Appendix 1B- Technical Specifications - Scoring Sheet

Instructions of Filling up of Appendix 1

BC	Description
Yes	Bidder's solution complies to this and/or provides this feature.
No	Bidder's solution does not comply to this and/or does not provide this feature.

Marks for specifications for will be allotted against the responses to each of the point mentioned as per the following marking pattern:

Scale	Description
10	Yes
0	No

Sheets will be scored on Yes/No compliance by the bidder. Yes/No responses will be marked as per the above table.
Each line item in the technical specifications sheet mentioned in Appendix 1B carries 10 marks. The marks allotted to the responses of the Bidder by the NABFINS, would be reduced to a scale proportionate to the marks allocated for the technical evaluation. It is important for the bidder to score 100% marks in Technical Specifications.

Notes

1	Bidder is expected to provide for all requirements irrespective of the functionality of the solution proposed. Hence the overall cost must include all the requirements where the rank provided is Yes.
2	In case the Bidder fails to provide a " Bidder Compliance" against any of the line items the response would be considered as incomplete and may not be scored, at NABFINS's discretion
3	Bidder is expected to provide the response by filling up the columns "Bidder' Compliance (BC)" and "Bidder Remarks" only. Bidder is advised not to make any changes to any information on the RFP documents for example insert a row or delete a row or modify any other information like change the functionality required, etc.
4	Every requirement needs to be treated as an individual requirement and should not be clubbed with any other requirement and the Bidder needs to provide a "Bidder's Compliance" for that individual requirement, in case the Bidder clubs the requirements the response would be treated as incorrect
5	The Evaluation Committee decided by the NABFINS would be marking this annexure already scored by the bidder and would be appropriately assigning the final marks. The NABFINS will have the discretion to change the marks against the Bidder's scored line item if the bidder/OEM is not able to showcase the same in Product walkthrough or Presentation.
6	The marks allotted to the responses of the Bidder by the NABFINS after carrying out the above steps above would be reduced to a scale proportionate to the marks allocated for the functional & technical evaluation for the respective module. It is important for the bidder to score 100% of the marks in the Technical Specifications

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]
1	Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter outside the boundaries of the country. The CSP will be bound by Indian law, Indian IT Law, and the applicable regulations. No data in any circumstances should be shared/copied/transmitted without' s consent/written permission of the NABFINS and it should be as per the Indian IT Law, RBI guidelines, NABFINS & NABARD policy & guidelines and other regulatory & statutory body in India	
2	The bidder will be responsible for provisioning of requisite network infrastructure (including switches, router, firewalls, load balancers, SFPs, other devices and anicilliary infrastructur) to ensure accessibility of the proposed infrastructures and applications at all time as per defined SLA's. **All the equipment's/Devices in the path must be in HA mode with no single point of failure.**	
3	CSP should have a multi-site infrastructure setup, with network performance between them sufficient to accomplish replication, so that NABFINS can architect for high availability with defined RTO and RPO.	
4	The bidder is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the bidder under this RFP.	
5	The proposed CSP should provide the Automated Disaster recovery for automated switcover to secondary site in case of failover, the same should be tested regulary during the DR drills performed on Quarterly basis or as directed by NABFINS	
6	The bidder shall provide NABFINS with the necessary logs for the services for security monitoring and incident alert management.	
7	Bidder shall provide interoperability support with regards to available APIs, data portability etc. for to utilize in case of change of bidder, migration back to in-house infrastructure, burst to a different cloud bidder for a short duration or availing backup or DR services from a different bidder.	
8	The bidder and CSP should adhere to the relevant standards published (or to be published) by DeitY/MeitY or relevant standards body setup or regulator like RBI, SEBI, AMFI / recognized by Government of India and notified to the bidder or CSP by DeitY/MeitY/SEBI/AMFI/RBI/or by any institution recognized by Govt. of India as a mandatory standard and/or regulations.	
9	NABFINS will have right to audit the data center facilities of CSP through any regulators or through any third parties as needed by the regulators and this may entail data localization, sovereignty, confidentiality, Data protection & data privacy, and such other things. It's bidder responsibility to enable the same, necessary provision should be incorporated by bidder with CSP to ensure the compliance to the same. The bidder should provide CSP's third-party audit reports on information security & data integrity, source code review including APIs, details about APIs encryption of payloads, authorization, and authentication API wise - every year irrespective of any audit on demand.	
10	The bidder shall ensure to protect confidential information from unauthorized disclosure and use	
11	Each of the environments provided should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment and setup such that users of the environments are in separate networks.	
12	Bidder is responsible to organize periodic trainings to NABFINS IT staff with latest relevant cloud services. Periodic security awareness training should be conducted for bidder's and NABFINS personnel involved. periodicity shall be defined by NABFINS and bidder for the updates/patches received Bidder shall also define metrics for periodically measuring performance and effectiveness of information security awareness level of the involved personnel from NABFINS and bidder	
13	If Indian government demand is received for any data, the process mentioned below has to be followed: a. Disclosure of data of any kind on legal/statutory compulsion should be done only after obtaining concurrence from the NABFINS b. Resist illicit demands that are invalid which are not permitted by the Indian Government or Indian IT Law or any other Indian Regulatory Authorities.	

14	Solution should have capability to provide Alerts & Monitoring interface. Solution should support Remote Administration for administrators.	
15	Solution should have Capability to integrate with the authentication servers (LDAP/ADFS etc.) and Integration with applications using API.	
16	The cloud infrastructure should have presence in at least 2 cities in India	
17	The solution should be encrypting data both at rest, data in motion, and in transit with SSL/TLS (minimum TLS 1.2).	
18	The Service uptime agreement for the proposed solution should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	
19	The same Service Level Agreement should be applicable to all included or related services or components that is required for the solution to be contracted for the requirement.	
20	The proposed solution should also have Service level commitments for virus detection and blocking, spam effectiveness, false positives as well as email delivery.	
21	Bidder to perform regular backup and recovery tests.	
22	Bidder to ensure that CSP's personnel controls are in place to provide a logical segregation of duties.	
23	Measured Service: Resource usage should be monitored, controlled, and reported; providing transparency for both the Bidder and NABFINS of the utilized service. Bidder should have reporting mechanism to measure the service/performance/availability level criteria as in SLA while billing or as an when NABFINS requires.	
24	**Resource pooling:** There must be a logical separation between each consumer's computing resources and network using virtualization and VPNs or other techniques . Bidder should provide details on how to segregate and protect NABFINS's data from other customer data and NABFINS applications in cloud environment.	
25	Bidder should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to NABFINS as and when asked by NABFINS. Bidder should provide confirmation to the NABFINS that NABFINS's data is rendered permanently inaccessible and the same should not remain available in any backup or distributed online media after exit of the contract.	
26	Bidder should provide right to audit the data centers in India. In addition: a. NABFINS's data should not cross Indian geographical boundaries (physically or logically). b. NABFINS must have "Rights to Audit" the CSP's compliance with the agreement including rights of access to the CSP's premises where relevant records and NABFINS's data is being held. c. Audit rights for the NABFINS or its appointed auditor (nominee) or regulators should be integral clause in agreement. d. Integration of all devices with NABFINS's SOC, SIEM & other security solution for monitoring as and when required by NABFINS. e. NABFINS should have access/ monitoring mechanism for Privilege user access (of CSP) to cloud based systems.	
27	**Security:** a. Virtual environment security: It includes resource allocation, hardening of OS, VM image encryption, VM monitoring, USB disabling on VMs, VM should be kept on dedicated partition and IP addresses should not be shared. b. Encryption and Key Management: Depending on sensitivity data is to be encrypted, transport layer encryption is to be ensured using SSL, VPN Gateway, SSH and TLS encryption. End-to-end process for managing and protecting encryption keys to be established and documented. Compliance is to be ensured on ongoing basis. c. Monitoring: Devices should be integrated with NABFINS's SOC, if so desired, for continuous monitoring for access monitoring, threat monitoring, audit logging, system usage monitoring, protection of log information, administrator and operator log monitoring, fault log monitoring d. The bidder shall provide the artifacts, security policies and procedures demonstrating its and CSP's compliance with the Security Assessment and Authorization requirements.	

28	In addition to Cloud Security (which includes protection of cloud data, support regulatory compliance & protect customers' privacy), the information security controls including change management, identity and access management, cryptographic controls, network security, data security, vulnerability management, virtualization security, Business continuity, incident management, log monitoring etc. should be implemented by on Cloud by CSP at all locations	
29	Controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS, DB, Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements and any other as required by NABFINS on cloud.	
30	Reverse Data Shifting: In the event of completion of the contract in normal course or on termination of contract, bidder shall shift the data back to NABFINS or any of its designated 3rd party's on-premises/ cloud hosted infrastructure. The bidder should sort out operability issue, if any, for smooth shifting of such data.	
31	NABFINS shall be evaluating the operations of the cloud services subscribed & implemented & effectiveness of security controls in the Cloud Computing environment, bidder should enable NABFINS in monitoring the same by providing requisite access, periodic reports, and management Information & dashboard material for reporting on control assessments	
32	The bidder should ensure Data segregation, confidentiality, privacy controls setup in line with the NABFINS's requirement	
33	In case of Exit/ change of CSP, bidder to ensure the following while formulating the exit plan i. Removal of all NABFINS's data on the cloud and assurance that all data has been rendered irrecoverable, upon termination of the cloud outsourcing arrangement in a time-bound manner. ii. Bidder shall detail out procedures to be used for deletion/destruction of data in a manner that data is rendered irrecoverable. iii. Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media). iv. Transferability of cloud outsourced services to a third party, another CSP or on premise to the NABFINS for continuity of service. v. The format and manner in which data is to be returned to the NABFINS, as well as support from the CSP to ensure accessibility of the data.	
34	Cloud architecture shall account for and shall be submitted by bidder regularly at periodic interval to NABFINS: a. Type of workload, b. Requirements of availability and resiliency, c. Security, d. Authentication, e. Performance, f. Operations and management. g. Logical segregation	
35	Security should be implemented at all layers i.e., Physical, Network, Data, Application, etc., of cloud architecture with multiple security controls.	
36	NABFINS's data should be isolated from other customers, to avoid comingling of data and application	

37	Cloud workload is protected against network-based attacks by implementing controls such as: a. Network segregation of workloads on the cloud shall be implemented based on their type (production, test, development) and purpose (user, server, interface, critical infrastructure segments etc.). b. A dedicated security network segment (landing segment) shall be implemented for terminating all ingress traffic to the cloud. c. All internet traffic to the workload on cloud shall be routed through DMZ. Other network segments in the cloud environment shall not have direct access to the Internet. d. Micro Segmentation shall be implemented on the cloud. e. All network segments in the Cloud environment shall be protected with security controls such as Firewall, IPS/IDS, anti-DDoS, AV, DLP, WAF, NAC etc. f. Direct network connection with cryptographic controls shall be implemented to secure the traffic between the cloud and on-premises environment.	
38	Implement principle of selective privileges and impose segregation of duties with appropriate access and authorization: a. To manage access rights to cloud services by the NABFINS's users, the CSP should provide user access management functions to the NABFINS. b. Segregation of privileged users and their activities must be documented. Access Control and Role Conflict Matrix to be defined and implemented. Access to Master/ Admin account for Cloud deployment shall be used by exception and shall not be used for operational activities. c. Multifactor authentication shall be implemented for user access to critical workloads and for all privileged access on the cloud. d. Users with privileged system access shall be clearly defined and regular user access reviews, at least once every three months, shall be conducted. e. Remote access by administrators and privileged users to the cloud environment over the Internet, shall not be permitted. f. In case of workloads providing compute resources over the Internet, remote access security measures such as two factor authentication and Virtual Private Network (VPN)/ encryption shall be implemented. Cloud-based virtual machine instances with a public IP shall not have open Remote Desktop Protocol (RDP)/Secure Shell Protocol (SSH) ports. Any system with an open RDP/SSH port shall be placed behind a firewall and require users to use a VPN to access it through the firewall. g. Cloud Service Provider/ Cloud Management Team should not have access to any application data of the NABFINS. h. Conditional access should be implemented for privileged users. i. Legacy authentication protocols should be disabled.	
39	To ensure confidentiality, integrity and non-repudiation of data-in-transit and data-at-rest, encryption controls in line with NABFINS's Cryptographic Policy, shall be implemented to secure data stored/processed/ transmitted in the cloud including data backups and logs. a. Critical/ sensitive data including PII/ SPDI, card holder data or account numbers shall be masked or encrypted. b. NABFINS shall have an option to implement 'Bring Your Own Key' as and when required. c. In case cloud based HSM is used, it should meet the FIPS 140-2 Level 3 and above criteria. d. HSMs and other cryptographic material should be stored on segregated secure networks with stringent access controls. e. In case CSP's keys are being used for encryption of NABFINS's data, such keys should be unique and not shared by other users	
40	Retention of NABFINS’s data on the cloud shall be in accordance with the extant guidelines of NABFINS’s Data Retention Policy.	
41	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to NABFINS on a period interval	
42	Secure Software Development Lifecycle (Secure SDLC) shall be followed for all applications in the cloud throughout the application lifecycle. Security assurance certificate shall be provided by the bidder to the NABFINS for applications provided by CSP/ Third Party.	
43	Secure Cloud APIs shall be implemented to develop the interfaces to interact with cloud services. Application integration and information exchange should happen over secured API channels.	

44	The systems in cloud infrastructure should be periodically updated with the latest anti- malware signatures, the bidder shall submit the period report on the same with NABFINS	
45	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with NABFINS on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	
46	File integrity monitoring should be implemented in order to ensure authenticated changes and to detect unapproved changes to files.	
47	Password Policy on the Cloud setup should be minimum as per the NABFINS's password Policy. For privileged users, it should be more stringent than that for normal users.	
48	Mechanism shall be implemented to detect service faults or outages in the cloud environment.	
49	Appropriate Business Continuity Plan and Disaster Recovery Plan shall be put in place for the workload on the cloud, based on the risk assessment. Bidder shall incorporate the business continuity requirements of the NABFINS in its BCP and DR Plan for NABFINS's workload. In case of critical workloads, bidder's or CSP's plans should be shared with the NABFINS	
50	Change/Configuration management procedures shall be aligned with the NABFINS's Change Management policy, including change request, approval procedures and notification mechanism.	
51	The cloud infrastructure should be periodically updated with the latest patches and assurance for the same shall be shared by bidder periodically (once in three months or as per NABFINS's discretion).	
52	Secure configuration settings related to OS/ database/ network devices/ virtual machines/ middleware should be implemented as per NABFINS's SCD or equivalent hardening guidelines.	
53	Audit logging should be enabled on all systems on cloud. An audit trail of user access event logs should be maintained to ensure compliance towards regulatory requirements. Duration of retention of Log & data in cloud should be in accordance with extant Data Retention Policy of the NABFINS.	
54	All logs of assets related to NABFINS's subscription/ tenant should be integrated with the NABFINS's SOC (as and when required). Report should be submitted at periodical intervals as defined by NABFINS or on Quarterly basis (before every billing cycle)	
55	Bidder shall regularly monitor the use of cloud services, forecast capacity requirements, and accordingly normalize the resources, post approval from NABFINS, to prevent information security incidents caused by resource shortages /malfunctions. Logical and detailed explanation along with the requirement should be provided for performance and capacity linkage and accordingly resources normalization should be submitted to NABFINS	
56	Roll-out / phasing-out of applications to / from cloud should follow the Data Migration Policy of the NABFINS.	
57	For secure deletion/destruction of data: a. Do not use Cryptographic Erase (CE) to purge media if the encryption was enabled after sensitive data was stored on the device without having been sanitized first. b. Do not use Cryptographic Erase (CE) if it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption.	
58	Information Security Awareness (including NABFINS's policies), education and training programs should include secure best practices for usage of Cloud, Cloud specific risks etc. to relevant stakeholders.	
59	Evidence of periodic security assessment of cloud environment such as Threat & Vulnerability Risk Assessments or equivalent or independent security assessments, should be provided by bidder at Quarterly intervals and/or as required by NABFINS.	
60	Periodic Security Assessments shall be performed to identify and mitigate risks in the Cloud setup and evidence for the same should be provided to the NABFINS.	
61	Bidder should arrange to ensure that periodic Vulnerability Assessment and Penetration Testing (VAPT) on periodic basis is performed on assets provisioned for NABFINS in cloud infrastructure at Quarterly intervals or as required by NABFINS.	

62	Comprehensive Security Review (CSR) of the application/service on the cloud shall be conducted on yearly or bi-yearly or as defined by NABFINS basis depending on the type of workload. Information security reviews should be conducted in case of transition or changes of bidder or CSP or during renewal of services	
63	Information security incident management process shall be established to discover, report, respond and prevent information security events and weaknesses effectively by bidder and CSP	
64	Security incidents should be notified to the relevant stakeholders and escalated in accordance with an escalation matrix and timelines formulated as per the criticality of the workload and in accordance with regulatory and extant guidelines.	
65	Requirements for forensic investigation including mechanism for acquisition of log data from CSP should be documented and reviewed & approved by NABFINS. Bidder shall provide reasonable access to necessary information to assist in any Forensic investigation arising due to an incident in the cloud	
66	The IS controls' implementation should cover all locations that support NABFINS's data storage and/ or processing requirements.	
67	Bidder to regularly and/or as per the frequency defined by NABFINS should submit evidence of conducting DR drills, and lessons learnt and their detailed recordings.	
68	Default admin and root users should be deleted/disabled, and access should be based on user specific IDs and all such accesses should be logged	
69	Bidder should deploy Active Directory (AD), Single Sign On (SSO) and strong Password Policy for End point and application access	
70	Proper access control is to be defined for protecting NABFINS data and access to the Data is strictly on Need-to-Know Basis	
71	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by NABFINS	
72	Bidder confirms and agrees the following: a. Right to audit to NABFINS with scope defined. b. Right to recall data by NABFINS ie., that is data removal (soft/permanent) from CSP systems. c. System in place of taking approvals for making changes in the application. d. Regulatory and Statutory compliance at vendor site. e. IT Act 2000 & its amendments, and other Acts/Regulatory guidelines f. Availability of Compensation clause to fall back upon in case of any breach of data (confidentiality, integrity, and availability), or incident that may result into any type of loss to NABFINS. g. No Sharing of data with any 3rd party without explicit written permission from competent Information Owner of the NABFINS including with the Law Enforcement Agency (if applicable), etc.	

73	CERT IN Empaneled auditor report's is required for the following: a. CSP's environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall and any access from an external entity is permitted through DMZ only b. CSP follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT c. Internet access is restricted on: Internal servers, database servers, Any other servers d. Ensuring security posture of their applications. Security Testing includes but is not limited to Appsec, API Testing, Source Code Review, VA, PT, SCD, DFRA, Process Review, Access Control etc. e. CSP has processes in place to permanently erase NABFINS data after processing or after a clearly defined retention period f. Log generation, storage, and review process to confirm whether proper log generation, storage, management, and analysis happens g. Whether the CSP has witnessed any security or privacy breach in the past 2 years	
74	If Indian government/RBI/Regulatory & statutory body demand is received for any data, the process mentioned below has to be followed: a. Disclosure of data of any kind on legal/statutory compulsion should be done only after obtaining concurrence from NABFINS. b. Resist illicit demands that are invalid which are not permitted by the Indian Government or Indian IT Law or any other Indian Regulatory Authorities	
75	Process and policies should be in place to stop by bidder and CSP and control data downloading/copying. The process and policies should be shared with NABFINS on regular interval or as desired by NABFINS. Data should not be allowed to be downloaded or to prepare copies unless explicitly approved by NABFINS.	
76	Information security controls implemented by bidder and any third party (if any) must be at least as robust as those which the NABFINS would have implemented had the operations been performed in-house. Such implementation should cover all locations that support NABFINS's data storage and/ or processing requirements. Certificate of Assurance supported by suitable evidence should be submitted by bidder, regarding status of controls implemented at all locations. In case of a single evidence/report, assurance that controls are consistent across all relevant locations processing/storing NABFINS's data should be obtained.	
77	Data must not be shared with outsiders without explicit & case specific approval of NABFINS. Data should not be allowed to be downloaded or to prepare copies unless explicitly approved.	
78	The key used by the vendor to encrypt NABFINS data should be different i.e., it should not be the same that was/is used for other clients	
79	CSP should ensure proper log generation, storage, management and analysis happens for the 3rd Party/Vendor application (including DFRA & access logs)	
80	CSP should have captive SOC or Managed Service SOC for monitoring their systems and operations	
81	Any/all decision pertaining to the proposed & provisioned applications and/or infrastructure and/or tools and/or services shall be obtained from NABFINS prior to provisioning	
82	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for NABFINS. Evidence of dedicated infrastructure (physical/logical) for NABFINS should be submitted.	
83	Rules are implemented on Firewalls of the 3rd Party/Vendor environment as per bidder approved process and rules & process are reviewed periodically.	
84	The Primary & secondary should be physically separate and should be at two different locations. Address of the same has to be provided in technical proposal	
85	Bidder should have in place procedures for emergency changes, including the roles and responsibilities, and that shall be documented.	

86	Mechanism shall be implemented for apprising details of sub-contracting of workload and periodically notifying changes in sub-contracting by CSP to NABFINS	
87	CSP should have Risk Framework in place for cloud adoption shall include but not be limited to following checks: · Type of service being outsourced · Application criticality · Classification of data · Cloud service model · Cloud deployment model · Data localization requirements and Laws affecting cross-border data transfer and storage · Legal, regulatory and compliance requirements · Data availability and recovery requirements · Data recovery in case of disaster and in case of contract termination · Feasibility to audit/review IT controls of the third party (CSP) or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets NABFINS's information security requirement. · Global security practices · Applicable threats, its likelihood and corresponding impact · Data segregation, confidentiality, privacy controls at the third party (cloud) · Sub-contracting · Continuous monitoring requirement · Exit strategy	
88	Bidder shall assist NABFINSs and provide all necessary documents and data for conducting Bidder's risk assessment during on boarding, periodically during life cycle and upon termination/transition of services.	
89	Threat Modelling of all activities being performed by CSP & bidder should be documented and should be shared with the NABFINS on periodic basis	
90	Bidder's and CSP also confirms that NABFINS reserve the right to Audit the premise/offices of any of its sub-contractor involved in the project as and when required by NABFINS	

TABLE B: Technical compliance		**Compliance [YES/NO]**
Architecture		
a)	The architecture of the system should follow modular application architecture that emphasizes separating the functionality of applications in independent services. All the components of the application should have the ability to be reused and replaced without affecting the rest of the system fostering agility, efficiency, and resilience.	
b)	The system should support cloud delivery model as this approach will allow to redeploy parts of or all the application to a cloud platform, whenever required.	
c)	The system must comply with organization's guiding principles & standards for enterprise information security/system architecture	
d)	The system must be optimized to minimize their power and memory footprint for better performance	
e)	Every design decision of the applications should take into account the optimum use of CPU, memory	
f)	System must be designed to be efficient, scalable, manageable, fast, frugal with resources, compos-able and SOA-style self-contained	
g)	The application architecture must be modular with different modules performing logically discrete functions, all modular services developed separately and composed together to construct an executable application program	

h)	The data architecture must classify data in a number of ways: function, purpose, structure, confidentiality, sensitivity	
i)	The solution should have a native support for cloud deployment model	
j)	The solution should have detailed, periodically updated data dictionary	
k)	Infrastructure diagrams, Security & network architecture, data flow diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution. The same is to be submitted to NABFINS at regular interval and as & when there is a change in the design & architecture by bidder and/or CSP	
Platform and Solution		
l)	Periodic benchmarking of proposed solution as desired by NABFINS	
m)	The solution should support to customize the product for different jurisdictions as per the local Regulations as well as client needs.	
n)	Solution is platform agnostic.	
o)	The Bidder shall deploy the solution in dedicated cloud instance procured in the name of NABFINS for hosting the application.	
p)	An administrator console to the NABFINS to implement/manage/change organization level archival, retention and Backup policies.	
q)	Browser software should support basic authentication, session authentication, active content filtering, additionally it should be designed to work well with supported proxy servers and virtual private network solutions	
Scalability and Performance		
r)	The solution should support dynamic elasticity to cope up with the change in user loads.	
s)	The solution should support horizontal and vertical scaling to meet the NABFINS's future requirement.	
t)	Scaling process to be clearly defined by the Bidder and should not involve any code changes.	
u)	The number of users who all are utilizing the Software Solution overall as well as at a given point in time should be available as a dashboard.	
v)	Ability to scale linearly	
w)	Solution should be able to scale to accommodate future usage loads, such as load balancing, clustering, support for additional CPU cores etc.	
x)	Solution should meet performance standards regardless of the location within India	
y)	Capability to handle sub second response time	
z)	Allow for high capacity to carry out transactions during high volume period	
Security		
aa)	The solution should comply with the security guidelines & principles of NABFINS, RBI, regulators and GOI	
bb)	Data should be protected at rest and in motion	
cc)	Secure mechanisms and protocols must be used for authentication	
dd)	When the application fails, it should fail to a state that rejects all subsequent security requests	
ee)	Every failure must be handled as per Risk Management Policy	
ff)	Application must be designed to recover to a known good state after an exception occurs	
gg)	A global error handler must be designed to catch unhandled exceptions and an appropriate logging and notification strategy must be designed	
hh)	Client account, transaction data or any sensitive information is encrypted when in motion and at rest.	
ii)	Solution should be implemented in higher security standards like Virtualization, Segregation of Servers, and compartmentalization. Secured Coding Practices, OWASP etc. to ensure 100% security of the Solution	
jj)	Client account, transaction data or any sensitive information is encrypted when in transit.	
kk)	Solution should comply with the IT Security Policy, Cyber Security Policy, and IT Policy of the NABFINS	
ll)	Encryption to be used for API, data traveling between platform and other interfacing applications. Integrity of data to be maintained at 100% of time.	

mm)	The Bidder shall create adequate controls ensuring that, when exception or abnormal conditions occur, resulting errors do not allow users to bypass security checks or obtain core dumps.	
nn)	The solution should be compliant with DC/DR strategy of NABFINS	
oo)	All the components of proposed solution (software, etc.) in the Primary site should be replicable at the secondary site (except for test and development environment).	
pp)	The proposed solution should have full capability to support database- database and storage-storage replication between primary and secondary site with a recovery point objective (RPO) and a recovery time objective (RTO) of the NABFINS.	
qq)	The replication between Primary site and secondary site should be possible in both directions.	
rr)	Support real time replication of data from production site to secondary site and permit manual and automatic shift of the application to the secondary site.	

TABLE C: Other Requirements		**Compliance [YES/NO]**
	Licensing and implementation requirements	
1	The solution can be put to use at NABFINS, NABFINS branches, Subsidiaries and associates (current and future)	
2	The solution should be deployed in Development, Test, training and Production (primary & secondary) and there should not be any restriction on the number of instances / deployments / users based on the licenses and any other limitation quoted in Commercial Bid	
	Support and Maintenance	
4	Bidder should fix bugs identified during the period of contract at no additional cost to the NABFINS.	
5	Bidder should warrant all the software against defects arising out of faulty design, workmanship etc. throughout the contract period.	
6	Bidder should ensure availability of technical expertise and SMEs to extend continuous support to the on-site team.	
7	Bidder will be responsible to manage day-to-day operations, system administration & maintenance, system support, troubleshooting, technical support, patching, configuration, deployment, change & release management, and support (L1, L2 & L3) and cloud-based DR & BCP activities.	
8	Bidder should resume operations from an alternate site with minimum downtime whenever required	
9	Bidder in consultation with NABFINS will decide on the Change Requests (CR) to be taken up for coding and estimate the man days required for each CR and prepare a User Requirement Document (URD). After URD approval from NABFINS, Bidder team will start working on the CRs. If URD is not available, Bidder team will start working on the approved CR.	
10	Bidder should perform system performance monitoring and publish uptime reports at the frequency desired by the NABFINS.	
11	Any change / upgrade / solution modification / patch suggested by the Bidder will be first communicated and discussed with the NABFINS; only after the confirmation and acceptance by the NABFINS shall it be applied to the production environment.	
12	Audit Trail - All transactions should be securely logged to detect any modifications.	
13	All historical records of deviation along with user audit trail should be logged for future reference.	
14	All overrides for credit approval or rejection should be logged to create audit trail that can be tracked.	
15	History of each parameter change should be logged.	
16	Users should be able to access audit trails of all the transactions, modifications/changes for audit purpose.	
	Reporting	

17	The system should support all the different reporting requirements of the NABFINS that includes MIS database instance, • Customizable user specific reports • Dashboard requirements • Technical Audit Log trail reports for access control logs • Reconciliatory reporting where needed • System health check dashboard formonitoring health of application including security vulnerabilities.	
	Performance Requirements	
18	The system should be configured to support **BUSINESS VOLUMTERICS** provided in the RFP. However as per NABFINS requirement the system should be scalable. There should not be any application/solutions dependency to increase the volumetrics except for system hardware (RAM, CPU, Storage). NABFINS should be able to increase the hardware requirement on demand from the cloud bidder.	
19	The proposed solution should be cost-effective, scalable and use standard platforms	
20	NABFINS may engage any third-party solution for performance monitoring of the proposed solution for which the Bidder should support at no additional cost to NABFINS.	
	Scalability Requirements	
21	Scaling process to be clearly defined by the Bidder and should not involve any code changes.	
	Compliance with NABFINS's policies	
22	The solution provider should not store or share any data outside the NABFINS's infrastructure.	
23	Ownership of data in the cloud - CSP should have no rights or licenses, including without limitation intellectual property rights or licenses, to use data owned by NABFINS for its own purposes by virtue of the transaction or claim any security interest in data owned by NABFINS	
24	The solution should ensure that the log collection, storage, management, integrations are done in a secured and tamper proof manner.	
25	Isolation of NABFINSs data from other customers of CSP	
26	Ownership of any/all data generated/fed/stored in the system lies with the NABFINS and CSP has no rights or licenses or any IPR on the data.	
27	Log retention should adhere to the time frame as per the NABFINS's log retention policy, details for retention shall be minimum for the period defined by regulatory and statutory authrority.	
28	Data retrieved by the solution from external financial information provider systems needs to be retained for a time frame as per the NABFINS's data retention policy.	
29	Remote access from Bidder's workplace to NABFINS's environment will be for limited prupose including development, support operations, deployments, debugging etc., the security compliance of this access is the responsibility of bidder and CSP	
30	Access to and disclosure of the NABFINSs information assets by the CSP -Information should only be used by the CSP strictly for the purpose of the contracted service, and in accordance with the terms of pertaining to such use	
31	Secure removal, return, retention and/ or destruction of assets and data belonging to NABFINS- Upon termination or upon the direction of the NABFINS	
32	CSP confirms and obligates himself to provide notification to the NABFINS in the event of any significant changes that may impact service availability (including controls and/or location) and security incidents i.e., breach of security or confidentiality (but not limited to)	
	Hardware	
33	The solution should support deployment on dedicated cloud instance for NABFINS. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements, back up disk & media based.	
34	The Bidder shall configure, deploy, support, and manage the set up for the NABFINS.	

35	The bidder is required to ensure the storage of data in secured environment for the period as defined by NABFINS. Once the services are discontinued by NABFINS, the bidder & CSP must ensure that data is removed from all environments of CSP & bidder	

#	Technical Requirements	Bidder's Compliance (Yes/ No)	Bidder's Remarks
	Deployment Options		
1	Vendor encrypts data transmissions end-to-end across the environment		
	Configuration		
2	Configuration and management through a single, web-based user interface		
3	No Root access required to install or operate agent.		
4	No use of OS primitive LD_Preload for discovering components - malware technique		
5	Automatically create a single visualization of the entire application topology with all components.		
6	No more than 2->4% overhead out of the box.		
7	Automatically baseline every metric measured by the solution.		
8	Ability to globalize alert definition with inbuilt policy engine (rather than have to setup individually per metric)		
9	The ability to provide a multi tenant environment		
10	SSL Encrypted data transmission between EVERY monitoring component.		
11	Distributed Transaction Profiling does not require any code changes.		
	Better Application Visibility and Control		
12	Provide correlated views of distributed business transaction between tiers/services		
13	The ability to automatically baseline every component within the Business Transaction – so we understand not just that business transaction is slow but specifically which component is breaching the baseline.		
14	Provide code level diagnostics (class & method-level visibility) of poorly performing BTs		
15	Solution does not disable monitoring functionality as a compromise to limit product overhead.		
	Reduce Mean Time To Repair		
16	Identify slow SQL queries without manual intervention		
17	Identify slow backends systems or external services without manual intervention		
18	Automatically discover code deadlocks		
19	Automatically send email containing hyperlink to identified problem		
20	Automatic analysis of end-to-end APM data to provide root cause analysis.		
	Usability		
21	Granular RBAC for flexible usage across teams (Example 1- Certain application visible to Team A & not Team B, Example 2 - Certain dashboards are visible to Role A & not Role B)		
	Runbook Automation and Alerting		

22	Policy Rules Engine & Alerting: * Ease of use: point-n-click rules wizard * Leverage multiple data inputs into analysis (app performance data, machine data and customer provided data) * Use Boolean logic to combine multiple conditions through AND / OR logic * Disable rule evaluation temporarily for predetermined maintenance windows * Trigger alerts or notifications when rules are violated (email, SMS or custom) * Use complex logic to combine different metrics into one trigger/alert		
	Business Criteria		
23	Validate technology can scale to support the business requirements of the application managed.		
	Analytics Platform		
24	Single UI incorporating Analytics and APM modules		
25	Analytics layer providing intelligence across data collected by APM modules		
26	Horizontally scalable big data repository capable of collecting and storing anticipated volume of metrics/events		
27	In context drill down between analytics data and APM data		
28	Configurable to collect not all, but specific desired transaction data/fields		
29	Alert off of metrics created in analytics based on search criteria		
30	Analytics data collection does not require full call method stack data		
31	No code changes required to pull custom (non-native) metrics into data repository		
32	Data collected, stored and analyzed in near real time, not hours, days, or weeks later.		
33	API to Input Custom Metrics -Analytics Events API		
34	Ability to chart result set in pre-defined dashboards		
35	Ability to chart result set in custom dashboards		
36	Dynamically baseline custom metrics.		
	Transaction Analytics		
37	Identify all transactions for a particular user in a certain time frame by searching user ID, email, orderID or other unique customer identifiers.		
	Platform Support		
38	Platform Support for Oracle, SQL Server, MySQL, DB2, Sybase, PostgreSQL, and MongoDB		
	Ease Of Deployment		

39	Measure and monitor all databases in your environment without impacting stability or performance.		
40	Low overhead, production safe monitoring technology.		
41	Agentless installation - ability to rapidly deploy and eliminate risk on production database servers		
	Root Cause Analysis		
42	Historical performance monitoring and trending - save 100% of historical data		
43	Report top database activities (e.g. Top SQL, Top Users, Top Programs)		
44	Report database activity profile over-time (identify patterns)		
45	Collect and store all database wait events and correlate with SQL/Stored Procedures		
46	Collect and store SQL/Stored Procedure Key Performance Indicators (CPU, Count, Reads/Writes)		
47	Collect and store database instance level statistics (table size, row count, indexes)		
48	Collect and store database server/host Key Performance Indicators (CPU, Memory, …)		
53	Provide Performance Comparison Reports		
54	Collect SQL Explain & Execution plans		
	Database Monitoring and Management		
55	Ability to co-relate slow query to calling application code		
56	Static and dynamic alerting on collected database metrics.		
	Monitoring Capabilities		
57	Monitor Machine availability, CPU Usage, Disk performance, Volume usage, Machine load, Memory, SWAP, Processes, Network Adapter(s)		
	Application to Machine Correlation		
58	Single UI for Server and Application monitoring		