

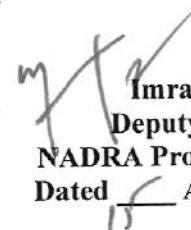
**EVALUATION REPORT**  
**(As Per Rule 35 of PP Rules, 2004)**

1. Name of Procuring Agency: HQ NADRA Islamabad
2. Method of Procurement: Single Stage (02) Envelope Methods
3. Title of Procurement: Procurement of Security Orchestration and Automated Response (SOUR) Technology
4. Tender Inquiry No.: NADRA-HQ-RFB-22/2024
5. PPRA Ref. No. (TSE): TS531982E
6. Date & Time of Bid Closing: 26<sup>th</sup> February, 2024 At 11:00 hrs.
7. Date & Time of Bid Opening: 26<sup>th</sup> February, 2024 At 11:30 hrs.
8. No of Bids Received: 07x Bids
9. Criteria for Bid Evaluation: As per Eligibility & Technical Evaluation Criteria Mentioned in Tender Documents
10. Details of Bid(s) Evaluation: As under: -

| Name of Bidder | Mars  |   | Evaluated Cost   | Rule/Regulation/SBD*/Policy/ Basis for Rejection / Acceptance as per Rule 35 of PP Rules, 2004.   |
|----------------|---|---|------------------|---|
|                | Technical (If applicable)   | Financial (If applicable)                 |                  |   |
| M/s Rewterz    | Qualified   | Only Technical qualification was required | Rs.72,437,850/-  | Bids of Seven firms i.e. M/s Rewterz, M/s Commtel, M/s Trillium, M/s Techaccess, M/s SN SKIES, M/s KIWIK & M/s DTC were received. Bids were opened on 26 <sup>th</sup> February, 2024. Bid of M/s DTC was found non responsive due to non-provision of supporting documents (non-active NTN & Affidavit is missing). As per technical evaluation report bid of M/s Commtel, M/s Trillium, M/s SN SKIES and M/s KIWIK were technically disqualified. Financial bids of the technically qualified firms i.e. M/s Rewterz and M/s Techaccess were opened on 28 <sup>th</sup> March, 2024. As per financial evaluation bid of M/s Rewterz was the most advantageous bidder. |
| M/s Commtel    | Technically Not Qualified   |   |                  |   |
| M/s Trillium   | Technically Not Qualified   |   |                  |   |
| M/s Techaccess | Qualified   | Only Technical qualification was required | Rs.235,530,512/- |   |
| M/s SN SKIES   | Technically Not Qualified   |   |                  |   |
| M/s KIWIK      | Technically Not Qualified   |   |                  |   |
| M/s DTC        | Non Responsive due to non-provision of supporting documents (non-active NTN & Affidavit is missing) |   |                  |   |

**Lowest Evaluated Bidder:** M/s Rewterz Information Security

11. Any other additional / supporting information, the procuring agency may like to share. Nil

  
**Imran Hashim**  
 Deputy Director  
 NADRA Procurement  
 Dated 15 April, 2024

12 nadsa 17424.6

## Bidder Evaluation Criteria

| Sr#            | Particulars                               | M/s Rewterz                    | M/s Commtel                    | M/s Trillium                   | M/s Techaccess                 | M/s SN Skies                   | M/s Kiwik                             |
|----------------|---|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|---------------------------------------|
| 1              | Bidder/ Firm has a valid NTN Registration | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                                   |
| 2              | Bidder/ Firm has a valid GST Registration | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | No                                    |
| 3              | Bidder/ Firm is active on ATL list of FBR | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                                   |
| 4              | Affidavit for Non-Blacklisting            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                                   |
| 5              | Letter of Bid                             | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                                   |
| 6              | Audited Bank Statements of last 2 years   | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | No                                    |
| 7              | Bidder must be authorized partner of OEM  | Yes                            | Yes                            | Yes                            | Yes                            | Yes                            | Yes                                   |
| <b>Remarks</b> |   | <b>All documents submitted</b> | <b>All documents submitted</b> | <b>All documents submitted</b> | <b>All documents submitted</b> | <b>All documents submitted</b> | <b>Incomplete document submission</b> |

**President:**  
Mr. Muhammad Baber Awan  
Director (Information Security)

**Member 1:**  
Mr. Muhammad Waseem Ali  
Deputy Director (Information Security)

**Member 2:**  
Mr. Junaid Zafar  
Deputy Director (Networks)

**Member 3:**  
Mr. Haroon Hafeez  
Deputy Director (TnD)

*[Signature]*  
19/3/2024

*[Signature: M Waseem]*

*[Signature: Junaid Zafar]*  
19/3/24

*[Signature: H Hafeez]*

Technical Evaluation

| Req/Requirement   | Description/Specification  | Ms Rewertz | Ms Commel  | Ms Trillium  | Ms Techaccess | Ms SN Skies | Ms Kiwik                            |
|---|--|------------|--|--|---------------|-------------|-------------------------------------|
| 1<br>General capabilities   | a. The SOAR technology must converge security orchestration and automation (SOA), security incident response (SIR) and case management, capabilities into a single solution.   | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | b. The platform must support to automate repeatable tasks, streamline workflows and security tasks for effective incident and case management.   | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | c. The platform must provide out-of-the-box integrations with well-known case management platforms and enable full automation of the ticketing process.  | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | d. The platform must support to eliminate manual tasks with automated playbooks to aggregate, parse, deduplicate, and manage millions of daily indicators across dozens of supported alert sources e.g. SIEM, EDR, vulnerability scanner, email, ticketing, threat intelligence feeds, network security controls, application security controls, IAM, PAM, etc.  | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | e. The platform must support machine learning, AI and other advanced features.   | Yes        | Not provided   | Not provided   | Yes           | Yes         | Not provided                        |
|   | f. The platform must support fully customized views, layouts, task lists, and flows with access control specific to users/roles.   | Yes        | Yes  | Yes  | Yes           | Yes         | Limited functionality is supported. |
|   | a. The platform should provide flexibility in terms of data format for ingestion. For example, it should be able to read and parse JSON, XML, text, HTML, etc.   | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | b. The integration with the SIEM platforms should allow ingestion of new alerts and any other information triggered on the SIEM platform. The platform should be able to integrate with SIEM products and obtain additional information using the query features. The platform should be able to push data to SIEM.  | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | c. The platform should provide multiple options to receive data. For example, Databases, APIs, Emails, Files, SIEM, etc.   | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
|   | d. The platform should support integration with leading SIEM vendors (e.g. Elasticsearch, Splunk, etc). The platform should support integration with leading threat intelligence products.   | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
| e. The platform should have a console showing list of all available integrations and supported actions. The platform should provide an option to enable/disable/configure the integrations with ease. | Yes  | Yes        | Yes  | Yes  | Yes           | Yes         |                                     |
| f. The service provider must provide any integration that is not available in their App Store without any extra cost.   | Yes  | Yes        | Yes  | Yes  | Yes           | Yes         |                                     |
| 2   | a. The platform should provide a feature to define series of actions in the form of a playbook that could be executed either automatically or on-demand. The platform should allow an easy mechanism for users to confirm or deny the activity, and the platform should record/display the user response and continue the execution of the playbook automatically without the need of any human intervention.                                | Yes        | Yes  | Limited functionality was displayed during the presentation. | Yes           | Yes         | Yes                                 |
|   | b. The platform must contain pre-defined playbooks for common use cases. A no-code visual editor should be available to create the playbooks with drag and drop capabilities without the need of using any scripting or programming language.  | Yes        | Visual editor with drag and drop capabilities is not provided. | Yes  | Yes           | Yes         | Yes                                 |
|   | c. The playbooks should have the option to send email to users for a confirmation of a certain activity. The playbooks should have the option to pause the execution until the response from the user is not received. Each playbook should be reusable with the help of custom rules. These rules should allow us to define conditions when a certain playbook will be executed automatically, without any human intervention. For example, | Yes        | Yes  | Yes  | Yes           | Yes         | Yes                                 |
| 3<br>Automation   |  |            |  |  |               |             |                                     |

McLuskey

HWK

Don

BAV

|  |   |     |   |   |     |   |     |   |     |
|--|---|-----|---|---|-----|---|-----|---|-----|
|  | execute a playbook automatically when a particular alert is received from the SIEM.   |     |   |   |     |   |     |   |     |
|  | The platform should automatically disable and flag a playbook if it has a configuration issue or if one of the actions used in the playbook is not available or it is disabled. The platform should have a playbook simulation option that allows the user to run a step-by-step execution with predefined input.   | Yes | Playbook simulation option is not provided. | Playbook simulation option is not provided. | Yes | Playbook simulation option is not provided. | Yes | Playbook simulation option is not provided. | --- |
|  | The platform should automatically trigger a workflow when an action with defined workflow is executed either manually or through a playbook. The workflows should provide a timer-based conditions so that the request is delegated based on approvers response in a given time period. The platform should provide logs for each playbook execution. The logs should display the visual flow of the execution of each playbook. The log should clearly show which actions were executed and the output of each action and decision. The platform should support nested playbooks/workflows.  | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform should allow for the centralized collection, aggregation, deduplication, enrichment of existing data with threat intelligence and conversion of intelligence into action.  | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform should have a section that lists all IOCs found across any alert, incident, or threat intelligence. The IOCs list should be searchable, sortable, and filterable.  | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform must support integration with third party systems via text files (CSV, XML), Database, API via Web Services and REST, or notification via structured email. The analysts should be able to add assets, affected vendors, affected products, and remediation details of the advisory.   | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | Every activity done against an advisory should be logged and displayed in the detail view in the form of a timeline. The timeline should display the name of the user who took the action, time of the action, and the details of the action. The platform should have an option to generate threat intelligence reports of a single advisory or multiple advisory that are present in the platform.  | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform should provide a separate view that should display the sortable, searchable, and filterable list of all the cases related to the threat intelligence. The platform should have an option that any advisory that has a case opened should display the list of cases in which the advisory is tagged.  | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform must have workflow automation and case management features to track status and compliance of potentially affected operators against IOCs/vulnerabilities for prevention, common containment and remediation. The platform should provide an option for team members to communicate with each other in the form of comments. The comments from different team members should be visible. The platform should enable Analysts to add detailed information about each incident, including Description, Analysis Details, Branch Details, Remediation Details, Asset Details, embed images in the description, analysis, and remediation detail section etc. | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |
|  | The platform should enable Analysts to easily change severity and priority of the incident, add other members to an incident, change category and status of an incident. Any member of an alert, investigation, or incident should be able to assign a task to another member by creating a task. The tasks should be able to be defined under a certain incident management lifecycle phase (e.g. Analysis, Containment, Evadication, Recovery, etc.) or a custom phase. The platform should correlate multiple alerts received from different sources and display the related alerts/incidents.   | Yes | Yes   | Yes   | Yes | Yes   | Yes | Yes   | --- |

McOsborn  
HWA

|  |   |  |   |            |            |  |            |
|--|---|--|---|------------|------------|--|------------|
| <p>3 Incident/Case Management</p>  | <p>c The incident details should show the timeline of all activities done on the incident. The incident details should allow analyst to select scoring options across different categories (functional impact, Observed Activity, Location, Threat Actor, etc.), and the final score should be dynamically updated and displayed with proper color coding. Each activity on the timeline should mention the time/date of the activity, user who did the activity along with an overview of the activity</p> | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>d The platform should have an option to attach files as evidence. The platform should allow analysts to send notification, approve and follow-up emails to the platform users as well the people who will not be using the platform.</p>  | <p>Yes</p>  | <p>Files other than images cannot be attached in the platform.</p>       | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>e The platform should not just allow converting an alert to incident, but also allow users to create an incident or case manually. The platform should allow administrators to customize incident/case categories, subcategories, dispositions, and detection methods for the incidents, tailor the categories, scoring options, values, priorities etc. The platform should provide option to generate reports for single incidents as well as all multiple/all incidents over a period of time.</p> | <p>Yes</p>  | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>f The platform should provide options to define escalation rules based on the combination of severities, priorities, asset classifications, and asset values. The platform should allow users with sufficient privileges to define escalation and SIA tracking rules. The feature should have options to define and track the incidents based on the time since last response recorded on an incident or the time within which an incident should be closed.</p>                                      | <p>Yes</p>  | <p>Escalations based on SIA tracking rules is not provided.</p>          | <p>Escalations based on SIA tracking rules is not provided.</p> | <p>Yes</p> | <p>Yes</p> | <p>SIA tracking is not provided. Escalations based on SIA breach is also not provided.</p> | <p>---</p> |
| <p>g The platform should automatically send escalation and SIA breach notifications based on the defined rules. The platform should be able to send a separate notification on SIA breach.</p>   | <p>Yes</p>  | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>a The platform should provide integration with asset management, solution, active directory etc. The platform should allow to group together multiple assets in hierarchical categories.</p>  | <p>Yes</p>  | <p>Yes</p>   | <p>Limited functionality was mentioned in the presentation.</p> | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>b The platform should allow assets to be tagged in alerts, investigations, incidents, vulnerabilities, threat intelligence, and cases. The platform should have a searchable, filterable, and sortable assets list view with option to customize the list of columns displayed on screen.</p>   | <p>Yes</p>  | <p>Yes</p>   | <p>Limited functionality was mentioned in the presentation.</p> | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>c The platform should provide a view that should provide list of all incidents, vulnerabilities, advisories, and risks in which the asset is tagged. The solution should provide functionality or support ingestion of severity/criticality of an asset and the ability calculate incidents severity based on assets criticality.</p>   | <p>Yes</p>  | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Limited functionality is provided.</p>  | <p>---</p> |
| <p>d The platform should have a separate vulnerability management view which should display a searchable, sortable, and filterable list of all vulnerabilities either added manually, or received from a third party vulnerability assessment tool.</p>  | <p>Yes</p>  | <p>Separate vulnerability management view is not provided currently.</p> | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>e The platform should provide integration with common vulnerability assessment (VA) tools to initiate vulnerability assessments. The list should display the entry, license in which the vulnerability was found, name of the vulnerability, color-coded severity, resolution status, and last modified date.</p>   | <p>Yes</p>  | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |
| <p>f The platform should have an option to import vulnerabilities from different data sources. The platform should support automatic initiation of assessments through playbooks when VA tools are integrated. Each vulnerability's detail view should have a list of devices in which the vulnerability was found.</p>  | <p>Yes</p>  | <p>Yes</p>   | <p>Yes</p>  | <p>Yes</p> | <p>Yes</p> | <p>Yes</p>   | <p>---</p> |

Misskhan

WVA

| 4. | The platform should allow custom displays with sorting and selection. The platform should provide labeling and tagging features. The platform should provide UI elements drag and drop features.   | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
|----|--|-----|--|--|-----|--|-----|-----|
| b. | The platform should allow zooming levels at time series, graphical & log view level. The platform should be able to play back particular events in a graphical way. The platform should have a web-based interface capable of running on any latest and supported web browser seamlessly.  | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| c. | The platform should provide various visualization options for deep dive investigation, compliance and reporting, detailed/intelligent search on raw and enriched data, auto-complete, auto suggest capabilities based on contextual data. The platform should provide flexible, widget-driven dashboards and reports to eliminate manual reporting.                                      | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| d. | The platform should have a default set of ready-to-use dashboards. For example, incidents dashboards, vulnerabilities dashboard, automation dashboard, threat intelligence dashboard, Asset dashboard, Cases dashboard, Risk dashboard, Prioritization dashboard, KPIs dashboards, LI dashboard, L2 dashboard, etc.  | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| e. | The platform should provide an option to create new dashboards and customize existing dashboards according to client needs. The platform should allow to define name and description of each dashboard.  | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| f. | The platform should have the KPIs dashboard or widgets to display MTTD, MTTR, Analyst activities, Recurring Vulnerabilities, Open Incidents, Closed incidents etc. The platform should allow users to set their default dashboard, with the option to auto refresh the dashboards at a set refresh rate. The platform should enable shareable dashboards.                                | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| g. | The platform should provide an automation dashboard for an overview of the number of actions and playbooks executed. The platform should show notification related to the decision making actions assigned to the user and provide quick access to them.   | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| h. | The platform should provide custom dashboards or widgets e.g. overview of number of alerts converted to investigation and number of investigations converted to incidents in a given period, cases open or closes, all the activities in the cases where the logged in user is involved, sorted by time, the list of all upcoming and due soon tasks assigned to the logged in user etc. | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |
| a. | The platform should have report generation and export capabilities with multiple supported formats (i.e. Excel, PDF, XML, CSV etc.). The platform should have the ability to schedule custom reports with periodic schedules. The platform should provide out-of-the-box reports for analysts.   | Yes | Yes  | Limited reporting features are provided. | Yes | Yes  | Yes | ... |
| b. | The platform should provide out-of-the-box reports for administrators. The platform should provide out-of-the-box reports for audit and compliance. The platform should provide out-of-the-box reports for executive management.   | Yes | Report customization cannot be performed by the platform user. Supplier will code the report template upon client request. | Limited reporting features are provided. | Yes | Report customization cannot be performed by the platform user. Supplier will code the report template upon client request. | Yes | ... |
| c. | The solution must be deployable in the customer's virtual environment. The solution must be provided as a Virtual Appliance or Software, running on Linux or Windows Server operating systems. The platform should be deployed passively into infrastructure.  | Yes | Yes  | Yes                                      | Yes | Yes  | Yes | ... |

HWA

Muslem

|   |  |     |  |     |     |     |     |      |
|---|--|-----|--|-----|-----|-----|-----|------|
| b | The platform should support high availability component architecture ensuring no single point of failure. Support DR failover / failback setup. The platform should flag and send notifications when there is a connection failure with one of the technologies integrated with the SCAR platform. The platform should have the option to send email based notifications. The platform should provide an option to view server health (CPU, RAM, disk usage, etc.). The platform should provide options for automatic and manual full backups and restore. | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| c | The platform should have an option to enable and use third-party authentication. The platform should have an option to invite new users. The platform should support Multi-Factor Authentication (MFA) for all users.  | Yes | MFA is not being provided in the platform currently. | Yes | Yes | Yes | Yes | .... |
| d | The platform should allow to combine users in custom groups. The platform should provide granular access control to restrict or allow any feature or view available in the platform.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| e | The platform should provide the option to apply restrictions on who can view, update, and delete the alerts, investigations, and incidents. The platform should provide a default list of user roles and privileges assigned to each role and also should have an option to define custom user roles and assign privileges to each user. The platform should log and display every activity and every action taken within the platform, log and display all authentication attempts including failed logins.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| f | The platform should be vertically scalable. The platform should not have restrictions on the number of alerts/records that can be ingested or created in the platform. The platform should have proper documentations on how-to guides, FAQs, knowledge base articles and community forums.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| a | The license of the platform must be of at least 03 years.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| b | The license must support at least 50 users.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| c | The vendor must perform extensive assessment of the underlying SIEM technology for comprehensive visibility and security orchestration.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| d | Provider must implement high availability solution with automatic failover in active/standby orientation in Primary and Secondary sites.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| e | Provider must integrate its platform with at least 50 custom NADRA technologies and all relevant standard technologies deployed at NADRA.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| f | The bidder must build, test, and deploy new playbooks/workflows required as per technical requirements without additional cost for the duration of the license.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| g | Provider must perform development, configuration, testing, deployment and reporting of KPI's like MTTD, MTTR, Dwell Time, Compliance Tracking etc.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| h | The HA solution should provide real time data replication/syncing of events between primary and secondary server using data synchronization or shared external storage.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| i | Must provide 24/7 customer/technical support service.  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| j | Should provide support to write integrations, create and update playbooks, implementing ticketing and escalations, create dashboards, user interface consoles and automations.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| k | Vendor must provide services for Solution Onsite Maintenance, Support, Customization, Software and Code updates (24x7).  | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| l | Vendor must provide detailed solution design, topology, data flows and related documentation of the complete solution.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |
| m | Must provide on-site O2 resident engineers for at least 01 year of the license duration.   | Yes | Yes  | Yes | Yes | Yes | Yes | .... |

M. Usman

HWA

*[Signature]*

*[Signature]*

|                             |   | Qualified        | Not Qualified        | Not Qualified        | Qualified        | Not Qualified        | Not Qualified        | Not Qualified  |
|-----------------------------|---|------------------|----------------------|----------------------|------------------|----------------------|----------------------|--|
| 11                          | Training Lock (Mawka CRM and)   | Yes              | Yes                  | Yes                  | Yes              | Yes                  | Yes                  | Not Qualified (incomplete technical documentation and absent on presentation/demo) |
|                             | a. The vendor must provide health check report after deployment of the complete system and on quarterly basis. OEM/Principal certified In-person training for deployment, configuration, and complete operability of the solution. Training dates can be decided after issuance of purchase order as per convenience of the user. department. | Yes              | Yes                  | Yes                  | Yes              | Yes                  | Yes                  | ---  |
|                             | b. The vendor should also provide a list of electronic and printed documentation for the installation, operation, use, and administration of the entire solution.   | Yes              | Yes                  | Yes                  | Yes              | Yes                  | Yes                  | ---  |
| <b>Qualification Status</b> |   | <b>Qualified</b> | <b>Not Qualified</b> | <b>Not Qualified</b> | <b>Qualified</b> | <b>Not Qualified</b> | <b>Not Qualified</b> |  |

President:  
Mr. Muhammad Baber Awan  
Director (Information Security)

*[Signature]*  
19/12/2024

Member 1:  
Mr. Muhammad Waseem Ali  
Deputy Director (Information Security)

*[Signature]*

Member 2:  
Mr. Junaid Zafar  
Deputy Director (Networks)

*[Signature]*  
19/12/24

Member 3:  
Mr. Haroon Hafeez  
Deputy Director (TNO)

*[Signature]*