**Request for Proposal (RFP) for Assessment of Requirements for Ensuring Information Security in Entities Operating Under Financial Sector**

1. **Introduction**

Unibank CB is seeking proposals from qualified firms to conduct a comprehensive assessment of our information security practices in accordance with **the requirements set forth by the Central Bank of the Republic of Azerbaijan for entities operating in the financial sector**. The objective of this assessment is to ensure compliance with applicable national legislation, identify gaps or vulnerabilities, and provide actionable recommendations for remediation and regulatory alignment.

1. **Background**

Unibank CB is a leading financial institution dedicated to providing secure and efficient financial services to our valued customers. As a trusted entity in the banking sector, we recognize the paramount importance of ensuring the confidentiality, integrity, and availability of our payment card transactions.

**2.1 Overview of the Banking System:**

Our banking system processes a vast number of payment card transactions daily, encompassing various financial activities such as withdrawals, deposits, fund transfers, and online purchases. The security and integrity of these transactions are critical not only for maintaining the trust of our customers but also for complying with industry regulations and standards.

**2.2 Importance of Compliance with Central Bank Information Security Requirements**

Compliance with the information security requirements established by the Central Bank of the Republic of Azerbaijan is critical for maintaining the integrity, confidentiality, and availability of financial data across institutions operating within the sector. As digital transformation accelerates and cyber threats evolve, ensuring alignment with national regulatory standards is essential for protecting sensitive customer information, enhancing operational resilience, and maintaining trust in the financial system. A robust assessment of current security practices enables institutions to identify gaps, strengthen controls, and ensure continued compliance with the Central Bank’s expectations.

1. **Scope of Work**

The selected firm will conduct a comprehensive assessment of Unibank CB’s information security practices, ensuring alignment with the regulatory requirements set forth by the Central Bank of the Republic of Azerbaijan. The assessment will encompass the following key areas:

* 1. **Information Security Management System (İnformasiya Təhlükəsizliyinin İdarə Edilməsi Sistemi)t:**
     1. **Governance and Policy Framework:**
        1. Evaluate the establishment, documentation, and implementation of the Information Security Management System (ISMS) in accordance with national standards.
        2. Assess the alignment of information security policies with organizational objectives and regulatory mandates.
     2. **Risk Management Processes:**
        1. Review methodologies for identifying, assessing, and mitigating information security risks.​
        2. Evaluate the effectiveness of risk treatment plans and ongoing risk monitoring activities.
  2. **Organizational Control Measures (Təşkilati Nəzarət Tədbirləri):**

**3.2.1 Access Control and Authorization:**

3.2.1.1 Assess the processes for granting, reviewing, and revoking access rights to information systems.

3.2.1.2 Evaluate the implementation of role-based access controls and segregation of duties.

* + 1. **Third-Party Management**
       1. Review policies and procedures governing the selection, onboarding, and monitoring of third-party service providers.​
       2. Assess contractual agreements to ensure they include appropriate information security clauses.​
  1. **Human Resources Security Controls (İnsan Resursları Üzrə Nəzarət Tədbirləri)**

**3.3.1 Employee Screening and Onboarding**

* + - 1. Evaluate background verification processes for new hires in sensitive positions.
      2. A​ssess the effectiveness of confidentiality agreements and security awareness during onboarding.

**3.3.2 Ongoing Training and Awareness**

* + - 1. Review the frequency and content of information security training programs.​
      2. Assess mechanisms for evaluating employee understanding and compliance with security policies.
  1. **Physical Security Controls (Fiziki Təhlükəsizlik Üzrə Nəzarət Tədbirləri)**

**3.4.1. Facility Access and Surveillance**

* + - 1. Assess the adequacy of physical barriers, surveillance systems, and access controls at critical facilities.​
      2. Evaluate procedures for visitor management and monitoring.

**3.4.2. Environmental Protections**

* + - 1. Review safeguards against environmental threats such as fire, flood, and power outages.​
      2. Assess the maintenance and testing of environmental control systems.
  1. **Technological Control Measures (Texnoloji Nəzarət Tədbirləri)**

**3.5.1. Network and System Security**

* + - 1. Conduct assessments of network architecture to identify potential vulnerabilities.​
      2. Evaluate the deployment and configuration of firewalls, intrusion detection/prevention systems, and anti-malware solutions.​

**3.5.2. Data Protection and Encryption**

* + - 1. Assess the implementation of data encryption for data at rest and in transit.​
      2. Review data masking and anonymization techniques for sensitive information.​

**3.5.3. Incident Response and Management**

* + - 1. Evaluate the existence and effectiveness of incident detection, reporting, and response mechanisms.​
      2. Review post-incident analysis and lessons learned processes.​
  1. **Reporting and Accountability (Hesabatlıq)**

**3.6.1. Documentation and Record-Keeping**

* + - 1. Assess the policies and procedures for maintaining logs and records of security events and incidents.​
      2. Evaluate the retention periods and protection measures for sensitive records.​

**3.6.2. Compliance Reporting**

* + - 1. Review the processes for internal and external reporting of compliance with information security standards and regulations.​
      2. Assess the mechanisms for addressing audit findings and implementing corrective actions.

**4. Reporting and Accountability**

**4.1. Assessment Report**

* + 1. Prepare a comprehensive report summarizing all identified findings, including detected vulnerabilities, non-compliance issues with national regulatory requirements, and opportunities for improving the organization’s information security posture.
    2. Classify findings based on risk severity, likelihood of exploitation, and potential impact on the confidentiality, integrity, and availability of critical information assets.

#### **4.2. Compliance Recommendations**

* + 1. Provide prioritized, actionable recommendations for remediation aligned with the requirements of the Central Bank of the Republic of Azerbaijan.
    2. Include implementation guidance for each recommendation, focusing on risk reduction, regulatory compliance, and sustainable improvements to the information security management system.

#### **4.3. Regulatory Alignment Matrix**

4.3.1. Present a traceable mapping of assessment results against the specific articles and clauses defined in the Central Bank’s regulatory framework (e.g., Sections 3 through 8 - <https://e-qanun.az/framework/56708>).

4.3.2 Highlight areas of full compliance, partial compliance, and non-compliance, along with related justifications and evidence.

## **The Work Contractor’s Obligations**

The assessment must be conducted by a company that is internationally accredited in the field of information security audits and possesses a minimum of 3 (three) years of proven experience in auditing information security within the financial sector,(in accordance with the requirements set forth by the Central Bank.)