Ref in RFP	Bidder Query	Bank Response
1.2 Training Page	Please confirm whether the Bank requires training on all or any specific standard detailed below 1. FFIEC Cybersecurity Assessment Tool (CAT) 2. ISO/IEC 27001 3. NIST Cybersecurity Framework (NIST CSF) 4.Basel Committee on Banking Supervision (BCBS) Guidelines 5.General Data Protection Regulation (GDPR)	Either FFIEC/NIST with ISO/IEC 27001. Further bank considers or explores being trained on BCBS and GDPR as further substantiations. This will be ascertained after the gap analysis and accordingly the areas and tools will be decided upon. The respondent may include unbundled pricing options for such trainings. It will be bank's discretion to accept or reject the same.
	Please confirm whether the training will consist of a basic overview of the selected frameworks or in-depth sessions aimed at understanding how to implement the frameworks.	The nature of training and the scope /coverage will depend on the severity of gaps during the audit.
	Please confirm the audience of these training (specific function or organisation-wide) and expected number of employees for each training.	Primarily the training will be attended by personnels in Digital, IT and IS teams. However, the necessitation to include more people will be discretionary on part of the bank. The number of employees to be included will be decided in close consultation with HR.
	Please confirm the number of training sessions the bidder is expected to provide, as well as the duration of each training session in days.	The bank opines that the duration of training could be one day, however the frequency can be decided on the adequacy and sufficiency of training.
	Please confirm whether the training will take place on premises or remotely.	It may be hybrid mode as deemed convenient to both parties but certain issues will

		have to be assessed physically only.
Page 2 clause no 4	**RFP Clause: Last Date of submission of RFP response** **(Closing Date): 11/10/2024 till 4:00 p.m.** *Request Bank to extend the bid submission deadline by 7 days to 18/10/2024 due to involvement of multiple internal stakeholders*	The timelines can't be extended since the RFP mentions the deadline explicitly. It is a regulatory requirement.
Page 21 clause 1.1.3 - Domain 3 - Protection	**RFP Clause: Data Hosting Outside Mauritius.** **Conduct due diligence on countries hosting customer information, ensure legal compliance, data protection, and jurisdiction considerations.** *We will check this control only at a design level by reviewing the architecture diagram to understand the data flows.* *Data localization assessment will not be covered as a part of the scope as it is considered to be a separate engagement.*	This is a requirement and the checks need to be assessed. The respondent can deliberate the same during the presentation
Page 21 clause 1.1.3 - Domain 3 - Protection	**RFP Clause: Regular Vulnerability Scanning:** Ensure regular scanning of outdated and unsupported hardware/software for vulnerabilities. *We will not perform Vulnerability Assessments/ Scans, Penetration Testing, Source Code Reviews, Red teaming exercise, scenario testing as a part of this engagement.* *Existing Vulnerability Assessments/ Scans, Penetration Testing, Source Code Reviews, Red*	This is a requirement and the checks need to be assessed. The respondent can deliberate the same during the presentation

	teaming exercise, scenario testing reports will be reviewed as a part of the assessment.	
Page 21 clause 1.1.3 - Domain 3 - Protection	**RFP Clause :Third-Party Service Providers** Due Diligence: Conduct due diligence on third-party service providers before engagement, documented and approved. Risk Management of Third-Party Providers: Evaluate third-party service providers' risk management, internal controls, and Information security capabilities. Ensure contracts include provisions for cybersecurity, data protection, confidentiality, audit rights, and continuity of service. Implement security controls equivalent to or stricter than those for on-premises assets for third-party connections. Conduct periodic risk assessments and audits of third-party service providers. *We will not perform Third Party Risk Assessment for vendors.* *Existing Third Party Risk Management Framework, Due-Diligence Reports, Third Party Risk Management / Assessments and Audit Reports will be reviewed.*	This is a requirement and the checks need to be assessed. The respondent can deliberate the same during the presentation
Page 54 Eligibility Criteria	**RFP Clause:** Bidder should have undertaken similar assignment in at least 3 banks in MAURITIUS in last 5 years.	Shall be suitably amended and notified
Page 60 Annex 7	*The line-items highlighted in the Financial Proposal (Annexure -7) are not matching the proposed scope of the project.*	We regret the inconvenience and note to send revised FPT.

(Financial Proposal Format)	*Kindly request Bank to share the updated Financial Proposal Template*.	
Others	*Kindly confirm the count of in-scope of applications (along with bifurcation of critical applications) for sampling purpose.*	Such information will be shared with final respondent/bidder.
	Kindly confirm whether the assessment can be conducted remotely or onsite? *If onsite, kindly list the locations (Office, DC, DR, NDC)*	A hybrid approach can be used but certain issues may need physical inspection or assessment.
	In accordance with standard industry practice, our aggregate liability under this engagement and in connection with the services shall be for direct damages and shall, in all circumstances and events, be limited to one time the fees paid to us. We shall not be liable for any indirect or consequential losses.	This is a requirement and the checks need to be assessed. The respondent can deliberate the same during the presentation.
	Notwithstanding anything to the contrary, kindly note that we do not provide any legal services directly or indirectly since we are not permitted to provide the same. Our scope is limited to technical/commercial aspect and our services will not include provision of any legal services or legal advice. No work performed by our employees shall be construed as legal service/legal advice.	This is a requirement and the checks need to be assessed. The respondent can deliberate the same during the presentation.