RFP – Security Operation Centre – Ref: RFP/ICT/2023/59

The bank is inviting bids from your firm for **"Security Operation Center- Ref: RFP/ICT/2023/59"** as per below scope of works and project specifications.

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 for ***Financial and Technical should be sent via two separate*** password protected email addressed to the ***Chairperson of Bid Opening Committee*** with subject **"Security Operation Center - Ref: RFP/ICT/2023/59"** at latest by **12.00 hrs.** (Mauritian Time) on **Friday, 22 September 2023.**

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

   - The procurement department on e-mail 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 **Friday, 22 September 2023**)
   - Proposal to be submitted as per template provided in the scope

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

   1. procurement@maubank.mu

   MauBank Ltd shall not consider any proposal that is received after the deadline and shall be declared late and rejected.

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.

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

Kindly acknowledge receipt of this mail while at the same time confirming your participation and your site visit schedule.

We look forward for your proposal

1. Introduction

The bank wish to implement a Security Information Event Management system to allow bank Security Operation Center to operate 24 x 7 thru an outsourcing company as well as provision of training and sizing of a centralize log repository to keeps logs for 7 years

3.1 Project Summary

The project consist of the following

- Design and architect model of the SIEM tool
- Implementation of the SIEM tool and log collection on various devices of the bank
- Customization of data sources and analyses
- Full documentation including but not limited to
    - Operational
    - Administration
    - Fall back procedures
- Capacity sizing for log storage for 7 years
    - 6 years off line log which is available within a day
    - 1 year on line log which is available within minutes
- Technical training for bank IT Security staff
- The solution must include log management, Next Generation SIEM, User Analytics behaviour, security analytics, security automation and orchestration engine, Incident management, incident response, advance correlation within the same platform with no additional 3rd party solution
- Supplier should provide with evidence and exemplary list and description of how log and machine data is collected by the solution
- Provide list of system on the platform fully developed and supported normalization logic out of the box by the solution
- Describe the out of the box content provided with the solution. Details the number of supported devices, rules, reports, queries, real time dashboard, modules, alert and threat feed integration etc.
- The solution must support full multi tenancy and full segregation
- The solution must support very granular level of role based access

3.1.1 Objectives

The SIEM solution provide a real time threat detection and response capabilities to protect organization against cyber-attack. The SIEM solution should be delivered by an integrated SecOps fabric made up of components that combine threat intelligence, advanced analytics and automation to help security team quickly identified and respond to threads. The Sec Ops fabric used machine learning and artificial intelligence algorithm to analyze massive amount of data from multiple sources. The solution shall use a closed loop approach to automate the incident response process, from detection to containment and remediation. This enable IT Security teams to respond quickly and efficiently to threats, reducing the time it takes to detect and mitigate attacks.

Bank is taking cyber security seriously and wish to prioritize vulnerabilities accurately, reduce time to remediation and improve bank security posture.

3.1.2 Background

The bank has most of its critical system on premise but the shift has started and gradually within two to three years we estimate that 40% of our critical services will be moved to cloud services. The activity of this project may both be on premise and on cloud critical system. The bank have various operating system flavors, different database technology, various critical application developed in various application languages and various communication and security technology devise. Currently bank has Qradar system and collect data from a dozen of critical system, there is no correlation of logs and neither user behavior analytics configured.

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 all security gaps are 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 bank various 24 x 7 services and ensure Confidentiality, Integrity and Availability of customer data

3.2 Project Scope

3.2.1 Implementation of SIEM tool, Monitoring of 24 x 7 of logs and sizing and keep logs for 7 years

Below is the project scope and detailed objectives of this project:

- The bank is ready to consider the following option base on cost, feasibility, performance, capability to deliver and security
  - OPEX Model
  - CAPEX model
  - Manage services
  - Outsource services
- In case there is no supplier who can meet full bank scope, the bank reserve the right to split the contract with two suppliers.
- Provide hardware sizing required to host the automated tool
- Specify operating system, database, web application and any other software required in the environment
- Specify initial storage required and estimate 7 years storage capacity planning
- Be able to write own rule and design work flow process for query / report generation

- The bank has application hosted both on premise and on cloud where logs will be required to push to the SIEM system
- Manage repositories and receive other key features like
    - Access control
    - Permission management
    - Advance security code protection process
- Identify Risk Factors: Determine the risk factors that need to be monitored on critical system.
- Define Risk Thresholds: Establish thresholds or limits for each risk factor. These thresholds define the acceptable range or limit beyond which an activity or event is considered risky. For example,
    - A high number of failed login attempts within a certain time frame may indicate a potential security breach.
- Develop mechanisms to continuously monitor the collected data and identify potential risks. This can involve real-time monitoring, periodic scans, and automated scheduled scan. Implement algorithms or rules that analyse the data and trigger alerts or notifications when a risk threshold is breached.
- Visualization and Dashboards: Create visual representations, such as charts or dashboards, to provide a quick overview of the system's risk status. These visualizations can help stakeholders easily understand and track risk levels, patterns, and trends.
- Continually update risk thresholds, rules, and monitoring mechanisms to adapt to evolving risks and ensure effective risk management log monitoring

- Log collection

    - Please provide the number of predefined parsing/normalization rules out of the box
    - Collect logs in real time and batch option
    - In sync event time for logs from system with incorrect timestamps
    - The Proposed solution must collect the logs in real-time and batch mode including different time zone
    - The proposed solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected log data
    - The proposed solution collector must support the option to filter out and drop some noisy logs at the collection layer before it reaches to the processing and indexing engine
    - The data collector/agent must be able to collect the logs through different methods, including but not limited to
        - UDP/TCP Syslog
        - SNMP
        - Cisco SDEE
        - NetFlow
        - JFlow
        - Sflow

- LogRhythm Universal Database Log Adapter for system and custom logs (e.g., audit, application, etc.) written to database tables (i.e. Oracle, SQL Server, MYSQL, etc.) (ODBC and OLE DB protocol)
- Checkpoint OPSEC/LEA
- Windows Event Logs (RPC) - this includes custom Event Logs (Windows Event Logs (local) – this includes custom Event logs
- Single-line Flat Files
- Multi-line Flat Files
- Compressed Flat Files (single and multi-line)
- NetApp CIFS
- eStreamer
- Metasploit
- Nexpose
- Nessus
- eEye Retina
- Qualys
- Tripwire
- API
- JSON format

- The proposed solution must support Windows Event log collection for Security, System, and Application events. Describe the process of ingesting and normalizing windows logs for search, correlation, alerting, reporting, etc.

File Integrity Monitoring

- The proposed must provide integrated built-in File Integrity Monitoring (FIM) not through a 3rd party software and it must be managed and monitored by the same NG-SIEM platform interface
- The proposed solution File Integrity Monitoring capability must capture the identity of the user generating the FIM events
- The proposed solution File Integrity / Endpoint Detection and Response capability must include support for both Windows and UNIX platforms. Provide a complete list of all that are supported.

- The proposed solution built-in FIM must pivot from a file access or change to a specific user. View a full timeline of their activity, including both file integrity monitoring (FIM) and other behavioral information.
- The prosed solution built-in FIM must selectively monitor file views, modifications and deletions, and modifications, as well as group, owner and permissions changes
- The proposed solution built-in FIM must alert on anomalous user activity related to important files. Reduce false positives by corroborating with other data

Log retention

- The proposed solution must store the raw logs and also the META data
- The proposed solution must utilize any storage methodologies for addressing different ages of log or event data
- The proposed solution must provide storage for long term trend visualization and analysis
- Are there any integrity checks performed on logs stored for long term retention
- The proposed solution must compress the archive logs

Log Analysis

- The proposed solution must analyze the logs in real time
- The proposed solution must support 4 layer of log classifications by default out of the box:
    - Layer 1: Audit – Operations - Security.
    - Layer 2: Classification.
    - Layer 3: Common Event.
    - Layer 4: MPE (Normalization Rule Name).
- Describe data enrichment capabilities, including the number and type of available fields
- The proposed solution must provide drill down, pivoting, and filtering capabilities to facilitate and accelerate investigations
- The proposed solution must represent large search results in a single view
- Describe the steps required to narrow search results to a specific type of log source from a specific server within the IT environment
- The proposed solution must perform DNS resolution for IP addresses

- Describe the real-time visualization options, features and capabilities of the dashboard
- Dashboard should allow for any type of drill down on information presented in the dashboard to view the underlying log data
- The proposed solution must allow for the easy creation of custom dashboards
- The proposed solution must contextualize the user information with a detailed information about the user attributes from the domain such as username, title, department, last time to log on, last time he failed in the password, email address...etc.
- The platform must have the capability to apply both security and operational analytics

Real Time advance Analytics

- Describe the solution's capabilities and interface for creating real-time advanced analytics rules
- The proposed solution must support the below out-of-the-box analytics rules:
  - Classifications types
  - Sub Classifications
  - Common Events (Sub Classification)
  - Message Processing Engine Rules (Parsing Rules)
  - Predefined Use Cases
  - Predefined Reports
- The proposed solution must employ advanced analytics and machine learning techniques
- The proposed solution must perform advanced analytics against all log data or a subset of the data.
- The proposed solution must have a risk based priority engine that can assign a risk value for all the logs, events and alarms natively at no additional cost
- The proposed solution must automatically determine threats based on suspicious patterns of behavior. How is the pattern discovery process automated
- The proposed solution must have the ability to automatically create whitelists of observed behavior (i.e. without manual intervention.)
- The proposed solution must have the ability to automatically learn behavioral or statistical baselines

- The proposed solution must offer the U.E.B.A natively out of the box at no additional cost
- The proposed solution must have the ability to leverage correlated or anomaly events back into other correlation or advanced analytics rules
- The proposed solution must incorporate data from multiple threat intelligence feeds into its' advanced analytics. It should support feeds from free or subscription based third-party vendors. There shouldn't be a hard limit to how many threat feeds the solution can integrate
- The proposed solution must provide updated analytics rules on a regular basis to detect new and emerging threats
- The proposed solution must allow the organization to build a filter and reuse it with multiple of correlation rules
- The proposed solution must be able to minimize false positives
- The solution must support many different types of correlation and analytics methods
    - Log:
        - ✓ Log Observed based correlation.
        - ✓ Non-Observed Compound based correlation.
        - ✓ Non-Observed Scheduled based correlation.
        - ✓ Session sequence based correlation.
    - Threshold:
        - ✓ Threshold observed based correlation.
        - ✓ Threshold non-observed compound based correlation.
        - ✓ Threshold non-observed scheduled based correlation.
    - Unique Value:
        - ✓ Unique value observed based correlation.
        - ✓ Unique value non-observed compound based correlation.
        - ✓ Unique values non-observed scheduled based correlation
    - Behavioral
        - ✓ Whitelist based correlation.
        - ✓ Blacklist based correlation.
        - ✓ Machine analytics based correlation.
        - ✓ Statistical based correlation.
        - ✓ Trend based correlation

Event and response alerting

- What methods of alerting are included in the solution (e.g. snmp, SMTP, Audio alerts etc.)?
- The proposed solution must provide an ability to interface with a third-party ITSM tool
- The proposed solution must provide out-of-the-box alarms designed to enforce continuous compliance and security best practices
- The proposed solution must provide the ability to create customized alarms, distributed to specific groups of individuals and prioritize alarms and alarm delivery.
- The proposed solution must email alarm notifications include risk rating priority level base on the granularity of the available rating.

Incident Response Automation

- The proposed solution must automate response to threats
- The solution should provide automated remediation
- Describe the capabilities, including what is provided out-of-the-box if applicable
- The proposed solution must take the actions below (Not limited to):
    - Disable AD user account
    - Quarantine an infected machine
    - Add IP to Firewall block list
    - Prevent the user from running non-authorized process or application
    - Enforce service to start
    - Enforce service to stop
    - Enforce service to be disabled
    - Add item to a watch list
    - Remove item from watch list
    - Disable local user account
    - Enforce the user to be logged off from a machine
    - Execute remote command
    - Delete file
    - Take memory dump

- The proposed solution must allow the customers to add their own automated remediation. Describe in detail the process for adding custom automated remediation

- The proposed solution automated remediation must provide a built-in hierarchy approval workflow, so the actions can be taken automatically or through an approval chain. Describe
- The proposed actionable engine must be embedded in the platform out of the box

User Event behavior Analytics base on Artificial Intelligence and Machine language

- The UEBA must be offered Fully Integrated within the proposed solution not through another separate integrated software
- The bidder must provide the list of UEBA use cases that they have out of the box
- The UEBA must be able to detect and respond to insider threats, compromised account, and privileged account abuse
- The UEBA must collect machine data from across your environment and fill in your forensic gaps with endpoint and network monitoring
- The UEBA must correlate log information to single identities to know the actors behind the actions impacting your environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations
- The UEBA must create a heuristic baseline of user activity by analysing behaviour, so it must perform multidimensional baselining, enabling the modelling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques
- The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modelling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques
- The UEBA must Use the heuristic baseline to detect unusual behaviors in real time, so it must continuously analyse current activity against baselines established for each identity and peer group. Detect behavioral deviations from user and peer group baselines
- The UEBA must Use the heuristic baseline to detect unusual behaviors in real time, so it must continuously analyze current activity against baselines established for each identity and peer group. Detect behavioral deviations from user and peer group baselines
- The UEBA must Detect threats of data exfiltration, privileged identity misuse and fraud

- The UEBA must provide case management, incident investigation, and extensive reporting, so it must accelerate investigation and response with embedded security orchestration and automation functionality. Use pre-staged actions to rapidly collect forensic data and invoke targeted countermeasures. Report on the results of your security program, including detection and response times
- The proposed solution must share the list of predefined out of the box use cases related to UEBA
- The platform must have this list of use cases out of the box and should have the ability to customize or build from scratch

Network behavior Analytics base on Artificial Intelligence and Machine language

- The platform must be able to ingest syslog and NetFlow logs to detect network anomalies based on a set of predefined rules
- The platform should be ready out of the box with some predefined use cases such as:

Mittre Att&ck Framework

- The platform must offer a list of predefined use cases to cover the MITRE ATT&CK use case
- The following MITTRE framework related Use Cases

Network Threat Detection and Response base on Artificial Intelligence and Machine Language

- The platform must be Machine Learning-Driven Network Threat Detection and Response
- The platform must help in securing the network against advanced persistent threats (APTs)
- The platform must have MITRE ATT&CK framework embedded out of the box. It must deliver a complete and accurate model of enterprise activity at the network, host, user, and process level and map incidents to the framework
- The platform must provide end-to-end enterprise activity at the network, host, user, and process level to help you detect threats like lateral movement, exfiltration, malware compromise, and ransomware in real time
- The platform must use distributed computing to scale data collection and analytics and co-locates analytic processing

- The platform must reduce false positives by over 90% and blocks advanced attacks
- The platform must support agentless cloud collection, so it can Ingest cloud data and models OS and workload behaviors across virtual machine and Kubernetes/containerized environments
- The platform should be easy to deploy and get up and running in fewer than 15 minutes
- The platform must have the capability to be bi-directionally integrated with other NG-SIEM solution
- The platform must have built-in IDS with predefined signature the keeps updated regularly
- The platform must have the capability to integrate with Vulnerability Management tools to reduce the false positives
- The platform must be able to integrate with the AD to get the users identities and map this to their network behavior for better visibility
- The platform must provide a recommendation with every incident detected
- The platform must have those incident categories out of the box:

    - Initial Compromise

        - ✓ Detected some vector used to get initial foothold into the network
        - ✓ Execution of adversary-controlled code detected
        - ✓ Adversary trying to have persistent presence (over system restarts and other failures)
        - ✓ Attempt to evade detection or avoid other defenses

    - Infection

        - ✓ Initial infection detected
        - ✓ Suspicious file was downloaded
        - ✓ Malware installed and callbacks to CNC servers are seen
        - ✓ Malware is attempting to spread laterally through the environment (e.g. ransomware)

    - Command and Control

        - ✓ Detection of C&C

    - Service Attack

        - ✓ Exploit against the specific service detected
        - ✓ (Distributed) Denial of Service attack is detected

- Recon and Discovery

  - ✓ Network host/port/sweep scan is detected
  - ✓ Vulnerability scan is detected
  - ✓ Application scan is detected

- Collection and Exfiltration

  - ✓ Sensitive file and other information being collected, prior to exfiltration
  - ✓ Host/user performs internal downloads AND external uploads AND
  - ✓ The score and the amount of data transferred raises suspicion AND
  - ✓ Such activity hasn't been attributed to that host/user before

- Suspicious Access

  - ✓ Brute force attack detected
  - ✓ User compromise detected
  - ✓ Access to the unusual resources that hasn't been seen before

- Privilege Escalation

  - ✓ Access to privileged data detected by an unauthorized user
  - ✓ Access to critical services is detected by an unauthorized user

- Ransomware

  - ✓ Ransomware – A malicious actor is encrypting files. No command-and-control channel is necessary for this attack pattern although such a pattern is often used.

- The platform must have the capability to do threat hunting based on:

  - ✓ Activity – all items below combined on the same screen
  - ✓ Geo-hunting – having a map view and filtering based on location
  - ✓ Anomaly – List of detected and scored anomalies for all users/hosts
  - ✓ HTTP – HTTP transactions
  - ✓ Connections – all non-specific network connections properties
  - ✓ DNS – DNS transactions
  - ✓ SSL – SSL connections certificate information

- ✓ Software – list of detected software on the network hosts
- ✓ SSH – SSH connections properties
- ✓ SMB– SMB/NetBIOS share/file access information
- ✓ Files – files downloaded over unencrypted connections

Security Orchestration Automation and Response

- The vendor must share the SOAR ecosystem that shows all the vendors that they have a bidirectional integration with out of the box
- The proposed solution must offer the SOAR (Security Orchestration, Automation and Response) function embedded in the platform not through an integration with another platform
- The proposed SOAR must be accessed from the same Web UI of the NG-SIEM platform not through plug-in/App and API integration
- The proposed built-in SOAR must not be limited to any function or to the number of incidents or actions per day, it must be Unlimited
- The proposed solution must provide incident tracking through an integrated security incident response platform.
- The security incident response platform must be fully integrated with analysis functions not through a separate Web UI or solution
- The proposed solution must calculate the mean time to detect and mean time to respond automatically and show that on the dashboard for the analysts
- The proposed solution built-in case management must allow any case to be shared with other collaborators, who can also add forensic evidence and annotations to expedite threat detection and response. All activity must be tracked as part of the case history, providing real-time status and a tamper-proof audit trail.
- The proposed solution must offer the play book functions embedded in the platform at no additional cost
- The solution must include incident tracking through a fully integrated Security Incident Response platform capable of designing Workflow and Executive Actions in response to Threat and Incidents triggered by the solution
- The SOAR Playbook must allow the Analyst to build their own incident response procedure/Playbook and track it through the Web UI The SOAR Playbook must allow the Analyst to build their own incident response procedure/Playbook and track it through the Web UI

- The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view must include relevant events, network activity data, correlated alerts, vulnerability data, etc.
- The solution must be able to automate response to known threats and through manual hierarchy approval workflow
- The solution must empower the IR/SOC teams with pre-packaged, customizable automation, reducing time to respond including the following User Cases:
  Endpoint Quarantine: Disable the port/device where a suspicious device is located.
  Suspend Users: If an account compromise is suspected, halt a user's account access—no matter what device they use.
  Collect Machine Data: In the case of malware, can gather data from the suspicious endpoint.
  Suspend Network Access: If data exfiltration is occurring, the incident response team can close the connection by updating your network infrastructure's access control list.
  Kill Processes: If an analyst detects an unknown or blacklisted process on a critical device, the Process can be terminated
    - The SOAR engine must allow the IR/SOC teams to have several action execution options:
      Automatic Execution: Configure actions to run in a fully automated manner to speed containment of high-risk threats especially for reoccurring actions.
      Approval-Based Execution: Configure actions to run after one or more approvals are provided. Actions can be configured for a single approver or a hierarchical chain of approvers before the action is initiated.
      Analyst-Triggered Execution: Execute an action manually to enable instantaneous execution of responses from within the Web UI.
      Remote Execution: Centrally manage the execution of actions across remote sites for the analysts to invoke actions delivered to and executed locally via the collector, enabling global incident response.
- The SOAR engine must not have any limit the number of SOC analysts or playbook templates that can be used

Administration

- The solution must include built-in case management to reduce mean-time-to-respond (MTTR) through real-time status tracking
- The solution built-in case management must allow any case to be shared with other collaborators, who can also add forensic evidence and annotations to expedite threat detection and response.
- The case management must ensure a tamper-proof audit trail through complete activity history
- The solution must support Seamless workflow Customization and Tagging through the UI
- The solution must support API for third-party integration
- The solution must provide Metrics and reports on mean time to detect (MTTD) and mean time to respond (MTTR) as KPI for team performance
- Does the solution provide centralized health monitoring of itself?
- Is there any inbuilt documentation, GUI driven or wizard guide for admin and users
- The proposed solution must integrate with Microsoft's Active Directory
- The proposed solution must allow an employee's access to the solution be suspended/deactivated temporarily without needing to delete and re-create the user details
- Does the solution enable the use of user profiles with stored attributes, such as: name, location, e-mail address, etc.? List the information that can be stored in a user's profile. Can users view &/or change their user profile details?
- Describe support for role-based access and delegated administration. Describe data access controls in detail

Reporting

- The proposed solution must offer all the reports out of the box at no additional cost
- Does the solution include pre-defined reports?
- How many pre-defined reports are included out-of-the-box?
- What pre-defined reports are included?
- Does the solution include Executive Level reports?
- Does the solution include reports directly aligned to support auditing/compliance
- Describe with details and list example report names
- Can filters be applied to pre-defined reports
- Can the user restrict the information in the report to a user-specified date range?

- Does the solution allow the generation of ad-hoc and custom reports and report templates
- What functionalities does the solution provide for customized report development?
- Does the solution allow reports to be viewed on-screen
- Can reports be exported from the solution into spreadsheets and/or databases?
- Can reports be scheduled and delivered to the recipients in an automated manner?
- Can reports be restricted to different levels of management within the company?
- Does the solution have a rest API to allow 3rd party tool to query and report the
- Does the platform have the capability to integrate with some open source tools

Compliance and Automation

- Provide information on what compliance requirements can be supported by the solution out-of-the-box, with minimal configuration (NESA, ISO 27001, NIST, SOX, PCI, etc.) at no additional cost
- Does the solution go beyond auditing/report support for compliance needs?
- Can the solution with real-time correlation and alerts have the ability to find root causes of non-compliance, etc.?
- Can compliance packages be customized?
- How often do compliance package updates occur?
- The proposed solution must offer all the compliance package reports out of the box at no additional cost

Operational Technology Security

- Classic Security Modelling
    - RSA VS CIA
        - Reliability, safety and availability vs confidentiality integrity and availability
- Passive Discovery and Analysis
    - NBAD / NDR based approach
    - Tap into the network traffic and start classifying many OT protocols, including CIP, COAP, ENIP, Modbus, OPCUA, and Profinet
- Machine Learning
    - UEBA and NTBA based detection
    - Pattern and timeline analysis
    - Action and error baselining and detection.

- Alerting capabilities for
    - Alerts on unusual network traffic
    - Alerts on unusual functions or configuration on ICS devices
    - Alerts on unusual behavior of the users accessing to the OT resources
    - Corroborated alerts based on OT environment
- DPA language
    - Identify traffic that is not natively classified
    - Extract details not normally extracted
    - Look for signatures in data payloads for specific kinds of traffic
- Analysis capability for Industrial Control System
    - Functions sent to the ICS devices
    - Responses from the ICS devices
    - Configuration changes on the ICS devices
    - Parameters sent to the ICS devices
- Support for Claroty (CTD – Claroty continuous threat detection)– OT Infrastructure
- Threat detection tool integration and out of the box use case availability

3.2.1 Out of Scope Functionalities

- Any network schematics changes will be out of scope
- Bypassing firewall and other security device of the bank to make the tool work effectively will be out of scope

3.3 System perspective

3.3.1 Constraints

- Force majeure
- Natural disaster event
- Pandemic

3.3.2 Issues

- Supplier access token limitation.
- Server downtime during maintenance and patching.
- Internet Bandwidth may impact the TAT of process.
- Network disruption.
- Resource unavailability to test from Supplier, IT and Business owners

Business Process Overview

4.1 Current Business Process (As-Is)

Currently Bank has Qradar system with minimal logs collection with no logs correlation and user behaviour analytics. This is a new process that bank wish to implement following the adaptation of NIST-800 framework and Bank of Mauritius guideline on Cyber and Technology risk

4.2 Current Business Process (To-Be)

The methodology approach will be as follows:

1. Banks has approximately two hundreds critical system including servers with different operating system flavours, routers, load balancers, Intrusion Prevention System, Firewalls, different category of switches, wireless controllers, IoT devices(UPS, Generators, HVAC system, IP Camera system among others), mail gateway, Forward Reverse and Web Proxy, databases, application, web services, API's and PowerShell and customized scripts.
2. The proposed solution will collect logs, filters logs, correlate log, provide a near real time dashboard on log analysis, detect and respond to any type of abnormal traffic, raise immediate alert, be able to take pre-defined action, provide daily report on area of concern, provide a risk register base on log analysis, provide a network pattern to determine bank network traffic and help to reduce bank attack surface.
3. To be able to connect to other log analyser like endpoint or any other system running in the bank
4. To able to keep logs for 7 years
5. Provide immediate forensics analysis from source to destination
6. Logs should be collected on various location such as
    a. Head office
    b. Sub office
    c. Branches
    d. Rodrigues Island (a branch outside Mauritius)

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

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

2. Supported documents (Annexures)

2.1 Technical Compliance
2.2 Bandwidth requirement
2.3 Management server
2.4 Information Security requirement
2.5 Price tabular format
2.6 Cloud Security Document

3. Assumption

1. Provide a full SDLC plan for the next 5 years to sustain the viability, reliability and of the automated tool and service
2. Supplier to showcase the capability to deliver and meet bank expectation on deliverables
3. Lesson learn help in future development with our business partners
4. A study of metrics which help reduce defects and policy violation while reviewing the parameters
5. Automated tool should stand independently to provide network malicious traffic
6. Supplier share all the in-built security features of the automated tool and how same is being kept updated throughout the SDLC
7. Product quality and meet bank compliance
8. Identify vulnerability faster
9. Minds that are agile, flexible and adapt to situation
10. Drive quality and consistency by pairing human creativity with a technology framework
11. Results correlate and normalize all data from all tools—no siloes data
12. The proposed solution must secure the communication during the log collection mechanism
13. The proposed solution must collect the logs through an agent-less

14. The proposed solution must support the ability to scan a Windows domain to automate discovery and event collection from windows hosts
15. The proposed solution must support Windows Event log collection for Security, System, and Application events
16. The proposed solution must support the ability to scan a Windows domain to automate discovery and event collection from windows hosts
17. The proposed solution must allow log collection to be continuous in the event communication with the back-end platform is temporarily interrupted
18. The proposed solution must include alerting that can be easily configured if a source stops sending log data
19. The proposed solution must support the collection of the Net flow logs without additional appliances or components
20. The proposed solution must have the capability to drop noisy logs at the collector level

4. 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
6. Regulatory requirement

Annexures

Technical Compliance

#	Description	Compliance (Yes / No)
1	The Security Threat Lifecycle Management – SOC Platform must have the Unlimited log data ingestion licensing model which would enable the end user to have the flexibility to add any data source / log source to the NextGen SIEM platform without any limitation on licensing or commercial impacts.	
2	Next Generation SIEM solution offering been in the Gartner's Leader quadrant for more than 3+ years continuously	
3	Security Automation and Orchestration engine (Complete Incident Response, Playbooks, Case Management and Automated Response) from the same platform vendor as NextGen SIEM	
4	User and Entity Behaviour Analytics should be available in the platform	

5	Network Threat Behaviour Analytics (both Flow based analytics and Deep packet inspection (PCAP) capabilities should be available in the platform)	
6	Security Analytics powering the machine analytics and search analytics for threat hunting in the platform	
7	Multitenancy (no additional cost or no additional instances to be rolled out) should be available in the platform with RBAC features.	
8	The proposed solution should never drop logs that are ingested to the platform.	
9	9.1 The Proposed Solution must offer all of the below built-in threat detection modules at no additional cost:	
	o User and Entity Behavioural Analytics Module.	
	o Network Threat Analytics Module.	
	o User Threat Analytics Module.	
	o Endpoint Threat Analytics module.	
	o Fraud Detection Module	
	o Multi-dimensional Behaviour Analytics Module	
	o Privileged user Monitoring Module.	
	o System Admin, Audit Network and Security Modules.	
	o Web Application defence module.	
	o APT Module.	
	o Honeypot Module.	
	o Core Threat Detection Module.	
	o Threat Intelligence Service Module.	
	9.2 The Proposed Solution must offer all of the below built-in Compliance Modules at no additional cost:	
	o ISO 27001 Compliance.	
	o PCI Compliance.	
	o GPG Module.	
	o SOX Module.	
	o NIST Compliance Module.	
	o COBIT-5 Frame Work Controls.	
10	The solution must support very granular level of role-based access.:	
	o Allow different teams to get an access to the same physical device and view date related to their department only	
	o It must support log source visualization on the SIEM platform itself	

	Description	Compliance (Yes / No)

11	The Proposed solution must collect the Machine Data, Network Data and User data in real-time as well as batch processing.	
12	The proposed solution must correct event time for machine data from systems with incorrect timestamps. Also, describe how the platform handles the machine data configured with different time zones.	
13	The proposed solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected machine (logs) / network (flows and packets) / user data (behavioural data).	
14	The data collector/agent must be able to collect the machine data through different methods, including but not limited to:	
	o UDP/TCP	
	o SNMP	
	o Cisco SDEE	
	o NetFlow	
	o JFlow	
	o Sflow	
	o AIX, Solaris, Linux, iSeries, any unix flavour (via 3rd party integration)	
	o Windows Event Logs (RPC) - this includes custom Event Logs (by using RPC not WMI).	
	o Windows Event Logs (local) – this includes custom Event logs	
	o Single-line Flat Files	
	o Multi-line Flat Files	
	o Compressed Flat Files (single and multi-line)	
	o NetApp CIFS	
	o eStreamer	
	o Metasploit	
	o Nexpose	
	o Nessus	
	o eEye Retina	
	o Tripwire	
	o API	
15	The proposed solution must secure the communication during the data collection mechanism	
16	The proposed solution must have the capability to data filtering at the collector level	

	Description	Compliance (Yes / No)
17	The U.E.B.A must be offered out of the box at no additional cost or license.	

18	The U.E.B.A must be able to detect and respond to insider threats, compromised account, and privileged account abuse.	
19	The U.E.B.A must collect machine data from across your environment and fill in your forensic gaps with endpoint and network monitoring.	
20	The U.E.B.A must correlate log information to single identities to know the actors behind the actions impacting your environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations	
21	The U.E.B.A must create a heuristic baseline of user activity by analysing behavior, so it must perform multidimensional baselining, enabling the modelling of a broad set of user behaviours. Baselines are used to detect anomalous behaviour via machine learning and other statistical analysis techniques.	
22	The U.E.B.A must Use the heuristic baseline to detect unusual behaviours in real time, so it must continuously analyse current activity against baselines established for each identity and peer group. Detect behavioural deviations from user and peer group baselines.	
23	The U.E.B.A must Detect threats of data exfiltration, privileged identity misuse and fraud.	
24	The U.E.B.A must Provide case management, incident investigation, and extensive reporting, so it must Accelerate investigation and response with embedded security orchestration and automation functionality. Use pre-staged Smart Response actions to rapidly collect forensic data and invoke targeted countermeasures. Report on the results of your security program, including detection and response times	

	Description	Compliance (Yes / No)
25	The proposed solution must analyse the collected data in real time	
26	The proposed solution must support 4 layer of log data classifications by default out of the box:	
	o Layer 1: Audit – Operation Security.	
	o Layer 2: Classification.	
	o Layer 3: Common Event.	
	o Layer 4: MPE (Rule Name).	
27	Describe data enrichment capabilities, including the number and type of available fields.	
28	The proposed solution must represent large search results in a single view	
29	Describe the steps required to narrow search results to a specific type of log source from a specific server within the IT environment.	
30	The proposed solution must perform geolocation to IP addresses	
31	The proposed solution must perform DNS resolution for IP addresses	

32	The proposed solution must contextualize the user information with a detailed information about the user attributes from the domain such as user name, title, department, last time to log on, last time he failed in the password, email address...etc.	
33	The solution should be capable of creating real-time advanced analytics rules. It shall be GUI-driven interface.	
34	The proposed solution must support the below out-of-the-box analytics rules:	
	o Classifications types	
	o Sub Classifications	
	o Common Events (Sub Classification)	
	o Message Processing Engine Rules	
	o Predefined Use Cases	
	o Predefined Reports	
35	The proposed solution must perform advanced analytics against all data or a subset of the data.	
36	The proposed solution must have a risk-based priority engine that can assign a risk value for all the logs, events and alarms natively at no additional cost	
37	The proposed solution must allow the organization to build a filter and reuse it with multiple of use cases / rules	
38	The proposed solution must be able to minimize false positives	
39	The solution must support 15 different types of correlation / Use cases:	
	o Behavioural:	
	ü Whitelist based correlation.	
	ü Blacklist based correlation.	
	ü Machine analytics-based correlation.	
	ü Statistical based correlation.	
	ü Trend based correlation	
	o Unique Value:	
	ü Unique value observed based correlation-based correlation.	
	ü Unique value non-observed compound-based correlation.	
	ü Unique values non-observed scheduled based correlation	
	ü Log Observed based correlation.	
	ü Non-Observed Compound based correlation.	
	ü Non-Observed Scheduled based correlation.	
	ü Session sequence-based correlation.	
	ü Threshold observed based correlation.	
	ü Threshold non-observed compound-based correlation.	
	ü Threshold non-observed scheduled based correlation.	

#	Description	Compliance (Yes / No)
40	The proposed solution must automate response to threats.	
41	The proposed solution must have the capabilities to calculate the Mean time to detect and Mean time to respond for all the incidents detected and responded using the platform as the key KPIs.	
42	4. The solution must have pre-built playbooks for Incident response and also have the capability to build new playbooks or customize the existing one.	
43	5. The proposed solution must take the actions below (Not limited to	
	o Disable user account	
	o Remove user from domain group	
	o Quarantine an infected machine	
	o Add IP to Firewall block list	
	o Prevent the user from running non-authorized process or application	
	o Enforce service to start	
	o Enforce service to stop	
	o Enforce service to be disabled	
	o Add item to a watch list	
	o Remove item from watch list	
	o Disable local user account	
	o Enforce the user to be logged off from a machine	
	o Extract the pcap file and open the leaked attachment	
	o Execute remote command	
	o Delete file	
	o Take memory dump	
44	The proposed solution must the customers to add their own automated remediation.	
45	The proposed solution automated remediation must provide a built-in hierarchy approval workflow.	
46	The proposed solution must be there in the platform out of the box at no additional cost.	
47	The proposed solution must provide incident tracking through an integrated security incident response platform	
48	The security incident response platform must be fully integrated with analysis functions not through a separate Web UI or solution	
49	The proposed solution must calculate the mean time to detect and mean time to respond automatically and show that on the dashboard for the analysts	

50	The proposed solution must have the compliance packages such as ISO, PCI, etc. as correlation rules, saved searches, saved reports out of the box with no additional cost.	
51	In addition to internal security incident response capabilities, describe how the solution provides integration with third-party software systems that our organization may utilize.	
52	The proposed solution built-in case management must allow any case to be shared with other collaborators, who can also add forensic evidence and annotations to expedite threat detection and response. All activity must be tracked as part of the case history, providing real-time status and a tamper-proof audit trail.	

Bandwidth requirement

	Head office Ebene	Secondary data Center	Branches
On Premise Solution			
Hybrid / Cloud Solution			

Management Server.

Bidder should supply the bank with two (2) management servers [Head Office (1) and DR (1)] that will be used to query the system and other related activities. The specification for the server is as follows

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	

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. Furthermore, it shall also provide data masking functionalities.	
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 to defend against SQL query poisoning shall be followed	
During implementation, secured protocols shall be used to communicate with the database and efficient indexing shall be implemented for rapid data retrieval.	
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.	

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	Manage service	
7	Support and maintenance 1 year upfront after commissioning	
8	Taxes	
9	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	Manage service					
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	Manage service	
7	Support and maintenance 1 year upfront after commissioning	
8	Taxes	
9	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	Manage service					
5	Any other					

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		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	**Hardening**	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		Multifactor authentication should be provided on the platform.	
5	**Identity Access Management**	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		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	**Pen Test**	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		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	**Network Control**	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		Is Anti-virus software is deployed on servers hosting the systems?	
31	**Antivirus**	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**	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	