TƏKLİF SORĞUSU (RFP)

Azərbaycan Respublikası Mərkəzi Bankının İnformasiya Təhlükəsizliyinə dair Tələblərə Uyğunluq Auditi

H.Zərdabi küçəsi 81K, Bakı, AZ 1122

Tel.: + 994 12 981

1. Giriş və Məqsəd

Yelo Bank (bundan sonra "Bank") kibertəhlükəsizlik sahəsində ixtisaslaşmış şirkətləri Azərbaycan Respublikası Mərkəzi Bankının (ARMB) İnformasiya Təhlükəsizliyinə dair tələblərinə uyğunluq auditi üzrə təkliflər təqdim etməyə dəvət edir.

Auditin məqsədi Bankın ARMB-nin 28 mart 2024-cü il tarixli, 14/2 nömrəli Qərarı ilə təsdiq edilmiş "Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər" çərçivəsindəki öhdəliklərə uyğunluğunun müstəqil və obyektiv qiymətləndirilməsidir.

Audit fəaliyyəti Azərbaycan Respublikası ərazisində qeydiyyatdan keçmiş hüquqi şəxs tərəfindən həyata keçirilməlidir. Auditoru müstəqil və Bank rəhbərliyindən müstəqil olmalıdır.

2. İş Əhatəsi

2.1 Tənzimləyici Əsas

Audit aşağıdakı normativ aktlar çərçivəsində aparılmalıdır:

- ARMB İdarə Heyətinin 28 mart 2024-cü il tarixli, 14/2 nömrəli Qərarı — "Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"
- Tətbiq olunan beynəlxalq standartlar: ISO 27001, ISO 27005, ISO 22301, NIST CSF

3. Audit Metodologiyası

Audit aşağıdakı beynəlxalq standartlara və çərçivələrə uyğun aparılmalıdır:

Standart / Çərçivə	Tətbiq Sahəsi	Tələb Olunan Əhatə
ARMB 14/2 Qərarı	Bütün audit istiqamətləri	Tam
ISO 27001:2022	Nəzarət çərçivəsi	İstinad
ISO 27005:2022	Risk qiymətləndirməsi	İstinad
ISO 22301:2019	Fəaliyyətin davamlılığı	İstinad
ISACA COBIT	İT idarəetmə qiymətləndirməsi	İstinad

Audit prosesi aşağıdakı mərhələləri əhatə etməlidir:

1. Planlaşdırma — əhatə dairəsinin dəqiqləşdirilməsi, sənəd sorğuları, başlanğıc görüşü
2. Sənəd nəzərdən keçirməsi — siyasət, prosedur, texniki konfiqurasiya sənədlərinin analizi
3. Müsahibələr — müvafiq şöbə rəhbərləri və texniki mütəxəssislərlə görüşlər
4. Texniki yoxlama — əsas texniki nəzarətlərin konfiqurasiya səviyyəsində yoxlanılması
5. Uyğunsuzluq analizi — ARMB tələblərinə uyğunsuzluqların müəyyənləşdirilməsi

6. Hesabat hazırlığı — nəticələrin sənədləşdirilməsi və tövsiyələrin formalaşdırılması
7. Yekun görüş — hesabatın müzakirəsi və Bank rəhbərliyi ilə nəticələrin paylaşılması

4. Hesabat Tələbləri

4.1 Ümumi Hesabat Standartları

Audit tamamlandıqdan sonra təchizatçı iki hesabat formatı təqdim etməlidir:

Hesabat Növü	Məzmun Tələbləri
Texniki Audit Hesabatı	• ARMB tələblərinin hər bir maddəsi üzrə uyğunluq statusu (Uyğun / Qismən Uyğun / Uyğun Deyil) • Hər uyğunsuzluq üçün: tələb maddəsi, mövcud vəziyyət, boşluğun təsviri, risk səviyyəsi • Sübutlar və müşahidələr — müsahibə qeydləri, sənəd istinadları, texniki tapıntılar • Hər tapıntı üçün xüsusi aradan qaldırma tövsiyəsi • Tövsiyələrin prioritetləşdirilməsi: Kritik / Yüksək / Orta / Aşağı • Aradan qaldırma yol xəritəsi — tövsiyə olunan müddətlərlə • Bankın mövcud İT yetkinlik səviyyəsinin ümumi qiymətləndirilməsi
İcraiyyə Xülasəsi Hesabatı	• Bank rəhbərliyi və İdarə Heyəti üçün texniki olmayan ümumi baxış • Uyğunluq vəziyyətinin ümumi mənzərəsi — uyğun, qismən uyğun və uyğun olmayan tələblərin sayı • Ən kritik boşluqlar və onların biznes riskinə təsiri • Strateji tövsiyələr və prioritetləşdirilmiş fəaliyyət planı • Müqayisəli uyğunluq matrisi — cədvəl formatında

4.2 Kritik Tapıntıların Bildirişi

Audit zamanı aşkar edilən istənilən kritik uyğunsuzluq — xüsusilə ARMB tənzimləyici tələblərini birbaşa pozan hallar — aşkar edildikdən sonra maksimum 24 saat ərzində Bankın təyin edilmiş əlaqə şəxsinə yazılı şəkildə bildirilməlidir. Bildiriş bunları əhatə etməlidir:

- Tapıntının mahiyyəti və təsirlənən tənzimləyici tələb
- Bankın mövcud vəziyyəti
- Potensial tənzimləyici risk
- Tövsiyə olunan dərhal tədbirlər

5. Sertifikasiya Tələbləri

Təchizatçı audit komandası üçün sertifikatlı kadr təmin etməlidir. Sertifikatlar tender təklifi sənədləri ilə birlikdə təqdim edilməlidir. Sertifikatlar təqdimetmə anında qüvvədə olmalıdır.

5.1 Audit Komandası

Rol	Tələb Olunan Sertifikat(lar)	Qeydlər

Aparıcı Auditor	ISO 27001 Lead Auditor (məcburi) CISA (üstünlük verilir); CISM və ya CISSP (üstünlük verilir) CRISC (üstünlük verilir); ISO 27005 sertifikatı (üstünlük verilir).	ARMB tənzimləyici tələbləri üzrə praktiki biliyə malik olmalıdır (2 nəfər)
Tənzimləyici Mütəxəssis		Azərbaycan bank tənzimləyici mühiti üzrə əvvəlki təcrübəni nümayiş etdirməlidir
İT Risk Mütəxəssisi		Risk qiymətləndirməsi və nəzarət çərçivəsi üzrə praktiki təcrübə

Tələb olunan sertifikat nüsxələrini əhatə etməyən təkliflər uyğunsuz sayıla bilər.

6. Təchizatçıya Uyğunluq Tələbi

- Azərbaycan Respublikasında qanuni qeydiyyatdan keçmiş hüquqi şəxs
- Maliyyə qurumları və ya tənzimlənən şirkətlər üçün İT/İnformasiya Təhlükəsizliyi auditlərini keçirməkdə minimum 3 (üç) il sübut edilmiş təcrübə
- Azərbaycan bank sektoru tənzimləyici tələbləri üzrə əvvəlki audit təcrübəsi üstünlük verilir
- Auditor müstəqil olmalı, Bankla maraqların toqquşması olmamalıdır
- Audit fəaliyyəti Azərbaycan Respublikası ərazisindən həyata keçirilməlidir
- Təchizatçı istənilən əhatə məlumatı almadan əvvəl Bankın standart Məxfilik Müqaviləsini (NDA) imzalamalıdır

7. Tələb Olunan Təklif Məzmunu

7.1 Texniki Təklif

- Şirkət profili: hüquqi qeydiyyat, fəaliyyət illəri, komanda həcmi, əsas müştərilər (maliyyə sektoru)
- Təklif olunan komanda: hər təyin edilmiş fərd üçün ad, rol və sertifikatlar
- Sertifikat nüsxələri: Bölmə 5.2-də sadalanan bütün tələb olunan sertifikatlar
- Audit metodologiyası: ARMB 14/2 tələbləri çərçivəsində tətbiq ediləcək yanaşmanın ətraflı təsviri
- İstinadlar: ən azı 3 əvvəlki müştəri üçün əlaqə məlumatı (maliyyə sektoru istinadları üstünlük verilir)
- Layihə cədvəli: başlanğıc/bitmə tarixlərini və əsas mərhələləri göstərən qrafik

7.2 Kommersiya Təklifi

- Audit xidməti üçün ümumi qiymət təklifi
- Ödəniş şərtləri: audit tamamlanması və hesabatın qəbulundan sonra
- Təkliflərin təqdim olunması qaydası:

Kommersiya təkliflərinizi aşağıdakı ünvana təqdim etməyiniz xahiş olunur:

Həsən bəy Zərdabi küç. 81K

Yelo Bank, Baş Ofis
Ləman Qurbanova
Əlaqə nömrəsi: +994 50 627 53 00

Kommersiya təklifi qapalı zərfdə təqdim edilməli və zərf dörd tərəfdən möhürlənmiş olmalıdır. Zərfin üzərində aşağıdakı mövzu mütləq qeyd edilməlidir:
"ARMB Tələblərinə Uyğunluq Auditi"

Tenderlə əlaqədar bütün suallar və izahatlar yazılı formada olmalı və Sifarişçinin nümayəndəsinin E-poçt ünvanına İcra Qrafiki çərçivəsində göndərilməlidir.
YELO BANK ASC
Kimə: Leyla Abbasova
E-poçt: leyla.abbasova@yelo.az
+994(55) 213 70 12

8. Təklif Qiymətləndirmə Meyarı

Meyar	Çəki
Kommersiya təklifi (xidmətin qiyməti)	100 %

- Təkliflər yalnız kommersiya təklifi, xidmətin qiyməti əsasında qiymətləndiriləcəkdir.
- 5-ci bəndə qeyd olunan sertifikat nüsxələrini əhatə etməyən təkliflər uyğunsuz sayılacaq
- ARMB 14/2 “Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər”in 3.7.-ci bəndinə uyğun olaraq audit keçirəcək mütəxəsislərin ən az 3 il sübut edilmiş təcrübələrinin olması mütləqdir.

9. İstifadə Olunan Anlayışlar

Termin	Tərif
ARMB	Azərbaycan Respublikasının Mərkəzi Bankı
ARMB 14/2	ARMB İdarə Heyətinin 28 mart 2024-cü il tarixli, 14/2 nömrəli Qərarı ilə təsdiq edilmiş İnformasiya Təhlükəsizliyinə dair Tələblər
Uyğunluq Auditi	Bankın tənzimləyici tələblərə uyğunluğunu müstəqil şəkildə qiymətləndirən proses
Uyğunsuzluq Analizi	Mövcud vəziyyət ilə tələb olunan vəziyyət arasındakı fərqlərin müəyyənləşdirilməsi
Uyğunluq Matrisi	Hər tənzimləyici tələb üzrə uyğunluq statusunu əks etdirən cədvəl
ISO 27001 Lead Auditor	ISO 27001 standartı üzrə audit keçirmək səlahiyyətinə malik sertifikatlı mütəxəssis
CISA	Certified Information Systems Auditor — ISACA tərəfindən verilən İT audit sertifikatı
CISM	Certified Information Security Manager — ISACA tərəfindən verilən İT təhlükəsizlik idarəetmə sertifikatı

CISSP	Certified Information Systems Security Professional — ISC2 tərəfindən verilən sertifikat
CRISC	Certified in Risk and Information Systems Control — ISACA tərəfindən verilən risk idarəetmə sertifikatı
NDA	Məxfilik Müqaviləsi (Non-Disclosure Agreement)
BCP	Fəaliyyətin Davamlılığı Planı (Business Continuity Plan)
DRP	Fəlakətin Bərpası Planı (Disaster Recovery Plan)
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework