Response to Pre Bid Queries - NABFINS/RFP/018/2024-25

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
-	IT setup at Head office, Bengaluru	What are the make and models of the 7 access switches?	The make and model of the devices will be shared with the successful bidder.
		What are the model and manufacturer of managed switch?	
		What are the make and model of the firewalls?	
		Are the firewalls managed locally or remotely? If remotely, who does manage them?	The firewall is managed locally by NABFINS IT Department.
		What operating systems are installed on the physical servers and VMs?	Windows Operating System.
		What virtualization platform is being used (e.g., VMware, Hyper-V)?	Hyper V virtualization platform is being used.
		How many VMs are hosted on each physical server?	There are 3 physical servers, with 2 VMs hosted on each physical server
12	The Information System Audit shall cover the entire Software Application (Core Microfinance Solution (CMS) Application)	As per the RFP, the IS Audit requires to be performed for only (Core Microfinance Solution (CMS). Is there any other application that requires to be scopped in along with this?	IS Audit to be performed for CMS software, NABFINS corporate website and NABFINS HO infrastructure setup
12	-	Can you specify the nature of these integrations (APIs, third-party services, internal systems) for security assessment?	Details will be shared with the successful bidder.
12	The audit shall clearly bring out the risk in the Software application, infrastructure at vendor's site, Nagpur, Maharashtra, Corporate website of NABFINS and IT setup at Head office, Bengaluru.	Can you specify the methodology and criteria for risk profiling? Is there a preferred risk assessment framework?	NABFINS is regulated by RBI and has its own set of policies, frameworks and SOPs in place. Bidder is required to conduct audit in accordance with these and identify any risks associated with the software, applications and HO infrastructure.
12	-	Will the IS Audit be performed remotely/ hybrid/ on site?	Audit to be performed in Hybrid mode (Bidder needs to visit NABFINS HO, from there access will be given to NABFINS' vendor site).
12	-	Is there any proposed approach for this IS Audit? Can the bidder propose a risk-based IS Audit approach?	Risk based IS audit approach to be adopted by bidder, provided it is as per the regulations and guidelines outlined by Reserve Bank of India (RBI)
12	Policy, Procedures, Standard Practices, Organization structure, IT Outsourcing & other Government and Regulatory Requirements	Will NABFINS provide specific internal security policies to align with the external standards? How many policies/standards will be scoped in?	NABFINS will provide policies, procedures and SOPs to the selected bidder. In case of any gaps, bidder to refer to extant RBI/other regulatory/statutory guidelines to ensure coverage of scope and compliance.

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
12	-	Are third-party systems/vendors expected to provide compliance evidence, or is the bidder responsible for auditing them?	The selected bidder needs to audit the third-party systems/services provided by third-party vendors and submit the observation report, along with compliance recommendations to NABFINS. NABFINS will, in turn, inform the third-party vendor for providing the compliance evidence.
	i. The auditor has to refer "IRDAI Total Control List" a list maintained by the Insurance Regulatory and Development Authority of India (IRDAI) which details all the insurance companies operating within India that are subject to their regulatory oversight, including both life and general insurance companies, essentially providing a comprehensive list of all insurers under their control. ii. The bidder has to provide recommendations to increase the effectiveness of the security controls.	Based on access to Insurer's Systems ,what is the scope confined to ?	The seleced bidder needs to conduct audit as per IRDAI guidelines and submit the audit report. As per IRDAI classification, NABFINS is a Category 3 insurance intermediary.
13	-	Kindly confirm if bidder is expected to perform and configuration changes on the in-scope systems to mitigate identified vulnerabilities. If yes, any specific severity vulnerabilities need to be resolved e.g. medium/high or all vulnerabilties to be mitigated.	Bidder need to conduct audit and submit the observations with recommendations. NABFINS IT department will be making changes as per the recommendations to mitigate vulnerabilities. After assessment of the changes, auditor need to sumbit the final report.
13	-	Is bidder expected to retest after mitigation of the identified vulnerabilities	No
13	-	Please confirm the hosting environment for the in-scope systems e.g. cloud provider, hybrid setup etc.	Hybrid
13	-	Will NABFINS provide necessary systems/infrastructure to host and setup?	No
13	-	Are there any specific network security controls expected to be tested, such as VPN detection, proxy blocking, or insecure Wi-Fi checks?	Yes. Details will be shared with the successful bidder.
13	API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities	Apart from OWASP API Top 10, are there any additional security frameworks or compliance requirements we need to follow?	No

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
12	-	Are third-party systems/vendors expected to provide compliance evidence, or is the bidder responsible for auditing them?	The selected bidder needs to audit the third-party systems/services provided by third-party vendors and submit the observation report, along with compliance recommendations to NABFINS. NABFINS will, in turn, inform the third-party vendor for providing the compliance evidence.
	i. The auditor has to refer "IRDAI Total Control List" a list maintained by the Insurance Regulatory and Development Authority of India (IRDAI) which details all the insurance companies operating within India that are subject to their regulatory oversight, including both life and general insurance companies, essentially providing a comprehensive list of all insurers under their control. ii. The bidder has to provide recommendations to increase the effectiveness of the security controls.	Based on access to Insurer's Systems ,what is the scope confined to ?	The seleced bidder needs to conduct audit as per IRDAI guidelines and submit the audit report. As per IRDAI classification, NABFINS is a Category 3 insurance intermediary.
13	-	Kindly confirm if bidder is expected to perform and configuration changes on the in-scope systems to mitigate identified vulnerabilities. If yes, any specific severity vulnerabilities need to be resolved e.g. medium/high or all vulnerabilties to be mitigated.	Bidder need to conduct audit and submit the observations with recommendations. NABFINS IT department will be making changes as per the recommendations to mitigate vulnerabilities. After assessment of the changes, auditor need to sumbit the final report.
13	-	Is bidder expected to retest after mitigation of the identified vulnerabilities	No
13	-	Please confirm the hosting environment for the in-scope systems e.g. cloud provider, hybrid setup etc.	Hybrid
13	-	Will NABFINS provide necessary systems/infrastructure to host and setup?	No
13	-	Are there any specific network security controls expected to be tested, such as VPN detection, proxy blocking, or insecure Wi-Fi checks?	Yes. Details will be shared with the successful bidder.
13	API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities	Apart from OWASP API Top 10, are there any additional security frameworks or compliance requirements we need to follow?	No

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
Scope of Work section II Corporate Website of NABFINS:	Corporate Website of NABFINS is the face of the Company wherein the dayto-day operational statistics of the Company are updated. The Website serves as a single source of information about the Company for the public including the customers of the Company, partners (B&DC/B&DF),prospective employees etc. In addition to the disclosure of details pertaining to the Company, the Website helps in the on boarding of new employees, B&DC partners, SLI clients as well as the reporting of grievances. Admin module facilitates the respective admins to login to their portal wherein the applications submitted by the above stakeholders can be viewed, accepted or rejected after due review	1) please share the size of the web page (eg: 200 pages, 100 pages) 2) please share the no.of roles employed in the application.	1) Corporate Website - 44 webpages 2) Details will be shared with the successful bidder.
Scope of Work section III Setup at Head office, Bengaluru:	The Head Office of NABFINS LIMITED, hosts the following infrastructure: 3 nos. of physical servers with multiple VMs 2 no. of Firewalls 1 no. of Managed switch 7 nos. of Access switch	Please share the no of VM running which need to be audited.Does it activity to be performed on site or can be conducted remotely over an VPN or any other remote connection	There are 3 physical servers, with 2 VMs hosted on each physical server. Audit of HO infrastructure has to be conducted onsite.
Scope of Work VAPT:	API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities:	Explicit API scope information is not defined in the RFP, please confirm if API VAPT is limited to the API associated within the web applications or is any specific API are in scope. If yes, please share the no.of API's to be assessed.	API VAPT is limited to the APIs associated with the web applications in scope.
-	Head Office Infrastructure	List of: Servers (Windows/Linux etc..) Workstations Switches Routers Firewalls/UTM Devices IDS & IPS Load Balancers	Head Office Infrastructure Servers (Windows/Linux etc..) = 3 Windows server Workstations = 130 approx Switches = 7 Routers = NA Firewalls/UTM Devices = 2 IDS & IPS = Yes Load Balancers = NA
		List of: External Facing Servers (Windows/Linux etc..) External Facing Routers External Facing Firewalls/UTM Devices	External Facing Servers (Windows/Linux etc..)= 2 External Facing Routers= NA External Facing Firewalls/UTM Devices= 3
		Location of Audit (Address) with contact person details:	NABFINS Limited Head Office, Bengaluru Vibin Bence Ph. No: 9072768488 Krishnaraj Ph. No: 9742928346

NABFINS Ltd. BENGALURU

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
Scope of Work section II Corporate Website of NABFINS:	Corporate Website of NABFINS is the face of the Company wherein the dayto-day operational statistics of the Company are updated. The Website serves as a single source of information about the Company for the public including the customers of the Company, partners (B&DC/B&DF),prospective employees etc. In addition to the disclosure of details pertaining to the Company, the Website helps in the on boarding of new employees, B&DC partners, SLI clients as well as the reporting of grievances. Admin module facilitates the respective admins to login to their portal wherein the applications submitted by the above stakeholders can be viewed, accepted or rejected after due review	1) please share the size of the web page (eg: 200 pages, 100 pages) 2) please share the no.of roles employed in the application.	1) Corporate Website - 44 webpages 2) Details will be shared with the successful bidder.
Scope of Work section III Setup at Head office, Bengaluru:	The Head Office of NABFINS LIMITED, hosts the following infrastructure: 3 nos. of physical servers with multiple VMs 2 no. of Firewalls 1 no. of Managed switch 7 nos. of Access switch	Please share the no of VM running which need to be audited.Does it activity to be performed on site or can be conducted remotely over an VPN or any other remote connection	There are 3 physical servers, with 2 VMs hosted on each physical server. Audit of HO infrastructure has to be conducted onsite.
Scope of Work VAPT:	API security assessment should be done against all known vulnerabilities including but not limited to latest OWASP vulnerabilities:	Explicit API scope information is not defined in the RFP, please confirm if API VAPT is limited to the API associated within the web applications or is any specific API are in scope. If yes, please share the no.of API's to be assessed.	API VAPT is limited to the APIs associated with the web applications in scope.
-	Head Office Infrastructure	List of: Servers (Windows/Linux etc..) Workstations Switches Routers Firewalls/UTM Devices IDS & IPS Load Balancers	Head Office Infrastructure Servers (Windows/Linux etc..) = 3 Windows server Workstations = 130 approx Switches = 7 Routers = NA Firewalls/UTM Devices = 2 IDS & IPS = Yes Load Balancers = NA
		List of: External Facing Servers (Windows/Linux etc..) External Facing Routers External Facing Firewalls/UTM Devices	External Facing Servers (Windows/Linux etc..)= 2 External Facing Routers= NA External Facing Firewalls/UTM Devices= 3
		Location of Audit (Address) with contact person details:	NABFINS Limited Head Office, Bengaluru Vibin Bence Ph. No: 9072768488 Krishnaraj Ph. No: 9742928346

NABFINS Ltd. BENGALURU

Section/para no. clause	Details given in the RFP	Pre Bid Queries from Bidders	NABFINS Response to Pre Bid Queries
		No. of screens in app	10 nos.
		No. of forms in the application (Module wise)	10 nos. (incl. all modules)
	Secure Code Review	No. of application(s) proposed for review platform used to develop the application(s) Name of the application(s) URL of the application(s) Size of the application(s) Name of the application(s) Lines of code (approx.) Location of Audit (Onsite - from your location / Offsite - from our location, remotely) If Onsite Audit to be conducted, Please mention the location of Audit (Address)	There is no source code review