

TENDER NOTICE

No. EA/02-45-2024

For Providing Analytics & Reporting Solutions (ARS)

1. Bids are invited from your esteemed Corporation for Providing Analytics and Reporting Solutions in Afghanistan as per RFP Annexure. This bid Document is also available on the Etisalat website (www.etisalat.af, Tenders).
2. RFP Deadline is **20 November 2024 Afghanistan time**.
3. Bid received after the above deadline shall not be accepted.
4. Bidders can provide either a sealed Hardcopy of the Proposal or a Softcopy of the Proposal through email. A hard copy can be submitted to Etisalat's Main office, Reception Desk (Tender Box). The softcopy shall be submitted through email (snabizada@etisalat.af) and cc: (Ihsanullah@etisalat.af) and marked clearly with the **RFP name, and number**.
5. The bidder shall submit the proposal with separate (Technical and Commercial) parts. The commercial part must be password password-protected document for a softcopy of the proposal, and we will request the password once here the concerned committee opens bids (starts the bid's Commercial evaluation). The bids shall be first evaluated technically. Technical evaluation will be based on the conformity to

required technical specifications and compliance matrix specified in the Bidding Documents. Only technically compliant bids that meet all the mandatory service-effecting requirements will be evaluated commercially.

6. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

7. All correspondence on the subject may be addressed to Ahmad Shikib Shalizi, Assistant Manager of Procurement, and Etisalat Afghanistan. Email snabizada@etisalat.af and Phone No. +93781204113.

Ihsanullah Zirak

Director Procurement and Supply Chain

Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat

Afghanistan

E-mail: ihsanullah@etisalat.af

(RFP)

For

**Providing Analytic and Reporting
Solution
for Etisalat Afghanistan**



1. DEFINITIONS

In this document, the following terms and meanings shall be interpreted as indicated:

1.1 Terms.

“Acceptance Test(s)” means the test(s) specified in the Technical Specifications to be carried out to ascertain whether the Goods, Equipment, System, Material, Items or a specified part thereof is able to attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

“Acceptance Test Procedures” means test procedures specified in the technical specifications and/or by the supplier and approved by EA as it is or with modifications.

“Approved” or “approval” means approved in writing.

“BoQ ” stands for Bill of Quantities of each job/work as mentioned in this contract and its annexes according to which the contractor shall supply equipment & services and subject to change by agreement of both parties.

“Bidding” means a formal procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract.

“Bid/Tender Document” means the Bid/Tender documents issued by EA for invitation of Bids/Offer along with subsequent amendments and clarifications.

“CIF” means “Cost Insurance Freight” as specified in INCOTERM 2010.

“Competent Authority” means the staff or functionary authorized by EA to deal finally with the matter in issue.

“Completion Date” means the date by which the Contractor is required to complete the Contract.

“Country of Origin” means the countries and territories eligible under the rules elaborated in the “Instruction to Bidders”.

“Contract” means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

“Contractor” means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

“Contractor’s Representative” means the person nominated by the contractor and named as such in the contract and approved by EA in the manner provided in the contract.

“Contract Documents” means the documents listed in Article (Contract Documents) of the Form of Contract (including any amendments thereto) or in any other article in this contract.

“Contract Price” means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

“Day” means calendar day of the Gregorian calendar.

“Delivery charges” means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

“D.D.P” means Delivered Duty Paid as defined in the Incoterms 2010 including the unloading responsibility of bidder/seller.

“Effective Date” means the date the Contract shall take effect as mentioned in the Contract.

“Etisalat Afghanistan (EA)” means the company registered under the Laws of Islamic Emirate of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to contractor in writing.

“Final Acceptance Certificate” means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

“Force Majeure” means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

“Goods Receipt Certificate” means certificate issued by the consignee certifying receipt of Goods in good order and condition.

“Liquidated Damages” mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

“L.o.A” means Letter of Award issued by EA to successful bidder with regard to the award of tender.

“Month” means calendar month of the Gregorian calendar.

“Offer” means the quotation/bid and all subsequent clarifications submitted by the Bidder

and accepted by EA in response to and in relation with the Bid Documents.

“Origin” means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

“EA's Representative” shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

“Specifications” means the specifications, provided in the Contract and its annexure and in EA Tender Specifications and where the Contract is silent and in cases of conflicting specifications appearing in the documents, based on the latest version of ITU-T recommendations.

“Supplier/Vendor” (used interchangeably) means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract acting individually alone or as a “prime contractor” for a consortium.

“Supplier's Representative” means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

“Warranty Period” shall mean the period of 12 months or any extended period starting from the acceptance of the delivered Goods in good order and conditions at consignee's certified by EA authorized representative (s).

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Providing Analytic & Reporting Solution in accordance with Etisalat specifications and Annexures.

3. Bill of Quantity (BoQ)

As per Annexure –A

4. Validity of Offers

The Tenders must be valid for a minimum of 90 days from the Tender closing date, or as may be specified by Purchaser in the Tender documents.

5. Price and Payment Term

5.1 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.

5.2 Advance payment shall be not made to the contractor.

5.3 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor subject to availability of prerequisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from the Project Director.

5.4 Payments are subject to deduction of income tax at the prevalent rate from the relevant invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue a certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

5.5 Payments against the entire contract will be made by EA based on the contractor's ability to meet payment milestones as defined in the Bid Documents in the following manner.

5.5.1 For Supply of Equipment (Hardware & Software);

5.5.1.1 EA will make payment equal to 50% of the amount of equipment on the arrival of Equipment at site of installation and certification by EA Project Director/Manager of their receipt in good condition.

5.5.1.2 Balance 50% of the amount of equipment will be paid on issuance of RFS for the complete system area in individual city.

5.5.2 For Installation, Testing, Commissioning and Professional Services (if available).

5.5.2.1 EA will make payment equal to 75% of amount of Services cost when equipment is offered for Acceptance Testing in individual city.

5.5.2.2 Balance 25% of the amount of Services cost will be made at the time of issuance of final PAC for complete system in individual city.

5.5.3 For System Support and Maintenance Services (if available).

5.5.3.1 EA will make payment on quarterly basis at end of each quarter, after support/service is delivered.

7. Penalty:

7.1 If the contractor fails to complete the said job on or before the Completion Date, the Contractor shall pay to the Purchaser as and by way of Penalty resulting from the delay, the aggregate sum of one percent (1%) of Total Contract price of the delayed services for each week and pro-rata for parts of week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total Contract Price of the service(s). In the event that delay is only in respect of small items which do not affect the effective utilization of the system, penalty shall be chargeable only on the value of such delayed items.

7.2 Any penalty chargeable to the Contractor shall be deducted from the invoice amounts submitted by the Contractor for payment, without prejudice to the Purchaser's rights.

8. Construction of Contract:

The Contract shall be deemed to have been concluded in the Islamic Emirate of Afghanistan and shall be governed by and construed in accordance with Islamic Emirate of Afghanistan Law.

9. Termination of the Contract

9.1 If during the course of the Contract, the Contractor shall be in breach of the Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

9.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract

not been terminated then the Contractor shall pay such excess to the Purchaser.

9.3 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.

9.4 Etisalat has the right to terminate this Contract without cause at any time by serving a 30-day prior written notice to the Contractor.

10. Local Taxes, Dues and Levies:

10.1 The Contractor shall be responsible for all government related taxes, dues and levies, including personal income tax, which may be payable in the Afghanistan or elsewhere.

10.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic Emirate of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/nonregistered companies.

Annexure-A

Scope of Work for Providing of Analytic and Reporting Solutions.

1. INTRODUCTION:

Etisalat Afghanistan has recognized the need to enhance its analytics and reporting capabilities to support its growing business requirements and drive data-driven decision-making. The proposed solution will integrate various data sources, provide robust data modeling and visualization, and deliver advanced analytics and reporting capabilities to support the organization's strategic objectives.

Therefore EA is seeking a comprehensive **Analytic and Reporting Solution** that leverages Artificial Intelligence (AI) and Machine Learning (ML) capabilities to deliver advanced data analysis, reporting, and business intelligence functionalities. The selected solution should provide a seamless and user-friendly experience for both technical and non-technical users, enabling data-driven decision-making across the organization.

2. Strategic Objectives:

2.1 Enhance data-driven decision-making capabilities across the enterprise:

- 2.1.2 Empower teams with real-time access to relevant, accurate data.
- 2.1.3 Promote a culture of fact-based decision making.
- 2.1.4 Improve alignment and collaboration between business units.

2.2 Increase operational efficiency and agility:

- 2.2.1 Streamline and automate manual reporting processes
- 2.2.2 Enable faster access to critical insights for timely decision making
- 2.2.3 Reduce reliance on IT-OSS for ad-hoc data requests.

2.3 Strengthen the organization's competitive position:

- 2.3.1 Gain deeper, data-driven understanding of market trends and customer behavior
- 2.3.2 Develop predictive analytics capabilities to support strategic planning.
- 2.3.3 Leverage advanced visualization and BI tools to enhance business intelligence.

3. Operational Objectives:

3.1 Implement a centralized, enterprise-wide analytic and reporting platform:

- 3.1.1 Evaluate and select the best-fit software solution.

- 3.1.2 Integrate the new platform with existing data infrastructure.
- 3.1.3 Establish a self-service BI environment for end-users.

3.2 Develop intuitive dashboards, reports, and visualization capabilities:

- 3.2.1 Design user-friendly interfaces tailored to the needs of various stakeholders.
- 3.2.2 Leverage advanced analytics functionalities, such as predictive modeling.
- 3.2.3 Ensure high user adoption through comprehensive training.

3.3 Optimize the analytic and reporting solution over time:

- 3.3.1 Continuously gather feedback from end-users
- 3.3.2 Enhance the platform based on evolving business requirements.
- 3.3.3 Implement robust data governance and security measures.

3.4 Establish a dedicated BI/Analytics Center of Excellence:

- 3.4.1 Provide ongoing support, maintenance, and platform enhancements.
- 3.4.2 Upskill employees and promote data literacy across the organization.
- 3.4.3 Serve as a strategic partner to business units for data-driven initiatives.

4. Project Scope:

The scope of Analytic and Reporting Solution project would include the following key elements:

- 4.1 Evaluate and select a business intelligence (BI) and analytics software solution.
- 4.2 Implement BI and Analytic solution and integrate into key data source across the organization.
- 4.3 Develop intuitive dashboards, reports, and advanced analytics functionalities, such as predictive modeling by leveraging AI and ML technology.
- 4.4 Migrate existing SAP BO/BI data and reports to new solution.
- 4.5 Provide Comprehensive User Training, documentation and operation user manual.

5. Scope of Work

The scope of work for an Analytic and Reporting Solution typically includes the following key components as part of the overall implementation and rollout activities

5.1 Data Connectivity and Integration:

- 5.1.1 Ability to seamlessly connect and integrate data from various system and data sources
(oracle, SQL, My SQL, Postgres, DB2, Mango Db...), as well as other business systems
-

(ERP, CRM, SAP BO/BI etc.)

- 5.1.2 Provide API/SFTP integration with other data sources and 3rd party system to process and analyse real time or near real time data.
- 5.1.3 Provide a secure and scalable data management framework to ensure data quality, integrity, and security.
- 5.1.4 Provide data transformation and ETL (Extract, Transform, Load) tools to cleanse, standardize, normalize and enrich data and prepare data for analysis.
- 5.1.5 Support for complex data structures (hierarchies, time-series, etc.) and data types (binary, xml, Json, text, images, videos, CSV, excel, float files, etc.).
- 5.1.6 The solution needs to provide advanced job scheduling capabilities, allowing users to define job, trigger and process dependencies based on specific rules and events.
- 5.1.7 The solution needs to provide rule-based case detection and time-based, event-based and condition-based trigger and scheduling abilities.
- 5.1.8 The solution needs to provide centralized process/job monitoring capabilities and realtime alerts and notification services.

5.2 Analytic dashboard and Reporting Capabilities:

- 5.2.1 Provide an intuitive and modern user interface for data exploration, visualization, and report generation.
- 5.2.2 Provide smart dashboard, drill-down capabilities, drag and drop interface, interactive filters and drill-down ability to gain insight in low-level details of each KPI.
- 5.2.3 Develop **Mobile App** that provides facilities for visualizing dashboards and reports on mobile devices to enhance accessibility and allow users to stay informed on the go.
- 5.2.4 Ask Data (Natural Language Query): Use natural language to ask questions about your data and get visual answers, create custom fields and calculation to transform data and uncover hidden patterns.
- 5.2.5 Offer a wide range of analytical functions, including trend lines and predictive modeling, churn prediction, customer segmentation, market share forecasting, trend analysis, and anomaly detection.

- 5.2.6 Utilize AI and ML algorithms to enhance the analytic capabilities, such as automated insights, natural language processing (NLP), and intelligent data preparation.
- 5.2.7 Provide interactive, conversational data exploration and support create interactive dashboards, reports, and ad-hoc analysis tools.

5.3 AI and ML Integration:

- 5.3.1 Incorporate advanced AI and ML algorithms to enable intelligent data processing, pattern recognition, and predictive insights.
- 5.3.2 Provide tools and interfaces for users to develop, train, and deploy custom ML models within the analytic platform.
- 5.2.8 Implement Machine Learning models to provide Predictive analysis, Fraud detection capability models to identify and prevent fraudulent activities.
- 5.2.9 Network Anomaly Detection to identify unusual network activity patterns that might indicate network issues or potential security threats.
- 5.3.3 Offer pre-built AI and ML models for common business use cases (e.g., demand forecasting, customer churn prediction, anomaly detection).
- 5.3.4 Ensure seamless integration and collaboration between the analytic tool and the organization's existing infrastructure (if applicable).

5.4 HR and Administrative KPI:

Interactive dashboards need to develop to visualize Human Resource along with other administrative data that include but not limited below organization KPIs.

5.4.1 Headcount and Workforce Composition

Total number of employees

Employee, demographics (age, gender, tenure, etc.)

Employee distribution by department, Grade, title, education, job function, or location}.

5.4.2 Talent Acquisition and Recruitment

Time to fill positions

Source of hire (employee, referral, job board, etc.)

Candidate pipeline metrics (applications, interviews, offers, acceptance rates) ✓

Cost per hire.

5.4.3 Employee Turnover and Retention:

Voluntary turnover rate

Involuntary turnover rate

Employee retention rate

Reasons for employee attrition 5.4.4 **Performance and Talent Management:**

Employee performance ratings

Promotion and internal mobility rates

Succession planning metrics

Training and development completion rates ✓ Support 360-Degree appraisal and feedback

5.4.5 Compensation and Benefits:

Average salary by job level, department, or location

Compensation competitiveness compared to industry benchmarks ✓ Employee benefits, bonus, over time utilization rates ✓ Employee expenses, insurance, education, travel, etc.

5.4.6 Employee Engagement and Satisfaction:

Employee engagement survey scores

Employee Net Promoter Score (eNPS)

Reasons for employee satisfaction or dissatisfaction

5.4.7 Diversity, Equity, and Inclusion (DEI):

Representation of underrepresented groups at different job levels

Diversity of the leadership team

Pay equity analysis

5.4.8 Compliance and Risk Management:

Incidents of workplace harassment or discrimination

Compliance with labor laws and regulations

Workplace safety metrics (e.g., incident rates, lost time, worker's compensation claims)

5.4.9 HR Operational Efficiency:

HR staff productivity (e.g., cases handled per HR generalist)

HR budget and expenses

HR technology utilization and adoption.

5.5 Migrate or develop Existing SAP BI/BO reports!

Etisalat Afghanistan is currently using the SAP Business Intelligence/Business Objects (SAP BI Platform BOE 4.2 SPS06/ Version 14.2.7.3069) platform to provide reporting, dashboarding, and analytics solutions to various departments within the organization, including Revenue Assurance, Finance, Marketing, and Sales.

This platform is enabling these departments to gain valuable data-driven insights into their business operations and customer behavior, So the existing report and dashboards currently running on SAP BI/BO need to be developed with enhancement and migrated to New platform by considering below key points.

- 5.5.1 Assess the existing reports, dashboards, and automated reports developed on the SAP BI/BO platform.
- 5.5.2 Determine which of these can be directly migrated to the new analytics solution, and which ones may need to be redeveloped to take advantage of the new platform's features and capabilities.
- 5.5.3 Ensure that the migration or redevelopment process preserves the key functionalities and insights provided by the existing reports and dashboards.
- 5.5.4 leverage the new platform's capabilities (AI&ML) to enhance the organization's datadriven decision-making processes and gain deeper insights into their business operations and customer behavior.

6. Implementation

6.1 Deployment and Integration

- 6.1.1 Support on-premises, cloud-based, or hybrid deployment models to align with the organization's IT infrastructure.
- 6.1.2 support virtualization and containerization technologies and provide flexible system architecture with Virtual Machine approach.
- 6.1.3 Provide APIs and integration capabilities to enable seamless connectivity with other business applications and systems.
- 6.1.4 Ensure easy deployment, configuration, and maintenance of the analytic solution, with minimal IT overhead.

6.2 User Experience, security and Collaboration

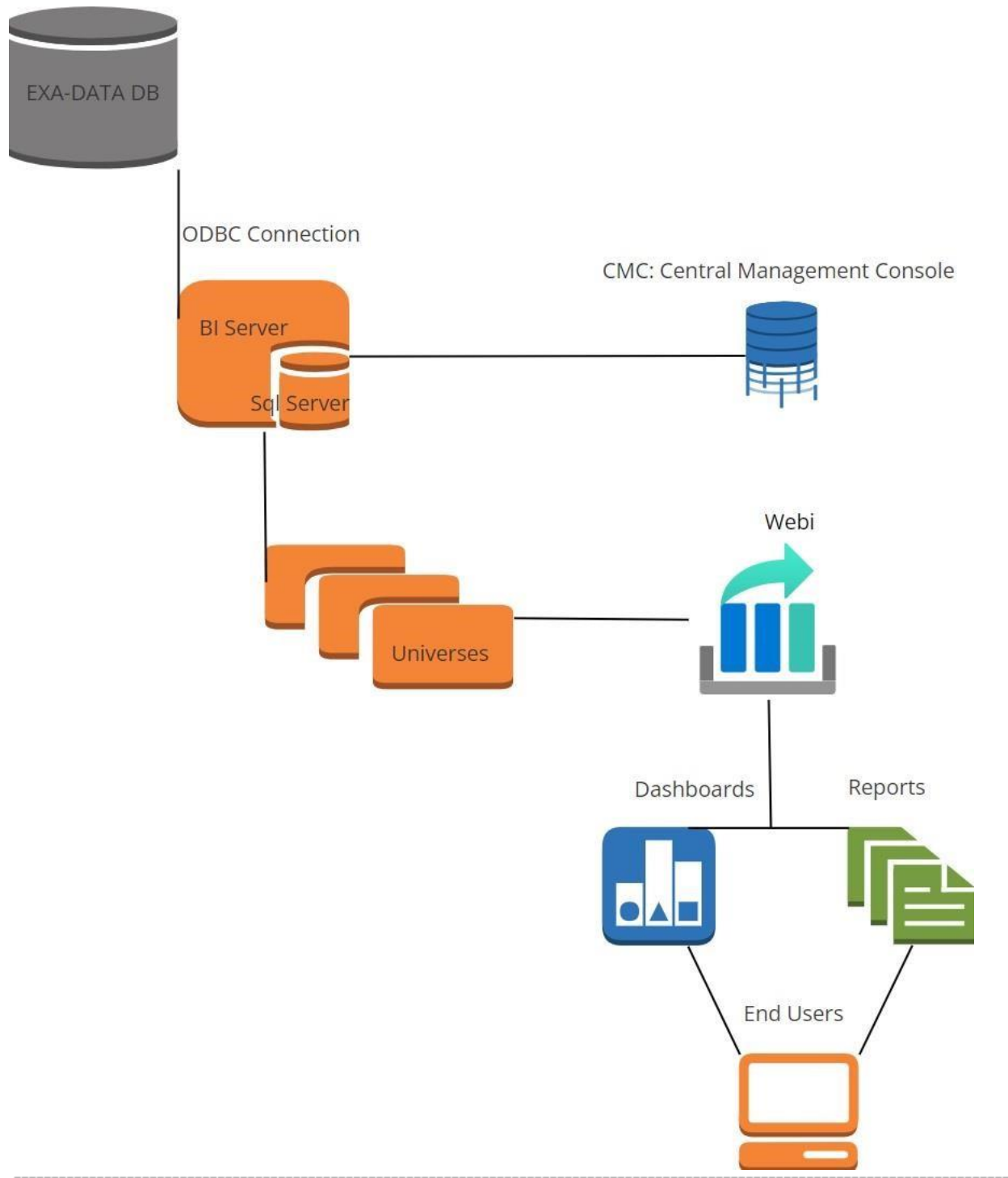
- 6.2.1 Deliver a responsive and intuitive user interface that caters to both technical and nontechnical users.
- 6.2.2 Offer self-service capabilities, allowing users to create, customize, and share reports and dashboards.
- 6.2.3 Provide collaborative features, such as real-time co-authoring, commenting, and sharing of analytical content.
- 6.2.4 Ensure the solution is accessible across various devices and platforms, including mobile and web-based interfaces.
- 6.2.5 Manage users, Provide role-based access controls, encryption, decryption features, logging capabilities, security compliance and automation process.
- 6.2.6 Support integration to security tools including but not limited to EDR, SIEM, MFA, PAM, IAM, NAC & Tenable Nessus.

6.3 Scalability and Performance:

- 6.3.1 Provide vertical and horizontal scaling techniques to handle growing data volumes, user demands, complex requirements and concurrent usage without compromising performance.
- 6.3.2 Offer load-balancing, failover, and disaster recovery mechanisms to ensure high availability and business continuity.
- 6.3.3 Provide a roadmap for future scalability and feature enhancements to address evolving business requirements.

Annex A

Existing SAP BI/BO diagram connection to Data Warehouse Platform (Exadata Oracle).



Annexure-B

Cybersecurity Requirements

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
 2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
 3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
 4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
 5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
 6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
 7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
 8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
 9. Vendor must use and install only licensed applications.
 10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
 11. Vendor must not use/install any application/service that is not required.
 12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
 13. Vendor must align their changes according to EA Change Management Policy.
 14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.
-

15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.
 16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.
 17. System must support Role Based Access Control, and Rule Based Access Control
 18. System must provide Strong authentication and authorization mechanisms
 19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.
 - Failed and successful logins
 - Modification of security settings
 - Privileged use or escalation of privileges
 - System events
 - Modification of system-level objects
 - Session activity
 - Account management activities including password changes, account creation, modification...
 - Event logs must contain the following details:
 - Date and time of activity
 - Source and Destination IP for the related activity
 - Identification of user performing activity
 - Description of an attempted or completed activity.
 20. The system must support live log retention of 1 Year and backup up to 3 years.
 21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
 22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
 23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.
 24. Vendor system's password configuration must be aligned with EA Information security policies.
-

25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

No.	Description	Compliance (YES/NO/NA)	Comments
1	Etisalat Security Requirements		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFX/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or		

No.	Description	Compliance (YES/NO/NA)	Comments
	Third Party Contracted to do the testing, with no additional cost		
1.5	<p>Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT.</p> <p>The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.</p>		
2	Security Architecture		
2.1	<p>The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.</p>		
2.2	<p>The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.</p>		
2.3	<p>The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ</p>		

No.	Description	Compliance (YES/NO/NA)	Comments
	and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	Password Security		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		

No.	Description	Compliance (YES/NO/NA)	Comments
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	Authentication		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	Authorization		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		

No.	Description	Compliance (YES/NO/NA)	Comments
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User...		
6	Software Security		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow...etc.		
6.6	For web portals, the proposed system includes all security controls to prevent/protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation...		

No.	Description	Compliance (YES/NO/ NA)	Comments
7	Security Event Logging		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	Public Cloud Security		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality ...) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or		

	support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	Virtualization and Container Security		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

RFP General Terms Compliance to be filled by Bidder.

S/N	Clause No. and General Terms	Comply (Yes/No)	Remarks
1	4. VALIDITY OF OFFERS:		
2	6. ACCEPTANCE OF OFFERS:		
3	7. REGISTRATION/LEGAL DOCUMENTS OF THE BIDDER		
4	8. PAYMENTS		
5	9. PENALTY:		
6	10. CONSTRUCTION OF CONTRACT:		
7	11. TERMINATION OF THE CONTRACT BY THE PURCHASER		
8	12. LOCAL TAXES, DUES AND LEVIES:		

The following Information must be submitted with offer.

Bidder Contact Details	
Bidder Name	
Bidder Address	
Bidder Email Address	
Bidder Phone Number	
Bidder Contact Person Name	
Bidder Contact Person Phone No	
Bidder Contact Person Email Address	
Bidder Registration License Number	
License Validity	
TIN Number /Tax Number	

===== end of documents =====