

TENDER NOTICE

RFP No. EA/02-54-2026

For Provision of Integrated Risk Management System

1. Bids are invited from your esteemed Corporation for Provision of integrated risk management system as per RFP Annexure. This bid Document is also available on the Etisalat website (www.eand.af, Tenders).
2. RFP Deadline is **08 October 2026 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@eand.af) and cc: (Ihsanullah@eand.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 items supplied must be new, genuine, and original. Counterfeit, copied, refurbished, used, repaired, or damaged items will be rejected immediately. The bidder shall submit a valid and updated Business License and a Corporate Bank Account in the registered name of the company as part of the bid submission. Cash payments and payments to personal/individual bank accounts will not be accepted. Payments will only be made to the bidder's verified corporate bank account registered under the company's legal name.

8. All correspondence on the subject may be addressed to Shoaib Nabizada, Sr. Analyst Procurement & Contracts, and Etisalat Afghanistan. Email snabizada@eand.af and Phone No. +93781204113.

Ihsanullah Zirak

Director Procurement and Supply Chain

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

E-mail: ihsanullah@eand.af

(RFP)

For

**Provision of Integrated Risk
Management System
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 Provision of Integrated Risk Management System 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 75% of the amount after delivery of the software/license and installation.

5.5.1.2 Balance 25% of the amount after completion of project and final acceptance certificated (FAC).

6. 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.

7. Termination of the Contract

7.1 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.

7.2 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.

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

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

8. Local Taxes, Dues and Levies:

8.1 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.

8.2 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:

Procurement of Integrated Risk Management System (IRMS) for Enterprise Risk Management and Internal Audit

1. Objective

The objective of this procurement is to implement a centralized, automated, and integrated Risk Management System that supports Enterprise Risk Management (ERM) and Internal Audit functions within a single platform.

The solution shall enable the organization to identify, assess, monitor, and mitigate risks while facilitating risk-based audit planning, audit execution, issue tracking, reporting, and governance oversight. The system shall provide end-to-end visibility of risks, controls, audit activities, remediation actions, and compliance obligations to support effective decision-making and organizational resilience.

2. Functional Scope

2.1 Enterprise Risk Management (ERM)

Risk Identification and Assessment

The solution shall:

- Maintain centralized enterprise risk registers.
- Capture risks across all organizational functions, including Information Technology, Finance, Human Resources, Operations, Procurement, Projects, and Strategic Initiatives.
- Support risk categorization, taxonomy, and hierarchical risk structures.
- Facilitate inherent and residual risk assessments.
- Support qualitative and quantitative risk assessment methodologies.
- Allow risk scoring based on likelihood, impact, velocity, and other configurable criteria.
- Support periodic risk reviews, reassessments, and approvals.
- Maintain historical risk records and assessment history.

Risk Treatment and Action Management

The solution shall:

- Assign risk treatment plans and mitigation actions.
 - Assign accountability to risk owners and action owners.
-

- Track mitigation progress and target completion dates.
- Support escalation mechanisms for overdue actions.
- Monitor effectiveness of mitigation activities.
- Enable linkage between risks, controls, objectives, and action plans.

Key Risk Indicator (KRI) Management

The solution shall:

- Define and monitor KRIs and thresholds.
- Generate alerts for threshold breaches.
- Support trend analysis and performance monitoring.
- Provide proactive reporting on emerging risks.

Risk Monitoring and Reporting

The solution shall:

- Provide real-time risk dashboards.
- Generate risk heat maps and risk trend reports.
- Support executive-level and board-level reporting.
- Provide consolidated enterprise risk views.
- Enable drill-down capability from enterprise-level risks to underlying details.

2.2 Internal Audit Management

Audit Universe Management

The solution shall:

- Maintain a centralized audit universe.
- Support categorization of auditable entities, processes, systems, projects, and departments.
- Link audit universe elements to enterprise risks and strategic objectives.
- Support periodic updates and risk assessments of auditable entities.

Risk-Based Audit Planning

The solution shall:

- Support annual and multi-year audit planning.
- Prioritize audit engagements based on risk assessments.
- Facilitate audit resource and capacity planning.

- Support audit plan approval workflows.
- Allow audit plan revisions and tracking of changes.

Audit Engagement Management

The solution shall:

- Support end-to-end audit lifecycle management.
- Create and manage audit engagements.
- Define audit objectives, scope, criteria, and audit programs.
- Manage audit schedules and resource assignments.
- Track audit milestones and completion status.

Workpaper and Evidence Management

The solution shall:

- Maintain electronic audit workpapers.
- Store audit evidence and supporting documentation.
- Provide document version control.
- Enable review and approval workflows.
- Ensure secure retention of audit documentation.

Audit Testing and Fieldwork

The solution shall:

- Record testing procedures and results.
- Support sampling methodologies.
- Document observations and exceptions.
- Track audit progress during fieldwork.
- Maintain full audit trails of testing activities.

Audit Findings and Recommendations

The solution shall:

- Capture audit findings and observations.
- Assign risk ratings to audit findings.
- Document root causes and recommendations.
- Track management responses.

- Maintain a centralized findings repository.

Corrective Action Tracking

The solution shall:

- Assign remediation actions to responsible management.
- Monitor implementation progress.
- Generate reminders and escalation notifications.
- Validate completion of corrective actions.
- Support closure approval processes.

Audit Reporting

The solution shall:

- Generate draft and final audit reports.
- Support configurable report templates.
- Produce executive and management reports.
- Track audit KPIs and performance metrics.
- Provide dashboards for Audit Management, Executive Management, and Audit Committees.

2.3 Governance, Controls and Assurance Management

The solution shall:

- Maintain a centralized control repository.
- Map controls to risks, policies, audit findings, and business processes.
- Support control ownership assignment.
- Track control effectiveness assessments.
- Facilitate control testing activities.
- Support Key Control Indicator (KCI) monitoring.
- Provide integrated reporting across risks, controls, and audits.

2.4 Policy and Compliance Management

The solution shall:

- Manage policy lifecycle activities including creation, review, approval, publication, and archival.
 - Maintain version control and document history.
-

- Support policy acknowledgement and attestation processes.
- Map policies and procedures to risks and controls.
- Maintain compliance obligations and requirements repositories.
- Support evidence collection and retention.
- Provide compliance status dashboards and reporting.

2.5 Integrated Risk and Audit Relationship Management

The solution shall:

- Integrate ERM and Internal Audit processes within a single platform.
- Link audit engagements to enterprise risks.
- Link audit findings to risk registers and controls.
- Automatically update risk profiles based on audit outcomes where applicable.
- Enable Internal Audit to leverage risk assessment results during audit planning.
- Provide consolidated dashboards covering risks, controls, audit engagements, findings, and remediation actions.
- Support a common repository for risks, controls, audits, actions, and evidence.

2.6 Workflow Automation and Collaboration

The solution shall:

- Provide configurable workflow management.
- Automate approval processes.
- Generate notifications, reminders, and escalations.
- Support task assignments and status tracking.
- Enable collaboration among Risk Owners, Control Owners, Auditors, Management, and Committee Members.
- Maintain activity logs and workflow histories.

2.7 Dashboards, Analytics and Reporting

The solution shall provide:

Executive Dashboards

- Enterprise risk status.
- Audit plan progress.

- High-risk findings.
- Overdue corrective actions.
- Risk and audit trends.

Management Dashboards

- Departmental risk profiles.
- Action plan status.
- Control assessment results.
- Audit engagement status.

Reporting Capabilities

- Configurable and ad hoc reports.
- Heat maps and trend analysis.
- Risk exposure reports.
- Audit coverage reports.
- Findings aging reports.
- Remediation status reports.
- Export capabilities to standard formats.

3. Technical Requirements

The solution shall:

- Be web-based or cloud-hosted.
- Support secure access from multiple locations.
- Provide role-based access control (RBAC).
- Support segregation of duties.
- Support Single Sign-On (SSO).
- Support multi-factor authentication (MFA).
- Encrypt data at rest and in transit.
- Maintain comprehensive audit logs.
- Support configurable workflows without extensive custom development.

- Provide open APIs for system integration.
- Support mobile-responsive access.
- Provide scalability to support future organizational growth.

4. Integration Requirements

The solution shall support integration with:

- Enterprise Resource Planning (ERP) systems.
- Identity and Access Management systems.
- Cybersecurity and Security Monitoring solutions.
- Service Management and Ticketing platforms.
- Document Management Systems.
- Business Intelligence and Reporting platforms.
- Email and collaboration platforms.

5. Operational Requirements

The vendor shall provide:

- Solution implementation services.
- System configuration and customization.
- Data migration support.
- User Acceptance Testing (UAT) support.
- Production deployment support.
- User and administrator training.
- Knowledge transfer to designated personnel.
- Technical documentation and user manuals.
- Post-implementation support and maintenance services.

6. Security Requirements

The solution shall:

- Maintain confidentiality, integrity, and availability of information.
- Support secure user authentication.
- Maintain detailed audit trails.

- Support secure evidence management.
- Implement data backup and recovery mechanisms.
- Provide disaster recovery capabilities.
- Support configurable retention and archival periods.

7. Compliance and Assurance Requirements

The solution shall:

- Maintain a centralized evidence repository.
- Support records retention and archival requirements.
- Maintain complete audit trails for all transactions and activities.
- Provide real-time monitoring of risks, audits, controls, and remediation activities.
- Support management attestations and approvals.
- Facilitate internal assurance and governance reporting.

8. Standards and Framework Alignment

The solution should support alignment with internationally recognized frameworks including:

- Institute of Internal Auditors (IIA) Global Internal Audit Standards.
- COSO Enterprise Risk Management Framework.
- ISO 31000 Risk Management Guidelines.
- COBIT.
- ISO 27001.
- NIST Cybersecurity Framework.
- Other industry-recognized governance, risk, and control frameworks as applicable.

9. Expected Outcomes

The implemented IRMS shall:

- Provide a single integrated platform for ERM and Internal Audit.
- Enhance risk visibility across the organization.
- Improve risk-based audit planning and execution.

- Strengthen governance and accountability.
- Improve monitoring of remediation activities.
- Reduce manual effort through workflow automation.
- Enhance management reporting and decision-making.
- Improve coordination between risk management and internal audit functions.
- Establish a consistent and structured approach to risk, control, and audit management across the organization.

Annexure-B

EA Cybersecurity Requirements

Overview

This document defines the minimum Cybersecurity requirements that must be considered and incorporated in the RFx documents for new projects and systems. The Cybersecurity requirements are created in adherence to Etisalat Afghanistan Cybersecurity Policies.

The cybersecurity requirements outlined in our RFPs and contracts serve as the foundation of our commitment to safeguarding sensitive data and ensuring the integrity of our operations. Compliance with these measures is not just a formality but an essential component in mitigating risks, maintaining legal compliance, and protecting the trust of our stakeholders. By adhering to our cybersecurity protocols, vendors play a key role in strengthening our digital infrastructure against evolving threats, thereby contributing to a secure and resilient business ecosystem. We urge vendors to recognize the significance of these requirements and partner with us in upholding the highest standards of cybersecurity excellence.

Important Note

Bidders, vendors, project managers, 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 Afghanistan Cybersecurity Department.

For any compliant items, further supporting documents must be submitted to the Cybersecurity Department for analysis and validation.

S.No	Description	Compliance (YES/NO/NA)	Comments
1	Security Requirements		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat Afghanistan 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 Afghanistan's Cybersecurity Audit (Vulnerability Assessment/Penetration Testing/Security Audit) before go-live/service acceptance by Etisalat Afghanistan. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues/vulnerabilities identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost even after going live.		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, Static/Dynamic Code Analysis, red teaming exercises and scans that check for compliance against the baseline security		

S.No	Description	Compliance (YES/NO/NA)	Comments
	standards or security best practices, before the new product or any of its releases is delivered to ETISALAT Afghanistan.		
1.6	The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution to Cybersecurity Department of Etisalat Afghanistan.		
1.7	Proposed system must not have dependency on end of life/end of support software or any such requirements.		
1.8	The proposed system (OS & Database) must be hardened with CIS control as per EA Secure Configuration Policy.		
1.9	Vendor must report any security incident or suspicious activity to Etisalat SOC team at soc@etisalat.af address.		
1.10	Vendor must ensure their operating systems/hardware are up to date and is not End of Life/End of support in next 3 years.		
1.11	EA has the right to request for vulnerabilities or penetration testing reports of web applications if vendor is supposed to deploy any in EA.		
1.12	The proposed system must not have any dependency on end of life/end of support software or any such requirements.		
1.13	Vendors must align all their services and configurations in accordance to EA Information Security policies and standards.		
1.14	Vendors must use and install only licensed applications.		
1.15	The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.		
1.16	Vendor must access the servers only through Etisalat PAM solution.		
1.17	In the event of a security concern or suspicious activity arising from the vendor's end, Etisalat reserves the right to suspend or revoke access during investigation from Etisalat's side.		
1.18	Vendor must align their changes according to EA Change Management Policy.		
1.19	Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.		
1.20	The database must encrypt admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.		
2	Security Architecture		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as UAE NESA (SIA) IA V2, UAE DESC (ISR), UAE TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	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		

S.No	Description	Compliance (YES/NO/NA)	Comments
	firmware that is not End of Life or End of Support.		
2.3	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 and access to internal sensitive data shall be secured through the middle tier application proxy and/or a standard Firewall Technology.		
2.4	The proposed solution shall not impact the existing Etisalat Afghanistan security controls or posture in any way.		
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 are strictly prohibited.		
3	Password Security		
3.1	All Operating Systems (e.g. Linux and Windows) must be hardened according to the official secure configuration baseline of Etisalat Afghanistan and to fully comply with Etisalat Afghanistan Security Policies.		
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/Threshold		
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)		
3.10	The hashing/encryption algorithm of the proposed solution must be in compliant with Etisalat Afghanistan cryptographic requirements.		
3.11	Forgetting or resetting password function must support MFA mechanism 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 integration with industry Privilege account Management (PAM) solutions.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent against password attacks including but not limited to Dictionary Attack, Brute		

S.No	Description	Compliance (YES/NO/NA)	Comments
	Force and Password Spraying mechanism.		
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 including but not limited to FTP, Telnet, NTLM v1, and 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 were deemed necessary.		
4.9	The proposed solution shall support integration with Identity and Access Management solution (IAM) for user lifecycle management via standard APIs.		
4.10	The proposed solution must support LDAP and RADIUS authentication.		
5	Authorization		
5.1	The proposed solution shall support role-based and Rule Based access controls that includes access profiles or security matrix (i.e., Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based / rule-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 per Etisalat Afghanistan's Cybersecurity Policies		
6.5	The proposed system enforces input and output validation to prevent Cyber-attacks including but not limited to SQL Injection, Buffer Overflow, XSS and SSRF...etc.		
6.6	For web portals, the proposed solution shall include all the security controls to prevent / protect the application against 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...		

S.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) Source and Destination IPs d) Transaction ID & session information e) Failed/Successful Logins f) Modification of Security Settings g) Privilege Escalation h) User Account Modification		
7.3	The proposed solution shall support the integration with Etisalat Afghanistan NTP server for time synchronization and accurate logging.		
7.4	The proposed solution shall support integration with IBM QRadar for Log Aggregation and Correlation.		
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 in full compliance with Etisalat Afghanistan's Cryptographic requirements.		
8.2	The Public Cloud setup that stores PII information shall be hosted in the UAE		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat Afghanistan (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 Afghanistan Cybersecurity Department		
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 Afghanistan's 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		

S.No	Description	Compliance (YES/NO/NA)	Comments
	applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
10	Artificial Intelligence and Machine Learning Security		
10.1	If the proposed solution uses AI/ML, it must ensure model integrity, prevent model poisoning, and protect training data from leakage.		
10.2	Any AI model must be explainable and auditable, especially for systems impacting customer services or security decisions		
10.3	AI/ML-based systems must include monitoring to detect adversarial inputs or behavioral drift.		
10.4	Access to AI training datasets must be role-based and logged.		
11	Encryption and Key Management		
11.1	All sensitive data at rest and in transit must be encrypted using strong encryption standards (AES-256, TLS 1.3, etc.).		
11.2	Key management must be handled via secure KMS (Key Management Systems) in compliance with Etisalat Afghanistan's Cryptographic Policy.		
11.3	Private keys and credentials must not be hardcoded into applications or scripts.		
12	Database Security		
12.1	The database must enforce the least privilege of access and role separation.		
12.2	Database activity monitoring (DAM) should be enabled and integrated with the SIEM.		
12.3	Sensitive fields (e.g., PII, financials) must be encrypted and masking enabled for non-privileged users.		
12.4	Default accounts and unused stored procedures must be disabled or removed.		
13	Network Security		
13.1	The solution must comply with Etisalat Afghanistan's network segmentation and zero trust architecture.		
13.2	2 All network connections must be protected using firewalls, IDS/IPS, and NDR (Network Detection and Response).		
13.3	Insecure protocols (e.g., Telnet, SMBv1) must be disabled.		
13.4	Remote access must be restricted and controlled through VPN, MFA, and PAM.		
14	API Security		
14.1	APIs must enforce authentication and authorization using OAuth2.0 or JWT standards.		
14.2	APIs must be protected against OWASP API Top 10		

Dated: August-2026

S.No	Description	Compliance (YES/NO/NA)	Comments
	vulnerabilities.		
14.3	API traffic must be logged and monitored with anomaly detection.		
14.4	Rate limiting and throttling mechanisms must be in place to prevent abuse.		
No.	Description	Compliance (YES/NO/NA)	Comments
15	Physical and Environmental Security		
15.1	Equipment housing critical data must reside in secure, access-controlled environments.		
15.2	Physical access to sensitive areas must be logged and monitored.		
15.3	Proper labeling, secure disposal, and asset lifecycle tracking must be implemented for all hardware.		
15.4	Surveillance and intrusion detection must be in place for all datacenter or server rooms used in the project.		
16	Infrastructure and Visibility		
16.1	All components of the infrastructure must support centralized logging and monitoring.		
16.2	The system must support integration with vulnerability scanners and patch management tools.		
16.3	Network and application topology must be documented and shared with EA Cybersecurity.		
16.4	Shadow IT and undocumented components must be reported and approved before deployment.		

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	10. CONSTRUCTION OF CONTRACT:		
6	11. TERMINATION OF THE CONTRACT BY THE PURCHASER		
7	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 =====