MauBank Ltd

Request for Proposal:
Endpoint Security Project

REFERENCE: RFP/ICT/2023/72

28 September 2023

1. Introduction

The bank wish to implement a state of the art AI based Anti-Virus Solution aimed at fortifying and safeguarding its critical infrastructure. The solution is required to significantly enhance its cybersecurity posture and provide advanced threat detection and prevention capabilities. This document outline the scope of work, objectives, technical requirement, evaluation criteria and other essential information for interested potential vendors

2. Background

The bank currently have a signature based end point protection. In an era of rapidly evolving cyber threats, traditional antivirus solutions are often unable to keep up with the complexity and sophistication of modern malware. Therefore, we are seeking an innovative AI-based antivirus solution to bolster our defense mechanisms against a wide range of cyber threats. This solution should leverage artificial intelligence, machine learning, deep learning and advanced algorithms to provide real-time threat detection, proactive prevention, threat hunting and efficient resource utilization

3.1 Project Summary

In a landscape characterized by relentless cyber threats, MauBank Ltd is poised to take a pioneering stride towards fortifying its digital domain. The implementation of an advanced AI-based antivirus solution underscores the bank's unwavering commitment to the security and trust of its clients, stakeholders, and digital operations. Through this project, the bank aspires not only to shield its infrastructure but also to serve as a beacon of best practices in cybersecurity within the financial sector. As the digital realm continues to evolve, this initiative stands as a testament to the bank’s dedication to innovation, security, and the continued pursuit of excellence in the face of ever-evolving cyber challenges.

3.1.1 Objectives

- The implementation of the automated tool is to reduce and mitigate any kind of malware activity in bank eco-system to comply with regulatory thru the implementation of the following features and functionalities.
- Advanced Threat Detection and Prevention: Implement an AI-driven antivirus solution capable of identifying known and unknown malware, including zero-day exploits, and preventing their execution or spread.
- Minimize False Positives and Negatives: The solution should aim to minimize both false positive and false negative detections, ensuring accurate threat identification without disrupting legitimate user activities.

- Resource Efficiency: The proposed solution must minimize its impact on system resources, such as CPU, memory, and network bandwidth, to ensure optimal user experience.
- Centralized Management: Implement a user-friendly centralized management dashboard that enables efficient monitoring, analysis, and response to detected threats.
- Adaptability: The solution should continuously adapt and learn from emerging threats to stay ahead of cybercriminals.
- Comprehensive Documentation and Training: Provide comprehensive documentation and training materials for seamless integration, management, and maintenance of the AI-based antivirus solution.
- The bidder will have to uninstall all currently installed AV / ATP / EDR and other Anti-malware agents from the endpoints and deploy the new solution smoothly without business impact.
- The bidder will have to help the bank in Network configurations if required and address all issues which may occur during deployment

3.1.2.1 Business Drivers

- The main business drivers identified as per below for the initial scope of this project.
    - Protect the bank's interest by meeting regulatory guidelines where the bank is required to ensure that malware activity is monitored, detected and prevented on 24 x 7 basis to enhance customer experience
    - To reduce risk factor on bank exposure, reputational and financial loss
    - Being more efficient and enhance the customer journey on day to day activity.

3.2 Project Scope

3.2.1 End Point Antivirus Solution

Item No	Item description and Technical Specification	Confirm Full specification of items offered	Details of Non-Compliance/Deviation (where applicable)
	Endpoint Protection Platform should meet the following:		
1.	The solution must be among the leaders in the latest Gartner Magic Quadrant / other independent benchmarking body for Endpoint Protection		
2.	Supplier should assess and know bank environment to ensure there is no barrier before deployment, on operating system, Network and Firewall and will be		

	solely on responsibility of supplier for resolution. Any omission will be at the cost of the supplier. These resolutions should be executed without causing any adverse impact on the bank's business operations.		
	A significant amount of bank's servers and PCs operate without internet connectivity, and no direct access to the internet will be granted. The solution must possess the capabilities to function with a relay server situated in the DMZ and should offer controlled management for signature / definition / binary updates.		
3.	The whole solution (agent and management solution) must demonstrate a high level of security, to withstand both insider and external attack. This applies to the security of the solution design, its deployment and operations encompassing all relevant security processes, technologies and certifications such as GDPR, ISO 27001, PCI-DSS, NIST, and other.		
4.	The solution should possess the capability utilizing Local Admin account, rather than being dependent on Domain Admin Account for agent / sensor / binary deployment. No domain admin credential will be provided only SA account with higher privilege will be provided.		
	Tamper Protection: The solution should support a seamless uninstallation process for the agent in cases where the protection keys are lost or unrecoverable		
5.	The whole solution must be centrally controlled from a single management console. Multiple domains should be visible and managed through one console.		
6.	One management platform for the whole environment with all capabilities - No switching between different platforms / Console to manage both Endpoints, servers, mobile and other		
5.	The management console must provide role-based access for users to log in, the solution management systems must support segregation of access and administrative tasks based on defined roles with the principle of least privilege.		
6.	The management console must support Two-Factor authentication for admin access with SSO capabilities.		

7.	NextGen AV Agent • The solution must prevent attacks when no network connectivity to the Internet is present. • The solution must use real-time technique to identify malware within a file, describe all technique used. • The solution must employ signature-less techniques and must not download signature to protect against the latest threat. • The solution must provide reputation-based file protection to prevent execution of applications that have the potential of being malicious. • The solution must provide capabilities to collect application properties, compare against known attributes (hash, name, publisher, etc.) to check for known malicious code, and to remove or quarantine suspicious applications. • The solution must prevent software exploits by enforcing in-memory protection. These methods guard against memory overflow attacks and against other attack methods that take advantage of zero-day software or OS vulnerabilities. • The solution should offer the capability to configure customized periodic scanning intervals. • The solution should provide the capability for real-time scanning at the kernel level. • The solution should have built-in control update capabilities for agent / sensor / binary version update and should offer the flexibility to select specific groups of machines for these updates. • The installation of agents should not require a reboot. • All upgrades are performed silently and automatically, without a reboot nor any user or admin overhead under the control supervision of a system admin • The solution must identify malicious files and prevent them from execution, including viruses,		

	Trojans, ransomware, spyware, crypto miners and any other malware type • The solution must identify malicious behavior of executed files\running processes\registry modifications\ memory access and terminate them at runtime, or raise an alert (exploits, fileless, Macros, PowerShell, WMI etc.). • The solution must support the creation of rules to exclude specific addressed/IP ranges • The solution must identify and block privilege escalation attacks. • The solution must identify and block reconnaissance attacks (scanning). • The solution must identify, and block credential theft attempts form either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).		
8.	Endpoint Detection & Response • The solution must cover the full kill chain of an attack. • The solution must provide the ability for incident data search and investigation within the Current/real-time/last known system state – search all systems for running processes. • The solution must provide the ability for incident data search and investigation within the Indicator Checks – periodically scan systems for artefacts derived from threat intelligence. • The solution must deliver scheduled hunting based on specific queries. • The solution must provide the capability for blocking unsigned application based on hash. • The solution must protect against File-less and malware free attacks. • The EDR Solution should be provided by the NextGen AV vendor and not rely on any third party.		

	• The solution must identify and block/alert on lateral movement (SMB relay, pass the hash, etc.). • The solution must identify user account malicious behavior, indicative of prior compromise • The solution must identify malicious interaction with data files. • The solution must identify data exfiltration via legitimate protocols (DNS tunnelling, ICMP tunnelling). • The solution must identify and block usage of common attack tools (Metasploit, Empire, Cobalt etc.). • The solution must have an internal protection mechanism against access and manipulation of unauthorized users. • The solution must continuously collect data on all the entities and their activities within the environment. • The solution must support the display of entity and activity data. • The solution must support dynamic analysis (i.e. sandbox). • The solution must support cross-organization queries. • The solution must support the means to execute forensic investigation. • The solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint. • The solution must support isolation and mitigation of malicious presence and activity globally across the entire environment. • The solution must support response automation.		
9.	Integration • The solution must have open-APIs to integrate with different security vendors: Email Security, NDR, SWG, SOAR, etc.		

	The solution should be able to integrate with any SIEM. List SIEM compatibility • The solution must provide REST APIs allowing the industrialization of certain processes.		
10.	Device Control • The endpoint solution should prevent unauthorized endpoint use of connected mobile devices and removable media. Most notably USB storage drives for Windows and Mac. • Identify the USB device and restrict Read, Write, Execute, etc. for Windows and Mac. • View the file-names written to USB storage devices. • Block or allow specific USB devices based on vendor, type or by serial number for Windows, Mac and portable devices.		
11.	Firewall Management • The solution must provide Host-Based Firewall capabilities for Windows and Mac Devices. • The solution must provide customizable network firewall rules. • The solution must provide ability for grouping Network Firewall Rules • The solution must provide automated switching of group firewall rules based on network located.		
12.	SOAR (Security orchestration, automation and response) • The solution must provide the SOAR functionality of creating automation workflows for response, out of the box, at no additional cost, and with no need to write code. • The solution should have the ability to send custom email with detection details, such as hostname, user, OS, IP address, MAC address. • Solution should have the ability to send channel notifications to concerned team • Solution should be able to send alert if it detects machines connected to the LAN but not on MauBank Ltd domain. (Detect Rogue / Shadow devices)		

13.	Asset Assessment • The solution should be integrated with AD. And should have an inventory of all the machines on the domain. • The system should be able to compare which are the unprotected and unmanaged systems and even unsupported systems • The solution must see what applications are currently running on which hosts without impacting your endpoints. • The solution should be able to prevent unapproved applications from running on the endpoints. (Application whitelisting) • The solution must analyze and show system resources (CPU, Disk Space, and Memory) with Capacity and Utilization and must have the ability to identify which process is causing any bottleneck - It must support Windows, Linux, AIX, Solaris and Mac. • The Solution should have capping capabilities to restrict CPU, RAM, Hard Disk consumption or provide documentation that 10% usage of resources will never be reached. If ever above 10% of resources usage is observed after deployment or after any upgrades, the supplier must investigate and fix same. • The solution must show failed login activities and any brute force attempts • The solution must show users/system (domain or local) with the password age. • The solution must show encrypted and un-encrypted HDD drives.		
14.	Vulnerability Management • Automated assessment for vulnerabilities without scanning based on historical pattern. • Initiate emergency patching for critical vulnerabilities with native integrations for Windows OS Unix and should follow control update procedure		

	• The solution must support File Integrity Monitoring (FIM). • The solution must have built-in vulnerability assessment. • The solution must provide the means to conduct Inventory Management. • The solution must provide log collection and retention. • The solution must include threat hunting. • The solution must support the discovery of unattended attack surfaces. •		
15.	Managed Threat Hunting • Managed Proactive Threat Hunting service 24 x 7 as an option • Provides a dedicated 24/7 team of security experts that hunt for threats, prioritize alerts, and guide response as an option • The threat hunting service should be provided by the EDR vendor and not rely on any third party. • The service must provide actionable alerts with remediation recommendations. The alerts must be crafted to provide detailed analysis needed to understand what happened and how to respond the incident. • The threat hunting service should NOT be based on managed alerts, it should be based on actual threat hunting performed on the raw telemetry events.		
16.	Managed Detection & Response (MDR) • 24/7 Management and monitoring for Endpoint Security including EDR as an option • 24/7 remote remediation for timely, hassle-free incident resolution as an option • MDR vendor must have their own Threat Intelligence Service. • In the event where the solution fails to provide protection and results in damage and financial loss to the bank, the vendor is obligated to provide cyber security insurance coverage.		

	• Supplier to provide an independent benchmarking of the solution. • Identify technical root cause and source of compromise at no additional cost • MDR vendor must provide a cyber-security Insurance amount on their proposed solution in case the latter fail to detect an attack which cause financial loss to the bank. • Amount of the cyber insurance to be specified • Supplier to provide Escalation Structure matrix • The vendor must provide the capability to reach the managed service team for questions, escalations etc. through a variety of methods such as Email, In-platform messaging system, access to a program manager (assigned single point of contact) • The bidder should comprehensively outline the delineation of responsibilities between the bank and the supplier, including the ownership of respective tasks. This should encompass a detailed list of tasks that are expected to be carried out by the supplier and those that fall under the bank's purview. • Provide detailed reporting about remediated systems. • Provide list of ownership between bank and supplier		
17.	User Access • Solution must be able to integrate with multi-cloud directory. • The solution should support multi-factor-authentication (MFA). • Provide customizable roles for users. • Ability to create a whitelist of IP address to restrict access to only a specific network.		
18.	Solution Model • Cloud management on Software as a Service (SaaS) model • The solution must be controlled from a single management console		

	• Security Assessment report (VAPT, Blackbox, Greybox, secure coding, amongst others) of the Platform must be shared with the bank on a yearly basis.		
19.	Identity Protection • The solution must provide full visibility AD authentication and access protocols, including, at least, NTLM, Kerberos, LDAP, LDAPS, RPC and RDP. • The solution should have built-in User and Behavioral Analytics (UBA) feature, coupled with the inherent capability to discern compromised passwords through advanced intelligence mechanisms; in turn, enables the system to proactively inhibit users from employing passwords that have been compromised, thus exemplifying a robust commitment to bolstering security protocols and safeguarding the sanctity of the user authentication process. • The solution must retrieve authentication information in real-time via deep packet inspection to provide a complete view of the protocol activity, and not just logs from third-parties. • For each detection and alert, the solution should provide guidance and mitigation actions for security analysts to take to stop and, if necessary, recover from the attack. • The solution must be able to prevent (block) activity resulting from users with compromised credentials. • The solution must integrate and share contextual data with EDR to provide full coverage across the entire MITRE ATTCK framework. • The solution provides the ability to configure decoy misconfigured or vulnerable accounts and assets, to lure attackers, and monitor activity against those deceptive assets.		

	• The solution must support third party identity providers (Azure Active Directory; Okta...) • The solution must also provide visibility into federation services, including multi-cloud ADFS domain. • The information collected from the solution should include at least the last 120 days of user's login activity. • The solution must include full visibility into the risks AD and online SSOs are exposed. In this sense, the solution must include both weaknesses and vulnerabilities that attackers could exploit, as well as signals of possible ongoing attacks. • The solution must provide discovery of privileged accounts, stealthy privileges through delegated permissions / ACLS, and classification of accounts human, executive, or service accounts. • The solution must be able to automatically learn the behavior of every user and device on the network, to auto-classify privileged users, service accounts. stale accounts, etc., and measure risk dynamically on each of them.		
20.	Platform Support • To include Windows desktop versions from Windows 7 SP1 and newer • To include Windows Server 2008 SP1 and newer • To include systems such as Red Hat, Ubuntu, Open SUSE, AIX, Solaris, Oracle linux • Include mobile operating systems Apple iOS and Google Android. The solution should be compatible and deployable via the bank Mobile Device Management. • Include support for Tablet, ATMs, Thin client • The solution must support Virtualized environments. • The solution should support containerized environments.		
21.	System Documentation		

	• Include detailed system documentation to show how the system will work, network diagrams, data flow and admin tasks.		
22.	Implementation of Endpoint Solution • The supplier should provide implementation services for the Endpoint solution. The supplier will be responsible to remove all existing AV, ATP, EDR, solution and deploy the selected product without impacting on business of the bank. • The professional services should be provided by a certified expert with proven experience of implementing the same product. • Certification to be submitted for team that will be part of the deployment on our site. • All policies must be reviewed / enhanced by new features from AI and ML of the solution and implemented by the service provider to cover the current AV / ATP / EDR Security control in place at the bank. The policies must be vetted by the solution provider to ensure that all the best practices are in place and a report should be provided to the bank to certify same. • Normal end-user with non-administrative privilege / Local Admin / Windows Admin users should not be able to stop the Solution from running • The solution should have customizable reports and all data must be accessible for at least 120 days.		
23.	Training • The certified expert will have to deliver training to support the team regarding the management of the solution, policies and reports that can be extracted.		
24.	Licensing • Supplier to provide different option of licensing on 1,000 nodes		
25.	Bidder Competencies		

	• The Bidder must have minimum 2 persons certified in the proposed solution, and the latest certification must be provided. Please specify the level of certification. The bank reserves the right to crosscheck same with vendor. • The bidder must have deployed the proposed solution to a minimum 3 to 5 clients in Mauritius / abroad. Provide detail information of person to contact. • The bidder should implement the solution on-site. Support on MDR may be managed from abroad. • The bidder should provide testimonials on the deployment of the proposed solution • The bidder must provide 24/7 support / MDR for the solution as an option		

Note that supplier will have to demonstrate capability on how to meet bank requirement on each point elaborated in above table. Any inappropriate information provided just to comply with bank requirement may lead to direct dismissal and jeopardize future business with bank.

Business Process Overview

4.1 Current Business Process (As-Is)

Currently bank has dual endpoint solution namely Symantec Endpoint Protection with EDR and Sophos full suite covering nearly 1,000 nodes. The Endpoint enable features are

- Endpoint firewall
- AV Scanning
- Block storage devices thru unique identification
- Advance Threat protection
- Detection and response
- Weekly schedule scan
- Quarantine and sand box
- Logs storage for forensics
- Tamper protection
- Malicious URL
- Remote deployment

4.2 Current Business Process (To-Be)

The methodology approach will be as follows:

1. The deployment will be in gradual manner not big bang
2. Priority will be given to servers on windows and unix followed by laptop and desktop
3. Removal of current endpoint solution and replace with proposed solution should be done on same day
4. The task can be performed in batches given we have different location and different component category
5. High probability that automated removal of endpoint may not be feasible, supplier have to provide necessary resources on all location of MauBank including Rodrigues to do manual removal and deployment of new endpoint
6. Supplier should note that not all workstation and server has direct internet connection access.
7. Supplier to demonstrate how they will address the constraint given that bank will not compromise on releasing internet access to those servers / workstation.
8. Those servers / workstation which do not have access to internet should go thru a relay system (This should be a feature in the proposed solution) thru proxy to reach internet
9. In case of issued encounter during automatic / manual deployment supplier should come forward to find resolution in a prompt manner
10. Failing to deploy the endpoint solution in the prescribe timeline agreed by both parties may entail to penalties which will be define in SLA
11. Supplier to provide a detail plan on the deployment taking into consideration all above parameters

4.3 Risk

- People risk
  - Availability of business team to conduct UAT in planned period
  - Delay in providing UAT result may impact on deliverables date
  - Unforeseen technical issues may impact deliverable date
  - Supplier unavailability due to a force majeure may impact deliverable date
- Technical risk
  - Network disruption
  - Server unavailability
  - Supplier resource unavailability

4.4 Business Requirements

The requirements in this document are prioritised as follows:

Value	Rating	Description
1	Critical	Force majeure on people availability at bank or supplier level
2	High	Resources allocated in the project Comprehensive testing

		Confirm scope of requirement Meet target date set
3	Medium	Support of the project sponsorship and members
4	Low	Issues that can be tackled post live

3. Supported documents (Annexures)

3.1 Technical Compliance
3.2 Bandwidth requirement
3.3 Management server
3.4 Information Security requirement
3.5 Price tabular format
3.6 Cloud Security document
3.7 Internal Control Compliance document

4. Assumption

1. Provide a full SLDC plan for the next 5 years to sustain the viability, reliability and of the automated tool.
2. Supplier share all the in-built security features of the automated tool and how same is being kept updated throughout the SDLC
3. The solution shall reduce the number of unwanted traffic going into production
4. Lesson learn help in future development with our business partners
5. A study of metrics which help reduce defects and policy violation while reviewing the parameters
6. The solution must have flexible server deployment options to match various types of environments. (On premise, Cloud and hybrid)
7. The solution must support rapid and seamless installation across all endpoints/servers in the environment.
8. The solution must support automated distribution on endpoints/servers that were joined to the environment following the initial installation.
9. Autonomously discover newly added machines and have the agent installed on them without need of manual configuration.
10. The solution must have a light footprint for minimal impact on the endpoint/server performance.
11. The solution must provide an encrypted communication between the management server and the agents on the endpoints/servers.
12. The solution must support all commonly used Operating Systems such as Windows, Linux, Solaris, and AIX among others.
13. The solution must support connection to Active Directory.
14. Granular authentication to the UI
15. Deployment to various OU groups with AD.
16. The solution must co-exist with all commodity and proprietary software on the endpoints\servers.
17. Seamless operation of the protected endpoint/server without bluescreens or process crashes
18. The solution must provide full protection for endpoints and servers that are offline from the organization's network.
19. Threat protection mechanism that do not rely on connectivity to the management server.

20. The solution must collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner.
21. Eliminate the need of manual configuration of rules or policies or reliance of additional devices
22. The solution must have the ability to specify a list of alert exclusion rules for the selected objects.
23. The solution must support deployment on multiple sites that report into a single management console.
24. The solution must have the ability to export the current configuration of the program in order to later be imported to the same or another computer
25. The solution must have the ability to enable/disable certain types of notifications
26. The solution must provide a central collection and processing of alerts in real-time.
27. The solution must have the ability to rate the severity of security alerts.
28. The solution must have the ability to block access to the program settings for end users
29. The solution must provide a central distribution of updates without need of user intervention and of restarting the endpoint/server
30. The solution must provide a central distribution of updates without need of user intervention and of restarting the endpoint/server.
31. The solution must have the ability to specify a schedule for downloading updates, Including the ability to disable automatic update.
32. The solution must assign a risk score to all objects within the protected environment
33. The solution must support the logging of events, alerts and updates.
34. The solution must support integration with email infrastructure to notify security personnel in case of alerts.
35. The solution must support standardized and customizable reports
36. Supplier to provide details how far they are compliant to bank assumption base on above listing.

5. Return on Investment

This requirement is from regulatory to address risk in our payment echo system. Gains from the successful implementation of this project are

1. Reduce bank surface attack
2. Reduce exploitable vulnerability which can lead to service disruption
3. Reduce data theft which can damage bank reputational image
4. Align with Bank of Mauritius guideline
5. Reduce financial loss

Technical Compliance

#	Item	Description	Comply Y / N	If comply provide explanation of compliance
1	System type	Whether solution is server based, Appliance, hybrid or fully cloud		

2	System Network Architecture	HA setup available		
3	System Admin	The administrator must be able to define role-based access		
4		The role-based access must be able to restrict a user's access to specific functions		
5	Operational requirement	The system must be scalable, provide a framework for future expansion		
6		The system must deliver sample dashboards out of the box for threat management, compliance management, and executive dashboards, among others.		
7		The system must provide ability to send notification of correlated alerts via Simple Network Management Protocol (SNMP) trap through Email, SMS, amongst others.		
8		The system must provide a mechanism to track security incidents across a wide range of relevant attributes		
9		The user must be able to filter incidents along the defined attributes.		
10		The system must provide advanced Managed Detection and Response (MDR) analytic detections including start/stop processes		
11		The system must provide file integrity monitoring.		
12	Log Management and Processing	The system must have a log collection and archive architecture that supports short-term (online) event storage.		
13		The system must provide support for easy collection of log		
14	System Reporting and Dashboards	The system must provide reporting on all items available		

15		The system must provide a configurable reporting engine for customized report creations which support various data representations such as Tabular, Graphical, Charts, among others.		
16		The system must support the ability to automate distribution of reports and schedule reports delivery.		
17		The system must provide templates for easy creation and delivery of reports at multiple levels e.g., executive, operations, business etc		
18		The system must provide default out-of-the-box reports for typical business and operational security issues		
19		The system must provide Findings Reports with tailored guidance and recommendations		
20		The system must provide emerging Threat Reports from threat intelligence		
21	Correlation and alerting	The system must provide alerting based on observed security threats from monitored devices and on established rules and policies		
22		The system must support prioritization of incidences based on thresholds through alert		
23		The system must provide capabilities to minimize false positives and deliver accurate results.		
24		The system must support easy creation of correlation rules.		
25		The system must provide realtime analysis of events and streaming view that supports full filtering capabilities.		
26		The system must be able to inspect packet data and network communication to facilitate identification of malicious activity		
27		Full incident validation to eliminate false positives.		

28	Network activity monitoring	The system must support traffic profiling		
29		The system must identify network traffic for potentially risky and banned applications		
30		The system must be able to profile traffic originating from or destined to the Internet by Geographic regions, in real-time.		
31	Advance threat management system	The system must provide the ability to contextually link reported security events with real-time knowledge of the assets that are being targeted		
32		The system must support Customer Behaviour Analytics (UBA) and machine learning capabilities for intelligent and predictive threat intelligence		
33	Industry standard	The system must be in the leaders' section of the Gartner Quadrant, Forrester or any other		
34	Data Protection	In case the solution is hybrid/on cloud, the vendor must comply with the relevant Data Protection laws.		
35	Proof of Concept (POC)	The selected bidder may be asked to conduct a proof of concept to demonstrate all the compatibility point that meet bank requirement failing which the bidder may be eliminated		
36	Support	An all-inclusive 24x7 on premise (if Appliance Base) or remote (for cloud base) support for the System for a period of five (5) years starting from the date of the System commissioning.		

Bandwidth requirement

	Head office Ebene	Sub office Ebene	Secondary data Center	Branches
On Premise Solution				

Hybrid / Cloud Solution				

Management Server.

The specification for the server is as follows in case bidder opt for on premise solution

Feature	Specify
Processor Architecture	
Processor Clock Speed	
Number of vCPU	
Multi-threading support	
Hyper threading support	
Virtualization support	
Memory	
Storage	
Network interface	
Operating system	
database	
Web browser	
Any other 3rd party tool	
Java support	

Pricing template

On premise option-1 onetime cost

#	Item description	Total Cost
1	Software license	
2	hardware	
3	Web base / 3rd party license	
4	implementation	
5	Training	
6	MDR	
7	Other	
8	Support and maintenance 1 year upfront after commissioning	
9	Taxes	
10	Total	

On premise option-1 maintenance cost for 5 years

#	Items description	Year-1	Year-2	Year-3	Year-4	Year-5
1	Software license					

2	hardware					
3	Web base / 3rd party license					
4	MDR					
5	Any other					

Hybrid / On Cloud oprion-2 onetime cost

#	Item description	Total Cost
1	Software license	
2	Cloud service	
3	Web base / third party license	
4	implementation	
5	Training	
6	MDR	
7	Oher	
8	Support and maintenance 1 year upfront after commissioning	
9	Taxes	
10	Total	

Hybrid / on Cloud Option-2 maintenance cost for 5 years

#	Items description	Year-1	Year-2	Year-3	Year-4	Year-5
1	Software license					
2	Cloud service					
3	Web base / third party license					
4	MDR					
5	Any other					

Information Security Requirements

Description of security features	Comply
If cloud architecture is used, the supplier should provide details on information stored in cloud. The Bidder should provide details on how the information is stored, segregated and secured	
The database proposed and implemented for the systems should allow for encryption of sensitive data, auditing of user access and transactions in the data base.	
Unnecessary database users (e.g. root, admin), default passwords and stored procedures shall be eliminated and the principle of least privilege for the application database	
During implementation, secured protocols shall be used to communicate with the database	
Restricted administrative access should be implemented.	
The solution provider shall apply the latest stable patches and updates available on all systems deployed.	

OS Hardening shall be performed for all systems deployed for this solution	
The application should provide the user the functionality to setup complex passwords consisting of uppercase, lowercase and special characters. The application should have a separate user administration module for user access administration.	
Proper mechanism shall be implemented to ensure that user access reviews are properly replicated to the DR site.	
User Access to modules shall be on a least privilege and on a need-to-know basis.	
The application should create session keys with lengthy strings or random number to prevent guessing of valid session key.	
Encryption of data and session key that is transferred between the user and the web servers should be implemented. HTTPs or equivalent secured implementation will be required for all web-based applications.	
Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions. Implementation of these controls helps ensure system integrity; that applicable system functions operate as intended; and that information contained by the system is relevant, reliable, secure and available when needed.	
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.	

Cloud Security Document

Compliance with the Regulator Guidelines			
1.	Please provide a description of the proposed cloud services, including details on:		
	i. type of IT assets involved;		
	ii. chosen cloud service model;		
	iii. chosen cloud deployment model;		
	iv. activities/functions to be hosted on cloud; and		
2.	Oversight	Has an assessment of the adequacy of the internal resources for an effective oversight on the cloud services been conducted?	
		Please provide the Shared Responsibility Matrix for the service.	
3.	Did the risk assessment cover the following:		
	evaluation of criticality and sensitivity of the IT assets and the materiality of the services;		
	evaluation of the impact of changes required to processes and procedures;		
	Assessment to determine whether a privately managed environment on a virtual private network is required where the bank intends to opt for a public cloud for hosting customer information;		
	identification of the roles and accountabilities of the bank and the cloud service provider under the shared responsibility model;		
	assessment of the adequacy of the control framework;		

	the impact of possible risk events including failure of cloud service provider, disruption of services, exit and the implications for transferring services in-house or to another cloud service provider, if required;	
	the adequacy of contingency and exit plan including the interoperability and portability of data and services;	
	the risk of foreign authorities having access to its data; and	
	the relevant regulatory and legislative requirements?	
4.	Did the supplier perform a vulnerability assessment and address all identified gap? If yes please share the latest report	
5.	Were the following factors considered in the assessment of materiality:	
	i. the nature (including criticality) of the services and of the IT assets;	
	ii. the potential direct/indirect impact that a confidentiality breach or failure or disruption of the services could have on the institution and its customers. This includes the ability of the bank to meet its legal and regulatory requirements and to continue its business operations and provide its services;	
	iii. the cost of the services as a share of total operating costs;	
	iv. the degree of difficulty to find or migrate to an alternative provider or to bring the services in-house;	
	v. the potential impact of the service on current and projected earnings, solvency, liquidity, funding and capital and risk profile; and	
	vi. the ability to maintain appropriate internal controls and meet regulatory requirements in case of operational failures by the service provider?	
6.	Please provide the name of the cloud service provider.	
7.	Please specify the type of cloud service provider (third party or intra-group entity)	
8.	Has the due diligence been documented and approved?	
9.	Were the following factors considered in the due diligence exercise:	
	i. the adequacy of the cloud service provider's risk management and internal control systems, information security capabilities, security controls including the controls for protecting the confidentiality, integrity and availability of data;	
	ii. the cloud service provider's compliance with the requirements of this guideline, the applicable data protection, confidentiality and information security regulations or other legislations and adherence to international IT standards;	
	iii. The willingness and ability of the cloud service provider to service commitments even under adverse conditions, for instance, in the event of a cyber-attack or data theft;	
	iv. the ability of the cloud service providers to recover outsourced systems and IT services within the stipulated recovery time objective;	
	v. the verification of whether the personnel of the cloud service provider (including employees and subcontractors) with access to customer information are subject to adequate background screening, security training, access approvals and confidentiality arrangements as allowed by applicable law;	

	vi. forward looking assessment of the financial and operational resilience of the cloud service provider; and	
	vii. an assessment of the proven track record of at least five years of the cloud service provider for such services?	
10.	Did the supplier take into consideration the findings of vulnerabilities assessment, penetration testing, audit and/or other reviews provided by the cloud service provider, where relevant?	
11.	Is the agreement between the cloud service provider and the bank in line with all the requirements set out in the Guideline?	
12.	What is the applicable law governing the agreement?	Mauritian Law
13.	Has the Supplier ensured that the agreement with the cloud service provider does not consist of clauses that would hinder the Bank from exercising its supervisory powers?	
14.	Does the agreement contain appropriate provisions to ensure compliance with the Data Protection Act 2017?	
15.	Does the agreement contain confidentiality obligations which are in line with the underlying objective of section 64 of the Banking Act 2004?	
16.	Does the agreement contain appropriate provisions on:	
	i. the right of audit (including remote audit) by the Bank, the financial institution, its external auditor, or any third party appointed by the Bank, the financial institution or its external auditor and right of access to relevant audit reports/ reports of other tests conducted by the cloud service provider;	
	ii. the obligation of the cloud service provider to cooperate with the Bank and provide access to information required by the Bank, the financial institution, its external auditor, or any third party appointed by the Bank; and	
	iii. the right of the Bank or any third party appointed by the Bank to promptly take possession of all the cloud services and data relating to the financial institution in the event the Bank decides to revoke the licence of the financial institution or appoints a conservator?	
17.	Please provide the type of network connection used for data transmission between the institution and the cloud service provider and the network security measures employed therein, accompanied by a detailed network diagram	
18.	Are the reviews, audits, testing and control functions performed in line with the requirements in the Guideline?	
19.	What is the schedule of audit, testing and other reviews to be conducted by the cloud service provider?	
20.	Which Information security standards does the cloud service provider meet? (e.g. PCI DSS, ISOxx, etc.…)	
21.	What certifications does the cloud service provider possess?	
22.	Does the financial institution meet all the requirements in respect of data location?	

23.	Has a due diligence been conducted on the countries where the data will be hosted by the supplier?		
33.	Does the cloud service provider make provision for law enforcements access based on a policy defined and agreed between the bank and the cloud service provider?		
24.	Does the cloud service provider adhere to Mauritian data protection laws (e.g. DPA 2017, ICTA, etc…) or to data protection laws which are equivalent to the Mauritian data protection laws? If no, please provide details on data protection laws that the cloud service provider adheres to.		
25.	Are Personally identifiable Information (PII) protected? If yes how?		
26.	Will personal data be exported? If yes, have the requirements under the DPA 2017 been met?		
27.	Data at rest	Are the data at rest encrypted?	
28.		What is the encryption strength?	
29.	Data in transit	Are the data in transit encrypted?	
30.		What is the encryption strength?	
31.	Processing data	Are data processed in a secured environment?	
32.	Data Ownership/Access	What are the measures in place to ensure retention of ownership rights of the data on cloud?	
33.		What are the measures in place to prevent unauthorized access to confidential information?	
34.	Data location	Specify the geographic locations where the data is:	
		i. processed.	
		ii. stored.	
35.	Terms and usage of cloud service	Describe the data and usage terms of the cloud service.	
36.	Exporting data	What are the methods available for exporting data?	
37.	Protocols for sharing/interfacing	What are the permissible methods for sharing/interfacing with cloud data?	
38.	Data examination	Describe how does the cloud service provider examine/monitor data of financial institution?	
39.	Are the contingency plans for the proposed cloud service in line with the requirements the Guideline?		

40.	Do the exit plans for the proposed cloud service cover all the requirements in the Guideline?		
41.	Termination of services	Is there a clear process for service termination? (e.g. Exit plan)	
42.		How long does it take for a full data wipe out? What are the arrangements in place for wiping of data?	
43.		How and when is the financial institution notified after deletion?	
44.		What are the alternative solutions/arrangements that have been identified?	
45.	Service	Are there clear mechanisms for monitoring the cloud services being provided?	
46.		What is the latency on the network?	
47.		What is the network bandwidth throughput?	
48.	Availability	What is the percentage time that the service is available and usable?	
49.	Elasticity	How fast can the cloud service provider provision or adjust a given service?	
50.	Service resilience	What are the fault tolerance levels and methods put in place by the cloud service provider? (e.g. Network resilience, Data resilience, etc…)	
51.	Disaster recovery	What is the maximum time taken to perform a disaster switch in case of a system outage?	
52.		What is the Recovery point objective (RPO)?	
53.		What is the Recovery time objective (RTO)?	
54.		What are the fallback measures FIs intend to take in case network connectivity between Mauritius and the outside world is disturbed for more than 1 hour?	
55.	Backup & restore	What are the provided methods of backup?	
56.		What is the backup retention period?	
57.		Does the backup utility adhere to your backup policy?	
58.		Are the backups encrypted?	
59.		What is the encryption strength?	
60.		What is the location of the backup storage?	
61.	Support	What type of support packages are available?	
62.		What is the chosen level of support?	

63.		What is the support service channel? (ticketing system, phone, email…)	
64.		What are the notification and alerting methods provided?	
65.		Is there a change request channel?	
66.	Incident management	Is there an incident management process in place?	
67.		Are incident reports provided?	
68.	Please provide the name of the sub-contractor for material cloud services. If any		
69.	Has a due diligence been conducted on the sub-contractor?		
70.	Please provide an assessment of the suitability of the cloud service provider's substitutability and of the portability of the data/services on cloud as easy, moderate or extremely difficult.		
Compliance with Internal Control			
1	**Hardening**	Do you perform security hardening of all system components (servers hosting the application, the network devices in the scope, the administrator's workstations having access to the application, etc)?	
2		If yes Provide details of hardening configurations in place for each system components where the bank's system will be hosted/accessed	
3		Are the hardening configuration standards reviewed at least annually against industry-accepted system hardening standards?	
4	**Identity Access Management**	Multifactor authentication should be provided on the platform.	

5		The password parameters should comply with the following Password Complexity: Passwords must be a mix of all of the following: a. Lower case alphabets b. Upper case alphabets c. Numbers d. Special characters (e.g. #, *, &, !, etc) e. Password Length should be configurable - to accommodate at least 8 characters f. Password Expiry should be configurable g. Password history should be configurable h. Prompt User to change password on first time login or after Set Password Expiry i. Account lock mechanism should be configurable for failed login attempts j. Disable inactive user accounts as per set days.	
6		The bidder should provide details on method used for password encryption, including details on encryption keys, encryption algorithm and storage of encryption keys Strong cryptography and secure protocols should be used as per industry standards and best practices. Password files are to be unreadable during storage	
7	**Session management**	Simultaneous login sessions with same user ID should not be allowed.	
8		The system should be configurable for the period of inactivity.	
9		The system should allow configuration of User session termination after the configured period of inactivity	

10	**Patching**	What is the process followed for patching of system components (servers hosting the application, the network devices in the scope, the administrators workstations having access to the application, etc)?	
11		What tools are used to verify patching level of system components?	
12		Provide details of scanning policy configured on each tools	
13		Please provide the bank with latest patching reports for all in scope system components	
14		Patching reports to be provided on a monthly basis	
15		The bidder should provide the product's roadmap for version upgrades to be compatible with latest security patches and OS releases.	
16	**Network Segmentation**	Is Network segmentation in place?	
17		If yes, please provide a network topology of the hosting environment, highlighting where the bank's systems will be placed	
18	**Pen Test**	Do you perform regular internal and external penetration tests on the hosting environment?	
19		If yes, at what frequency?	
20		If yes, please share latest internal and external penetration test reports to the bank	
21		Penetration test reports to be shared regularly with the bank as and when these are executed or based on request.	
22		MauBank will be performing independent Penetration Testing on the Application on regular frequency, the hosting environment should be able to support same	

23		Any identified vulnerability during the pentest should be fixed by the vendor in a timely manner depending on criticality based on Vulnerability Handling	
24	**Network Control**	Will Other services be hosted on server hosting the application?	
25		If shared platform is being used how data segregation is being done, should be shared with the bank.	
26		Is there a Web Application Firewall in place to protect the Application?	
27		Is there an Intrusion Prevention System in place to protect the Application?	
28		Is there DDOS protection in place to protect the Application?	
29		If yes evidence regarding Anti-DDoS protection testing must be provided	
30	**Antivirus**	Is Anti-virus software is deployed on servers hosting the systems?	
31		If yes, Antivirus installed and configuration applied must be shared	
32		IF Yes Anti-virus software should: • be always up-to-date • Perform periodic scans • Generate audit logs	
33	**Vulnerability Assessment**	Are Internal and external network vulnerability scans are run regularly?	
34		If yes, what is the frequency of the scans?	
35		What is the process to review the VA results and closing of risks identified?	
36		Provide details of scanning software used and policy configured for the scans	
37		Any identified vulnerability during the vulnerability scanning should be fixed by the vendor in a timely manner depending on criticality	
38		Please share latest vulnerability scan results with the bank on an agreed timeline or when required.	
39	**Vulnerability Handling**	Critical severity Vulnerabilities should be addressed within 15 days from reported date	

40		High severity Vulnerabilities should be addressed within 1 months	
41		Medium severity Vulnerabilities should be addressed within 2 months from reported date	
42		Low severity Vulnerabilities should be addressed within 3 months from reported date	
43	**Access Control**	What is the process to manage logical access to system components (servers, network devices, etc)	
44		Are generic users used for server/Network management?	
45		How will management of the Application be carried out (update of applications, etc). Please provide full details on process, responsibilities, and technical details	
46		System to provide for user profile based access control.	
47		System to allow user-specific special access level over and above profile based access control.	
48		System to provide Admin - modify / users view only access rights.	
49		System to provide an admin module to create, manage users with distinct privileges.	
50	**Audit Trails**	Are Audit trails enabled on all systems in scope of hosting the Application/systems?	
51		If in place are at least events below logged? User identification, Type of event, Date and time, Success or failure indication, Origination of event, Identity or name of affected data, system component, or resource.	
52		Are audit trails sent to a SIEM for analysis and correlation?	
53		All audit logs to be retained for at least one year (online) and offline for 7 years	

54		Are all system clocks synchronized to a central NTP?	
55		If yes evidence regarding NTP config on sample devices impacting MauBank must be provided if selected	
56	**Security Monitoring**	Is there 24/7 Monitoring of alerts from security systems?	
57		If yes, please share details of escalation process in case high risk security incidents are detected	
58	**Information Security Policy**	All personnel acknowledge in writing or electronically that they have read and understood the security policies/procedures	
59		Is there a Data retention and disposal policies, procedures in place	
60		What is the exit mechanism in place to provide for the deletion of all data stored on the cloud servers, in the event that MauBank terminates the hosting services?	
61	**Audit and Visit**	MauBank and the Bank of Mauritius must be allowed the right to visit/audit the facility to check compliance to the policies and controls on MauBank systems as and when required This must be formally specified in the contract between the bank and the service provider	
62	**Data Privacy**	Can the system record retention period for data being stored? If yes, provide full details on the mechanism in place to record retention period, review expired data and process to purge expired data.	
63	**Browser support**	The application/system must support the latest version of default browser shipped with supported devices	
64	**End User privileges**	The users must be able to run the application with least privilege on their devices	

65	**Logical Access Control Feeds**	Reports of logical access rights configured in the system should be made available as per banks required format Reports should be automatically generated on a daily/Monthly and saved in CSV format in a specific folder determined by the bank	
66	**WebApp**	The bidder should follow secure coding practices as per Industry standards and best practices? Input Validation, Output Encoding, Authentication and Password Management, Session Management, Access Control, Cryptographic Practices, Error Handling and Logging, Data Protection, Communication Security, System Configuration, Database Security, File Management, Memory Management, General Coding Practices Industry standards and best practices must be followed during web application development such as OWASP: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring The bidder should provide evidence of Independent code reviews	
67	**Open Source Libraries**	Provide the list of Open Source libraries/software's required for the running of the solution e.g. Java	

68		Vulnerabilities identified in any of the above Open source libraries/software's should be handled as per Vulnerability Handling	
69	**No Screenshot**	Screenshot capture should be disabled on all Platforms when the application runs or user access same.	
70	**Watermark (if applicable)**	Watermark should display the username who is logged in with time stamps for all documents being viewed.	
71		Watermark should be present throughout the page	
72		Watermark should be visible on the captured picture if screen content is captured using a camera	
73		Watermark removal should not be part of global parameter (It should be part of the solution). That is the administrator should not have the access to disable the watermark	
74		If screenshots cannot be disabled Watermark should be captured in print screen as well.	
75	**Application audit Logs**	Implement audit trails to link all access to system components to each individual user. All actions taken by any individual on the platform be it front end or back end should be logged Access to all audit trails should be restricted and tamperproof. Logs must include at least User identification, Type of event, Date and time, Success or failure indication, Origination of event, Identity or name of affected data, system component, or resource.	
76		The application audit trail logs should be easily exportable into standard formats for analysis (csv, syslog, etc)	
77		The system should provide an online search facility of audit trails.	

78		The System should synchronize its time settings with a reliable NTP server	
79		Retain application audit trail history for at least one year online and 7 years offline	
80	**File-integrity**	All file changes, uploads, must be logged and only authorized users should be allowed to upload and amend documents. All activities should be logged as per above Application and System Logs	
81	**File sharing**	The application should not provide sharing facilities of documents - Users should not be allowed to forward, share, email or exfiltration documents outside.	
82	**Regular test security system and processes**	Run internal, external network vulnerability scans and App/Penetration testing. Reports must be shared with MauBank	
83		Application security testing by external parties' evidence to be provided to MauBank and report should be shared with MauBank whenever there are major changes.	
84	**Infrastructure Security Performance**	Patching cadence (days to patch and EOL OS as measured by Systems / Patch Manager)	
85	**Data Breach**	what is the shared responsibility provide different level of security provided Service provider to provide all necessary logs to facilitate any investigation or forensic report	

INSTRUCTION TO BIDDERS

1. Bids shall remain valid for the period of **120 days** after the submission deadline date as prescribe below. MauBank shall reject a quote valid for a shorter period as non- responsive.

2. Your response addressed to the Chairperson of Bid Opening Committee should be sent through a password protected email to the Procurement department with subject "**End Point Security Project - Ref: RFP/ICT/2023/72"** latest by **12.00 hrs.** (Mauritian Time) on **Monday, 16 October 2023.**

   Your proposal response must be password oriented strictly sent to: -

   - The procurement department on the following address - procurement@maubank.mu
   - The password to open the proposal should be shared on Bidopeningcommittee@maubank.mu just after the closure date and time (i.e. between **12.05 hrs. to 12.15 hrs.** (Mauritian Time) on **Monday, 16 October 2023**)

3. Any bidder having any other query pertaining to the above RFQ should write to the below email address:

   1. procurement@maubank.mu

4. MauBank Ltd reserves the right to accept or reject any proposal, and to annul the procurement process and reject all bids at any time prior to contract award, without thereby incurring any liability to Bidders.

5. MauBank Ltd will reject a proposal for award if it determines that the Bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive or obstructive practices in competing for the contract in question.

6. Bidder not on the preferred list of Supplier till date, need to fill in the information sheet and also provide the KVY documents from Vendors Onboarding window.

If the email size & attachments are more 10 MB, kindly send your proposal in split emails or via drop box or we transfer.

Annexure 1.

MUTUAL CONFIDENTIALITY AGREEMENT ('Agreement')

DATE: .....th October 2023

PARTIES

I. MauBank Ltd, ("**MauBank** ") whose registered office is at 25, Bank Street, Cybercity, Ebene 72201, Republic of Mauritius

II. ……., whose registered office is at…….

……
together, the "**Parties**" and each a "**Party**".

RECITALS

A. In the course of discussions and correspondence between the Parties relating to the Proposed Transaction, each of the Parties will receive Confidential Information concerning the other, its Group, the Client and/or the Proposed Transaction.

B. Each Party recognises and acknowledges the competitive value and confidential nature of such Confidential Information and that damage could result to the other Party if it is disclosed to any third party.

C. This Agreement sets out the conditions on which each Party discloses to and receives from the other Party, Confidential Information.

1. DEFINITIONS

1.1 The following definitions apply in this Agreement:

"**Client**" means any underlying obligor or the company constituting the subject matter of the Proposed Transaction;

"**Confidential Information**" means all information relating to the Client, the Client Group and/or the Proposed Transaction, provided by the Disclosing Party (or disclosed on its behalf) to the Receiving Party and includes:

(a) all information relating to the Proposed Transaction or associated with the activities of the Client and its Group (including, its business affairs, financial dealings, operations, commercial strategies, technical information, product information, clients and supplier information, goodwill and reputation, know-how, proprietary rights, designs, trade secrets and market opportunities); and

(b) all documents that contain, reflect or use any information described in (a) above which

can be either disclosed, offered, delivered, copied, acquired by observation or participation and communicated either directly or indirectly orally, in writing, electronically, in machine readable form, text, drawings, financial models, projections, plans, specifications, analyses, compilations, comparisons, evaluations, studies, designs, applications, notes, reports, records, extracts or any other means of representing or recording and recalling information, marked as confidential,

but excludes information which:

(i) the Receiving Party already controlled, possessed or developed independently, prior to receipt from the Disclosing Party; or

(ii) was public knowledge at the time it was disclosed under this Agreement or becomes available to the public without breach of this Agreement; or

(iii) the Receiving Party lawfully receives without any such restrictions or obligations of confidentiality from a third party who in turn (to the best of the Receiving Party's knowledge and belief) received such information legally and not in breach of any obligation of confidentiality.

"**Disclosing Party**" means, in relation to any Confidential Information, the Party or its Group member which discloses such information;

"**Group**" means, in relation to a Party or the Client, that Party or the Client, each of that Party's or the Client's holding companies and subsidiaries and each subsidiary of each of its holding companies and (where applicable) representative and branch offices in any jurisdiction;

"**Permitted Person(s)**" means the directors, employees, agents and professional advisors of the Receiving Party's Group that have a need to receive Confidential Information in connection with the Permitted Purpose and that are under a duty of confidentiality to the Receiving Party;

"**Permitted Purpose**" means evaluating and negotiating the Proposed Transaction;

"**Proposed Transaction**" means **End Point Security - Ref: RFP/ICT/2023/72***;* and

"Receiving Party" means, in relation to any Confidential Information, the Party or its Group member which receives such information.

2. CONFIDENTIALITY UNDERTAKING FROM THE RECEVING PARTY

2.1 In consideration for the Disclosing Party agreeing to make available to the Receiving Party certain Confidential Information, the Receiving Party agrees to:

(a) keep the Confidential Information confidential and not (without the Disclosing Party's prior written consent) disclose it to anyone other than Permitted Persons or as provided for by Clause 3 below;

(b) keep confidential and not disclose to anyone the fact that the Confidential Information has been made available to the Receiving Party;

(c) use the Confidential Information only for the Permitted Purpose (unless disclosed under Clause 3);

(d) use reasonable endeavours to ensure that any person to whom the Receiving Party discloses any Confidential Information to (unless disclosed under Clause 3) is under a duty of confidentiality to the Receiving Party, similar to the Receiving Party's obligations under this Agreement;

(e) not make enquiries of any Client Group member or any of their directors, employees, agents or advisers relating directly or indirectly to the Proposed Transaction; and

(f) provide secure storage for all such Confidential Information in the Receiving Party's possession or control and apply at least the same security measures or degree of care as that which it would apply to its own confidential or proprietary information.

2.2 The undertakings are given by the Receiving Party for the benefit of the Disclosing Party without implying any fiduciary obligations on the part of the Receiving Party.

3. PERMITTED DISCLOSURE

3.1 The Disclosing Party agrees that the Receiving Party may disclose Confidential Information:

(a) to any insurers, auditors or service providers of the Receiving Party's Group;

(b) to any other person with the Disclosing Party's prior written consent provided that they are or will be under a duty of confidentiality to the Receiving Party;

(c) where requested or required by any court of competent jurisdiction or any applicable judicial, governmental, supervisory, regulatory or self-regulatory body;

(d) where required by the rules of any stock exchange on which the shares or other securities of any member of the Receiving Party's Group are listed; or

(e) where required by the laws or regulations of any country with jurisdiction over the affairs of any member of the Receiving Party's Group.

[3.2 If disclosure is required in the circumstances contemplated in Clause 3.1 (c), Clause 3.1 (d) or Clause 3.1 *(e),* the Receiving Party will (except where the disclosure is to a supervisory or regulatory body during the ordinary course of its supervisory or regulatory function over a member of the Receiving Party's Group), to the extent permitted:

(a) notify the Disclosing Party of the disclosure (prior to such disclosure if reasonably practicable); and

(b) if deemed appropriate by the Receiving Party, discuss with the Disclosing Party the content and extent of such disclosure.]'

4. NOTIFICATION OF UNAUTHORISED DISCLOSURE

4.1 The Receiving Party will promptly advise the Disclosing Party the circumstances (to the extent reasonably practicable and permitted) of any unauthorized disclosure, misappropriation or misuse by any Permitted Person or other third party of any Confidential Information upon the Receiving Party being put on notice of the same.

5. RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

5.1 All Confidential Information disclosed by the Disclosing Party (or on its behalf) will be deemed to be the property of the Disclosing Party and the Receiving Party and the Permitted Persons will have no rights in title except as expressly agreed to by the Disclosing Party. If the Disclosing Party requests in writing, the Receiving Party will:

(a) either return or destroy all Confidential Information in the possession of the Receiving Party;

and

(b) use reasonable endeavours to procure that the Permitted Persons return or destroy such Confidential Information.

5.2 This Clause will not apply to the extent that any applicable law, rule or regulation or any applicable judicial, governmental, supervisory or regulatory body or the Receiving Party's internal policy requires it or any Permitted Person to retain any such Confidential Information. The obligations of confidentiality under this Agreement will continue to apply in such circumstances.

6. CONTINUING OBLIGATIONS AND EXPIRY

6.1 The obligations in this Agreement are continuing and will cease on the earliest of:

(a) if either Party becomes a party to or otherwise acquires (by assignment or sub participation) an interest, direct or indirect in the Proposed Transaction;

(b) the date of execution of a definitive agreement between the Parties with respect to the Proposed Transaction; and

(c) twelve months from the date of this Agreement.

7. NO REPRESENTATION

7.1 The Receiving Party acknowledges and agrees that the Disclosing Party:

(a) makes no express or implied representation or warranty as to, or assumes any responsibility for, the accuracy, reliability or completeness of any of the Confidential Information or any other information supplied by the Disclosing Party or any Client Group member or the assumptions on which it is based; or

(b) is under no obligation to update or correct any inaccuracy in the Confidential Information or any other information supplied by the Disclosing Party or any Client Group member or be otherwise liable to the Receiving Party or any other person in respect to the Confidential Information or any such information.

8. REMEDIES

8.1 The Receiving Party acknowledges and agrees that the Disclosing Party or the Client Group members may be irreparably harmed by any breach of this Agreement and damages may not be an adequate remedy. It is agreed that the Disclosing Party is entitled to seek an injunction or specific performance or similar remedy against any conduct or threatened conduct which is or would be a breach of this Agreement.

9. MISCELLANEOUS

9.1 This Agreement sets out the full extent of the Parties' obligations. Failure or delay by the Disclosing Party to enforce any of its rights under this Agreement shall not be taken as or deemed to be a waiver of such right. No waiver or amendment of any provision of this Agreement shall be valid or binding unless the waiver or amendment is made in writing and signed by the duly appointed representatives of both Parties.

9.2 If any provision of this Agreement is found by any court of competent jurisdiction to be invalid or unenforceable, such provision shall not affect the other provisions of this Agreement, which shall remain in full force and effect. The Parties shall use reasonable endeavours to find a new provision, resembling the invalid one, taking the original intent and purpose into consideration.

9.3 All notices under this Agreement shall be in writing and shall be sent by fax or first class registered or recorded delivery post to the Party being served at its address specified above and marked for the attention of that Party's signatory of this Agreement. The date of service shall be deemed to be the day following the day on which the notice was transmitted or posted as the case may be.

9.4 Nothing contained in this Agreement shall be construed to create an exclusive contractual arrangement, association, trust partnership or joint venture or impose a trust or partnership or fiduciary duty, obligation or liability between the Parties other than provided in this Agreement or to create any duty, standard of care or liability to any third party.

9.5 This Agreement is personal to the Parties and shall not be assigned or otherwise transferred in whole or in part by either Party without the prior written consent of the other Party.

9.6 This Agreement may be executed in any number of counterparts and this has the same effect as if the signatures on the counterparts were on a single copy of this Agreement.

9.7 This Agreement constitutes the entire Agreement and understanding between the Parties and supersedes any previous agreement, understanding, warranties and arrangements between the Parties relating to the Confidential Information and the Proposed Transaction.

10. INSIDE INFORMATION

10.1 The Parties acknowledge that some or all of the Confidential Information may be price-sensitive information and that the use of such information may be regulated or prohibited by applicable legislation including securities laws relating to insider dealing, market abuse or market misconduct. The Parties undertake not to use any Confidential Information for any unlawful purpose.

11. THIRD PARTY RIGHTS

11.1 Unless stated otherwise in this Agreement:

(a) a person not a Party to this Agreement has no right to enjoy or enforce any benefit under it; and

(b) the consent of any person not a Party to this Agreement is not required to amend this Agreement.

11.2 Notwithstanding any provisions of this Agreement, the Parties do not require the consent of any Client Group member or any member of either Party's Group to rescind or vary this Agreement at any time.

12. LIMITATION OF LIABILITY

12.1 Each Party excludes all liability for indirect, consequential, special or punitive loss or damage, including loss of business, profit or goodwill (whether the loss arises in contract, tort, under any statute or otherwise in connection with this Agreement) even if:

(a) the loss was reasonably foreseeable; or

(b) the other Party knew of the likelihood of the loss.

12.2 Each Party remains liable for any direct loss the other Party suffers arising from the first-mentioned Party's fraud, gross negligence or willful misconduct.

13. GOVERNING LAW AND JURISDICTION

13.1 This Agreement and any non-contractual obligations arising out of or in connection with it is governed by the laws in force in Mauritius and the Parties submit to the non-exclusive jurisdiction of the courts of that place.

13.2 The Parties shall attempt to solve any dispute arising out of or in connection with this Agreement by means of alternative dispute resolution such as but without limitation mediation. Any dispute, controversy or claim which may arise under this Agreement or the breach, termination or invalidity thereof which could not be resolved amicably, shall be resolved by arbitration by three (3) arbitrators appointed as follows: each Party shall appoint one arbitrator and the third arbitrator shall be appointed by mutual agreement of the two arbitrators failing which, the latter shall be appointed by a Judge of the Supreme Court of Mauritius sitting in Chambers. The place of arbitration shall be Mauritius, the costs of arbitration shall be borne by the losing party, the language of arbitration shall be English and the decision of the arbitrator shall be final binding and enforceable on both Parties and not subject to any appeal.

EXECUTED AS AN AGREEMENT IN TWO ORIGNALS ON: ….th October 2023

SIGNED for and on behalf of
MauBank Ltd
by its duly authorized representatives:

Name: ……
Title: ……..

Name: ……
Title: ……..

SIGNED for and on behalf of

……

by its duly authorised representative:

Signature of Representative

Name: …….

Title: ……