№ 2/2025 səh.115-121

UOT 336.77.01
DOI 10.30546/JIECM.2025.2.2056

RƏQƏMSAL BANKÇILIQ MÜHİTİNDƏ RİSKLƏRİN İDARƏ EDİLMƏSİ VƏ AUDİT MEXANİZMLƏRİNİN İNKİŞAFI

Kənan Nüsrət oğlu Atayev

Bakı Biznes Universiteti

kenan.atayev.1998@mail.ru

Xülasə: *Məqalədə rəqəmsal bankçılıq mühitində risklərin təsnifatı, onların idarə olunması metodları və audit mexanizmlərinin inkişaf istiqamətləri araşdırılmışdır. Ənənəvi bank riskləri (kredit, bazar, likvidlik, əməliyyat, strateji, nüfuz və layihə riskləri) ilə yanaşı, rəqəmsallaşma dövründə meydana çıxan yeni risklər – kibertəhlükə, texnoloji asılılıq, rəqəmsal reputasiya və hüquqi risklər sistemli şəkildə təhlil olunmuşdur. Bank sektorunda risklərin idarə edilməsində ənənəvi yanaşmalar (kapital adekvatlığı, diversifikasiya, sığorta və limitlər) ilə yanaşı, müasir texnologiyalardan – süni intellekt əsaslı monitorinq sistemləri, RegTech həlləri və fasiləsiz audit mexanizmlərindən istifadənin əhəmiyyəti göstərilmişdir. Araşdırmada həmçinin İT auditi və kiber risklərin auditi istiqamətində beynəlxalq təcrübələr müqayisə edilmiş və Azərbaycan bank sektoru üçün tətbiq imkanları qiymətləndirilmişdir. Nəticələr göstərir ki, bankların dayanıqlı inkişafı və maliyyə sabitliyi üçün müasir risk idarəetmə yanaşmalarının tətbiqi, audit funksiyalarının gücləndirilməsi və kibertəhlükəsizlik tədbirlərinin genişləndirilməsi vacibdir.*

Açar sözlər: *rəqəmsal bankçılıq, risklərin idarə edilməsi, kibertəhlükəsizlik, audit mexanizmləri, informasiya texnologiyaları auditi.*

Giriş. Risk anlayışı müxtəlif dillərdə zərər, təhlükə, istənilməyən nəticələr ilə üzləşmə ehtimalı mənasına gəlir. Risk – ehtimal olunan və ya gözlənilməz hadisələrin baş verməsi nəticəsində yaranan xərclərin (zərərin) bankın kapitalına mənfi təsir göstərməsi ehtimalıdır [5]. Banklar bəzən fəaliyyətləri ilə bağlı bir sıra qərarlar almazdan öncə mövcud olan qeyri-müəyyənliyi aradan qaldırmaq üçün müxtəlif versiyalar hazırlayırlar. Lakin bu versiyalar ilə gerçəklərin üstüstə düşməməsi risk amilini ortaya çıxarır [4]. Kommersiya bankları fəaliyyətləri boyunca çoxsaylı risklərlə üzləşməsinə baxmayaraq, etibarlılıq və təhlükəsizlik kimi xüsusiyyətləri qorumalıdırlar. Bu səbəbdən risklərin səmərəli idarə olunması strateji bank menecmentinin əsas funksiyalarından birinə çevrilmişdir. Azərbaycanda bank sektorunda risk menecmenti məsələləri ümumdövlət əhəmiyyətli bir sahə kimi qiymətləndirilir. Bankların uzunmüddətli dayanıqlılığı, davamlı inkişafı, stabil gəlirliliyi və qanunvericiliyə uyğun fəaliyyət göstərməsi üçün korporativ risk idarəetmə sistemi vacibdir.

Son illərdə rəqəmsal texnologiyaların sürətli tətbiqi bankçılıq mühitində risk mənzərəsini əhəmiyyətli dərəcədə dəyişmişdir. Rəqəmsallaşma nəticəsində banklar ənənəvi risklərlə yanaşı, kiber təhlükəsizlik, texnoloji asılılıq, reputasiya kimi yeni risklərlə üzləşirlər. Bu isə risklərin idarə edilməsində müasir yanaşmaların tətbiqini və eyni zamanda informasiya texnologiyaları (İT) auditinin rolunun artmasını şərtləndirir.

Mövzunun aktuallığı. Müasir dövrdə bank sektorunda rəqəmsallaşma prosesi sürətlə inkişaf edir və bu proses yeni risklərin meydana çıxmasına səbəb olur. Ənənəvi risklərlə yanaşı, kiber təhlükəsizlik, texnoloji asılılıq və rəqəmsal reputasiya kimi risklər artıq bankların fəaliyyətində prioritet mövqeyə çıxmışdır. Azərbaycan bank sektorunda da rəqəmsal transformasiya dövlətin maliyyə sabitliyi və dayanıqlı iqtisadi inkişaf strategiyasının mühüm tərkib hissəsi hesab olunur. Bu baxımdan, risklərin idarə olunması mexanizmlərinin təkmilləşdirilməsi və müasir audit yanaşmalarının tətbiqi bankların uzunmüddətli etibarlılığını təmin etmək baxımından xüsusi aktuallıq kəsb edir.

Tədqiqatın məqsədi. Tədqiqatın əsas məqsədi rəqəmsal bankçılıq mühitində yaranan ənənəvi və müasir risklərin təsnifatını aparmaq, bu risklərin idarə olunması üçün tətbiq olunan metod və mexanizmləri təhlil etmək, həmçinin müasir dövrdə audit funksiyasının inkişaf istiqamətlərini müəyyənləşdirməkdir. Bununla yanaşı, Azərbaycan bank sektorunda risk menecmenti və audit sistemlərinin beynəlxalq təcrübə fonunda qiymətləndirilməsi və inkişaf perspektivlərinin müəyyənləşdirilməsi də məqsəd kimi qarşıya qoyulmuşdur.

Tədqiqat obyekti. Tədqiqatın obyekti Azərbaycan Respublikasının kommersiya banklarının risk menecmenti və audit mexanizmləridir. Buraya bankların daxili risk idarəetmə strukturları, tətbiq olunan ənənəvi və müasir risklərin idarə olunması alətləri, daxili və xarici audit fəaliyyətləri, İT auditi, fasiləsiz audit və kiber risklərin auditi daxildir.

Tədqiqat metodları. Tədqiqatda elmi-analitik, müqayisəli təhlil, sistemli yanaşma və statistik metodlardan istifadə olunmuşdur. Analitik metod vasitəsilə mövcud risklərin təsnifatı aparılmış, müqayisəli yanaşma əsasında ənənəvi və müasir risk idarəetmə mexanizmləri dəyərləndirilmişdir. Statistik məlumatların təhlili ilə Azərbaycan bank sektorunda risklərin dinamikası izlənilmiş, sistemli yanaşma ilə isə risklərin idarə olunması və audit funksiyalarının qarşılıqlı əlaqəsi öyrənilmişdir.

MATERİALLAR VƏ MÜZAKİRƏLƏR

Ənənəvi bank risklərinin təsnifatı və idarə olunması. Ənənəvi bank riskləri dedikdə kommersiya banklarının fəaliyyətində ən çox rast gəlinən maliyyə və qeyri-maliyyə riskləri nəzərdə tutulur. Bank riski, müəyyən maliyyə əməliyyatlarının həyata keçirilməsi nəticəsində bankın öz resurslarının bir hissəsini itirməsini, gəlirlərin əldə edilməməsini və ya əlavə xərclərin yaranması ehtimalını (təhlükəsini) özündə ehtiva edir [3, s.8]. Azərbaycan bank sektorunda qüvvədə olan tənzimləyici çərçivəyə əsasən banklar fəaliyyətləri zamanı qarşılaşdıqları 7 əsas risk növünü müəyyən edib idarə etməlidirlər. Bu risklər aşağıdakılardır:

Kredit riski. Borcalanın bank qarşısında kredit öhdəliklərini vaxtında və tam icra etməməsi səbəbindən bankın zərərə məruz qalması ehtimalıdır. Bu risk, həm real sektorda, həm də maliyyə sektorunda fəaliyyət göstərən subyektlərdə yer ala bilir. Kredit riski, real sektora aid olan müəssisələri tərəfindən müştərilərə məhsul və xidmətlərin əmtəə (kommersiya) krediti şərtlərinə uyğun olaraq təklif etməsi zamanı meydana gəlir. Bu riskin təzahür formaları satılan məhsullar üçün ödənişlərin vaxtında edilməməsi və ya da ümumiyyətlə həyata keçirilməməsi, eləcə də vaxtı ötmüş debitor borclarının inkassasiya olunmasına sərf edilən xərclərin artması kimi müşahidə oluna bilər [1, s.89-90].

Bazar riski. Faiz dərəcələri, valyuta məzənnələri, qiymətli kağızların dəyəri və əmtəə qiymətlərindəki əlverişsiz dəyişikliklər nəticəsində bankın maliyyə vəziyyətinə mənfi təsir göstərə biləcək itki riskidir. Bazar riski çərçivəsində faiz dərəcəsi riski, valyuta riski, kapital (qiymətli kağızlar) riski və əmtəə riski kimi alt kateqoriyalar mövcuddur.

Likvidlik riski. Bankın öz öhdəliklərini (o cümlədən, depozitlərin geri çəkilməsi tələblərini) vaxtında və effektiv şəkildə yerinə yetirə bilməməsi nəticəsində yaranan riskdir. Likvidlik riskləri dedikdə iki birbirinə tamamilə zidd, fərqli risk növləri başa düşülür: 1. Aktivlərin likvidlik riski mövcud maliyyə aktivinin satışı zamanı yaranmağa başlayır. Bu risk növü dəyərin əhəmiyyətli dərəcədə azalmasına gedilmədən, aktivin tez bir zamanda satışının mümkünsüzlüyü deməkdir. Likvidliyin əsas ölçüsü alış və satış qiyməti arasındakı bazar fərqidir. 2.Fondlaşdırmanın (vəsaitlərin cəlb edilməsinin) likvidlik riski əlverişsiz şəraitdə şirkətin öhdəliklərini yerinə yetirmək, kontragentlərin tələblərini pul resursları ilə ödəmək qabiliyyətinin azalması ilə əlaqədardır, yəni bu risk növünü ödəmə qabiliyyəti riski də adlandırmaq olar [1, s.233-234] .

Əməliyyat riski. Daxili proseslərin qeyri-kafi olması, işçilərin səhvləri, informasiya sistemlərində nasazlıqlar və ya xarici hadisələr (məs., kənar fırıldaqçılıq, təbii fəlakətlər) ucbatından bankın zərərə uğrama ehtimalıdır. Əməliyyat riskinin tərkibinə İT riski (texnologiya infrastrukturunda problem riskləri), hüquqi risk, komplayens riski (qanunvericiliyə və tənzimləyici tələblərə uyğunluğun pozulması riski) və digər alt risklər daxildir.

Strateji risk. Bankın strateji hədəflərinin düzgün müəyyən edilməməsi və ya icrada yanlış qərarlar nəticəsində maliyyə itkiləri ilə üzləşmə riskidir.

Nüfuz riski. Banka qarşı ictimai etimadın azalması, mənfi rəy və imicin formalaşması səbəbilə müştərilərin və tərəfdaşların bankla işgüzar əlaqələrini məhdudlaşdırmasına yol açа biləcək riskdir. (Nüfuz riskinin reallaşması, məsələn, bank haqqında kütləvi informasiya vasitələrində və ya sosial şəbəkələrdə mənfi xəbərlərin yayılması nəticəsində mümkündür.)

Layihə riski. Bankın maliyyələşdirdiyi və ya həyata keçirdiyi layihələrin gedişində yol verilən səhvlər, düzgün planlaşdırmama və ya kənar maneələr səbəbilə həmin layihənin uğursuzluqla nəticələnməsi riskidir.

Bu ənənəvi risklərin hər birini effektiv idarə etmək üçün banklar müvafiq siyasət və prosedurlar tətbiq edirlər. Risklərin idarə edilməsi prosesi risklərin müəyyənləşdirilməsi, qiymətləndirilməsi, azaldılması (və ya transferi) və davamlı monitorinqi kimi mərhələləri əhatə edir. Bank daxilində risk menecment funksiyası adətən üç müdafiə xətti modeli üzrə qurulur: birinci xəttdə biznes bölmələri risklərin gündəlik idarə olunmasına cavabdehdir, ikinci xəttdə risk menecmenti və komplayens funksiyaları riskləri nəzarətdə saxlayır, üçüncü xəttdə isə müstəqil daxili audit risk idarəetməsinin effektivliyinə nəzarət edir. Mərkəzi Bankın normativ sənədlərində də banklarda risklərin idarə edilməsi sisteminin əsas elementləri sıralanır: risklərin idarə edilməsi strategiyası və risk iştahası, risk idarəetmənin təşkilati strukturu, risk siyasəti (müdafiə xətləri prinsipinə əsasən), risk limitləri, yeni məhsul və xidmətlər üzrə risk qiymətləndirilməsi, konsolidə olunmuş məlumat bazası əsasında risk hesabatlığı və fövqəladə hallara hazırlıq planı kimi komponentlər bu sistemin tərkib hissəsidir.

Rəqəmsal bankçılıq mühitində spesifik risklər. Son dövrlər bank xidmətlərinin rəqəmsallaşması və onlayn kanalların genişlənməsi nəticəsində risklərin xarakteri də dəyişmişdir. Əgər ənənəvi risklər (kredit, likvidlik və s.) uzun müddətdir məlumdursa, rəqəmsal bankçılıq mühitində bir sıra yeni, spesifik risklər meydana çıxır və ya ön plana keçir. Beynəlxalq araşdırmalar göstərir ki, bank rəhbərliyinin demək olar yarısı kibertəhlükəsizliyi artıq ən vacib təhdidlərdən biri kimi görür. Aşağıda rəqəmsal bankçılıq mühitində xüsusilə önəm daşıyan risklər şərh edilmişdir:

1. Kibertəhlükə riski. Bankın informasiya sistemlərinə, şəbəkələrinə və müştəri məlumatlarına yönəlmiş kiber hücumlar (məsələn, haker hücumları, viruslar, dağıdıcı proqramlar) nəticəsində maliyyə itkiləri və ya məlumat sızması baş vermə riskidir. Rəqəmsal dövrdə kibercinayətkarlıq artdığı üçün bu risk banklar üçün ən kritik təhdidlərdən birinə çevrilmişdir. Məsələn, bir sorğuda bank rəhbərliyinin 48%-i kibertəhlükəni ilk üç riskdən biri kimi dəyərləndirmişdir. Kiber risklərin gerçəkləşməsi nümunələrinə müştəri hesablarının onlayn oğurlanması, ödəniş sistemlərinin sındırılması və böyük həcmli müştəri məlumatlarının internetə sızması kimi hallar daxildir.

2. Texnoloji asılılıq riski. Bank infrastrukturunun və əməliyyatlarının texnologiyadan həddən artıq asılı olmasından irəli gələn riskdir. Müasir banklar core-banking sistemləri, onlayn ödəniş platformaları, bulud xidmətləri kimi texnoloji həllərə güvənirlər. Bu sistemlərdən hər hansı birinin nasazlığı və ya əlçatmaz olması (məsələn, serverlərin sıradan çıxması) nəticəsində bankın fəaliyyəti iflic ola bilər, müştərilərə xidmət dayanır və nəticədə maliyyə zərəri ilə yanaşı nüfuza da zərbə dəyir. Eyni zamanda, bankın kritik İT funksiyalarının kənar təchizatçılardan asılı olması (outsourcing) da asılılıq riskini artırır.

3. Rəqəmsal reputasiya riski. Rəqəmsal mühitdə bankın nüfuzuna xələl gəlməsi riski ənənəvi reputasiya riskinin daha sürətli və geniş miqyaslı formasıdır. İnternet və sosial media vasitəsilə müştərilərin mənfi rəyləri, kibertəhlükə insidentləri barədə xəbərlər və ya onlayn xidmətdə fasilələr sürətlə yayıla bilər. Nəticədə bankın imicinə ciddi ziyan dəyir və müştəri etimadı sarsılır. Rəqəmsal transformasiyaya adekvat yatırımlar etməyən və kibertəhlükələrə hazır olmayan təşkilatların məhz kiber və reputasiya risklərinə daha çox açıq olduğu qeyd edilir. Bu baxımdan, banklar reputasiya riskini azaltmaq üçün operativ kommunikasiya strategiyaları, müştəri məlumatlarının qorunması və fasiləsiz xidmət təminatı üzərində çalışmalıdırlar.

4. Hüquqi risklər. Rəqəmsal bankçılıq sahəsində hüquqi risklər əsasən bankın qanunvericiliyin yeni tələblərinə və tənzimləyici normalara uyğunlaşmaması ilə bağlıdır. Məsələn, müştəri məlumatlarının

qorunması haqqında qanunların (məsələn, məlumat məxfiliyi qanunları) pozulması, onlayn ödənişlərdə dələduzluq halları səbəbilə sanksiyalar və cərimələr, eləcə də transsərhəd elektron xidmətlər göstərərkən müxtəlif ölkələrin tələblərinə əməl edilməməsi nəticəsində yarana bilən risklər bu kateqoriyaya aiddir. Banklar rəqəmsal sahədə hüquqi riskləri azaltmaq üçün RegTech həllərdən (tənzimləməyə uyğunluq texnologiyalarından) istifadə etməyə, daxili qaydaları mütəmadi yeniləməyə və hüquqşünasların, uyğunluq mütəxəssislərinin rəyini almağa çalışırlar.

Risklərin idarə olunması metod və mexanizmləri. Risklərin idarə edilməsi banklar üçün stratejik bir məsələdir. Güclü risk idarəçiliyinə malik olan banklar qarşılaşa biləcəkləri bazar, kredit, əməliyyat və digər riskləri ətraflı araşdırır, mümkün böhranlar zamanı ola biləcək itkilərini əvvəlcədən müəyyənləşdirir və bu itkiləri minimuma endirmək üçün tədbirlər görür, götürdükləri riskləri əldə edə biləcəkləri qazancla müqayisə edir və bu riski almağa dəyib-dəymədiyini əvvəlcədən qiymətləndirir [2]. Bank risklərinin idarə edilməsində ənənəvi yanaşmalar uzun illərdir tətbiq olunaraq öz effektivliyini sübut etmiş alətlərdir. Bunların başında bankın kifayət qədər kapital ehtiyatının olmasını təmin edən kapital adekvatlığı normativləri dayanır. Bazel razılaşmalarına əsasən beynəlxalq banklar risklərlə örtülməsi üçün ən azı 8% kapital adekvatlığı əmsalını qorumağa borcludurlar. Azərbaycanda da tənzimləyici qurumlar banklara minimal kapital adekvatlığı tələbləri qoyur ki, bu da gözlənilməz zərər hallarında bankın dayanıqlığını təmin etməyə yönəlib. Ənənəvi risk idarəetməsinin digər vacib üsulu risklərin diversifikasiyasıdır. Diversifikasiya prinsipinə görə bank risklərini azaltmaq üçün aktivlərini və əməliyyatlarını müxtəlif istiqamətlər (müştəri qrupları, sektorlar, valyutalar və s.) üzrə yaymalıdır.

Məsələn, kredit portfelinin diversifikasiyası – kreditlərin müxtəlif sahələrə və müştəri kateqoriyalarına paylanması – bir borcalanın defoltunun bankı iflasa uğratmamasına şərait yaradır. Eynilə, investisiya portfelinin şaxələndirilməsi bazar riskini azaltmaq üçün istifadə edilir. Bunlarla yanaşı, ənənəvi alətlərdən ehtiyat (proviziya) yaradılması, sığortalanma (məsələn, kredit sığortası) və risk limitlərinin tətbiqi (müəyyən əməliyyatlara həd qoyulması) da geniş yayılmışdır.

Rəqəmsal dövrün gətirdiyi yeni risklər qarşısında banklar müasir texnologiyalardan faydalanan innovativ risk idarəetmə metodlarına müraciət edirlər. Bu istiqamətdə ilk növbədə kiber təhlükəsizlik tədbirlərini qeyd etmək lazımdır. Banklar informasiya təhlükəsizliyi çərçivəsində gücləndirilmiş İT təhlükəsizlik infrastrukturunu qurur, şifrələmə, çoxmərhələli identifikasiya, firewall və antivirus sistemləri tətbiq edir, həmçinin 24/7 rejimində fəaliyyət göstərən Təhlükəsizlik Əməliyyat Mərkəzləri (SOC) vasitəsilə şübhəli fəaliyyətləri izləyirlər. Kibertəhlükəsizlik tədbirləri sayəsində banklar kiber hücumların qarşısını almağa və ya insident baş verdikdə zərərləri minimuma endirməyə çalışır.

Digər müasir yanaşma süni intellekt (Sİ) əsaslı monitorinq sistemləridir. Süni intellekt və maşın öyrənməsi alqoritmləri böyük həcmli əməliyyat məlumatlarını real vaxtda təhlil edərək anormal halları (məsələn, dələduzluq tranzaksiyaları, şübhəli əməliyyatlar) aşkarlaya bilir. Məsələn, Risk İdarəetmə Assosiasiyasının 2023-cü il sorğusuna əsasən bankların 84%-i məhz fırıldaqçılığın aşkar edilməsində, 32%-i isə kredit riskinin qiymətləndirilməsində süni intellekt modellərindən istifadə edir. Bundan əlavə, süni intellekt bankların proaktiv risk monitorinqi aparmasına, yəni potensial problemləri öncədən proqnozlaşdırıb tədbir görməsinə imkan verir. Məsələn, bəzi qabaqcıl banklar İT infrastrukturunda nasazlıqları öncədən xəbər verən və sistem fasilələrini minimuma endirən ağıllı monitorinq alətlərini tətbiq edirlər. Nəhayət, son illərdə önə çıxan anlayışlardan biri də RegTech (Regulatory Technology) həlləridir. RegTech bankların tənzimləyici tələblərə uyğynluq proseslərini avtomatlaşdırmasına xidmət edən texnoloji vasitələrdir. Buraya məsələn real vaxt rejimində şübhəli əməliyyatların aşkarlanması üçün AML (antipul yuyulma) proqramları, müştərini tanı (e-KYC) sistemləri, hesabatvermə platformaları və s. daxildir. RegTech tətbiqi sayəsində banklar həm uyğunluq risklərini azaldır, həm də compliance funksiyasının effektivliyini artırırlar. Ümumilikdə, müasir risk idarəetmə yanaşmaları banklara sürətlə dəyişən risk mühitinə adaptasiya olub riskləri daha çevik və dəqiq şəkildə ölçməyə və idarə etməyə imkan verir.

Audit funksiyası: ənənəvi və müasir yanaşmalar. Banklarda audit funksiyası risklərin idarə olunması sisteminin ayrılmaz tərkib hissəsidir. Audit fəaliyyətinin məqsədi bankın maliyyə

hesabatlarının düzgünlüyünü yoxlamaq, əməliyyatların daxili və xarici tələblərə uyğunluğunu qiymətləndirmək və risk idarəetməsinin effektivliyinə nəzarət etməkdən ibarətdir. Audit iki əsas formada həyata keçirilir: daxili audit (bankın öz nəzarət mexanizmi) və xarici audit (müstəqil auditorlar tərəfindən illik maliyyə auditləri). Ənənəvi yanaşmada daxili audit əsasən periodik, yəni müəyyən aralıqlarla (adətən illik) yoxlamalar aparırdı. Adətən audit planına uyğun olaraq bankın müxtəlif sahələrində yoxlamalar həyata keçirilirdi. Klassik audit daha çox mühasibat uçotu, kredit portfeli, əməliyyat uyğunluğu kimi sahələrə fokuslanırdı. Lakin rəqəmsal dövrdə audit funksiyasının da əhatə dairəsi və metodları əhəmiyyətli dərəcədə genişlənmişdir. Aşağıda auditə müasir yanaşmanın üç mühüm aspekti qeyd olunur:

İT auditi. Banklarda informasiya texnologiyaları (İT) auditi daxili audit funksiyasının müasir istiqamətlərindən biridir. İT auditi bankın informasiya sistemlərinin və texnoloji infrastrukturunun etibarlılığını, təhlükəsizliyini və effektivliyini qiymətləndirməyə yönəlir. İT auditorları bankdaxili müxtəlif sistemlər üzrə daxili nəzarət sistemlərinin adekvatlığını yoxlayır, İT sahəsində mövcud riskləri (məsələn, sistem boşluqları, məlumat təhlükəsizliyi açıqları) müəyyən edir və həllinə dair tövsiyələr verir. Məsələn, bir bankın İT audit şöbəsi core banking sisteminin fasiləsiz işləməsini, ehtiyat serverlərin mövcudluğunu, verilənlərin mütəmadi backup olunmasını və informasiya təhlükəsizliyi prosedurlarına əməl olunmasını yoxlaya bilər. İT audit nəticəsində aşkar edilmiş çatışmazlıqların aradan qaldırılması üçün rəhbərliyə hesabat təqdim olunur və bununla bankın texnoloji risklərinin azaldılmasına töhfə verilir.

Fasiləsiz (davamlı) audit. Ənənəvi daxili audit adətən müəyyən intervallarla (məsələn, illik) aparıldığı halda, müasir bankçılıqda fasiləsiz audit konsepsiyası yaranmışdır. Fasiləsiz audit – texnologiyaların köməyi ilə audit prosesinin real vaxt rejimində və ardıcıl şəkildə icra edilməsidir. Belə audit modelində daxili auditorlar bank əməliyyatlarını fasiləsiz monitorinq edərək potensial uyğunsuzluq və riskləri anında müəyyən etməyə çalışırlar. Araşdırmalara görə, daxili auditin əsas vəzifəsi risklərin idarə edilməsinin məqbul çərçivədə həyata keçirilməsinə təminat verməkdirsə, fasiləsiz audit bu təminatı daha çevik və tam şəkildə həyata keçirməyə imkan verir. Fasiləsiz audit sistemi əhəmiyyətli risk göstəricilərini real vaxtda izləyən kompleks analitik mexanizmdir və daxili nəzarət sisteminin daimi təftişini həyata keçirir. Məsələn, fasiləsiz audit vasitəsilə gün ərzində minlərlə tranzaksiyanın avtomatik analizi aparılıb dərhal qaydalardan kənara çıxma halları barədə xəbərdarlıq yaradılır. Bu yanaşma sayəsində ənənəvi audit dövrünü gözləmədən riskli vəziyyətlər vaxtında aşkarlanır və operativ tədbir görülə bilir. Fasiləsiz auditin tətbiqi üçün banklar data analitikası alətlərindən, xüsusi audit proqram təminatından və hətta süni intellektin monitorinq gücündən yararlanırlar.

Kiber risklərin auditi. Rəqəmsallaşma dövründə banklarda kiber risklərin auditi ayrıca əhəmiyyət kəsb edir. Burada məqsəd bankın kibertəhlükəsizlik sahəsində qəbul etdiyi tədbirlərin və prosedurların effektivliyini müstəqil qiymətləndirməkdir. İT auditinin tərkib hissəsi kimi, kiber risk auditi çərçivəsində bankın şəbəkə mühitinin zəiflik testləri (penetrasiya testləri) aparılır, informasiya təhlükəsizliyi üzrə siyasət və qaydaların tətbiqinə riayət olunub-olunmaması yoxlanılır, insident idarəetmə prosedurları gözdən keçirilir. Mərkəzi Bank və digər tənzimləyicilər də banklarda kibertəhlükəsizlik auditlərinin aparılmasını təşviq edir. Məsələn, bir çox banklara hər il xarici mütəxəssislər tərəfindən penetrasiya testləri keçirilməsi, ISO 27001 informasiya təhlükəsizliyi standartına uyğunluğun auditi və s. tövsiyə olunur. Kiber risklərin auditi nəticəsində hazırlanmış hesabatlar bank rəhbərliyinə informasiya təhlükəsizliyinin vəziyyəti barədə obyektiv təsəvvür yaradır və boşluqların aradan qaldırılması üçün fəaliyyət planı tərtib etməyə imkan verir.

Tədqiqatın elmi yeniliyi. Tədqiqatda rəqəmsal bankçılıq mühitində ənənəvi və müasir risklərin paralel şəkildə təsnifatı aparılmış, onların idarə edilməsində istifadə olunan mexanizmlər müqayisəli şəkildə təhlil edilmişdir. Elmi yenilik ondan ibarətdir ki, Azərbaycan bank sektoru kontekstində risklərin idarə edilməsi ilə audit funksiyalarının inteqrasiyası ilk dəfə sistemli yanaşma əsasında qiymətləndirilmişdir. Bununla yanaşı, İT auditi, fasiləsiz audit və kiber risklərin auditi kimi müasir

anlayışların yerli bank praktikası üçün tətbiq imkanları araşdırılmış və beynəlxalq təcrübə fonunda onların uyğunlaşdırılması yolları müəyyənləşdirilmişdir.

Tədqiqatın tətbiqi əhəmiyyəti. Tədqiqat nəticələri kommersiya bankları, tənzimləyici qurumlar və audit təşkilatları üçün praktik əhəmiyyət kəsb edir. Məqalədə təqdim olunan yanaşmalar bankların risk idarəetmə siyasətlərinin təkmilləşdirilməsinə, audit xidmətlərinin müasir tələblərə uyğunlaşdırılmasına və kiber risklərin azaldılmasına dair konkret tövsiyələr verir. Həmçinin, RegTech və süni intellekt əsaslı monitorinq sistemlərinin tətbiqi ilə bağlı irəli sürülən təkliflər yerli bankların beynəlxalq maliyyə sisteminə inteqrasiyasını asanlaşdırmağa xidmət edə bilər.

Tədqiqat işinin iqtisadi səmərəsi. Tədqiqatın nəticələri bank sektorunda risklərin daha effektiv idarə olunmasına və audit funksiyalarının gücləndirilməsinə imkan verərək maliyyə sabitliyinin möhkəmlənməsinə töhfə verir. Müasir risk idarəetmə və audit mexanizmlərinin tətbiqi nəticəsində potensial maliyyə itkilərinin qarşısı alınacaq, əməliyyat xərcləri azalacaq və bankların gəlirlilik səviyyəsi yüksələcəkdir. İqtisadi səmərənin digər mühüm tərəfi isə müştəri etimadının artması və rəqəmsal xidmətlərə daha geniş cəlbetmə imkanlarının yaranmasıdır ki, bu da bütövlükdə ölkənin maliyyə bazarının dayanıqlığını gücləndirəcəkdir.

Nəticə. Azərbaycan bank sektorunda risklərin idarə olunması sahəsi davamlı inkişaf etdirilməli olan önəmli bir istiqamətdir. Aparılan təhlil göstərir ki, ənənəvi risk növlərinin effektiv idarə edilməsi üçün ölkəmizdə möhkəm normativ baza mövcuddur və banklar kredit, bazar, likvidlik kimi riskləri idarə etməkdə müəyyən təcrübəyə malikdir. Lakin rəqəmsal bankçılığın sürətli inkişafı yeni risklərin meydana çıxmasına gətirib çıxarmışdır ki, bu risklərə qarşı mübarizədə mütləq şəkildə müasir yanaşmalar tətbiq olunmalıdır. Banklar kibertəhlükəsizlik imkanlarını gücləndirməli, informasiya sistemlərinə davamlı investisiya etməli və kiber insidentlərin qarşısının alınması üçün qabaqlayıcı tədbirlər görməlidir. Eyni zamanda, süni intellekt və data analitikası kimi alətlərdən istifadənin genişləndirilməsi risklərin daha tez aşkarlanması və qərarların məlumatlara əsaslanaraq verilməsinə töhfə verəcəkdir. Tənzimləyici orqanlar da RegTech həllərinin tətbiqini təşviq edərək banklara uyğunluq proseslərini avtomatlaşdırmaqda dəstək ola bilərlər.

Bundan əlavə, audit funksiyasının təkmilləşdirilməsi xüsusi diqqət tələb edir. Banklarda İT auditi sahəsində kadr potensialı artırılmalı, daxili auditorlar müasir İT riskləri barədə mütəmadi təlimlər almalıdırlar. Daxili audit xidmətləri fasiləsiz audit prinsiplərini mərhələli şəkildə öz fəaliyyətlərinə inteqrasiya etməlidirlər ki, hər hansı bir riskli proses dərhal nəzarətə götürülə bilsin. Kibertəhlükələrin auditində beynəlxalq standartlardan (məsələn, ISO 27001) və çərçivələrdən faydalanmaq, eləcə də müstəqil kibertəhlükəsizlik auditlərinin keçirilməsini təmin etmək vacibdir. Nəticə etibarilə, banklarda risk menecmenti və audit funksiyalarının gücləndirilməsi maliyyə sisteminin dayanıqlığını artıracaq, potensial itkilərin və böhran vəziyyətlərinin qarşısını alacaqdır. Bu istiqamətdə yerli təcrübənin zənginləşdirilməsi üçün həm beynəlxalq qabaqcıl təcrübələrdən yararlanmaq, həm də yerli tədqiqat və inkişaf fəaliyyətlərini stimullaşdırmaq tövsiyə olunur.

ƏDƏBİYYAT

1. Aşurbəyli N. “Maliyyə risklərinin idarə edilməsi”. Bakı: (2024), səh: 89-234
2. Alicanoğlu C. “Bankalarda risk yönetimi ve Türk bankacılık sektörü üzerine bir araştırma”. 2018
3. Məmmədov İ. “Banklarda risk menecmenti”. Bakı: (2021), səh: 8
4. Məmmədov Z.F., İbrahimov Z.H. “Pul,kredit,banklar”. Bakı: (2009)
5. Banklarda risklərin idarə olunması haqqında qaydalar: https://www.cbar.az

№ 2/2025 səh.115-121

УДК 336.77.01

УПРАВЛЕНИЕ РИСКАМИ И РАЗВИТИЕ МЕХАНИЗМОВ АУДИТА В СРЕДЕ ЦИФРОВОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Кенан Нусрат оглы Атаев
Бакинский Бизнес Университет
Баку, Азербайджан
kenan.ataev.1998@mail.ru

Резюме: *В статье рассматриваются классификация рисков в среде цифрового банкинга, методы управления ими и направления развития механизмов аудита. Наряду с традиционными банковскими рисками (кредитным, рыночным, риском ликвидности, операционным, стратегическим, репутационным и проектным) системно анализируются новые риски, возникшие в эпоху цифровизации: киберриск, технологическая зависимость, цифровая репутация и юридические риски. Наряду с традиционными подходами к управлению рисками в банковском секторе (достаточность капитала, диверсификация, страхование, лимиты) показана важность использования современных технологий – систем мониторинга на основе искусственного интеллекта, RegTech-решений и механизмов непрерывного аудита. В исследовании также сравниваются международные практики в области ИТ-аудита и аудита киберрисков, оцениваются возможности их применения в банковском секторе Азербайджана. Результаты показывают, что для устойчивого развития банков и финансовой стабильности важно применять современные подходы к управлению рисками, усиливать аудиторские функции и расширять меры кибербезопасности.*

Ключевые слова: *цифровой банкинг, управление рисками, кибербезопасность, механизмы аудита, аудит информационных технологий.*

UDC 336.77.01

RISK MANAGEMENT AND DEVELOPMENT OF AUDIT MECHANISMS IN THE DIGITAL BANKING ENVIRONMENT

Kenan Nusrat oglu Atayev
Baku Business University
kenan.atayev.1998@mail.ru

Summary: *The article examines the classification of risks in the digital banking environment, methods for their management, and the development directions of audit mechanisms. Along with traditional banking risks (credit, market, liquidity, operational, strategic, reputation, and project risks), new risks that have emerged in the era of digitalization – cyber risk, technological dependence, digital reputation, and legal risks – are systematically analyzed. Along with traditional approaches to risk management in the banking sector (capital adequacy, diversification, insurance, and limits), the importance of using modern technologies – artificial intelligence-based monitoring systems, RegTech solutions, and continuous audit mechanisms – is shown. The study also compares international practices in IT audit and cyber risk audit and assesses their application possibilities for the Azerbaijani banking sector. The results show that for the sustainable development of banks and financial stability, it is important to apply modern risk management approaches, strengthen audit functions, and expand cybersecurity measures.*

Keywords: *digital banking, risk management, cybersecurity, audit mechanisms, information technology audit.*

Redaksiyaya daxilolma: 02.08.2025
Çapa qəbul olunma: 15.11.2025