OIL & GAS DEVELOPMENT COMPANY LIMITED
PROCUREMENT DEPARTMENT (LOCAL), ISLAMABAD
SCHEDULE OF REQUIREMENT

Material :**UPGRADATION OF SIEM SOLUTION, PROCUREMENT OF MOBILE DEVICE MANAGEMENT AND IDENTITY ACCESS MANAGEMENT**

Due Date:

Tender Enquiry No: **PROC-LH/PT/SYS-18133**

Bid Bond Value : RS. 2,380,000/-

Attachment(if any) : YES

EVALUATION WILL BE CARRIED OUT ON FULL

Sr No	Description	Quantity	Make/Brand offered	Unit	Unit Price (PKR) Inclusive Of All Taxes Except GST	Unit Price (PKR) Inclusive of GST	Total Price (PKR) Inclusive of GST	Delivery Period Offered	deviation from Tender Spec. If Any
1	Identity and Access Management Software Solution for 2500 Users	1		Number					
2	Installation, Configration, Implementation, Testing & Training Services	1		Number					
3	SIEM Software Solution upgrade with License for 1500 EPS	1		Number					
4	Installation, Configration, Implementation, Testing & Training Services	1		Number					
5	Mobile Device Management Software solution for 100 devices	1		Number					
6	Installation, Configration, Implementation, Testing & Training Services	1		Number					
7	Maintenance & Support Services for 01 year regarding IAM, MDM and SIEM Solution	1		Number					

Special Note: The prospective bidders also download the master set of Tender Document

- The prospective bidders may keep in touch with OGDCL web site for downloading the clarifications/amendments (if any) issued by OGDCL.
- DELIVERY TERM: WITHIN 60 DAYS FOR DELIVERY OF SOFTWARE SOLUTION AND 180 DAYS FOR COMPLETION OF PROJECT AS PER TOR. PAYMENT TERMS: 40% AFTER DELIVERY OF HARDWARE (EXCLUDING SUPPORT SERVICES) AND 60% AFTER COMPLETION OF PROJECT AS PER TOR.BID VALIDITY: 120 DAYS.

OIL & GAS DEVELOPMENT COMPANY LIMITED
PROCUREMENT DEPARTMENT (LOCAL), ISLAMABAD
SCHEDULE OF REQUIREMENT

Mandatory Checklist

Please confirm the compliance of the following mandatory information along with the bid(s) (failing which bids(s) will not be accepted)

Documents	To be Attached with the Technical/Financial Bids	Compliance	
Original Bid Bond	Technical Bid	Yes ☐	No ☐
Copy of NTN Certificate	Technical Bid	Yes ☐	No ☐
Copy of GST Certificate	Technical Bid	Yes ☐	No ☐
Confirmation that the Firm is appearing on FBR's Active Taxpayer List	Technical Bid	Yes ☐	No ☐
Duly signed and stamped **Annexure–A (Un–priced)**	Technical Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–B**	Technical Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–D**	Technical Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–L** on Company's Letterhead	Technical Bid	Yes ☐	No ☐
Duly signed and stamped **Annexure–M** on Company's Letterhead	Technical Bid	Yes ☐	No ☐
Duly signed and stamped **Annexure–N** on Non–Judicial Stamp Paper duly attested by Notary Public	Technical Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–A (Priced)**	Financial Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–C**	Financial Bid	Yes ☐	No ☐
Duly filled, signed and stamped **Annexure–E**	Financial Bid	Yes ☐	No ☐

OIL & GAS DEVELOPMENT COMPANY LIMITED
PROCUREMENT DEPARTMENT (LOCAL), ISLAMABAD
SCHEDULE OF REQUIREMENT

For the Vendors/Contractors who opt to submit Bank Draft/Call Deposit/Pay order against Bid Bond/Performance Bond, our Accounts Department has finalized an arrangement for online payment to such Vendors/Contractors, which will be processed through (IBFT & LFT) for which following information is required:

i.	IBAN No. (International Bank Account Number 24 Digits)	
ii.	Vendor Name as per Title of their Bank Account	
iii.	Contact No.of Company's CEO/ Owner (Mobile & Landline)	
iv.	Bank Name.	
v.	Bank Branch Name and Code	

Name, Sign and Stamp of the authorized official of the Bidder(s) _____

Upgrade of SIEM & Procurement of Mobile Device Management System, Identity & Access Management System

Terms & Conditions

****

Note: Bidders are requested to read this document carefully and provide complete information required in this T&C. All information required in the Vendor Qualification & Professional Staff details must be provided. OGDCL reserves the right to reject Proposals with in-complete or partial information.

Introduction

The Oil and Gas Development Company (OGDCL) is soliciting proposals from experienced professional services organizations to assist in the establishment and setup of a comprehensive cyber security Program. The objective is to identify, protect, detect, respond and recover OGDCL's IT/OT assets using the following steps:

Step 1: Prioritize and Scope – Identify OGDCL's business/mission objectives and high-level organizational priorities. Recommend strategic decisions regarding cybersecurity implementation. Determine the scope of systems and assets that support the selected business lines and processes.

Step 2: Orient - Identify related systems and assets, regulatory requirements, and overall risk approach for the business lines or process within scope. Consult sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile - Develop a Current Profile of OGDCL by indicating which Category and Subcategory outcomes are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment - Refer to OGDCL's overall risk management process or previous risk assessment activities to analyze the operational environment and discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. Identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile - Create a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing OGDCL's desired cybersecurity outcomes. Consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps - Compare the Current Profile and the Target Profile to determine gaps. Create a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. Determine resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner, guide OGDCL to make informed decisions about cybersecurity activities, support risk management, and enable the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan - Determine which actions to take to address the gaps identified in the previous step and adjust OGDCL's current cybersecurity practices. Recommend a risk assessment frequency to improve the quality of risk assessments through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile, to align OGDCL's cybersecurity program with the desired goals.

INTRODUCTION TO WORK

Bids are invited for the following components:

1. Provision of software solution for Identity & Access Management System
2. Software solution for Mobile Device Management System
3. Up-gradation of Security Information Event & Log Management System
4. Installation, configuration, integration, training & implementation services

PROPOSALS

The firms are required to send Financial Proposal as well as Technical Proposal for this project in separate sealed envelopes.

TECHNICAL PROPOSAL

Technical Proposal should be submitted covering the following details;

i. Brief about the Firm, its support facilities with years of service in Pakistan.
ii. Details about each software solution provided as per Annex I
iii. Details of services and training as per Annex II
iv. Integration and interoperability requirements for integrated security as per Annex III
v. Details regarding Mandatory Requirements & Technical Evaluation Criteria as per Annex- IV
vi. Experience of working in large public sector organization.
vii. Provide the detailed mechanism of annual technical support.
viii. Schedule of Supply, installation, configuration, implementation & testing of the proposed solution.

FINANCIAL PROPOSAL

Financial Proposals should give the costs for maintenance & support of all the items associated with the offered solutions for 01 year as detailed below.

i. Software purchase, licenses fee
ii. Installation/configuration, integration & implementation cost.
iii. Annual Charges for continuous vendor technical support.
iv. Training Costs (Hands-on Local) if any

DURATION OF PROJECT/DELIVERY PERIOD:

- The delivery of software solution should be made within 60 (Sixty) days after issuance of Purchase Order.
- Installation/Configuration, implementation, Training & Testing Services should be completed in 180 (One Hundred & Eighty) days after delivery of software solution.
- One year Support Services period will start after completion/signing off of the project.
- Bidder is required to furnish fortnightly progress reports of the activities under taken in due course of time.
- The bidder shall submit detailed project plan defining activities, sub-activities etc. in the form of

Gantt chart.

PAYMENT TERMS:

- The 40% of total amount (excluding one year support services) will be paid after delivery of software licenses.
- 60% payment of project cost (excluding one year support services) will be made after completion of project including Installation/Configuration, implementation, Testing & Training.
- Payment of Support Services will be made on quarterly bases, after performance of services.

PROJECT DELIVERABLES:

1. Documentation Requirements

   Technical and Project documentation being developed and delivered as part of the solution should be managed in accordance with the configuration management plan. The bidder should use tool that allow for version control, check-in/check-out and security management.

   i. Describe the methodology for documentation management throughout the project.

   ii. Describe the process for disaster recovery, performance tuning, and debugging aids.

2. It should include but not limited to :
   a. Detail Project Plan/Project Schedule
   b. Pre-requisite document for installation of the solution
   c. High Level Design Document
   d. Low Level Design Document
   e. Customized guide (Step by step installation/configuration Guide)
   f. Proposed Solution's Presentation in PDF
   g. Integration Plan of Applications if involved in new solution
   h. User Acceptance Tests
   i. SOP's regarding solution

IMPLEMENTATION & TRAINING:

The selected bidder will be responsible for complete implementation and deployment of the new proposed solution. The bidder shall provide initial and ongoing educational and training services for the development, implementation, and use of the new processes and software. In addition to OGDCL user training on the software application, identify training requirements for technical and professional staffs, managers, and end users.

i. Provide a detailed description of the training program, including deliverables that will be produced as part of the solution for the successful execution of the project.

ii. Describe any overview of other training options including those from third-party providers, training catalog, certification programs etc.

TESTING OF SOLUTIONS:

In testing phase, the bidder is required to perform the testing regarding all software solutions mentioned in the bid including Test for SIEM & MDM solution. This testing must be complete from all aspects to meet the challenges/requirement of the OGDCL.

DEPENDENCIES & RISKS:

The bidder is required to submit dependencies & risks involved in project proposal. The bidder can visit the existing data center of OGDCL before submission of proposal.

Annex-I

Technical & Functional details of Solutions

The bidder will propose a cybersecurity platform to support the fore-mentioned methodology, aggregate inputs from the existing security tools and facilitate execution of the following activities to provide a unified security management platform.

Identify

Asset Management

1. Inventory physical devices and systems within OGDCL
2. Inventory software platforms and applications within OGDCL
3. Map OGDCL communication and data flows
4. Catalog external information systems
5. Prioritize hardware, devices, data, and software based on their classification, criticality, and business value
6. Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders such as suppliers, customers and partners

Business Environment

1. Identify and communicate OGDCL's role in the supply chain
2. Identify and communicate OGDCL's place in critical infrastructure and Oil and Gas sector
3. Establish and communicate priorities for OGDCL mission, objectives, and activities
4. Establish dependencies and critical functions for delivery of critical services
5. Establish resilience requirements to support delivery of critical services for all operating states

Governance

1. Establish OGDCL information security policy
2. Coordinate Information security roles & responsibilities and align with internal roles and external partners

3. Explain and Manage Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations
4. Validate that Governance and risk management processes address cybersecurity risks

Risk Assessment

1. Identify and document asset vulnerabilities
2. Specify how Threat and vulnerability information is received from information sharing forums and sources
3. Identify and document both internal and external threats
4. Identity Potential business impacts and likelihoods
5. Use Threats, vulnerabilities, likelihoods, and impacts to determine risk
6. Identify and prioritize Risk responses based on NIST's RISK Management framework (800-37)

Risk Management Strategy

1. Establish Risk management processes that are managed and agreed to by OGDCL stakeholders
2. Determine and clearly express OGDCL risk tolerance
3. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

Protect

Identity Management

Propose and Implement an Identity and Access Management solution as specified in detailed technical system specifications section below.

1. Manage identities and credentials for authorized devices and users.
2. Manage and Protect Physical access to assets
3. Manage Remote access
4. Manage Access permissions by incorporating the principles of least privilege and separation of duties
5. Incorporate network segregation where applicable to protect network integrity
6. Proof and bound identities to credentials and assert in interactions when appropriate
7. Authenticate users, devices and other assets commensurate with the risk of interaction

Awareness & Training

Propose and implement a security Awareness and Training solution

1. Train and inform all users.
2. Privileged users understand roles & responsibilities.
3. Ensure that Third-party stakeholders (e.g., suppliers, customers, partners) understand

roles & responsibilities

4. Ensure that Senior executives understand roles & responsibilities
5. Ensure that Physical and information security personnel understand roles & responsibilities

Identity and Access Management System
Technical System Specifications
A comprehensive solution with a full complement of IAM capabilities to meet current and future needs of users, external resources and guests, including but not limited to:

Indicate whether the proposed solution for each requirement is:

(S) Standard, out of the box
(CO) Configurable using settings within the delivered solution
(CU) Customizable via software coding
(NA) Not Available

Any item not listed as standard or configurable must include an estimated level of effort to provide that functionality.

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	Unique identifier –unique, unchangeable identifier associated with each identity maintained. If a user leaves and later returns to the Organization in a former or new role, the same original unique identifier is used.	
2	A Centralized identity directory/repository that supports multiple concurrent identity-related roles and affiliations and stores both current and historical data	
3	An extensible identity directory/repository schema that allows the solution to capture additional user-defined roles, attributes, and metadata, above and beyond the vendor's standard identity repository	
4	Can accept/capture identity and entitlement data be using REST Services, SOAP Services or plain text file.	
5	The platform supports dynamic linking of accounts	
6	Includes methods for matching an identity to disparate applications, user accounts and entitlements	
7	Provides the ability to migrate, consolidate and/or leverage pre-existing unique identifiers in the new IAM directory/identity repository	
8	When an identity-related change occurs in a non-authoritative system or outside of normal ILM processes, there is a mechanism for reconciling connected (source or target) systems	
9	Flexible views and management - the identity directory/repository data may be filtered, sorted, viewed and managed in a variety of ways, based upon defined access permissions for administrators, department designees, or others	
10	Method for identifying orphaned accounts and for allowing an administrator to flag the account for remediation	

11	Has the ability to associate a standard user account and an administrative user account in a single application with the individual's central identity record	
12	Flat files may be used to populate and maintain the directory/repository	
13	Provides the capability for distributed designees to create and assign attributes to ids in the directory/repository	
14	APIs are provided to allow access to the identity repository data for federated local Authorization	
15	Provides the ability to detect identity life cycle events as they occur in an authoritative source and transform them into add, modify or delete events	
16	Multiple concurrent constituency types are supported via Identity Lifecycle Management (ILM) processes and other user-defined constituency types, or roles	
17	Individual/Department sponsorship for nonemployee can be added by designees via granular access to the system	
18	Has the ability to connect to multiple authoritative sources for identity creation, maintenance and de-activation	
19	Manual entry capability for ILM events - Ability for administrators to directly create, update or remove identities and associated identity attributes in the identity repository	
20	Batch-driven identity life cycle events are supported – the ability to import identity data files that have been extracted from an authoritative source into the identity repository, for *both* full batch processing (entire identity record is replaced) and change-log batch processing (only affected identity attributes are updated)	
21	Supports future-dated items (both toggle on and toggle off)	
22	Both On-premise and Cloud-hosted authoritative sources are able to be leveraged for ILM event detection and synchronization	
23	Has the ability to transition individuals between constituency types or roles, while maintaining their original identity record and unique identifier so as to maintain a complete history of the user's identity life cycle	
24	Single Sign-On capabilities including SAML, HTTP Proxy, Web Services and directory services.	
25	Multi Factor authentication services using TOTP, SMS and Email.	
26.	System security protection against, DDOS and Dictionary Access	
27.	Portal Based SSO along with Multi-Factor Authentication for external users and internal users based on user roles	

Self-Service

System Specifications – Self Service Function

Provide a written overview of the self-service functionality and ease of use. Include the process of managing and reducing the need for password reset.

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	Capability to setup Self-Service registration requests	
2	Ability to provide Self-service and delegated administration requests for both new and existing users	
3	Provides ease of ability to customize and extend the UI of the self-service access request process	
4	Provides the ability to view the workflow steps of a given access request, including the ability to identity the appropriate approver	
5	Provides the ability to view access request status	
6	Provides the ability for requestor or approver to enter effective dates (start and end) for the requested access	
7	Does the system flag high-risk or out-of-compliance access requests?	
8	Capability of identifying dependencies &/or parent/child relationships to facilitate identification & request of all roles needed?	
9	Approvers are able to approve, reject, or modify access requests at fine grained Levels	

Automated Workflow

System Specifications – Workflow Capabilities

Provide a detailed description of the workflow capabilities within the proposed solution.

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	A workflow engine and workflow processing are included as part of the IAM Offering	
2	A web-based, user-friendly interface is provided for managing all work list items	
3	Supports the ability to require users to acknowledge requirements, policies, etc. as part of the overall access request workflow.	
4	Supports the ability to remove user access and/or de-provision users without user Notification	
5	Email notifications notify participants of status changes and work items	
6	Communication options can be set for each workflow step to send after the step is approved or denied	
7	Administrative overrides are available to block email notifications per workflow Step	

8	A web-based interface is provided for monitoring the history, status, and progress of work-flow items	
9	Conditional workflow processing is delivered as part of the workflow engine, where workflow steps can be dynamically determined by the outcome of other workflow steps	
10	Multiple approvers can be specified and required for certain access types, such as access to sensitive data as well as certain user types	
11	Multiple approvers can all be required to approve or any one of the approvers can approve	
12	The workflow engine supports integration with external applications and services (outbound calls) via Web services, APIs, etc., with the ability to accept return codes, process data and monitor the status of activity from the external application	
13	The workflow tool includes graphical workflow design UI	
14	A set of predefined workflow templates, that can be modified, is provided	
15	Offline workflow testing is supported, prior to committing workflow changes in production	
16	Approvers may reroute workflow tasks back to the originator or previous approvers for additional input or clarifying information	
17	Electronic signature capability exists for workflow approvals	
18	If a workflow step is denied the approver is required to document an explanation that is retained with the workflow step in historical data	
19	Workflow steps can be dynamically added and/or deleted by a workflow approver with appropriate authority	
20	Workflow approver assignments are managed through the system. Business rules and appropriate security govern who can manage assignments. Changes in workflow approver assignments do not impact historical workflow approval/denial data but do impact currently active and future workflow steps	
21	Access policies are applied consistently across all operations	
22	Policies are represented and managed in a graphical user interface	
23	The solution promotes configuration over customization of policies; custom coding is rarely, if ever, required	
24	The solution allows for both business and technical roles and policies to be assigned. Hierarchal role model is supported: roles inherit permissions from other roles via a structured inheritance	
25	Separation of duty policy definitions and enforcement capability: if a user is assigned to one role, or role set, that user is prohibited from being assigned to another role or role set	
26	Retrofit/reapply role and policy permissions: once a policy has been updated, the solution provides a mechanism to reapply roles and policies to users	
27	There is support for access assignment expiration dates (example: auto-expire contractor accounts after n days)	
28	Policy and role preview/sandboxing: there is the ability to preview the impact of changes before the change is committed	
29	Top-down role modeling tools are provided to aid in the design and management of roles	
30	The solution supports the ability to import *application* roles, or responsibilities, from HRMS	
31	Reviewers have the ability to view access by user and to certify users' access to entitlements, roles or related items	
32	Reviewers have the ability to view access by roles and to certify users assigned to a role as well as the entitlements associated with a role	
33	Reviewers have the ability to view access by entitlement and to certify all users assigned to a specific entitlement	

34	Access certification scope may be limited to a particular individual or a specific group of users (such as those with a particular attribute value)	
35	There is a flexible scheduling utility that allows organizations to define the intervals in which access certifications will be run, including the ability to run annually, semiannually, quarterly, weekly or daily	
36	The solution supports a delta certification that includes only the user or entitlement data that has changed since the last certification	
37	The solution provides access certification reports and dashboards that allow an administrator to track the status of an access certification campaign	
38	Sponsor review certifications are supported (such as a sponsor for a contractor account), allowing sponsors to certify that a user is still under his/her sponsorship	
39	The solution allows detailed mapping between systems of record, identity repository and target systems	

Password Management

System Specifications – Password Management Services

Please provide an overview of the password management functions in the proposed solution and describe how they are typically managed.

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	Has an option to set the initial password for user accounts and force the user to change the password upon first login	
2	Enforces all typical password policy constraints, including password expiration, password length, password history, complexity, and restrictions against dictionary words, repeating characters, sequential characters, use of full or partial names, etc.	
3	Supports password recovery using customizable knowledge-based security questions	
4	Supports a locally configurable number of security questions the user must establish	
5	Includes an "option" to force users to establish security questions at the time of account claiming or first logon	
6	Supports options for streamlined, early (yet secure) account claiming and activation process for new hires.	
7	Failed login attempts lockout: the solution allows organizations to lock a user out of the system after a locally configurable number of failed login attempts	
8	Supports automated password synchronization across multiple password stores	
9	Passwords, password history, and challenge questions/answers are encrypted during transit and storage	
10	Password recovery can be initiated using a one-time password sent to the user's registered mobile device or alternate email address	
11	Supports locally configurable lockout timers to address password-guessing and dictionary attacks	

Reporting

System Specifications – Reporting System

Describe how your proposed solution handles reporting needs of this size, scale and scope? What report templates are available, if any, to simplify reporting needs?

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	Ability to maintain a historical snapshot of identity data and report on a user's access at any time	
2	A comprehensive set of predefined audit reports on common security-related functions are provided	
3	Audit reports can be scheduled to run at particular times and intervals, upon particular events, or upon demand	
4	Dormant or inactive account detection capability exists	
5	Provides the ability to restrict what data elements are available to the third-party reporting tool	

Operation

System Specifications

Please provide a draft template of an implementation plan for your product at OGDCL.
As the proposed solution touches every user, and the access to systems they need to complete their work, provide a detailed plan that provides an understanding of the implementation process to assist the OGDCL in planning its end of the engagement.

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	Ability to be fully installed, configured, and operational onsite at user facility	
2	Does an install wizard exist for deployment of the software?	
3	Configurable for high availability (e.g. the system architecture supports standard industry concepts of redundancy, synchronization across redundant components, DR, and high availability monitoring)	
4	Includes a mechanism for strong authentication/MFA for administrators	
5	Supports SAML integrations for Single Sign On and has been proven to work with multiple partners.	
6	Includes integration APIs to allow third-party systems to access IAM data and functions	
7	Includes a robust set of configurable system security policies to ensure fine-grained security controls that restrict access to data and functions in the system	

Detect

Propose and Implement a SIEM solution as specified in Appendix B.

Propose and Implement a Mobile Device Management Solution as specified in Appendix C.

Anomalies and Events

1. Establish and manage a baseline of network operations and expected data flows for users and systems
2. Analyze detected events to understand attack targets and methods.
3. Aggregate and correlate event data from multiple sources and sensors
4. Determine Impact of events
5. Establish Incident alert thresholds

Continuous Monitoring

1. Monitor the network to detect potential cybersecurity events.
2. Monitor the physical environment to detect potential cybersecurity events
3. Monitor personnel activity to detect potential cybersecurity events
4. Detect malicious code
5. Detect Unauthorized mobile code is detected
6. Monitor external service provider activity to detect potential cybersecurity events
7. Perform monitoring for unauthorized personnel, connections, devices, and software
8. Perform Vulnerability scans

Detection Process

1. Define roles and responsibilities for detection to ensure accountability
2. Detection activities should comply with all applicable requirements
3. Test detection processes
4. Communicate event detection information to appropriate parties
5. Continuously Improve Detection processes

Analysis

1. Investigate notifications from detection systems
2. Understand the impact of the incident
3. The proposed solution should perform forensics
4. Incidents should be categorized consistent with response plans
5. The proposed solution must mitigate the incidents
6. Newly identified vulnerabilities should be mitigated or documented as accepted risks

Improvements

1. The Response plans must incorporate lessons learned
2. Update response strategies

Recover

Recovery Planning

1. Execute recovery plan during or after an event

Improvements

1. Recovery plans must incorporate lessons learned
2. Update Recovery strategies

Communications

1. Manage public relations
2. Repair reputation after an event
3. Communicate recovery activities to internal stakeholders and executive and management teams

Technical System Specifications - Security Information and Event Management (SIEM)

Please provide detailed project plan for SIEM Implementation at OGDCL

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1	A solution that can automatically analyze and correlate activity across multiple data sources including logs, events, network flows, user activity, vulnerability information and threat intelligence to identify known and unknown threats	
2	Have ability to ingest Security events: From firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems, databases and more	
3	Have visibility on Layer 7 application context from network and application traffic	
4	User and asset context contextual data from identity and access management products and vulnerability scanners	
5	Endpoint events from the Windows event log, Sysmon, EDR solutions and more	
6	Collect and correlate application logs from enterprise resource planning (ERP) solutions, application databases and other systems	
7	Provide threat intelligence from multiple sources	
8	Ability to detect slight changes in the network	
9	Ability to detect user or system behavior that may indicate unknown threats, such as malicious insiders, compromised credentials or file-less malware.	
10	Integration with other security products and work a part of overall integrated automatic security.	
11	Monitor and analyze Layer 7 application traffic	
12	Have predefined built-in rules and customizable security rules for identification, protection, detection, response or escalations and recovery by working with other security products as integrated security	
13	By sensing dangerous default settings, misconfigurations and software flaws the solution must help take corrective action before an attack occurs	
14	Single, consolidated view of vulnerabilities to access any vulnerable asset from a single dashboard	
15	Prioritize and remediation and mitigation of vulnerabilities found on scanned assets.	

16	The solution must help ensure compliance by conducting regular network scans and maintaining detailed audit trails	
17	It must categorize each vulnerability with a severity rating and an exposure score. In addition to scanning assets both internally and externally	
18	Enable security teams to create tickets to manage remediation activities and specify exceptions with a full audit trail	
19	Provides the transparency, accountability, and measurability critical to an organization's success in meeting regulatory mandates and reporting on compliance	
20	The solution must have ability to correlate and integrate threat intelligence feeds yields more complete metrics for reporting on IT risks for auditors	
21	Easily address and manage industry compliance requirements	
22	Address risk and regulatory exposure by providing default setting compliance packages for ISO 27001, Data Security (PCI DSS) and others applicable to Oil and Gas industry	
23	The solution must create a catalog and manage assets in the whole IT infrastructure	
24	The solution must list and keep track record of all the vulnerabilities on that assets.	
25	The flexible, scalable architecture of the solution must be designed to support both large and small organizations with a variety of needs	
26	It must deliver integrated automatic failover and full-disk synchronization between systems without the need for additional third-party fault management products	

Technical System Specifications - Mobile Device Management

No	Description	(S) Standard (CO) Configurable (CU) Customizable (NA) Not available
1.	Securely provisioning to mobile devices and identity management	
2.	Solution must have a built-in anti-malware to guard against malware	
3.	Ability to provide data expense management	
4.	Integration with other security systems for threat monitoring and intelligence	
5.	Securely de-provision enterprise data	
6.	Gain visibility & control over iOS, Android, Windows Mobile, Windows & MacOS devices	
7.	Distribute, manage & protect applications across mobile devices	
8.	Provide conditional access to trusted devices & single sign-on & touch access to apps	
9.	Attain insights & alerts to discover vulnerabilities, boost productivity & improve IT efficiency	
10.	Cognitive recommendations for policies based on peer, regional, and industry data	
11.	Separate work & personal mobile apps & data on devices	
12.	Prevent costly overages by monitoring & enforcing mobile data usage	
13.	Contain & encrypt corporate email, contacts & calendar	
14.	Should have an AI sidekick that boosts employee productivity & delivers end-user support in real-time	
15.	Understand which apps need attention and prioritization via app intelligence and reporting	
16.	Preserve the native VPN experience for iOS & Android users	
17.	Access corporate intranet, websites & web apps without initiating a VPN session	
18.	Grant secure access to work documents in an encrypted container	
19.	Enable security-rich mobile access to corporate file repositories	
20.	Protect access to private, enterprise apps & prevent data loss	
21.	Enhance enterprise apps with seamless access to	

	internal corporate data	
22.	Empower users to securely create, edit & save mobile content	
23.	Allow users to synchronize documents across managed mobile devices	
24.	Remediate risks from mobile malware & compromised devices	
25.	Obtain real-world remote device views & perform remote control functions quickly	
26.	Identify, report & schedule distribution of OS patches & push updates to 3rd party apps	
27.	Deliver real-time mobile threat detection, malware prevention & data exfiltration avoidance	

Annex II

Support Services & Licenses/Subscriptions

Software Licenses/Subscriptions:

All quoted software licenses/subscriptions should be valid for 01 year.

Services:

The following services shall be provided and the selected firm will also be required to provide maintenance and support services for a period of 01 year, extendable to further 03 years on annual basis with mutual consent:

1. **Solution Installation, Configuration and Services**:
    a. Installation, configuration and implementation of provided solution
    b. Testing and hand over to the OGDCL staff.
2. **Training Services**:
    a. Vendor has to provide administrator level training for 06 OGDCL IT staff for Solution installation, configuration and implementation.
    b. The training should be conducted in OGDCL's premises.

Annex III

Integration and Interoperability requirements for integrated security:

The OGDCL has a large number of enterprise systems that will need to connect to the security system to achieve the vision of integrated security.

- Describe how the solution will integrate with all security products and provides one interface as integrated security dashboard? The system should be able to tell live state of security, state of compliance and state of risk.
- Describe how the security system or tool will integrate security management roadmap with people, processes and technologies.
- Describe how the proposed integrated solution will work with other security systems and provides a consolidated view of compliance status with mandatory and optional controls specific for Oil and Gas Industry.

Annex IV

Mandatory Requirements & Technical Evaluation Criteria

Note: Bidders are advised to carefully read the Mandatory Requirements, Evaluation Criteria and provide complete information in each category in their Technical Proposal. Incomplete or partial information will not be weighed up.

Mandatory Requirements

1. SECP Registration in Pakistan
2. Registered business in Pakistan with an NTN and GST
3. Presence at Islamabad/ Rawalpindi
4. Manufacturer authorization letter
5. Agreement for subcontracting, if intends to subcontract the Project

Technical Evaluation Criteria

Sr. #	Description	Allocated Score	Remarks
1	**Company profile** Years of experience in solution implementation of similar technology as mentioned in TOR under technical specifications.	**25**	Firm having 10 year experience will get 20 marks. For each additional one year experience, 01 mark will be given, up to maximum 0f 25 marks.
2	**Average Turnover for last 03 Years Pak Rupees in Million** Please enclose last 03 years audited financial statements	**15**	Firm with average turnover of Rs. 500 Million will get 11 marks. For each additional 50 Million turnover, 01 mark will be given, up to maximum of 15 marks.
3	**Professional Experience** List of Similar Nature Deployments (at least 5). Valid documentary proofs/Certificates must be attached.	**35**	Firm having 5 deployments will get 25 marks. Firms having more than 5 deployments will get prorated score, up to maximum of 35 marks
4	**Project team and Certified staff** for quoted solutions i,e, Identity Access Management, Mobile Device Management & SIEM. Valid documentary evidence required along with staff resumes, professional certifications and past experience.	**25**	Bidder with full compliance will get 25 marks. (9+8+8)
	Total Score	**100**	
	Qualifying Score	75	70% marks are mandatory for each above Serial No

Annexure V

Financial Bid Evaluation Criteria

Only technical qualified bidders will be considered for financial evaluations. Financial bids will be evaluated on full consignment wise.