually mention credentials in script. It is also required for remote troubleshooting, agent deployment etc. Please be guided by RFP
	21	Section A - Enterprise Patch Management solution Sr. No. 91. The solution must support Wi-Fi profile deployment to Windows endpoints.	Wireless profile provisioning on Windows endpoints is a native Active Directory capability, delivered through the "Wireless Network (IEEE 802.11) Policies" Group Policy extension, and through Microsoft Intune for mobile and cloud-managed estates. It is available to the Bank at no incremental cost. In a bank, enterprise wireless profiles carry 802.1X / EAP configuration and, commonly, machine or user certificates issued by the Bank's PKI. Their provisioning is therefore properly owned and controlled by the network and information security functions through the Bank's NAC and certificate infrastructure, and not distributed as a payload by a patch management tool. The requirement bears no relationship to patch currency or vulnerability remediation. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where Wi-Fi profiles are deployed through the proposed solution's native script or package	Please be guided by RFP

	22	Section A - Enterprise Patch Management solution Sr. No. 98. Solution is subject to regular penetration testing / vulnerability assessment exercise. Any vulnerability found in the solution will be patched by vendor as per defined timelines by NHB.	We accept in principle that the proposed solution will be subject to the Bank's periodic VAPT exercises and that the OEM will remediate vulnerabilities identified in its product. We seek the following clarifications and amendments, as the clause is presently not capable of being priced or accepted at bid stage: (i) Remediation timelines: the clause requires remediation "as per defined timelines by NHB", but no timelines are defined anywhere in the RFP. A product OEM operates a single, published, severity-based vulnerability remediation SLA applied uniformly across its global installed base, and cannot undertake customer-specific remediation timelines that are undefined at bid stage and to be fixed unilaterally after award. We request the authority to publish the intended remediation timelines by CVSS severity band (Critical / High / Medium / Low) in the RFP itself, so that bidders can evaluate, price and accept them. (ii) Scope of the OEM's remediation obligation: we request the authority to confirm that the obligation extends only to vulnerabilities in the OEM's own product-delivered code, packages, libraries and components, and expressly excludes the underlying operating system, database, web server, middleware and other customer-provisioned infrastructure on which the solution is installed, together with the hardware, hypervisor, network and endpoint estate. Patching, hardening and vulnerability remediation of the operating system and database layer remain the responsibility of the Bank or its system integrator, in accordance with standard software licensing practice. (iii) Third-party and OS-inherited findings: where a VAPT finding arises from a third-party or open-source component, the OEM's obligation should be to incorporate the upstream fix within its published SLA once that fix is released by the upstream maintainer, and to provide a documented mitigation or compensating control in the interim. (iv) Conduct of the exercise: we request confirmation that VAPT will be performed on the Bank's own instance in a non-production environment, under a mutual non-disclosure agreement, with findings and evidence shared with the OEM to enable validation and remediation, and that reverse engineering, decompilation and public disclosure of findings are excluded. **(v) We request that the clause be amended to record that remediation is "as per the OEM's published vulnerability remediation SLA, or such timelines as are specified in the RFP", in place of timelines to be defined after award.**	Kindly Refer Section 12.17 of RFP for timelines of closure of observations. Bidder has to to comply with observations pertaining to all supplied software components.
	23	Section C - Unified Enterprise Management Solution Sr. No. 7. The solution should support bi-directional CMDB sync along with auto-ticketing between the monitoring tool and ManageEngine ServiceDesk Plus.	The clause names a specific third-party OEM product as the mandatory integration target. As drafted, it is capable of being read as requiring a pre-built, product-specific connector to ManageEngine ServiceDesk Plus, which in practice is offered natively by that OEM's own monitoring products with the effect of favouring a single OEM's stack, contrary to the requirement in Rule 144(i) of GFR 2017 that specifications not indicate a requirement for a particular trade mark or trade name. Bi-directional CMDB synchronisation and automated ticket creation, update and closure are standard interoperability functions that any modern monitoring platform delivers through documented REST APIs and webhooks. We therefore request the authority to confirm: (i) that compliance will be accepted where bi-directional CMDB synchronisation and auto-ticketing are implemented through documented REST APIs and webhooks, and a pre-built ManageEngine-specific connector is not insisted upon; (ii) the edition, version and deployment model of the ManageEngine ServiceDesk Plus on-premise instance, and whether its REST API, CMDB / CI APIs and CI relationship APIs are licensed and enabled in that edition; (iii) the CI classes, attributes and relationship types to be synchronised, the direction of authority for each (which system is the master for each attribute), and the expected synchronisation frequency and volume; (iv) that the Bank will provide API access, authentication tokens, a test instance and the necessary support from its incumbent ManageEngine partner during integration and testing; and (v) that any configuration, licensing, customisation or professional-services effort required on the ManageEngine ServiceDesk Plus side sits with the Bank or its incumbent ITSM partner and is outside the bidder's scope and price. This information is necessary for all bidders to estimate integration effort accurately and to quote on a comparable basis.	Integration will be scope of bidder only. Bank will provide access of API of Service Desk Plus.
	24	Section C - Unified Enterprise Management Solution Sr. No. 33. The proposed solution should provide Network Detection and Response (NDR) capabilities to continuously monitor network traffic, detect anomalous or malicious activities, and enable rapid investigation and response to security incidents.	Network Detection and Response is a distinct security product category represented by platforms such as Darktrace, ExtraHop Reveal(x), Vectra AI and Cisco Secure Network Analytics and is not a function of an enterprise monitoring or observability platform. The two differ in three material respects: (i) Data plane: NDR requires full packet capture and deep packet inspection fed by SPAN, mirror or network TAP infrastructure, together with the associated capture appliances and storage. An enterprise management solution consumes flow telemetry (NetFlow, sFlow, J-Flow, IPFIX) and SNMP, which is metadata about conversations and is sufficient for performance, capacity and utilisation analytics but not for payload-level threat detection. (ii) Detection engine: NDR detection is built on attack-behaviour models, command-and-control and lateral-movement analytics and curated threat intelligence, maintained by a security research organisation. Monitoring platforms baseline performance behaviour, which is a different analytic objective. (iii) Response: the "Response" element of NDR requires enforcement authority over firewalls, NAC and EDR to block, isolate or terminate sessions. An enterprise monitoring platform neither holds nor should hold that authority, which in the Bank's architecture properly sits with its SOC, SIEM/SOAR and network security controls. Including NDR within the scope of a Unified Enterprise Management Solution therefore both mismatches the product category and materially narrows the eligible bidder set to the small number of OEMs that market a bundled NDR module, with a consequent effect on price discovery. **We request the authority to delete this clause from Section C, the capability being properly procured and operated as part of the Bank's security stack. In the alternative, we request that compliance be accepted on the basis of flow-based traffic baselining and anomaly detection with alert forwarding to the Bank's SIEM/SOC for investigation and response — which is already required at Sr. No. 63 of this Section and which we**	Kindly refer corrigendum
	25	Section C - Unified Enterprise Management Solution Sr. No. 75. The proposed solution should provide monitoring for SAP systems, including performance metrics, system health, and key operational parameters.	SAP environments are instrumented through interfaces controlled by SAP itself principally SAP Solution Manager and SAP Focused Run, and at the technical layer the CCMS / SAPControl web service, the /SDF/MON monitoring infrastructure and, on the Java stack, JMX. SAP does not permit byte-code instrumentation of the ABAP stack by third-party APM agents, and the installation of third-party agents on SAP application servers is governed by SAP's own support and certification policy, which can affect the customer's SAP support entitlement where unapproved agents are deployed. The extent to which any third-party solution can monitor SAP is therefore determined by the access the Bank's SAP landscape and SAP support agreement permit, and not by the capability of the monitoring product. To enable accurate and comparable responses from all bidders, we request the authority to confirm: (i) the SAP landscape in scope the products, the stack (ABAP, Java, HANA, S/4HANA) and the number of systems and instances; (ii) whether the Bank will enable and grant access to the SAPControl web service, CCMS and/or JMX interfaces, and provide a dedicated read-only monitoring service user with the necessary authorisations; (iii) whether the installation of a third-party monitoring or APM agent on SAP application servers is permitted under the Bank's SAP support and licensing agreement; and (iv) that where such access or agent installation is not permitted, compliance will be accepted on the basis of infrastructure-level monitoring of the SAP hosts operating system, database, availability, port and service response and resource utilisation or, failing that, that the clause be withdrawn from the mandatory specifications.	We are using SAP ECC 6 EHP 7 with SQL Server database. We are using two instances CI & DI.
	26	Section A - Enterprise Patch Management solution Sr. No. 32. The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status. [Read with Sr. No. 73: "...OS imaging and deployment of Windows operating systems from the cloud-connected management	Sr. No. 32 requires the compliance dashboard to be a "cloud dashboard", and Sr. No. 73 refers to a "cloud-connected management console". We seek clarification, as this wording appears inconsistent with the deployment posture that a regulated financial institution would ordinarily require, and with the balance of this Section which contemplates on-premise distribution points, air-gapped and closed-network patching (Sr. No. 6) and local content distribution. For a Housing Finance regulator and refinance institution, endpoint inventory, patch state and vulnerability posture constitute sensitive operational security data, and its residence in a vendor-operated cloud tenant raises data localisation, data residency and third-party risk considerations under the RBI framework, together with the corresponding outsourcing governance obligations. Mandating a cloud-hosted console also has the effect of excluding on-premise deployment models, which is restrictive without an evident functional rationale, since the substance of the requirement real-time compliance status, endpoint health classification and drill-down to device level is delivered identically by an on-premise centralised console. **We request the authority to confirm whether the solution is to be deployed on-premise within the Bank's data centre, and accordingly to substitute the words "centralised cloud dashboard" at Sr. No. 32 with "centralised management dashboard", and "cloud-connected management console" at Sr. No. 73 with "centralised management console", retaining all functional requirements of both clauses unchanged. We**	Kindly refer corrigendum

	27	Section C - Unified Enterprise Management Solution Sr. No. 66. ...must keep historical rate and Ip to Ip, Ip to protocol, protocol to protocol conversation data for a minimum of 3 months... maximum 15 minute window granularity. Sr. No. 67. Future Scalability – the system should be capable of supporting at least 15 thousand network flow per second on single server...	These clauses prescribe flow retention, granularity and throughput figures without stating the underlying environment parameters against which they are to be sized. Flow collector sizing, storage volume and licence quantum are a direct function of the sustained and peak flow rate, the number of exporters and monitored interfaces, and the retention and granularity policy applied at each tier. To enable all bidders to size the solution correctly and to quote on a uniform basis, we request the authority to confirm: (i) the number of flow-exporting devices and the total number of monitored interfaces from which flow is to be collected; (ii) the expected sustained and peak flows per second at the aggregate level, and whether the 15,000 flows per second at Sr. No. 67 is the sustained figure, the peak figure or a headroom requirement; (iii) whether the three-month retention at Sr. No. 66 is required at raw conversation granularity throughout, or whether rolled-up 15-minute aggregation is acceptable for the full three-month window raw and aggregated retention differ by an order of magnitude in storage; (iv) whether the storage required for the flow retention tier is to be provided by the Bank or is to be included in the bidder's scope, and if the latter, the storage type and protection level to be assumed; and (v) whether the "single server" requirement at Sr. No. 67 refers to a single flow collector node, and the server specification the Bank expects that figure to be achieved on. Absent these parameters, bids will not be comparable on a like-for-like basis.	Please be guided by RFP. Details of network devices already provided in RFP.
	28	Section C - Unified Enterprise Management Solution Sr. No. 61. The proposal solution should support AI/ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspicious behaviour in network traffic, device performance and application metrics. Alerts are triggered for deviations so Network team can respond to issues early.	We request the authority to confirm the intended scope of this clause, specifically that it is directed at operational anomaly detection for performance and availability management, and not at security threat detection, which is the subject of the Bank's SIEM and security stack and which we have separately queried at Sr. No. 33. **We further request confirmation that compliance will be accepted where the solution provides machine-learning-based dynamic and adaptive thresholding on performance metrics, automatic baselining of normal behaviour with deviation alerting, forecasting and predictive analytics on capacity metrics, and baseline flow policies for detection of anomalous traffic behaviour as already required at Sr. No. 23, Sr. No. 24, Sr. No. 38, Sr. No. 39 and Sr. No. 63 of this Section without requiring a separately licensed security analytics or user-and-entity-behaviour-analytics engine.** The word "suspicious" in the present drafting introduces a security connotation that overlaps with the NDR requirement at Sr. No. 33 and would, if read as a threat-detection requirement, restrict participation to OEMs bundling a security analytics module.	Kindly refer corrigendum
	29	Total number of implementations/supports of IT Services Management Solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points)	For wider participation we request you to kindly amend this clause as: Total number of implementations/supports of IT Services Management Solutions by bidder/OEM. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points)	Please be guided by RFP
	30	Number of years of experience of the bidder in implementation/support of IT Services Management Solutions. a. ≥ 6 years: 10 Marks b. ≥ 4 to <6 Years: 06 Marks c. ≥ 2 to <4 Years: 2 Marks	We request you to kindly amend this clause as: Number of years of experience of the bidder in implementation /support of IT Services Management Solutions/NMS. a. ≥ 6 years: 10 Marks b. ≥ 4 to <6 Years: 06 Marks c. ≥ 2 to <4 Years: 2 Marks	Kindly refere corrigendum
	31	Total number of implementations of proposed Enterprise Patch Management solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India a. >=6: 10 Marks b. >=4 and <=5: 6 Marks c. >=2 and <=3: 2 Marks	As a System Integrator, we propose solutions in accordance to the specific requirements of the project, utilizing products and solutions from various reputed OEMs. Hence, we request you to kindly amend this clause as: Total number of implementations of Enterprise Patch Management solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India either by the bidder or the OEM. a. >=6: 10 Marks b. >=4 and <=5: 6 Marks c. >=2 and <=3: 2 Marks	Please be guided by RFP
	32	Total number of implementations of proposed Active Directory Management & Active Directory Audit Solution solution in Govt. Sector /PSU /PSBs/FIs/Large Corporate* in India a. >=6: 10 Marks b. >=4 and <=5: 6 Marks c. >=2 and <=2	We request you to kindly amend this clause as: Total number of implementations/ Migration of Active Directory Management & Active Directory Audit Solution solution in Govt. Sector /PSU /PSBs/FIs/Large Corporate* in India a. >=3: 10 Marks b. >=2 : 6 Marks c. >=1 : 2 Marks	Please be guided by RFP
	33	Total number of implementations of proposed Unified Enterprise Management Solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India a. >=6: 10 Marks b. >=4 and <=5: 6 Marks c. >=2 and <=3: 2 Marks	We request you to kindly amend this clause as: Total number of implementations of Unified Enterprise Management Solution/EMS in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India a. >=3: 10 Marks b. >=2 : 6 Marks c. >=1 : 2 Marks	Please be guided by RFP
	34	Commercial Bid Format	In the commercial bid format there are 02 sheets i.e. sheet 3 and sheet 1. As per our understanding sheet 3 is not applicable to this RFP. Kindly confirm if our understanding is correct.	Only sheet 1 to be considered
	35	The Bidder should have experience in implementation/support of IT Services Management Solutions in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs. Experience criteria is relaxed for MSE & Startup	For wider participation we request you to kindly amend this clause as: The Bidder should have experience in implementation/support of IT Services Management Solutions in at least 1 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs. Experience criteria is relaxed for MSE & Startup or The Bidder/OEM should have experience in implementation/support of IT Services Management Solutions in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs. Experience criteria is relaxed for MSE & Startup	Please be guided by RFP
Bidder 3				
	Sr No	**Relevant Clause of RFP**	**Query / Request to the Authority**	**Bank Reply**

	1	General – Section A: Enterprise Patch Management Solution (Overall scope of Section A)	Section A of the RFP is titled "Enterprise Patch Management solution"; however, a significant number of specifications listed under this Section describe capabilities that belong to distinct and separately licensed product categories, and not to Patch Management: (a) Unified Endpoint Management / Client Management BIOS firmware and hardware driver patching (Sr. 3), zero-touch PXE OS provisioning and user profile migration (Sr. 75, 76), centralised printer management (Sr. 86), network drive mapping (Sr. 87), agent rebranding (Sr. 88) and Wi-Fi profile deployment (Sr. 91); (b) Endpoint Protection Platform / EDR – on-access antivirus scanning during read and write operations (Sr. 57) and network quarantine / isolation of endpoints (Sr. 54); (c) Encryption Management – BitLocker policy enforcement, recovery key escrow, key rotation and technician role restriction (Sr. 58 to 61); (d) Vulnerability Assessment / Security Configuration Management – zero-day identification (Sr. 52) and endpoint security misconfiguration scanning (Sr. 53). The simultaneous mandating of all four categories as native, single-console capabilities under a Patch Management tender is met natively by only one or two global OEM suites. The effect, whether or not intended, is that specialised and fully capable Enterprise Patch Management OEMs including OEMs that comply with the entirety of the core patch, software distribution, asset discovery, remote control and reporting requirements of this Section stand excluded at the technical evaluation stage on account of adjacent-category features that do not contribute to the Bank's patch and vulnerability remediation objective. Rule 144(i) of the General Financial Rules, 2017 requires that the subject matter of procurement be described in terms that are "objective, functional, generic and measurable" and that the description shall not indicate a requirement for a particular trade mark, trade name or brand. Rule 173(ix) further requires that specifications be broad-based to the extent feasible in order to attract a sufficient number of bidders. The Central Vigilance Commission's standing guidance on framing of tender specifications is to the same effect. We therefore request the authority, in the interest of fair and wider participation and of value for the Bank, to either (i) delete the specifications identified at (a) to (d) above from Section A, or (ii) reclassify them as "desirable / non-mandatory" specifications that are not scored and are not treated as grounds for technical disqualification. Clause-wise queries with the specific technical basis for each are submitted separately below.	Kindly refer corrigendum
	2	Section A - Enterprise Patch Management solution Sr. No. 2. Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	The clause prescribes an absolute catalogue threshold of "1000+ third party software" without publishing the list of applications actually deployed in the Bank's environment. A raw catalogue count is not an objective or measurable indicator of fitment for the following reasons: (i) Counting methodology is not standardised across OEMs some OEMs count each application once, others count every version, edition, language pack and 32-bit/64-bit architecture as a separate title, so that the same real-world coverage can be published as 400 or as 5,000 depending on the method of counting. (ii) A large catalogue number does not assure coverage of the specific OS, database, middleware and desktop applications in use at NHB, which is the only coverage that has value to the Bank. (iii) The figure as worded corresponds to the published catalogue claim of a single OEM, and therefore operates as a brand-linked qualifier rather than a functional requirement, contrary to Rule 144(i) of GFR 2017. We request the authority to publish, in the corrigendum, the list of business-critical operating systems, databases, middleware and third-party desktop applications deployed at NHB that are required to be patched, and to evaluate compliance on the basis of demonstrated coverage of that list, supported by the OEM's published patch catalogue and the ability to on-board any uncovered application through custom package/script deployment. We confirm our ability to patch the operating systems, databases and middleware expressly named in this clause.	Kindly refer corrigendum
	3	Section A - Enterprise Patch Management solution Sr. No. 3. The solution must support BIOS firmware and hardware driver patching from the central console as a native capability without requiring a separate driver management tool.	BIOS/UEFI firmware and hardware driver updates are not published through the vendor-neutral patch distribution channels that patch management platforms consume (Microsoft Update Catalogue / WSUS, and application vendors' public update repositories). They are released exclusively by the hardware OEM, in hardware-OEM-specific formats, and are distributed through that OEM's own client management utility for example Dell Command | Update and Dell Client Catalog, HP Image Assistant, Lenovo System Update / Thin Installer, and Intel Driver & Support Assistant. Any tool that offers "native" BIOS and driver patching does so through a proprietary, per-OEM integration built into a Unified Endpoint Management suite; it is therefore a UEM capability and not a Patch Management capability, and its availability is itself limited to the specific hardware makes for which that integration exists. We would also submit, for the Bank's consideration, that unattended fleet-wide automation of BIOS/firmware flashing is not regarded as good practice in a regulated banking environment: firmware updates are model-specific, are not reversible in the manner of an OS patch, carry a risk of rendering an endpoint unbootable if interrupted, and are ordinarily executed as change-controlled, model-wise campaigns by the hardware OEM's own utility. Accordingly, we request the authority to delete this clause from the scope of the Enterprise Patch Management solution. In the alternative, we request that compliance be accepted where BIOS firmware and driver updates are deployed through the proposed solution's native software / package / script deployment module, invoking the hardware OEM's own update utility which delivers the same operational outcome from the same central console, using the hardware OEM's tested and supported update payloads.	Please be guided by RFP
	4	Section A - Enterprise Patch Management solution Sr. No. 4. The solution must support automated patch deployment for antivirus and security definition updates as a native task type.	Antivirus and endpoint security OEMs distribute engine updates and virus/threat definition signatures exclusively through their own authenticated, proprietary update infrastructure for example Broadcom/Symantec LiveUpdate, Trend Micro ActiveUpdate, Sophos Central, and the vendor-controlled cloud tenants of CrowdStrike and SentinelOne. These OEMs deliberately do not expose signed definition repositories for consumption by third-party patch management tools; this is a security control enforced on the antivirus OEM's side, since an externally mediated signature channel would itself become an attack path into the endpoint protection stack. It is therefore not a limitation of any particular patch management product. Operationally, definition updates are released several times a day and are designed to apply continuously and automatically. Routing them through a patch management scan–approve–schedule–deploy workflow would introduce hours of latency into signature currency and would degrade, not improve, the Bank's endpoint protection posture. We request the authority to accept compliance where (i) Microsoft Defender security intelligence and Windows security definition updates are deployed natively by the proposed solution, (ii) third-party antivirus engine and definition updates continue to be delivered by the antivirus OEM's own native update mechanism, and (iii) the proposed solution reports antivirus presence, version and definition currency as part of endpoint compliance and inventory. We further request confirmation that this clause will not be applied as a ground for technical disqualification.	Kindly refer corrigendum
	5	Section A - Enterprise Patch Management solution Sr. No. 19. The Endpoint Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network and it should continue to enforce, while the device is disconnected from the network.	Two issues arise on this clause. First, the clause is drafted in terms of "Endpoint Management software", whereas the Section is titled and scoped as an "Enterprise Patch Management solution". We request the authority to align the terminology, so that bidders are evaluated against the product category actually being procured. Second, the requirement that the solution "continue to enforce while the device is disconnected from the network" is not technically achievable by any patch management product, because patch enforcement requires the patch binary itself. Where an endpoint is disconnected, the agent can and does continue to evaluate the locally cached patch baseline, maintain the compliance state offline, apply patch content already staged locally, and report and remediate on reconnection; it cannot, however, install a patch that has not been downloaded. A clause worded as an absolute enforcement obligation while offline is therefore not capable of being complied with, or of being objectively evaluated, by any bidder. Suggested Clause: "The Patch Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network, applying locally cached patch content while offline and completing remediation and reporting automatically upon reconnection."	Please be guided by RFP
	6	Section A - Enterprise Patch Management solution Sr. No. 52. The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available.	A patch management platform identifies vulnerabilities deterministically, by correlating the installed software and version inventory of each endpoint against published vulnerability intelligence NIST NVD CVE records and OEM security advisories. A zero-day vulnerability is, by definition, one for which no advisory, no CVE record and no vendor patch exists at the time of exploitation. It is consequently not discoverable by inventory-to-advisory correlation, and can only be surfaced by behavioural and heuristic detection, exploit-technique analytics or threat-intelligence telemetry — which are the functions of Endpoint Detection and Response, Extended Detection and Response and Threat Intelligence platforms, and are separately procured and separately operated by the Bank's information security function. Because no patch management product can demonstrate this capability, the clause cannot be objectively evaluated and cannot be complied with truthfully by any bidder; it can only be answered affirmatively by a bidder offering a bundled EDR/XDR module, which is outside the scope of this Section. We request the authority to delete this clause from Section A. In the alternative, we request that it be limited to the following, which is measurable and which we fully support: identification of published CVEs affecting managed endpoints, including CVEs for which the vendor has not yet released a patch, together with the vendor-published workaround or mitigation guidance and the CVSS severity, so that the Bank has visibility of unpatched exposure pending vendor release.	Kindly refer corrigendum

	7	Section A - Enterprise Patch Management solution Sr. No. 53. The solution must scan managed endpoints for security misconfigurations and enable remediation from the console.	Security configuration assessment the evaluation of operating system and application settings against CIS Benchmarks, SCAP or DISA STIG baselines is the function of a Security Configuration Management or Vulnerability Assessment product, and is a distinct discipline from patch remediation. In a bank of NHB's profile these controls are ordinarily already delivered through Active Directory Group Policy hardening baselines, the endpoint protection / EDR platform, and a dedicated vulnerability assessment tool. We would respectfully draw the authority's attention to Sr. No. 55 of this very Section, which requires the proposed solution to provide documented public REST APIs for integration with vulnerability tools, expressly naming Tenable, Rapid7 and CrowdStrike. The RFP therefore already contemplates that vulnerability assessment and endpoint security tooling are separately owned and separately deployed at the Bank. Requiring the Patch Management solution to additionally duplicate that scanning capability adds licence and operational cost without adding any control, while restricting eligibility to the small number of UEM suites that bundle a configuration-assessment module. We request the authority to delete this clause. In the alternative, we request that compliance be accepted through the documented API integration already required under Sr. No. 55, whereby misconfiguration and vulnerability findings from the Bank's existing VA/EDR platform are ingested and the corresponding remediation is executed from the proposed solution's console.	Please be guided by RFP
	8	Section A - Enterprise Patch Management solution Sr. No. 54. The solution must support system quarantine policies isolating non-compliant or compromised endpoints from the network until remediation is confirmed.	Network quarantine and isolation are enforced at the network access control layer or at the host security layer by 802.1X / Network Access Control platforms such as Cisco ISE, Aruba ClearPass or Forescout, by EDR host-isolation, or by centrally managed host firewall policy. A patch management agent has no authority over switch port state, VLAN assignment, DHCP scope or session termination, and therefore cannot enforce quarantine; any product that claims this capability does so by bundling an EDR or host-firewall driver, which is a separate product category and a separate licence. We would also submit that in a regulated banking environment the automated disconnection of an endpoint from the network is a high-impact action with direct availability and business-continuity consequences, and is properly owned and authorised by the Bank's information security and network functions through its NAC/EDR controls, rather than triggered as a by-product of a patch compliance state. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the proposed solution continuously publishes endpoint patch-compliance posture through documented REST APIs and SIEM integration both already required under Sr. No. 55 and Sr. No. 94 enabling the Bank's existing NAC or EDR platform to enforce quarantine on that basis, which is the architecturally correct point of enforcement.	Kindly refere corrigendum
	9	Section A - Enterprise Patch Management solution Sr. No. 57. The proposed solution should ensure that files are scanned for infections during both read and write operations.	This clause is a description of real-time, on-access antivirus scanning implemented through a file-system filter driver. It is a core function of an Endpoint Protection Platform and has no relationship to patch identification, approval, distribution or remediation, which is the subject matter of this Section. NHB will, as a regulated entity, already have a licensed antivirus / EDR solution deployed across its endpoint estate. Introducing a second real-time on-access scanning engine on the same endpoints is not merely duplicative but is affirmatively undesirable: concurrent file-system filter drivers are a recognised cause of file-lock contention, I/O latency, application instability and mutual quarantine events, and antivirus OEMs expressly advise against running two real-time scanning engines on one host. Mandating this capability within a Patch Management tender would also restrict participation to OEMs offering a bundled antivirus engine. We request the authority to delete this clause from Section A, the capability being already provided by the Bank's existing endpoint protection solution.	Kindly refer corrigendum
	10	Section A - Enterprise Patch Management solution Sr. No. 58. The solution must support BitLocker encryption status monitoring, policy enforcement, and recovery key management for managed Windows endpoints.	BitLocker lifecycle management policy enforcement, recovery key escrow and key custody is a native Microsoft Windows capability, delivered without additional cost to an organisation already licensed for Windows Enterprise / Microsoft 365 through Active Directory Domain Services and Group Policy, and through Microsoft Intune or Microsoft Configuration Manager (which have succeeded MBAM as Microsoft's supported BitLocker administration route). It is an Encryption Management function, not a Patch Management function. Beyond the question of scope, we would submit that requiring BitLocker recovery keys to be escrowed inside a third-party operational management tool is a material expansion of the Bank's key-custody risk surface. The recovery key is the single credential that defeats full-disk encryption on every managed endpoint. Placing a second, non-Microsoft copy of that key store inside a patch management database creates an additional custodian, an additional access control boundary, an additional backup and retention obligation, and an additional audit scope under the Bank's cryptographic key management controls without any corresponding security benefit, since Active Directory already holds the authoritative escrow. We request the authority to delete Sr. No. 58 from Section A, the capability being natively available to the Bank through Active Directory / Group Policy and Microsoft Intune. In the alternative, we request that compliance be limited to read-only reporting of BitLocker encryption status as part of endpoint inventory and compliance reporting, with policy enforcement and recovery key custody remaining with Microsoft's native tooling.	This is required functionality. Please be guided by RFP.
	11	Section A - Enterprise Patch Management solution Sr. No. 59. Support periodic rotation of bitlocker keys.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds, namely that BitLocker key lifecycle management is an Encryption Management function outside the scope of an Enterprise Patch Management solution. We would add that periodic rotation of BitLocker recovery keys is itself a native Windows capability, available through the manage-bde command set and through Microsoft Intune's recovery key rotation policy, and can be invoked centrally by the Bank at no additional licence cost. A third-party rotation mechanism operating on the same keys introduces the risk of divergence between the key held in Active Directory and the key held by the third-party tool, which is precisely the failure mode that renders an encrypted endpoint unrecoverable. We request the authority to delete this clause from Section A.	Kindly refer corrigendum
	12	Section A - Enterprise Patch Management solution Sr. No. 60. The solution should support TPM and Non-TPM devices for Bitlocker encryption.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. We would further submit that whether BitLocker may be enabled on a device without a compatible TPM is determined entirely by a Windows operating system policy setting the Group Policy option "Require additional authentication at startup / Allow BitLocker without a compatible TPM" and by the corresponding startup authentication method (password or startup key). It is a Windows configuration state, not a differentiating capability of any management product, and no third-party tool can enable BitLocker on a non-TPM device except by setting that same Windows policy. We request the authority to delete this clause from Section A.	Kindly refer corrigendum
	13	Section A - Enterprise Patch Management solution Sr. No. 61. Restrict technician roles for BitLocker and recovery key access, enhancing security controls in enterprise environments.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. It presupposes that the Bank's BitLocker recovery keys are held within the proposed Patch Management solution, and requires role-based access control over that key store. If, as requested at Sr. No. 58, recovery key custody remains with Active Directory and Microsoft Intune, the corresponding access restriction is enforced by Active Directory delegation and Intune role-based access control, which are the Bank's authoritative and auditable controls for this purpose. We request the authority to delete this clause from Section A. We confirm that the proposed solution provides granular role-based access control and full audit logging over all administrative functions and data within its own scope.	Please be guided by RFP
	14	Section A - Enterprise Patch Management solution Sr. No. 75. The solution must support zero-touch OS deployment enabling new endpoints to be automatically imaged without administrator physical intervention, using PXE boot or equivalent mechanism.	We note that Sr. No. 73 and Sr. No. 74 of this Section already require OS image creation, capture, template-based customisation and deployment from the management console, and we are compliant with those requirements. Sr. No. 75 goes further and mandates zero-touch, PXE-boot-based bare-metal provisioning without any administrator intervention. We request reconsideration of this additional requirement for the following reasons: (i) PXE-based provisioning is an OS Deployment function delivered by Microsoft Deployment Toolkit, Windows Deployment Services, Microsoft Configuration Manager or Windows Autopilot, or by the hardware OEM's factory provisioning service. It is a build-and-provisioning discipline distinct from patch and vulnerability remediation. (ii) It is a one-time-per-device activity performed at the point of hardware induction or refresh, ordinarily by the Bank's desktop build team, and does not recur through the endpoint's operational life unlike patching, which is continuous. (iii) It requires enabling PXE/TFTP boot services and DHCP option changes (Options 66/67 or IP helper configuration) across the Bank's network segments. Unauthenticated network boot is a control the Bank's network security policy would normally restrict, and enabling it bank-wide is a network and security change well outside the scope of a patch management engagement. (iv) Mandating it as a native requirement narrows the eligible field to full Unified Endpoint Management suites. We request the authority to delete Sr. No. 75, or to reclassify it as a desirable, non-scored requirement, retaining Sr. No. 73 and Sr. No. 74 as the mandatory OS deployment specifications.	Kindly refer corrigendum

	15	Section A - Enterprise Patch Management solution Sr. No. 76. The solution must support user profile migration as part of OS deployment, preserving user data, desktop settings, and application preferences during OS refresh or upgrade cycles.	User state migration is delivered by Microsoft's User State Migration Tool, which is supplied free of charge as part of the Windows Assessment and Deployment Kit, and in most enterprises is rendered largely unnecessary by OneDrive Known Folder Move, roaming user profiles or FSLogix profile containers, all of which are Microsoft entitlements the Bank is likely already to hold. Like PXE provisioning, profile migration is an episodic activity tied to hardware refresh and OS upgrade cycles, and is not part of the continuous patch and vulnerability remediation lifecycle that this Section is procuring. Its inclusion as a mandatory technical specification excludes otherwise fully capable Enterprise Patch Management platforms on a ground unconnected with the Bank's security objective. We request the authority to delete this clause from Section A, or in the alternative to reclassify it as a desirable, non-scored requirement.	Kindly refer corrigendum
	16	Section A - Enterprise Patch Management solution Sr. No. 86. The solution must support centralised printer management deploying and configuring network and local printers to Windows endpoints.	Centralised printer deployment and configuration on domain-joined Windows endpoints is a native Active Directory capability, delivered through the "Deployed Printers" Group Policy extension and Group Policy Preferences, and through Microsoft Universal Print for cloud-managed estates. It is available to the Bank at no incremental cost and is the standard, Microsoft-supported method in an Active Directory environment. It is a desktop administration and end-user configuration task that has no bearing on patch currency, vulnerability exposure or endpoint compliance, which are the objectives of this Section. Mandating it as a native Patch Management specification restricts participation to bundled Unified Endpoint Management suites without any corresponding benefit to the Bank. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where printer deployment and configuration are delivered through the proposed solution's native script and package deployment module, which achieves the identical outcome from the same central console.	Please be guided by RFP
	17	Section A - Enterprise Patch Management solution Sr. No. 87. The solution must support network drive mapping mapping network shares to specific drive letters on Windows endpoints.	This clause is submitted on the same grounds as our query on Sr. No. 86. Mapping network shares to drive letters is a native Active Directory function performed through Group Policy Preferences Drive Maps, or through logon scripts, in every domain environment. It is user-context desktop configuration, is dependent on the user's group membership and share permissions rather than on the endpoint's patch state, and bears no relationship to patch or vulnerability management. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where drive mapping is delivered through the proposed solution's native script deployment module.	Please be guided by RFP
	18	Section A - Enterprise Patch Management solution Sr. No. 88. The management agent must support rebranding to display under the organisation's name and branding.	White-labelling of an OEM's management agent is a cosmetic presentation feature offered by a limited number of OEMs. It delivers no security, operational, compliance or performance benefit to the Bank, and it does not relate in any way to the functional objective of patch and vulnerability remediation. Its inclusion as a mandatory technical specification is therefore restrictive of competition without a corresponding procurement rationale, and does not meet the test in Rule 144(i) of GFR 2017 that specifications be objective and functional. We would further submit that agent rebranding is affirmatively undesirable in a banking environment from a security operations standpoint. Concealing the true vendor identity of a privileged agent binary that runs with SYSTEM rights complicates antivirus and EDR allow-listing, weakens the Bank's ability to attribute a running process to a known vendor during incident triage and forensic review, and obscures the software inventory and SBOM record that the Bank is expected to maintain. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the end-user-facing elements of the agent self-service portal, end-user notifications and remote-session consent prompts can be branded with the Bank's name and logo, while the underlying signed agent binary and service retain the OEM's verifiable identity.	Kindly refer corrigendum
	19	Section A - Enterprise Patch Management solution Sr. No. 89. The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.	We request the authority to confirm that compliance with this clause is satisfied where the proposed solution centrally creates, modifies and deletes Windows registry keys and values on targeted endpoints and endpoint groups through its native script / configuration deployment module, executed from the central console with scheduling, targeting, execution status and audit logging as distinct from requiring a separately named "registry management" module in the product's user interface. We confirm that we provide central set/reset of registry values on targeted Windows machines and seek this confirmation solely to ensure that all bidders are evaluated on the functional outcome rather than on the naming of a product module.	Registry value modification is required for various configurations. Please be guided by RFP
	20	Section A - Enterprise Patch Management solution Sr. No. 90. The solution must include a built-in credential manager for administrative credentials used in remote operations.	We seek the Bank's clarification on the intended architecture for this requirement, since the clause as drafted may sit in tension with the Bank's privileged access management controls. Under the RBI Cyber Security Framework and prevailing BFSI practice, privileged administrative credentials are expected to be vaulted, rotated and brokered centrally through a dedicated Privileged Access Management solution such as CyberArk, ARCON or BeyondTrust with check-out approval and session recording, precisely so that privileged secrets are not replicated into each operational management console. A requirement that a patch management tool maintain its own independent store of domain administrative credentials creates an additional privileged secret repository, an additional custodian and an additional audit scope. We accordingly request the authority to confirm: (i) whether NHB has an existing PAM platform with which the proposed solution is expected to integrate for credential brokering, and if so which platform and by what interface; (ii) that compliance will be accepted where administrative credentials are held in the solution's own encrypted credential store with role-based access control, audit logging and no plain-text retrieval, and/or are brokered from the Bank's PAM or Active Directory rather than stored in the tool; and (iii) whether the Bank requires credential rotation to be performed by the proposed solution or by its PAM platform.	This functionality is required for executing custom scripts without manually mention credentials in script. It is also required for remote troubleshooting, agent deployment etc. Please be guided by RFP
	21	Section A - Enterprise Patch Management solution Sr. No. 91. The solution must support Wi-Fi profile deployment to Windows endpoints.	Wireless profile provisioning on Windows endpoints is a native Active Directory capability, delivered through the "Wireless Network (IEEE 802.11) Policies" Group Policy extension, and through Microsoft Intune for mobile and cloud-managed estates. It is available to the Bank at no incremental cost. In a bank, enterprise wireless profiles carry 802.1X / EAP configuration and, commonly, machine or user certificates issued by the Bank's PKI. Their provisioning is therefore properly owned and controlled by the network and information security functions through the Bank's NAC and certificate infrastructure, and not distributed as a payload by a patch management tool. The requirement bears no relationship to patch currency or vulnerability remediation. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where Wi-Fi profiles are deployed through the proposed solution's native script or package deployment module.	Please be guided by RFP
	22	Section A - Enterprise Patch Management solution Sr. No. 98. Solution is subject to regular penetration testing / vulnerability assessment exercise. Any vulnerability found in the solution will be patched by vendor as per defined timelines by NHB.	We accept in principle that the proposed solution will be subject to the Bank's periodic VAPT exercises and that the OEM will remediate vulnerabilities identified in its product. We seek the following clarifications and amendments, as the clause is presently not capable of being priced or accepted at bid stage: (i) Remediation timelines: the clause requires remediation "as per defined timelines by NHB", but no timelines are defined anywhere in the RFP. A product OEM operates a single, published, severity-based vulnerability remediation SLA applied uniformly across its global installed base, and cannot undertake customer-specific remediation timelines that are undefined at bid stage and to be fixed unilaterally after award. We request the authority to publish the intended remediation timelines by CVSS severity band (Critical / High / Medium / Low) in the RFP itself, so that bidders can evaluate, price and accept them. (ii) Scope of the OEM's remediation obligation: we request the authority to confirm that the obligation extends only to vulnerabilities in the OEM's own product-delivered code, packages, libraries and components, and expressly excludes the underlying operating system, database, web server, middleware and other customer-provisioned infrastructure on which the solution is installed, together with the hardware, hypervisor, network and endpoint estate. Patching, hardening and vulnerability remediation of the operating system and database layer remain the responsibility of the Bank or its system integrator, in accordance with standard software licensing practice. (iii) Third-party and OS-inherited findings: where a VAPT finding arises from a third-party or open-source component, the OEM's obligation should be to incorporate the upstream fix within its published SLA once that fix is released by the upstream maintainer, and to provide a documented mitigation or compensating control in the interim. (iv) Conduct of the exercise: we request confirmation that VAPT will be performed on the Bank's own instance in a non-production environment, under a mutual non-disclosure agreement, with findings and evidence shared with the OEM to enable validation and remediation, and that reverse engineering, decompilation and public disclosure of findings are excluded. (v) We request that the clause be amended to record that remediation is "as per the OEM's published vulnerability remediation SLA, or such timelines as are specified in the RFP", in place of timelines to be defined after award.	Kindly Refer Section 12.17 of RFP for timelines of closure of observations. Bidder has to to comply with observations pertaining to all supplied software components.

	23	Section C - Unified Enterprise Management Solution Sr. No. 7. The solution should support bi-directional CMDB sync along with auto-ticketing between the monitoring tool and ManageEngine ServiceDesk Plus.	The clause names a specific third-party OEM product as the mandatory integration target. As drafted, it is capable of being read as requiring a pre-built, product-specific connector to ManageEngine ServiceDesk Plus, which in practice is offered natively by that OEM's own monitoring products with the effect of favouring a single OEM's stack, contrary to the requirement in Rule 144(i) of GFR 2017 that specifications not indicate a requirement for a particular trade mark or trade name. Bi-directional CMDB synchronisation and automated ticket creation, update and closure are standard interoperability functions that any modern monitoring platform delivers through documented REST APIs and webhooks. We therefore request the authority to confirm: (i) that compliance will be accepted where bi-directional CMDB synchronisation and auto-ticketing are implemented through documented REST APIs and webhooks, and a pre-built ManageEngine-specific connector is not insisted upon; (ii) the edition, version and deployment model of the ManageEngine ServiceDesk Plus on-premise instance, and whether its REST API, CMDB / CI APIs and CI relationship APIs are licensed and enabled in that edition; (iii) the CI classes, attributes and relationship types to be synchronised, the direction of authority for each (which system is the master for each attribute), and the expected synchronisation frequency and volume; (iv) that the Bank will provide API access, authentication tokens, a test instance and the necessary support from its incumbent ManageEngine partner during integration and testing; and (v) that any configuration, licensing, customisation or professional-services effort required on the ManageEngine ServiceDesk Plus side sits with the Bank or its incumbent ITSM partner and is outside the bidder's scope and price. This information is necessary for all bidders to estimate integration effort accurately and to quote on a comparable basis.	Integration will be scope of bidder only. Bank will provide access of API of Service Desk Plus.
	24	Section C - Unified Enterprise Management Solution Sr. No. 33. The proposed solution should provide Network Detection and Response (NDR) capabilities to continuously monitor network traffic, detect anomalous or malicious activities, and enable rapid investigation and response to security incidents.	Network Detection and Response is a distinct security product category represented by platforms such as Darktrace, ExtraHop Reveal(x), Vectra AI and Cisco Secure Network Analytics and is not a function of an enterprise monitoring or observability platform. The two differ in three material respects: (i) Data plane: NDR requires full packet capture and deep packet inspection fed by SPAN, mirror or network TAP infrastructure, together with the associated capture appliances and storage. An enterprise management solution consumes flow telemetry (NetFlow, sFlow, J-Flow, IPFIX) and SNMP, which is metadata about conversations and is sufficient for performance, capacity and utilisation analytics but not for payload-level threat detection. (ii) Detection engine: NDR detection is built on attack-behaviour models, command-and-control and lateral-movement analytics and curated threat intelligence, maintained by a security research organisation. Monitoring platforms baseline performance behaviour, which is a different analytic objective. (iii) Response: the "Response" element of NDR requires enforcement authority over firewalls, NAC and EDR to block, isolate or terminate sessions. An enterprise monitoring platform neither holds nor should hold that authority, which in the Bank's architecture properly sits with its SOC, SIEM/SOAR and network security controls. Including NDR within the scope of a Unified Enterprise Management Solution therefore both mismatches the product category and materially narrows the eligible bidder set to the small number of OEMs that market a bundled NDR module, with a consequent effect on price discovery. We request the authority to delete this clause from Section C, the capability being properly procured and operated as part of the Bank's security stack. In the alternative, we request that compliance be accepted on the basis of flow-based traffic baselining and anomaly detection with alert forwarding to the Bank's SIEM/SOC for investigation and response — which is already required at Sr. No. 63 of this Section and which we fully support.	Kindly refer corrigendum
	25	Section C - Unified Enterprise Management Solution Sr. No. 75. The proposed solution should provide monitoring for SAP systems, including performance metrics, system health, and key operational parameters.	SAP environments are instrumented through interfaces controlled by SAP itself principally SAP Solution Manager and SAP Focused Run, and at the technical layer the CCMS / SAPControl web service, the /SDF/MON monitoring infrastructure and, on the Java stack, JMX. SAP does not permit byte-code instrumentation of the ABAP stack by third-party APM agents, and the installation of third-party agents on SAP application servers is governed by SAP's own support and certification policy, which can affect the customer's SAP support entitlement where unapproved agents are deployed. The extent to which any third-party solution can monitor SAP is therefore determined by the access the Bank's SAP landscape and SAP support agreement permit, and not by the capability of the monitoring product. To enable accurate and comparable responses from all bidders, we request the authority to confirm: (i) the SAP landscape in scope the products, the stack (ABAP, Java, HANA, S/4HANA) and the number of systems and instances; (ii) whether the Bank will enable and grant access to the SAPControl web service, CCMS and/or JMX interfaces, and provide a dedicated read-only monitoring service user with the necessary authorisations; (iii) whether the installation of a third-party monitoring or APM agent on SAP application servers is permitted under the Bank's SAP support and licensing agreement; and (iv) that where such access or agent installation is not permitted, compliance will be accepted on the basis of infrastructure-level monitoring of the SAP hosts operating system, database, availability, port and service response and resource utilisation or, failing that, that the clause be withdrawn from the mandatory specifications.	We are using SAP ECC 6 EHP 7 with SQL Server database. We are using two instances CI & DI.
	26	Section A - Enterprise Patch Management solution Sr. No. 32. The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status. [Read with Sr. No. 73: "...OS imaging and deployment of Windows operating systems from the cloud-connected management console..."]	Sr. No. 32 requires the compliance dashboard to be a "cloud dashboard", and Sr. No. 73 refers to a "cloud-connected management console". We seek clarification, as this wording appears inconsistent with the deployment posture that a regulated financial institution would ordinarily require, and with the balance of this Section which contemplates on-premise distribution points, air-gapped and closed-network patching (Sr. No. 6) and local content distribution. For a Housing Finance regulator and refinance institution, endpoint inventory, patch state and vulnerability posture constitute sensitive operational security data, and its residence in a vendor-operated cloud tenant raises data localisation, data residency and third-party risk considerations under the RBI framework, together with the corresponding outsourcing governance obligations. Mandating a cloud-hosted console also has the effect of excluding on-premise deployment models, which is restrictive without an evident functional rationale, since the substance of the requirement real-time compliance status, endpoint health classification and drill-down to device level is delivered identically by an on-premise centralised console. We request the authority to confirm whether the solution is to be deployed on-premise within the Bank's data centre, and accordingly to substitute the words "centralised cloud dashboard" at Sr. No. 32 with "centralised management dashboard", and "cloud-connected management console" at Sr. No. 73 with "centralised management console", retaining all functional requirements of both clauses unchanged. We confirm full compliance with the functional substance of both clauses.	Kindly refer corrigendum
	27	Section C - Unified Enterprise Management Solution Sr. No. 66. ....must keep historical rate and Ip to Ip, Ip to protocol, protocol to protocol conversation data for a minimum of 3 months... maximum 15 minute window granularity. Sr. No. 67. Future Scalability – the system should be capable of supporting at least 15 thousand network flow per second on single server...	These clauses prescribe flow retention, granularity and throughput figures without stating the underlying environment parameters against which they are to be sized. Flow collector sizing, storage volume and licence quantum are a direct function of the sustained and peak flow rate, the number of exporters and monitored interfaces, and the retention and granularity policy applied at each tier. To enable all bidders to size the solution correctly and to quote on a uniform basis, we request the authority to confirm: (i) the number of flow-exporting devices and the total number of monitored interfaces from which flow is to be collected; (ii) the expected sustained and peak flows per second at the aggregate level, and whether the 15,000 flows per second at Sr. No. 67 is the sustained figure, the peak figure or a headroom requirement; (iii) whether the three-month retention at Sr. No. 66 is required at raw conversation granularity throughout, or whether rolled-up 15-minute aggregation is acceptable for the full three-month window raw and aggregated retention differ by an order of magnitude in storage; (iv) whether the storage required for the flow retention tier is to be provided by the Bank or is to be included in the bidder's scope, and if the latter, the storage type and protection level to be assumed; and (v) whether the "single server" requirement at Sr. No. 67 refers to a single flow collector node, and the server specification the Bank expects that figure to be achieved on. Absent these parameters, bids will not be comparable on a like-for-like basis.	Please be guided by RFP. Details of network devices already provided in RFP.
	28	Section C - Unified Enterprise Management Solution Sr. No. 61. The proposal solution should support AI/ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspicious behaviour in network traffic, device performance and application metrics. Alerts are triggered for deviations so Network team can respond to issues early.	We request the authority to confirm the intended scope of this clause, specifically that it is directed at operational anomaly detection for performance and availability management, and not at security threat detection, which is the subject of the Bank's SIEM and security stack and which we have separately queried at Sr. No. 33. We further request confirmation that compliance will be accepted where the solution provides machine-learning-based dynamic and adaptive thresholding on performance metrics, automatic baselining of normal behaviour with deviation alerting, forecasting and predictive analytics on capacity metrics, and baseline flow policies for detection of anomalous traffic behaviour as already required at Sr. No. 23, Sr. No. 24, Sr. No. 38, Sr. No. 39 and Sr. No. 63 of this Section without requiring a separately licensed security analytics or user-and-entity-behaviour-analytics engine. The word "suspicious" in the present drafting introduces a security connotation that overlaps with the NDR requirement at Sr. No. 33 and would, if read as a threat-detection requirement, restrict participation to OEMs bundling a security analytics module.	Kindly refer corrigendum

	29	Section B - Active Directory Management and Auditing Sr. No. 2 - The solution should have a unified console where all the key features of the solution as per the specifications are available in the form of a centralized dashboard for ease of access and monitoring.	No, Different consols as per module , request to delet clause	Kindly refer corrigendum
	30	Section B - Active Directory Management and Auditing Sr. No. 3 - The access to the GUI console(s) should have proper authentication and authorization mechanisms including Multi-Factor Authentication, Role Based Access Control (RBAC) etc. This should be applicable for the centralized/unified solution dashboard as well as any GUI consoles that are part of the supplied solution	Pls. delet clause as RBAC , MFA and other mechanism is thru individual module's console.	Kindly refer corrigendum
	31	Section B - Active Directory Management and Auditing Sr. No. 6 - Solution should have the feature to Audit Windows File servers, who, when, from where access the files.	Recommended to audit AD , Logon activity , AD Query & win file server. Request to add.	Please be guided by RFP
	32	Section B - Active Directory Management and Auditing Sr. No. 50 - The solution should provide comprehensive reporting, storage and retrieval of Active Directory logs from all domain controllers..	Solution should have Agent-based to (1) eliminate need native event logs, (2) allow for object protection, (3) optimized/configurable data transfer, and (4) real-time alerts , due to agent it can capture real time event at schema level not on log generation level . request to incorporate.	Please be guided by RFP

Bidder 4

	S.No.	Relevant Clause of the RFP	Query	Bank Reply
	1	**250000** **ATC Pg no. 21 Clasue NO. 9.12** All the Bids must be accompanied by a refundable interest free security deposit of Rs.2,00,000/- (Rs. Two Lakhs only), by way of an e-payment in favour of National using Bank.	We request the Bank to kindly clarify the EMD amount, as there is a discrepancy between the tender documents: GeM Document: EMD amount mentioned as ₹2,50,000 ATC, Page 21, Clause 9.12: EMD amount mentioned as ₹2,00,000 Kindly confirm the applicable EMD amount to be considered for bid submission. Additionally, we request the Bank to kindly specify the validity period of the EMD.	Kindly refer corrigendum
	2	After sign-off/go-live. Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. 80% of Total Solution Cost (as per commercial bid format) will be released.	**We request the Bank to kindly amend the payment terms for the Total Solution Cost from 80% upon Sign-off/Go-Live to 80% upon Delivery.** **Justification:** The proposed solution involves significant upfront costs towards procurement, logistics, deployment readiness, and associated resources. Therefore, releasing 80% of the Solution Cost upon delivery will help align the payment milestone with the vendor's upfront financial commitments and ensure smooth and timely implementation of the solution.	Please be guided by RFP.
	3	At the end of every subsequent year (2nd year onwards) 10% of Total Solution Cost	**We request the Bank to kindly amend the payment terms for the 2nd and 3rd years from 10% of the Total Solution Cost at the end of each respective year to the following:** 10% of the Total Solution Cost – At the time of Sign-off Remaining 10% of Total Solution Cost – Against submission of PBG Justification: The proposed payment structure will help align the payment milestones with the completion and sign-off of the solution, while the PBG provides adequate security to the Bank for the remaining payment obligation.	Please be guided by RFP.
	4	General – Section A: Enterprise Patch Management Solution (Overall scope of Section A)	Section A of the RFP is titled "Enterprise Patch Management solution"; however, a significant number of specifications listed under this Section describe capabilities that belong to distinct and separately licensed product categories, and not to Patch Management: (a) Unified Endpoint Management / Client Management BIOS firmware and hardware driver patching (Sr. 3), zero-touch PXE OS provisioning and user profile migration (Sr. 75, 76), centralised printer management (Sr. 86), network drive mapping (Sr. 87), agent rebranding (Sr. 88) and Wi-Fi profile deployment (Sr. 91); (b) Endpoint Protection Platform / EDR – on-access antivirus scanning during read and write operations (Sr. 57) and network quarantine / isolation of endpoints (Sr. 54); (c) Encryption Management – BitLocker policy enforcement, recovery key escrow, key rotation and technician role restriction (Sr. 58 to 61); (d) Vulnerability Assessment / Security Configuration Management – zero-day identification (Sr. 52) and endpoint security misconfiguration scanning (Sr. 53). The simultaneous mandating of all four categories as native, single-console capabilities under a Patch Management tender is met natively by only one or two global OEM suites. The effect, whether or not intended, is that specialised and fully capable Enterprise Patch Management OEMs including OEMs that comply with the entirety of the core patch, software distribution, asset discovery, remote control and reporting requirements of this Section stand excluded at the technical evaluation stage on account of adjacent-category features that do not contribute to the Bank's patch and vulnerability remediation objective. Rule 144(i) of the General Financial Rules, 2017 requires that the subject matter of procurement be described in terms that are "objective, functional, generic and measurable" and that the description shall not indicate a requirement for a particular trade mark, trade name or brand. Rule 173(ix) further requires that specifications be broad-based to the extent feasible in order to attract a sufficient number of bidders. The Central Vigilance Commission's standing guidance on framing of tender specifications is to the same effect. We therefore request the authority, in the interest of fair and wider participation and of value for the Bank, to either (i) delete the specifications identified at (a) to (d) above from Section A, or (ii) reclassify them as "desirable / non-mandatory" specifications that are not scored and are not treated as grounds for technical disqualification. Clause-wise queries with the specific technical basis for each are submitted separately below.	Kindly refer corrigendum

	5	Section A - Enterprise Patch Management solution Sr. No. 2. Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	The clause prescribes an absolute catalogue threshold of "1000+ third party software" without publishing the list of applications actually deployed in the Bank's environment. A raw catalogue count is not an objective or measurable indicator of fitment for the following reasons: (i) Counting methodology is not standardised across OEMs some OEMs count each application once, others count every version, edition, language pack and 32-bit/64-bit architecture as a separate title, so that the same real-world coverage can be published as 400 or as 5,000 depending on the method of counting. (ii) A large catalogue number does not assure coverage of the specific OS, database, middleware and desktop applications in use at NHB, which is the only coverage that has value to the Bank. (iii) The figure as worded corresponds to the published catalogue claim of a single OEM, and therefore operates as a brand-linked qualifier rather than a functional requirement, contrary to Rule 144(i) of GFR 2017. We request the authority to publish, in the corrigendum, the list of business-critical operating systems, databases, middleware and third-party desktop applications deployed at NHB that are required to be patched, and to evaluate compliance on the basis of demonstrated coverage of that list, supported by the OEM's published patch catalogue and the ability to on-board any uncovered application through custom package/script deployment. We confirm our ability to patch the operating systems, databases and middleware expressly named in this clause.	Kindly refer corrigendum
	6	Section A - Enterprise Patch Management solution Sr. No. 3. The solution must support BIOS firmware and hardware driver patching from the central console as a native capability without requiring a separate driver management tool.	BIOS/UEFI firmware and hardware driver updates are not published through the vendor-neutral patch distribution channels that patch management platforms consume (Microsoft Update Catalogue / WSUS, and application vendors' public update repositories). They are released exclusively by the hardware OEM, in hardware-OEM-specific formats, and are distributed through that OEM's own client management utility for example Dell Command | Update and Dell Client Catalog, HP Image Assistant, Lenovo System Update / Thin Installer, and Intel Driver & Support Assistant. Any tool that offers "native" BIOS and driver patching does so through a proprietary, per-OEM integration built into a Unified Endpoint Management suite; it is therefore a UEM capability and not a Patch Management capability, and its availability is itself limited to the specific hardware makes for which that integration exists. We would also submit, for the Bank's consideration, that unattended fleet-wide automation of BIOS/firmware flashing is not regarded as good practice in a regulated banking environment: firmware updates are model-specific, are not reversible in the manner of an OS patch, carry a risk of rendering an endpoint unbootable if interrupted, and are ordinarily executed as change-controlled, model-wise campaigns by the hardware OEM's own utility. Accordingly, we request the authority to delete this clause from the scope of the Enterprise Patch Management solution. In the alternative, we request that compliance be accepted where BIOS firmware and driver updates are deployed through the proposed solution's native software / package / script deployment module, invoking the hardware OEM's own update utility which delivers the same operational outcome from the same	Please be guided by RFP
	7	Section A - Enterprise Patch Management solution Sr. No. 4. The solution must support automated patch deployment for antivirus and security definition updates as a native task type.	Antivirus and endpoint security OEMs distribute engine updates and virus/threat definition signatures exclusively through their own authenticated, proprietary update infrastructure for example Broadcom/Symantec LiveUpdate, Trend Micro ActiveUpdate, Sophos Central, and the vendor-controlled cloud tenants of CrowdStrike and SentinelOne. These OEMs deliberately do not expose signed definition repositories for consumption by third-party patch management tools; this is a security control enforced on the antivirus OEM's side, since an externally mediated signature channel would itself become an attack path into the endpoint protection stack. It is therefore not a limitation of any particular patch management product. Operationally, definition updates are released several times a day and are designed to apply continuously and automatically. Routing them through a patch management scan–approve–schedule–deploy workflow would introduce hours of latency into signature currency and would degrade, not improve, the Bank's endpoint protection posture. We request the authority to accept compliance where (i) Microsoft Defender security intelligence and Windows security definition updates are deployed natively by the proposed solution, (ii) third-party antivirus engine and definition updates continue to be delivered by the antivirus OEM's own native update mechanism, and (iii) the proposed solution reports antivirus presence, version and definition currency as part of endpoint	Kindly refer corrigendum
	8	Section A - Enterprise Patch Management solution Sr. No. 19. The Endpoint Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network and it should continue to enforce, while the device is disconnected from the network.	Two issues arise on this clause. First, the clause is drafted in terms of "Endpoint Management software", whereas the Section is titled and scoped as an "Enterprise Patch Management solution". We request the authority to align the terminology, so that bidders are evaluated against the product category actually being procured. Second, the requirement that the solution "continue to enforce while the device is disconnected from the network" is not technically achievable by any patch management product, because patch enforcement requires the patch binary itself. Where an endpoint is disconnected, the agent can and does continue to evaluate the locally cached patch baseline, maintain the compliance state offline, apply patch content already staged locally, and report and remediate on reconnection; it cannot, however, install a patch that has not been downloaded. A clause worded as an absolute enforcement obligation while offline is therefore not capable of being complied with, or of being objectively evaluated, by any bidder. Suggested Clause: "The Patch Management software must be able to continuously assess and remediate Patch compliance while devices are connected or disconnected from the network, applying locally cached patch	Please be guided by RFP
	9	Section A - Enterprise Patch Management solution Sr. No. 52. The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available.	A patch management platform identifies vulnerabilities deterministically, by correlating the installed software and version inventory of each endpoint against published vulnerability intelligence NIST NVD CVE records and OEM security advisories. A zero-day vulnerability is, by definition, one for which no advisory, no CVE record and no vendor patch exists at the time of exploitation. It is consequently not discoverable by inventory-to-advisory correlation, and can only be surfaced by behavioural and heuristic detection, exploit-technique analytics or threat-intelligence telemetry — which are the functions of Endpoint Detection and Response, Extended Detection and Response and Threat Intelligence platforms, and are separately procured and separately operated by the Bank's information security function. Because no patch management product can demonstrate this capability, the clause cannot be objectively evaluated and cannot be complied with truthfully by any bidder; it can only be answered affirmatively by a bidder offering a bundled EDR/XDR module, which is outside the scope of this Section. We request the authority to delete this clause from Section A. In the alternative, we request that it be limited to the following, which is measurable and which we fully support: identification of published CVEs affecting managed endpoints, including CVEs for which the vendor has not yet released a patch, together with the vendor-published workaround or mitigation guidance and the CVSS severity, so that the Bank has visibility of unpatched exposure pending vendor release.	Kindly refer corrigendum
	10	Section A - Enterprise Patch Management solution Sr. No. 53. The solution must scan managed endpoints for security misconfigurations and enable remediation from the console.	Security configuration assessment the evaluation of operating system and application settings against CIS Benchmarks, SCAP or DISA STIG baselines is the function of a Security Configuration Management or Vulnerability Assessment product, and is a distinct discipline from patch remediation. In a bank of NHB's profile these controls are ordinarily already delivered through Active Directory Group Policy hardening baselines, the endpoint protection / EDR platform, and a dedicated vulnerability assessment tool. We would respectfully draw the authority's attention to Sr. No. 55 of this very Section, which requires the proposed solution to provide documented public REST APIs for integration with vulnerability tools, expressly naming Tenable, Rapid7 and CrowdStrike. The RFP therefore already contemplates that vulnerability assessment and endpoint security tooling are separately owned and separately deployed at the Bank. Requiring the Patch Management solution to additionally duplicate that scanning capability adds licence and operational cost without adding any control, while restricting eligibility to the small number of UEM suites that bundle a configuration-assessment module. We request the authority to delete this clause. In the alternative, we request that compliance be accepted through the documented API integration already required under Sr. No. 55, whereby misconfiguration and	Please be guided by RFP

	11	Section A - Enterprise Patch Management solution Sr. No. 54. The solution must support system quarantine policies isolating non-compliant or compromised endpoints from the network until remediation is confirmed.	Network quarantine and isolation are enforced at the network access control layer or at the host security layer by 802.1X / Network Access Control platforms such as Cisco ISE, Aruba ClearPass or Forescout, by EDR host-isolation, or by centrally managed host firewall policy. A patch management agent has no authority over switch port state, VLAN assignment, DHCP scope or session termination, and therefore cannot enforce quarantine; any product that claims this capability does so by bundling an EDR or host-firewall driver, which is a separate product category and a separate licence. We would also submit that in a regulated banking environment the automated disconnection of an endpoint from the network is a high-impact action with direct availability and business-continuity consequences, and is properly owned and authorised by the Bank's information security and network functions through its NAC/EDR controls, rather than triggered as a by-product of a patch compliance state. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the proposed solution continuously publishes endpoint patch-compliance posture through documented REST APIs and SIEM integration both already required under Sr. No. 55 and Sr. No. 94 enabling the Bank's existing NAC or EDR platform to enforce quarantine on that basis, which is the architecturally correct point of enforcement.	Kindly refere corrigendum
	12	Section A - Enterprise Patch Management solution Sr. No. 57. The proposed solution should ensure that files are scanned for infections during both read and write operations.	This clause is a description of real-time, on-access antivirus scanning implemented through a file-system filter driver. It is a core function of an Endpoint Protection Platform and has no relationship to patch identification, approval, distribution or remediation, which is the subject matter of this Section. NHB will, as a regulated entity, already have a licensed antivirus / EDR solution deployed across its endpoint estate. Introducing a second real-time on-access scanning engine on the same endpoints is not merely duplicative but is affirmatively undesirable: concurrent file-system filter drivers are a recognised cause of file-lock contention, I/O latency, application instability and mutual quarantine events, and antivirus OEMs expressly advise against running two real-time scanning engines on one host. Mandating this capability within a Patch Management tender would also restrict participation to OEMs offering a bundled antivirus engine. We request the authority to delete this clause from Section A, the capability being already provided by the Bank's existing endpoint protection solution.	Kindly refer corrigendum
	13	Section A - Enterprise Patch Management solution Sr. No. 58. The solution must support BitLocker encryption status monitoring, policy enforcement, and recovery key management for managed Windows endpoints.	BitLocker lifecycle management policy enforcement, recovery key escrow and key custody is a native Microsoft Windows capability, delivered without additional cost to an organisation already licensed for Windows Enterprise / Microsoft 365 through Active Directory Domain Services and Group Policy, and through Microsoft Intune or Microsoft Configuration Manager (which have succeeded MBAM as Microsoft's supported BitLocker administration route). It is an Encryption Management function, not a Patch Management function. Beyond the question of scope, we would submit that requiring BitLocker recovery keys to be escrowed inside a third-party operational management tool is a material expansion of the Bank's key-custody risk surface. The recovery key is the single credential that defeats full-disk encryption on every managed endpoint. Placing a second, non-Microsoft copy of that key store inside a patch management database creates an additional custodian, an additional access control boundary, an additional backup and retention obligation, and an additional audit scope under the Bank's cryptographic key management controls without any corresponding security benefit, since Active Directory already holds the authoritative escrow. We request the authority to delete Sr. No. 58 from Section A, the capability being natively available to the Bank through Active Directory / Group Policy and Microsoft Intune. In the alternative, we request that compliance be limited to read-only reporting of BitLocker encryption status as part of endpoint inventory and compliance reporting, with policy enforcement and recovery key custody remaining with Microsoft's native tooling.	This is required functionality. Please be guided by RFP.
	14	Section A - Enterprise Patch Management solution Sr. No. 59. Support periodic rotation of bitlocker keys.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds, namely that BitLocker key lifecycle management is an Encryption Management function outside the scope of an Enterprise Patch Management solution. We would add that periodic rotation of BitLocker recovery keys is itself a native Windows capability, available through the manage-bde command set and through Microsoft Intune's recovery key rotation policy, and can be invoked centrally by the Bank at no additional licence cost. A third-party rotation mechanism operating on the same keys introduces the risk of divergence between the key held in Active Directory and the key held by the third-party tool, which is precisely the failure mode that renders an encrypted endpoint unrecoverable. We request the authority to delete this clause from Section A.	Kindly refer corrigendum
	15	Section A - Enterprise Patch Management solution Sr. No. 60. The solution should support TPM and Non-TPM devices for Bitlocker encryption.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. We would further submit that whether BitLocker may be enabled on a device without a compatible TPM is determined entirely by a Windows operating system policy setting the Group Policy option "Require additional authentication at startup / Allow BitLocker without a compatible TPM" and by the corresponding startup authentication method (password or startup key). It is a Windows configuration state, not a differentiating capability of any management product, and no third-party tool can enable BitLocker on a non-TPM device except by setting that same Windows policy. We request the authority to delete this clause from Section A.	Kindly refer corrigendum
	16	Section A - Enterprise Patch Management solution Sr. No. 61. Restrict technician roles for BitLocker and recovery key access, enhancing security controls in enterprise environments.	This clause is consequential to Sr. No. 58 and is submitted on the same grounds. It presupposes that the Bank's BitLocker recovery keys are held within the proposed Patch Management solution, and requires role-based access control over that key store. If, as requested at Sr. No. 58, recovery key custody remains with Active Directory and Microsoft Intune, the corresponding access restriction is enforced by Active Directory delegation and Intune role-based access control, which are the Bank's authoritative and auditable controls for this purpose. We request the authority to delete this clause from Section A. We confirm that the proposed solution provides granular role-based access control and full audit logging over all administrative functions and data within its own scope.	Please be guided by RFP
	17	Section A - Enterprise Patch Management solution Sr. No. 75. The solution must support zero-touch OS deployment enabling new endpoints to be automatically imaged without administrator physical intervention, using PXE boot or equivalent mechanism.	We note that Sr. No. 73 and Sr. No. 74 of this Section already require OS image creation, capture, template-based customisation and deployment from the management console, and we are compliant with those requirements. Sr. No. 75 goes further and mandates zero-touch, PXE-boot-based bare-metal provisioning without any administrator intervention. We request reconsideration of this additional requirement for the following reasons: (i) PXE-based provisioning is an OS Deployment function delivered by Microsoft Deployment Toolkit, Windows Deployment Services, Microsoft Configuration Manager or Windows Autopilot, or by the hardware OEM's factory provisioning service. It is a build-and-provisioning discipline distinct from patch and vulnerability remediation. (ii) It is a one-time-per-device activity performed at the point of hardware induction or refresh, ordinarily by the Bank's desktop build team, and does not recur through the endpoint's operational life unlike patching, which is continuous. (iii) It requires enabling PXE/TFTP boot services and DHCP option changes (Options 66/67 or IP helper configuration) across the Bank's network segments. Unauthenticated network boot is a control the Bank's network security policy would normally restrict, and enabling it bank-wide is a network and security change well outside the scope of a patch management engagement. (iv) Mandating it as a native requirement narrows the eligible field to full Unified Endpoint Management suites.	Kindly refer corrigendum
	18	Section A - Enterprise Patch Management solution Sr. No. 76. The solution must support user profile migration as part of OS deployment, preserving user data, desktop settings, and application preferences during OS refresh or upgrade cycles.	User state migration is delivered by Microsoft's User State Migration Tool, which is supplied free of charge as part of the Windows Assessment and Deployment Kit, and in most enterprises is rendered largely unnecessary by OneDrive Known Folder Move, roaming user profiles or FSLogix profile containers, all of which are Microsoft entitlements the Bank is likely already to hold. Like PXE provisioning, profile migration is an episodic activity tied to hardware refresh and OS upgrade cycles, and is not part of the continuous patch and vulnerability remediation lifecycle that this Section is procuring. Its inclusion as a mandatory technical specification excludes otherwise fully capable Enterprise Patch Management platforms on a ground unconnected with the Bank's security objective. We request the authority to delete this clause from Section A, or in the alternative to reclassify it as a desirable, non-scored requirement.	Kindly refer corrigendum

	19	Section A - Enterprise Patch Management solution Sr. No. 86. The solution must support centralised printer management deploying and configuring network and local printers to Windows endpoints.	Centralised printer deployment and configuration on domain-joined Windows endpoints is a native Active Directory capability, delivered through the "Deployed Printers" Group Policy extension and Group Policy Preferences, and through Microsoft Universal Print for cloud-managed estates. It is available to the Bank at no incremental cost and is the standard, Microsoft-supported method in an Active Directory environment. It is a desktop administration and end-user configuration task that has no bearing on patch currency, vulnerability exposure or endpoint compliance, which are the objectives of this Section. Mandating it as a native Patch Management specification restricts participation to bundled Unified Endpoint Management suites without any corresponding benefit to the Bank. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where printer deployment and configuration are delivered through the proposed solution's native script and package deployment module, which achieves the identical outcome from the same central console.	Please be guided by RFP
	20	Section A - Enterprise Patch Management solution Sr. No. 87. The solution must support network drive mapping mapping network shares to specific drive letters on Windows endpoints.	This clause is submitted on the same grounds as our query on Sr. No. 86. Mapping network shares to drive letters is a native Active Directory function performed through Group Policy Preferences Drive Maps, or through logon scripts, in every domain environment. It is user-context desktop configuration, is dependent on the user's group membership and share permissions rather than on the endpoint's patch state, and bears no relationship to patch or vulnerability management. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where drive mapping is delivered through the proposed solution's native script deployment module.	Please be guided by RFP
	21	Section A - Enterprise Patch Management solution Sr. No. 88. The management agent must support rebranding to display under the organisation's name and branding.	White-labelling of an OEM's management agent is a cosmetic presentation feature offered by a limited number of OEMs. It delivers no security, operational, compliance or performance benefit to the Bank, and it does not relate in any way to the functional objective of patch and vulnerability remediation. Its inclusion as a mandatory technical specification is therefore restrictive of competition without a corresponding procurement rationale, and does not meet the test in Rule 144(i) of GFR 2017 that specifications be objective and functional. We would further submit that agent rebranding is affirmatively undesirable in a banking environment from a security operations standpoint. Concealing the true vendor identity of a privileged agent binary that runs with SYSTEM rights complicates antivirus and EDR allow-listing, weakens the Bank's ability to attribute a running process to a known vendor during incident triage and forensic review, and obscures the software inventory and SBOM record that the Bank is expected to maintain. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where the end-user-facing elements of the agent self-service portal, end-user notifications and	Kindly refer corrigendum
	22	Section A - Enterprise Patch Management solution Sr. No. 89. The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.	We request the authority to confirm that compliance with this clause is satisfied where the proposed solution centrally creates, modifies and deletes Windows registry keys and values on targeted endpoints and endpoint groups through its native script / configuration deployment module, executed from the central console with scheduling, targeting, execution status and audit logging as distinct from requiring a separately named "registry management" module in the product's user interface. We confirm that we provide central set/reset of registry values on targeted Windows machines and seek this confirmation solely to ensure that all bidders are evaluated on the functional outcome rather than on the naming of a product module.	Registry value modification is required for various configurations. Please be guided by RFP
	23	Section A - Enterprise Patch Management solution Sr. No. 90. The solution must include a built-in credential manager for administrative credentials used in remote operations.	We seek the Bank's clarification on the intended architecture for this requirement, since the clause as drafted may sit in tension with the Bank's privileged access management controls. Under the RBI Cyber Security Framework and prevailing BFSI practice, privileged administrative credentials are expected to be vaulted, rotated and brokered centrally through a dedicated Privileged Access Management solution such as CyberArk, ARCON or BeyondTrust with check-out approval and session recording, precisely so that privileged secrets are not replicated into each operational management console. A requirement that a patch management tool maintain its own independent store of domain administrative credentials creates an additional privileged secret repository, an additional custodian and an additional audit scope. We accordingly request the authority to confirm: (i) whether NHB has an existing PAM platform with which the proposed solution is expected to integrate for credential brokering, and if so which platform and by what interface; (ii) that compliance will be accepted where administrative credentials are held in the solution's own encrypted credential store with role-based access control, audit logging and no plain-text retrieval, and/or are brokered from the Bank's PAM or Active Directory rather than stored in the tool; and (iii) whether the Bank requires credential rotation to be performed by the proposed solution or by its PAM platform.	This functionality is required for executing custom scripts without manually mention credentials in script. It is also required for remote troubleshooting, agent deployment etc. Please be guided by RFP
	24	Section A - Enterprise Patch Management solution Sr. No. 91. The solution must support Wi-Fi profile deployment to Windows endpoints.	Wireless profile provisioning on Windows endpoints is a native Active Directory capability, delivered through the "Wireless Network (IEEE 802.11) Policies" Group Policy extension, and through Microsoft Intune for mobile and cloud-managed estates. It is available to the Bank at no incremental cost. In a bank, enterprise wireless profiles carry 802.1X / EAP configuration and, commonly, machine or user certificates issued by the Bank's PKI. Their provisioning is therefore properly owned and controlled by the network and information security functions through the Bank's NAC and certificate infrastructure, and not distributed as a payload by a patch management tool. The requirement bears no relationship to patch currency or vulnerability remediation. We request the authority to delete this clause from Section A. In the alternative, we request that compliance be accepted where Wi-Fi profiles are deployed through the proposed solution's native script or package	Please be guided by RFP
	25	Section A - Enterprise Patch Management solution Sr. No. 98. Solution is subject to regular penetration testing / vulnerability assessment exercise. Any vulnerability found in the solution will be patched by vendor as per defined timelines by NHB.	We accept in principle that the proposed solution will be subject to the Bank's periodic VAPT exercises and that the OEM will remediate vulnerabilities identified in its product. We seek the following clarifications and amendments, as the clause is presently not capable of being priced or accepted at bid stage: (i) Remediation timelines: the clause requires remediation "as per defined timelines by NHB", but no timelines are defined anywhere in the RFP. A product OEM operates a single, published, severity-based vulnerability remediation SLA applied uniformly across its global installed base, and cannot undertake customer-specific remediation timelines that are undefined at bid stage and to be fixed unilaterally after award. We request the authority to publish the intended remediation timelines by CVSS severity band (Critical / High / Medium / Low) in the RFP itself, so that bidders can evaluate, price and accept them. (ii) Scope of the OEM's remediation obligation: we request the authority to confirm that the obligation extends only to vulnerabilities in the OEM's own product-delivered code, packages, libraries and components, and expressly excludes the underlying operating system, database, web server, middleware and other customer-provisioned infrastructure on which the solution is installed, together with the hardware, hypervisor, network and endpoint estate. Patching, hardening and vulnerability remediation of the operating system and database layer remain the responsibility of the Bank or its system integrator, in accordance with standard software licensing practice. (iii) Third-party and OS-inherited findings: where a VAPT finding arises from a third-party or open-source component, the OEM's obligation should be to incorporate the upstream fix within its published SLA once that fix is released by the upstream maintainer, and to provide a documented mitigation or compensating control in the interim. (iv) Conduct of the exercise: we request confirmation that VAPT will be performed on the Bank's own instance in a non-production environment, under a mutual non-disclosure agreement, with findings and evidence shared with the OEM to enable validation and remediation, and that reverse engineering, decompilation and public disclosure of findings are excluded. (v) We request that the clause be amended to record that remediation is "as per the OEM's published vulnerability remediation SLA, or such timelines as are specified in the RFP", in place of timelines to be defined after award.	Kindly Refer Section 12.17 of RFP for timelines of closure of observations. Bidder has to to comply with observations pertaining to all supplied software components.

	26	Section C - Unified Enterprise Management Solution Sr. No. 7. The solution should support bi-directional CMDB sync along with auto-ticketing between the monitoring tool and ManageEngine ServiceDesk Plus.	The clause names a specific third-party OEM product as the mandatory integration target. As drafted, it is capable of being read as requiring a pre-built, product-specific connector to ManageEngine ServiceDesk Plus, which in practice is offered natively by that OEM's own monitoring products with the effect of favouring a single OEM's stack, contrary to the requirement in Rule 144(i) of GFR 2017 that specifications not indicate a requirement for a particular trade mark or trade name. Bi-directional CMDB synchronisation and automated ticket creation, update and closure are standard interoperability functions that any modern monitoring platform delivers through documented REST APIs and webhooks. We therefore request the authority to confirm: (i) that compliance will be accepted where bi-directional CMDB synchronisation and auto-ticketing are implemented through documented REST APIs and webhooks, and a pre-built ManageEngine-specific connector is not insisted upon; (ii) the edition, version and deployment model of the ManageEngine ServiceDesk Plus on-premise instance, and whether its REST API, CMDB / CI APIs and CI relationship APIs are licensed and enabled in that edition; (iii) the CI classes, attributes and relationship types to be synchronised, the direction of authority for each (which system is the master for each attribute), and the expected synchronisation frequency and volume; (iv) that the Bank will provide API access, authentication tokens, a test instance and the necessary support from its incumbent ManageEngine partner during integration and testing; and (v) that any configuration, licensing, customisation or professional-services effort required on the ManageEngine ServiceDesk Plus side sits with the Bank or its incumbent ITSM partner and is outside the bidder's scope and price. This information is necessary for all bidders to estimate integration effort accurately and to quote on a comparable basis.	Integration will be scope of bidder only. Bank will provide access of API of Service Desk Plus.
	27	Section C - Unified Enterprise Management Solution Sr. No. 33. The proposed solution should provide Network Detection and Response (NDR) capabilities to continuously monitor network traffic, detect anomalous or malicious activities, and enable rapid investigation and response to security incidents.	Network Detection and Response is a distinct security product category represented by platforms such as Darktrace, ExtraHop Reveal(x), Vectra AI and Cisco Secure Network Analytics and is not a function of an enterprise monitoring or observability platform. The two differ in three material respects: (i) Data plane: NDR requires full packet capture and deep packet inspection fed by SPAN, mirror or network TAP infrastructure, together with the associated capture appliances and storage. An enterprise management solution consumes flow telemetry (NetFlow, sFlow, J-Flow, IPFIX) and SNMP, which is metadata about conversations and is sufficient for performance, capacity and utilisation analytics but not for payload-level threat detection. (ii) Detection engine: NDR detection is built on attack-behaviour models, command-and-control and lateral-movement analytics and curated threat intelligence, maintained by a security research organisation. Monitoring platforms baseline performance behaviour, which is a different analytic objective. (iii) Response: the "Response" element of NDR requires enforcement authority over firewalls, NAC and EDR to block, isolate or terminate sessions. An enterprise monitoring platform neither holds nor should hold that authority, which in the Bank's architecture properly sits with its SOC, SIEM/SOAR and network security controls. Including NDR within the scope of a Unified Enterprise Management Solution therefore both mismatches the product category and materially narrows the eligible bidder set to the small number of OEMs that market a bundled NDR module, with a consequent effect on price discovery. We request the authority to delete this clause from Section C, the capability being properly procured and operated as part of the Bank's security stack. In the alternative, we request that compliance be accepted on the basis of flow-based traffic baselining and anomaly detection with alert forwarding to the Bank's SIEM/SOC for investigation and response — which is already required at Sr. No. 63 of this Section and which we fully	Kindly refer corrigendum
	28	Section C - Unified Enterprise Management Solution Sr. No. 75. The proposed solution should provide monitoring for SAP systems, including performance metrics, system health, and key operational parameters.	SAP environments are instrumented through interfaces controlled by SAP itself principally SAP Solution Manager and SAP Focused Run, and at the technical layer the CCMS / SAPControl web service, the /SDF/MON monitoring infrastructure and, on the Java stack, JMX. SAP does not permit byte-code instrumentation of the ABAP stack by third-party APM agents, and the installation of third-party agents on SAP application servers is governed by SAP's own support and certification policy, which can affect the customer's SAP support entitlement where unapproved agents are deployed. The extent to which any third-party solution can monitor SAP is therefore determined by the access the Bank's SAP landscape and SAP support agreement permit, and not by the capability of the monitoring product. To enable accurate and comparable responses from all bidders, we request the authority to confirm: (i) the SAP landscape in scope the products, the stack (ABAP, Java, HANA, S/4HANA) and the number of systems and instances; (ii) whether the Bank will enable and grant access to the SAPControl web service, CCMS and/or JMX interfaces, and provide a dedicated read-only monitoring service user with the necessary authorisations; (iii) whether the installation of a third-party monitoring or APM agent on SAP application servers is permitted under the Bank's SAP support and licensing agreement; and (iv) that where such access or agent installation is not permitted, compliance will be accepted on the basis of infrastructure-level monitoring of the SAP hosts operating system, database, availability, port and service response and resource utilisation or, failing that, that the clause be withdrawn from the mandatory specifications.	We are using SAP ECC 6 EHP 7 with SQL Server database. We are using two instances CI & DI.
	29	Section A - Enterprise Patch Management solution Sr. No. 32. The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status. [Read with Sr. No. 73: "...OS imaging and deployment of Windows operating systems from the cloud-connected management	Sr. No. 32 requires the compliance dashboard to be a "cloud dashboard", and Sr. No. 73 refers to a "cloud-connected management console". We seek clarification, as this wording appears inconsistent with the deployment posture that a regulated financial institution would ordinarily require, and with the balance of this Section which contemplates on-premise distribution points, air-gapped and closed-network patching (Sr. No. 6) and local content distribution. For a Housing Finance regulator and refinance institution, endpoint inventory, patch state and vulnerability posture constitute sensitive operational security data, and its residence in a vendor-operated cloud tenant raises data localisation, data residency and third-party risk considerations under the RBI framework, together with the corresponding outsourcing governance obligations. Mandating a cloud-hosted console also has the effect of excluding on-premise deployment models, which is restrictive without an evident functional rationale, since the substance of the requirement real-time compliance status, endpoint health classification and drill-down to device level is delivered identically by an on-premise centralised console. We request the authority to confirm whether the solution is to be deployed on-premise within the Bank's data centre, and accordingly to substitute the words "centralised cloud dashboard" at Sr. No. 32 with "centralised management dashboard", and "cloud-connected management console" at Sr. No. 73 with "centralised management console", retaining all functional requirements of both clauses unchanged. We confirm full	Kindly refer corrigendum
	30	Section C - Unified Enterprise Management Solution Sr. No. 66. ...must keep historical rate and Ip to Ip, Ip to protocol, protocol to protocol conversation data for a minimum of 3 months... maximum 15 minute window granularity. Sr. No. 67. Future Scalability – the system should be capable of supporting at least 15 thousand network flow per second on single server...	These clauses prescribe flow retention, granularity and throughput figures without stating the underlying environment parameters against which they are to be sized. Flow collector sizing, storage volume and licence quantum are a direct function of the sustained and peak flow rate, the number of exporters and monitored interfaces, and the retention and granularity policy applied at each tier. To enable all bidders to size the solution correctly and to quote on a uniform basis, we request the authority to confirm: (i) the number of flow-exporting devices and the total number of monitored interfaces from which flow is to be collected; (ii) the expected sustained and peak flows per second at the aggregate level, and whether the 15,000 flows per second at Sr. No. 67 is the sustained figure, the peak figure or a headroom requirement; (iii) whether the three-month retention at Sr. No. 66 is required at raw conversation granularity throughout, or whether rolled-up 15-minute aggregation is acceptable for the full three-month window raw and aggregated retention differ by an order of magnitude in storage; (iv) whether the storage required for the flow retention tier is to be provided by the Bank or is to be included in the bidder's scope, and if the latter, the storage type and protection level to be assumed; and (v) whether the "single server" requirement at Sr. No. 67 refers to a single flow collector node, and the server specification the Bank expects that figure to be achieved on. Absent these parameters, bids will not be comparable on a like-for-like basis.	Please be guided by RFP. Details of network devices already provided in RFP.

	31	Section C - Unified Enterprise Management Solution Sr. No. 61. The proposal solution should support AI/ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspicious behaviour in network traffic, device performance and application metrics. Alerts are triggered for deviations so Network team can respond to issues early.	We request the authority to confirm the intended scope of this clause, specifically that it is directed at operational anomaly detection for performance and availability management, and not at security threat detection, which is the subject of the Bank's SIEM and security stack and which we have separately queried at Sr. No. 33. We further request confirmation that compliance will be accepted where the solution provides machine-learning-based dynamic and adaptive thresholding on performance metrics, automatic baselining of normal behaviour with deviation alerting, forecasting and predictive analytics on capacity metrics, and baseline flow policies for detection of anomalous traffic behaviour as already required at Sr. No. 23, Sr. No. 24, Sr. No. 38, Sr. No. 39 and Sr. No. 63 of this Section without requiring a separately licensed security analytics or user-and-entity-behaviour-analytics engine. The word "suspicious" in the present drafting introduces a security connotation that overlaps with the NDR requirement at Sr. No. 33 and would, if read as a threat-detection requirement, restrict participation to OEMs bundling a security analytics module.	Kindly refer corrigendum
	32	6.1. Statement of Wok 1. Vendor is required to implement the mentioned tools at DC. The bidder shall ensure that the proposed solutions are technically capable of deployment in a Disaster Recovery (DR) environment, if required by NHB in the future.	The RFP states that the proposed solution is required to be implemented at the Data Centre (DC) and should be technically capable of future deployment at the Disaster Recovery (DR) site, if required by NHB. Kindly clarify whether High Availability (HA) deployment at DC and/or DR deployment is required from Day One. If yes, please confirm whether all necessary software licences, DR licences and infrastructure sizing are to be included in the current scope. Further, kindly specify the required deployment architecture (Active-Active or Active-Passive), along with the expected RPO (Recovery Point Objective), RTO (Recovery Time Objective), and the scope of DR implementation and licensing.	HA is not required. Installation is required at DC only. For, future price of DR installation, kindly refer corrigendum.
	33	6.5. Maintenance & Technical Support services for Manage Engine Service Desk Plus solution:	NHB has mentioned existing ManageEngine ServiceDesk Plus Enterprise Edition with 10 Technicians/2000 Nodes. Kindly provide the exact deployed product version, build number, database version, architecture, deployment topology and all currently enabled modules, so that bidder can correctly assess compatibility, migration and upgrade requirements	Bank is using ManageEngine ServiceDesk Plus Enterprise Edition version 15.2
	34		NHB has stated that centralized ManageEngine solution is currently implemented as EMS. Kindly provide exact product names, editions, versions/builds, modules, licence quantities and current deployment architecture.	Bank is using OP Manager presently.
	35	Annexure XVIII – Solution Compliance Statement 9 The proposed solution should be able to accommodate network growth of up to 500 devices with any number of metrics (Ports, IP address etc.) on individual device.	The RFP requires scalability up to 500 devices with any number of metrics. Kindly clarify whether 500 devices is a mandatory Day-1 licence or future scalability requirement, and whether the bidder should quote licence capacity for 400 or 500 devices.	Kindly refer corrigendum. Bidder should quote licenses as per Commercial Bid Format.
	36	Database Monitoring 102 The proposed solution should monitor Microsoft SQL Server instances, including database performance, availability, query execution, and resource utilization.	Kindly provide the number of SQL Server, Oracle, No SQL and in-memory database instances, versions and production/non-production distribution for accurate database monitoring sizing.	Total Production SQL Server -25 Total Oracle Server - 12
	37	5. Installation, Commissioning and Operationalization of the complete solution: within 45 days of acceptance of work order.	Considering the overall scope of work, including solution deployment, configuration, integration with existing systems, user training, and production operationalization, the stipulated implementation timeline of 45 days appears to be very stringent. We request NHB to extend the implementation timeline to 90–120 days from the date of acceptance of the Work Order to facilitate successful implementation and ensure the quality and stability of the deployed solution.	Please be guided by RFP
	38	Bidder must specify hardware requirements based on their understanding of the overall solution architecture based on requirement. The same must be documented and shared with NHB along with justification/reasonability. It is to be noted that NHB will provide virtual servers and not physical servers to meet these hardware requirements.	Kindly Clarify the below points - 1. We understand that the required vCPU/virtual infrastructure will be provided by NHB, while the Operating System and Database licenses will be provided by the successful bidder. Please confirm our understanding. 2. Please help with the below infra details to propose the best suitable compatible solution: a. Underlying Virtualization Platform. b. Underlying Server and Storage make/models. 3. Since the Bank is providing the infrastructure, could you please clarify who will be responsible for configuring the required VMs/workloads and who will handle their maintenance and support during the Operations & Maintenance (O&M) phase?	Bank will provide VM on HyperV/Vmware. Underlying server and storage details will be shared with Successful bidder. Impelemenation will be done by the bidder.
	39	Any other components like middleware/software/licenses etc. required in connection with the work will be supplied and maintained by the vendor. Bidder is responsible for providing end-to-end solutions (Comprising Solution Software, licenses, OS, Middleware, Database- latest or compatible with annual technical support)	4.We request your assistance in providing the physical server configuration details, as Microsoft licensing is based on the number of physical cores. 5. Please confirm if SA is required in case Microsoft Licenses are part of the solution.	1. Yes 2. Bank will provide VM on HyperV/Vmware. Further detail will be shared by successul bidder.

Bidder 5

	S. No.	Relevant Clause of the RFP	Query	Bank's Reply
	1	The Bidder should have experience in implementation/ support of IT Services Management Solutions in at least 2 Public Sector Bank / Financial Institution / PSU / Government Organization / Large Corporates** in India during the last 5 FYs. Experience criteria is relaxed for MSE & Startup	As per the RFP clause, the experience criteria is relaxed for MSEs & Startups. We request the Buyer to kindly clarify whether a bidder registered as an MSE under Udyam Registration in the Service Category is also eligible for relaxation/exemption from the prescribed experience requirement of implementation/support of IT Service Management Solutions in at least 2 Public Sector Banks / Financial Institutions / PSUs / Government Organizations / Large Corporates in India during the last 5 financial years. Kindly confirm whether the above experience relaxation is applicable to MSE bidders registered under the Service Category as well.	Please be guided by RFP
	2	Section 6.3 - Active Directory Management Scope	As per Section 6.3, the RFP mandates comprehensive Active Directory management, granular delegation, GPO auditing, and identity lifecycle workflows. Kindly clarify whether dedicated AD management tools are mandatory, or if bidders can propose standard endpoint management solutions integrated with third-party/OEM AD management modules to meet compliance.	Please be guided by RFP
	3	Section 6.5 - ManageEngine ServiceDesk Plus AMC	Section 6.5 specifies ongoing AMC, support, and license additions for ManageEngine ServiceDesk Plus. We request the Buyer to clarify whether integration between the proposed Unified Enterprise Management/Patching solution and ManageEngine ServiceDesk Plus requires out-of-the-box native connectors or if standard REST API / webhook-based integration is fully acceptable.	REST API/webhook based integration is fully acceptable
	4	Section 6.4 - Unified Enterprise Management & In	As per Section 6.4, the RFP scope includes Unified Enterprise Management covering network/APM monitoring alongside endpoint patch management. Kindly clarify whether bidders are permitted to propose an integrated OEM bundle (combining an enterprise patching platform with dedicated network observability modules) to satisfy 100% of the functional scope.	yes

	5	The solution must natively detect CVEs on managed endpoints and display them with CVSS score, severity classification, and affected application details without a separate vulnerability scanner.	The bidder would like to clarify that this requirement is a specialized capability of vulnerability management/scanning solutions, whereas Section 6.4 is scoped for Endpoint/Patch Management. The bidder therefore requests removal of this requirement. Alternatively, the bidder requests that integration with a vulnerability management solution from a different OEM than the proposed patch management solution be permitted.	Kindly refer corrigendum
	6	The solution must identify zero-day vulnerabilities on managed endpoints threats for which no patch is yet available	The bidder requests removal of this item, as no solution can independently detect or identify a zero-day vulnerability before it is disclosed by the respective vendor/OEM (e.g., Microsoft, RHEL). Therefore, the stated requirement is technically not accurate.	Kindly refer corrigendum
	7	The proposed solution should ensure that files are scanned for infections during both read and write operations.	The bidder requests removal of this item, as scanning for infections, malicious code, or viruses is not a core capability of patch management solutions. Such functionality is typically provided by endpoint security/antivirus solutions; hence, the stated requirement is not technically aligned with the scope.	Kindly refer corrigendum
	8	Support for patching standard desktop applications (e.g., Microsoft, Google Chrome, Mozilla etc) as well as VDI environments.	As explained in pre-bid meeting, please remove "VDI" from the requiremnet as VDI are not patched by a patch management solution.	Kindly refer corrigendum
	9	The solution must support user profile migration as part of OS deployment, preserving user data, desktop settings, and application preferences during OS refresh or upgrade cycles.	As discussed during the pre-bid meeting, the bidder requests removal of this requirement, as user migration and user data synchronization, backup, or restoration are not core capabilities of endpoint management solutions. While endpoint management solutions may support OS imaging, user data management is typically handled through Active Directory and GPO policies.	Kindly refer corrigendum
	10	The proposed EMS solution must comply with the following standards: 27034-1 for application security, ISO 27001:2022 for information security management, GDPR or DPDP for data privacy, and SOC 2 Type 2 for service organization controls. This ensures robust security, regulatory compliance, and comprehensive data protection across all managed network operations. Valid supporting documents must be submitted with the bid.	Please consider the following revised clause: Revised Clause: *The proposed EMS solution must comply with the following standards: 27034-1 for application security, ISO 27001:2022 for information security management, GDPR or DPDP for data privacy, and SOC 2 Type 2 for service organization controls. This ensures robust security, regulatory compliance, and comprehensive data protection across all managed network operations. Valid supporting documents must be submitted with the bid for ISO-27001:2022, SOC2.*	Kindly refer corrigendum
	11	The proposed solution must be a natively unified observability platform, to seamlessly integrate fullstack monitoring, log analytics, application performance monitoring (APM), flow analytics, compliance tracking, netroute tracing, and telemetry correlation within a single cohesive system—without requiring any third-party plugins, tool-switching, or modular bolt-ons.	Please consider the following revised clause: Revised Clause: *The proposed solution must be a unified observability desgin, to seamlessly integrate fullstack monitoring, log analytics, application performance monitoring (APM), flow analytics, compliance tracking, netroute tracing, and telemetry correlation.*	Kindly refer corrigendum
	12	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Correlation, and root cause analysis, Reporting and analytics	Please consider the following revised clause: Revised Clause: *The Monitoring Solution should provide offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Correlation, and root cause analysis, Reporting and analytics*	Please be guided by RFP
	13	The system must not use any open-source thirdparty relational or time-series databases for reporting data. It should use a native, proprietarybuilt reporting database for high-speed, highvolume observability workloads and security constarins.	Please consider the following revised clause: Revised Clause: *The system must not use any open-source third party relational or time-series databases for reporting data. It should use a native/built-in or third party enterpise reporting database for high-speed, highvolume observability workloads and security constarins.*	Kindly refer corrigendum
	14	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring	Please consider the following revised clause: Revised Clause: *All the required modules should be preferably from same OEM or mutiple OEM however should be tightly integrated for single pane of glass view of enterprise monitoring*	Please be guided by RFP
	15	The proposed solution should allow the application of advanced statistical transformations and functions over selected KPIs, including but not limited to: Anomaly Detection Forecasting Moving Average Median Function Logarithmic Scale Transformation Delta/Derivative Functionality	Please consider the following revised clause: Revised Clause: *The proposed solution should allow the advanced statistical transformations and functions over selected KPIs, including but not limited to: Anomaly Detection, Forecasting.*	Kindly refer corrigendum
	16	The proposed solution should provide Network Detection and Response (NDR) capabilities to continuously monitor network traffic, detect anomalous or malicious activities, and enable rapid investigation and response to security incidents.	The bidder request removal of this item as NDR capability is not a function of monitoring/observability.	Kindly refer corrigendum
	17	The system must support out-of-the-box CIS benchmarks tailored specifically for network devices.	Please consider the following revised clause: Revised Clause: *The system must support CIS benchmarks configuraiton tailored specifically for network devices.*	Kindly refer corrigendum
	18	The proposed solution must possess valid CIS Benchmarks Certification for Compliance Assessment, attesting its compliance with the security configuration guidelines and best practices prescribed by the Center for Internet Security (CIS)	The bidder requests removal of this item, as it is not related to Network Configuration Management but rather to Endpoint Management. Alternatively, the bidder requests that the assessment/certification be permitted for Endpoint Management instead of Network Management.	Kindly refer corrigendum
	19	The platform should provide comprehensive out of the box organization wide vulnerability dashboard which should help identify actionable vulnerabilities to remediate.	The bidder requests removal of this item, as vulnerability assessment is not an out-of-the-box capability of Network Configuration Management (NCM) solutions and is typically provided by dedicated vulnerability assessment/scanning tools. As discussed during the pre-bid meeting, the requirement appears to align with an OEM offering that bundles VA and NCM rather than an inherent NCM capability. Alternatively, the requirement may be considered compliant through integration with the NIST vulnerability database.	Please be guided by RFP

	20	The proposal solution should support AI\ML based Anomaly detection: Learn the environment's normal patterns and automatically detect abnormal or suspecious behaviour in network traffic, device performance and application metrics, Alets are triggered for deviations so Network team can respond to issues early.	The bidder requests removal of this item, as the stated capability appears to be specific to a particular OEM/solution. Such requirements may restrict participation from other qualified OEMs and limit broader competition.	Kindly refer corrigendum
	21	The proposed solution should support agentbased auto-instrumentation for Java and .NET applications, including compatibility with a wide range of modern frameworks such as Spring Boot, ASP.NET and others without requiring code changes.	Please consider the following revised clause: Revised Clause: *The proposed solution should support agentbased auto-instrumentation for Java and .NET applications, including compatibility with a wide range of modern frameworks such as Spring Boot, ASP.NET and others without requiring code changes. Additionally, it should allow for the manual insertion of JS snippets into the HTML header where automatic injection is not feasible, ensuring flexibility.*	Kindly refer corrigendum

Bidder 6

SL No	Relevant Clause of the RFP	Point and Page number	Query	Bank Reply
1	Clause 6.1.1	Point 1 Page number 10	Since NHB currently requires deployment at DC only and DR deployment may be considered in future, please confirm whether separate DR licenses /Implemenations cost are required to be quoted at this stage ?	Kindly refer corrigendum for future cost.
2	Clause 6.1.8	Point 8 Page number 10	Kindly clarify the existing tools from which migration is expected and the specific data sets to be migrated (configuration, historical logs, tickets, reports, etc.).	At present bank is using Manage Engine Endpoint Central, OP Manager and AD360.
3	Clause 6.1.11	Point 11 Page number 10	Please provide details of the existing SIEM solution and other third-party platforms proposed for integration to enable accurate effort estimation.	Present SIEM solution is Elastic Search. Bank is also using PeopleSoft HRMS, Manage Engine Service Desk Plus.
4	Clause 6.1.18	Point 18 Page number 11	Kindly confirm the Required Hradwares ,Compute, Infra for Deploying the applications that will be provided by NHB.	Yes
5	Clause 6.2(a)	Point a Page number 11	Kindly clarify whether future expansion beyond 320 endpoints and 180 servers will be procured separately using optional license pricing mentioned in the commercial bid.	Yes
6	Clause 6.2(l)	Point l Page number 12	Please share details of the vulnerability management tools currently deployed at NHB for integration with the Patch Management Solution.	At present no such tool is deployed. However, bidder is to integrate if NHB deploy during the contract period.
7	Clause 6.3(r)	Point r Page number 13	Kindly provide details of HRMS, IDAM and other applications for which API-based integration will be required.	Bank is PeopleSoft HRMS at present. No IDAM solution is deployed. However, more solutions may pe procured by the bank during period of contract.
8	Clause 6.3(v)	Point v Page number 14	Please specify the average daily Active Directory log volume to size storage appropriately for one-year retention.	Present volume is 25 GB per month.
9	Clause 6.4(a)	Point a Page number 14	Please clarify whether the 400 monitoring devices include servers, network devices, virtual machines and applications collectively or only infrastructure devices.	Kindly refer corrigendum.
10	Clause 6.4(l)	Point l Page number 15	Kindly share the approximate number of IP subnets and IP addresses to be managed under the IPAM requirement.	At present approx. 65 subnets and 600 IP addresses. However, same may be increased during period of contract.
11	Clause 6.5(a)	Point a Page number 15	Kindly confirm the existing version/build/On premises or Cloud version of ServiceDesk Plus Enterprise Edition deployed at NHB.	Bank is using On-premise Service Desk Plus 15.2 version.
12	Clause 6.5(b)	Point b Page number 15	Please clarify whether only three additional technician licenses are required or if migration to the latest supported version is also expected under this scope.	Please be guided by RFP.
13	Clause 6.6(b)	Point b Page number 15	Kindly define the expected response time and duration for onsite engineer support in urgent scenarios.	Please be guided by RFP.
14	Clause 7.3	Point 3 Page number 17	Please clarify whether OEM End-of-Support confirmation letter on OEM letterhead will be sufficient for compliance.	Yes
15	Clause 7.5	Point 5 Page number 17	Considering integration, migration, testing, audit compliance and training activities, kindly consider extending the implementation timeline from 45 days to 90 days.	Please be guided by RFP.
16	Clause 8	Point 8 Page number 17	Please confirm whether any contract extension beyond 3 years will be based on mutual agreement and separate purchase order issuance.	Please be guided by RFP.
17	Clause 10.0	Point 10.0 Page number 31	Please clarify whether OEM implementation experience can be considered along with bidder experience for technical evaluation.	Please be guided by RFP.
18	General	Page number 31	Kindly confirm whether implementation references/ Experince will be considered only for ManageEngine Solution or Similar	Please be guided by RFP.
19	Clause 10.0 Technical Evaluation	Point 10.0 Page number 31	Kindly confirm whether implementation references using ManageEngine products in PSU/Banks/FIs will be accepted as evidence for scoring against relevant solution categories.	Please be guided by RFP.
20	Clause 11.2(a)	Point a Page number 35	Request NHB to consider releasing 90% of solution cost upon successful Go-Live and sign-off to align with OEM licensing costs incurred upfront.	Please be guided by RFP.
21	Clause 12.17.1	Point 17.1 Page number 38	There appears to be a variance between Clause 9.13 (45 days implementation) and penalty clause referring to implementation within 40 days. Kindly clarify the applicable timeline.	Kindly refer Corrigendum.
22	Clause 12.17.2	Point 17.2 Page number 39	Kindly confirm whether downtime attributable to NHB infrastructure, third-party connectivity, virtualization platform or power failures will be excluded from SLA calculations.	Please be guided by RFP section 12.17.2
23	General	General	Since NHB currently has existing ManageEngine deployments (ServiceDesk Plus, Endpoint Central, EMS), please confirm whether leveraging existing infrastructure and integration components will be permitted and preferred.	Please be guided by RFP.
24	Clause 6.1.18 & 6.1.21	Point 18 and 21 page number 11	NHB has stated that virtual servers and infrastructure will be provided by the Bank. Kindly confirm that bidders are not required to quote any hardware (server/storage/network) and only need to provide sizing recommendations for the virtual infrastructure.	Hardware will be provided by the bank as per recommendations of bidder.
25	General	General	Clarify whether NHB will provide Windows/Linux OS and SQL/Oracle database licenses for the solution VMs, because the BOQ includes separate line items for OS and Database licenses, while the RFP also states NHB is providing the infrastructure	Please be guided by RFP.
26	Clause 6.1.22	Point 22 Page number 11	Kindly clarify whether 24x7 support requires dedicated resident engineers or remote support ?	24x7 support should be available on remote site.
27	General	General	Request NHB to clarify that audit observations arising from customer infrastructure, OS hardening, database configuration, or third-party products shall be outside bidder responsibility	Compliance of Audit observations pertaining to any components supplied by bidder, is sole responsibility of bidder itself.
29	Clause 9.14	page number 23	Request NHB to reduce Performance Bank Guarantee from 5% to 3% of contract value	Please be guided by RFP.
30	Clause 6.1.3	point 3 Page number 10	Kindly confirm whether OEM bundled databases (PostgreSQL, SQL Express, etc.) will be acceptable if supported by the proposed solution architecture	Yes
31	Clause 10 - Technical Evaluation	General	Request NHB to consider the combined experience and credentials of both the Bidder and OEM for implementation references, project experience, customer credentials, and technical evaluation scoring.	Please be guided by RFP.
32	Annexure XVIII – Solution Compliance Statement	Annexure XVIII – Solution Compliance Statement	Does the proposed solutions to be configured in HA mode (Failover) In DC ?	No
33	Clause 6	Page 10	Can NHB confirm whether bidders may propose products from multiple OEMs across Patch Management, AD Management/Audit, and Unified Enterprise Management categories, or whether all solutions must be from a single OEM?	Different OEM products may be proposed.

Bidder 7

	S.No.	Relevant Clause of the RFP	Query	Bank Response

	1	Point 6.10. Audit Requirements Any audit exercise, including but not limited to VAPT/Internal Audit/External Audit/IS Audit/RBI/Regulatory Audit etc. when conducted, it shall be the Successful bidder's responsibility to rectify the gaps unearthed during these audit exercises at no additional cost to the bank during the contract period. Further, it shall be the responsibility of the selected bidder to close/comply with the audit observations as per the Bank's policy. No additional cost would be paid by Bank.	We request clarification that the bidder's responsibility for closure of audit observations shall be limited to issues directly attributable to the solution, licenses, configurations and services supplied under this contract and within the standard supported capabilities of the proposed OEM products. Any observations arising from Bank infrastructure, third-party products, regulatory enhancements, customizations, additional integrations, additional licenses/modules or scope items beyond the RFP shall be handled through mutually agreed change requests and commercials. The bidder shall not be liable for remediation of audit observations where resolution requires procurement of additional OEM licenses, modules, third-party products, hardware, software, or services not included in the original bid.	Compliance of Audit observations pertaining to any components supplied by bidder, is sole responsibility of bidder itself.
	2	Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	Request to remove Oracle database patching.	Kindly refer corrigendum.
	3	Point 22 and 44 are repeated and required change Solution should enable Agents to dynamically connect to the next nearest Distribution point if the assigned Distribution point is not available.	Changes requested as below The solution should support a Distribution Server architecture to optimize bandwidth utilization. Agents should not need to communicate directly with the Central Endpoint Management Server. Instead, they should be able to access the Distribution Server locally to: • Receive and apply patches. • Retrieve and apply configuration policies. • Download and install software packages. • Obtain required updates and content locally. This architecture will reduce bandwidth consumption, minimize direct traffic to the Central Endpoint Management Server, and improve the efficiency of endpoint management across distributed locations	Kindly refer corrigendum.

Bidder 8

	S. No.	Relevant Clause of the RFP	Query	Bank Reply
	1	**Endpoint licensing:** The RFP mentions 560 laptops/desktops, whereas the Patch Management solution is specified for 320 endpoints.	Please clarify whether the Patch Management license requirement is limited to 320 endpoints or whether all 560 endpoints are required to be covered. If 320 is the initial quantity, please clarify the expansion mechanism and applicable commercial model for additional endpoints.	Please by guided by RFP
	2	**Server licensing** The current environment mentions: 46 physical servers 172 VMs while the Patch Management requirement specifies 180 servers.	Please confirm whether the 180-server licensing quantity includes both physical and virtual servers, and whether Kubernetes/container workloads are included in this count.	Please by guided by RFP
	3	**UEM 400 devices** UEM specifies: 400 monitored devices while the current infrastructure summary contains endpoints, servers, VMs and network devices exceeding this number.	Please clarify the exact definition of "device" for UEM licensing and provide the expected licensed quantity for servers, VMs, endpoints, network devices, cloud resources and applications.	Kindly refer corrigendum pertaning to Commercial Bid format.
	4	**Network device count** The RFP states 77 network devices, while UEM specifically mentions 80 network devices for configuration management and NetFlow analysis.	Please confirm whether 80 is the final licensed quantity and whether it includes routers, switches, firewalls, wireless controllers and other IP devices.	Yes
	5	**DC / DR Clarification – HIGH PRIORITY** There is an important ambiguity. One section says implementation is required at DC and the solution should be capable of future DR deployment. However, the implementation penalty section refers to: One-time Implementation & Integration at DC & DR sites and a 45-day implementation timeline.	Please clarify whether complete implementation, configuration, integration, testing and commissioning are required at both DC and DR as part of the current scope, or whether DR capability is only required for future deployment. This is a major commercial issue.	Kindly refer corrigendum.
	6	**NHB says it will provide virtual servers rather than physical servers for the solution.** But the solution includes: -APM -Network Flow -NDR -Database monitoring -Log analytics -AI/ML -IPAM -Configuration management	Please provide the available VM infrastructure specifications at DC and DR, including CPU, RAM, storage type, IOPS, network throughput, virtualization platform/version and available expansion capacity.	Bidder must specify compute requirement as per of Technical Bid. Bank will provide VM on HyperV/Vmware. Underlying server and storage details will be shared with Successful bidder.

	7	**Sizing Information – CRITICAL** The RFP does not give sufficient information to accurately size an enterprise observability platform.	Please provide the expected/average and peak monitoring metrics, events, logs, traces, NetFlow/sFlow/IPFIX and application telemetry volumes for sizing purposes. Specifically request: Events/sec Network flows/sec Number of interfaces Number of metrics Metrics collection frequency APM transactions/sec Trace volume Database instances Applications requiring APM Log volume/day Retention Number of cloud resources	For application requiring APM, kindly refer corrigendum. Total Production SQL Server -25 Total Oracle Server - 12 Kindly refer Section 5 of RFP.
	8	SIEM Integration – HIGH PRIORITY The RFP requires integration with the existing SIEM and even refers to current/future SIEM integrations. However, it does not clearly specify: SIEM OEM Version Architecture API Data volume Use cases Integration method	Please provide the existing SIEM OEM, version, deployment architecture, integration/API specifications, expected data volume and required integration use cases.	Bank is using Elastic Search SIEM.
	9	**Future SIEM" Requirement** The RFP says integration with the current SIEM and any future SIEM, without extra cost.	Please clarify the scope and number of future SIEM integrations covered under the quoted price and whether future integrations will be limited to standard APIs/connectors supported natively by the proposed solution.	In the event that the Bank replaces its SIEM solution during the contract period, the successful Bidder shall integrate the proposed solution with the newly adopted SIEM platform at no additional cost to the Bank.
	10	**NDR Requirement** The UEM section asks for NDR capabilities. But it is unclear whether NHB expects: Full NDR Flow-based detection Basic anomaly detection Packet inspection IDS/IPS functionality	Please clarify the expected scope of NDR functionality, including whether full packet inspection, IDS/IPS, encrypted traffic analysis, behavioural analytics and threat detection are required, or whether NetFlow/sFlow/IPFIX-based anomaly detection will be considered sufficient.	Kindly refer corrigendum.
	11	**15,000 Flow/sec Requirement** This is a significant technical requirement. The RFP requires the solution to support at least 15,000 network flows per second on a single server.	Please confirm the current average and peak NetFlow/sFlow/IPFIX traffic rate and whether the 15,000 flows/sec requirement is a mandatory Day-1 production requirement or a future scalability requirement	It is mandatory from Day-1
	12	**APM Scope – VERY LARGE** The APM requirements include: Java .NET Node.js PHP Python SAP Distributed tracing Microservices Service maps Trace correlation Transaction monitoring Custom instrumentation Custom metrics	Please provide the list of applications currently planned for APM monitoring, including application technology, number of instances, production/non-production classification and expected transaction volume. Otherwise, APM sizing and implementation effort cannot be accurately estimated.	Bidder is to provide APM monitoring for 30 applications including SAP.
	13	**Database Monitoring** The RFP requires monitoring of: SQL NoSQL In-memory databases Query performance Deadlocks Connection pools SQL Server DB latency DB failures	Please provide the complete database inventory, including database type, version, number of instances, production/non-production classification and expected monitoring scope.	Total appox. SQL Server database servers are 33. Total Oracle Servers are 13. However, if bank implement other database instances, bidder should monitor the same also.
	14	**Kubernetes** The current environment specifically mentions Kubernetes. But the RFP does not clearly define Kubernetes monitoring requirements.	Please clarify whether Kubernetes monitoring is part of the mandatory UEM scope and provide the number of clusters, nodes, namespaces and workloads requiring monitoring.	Please by guided by RFP
	15	**SAP Monitoring** SAP is part of NHB's current environment and SAP monitoring is explicitly required.	Please provide the SAP landscape details, including SAP version, number of instances, modules, application servers and database platform, and clarify the expected depth of SAP monitoring.	We are using SAP ECC 6 EHP 7 with SQL Server database. We are using two instances CI & DI.
	16	**Cloud Monitoring** The RFP requires cloud monitoring.	Please provide details of the cloud platforms currently in use, including AWS/Azure/GCP, number of subscriptions/accounts/projects, resources and services that need to be monitored.	The cloud adoption strategy of the Bank is evolving, and cloud platforms and services may be onboarded during the contract period as per business and regulatory requirements.

	17	**AD Architecture** The RFP states: 3 domain controllers DC and DR Active-Active Writable + Read-only DCs Approximately 460 active users	Please provide the current AD topology diagram, domain/forest details, DC operating system versions, writable/RODC distribution, sites/subnets and DNS architecture.	Present Operating System is Windows Server 2016. However, same may be upgraded during period of contract. Present AD is single domain & single forest.
	18	**HRMS / IDAM Integration** The AD solution must integrate with HRMS/IDAM for automated joiner/mover/leaver workflows.	Please provide the HRMS and IDAM product names, versions, available APIs and expected provisioning/deprovisioning workflows.	Bank is PeopleSoft HRMS at present. No IDAM solution is deployed. However, more solutions may pe procured by the bank during period of contract.
	19	**MFA / SSO Scope** The RFP includes MFA for: Password reset Account unlock Windows macOS Linux VPN OWA SSO and SAML/OAuth/OIDC-based SSO.	Please clarify whether MFA and SSO are expected to be provided as native functionality of the proposed AD solution or whether integration with NHB's existing MFA/SSO platform is acceptable.	MFA and SSO should be native functionality of proposed solution.
	20	**AD Backup / Recovery** This is a significant requirement. The solution must support: Forest recovery Bare-metal recovery Object-level recovery GPO recovery FSMO recovery Isolated restore testing Clean OS recovery	Please clarify whether AD backup storage will be provided by NHB or should be included in the proposed solution. Also provide the required backup retention, RPO and RTO	Kindly refer RFP section 6.1. (21)
	21	**AD Log Retention** The RFP requires one-year retention within the solution and archival beyond one year.	Please specify the expected AD event/log volume per day and required archive retention period beyond one year for accurate storage sizing.	Approx 25 GB per month
	22	**Data Residency / Cloud Clarification** The RFP contains a strong requirement that the AD solution must not send internal data outside the Bank network.	Please confirm whether all proposed components must be completely on-premises and whether any SaaS/cloud-based management, telemetry, licensing or support components are permitted. This is very important when evaluating OEM products.	Please by guided by RFP
	23	**Patch Management – Air-Gapped Environment** The patch solution must support air-gapped/closed networks.	Please provide details of the air-gapped/isolated environments, number of endpoints/servers and expected patch distribution mechanism.	Present number of air-gapped/isolated desktops & servers are 10
	24	Patch Management – Third-Party Applications The requirement calls for patching 1,000+ third-party applications and database/middleware patching.	Please provide the expected list of third-party applications and confirm whether all 1,000+ applications are mandatory for Day-1 support or whether this is a product capability requirement.	Kindly refer corrigendum.
	25	. **OS Deployment Requirement** The patch solution unexpectedly includes: OS imaging Bare-metal deployment PXE Zero-touch deployment Profile migration	Please clarify whether OS imaging/zero-touch deployment is part of the mandatory implementation scope or only a required product capability.	Kindly refer corrigendum.
	26	**Remote Control** The RFP requires remote control with and without user consent. This has security implications.	Please clarify the operational and approval requirements for remote-control sessions without user consent, including audit, authorization, session recording and privileged access controls.	Please by guided by RFP
	27	**Existing ServiceDesk Plus** The RFP specifies: 10 technicians / 2,000 nodes + 3 additional technicians.	Ask NHB to provide: 1.Current ServiceDesk Plus version 2.Build number 3.Database type/version 4.Current architecture 5.Existing customizations 6.Number of active tickets 7.Number of business rules 8.Number of workflows 9. Number of integrations 10. Number of APIs 11. Current CMDB size 12. Current attachment/storage size	Bank is using Service Desk Plus Enterprise On-Premise implementaion. Version is 15.2 Build 15280.
	28	**ITSM Integration** The UEM must integrate with the existing ManageEngine ServiceDesk Plus On-Premise and provide: Bi-directional CMDB synchronization Auto-ticketing	Please provide the existing ServiceDesk Plus API/integration architecture and clarify the exact objects/fields required for bi-directional CMDB synchronization.	Kindly refer OEM provided API documentation.

	29	**OEM Requirement** NHB requires: OEM-backed support OEM escalation OEM support in India 24×7 support center in India Escalation matrix Back-to-back OEM arrangemen	Please confirm whether OEM support must be directly contracted with the bidder or whether authorized distributor/OEM partner support with documented back-to-back OEM support will be acceptable.	Please by guided by RFP
	30	. **Upgrade Risk** The vendor must provide: Major releases Minor releases Patches Feature enhancements during the contract at no additional cost, including implementation/professional services.	Please clarify whether major product version upgrades requiring architectural changes, additional compute/storage, database migration or professional services are included at no additional cost.	Please by guided by RFP
	31	**Audit Risk** The vendor must support VAPT/IS/RBI/regulatory audit observations and rectify gaps at no additional cost.	Please clarify whether audit remediation is limited to vulnerabilities/configuration issues directly attributable to the supplied solution, and whether remediation requiring product redesign, additional licenses or major architectural changes will be treated separately	Bidder has to to comply with observations pertaining to all supplied software components.
	32	**Acceptance Criteria** The RFP states that acceptance occurs after successful: Deployment Testing Validation Functional compliance Technical compliance Performance compliance	Please provide the detailed UAT/acceptance test cases, performance benchmarks, acceptance criteria and sign-off procedure for each solution. This is a very important question.	Bidder has to provide Compliance with all functional, technical, security, integration, reporting, and operational requirements specified in the RFP.
	33	**Training** **Requirements include:** Certified training for 5 NHB IT personnel General administrator training Resident engineer/location-specific training OEM configuration/training At least 3 days for UEM	Please clarify the number of training batches, participants, training location and whether OEM-certified training/examination/certification fees are included in the quoted price	Please by guided by RFP
Bidder 9				
	Section A - Enterprise Patch Management solution			
	Sr. No.	**Technical Specifications of Enterprise Patch Management solution**	**Remarks & Change request**	Bank Response
	2	Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc) and minimum 1000+ third party software natively - without a separate patching tool.	Solution is capable to any Database and middle ware patching subject to provide Ptach without any restriction . respective OEM like Oracle are restricting patch download thru their native tool only. Microsoft allows to download patch hence MS SQL patching is possible. Request to relax this point.	Kindly refer corrigendum.
	32	The solution must provide a centralised cloud dashboard for real-time patch compliance with endpoint health classifications (Healthy / Vulnerable / Highly Vulnerable) and drill-down to individual device patch status.	Cloud dashboard is available only cloud hosted solution, we are proposing on prem solution hence this clause needs to be removed.	Kindly refer corrigendum.
	63	Ability to patch databases (e.g., Oracle, MySQL, PostgreSQL etc) and middleware applications (e.g., Apache Tomcat, IIS, WebLogic etc)	repetition of clause 2.	Kindly refer corrigendum.
	92	Integration with existing ServiceDesk tools.	we can Rest API , existing solution OEM should ready to integrate.	Bank will provide access of API of Service Desk Plus.
	Sr. No.	**Technical Specifications Active Directory Management and Auditing Solution**		
	2	The solution should have a unified console where all the key features of the solution as per the specifications are available in the form of a centralized dashboard for ease of access and monitoring.	our solution has modular approach and architecture , Request to allow multiple console	Kindly refer corrigendum.
	3	The access to the GUI console(s) should have proper authentication and authorization mechanisms including Multi-Factor Authentication, Role Based Access Control (RBAC) etc. This should be applicable for the centralized/unified solution dashboard as well as any GUI consoles that are part of the supplied solution.	Request to remove centralized/unified console	Kindly refer corrigendum.
	6	Solution should have the feature to Audit Windows File servers, who, when, from where access the files.	Recommended to audit AD , Logon activity , AD Query & win file server. Request to add.	Please be guided by RFP
	Active Directory Auditing and event log management- recommendation			
			Solution should have Agent-based to (1) eliminate need native event logs, (2) allow for object protection, (3) optimized/configurable data transfer, and (4) real-time alerts , due to agent it can capture real time event at schema level not on log generation level . request to incorporate. Technically if any solution reads generated logs it should not be real time.	Please be guided by RFP

Bidder 10

S.No.	RFP Page No.	Relevant Clause of the RFP	Query	Bank Response
1	46	**Annexure –V - Minimum Eligibility** **Clause No. 4** Bidder should be profit making for two FYs in any of last four FYs i.e. FY 2021-22, 22-23, 23-24 & 24-25.	**We request NHB to modify the clause as under:** Bidder should be profit making /**Positive Networth** for two FYs in any of last four FYs i.e. FY 2021-22, 22-23, 23-24 & 24-25.	Kindly refer corrigendum.
2	47	**Annexure –V - Minimum Eligibility** **Clause No. 9** The bidder must have reported positive Profit After Tax (PAT) in at least 2 out of the last 3 completed financial years (FY 2022–23 to 2024–25)	We understand that said clause is repetation of clause No. 4 above, we request you to kindly remove the clause.	Please be guided by RFP
3	28	**Technical Bids (Marks Distribution), Clause No. 1** Total number of implementations/supports of IT Services Management Solutions by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points)	**We request NHB to modify the clause as under:** Total number of implementations/supports of **IT Services Management /NMS/EMS Solutions** by bidder. (Only Work Completion Certificate (upto last 10 years) will be considered for award of points)	Kindly refer corrigendum.
4	28	**Technical Bids (Marks Distribution), Clause No. 2** Number of years of experience of the bidder in implementation/support of IT Services Management Solutions	**We request NHB to modify the clause as under:** Number of years of experience of the bidder in implementation/support of **IT Services Management/NMS/EMS Solutions.**	Kindly refer corrigendum.
5	29	**Technical Bids (Marks Distribution), Clause No. 4** Total number of implementations of proposed Enterprise Patch Management solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India a. >=6 - 10 Marks b. >=4 and <=5 - 6 Marks	We understand that said clause will be met by proposed OEM, Kindly confirm.	Please be guided by RFP
6	29	**Technical Bids (Marks Distribution), Clause No. 5** Total number of implementations of proposed Active Directory Management & Active Directory Audit Solution solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India a. >=6 - 10 Marks b. >=4 and <=5 - 6 Marks	We understand that said clause will be met by proposed OEM, Kindly confirm.	Please be guided by RFP
7		**Technical Bids (Marks Distribution), Clause No. 6** Total number of implementations of proposed Unified Enterprise Management Solution in Govt. Sector/PSU/PSBs/FIs/Large Corporate* in India	We understand that said clause will be met by proposed OEM, Kindly confirm.	Please be guided by RFP
8		Additional Clause	We request NHB to include Below caluse In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations. In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank.	Please be guided by RFP
9	31	11.2 Payment Terms: Stage No. 1 **Schedule/Event:** After sign-off/go-live. Bank will provide sign-off subject to pre-deployment audit of the proposed solution by bank appointed external IS auditor. **Payment details/frequency.** 80% of Total Solution Cost (as per commercial bid format) will be released. 100% of Total Implementation Cost (as per commercial bid format) will be released. This payment shall be released after the mentioned compliance has been met.	We request bank to modify the clause as under: 70% payment will be made against delivery of proposed solution 20% Payment will be made against implementation 10% Payment will be made sign-off/go-live.	Please be guided by RFP
10	31	**11.2 Payment Terms:** Stage No. 2 **Schedule/Event:** At the end of every subsequent year (2nd year onwards) **Payment details/frequency.** 10% of Total Solution Cost		Please be guided by RFP
11	19	**Implementation schedule** Stage -1 - **Schedule of Delivery - Solution Delivery** **Timelines** - Within 15 days from the date of award of tender. **Stage -2** - **Schedule of Delivery -** Solution Delivery **Timelines -** Within 45 days from the date of award of	We request bank to modify the clause as under: **Implementation schedule** Stage -1 - **Schedule of Delivery** - Solution Delivery **Timelines** - Within 45 days from the date of award of tender. **Stage -2** - **Schedule of Delivery -** Solution Delivery **Timelines -** solution implementation in 75 days	Kindly refer corrigendum.
12	4	Centralized Manage Engine solution is implemented at DC, New Delhi, as EMS and to automate asset management and other infra management modules.	It is requested to kindly confirm the details of EMS solution implemented also confirm whether this EMS will be continued in integrated solutioning with ITSM or replaceed with ITSM.	Bank will continue to use Manage Engine Service Desk Plus. Remaining solutio viz. AD360, OP Manager, and Endpoint Central will be replaced as part of the scope of this RFP.
13	5	on-premises IT Services Management tools i.e. Enterprise Patch Management Solution, Active Directory Management & Active Directory Audit Solution, Unified Enterprise Management Solution with warranty, AMC, and Technical Support of the solutions at NHB's DC at New Delhi for a period of 3 years.	It is requested to kindly confirm that ITSM will be implemented at DC-Delhi/NCR only there is no requirement at DR Mumbai, please confirm	Bidder has to implement at DC. Kindly refer corrigendum for DR implementation.
14	6	6.1. Statement of Wok 1. Vendor is required to implement the mentioned tools at DC. The bidder shall ensure that the proposed solutions are technically capable of deployment in a Disaster Recovery (DR) environment, if required by NHB in the future.	As of now, the requirement is limited to the DC only. However, if required in the future, the same can be extended/implemented at DR location subject to cost considerations and technical feasibility/viability. Kindly confirm.	Kindly refer corrigendum.

15	7	18.Bidder must specify hardware requirements based on their understanding of the overall solution architecture based on requirement. The same must be documented and shared with NHB along with justification/reasonability. It is to be noted that NHB will provide virtual servers and not physical servers to meet these hardware requirements.	we understand that for hosting the below solutions, server in virtualized environment at DC Delhi/NCR on-prim will be in NHB scope, sify needs to share sizing only: 1.Enterprise Patch Management Solution, 2. Active Directory Management & Active Directory Audit Solution & 3.Unified Enterprise Management Solution. Please confirm	Bidder must specify compute requirement as per of Technical Bid. Bank will provide VM on HyperV/Vmware.
16	7	12. Vendor will depute requisite engineer onsite for smooth deployment within prescribed time schedule.	We understand that 1 RE onsite is required during project implementation stage only at DC/NCR Delhi during this phase only. Please confirm	Yes
17	7	21. NHB proposes to provide all necessary hardware infrastructure such as computing and storage capacity at DC & DR locations	Need clarity regarding the hardware infrastructure such as computing and storage capacity: This will be in Bidder scope. Only server will be provided by NHB as per point no 12 as mentioned above, please confirm	Bank will provide compute and storage only.
18	7	6.2. The proposed Enterprise Patch Management Solution shall have the following broad features: a) The solution should be licensed from Day-1 for the parameters below: I. Number of endpoints: 320 II. Number of servers: 180 III. Number of Administrator/technician resources: 4	Please confirm that these no of licenses are fixed at day1 but might get increase in due course of roadmap, please confirm	Yes
19	8	d) The key details of current Active Directory architecture of the Bank are mentioned below: RFP for Procurement and Implementation of IT Services Management Solutions I. Domain controllers are equally distributed across DC and DR sites of the Bank in Active-Active mode. Setup consists of both writeable and read only domain controllers. ii. Domain controller servers are being used as DNS servers in all endpoints and servers.	Please confirm: 1.Operating system and sizing of existing Writable and Read-Only Domain Controllers deployed at the DC and DR sites. 2.DNS services are AD-integrated and whether DNS is hosted exclusively on the Domain Controllers or if any dedicated/additional DNS servers are also deployed.	1. Present Operating System is Windows Server 2016. However, same may be upgraded during period of contract. 2. DNS is hosted on Domain Conroller.
20	10	The Bidder should configure and size the solution to retain all the logs from Active Directory solution for duration of 1 year within the supplied AD Management solution. The solution should have provision to archive the Active Directory log data beyond one year and store the same in external backup storage for the duration of the contract period.	Please clarify whether the external backup storage for AD logs beyond one year will be provided by NHB or is it required to be sized and supplied by the bidder. Please confirm	Bank will provide compute and storage only.
21	10	The Bidder should ensure that Artificial Intelligence/Machine Learning capabilities are available in the supplied solution and configured as per requirements of the Bank for identification and reporting of suspicious behaviour, login patterns etc.	Please clarify whether AI/ML functionality is required to be fully on-premise or whether any OEM cloud/SaaS dependency is permitted.	Please be guided by RFP
22	10	The solution should be licensed from Day-1 for the parameters below: a. Number of devices for monitoring: 400 b. Minimum Number of Administrator/technicians resources: 4 c. Number of network devices for configuration	Please confirm the Device-wise breakup of the 400 monitored devices and 80 network devices to enable us to accurate sizing/licensing.	Devices of monitoring includes Servers, Firewall, ESXI, NetApp & Hitachi Storage, Switches etc.
23	11	Maintenance & Technical Support services for Manage Engine Service Desk Plus solution:	We understand that this is the running Solution at NHB, please confirm that whether other equivalent OEM Solution can be proposed or not.	Maintenance & Technical Support services for Manage Engine Service Desk Plus solution is to be provided by bidder.
24	11	b) The bidder shall provide three (03) additional technician licenses for the existing ServiceDesk Plus deployment. The licenses shall be fully compatible with the currently deployed version and architecture of the ServiceDesk Plus solution. The bidder shall carry out installation, activation, integration, migration (if required), and configuration of the additional licenses, ensuring seamless operation without disruption to existing services. Support and subscription services for the additional licenses shall be provided throughout the contract period. The scope shall include OEM-backed support, software updates, version upgrades, troubleshooting, performance optimization, configuration assistance, and incident resolution, training, VAPT/audit observations closure as applicable etc	Please clarify whether OEM support/subscription renewal costs for the existing ServiceDesk Plus environment are included in the bidder's scope. Also provide the existing architecture of Manage Engine with process flow. Please confirm	Bank is using Service Desk Plus Enterprise On-Premise implementaion. Version is 15.2 Build 15280. OEM support/subscription renewal costs for the existing ServiceDesk Plus are included in bidder's scope.
25	11	6.6 One contact number for all support (user/technical) needs would be preferred. Vendor should provide the address and telephone number for the general customer/ technical support location at Delhi/NCR.	Need clarity wrt to this clause, what is the expectation from Bidders , whether to provide only Support contact or manpower need to be deployed to manage calls on-prim or from remote, please clarify.	Please be guided by RFP
26	98	Real-time or interval-based patch deployment status monitoring.	We understand that the requirement for centralized monitoring at DC Delhi , please clarify whether the Patch Management cloud dashboard is permitted. Also confirm that this reporting tool deployment required in HA as Active-Passive mode or standalone deployment.	Standalone deplyment is required at DC only. For DR implementation, kindly refer corrigendum. Proposed solution should be on-premise.
27	106	34.Solution should support incremental backups for Active Directory Forest/specific domain controllers such that the full backup is not required to be taken on each cycle	Please confirm that backup repository/storage, recovery infrastructure and associated compute/storage resources will be provided by NHB.	Bank will provide compute and storage only.
28	108	The event log retrieval and reports should ensure that the data from all domain controllers are provided as a unified report and there should not be a need to separately query for each domain controller and manually consolidate the logs	Please provide the number of domain controllers, estimated events/sec and current AD log volume so that the bidder can accurately size the proposed AD auditing solution	At present 3 domain controllers are implemented. Total monthly AD log volume is approx. 25 GB.
29	General	General	Please confirm : 1.Power/Rack/Earthing other passive infra if required will be provided by NHB at DC required for deployment of solutions.	yes
Bidder 11				

	S. No.	Relevant Clause of the RFP	Query	Bank Response
	1	**Section C - Unified Enterprise Management Solution** **Point No.3** The Proposed Solution should support both Windows and Linux OS for deployment, and should be 64-bit application to fully utilize the server resources on which it is installed.	As each OEM may have its own deployment architecture and may support either Windows or Linux operating systems, restricting the deployment to specific operating systems may limit participation from otherwise qualified OEMs. Therefore, we request the authority to kindly modify the clause to allow wider participation. Suggested Clause: "The proposed solution should support **deployment on either Windows Or Linux** operating systems and should be a 64-bit application to ensure efficient utilization of the available server resources."	Kindly refer corrigendum.
	2	**Section C - Unified Enterprise Management Solution** **Point No.11** The proposed solution must be a natively unified observability platform, to seamlessly integrate full-stack monitoring, log analytics, application performance monitoring (APM), flow analytics, compliance tracking, netroute tracing, and telemetry correlation within a single cohesive system—without requiring any third-party plugins, tool-switching, or modular bolt-ons.	NMS and APM are distinct solution components, each addressing different monitoring requirements. Mandating a single URL for both NMS and APM may restrict MII OEMs that provide these capabilities as separate but seamlessly integrated solutions. To encourage wider participation and allow flexibility in solution architecture, we request the authority to kindly modify the requirement to allow NMS and APM to be offered as an integrated suite, with the capability to provide unified visibility and seamless integration between the two solutions.	Kindly refer corrigendum.
	3	**Section C - Unified Enterprise Management Solution** **Point No. 20** All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring	To allow wider participation, we request that the clause be modified to allow modules from the same OEM or different OEMs, provided they are tightly integrated and provide a single-pane-of-glass view. **However, the complete solution ownership and accountability should remain with a single OEM**. So we request you to modify the clause as: All the required modules **should be either from same OEM or should be tightly integrated** for single pane of glass view of enterprise monitoring	Please be guided by RFP
	4	**Section C - Unified Enterprise Management Solution** **Point No.4** The proposed EMS solution must comply with the following standards: 27034-1 for application security, ISO 27001:2022 for information security management, GDPR or DPDP for data privacy, and SOC 2 Type 2 for service organization controls. This ensures robust security, regulatory compliance, and comprehensive data protection across all managed network operations. Valid supporting documents must be submitted with the bid.	We request that the clause be modified to **allow SOC 3, SOC 2 or higher certification**, as SOC 2 reports may have sharing restrictions and may only be provided under NDA. This will enable wider participation while maintaining the required security assurance.	Kindly refer corrigendum.
	5	**Section C - Unified Enterprise Management Solution** **Point No.19** The system must not use any open-source third-party relational or time-series databases for reporting data. It should use a native, proprietary-built reporting database for high-speed, high-volume observability workloads and security constarins.	We request that the clause be modified to allow standard databases such as PostgreSQL, MySQL, MS SQL, MongoDB, or equivalent, instead of mandating a proprietary database, to enable wider participation.	Kindly refer corrigendum.