Appendix 1B- Technical Specifications - Scoring Sheet

Instructions of Filling up of Appendix 1B

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. **All requirement stated in the technical specification is mandatory and 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.
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]	Remarks
1	Solution 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, as amended from time to time. 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, other devices and ancilliary infrastructure etc.) to ensure accessibility of the proposed infrastructures and applications at all time as per defined SLA's.		
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 between primary site (DC) and secondary site (DR).		
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 automated switchover 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/ Other regulatory entities.		
6	The bidder shall provide NABFINS with all the 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. 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.		
8	The bidder and CSP should adhere to the relevant standards published (or to be published) by DeitY/MeitY or relevant standard bodies or regulators like RBI, SEBI, IRDAI / recognized by Government of India and notified to the bidder or CSP by DeitY/MeitY/SEBI/IRDAI/RBI/or by any institution recognized by Govt. of India as a mandatory standard and/or regulations.		
9	NABFINS and its auditor(s) will have right to audit the infrastructure allocated to NABFINS 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 that all confidential information is protected against unauthorized access, disclosure, alteration, use, or distribution through appropriate administrative, technical, and physical security controls.		
11	The SIEM should support configuration of alert severity and prioritization, notification mechanisms (such as Email, SMS, Microsoft Teams, and other channels), integration with ITSM platforms (e.g., ServiceNow and Jira), and incident workflows, including automated escalation and response processes.		
12	If Indian government or NABFINS 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 or NABFINS authorized personnels 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.		
13	Solution should have Management dashboard/console along with capability to provide Alerts & Monitoring interface. Access control list(ACL) based mechanism must be supported along with access logs (PIM/PAM)		
14	Solution should have Capability to integrate with the authentication servers (LDAP/ADFS etc.) and Integration with applications using API.		
15	The cloud infrastructure should have presence in at least 2 cities (Geographically separated) in India		
16	The solution should be encrypting data both at rest, data in motion, and in transit with TLS (minimum TLS 1.2).		
17	The Service uptime agreement for the proposed solution should meet the monthly uptime commitments and have a transparent monthly credit calculations in case of uptime not being met for any services.		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
18	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.		
19	Mechanism for automated email trigger in case of cyber attacks/ virus attack/ malware etc. to be provided by the bidder.		
20	Bidder to perform backup on a daily basis and half-yearly back-up restore tests in presence of NABFINS staff.		
21	Bidder to ensure that CSP's personnel controls are in place to provide a logical segregation of duties.		
22	NABFINS Infrastructure should be in a Virtual Private Cloud. 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.		
23	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.		
24	The bidder shall facilitate and support IT audits as required by NABFINS and shall provide NABFINS with the right to audit the procured SIEM solution, including the associated services, infrastructure, controls, and processes. In addition, the bidder shall ensure the following: a. Data Residency: All NABFINS data, including logs, metadata, backups, and processed information, shall remain within the geographical boundaries of India. Data shall not be stored, processed, replicated, or transmitted outside India, either physically or logically. b. Integration: The SIEM solution shall support integration with NABFINS' ITSM platform, SaaS applications, cloud infrastructure, on-premises infrastructure, endpoint protection solutions, network devices, databases, identity and access management systems, and other security solutions as required by NABFINS for centralized security monitoring and incident management. c. Privileged Access Monitoring: The solution shall provide mechanisms to monitor, log, and audit all privileged user activities performed by the Cloud Service Provider (CSP) or its administrators on cloud-hosted systems. NABFINS shall have visibility into such privileged access activities through reports, alerts, and audit logs.		
25	**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 and Logs: 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 etc. Logs should be available for downloading by NABFINS as and when required. d. The bidder shall provide the artifacts, security policies and procedures demonstrating its and CSP's compliance with the Security Assessment and Authorization requirements. e. Bidder should follow all IT / IS policies of NABFINS		
26	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, network security, data security, vulnerability management, virtualization security, Business continuity, incident management, log monitoring etc. should be implemented on Cloud by CSP at all locations.		
27	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 per regulatory requirement and as required by NABFINS on cloud.		
28	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 in the format/ template devised by NABFINS.		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
29	Bidder should enable NABFINS in monitoring security controls by providing requisite access, periodic reports, management Information & dashboard material for reporting on control assessments.		
30	The bidder should ensure Data segregation, confidentiality, privacy controls setup in line with the NABFINS's requirement		
31	In case of Exit/ change of CSP, bidder to ensure the following while formulating the exit plan only after approval of NABFINS: 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. vi. Access, visibility, controls, performance etc. available in the existing CSP must be made available on transfer to another CSP. vii. Backup of all data stored in our database along with mapping documents.		
32	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		
33	Security should be implemented at all layers i.e., Physical, Network, Data, Application, gateway etc., of cloud architecture with multiple security controls.		
34	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) 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 virtual appliance, 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.		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
35	Implement principle of selective privileges and impose segregation of duties with appropriate access and authorization: a. 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. b. Multifactor authentication shall be implemented for user access to critical workloads and for all privileged access on the cloud. c. Users with privileged system access shall be clearly defined and regular user access review shall be conducted once in a month and the corresponding report is to be shared with NABFINS. d. Remote access by administrators and privileged users to the cloud environment over the Internet without MFA, shall not be permitted. e. 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. j. A granular access control policy should be implemented for access to any cloud resource.		
36	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. 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 of the cloud service.		
37	Retention of NABFINS's data on the cloud shall be in accordance with the extant guidelines of NABFINS's Data Retention Policy.		
38	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 periodic interval. (monthly)		
39	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/ Vendor/Third Party.		
40	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.		
41	The systems in cloud infrastructure should be updated with the latest anti- malware signatures, the bidder shall submit the monthly report on the same with NABFINS.		
42	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.		
43	CSP/Bidder should ensure Zero Trust & SASE (secure access service edge)		
44	File integrity monitoring should be implemented in order to ensure authenticated changes and to detect unapproved changes to files.		
45	Password Policy on the Cloud setup should be followed as per the NABFINS's password Policy. For privileged users, it should be more stringent than that for normal users.		
46	Mechanism shall be implemented to detect service faults or outages in the cloud environment.		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
47	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. Appropriate Disaster recovery solution should be in place to ensuring the compliance to BCP and DR Continuity.		
48	Change/Configuration management procedures shall be aligned with the NABFINS's Change Management policy, including change request, approval procedures and notification mechanism.		
49	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).		
50	Secure configuration settings related to OS/ database/ network devices/ virtual machines/ application/ middleware should be implemented and documents/ compliance certificate for the same may be submitted to NABFINS.		
51	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.		
52	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)		
53	Roll-out / phasing-out of applications to / from cloud should follow the Data Migration Policy of the NABFINS.		
54	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.		
55	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.		
56	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.		
57	Bidder should conduct periodic Vulnerability Assessment and Penetration Testing (VAPT) and IS Audit is performed on assets (solution and infrastructure) as per NABFINS Defined policy according to the regulatory requirements. and if required NABFINS to have right to conduct VAPT for the solution and IS Audit for solution and infrastructure.		
58	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		
59	Information security incident management process shall be established to discover, report, respond and prevent information security events and weaknesses effectively by bidder and CSP		
60	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.		
61	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		
62	The IS controls' implementation should cover all locations that support NABFINS's data storage and/ or processing requirements.		
63	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.		
64	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		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
65	Bidder should deploy strong Password Policy for End point and application access. The application should be capable of integrating with AD and SSO.		
66	Proper access control is to be defined for protecting NABFINS data and access to the Data is strictly on Need-to-Know Basis		
67	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		
68	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, DPDP 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.		
69	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 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 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		
70	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		
71	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.		
72	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.		
73	Data (Online, backed up or local copy) must not be shared with outsiders (Any personnels) without explicit & case specific approval of NABFINS. Data should not be allowed to be downloaded or to prepare copies unless explicitly approved.		
74	The key used by the vendor to encrypt NABFINS data should be(unique) different i.e., it should not be the same that was/is used for other clients		
75	CSP should ensure proper log generation, storage, management and analysis happens for the 3rd Party/Vendor application (including DFRA & access logs)		
76	CSP should have captive SOC or Managed Service SOC for monitoring their systems and operations		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
77	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.		
78	The application and DB is/will be hosted separately on a dedicated instance for NABFINS. Evidence of dedicated instance for NABFINS should be submitted.		
79	The Primary Site and secondary site of CSP proposed for the project should be Geographical separated in India.		
80	Bidder should have in place procedures for emergency changes, including the roles and responsibilities, and that shall be documented.		
81	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		
82	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.		
83	Threat Modelling of all activities being performed by CSP & bidder should be documented and should be shared with the NABFINS on periodic basis		
84	Bidder's and CSP also confirms that NABFINS reserve the right to Audit the solution procured by NABFINS as and when required by NABFINS. Bidder should submit the compliance on behalf of the CSP, taking full responsibility of arranging the same as and when required by NABFINS		
85	NABFINS during the contract stage may change the architecture at any time, based on the software changes or migration of different tech stack. Bidder should ensure the compliance to the change within the defined timelines, as agreed by NABFINS		

TABLE B: Technical compliance		Compliance [YES/NO]	Remarks
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)	System must be designed to be efficient, scalable, manageable, fast, frugal with resources, compos-able and SOA-style self-contained		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
f)	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		
g)	The data architecture must classify data in a number of ways based on function, purpose, structure, confidentiality, sensitivity		
h)	The solution should have a native support for cloud deployment model		
i)	The solution should have detailed, periodically updated data dictionary which should be shared with NABFINS on the periodicity as specified by NABFINS		
j)	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			
k)	Periodic benchmarking of proposed solution as desired by NABFINS		
l)	The solution should support to customize the product for different jurisdictions as per the local Regulations as well as client needs.		
m)	Solution is platform agnostic.		
n)	The Bidder shall deploy the solution in dedicated instance for NABFINS for hosting the application.		
o)	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			
p)	The solution should support dynamic elasticity to cope up with the change in user loads.		
q)	The solution should support horizontal and vertical scaling to meet the NABFINS's future requirement.		
r)	Scaling process to be clearly defined by the Bidder and should not involve any code changes.		
s)	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.		
t)	Ability to scale linearly		
u)	Solution should be able to scale to accommodate future usage loads, such as load balancing, clustering, support for additional CPU cores etc.		
v)	Solution should meet performance standards regardless of the location within India		
w)	Capability to handle sub second response time		
x)	Allow for high capacity to carry out transactions during high volume period		
y)	Proposed Cloud should provide autoscaling, network load balancer, application load balancer for ensuring the compliance to the RFP		
z)	Bidder is required to ensure that NABFINS Cloud infrastructure is secure and access to the infra is allowed only through VPN.		
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 with no changes to data.		
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		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
jj)	Client account, transaction data or any sensitive information is encrypted when in transit.		
kk)	Solution should comply with all IT policies (IT Security Policy, IT Policy, Cloud Policy, Data Migration Policy etc.) of 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).		
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.		
ss)	Shared database services should not be used, database, clusters and all other resources must be setup separately for NABFINS.		
tt)	Bidder to note that only latest version of the software, OS and DB should be provided.		
uu)	Bidder to ensure that root access of the database configured for NABFINS and only designated user (approved by NABFINS) should be provided access of database for maintenance activity		
TABLE C: Other Requirements		**Compliance [YES/NO]**	**REMARKS**
	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 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 L2 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, security monitoring, 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	Bidder should provide the access to NABFINS of the EMS tool utilised by bidder for monitoring the utilization and maintenance of SLAs defined in the RFP. NABFINS should have real time view of the data. NABFINS should have a access to review and view the alerts, logs, tickets, and SLA compliance on a real time basis.		
12	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.		
13	Audit Trail - All transactions should be securely logged to detect any modifications.		
14	All historical records of deviation along with user audit trail should be logged for future reference.		
15	should be Configure correlation rules, threat detection use cases, IOC-based detection,anomaly detection where applicable and Implement MITRE ATT&CK mapping,etc..		
16	History of each parameter change should be logged.		

S.No	TABLE A:- Specifications/Features	Compliance [YES/NO]	Remarks
17	Identified Users should be able to access audit trails of all the transactions, modifications/changes for audit purpose.		
	Reporting		
18	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 • System health check dashboard formonitoring health of application including security vulnerabilities.		
	Performance Requirements		
19	The system should be configured to support **BUSINESS VOLUMETRICS** provided in the RFP. As per NABFINS requirement, the system should be scalable (hardware and software). Application should run smoothly without any lag.		
20	The proposed solution should be cost-effective, scalable and use standard platforms		
21	NABFINS may engage, during the contract, any third-party solution for hardware/Application performance monitoring (EMS) of the proposed solution for which the Bidder should support at no additional cost to NABFINS.		
	Scalability Requirements		
22	Scaling process to be clearly defined by the Bidder and should not involve any code changes.		
	Compliance with NABFINS's policies		
23	The solution provider should not store or share any data outside the NABFINS's infrastructure.		
24	Ownership of data in the cloud - CSP should have no rights or licenses, to use data owned by NABFINS for its own purposes by virtue of the transaction.		
25	The solution should ensure that the log collection, storage, management, integrations are done in a secured and tamper-proof manner.		
26	Isolation of NABFINS's data from other customers of CSP		
27	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.		
28	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 authority.		
29	Data, if 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.		
30	Bidder/ OEM to monitor NABFINS environment for any security breaches or for compliance purposes and should submit the access log report to NABFINS.		
31	Access to and disclosure of the NABFINS's information assets by the Bidder/CSP - Information should only be used by the Bidder/ CSP strictly for the purpose of the contracted service, and in accordance with the terms of pertaining to such use.		
32	Secure removal, return, retention and/ or destruction of assets and data belonging to NABFINS- Upon termination or upon the direction of the NABFINS		
33	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		
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		