Addendum/Clarifications No.1

Supply and Implementation of a Threat Intelligence Sharing Platform for the Banking sector

We refer to the RFP for "*Supply and Implementation of a Threat Intelligence Sharing Platform for the Banking sector",* launched on 18th August 2025.

Following queries raised from potential bidders, the responses of the Bank are as follows:

Query Serial No.	Current Specification	Query (In terms of Clarification or Modification or Addition of New clause)	Clarifications
1.	Hybrid (to be filled if on cloud); Item No. 4: Bidders to ensure that it should abide to the Bank's Guideline on use of Cloud Services and fill the table its Annex	The 'Annex' cannot be opened	The Annex is now available and can be downloaded from the website.
2.		What is the primary pain point or challenge you are trying to address with the implementation of a Threat Intelligence Platform?	The primary challenge we aim to address through the implementation of a Threat Intelligence Platform is the difficulty in consolidating, analysing, and operationalising threat data from multiple disparate sources. At present, this process is highly manual and time-consuming.
3.		Which SIEM system are you currently utilising?	Rapid7
4.		To confirm if you have a SOC in place? Is it managed internally by your team or by a third-party provider?	Yes, we do have a SOC, and it is managed by a third-party provider
5.		Approximately how many hosts are you looking to cover with this new solution?	All the19 commercial banks initially and then later to other financial institutions
6.		Please advise on the estimated number of BOM security admin users that shall need access toward the threat intelligence portal.	The Bank of Mauritius will require access for up to 15 security and administrative users to manage, govern, and oversee the Threat Intelligence Sharing platform.
7.		Please advise if the participants (19 to start, 60 in the next 3 years) need access to the platform or is it just the	For planning purposes, assume up to 5 users per entity and the solution should be scalable as the number of entities grows

Query Serial No.	Current Specification	Query (In terms of Clarification or Modification or Addition of New clause)	Clarifications
		BOM security admins who will have access.	from 19 in Year 1 to 60 in Year 3.
8.	The bidder may provide current and potential contracts in hand and any other relevant information to enable the Bank to take a view of its future financial strength.	Can we include financial statements for financial strength?	Financial statements can also be submitted
9.	Application shall be designed to capture all user access and activity in the system. Logs shall be kept for auditing purposes. Archiving and rapid retrieval of these logs shall be a mandatory feature.	Please let us know the retention time for which the logs need to be retained.	As per legal and regulatory requirements, system logs are typically required to be retained for a period of 7 years.
10.	The platform should support interoperability and integration with other threat intelligence platforms and tools and have supporting API documentation. The provider must support licenses for common integrations.	Please let us know the type of platforms with which the TISP needs to be integrated.	At this stage, we do not have a finalized list of specific platforms for integration. However, the Threat Intelligence Sharing Platform (TISP) will be designed to support interoperability with commonly used security and threat intelligence solutions, such as SIEM platforms (Rapid7), SOAR platforms, Threat Intelligence Platforms, Endpoint security solutions (Microsoft), and Network security tools.
11.		What is the expected duration for the implementation phase from contract signing to go-live?	As per Section 6.4 of the RFP, bidders are required to provide a detailed implementation plan for the Threat Intelligence Sharing (TIS) project, including a timeline and project governance framework.
12.	The platform should be able to ingest, process, and export threat intelligence data from various sources and feeds, such as open source, commercial, government, industry, and internal reporting.	Please let us know the data feeds that need to be integrated with the TISP.	At this stage, the project requirement is to support ingestion, processing, and export of data from multiple categories of feeds, including: Open-source intelligence, Commercial threat feeds, Government feeds, Industry-specific sharing communities, and Internal enterprise reporting and telemetry. The platform should be designed to flexibly integrate

Query Serial No.	Current Specification	Query (In terms of Clarification or Modification or Addition of New clause)	Clarifications
			with these categories of sources. A definitive list of specific data feeds and providers will be finalized during the project's requirements-gathering phase in consultation with the client's operational and regulatory needs.
13.	The platform must comply with the relevant data protection and privacy regulations and policies.	Please provide a list of relevant data protection and privacy regulations that need to adhere.	The platform must comply with all applicable data protection and privacy regulations and organizational policies, in particular the Data Protection Act 2017 (Mauritius) and the General Data Protection Regulation (GDPR).
14.	Successful bidders should provide training and support to the participants to ensure their effective and efficient use of the platform.	Please let us know the number of participants for the training session.	To be provided at a later stage
15.	Maintenance cost for 5 years (excluding first year where the solution is expected to be under warranty for the first year).	We understand that the pricing needs to be shared for 6 years (warranty for 1 year and 5-year maintenance cost). Please confirm.	This is correct. Detailed information and the format for sharing the pricing are provided in Annexure F of the RFP.
16.	The Bank is seeking qualified vendors capable of supplying, installing and configuring TIS Tool.	Please clarify if the scope is limited to supply and implementation of TIS Tool OR if Service Provider should also provide ongoing Service to maintain the TIS tool, threat intelligence integrations, updates and sharing with community etc.?	The scope of the RFP covers both the supply and implementation of the Threat Intelligence Sharing (TIS) Tool as well as the provision of ongoing services, including maintenance of the tool, integration with threat intelligence feeds, updates, provide reports, and facilitation of intelligence sharing within the banking community, in line with the requirements of the RFP.
17.	The Bank is seeking qualified vendors capable of supplying, installing and configuring TIS Tool.	Regarding the TIS tool - is commercial/licensed tool required, or open source is acceptable?	Bidder to propose
18.	The platform should support interoperability and integration with other threat intelligence platforms and tools and have supporting API documentation. The provider must	Please provide the tentative list of integrations requirement.	At a minimum, the solution should provide APIs and support for integration with: • Standard threat intelligence formats and protocols • Security Information and Event Management (SIEM) platforms

Query Serial No.	Current Specification	Query (In terms of Clarification or Modification or Addition of New clause)	Clarifications
	support licensees for common integrations.		• Security Orchestration, Automation and Response (SOAR) platforms • Endpoint Detection and Response (EDR) and Intrusion Detection/Prevention Systems (IDS/IPS) • Firewall and Threat Detection Systems • External Threat Intelligence Feeds from commercial or open-source providers The Bank does not prescribe a fixed list of tools but expects bidders to propose integrations based on industry standards and best practices.
19.	The platform should be able to handle large volumes of threat intelligence data and support a growing number of participants (19 to start, 60 in the next 3 years) and sources.	To clarify the understanding, in Year 1 there will be 19 entities who will be accessing the TIS and will grow to 60 entities in Year 3. How many users from each entity will be accessing the TIS?	For planning purposes, assume up to 5 users per entity and the solution should be scalable as the number of entities grows from 19 in Year 1 to 60 in Year 3.
20.	The platform should provide situational awareness and threat intelligence reports that summarise the current and emerging threats and trends and provide strategic and operational guidance to the participants.	Is this expected OOB from the tool or can it be provided as separate report as part of Service?	Bidders are free to propose the approach best supported by their solution, provided that the overall requirement is met. Proposals should clearly indicate whether such reporting is generated natively by the platform, delivered as part of managed services, or through a combination of both.
21.	The bidder must provide an additional 8 hours of RFI (Requests for Intelligence) support to the community per month.	Total 8 Hours per month to all entities combined or per entity?	The requirement is for a total of 8 hours of RFI support per month for the entire community combined, not per entity. The Service Provider will be expected to manage and prioritise these requests across participating entities in coordination with the Bank of Mauritius.
22.	The bidder must provide at least 1 full day of professional intelligence training to community members per year.	Please specify the agenda for training and number of participants. Clarify the mode of delivery - onsite, or online?	Up to 2 nominated participants per entity, plus representatives from the Bank of Mauritius. Bidders should assume approximately 50 participants in Year 1, with scalability as the number of entities increases.

Query Serial No.	Current Specification	Query (In terms of Clarification or Modification or Addition of New clause)	Clarifications
			The training may be conducted either onsite or online. Bidders are encouraged to propose a flexible delivery model (onsite, online, or hybrid) to ensure participation by all entities, with onsite delivery at the Bank of Mauritius being the preferred option where feasible.
23.	Can the Bank please clarify that the ultimate terms of the contract will be agreed with the preferred party as there are some that we would like to discuss in further detail?		The draft contract terms and conditions are included in the RFP and will form the basis of the agreement. Bidders are expected to accept the general terms as set out in the RFP. Any proposed deviations or clarifications should be clearly highlighted in the bid submission for the Bank's consideration.

Bank of Mauritius
2nd September 2025