Pre-bid response - RFP for Selection of Vendor For Information Security (IS) Audit of Core Micro-Finance Solution on Cloud. Tender No. NABFINS/RFP/015/2024-25

Sl. No	Reference	RFP Page No.	RFP Clause	Query	Reply
1	Section 6.1 Detailed Sscope of Work	15	"Development of Risk profiles and drawing up of risk matrix taking into account Inherent business risk and effectiveness of the control system for monitoring the risk"	Can you specify the methodology and criteria for risk profiling? Is there a preferred risk assessment framework?	The bidder to identify and conduct the audit as per the industry standards and the systems and processes of NABFINS. Please refer "section 6.1.1 Standards to adhere" of the RFP
2	Section 6.1 Detailed Sscope of Work	15	"Preparation of Risk Matrix should be based upon Risk Analysis of all the Information Systems of NABFINS."	Will the Risk Matrix cover only core banking applications, or should it include third-party integrations and vendor applications?	Core Microfinance Solution and all the associated interfaces of the core microfinance solution
3	Section 6.1 Detailed Sscope of Work	15	"Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination."	Are there any predefined risk thresholds or scoring mechanisms that the bidder should follow?	Discussion on this will be conducted with the successful bidder
4	Section 6.1 Detailed Sscope of Work	16	"IS Audit for each of the systems should cover, but not limited to, the following aspects..."	Are all 16 aspects of IS Audit mandatory, or can the bidder propose a risk-based prioritization approach?	All the 16 aspects of IS Audit are mandatory. However, the successful bidder can propose a risk-based prioritisation covering all 16 aspects
5	Section 6.1 Detailed Sscope of Work Subsection 6.1.1 Standards to Adhere	16	"Standards to adhere: NCIIPC, NIST 800-115, Cert-In Guidelines, RBI IS Audit Guidelines, Industry Standard IS Audit Frameworks."	Will NABFINS provide specific internal security policies to align with these external standards?	Yes
6	Section 6.2 Proposed Approach	16	"Bidder is expected to provide their Approach and methodology for conducting the Audit..."	Are there any preferred audit tools or frameworks that NABFINS expects the bidder to use?	NABFINS does not have any specific preference for audit tools.The audit should comprehensively cover the Scope of Work as defined in the requirements.Tools, services, and infrastructure required for automating the entire end-to-end IS audit process must be factored in by the bidder
7	Section 6.3 System Architecture details	17	"System Architecture Details: 200 webpages, 2 DB instances, Oracle 19c, Amazon Linux 2023, Tomcat, Finpage, 1 WAF, 1 Load Balancer."	Will the bidder be provided with administrative access to conduct security configuration reviews, or will this be done in coordination with NABFINS IT team?	NABFINS IT team will assist the bidder in providing with administrative access
8	Section 6.3 System Architecture details	17	"Integration Touchpoints: 20"	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
9	Section 6.1 Detailed Sscope of Work	15	"Source Code Review"	Will the source code review be limited to critical applications, or does it include all in-scope applications? Will secure code review tools be provided by NABFINS?	Please refer to Addendum No. 1 for scope revision with respect to source code review.
10	Section 6.1 Detailed Sscope of Work	15	"Source Code Review"	Determine if we are expected to perform a source code review as part of the audit or if the focus should be on assessing whether CERT-In SDLC controls have been followed and verifying that periodic reviews are happening.	Please refer to Addendum No. 1 for scope revision with respect to source code review.
11	Section 6.1 Detailed Sscope of Work	15	"Cloud Security Review"	Are there specific cloud security benchmarks (e.g., CIS benchmarks, NIST cloud security) that the bidder should adhere to?	Bidder has to follow all government, NIST and regulatory standards and guidelines to fulfil this requirement

NABFINS Ltd.
BENGALURU

Sl. No	Reference	RFP Page No.	RFP Clause	Query	Reply
12	Section 6.1 Detailed Sscope of Work	15	"Cloud Security Review"	Clarify the scope regarding cloud security – whether we need to focus solely on AWS security certifications or if tools like AWS Config and AWS Security Hub should be used to assess cloud resource configurations against security best practices.	The bidder to identify and factor in the necessary tools of AWS to complete the scope of cloud security review
13	-	-	General	Confirm whether visits to the application development vendor's site and/or BC site are necessary, depending on whether the development is in-house or outsourced.	The audit will be conducted from the HO of NABFINS - 3072, 14th Cross, Krishna Rajendra Rd, Siddanna Layout, Banashankari Stage II, Bengaluru, Karnataka 560070
14	-	-	General	Is audit and reporting both to be done onsite?	Yes
15	-	-	General	Are we allowed to use organisation computers or Nabfins will be providing devices for the audit	No, NABFINS IT team will assist the bidder in providing with administrative access to perform the Audit.Tools, services, and infrastructure required for automating the entire end-to-end IS audit process must be factored in by the bidder
16	-	-	General	For the following sections is the bidder expected to perform the technical security audit and provide a report as a part of the evidence repository or will the bidder be provided with a report for the activity carried out which will have to be assessed to completeness. a. Technical Security Review - -Cloud security (AWS/Linux). -Network and firewall security assessment. -API and Web Application Security review. b. Operational Security & Best Practices - -Secure code practices for Finpage application. -Business Continuity & Disaster Recovery (BCP/DR) assessment. -Patch management and cybersecurity resilience testing.	Bidder to perform the necessary audit and submit the reports as per the project timelines mentioned in Section 6.4
17	-	-	General	Will testing laptops be provided by Nabfins as per specifications given or organisations can bring their pre-configured laptops for testing	NABFINS will not provide pre-configured laptops for testing. However, the NABFINS IT team will assist the bidder by granting administrative access to perform the Audit. The bidder must account for all necessary tools, services, and infrastructure required to automate the end-to-end IS audit process.
18	-	-	General	What is the application stack to be tested for the source code review component?	Details will be shared with the successful bidder.
19	-	-	General	We kindly request an extension of the submission date	Please be guided by the RFP

NABFINS Ltd.
BENGALURU