ЗАТВЕРДЖЕНО
Рішенням Наглядової ради
АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»
Протокол від 06.03.2025 р. № 14

ПОГОДЖЕНО
Рішенням Правління
АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»
Протокол від 03.03.2025 р. № 17

ПОЛОЖЕННЯ ПРО УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ БАНКУ ТА БАНКІВСЬКОЇ ГРУПИ АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

Зареєстровано в реєстрі
внутрішніх нормативних документів
АТ «БАНК «УКРАЇНСЬКИЙ
КАПІТАЛ»
№ 1909

м. Київ - 2025

ЗМІСТ

ГЛОСАРІЙ

Аутсорсер	організація будь-якої форми власності, фізична особа - підприємець або особа, яка провадить незалежну професійну діяльність, обрана банком для виконання на умовах аутсорсингу окремих робіт/функцій банку
Аутсорсинг	передавання функцій Банку на виконання аутсорсеру на договірній та регулярній основі з метою оптимізації витрат і процесів у Банку.
Банк	АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ».
банківська група (національна)	група юридичних осіб, які мають спільного контролера, складається з двох або більше українських фінансових установ та/або компаній, для яких надання банківських послуг є переважним видом діяльності
Бізнес-процес	сукупність взаємопов'язаних або взаємодіючих видів діяльності, спрямованих на створення певного продукту або послуги
Відділення	Відокремлений підрозділ Банку, який не має статусу юридичної особи, здійснює операції від імені Банку в межах наданих дозволів, те не має окремого балансу.
Відповідальна особа Банківської Групи (Банк)	Банк, який має забезпечити виконання вимог, установлених Національним банком України до Банківської Групи, та погодити її з Національним банком України – АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»
Ризик інформаційної безпеки	імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик.
Ризик інформаційно комунікаційних технологій	імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок несправності або невідповідності інформаційно-комунікаційних технологій бізнес-потребам банку, що може призвести до порушення їх сталого функціонування, або недоліків в організації управління такими технологіями
Інформаційна система щодо управління ризиками	сукупність технічних засобів, методів і процедур, що забезпечують реєстрацію, зберігання, оброблення, моніторинг і своєчасне формування достовірної інформації для звітування (інформування), аналізу та прийняття своєчасних та адекватних управлінських рішень щодо управління ризиками.
Ініціатор	Колегіальний орган / структурний підрозділ / працівник Банку, які відповідно до цього Положення мають право ініціювати/виступити з ініціативою щодо створення нового/ вдосконалення/ зміни існуючого продукту/процесу/послуги.
Капітал на покриття операційного ризику	–кількісна оцінка операційного ризику, яка полягає у розрахунку величини капіталу, що постійно перебуває під ризиком і відтак може бути втрачений навіть під час звичайної діяльності.
Ключовий індикатор ризику (Key Risk Indicators - KRI)	показник, який динамічно змінюється в часі та відображає зміну характеру операційного ризику. KRI використовується банком для раннього виявлення негативних тенденцій/явищ, пов'язаних з підвищенням операційного ризику, що притаманні процесам. дозволяє слідкувати за рівнем операційного ризику у визначеному індикатором процесі.

Новий банківський продукт	1) новий вид діяльності або новий вид фінансових послуг, визначених статтею 47 Закону України “Про банки і банківську діяльність” та статтею 4 Закону України “Про фінансові послуги та фінансові компанії”; 2) вихід на новий ринок з наявними видами діяльності або видами фінансових послуг; 3) унесення змін до наявних видів діяльності або видів фінансових послуг, що вимагають змін ІТ-ресурсів та/або процедур, внутрішніх Банківських документів, порядку взаємодії працівників (підрозділів) Банку, необхідних для їх реалізації та супроводження; 4) унесення істотних змін до умов надання послуг, включаючи цінові.
Операційний ризик	імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик уключає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик
Передавання ризику	передавання Банком своєї відповідальності за ризик іншим особам за винагороду зі збереженням наявного рівня ризику.
Пом'якшення ризиків	комплекс заходів, спрямованих на зменшення ймовірності виникнення ризику та/або зменшення впливу ризику на результати діяльності Банку
Прийняття ризиків	утримання ризиків на рівні, що перебуває в межах визначеної Банком схильності до ризиків (ризик-апетиту) та не створює загрози для інтересів вкладників, інших кредиторів, власників Банку та фінансової стійкості Банку.
Подія операційного ризику	подія, що настає в результаті невідповідного чи помилкового перебігу внутрішніх процесів та функціонування систем, невідповідних чи помилкових дій/бездіяльності людей, або втрат внаслідок дії зовнішніх факторів.
Підрозділ	структурний/відокремлений підрозділ Банку
Ризик-апетит до операційного ризику (схильність до ризику)	сукупна величина операційного ризику, визначена наперед та в межах допустимого рівня ризику, щодо якого Банк прийняв рішення про доцільність/необхідність його утримання з метою досягнення його стратегічних цілей та виконання бізнес-плану.
Ризик-координатор	керівник/призначені працівники підрозділів Банку **першої лінії** захисту (бізнес-підрозділи та підрозділи підтримки Банку), що є відповідальними за внутрішній контроль ризиків, які виникають у сфері їх відповідальності. Підрозділи першої лінії захисту є власниками таких ризиків та відповідають за виявлення та оцінювання ризиків, ужиття управлінських заходів та звітування щодо таких ризиків. Керівники учасників Банківської групи або особи призначені відповідальними за управління ризиками учасника БГ
Стрес-сценарій	модель можливого розвитку подій (обставин) унаслідок впливу різних факторів ризиків, виникнення яких може завдати шкоди фінансовому стану та/або ліквідності Банку.
Стрес тестування	метод вимірювання ризику, що дає змогу оцінити потенційні несприятливі результати впливу ризиків як величину збитків, що можуть стати наслідком шокових змін різних факторів ризиків (курсів іноземних валют, процентних ставок та/або інших факторів), які відповідають виключним (екстремальним), але ймовірним подіям

Уникнення ризику	відмова від здійснення певних операцій або припинення ділових відносин, які наражають банк на ризик
Система управління операційним ризиком	сукупність належним чином задокументованих і затверджених політики, методик і процедур управління операційним ризиком, які визначають порядок дій, спрямованих на здійснення систематичного процесу виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення операційних ризиків на всіх організаційних рівнях.
Юридичний ризик	імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок неочікуваного застосування норм законодавства через можливість їх неоднозначного тлумачення або унаслідок визнання недійсними умов договору у зв'язку з їх невідповідністю вимогам законодавства України

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про управління операційним ризиком банку та банківської групи АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» (далі – Положення) є внутрішнім нормативним документом АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» (далі – Банк), що регламентує процес управління операційним ризиком, ідентифікації, оцінки, моніторингу та контролю за операційними ризиками у Банку та основні принципи та порядок управління операційним ризиком у Банківської Групи (далі-БГ), основні принципи взаємодії між учасниками Банківської Групи з питань здійснення управління операційним ризиком.

1.2. Гранична вартість операційного ризику визначається **на рівні 3000 грн**. (Три тисячі гривень), сума нижче якої, як правило, не застосовується процедура реагування на ризик.

Розрахунок рівня операційного ризику для виміру матеріальності очікуваних та ймовірних втрат/ відображає шкалу впливу яка виражена загальною сумою фінансових втрат протягом одного року:

Бали рівня ризику	Фінансовий вплив/очікувані втрати //грн. або екв. в іноземній валюті/
5	Сума, що характеризує безпосередній ризик для життєздатності Банку, у разі, якщо є обґрунтовані підстави для віднесення Банку до категорії проблемних, неплатоспроможних або ліквідації.
4	більше 150 000
3	від 50 000 до 150 000 (включно)
2	від 25 000 до 50 000 (включно)
1	3000 до 25 000 (включно)

1.3. Система управління операційним ризиком інтегрується в загальну систему управління ризиками Банку.

1.4. Система управління операційним ризиком носить децентралізований характер, тобто в процес управління операційним ризиком задіяні всі підрозділи Банку і всі його працівники.

1.5. Необхідність управління операційним ризиком визначається значним розміром можливих втрат Банку, пов'язаних з реалізацією подій операційного ризику, що створює загрозу фінансовій стабільності Банку, його іміджу і репутації.

1.6. Це Положення розроблено з урахуванням вимог:

- Закону України «Про банки і банківську діяльність», зі змінами;
- Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого постановою Правління Національного банку України від 11.06.2018 № 64 зі змінами;
- Положення про порядок визначення банками України мінімального розміру операційного ризику, затвердженого постановою Правління НБУ від 24.12.2019 № 156 із змінами;
- Методичних рекомендацій щодо організації корпоративного управління в банках України, схвалених рішенням Правління Національного банку України від 03.12.2018 № 814-рш із змінами;
- Міжнародної конвергенції вимірювання капіталу і стандартів капіталу: переглянуті підходи, Базельській комітет з банківського нагляду;
- Принципів належного управління операційним ризиком, Базельській комітет з банківського нагляду;
- Кодекс корпоративного управління: ключові вимоги і рекомендації, затверджених рішенням Національної комісії з цінних паперів та фондового ринку від 12 березня 2020 року N 118
- Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління Національного банку України від 02.07.2019 № 88;
- Політики корпоративного управління Банківської Групи АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»;

- Стратегія управління ризиками банківської групи на 2024-2025 роки АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»;
- Стратегія управління ризиками на 2024-2025 роки АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»;
- Концепції управління ризиками АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»;
- Політики управління операційним ризиком АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»;
- інших нормативно-правових актів України, Національного банку України (далі - НБУ) щодо управління ризиками та внутрішніх нормативних документів Банку.

1.7. Терміни уживаються в Положенні у значенні, наведеному в Глосарії. Тлумачення інших термінів, що використовуються в Положенні, відповідає визначеним чинним законодавством, нормативними документами НБУ та внутрішньобанківським нормативним актам.

1.8. Положення є невід'ємною частиною системи управління ризиками Банку. Вимоги та правила, що встановлюються цим Положенням є обов'язковими до виконання та використання усіма органами управління та контролю, підрозділами і працівниками Банку

1.9. Положення є обов'язковим до виконання всіма учасниками Банківської Групи та всіма структурними/ відокремленими підрозділами Відповідальної особи Банківської Групи.

1.10. Функціонування системи управління ризиком інформаційної безпеки та ризиком інформаційно-комунікаційних технологій регламентується окремим внутрішнім нормативним документом.

2. ПОРЯДОК УПРАВЛІННЯ ОПЕРАЦІЙНИМИ РИЗИКАМИ НА РІВНІ БАНКІВСЬКОЇ ГРУПИ

2.1. Відповідальна особа створює адекватну систему управління операційним ризиком на рівні Банківської Групи, що має забезпечувати дотримання всіма учасниками Банківської Групи законодавства України, нормативів, правил, внутрішніх політик, стандартів і кодексів, що стосуються діяльності кожного учасника Банківської Групи, та визначає принципи та порядок управління операційним ризиком на рівні Банківської Групи. Управління операційним ризиком на рівні Банківської Групи є складовою системи внутрішнього контролю Банківської Групи.

2.2. Наглядова рада та Правління Відповідальної особи, а також керівники інших учасників Банківської Групи, або призначені ними уповноважені особи – ризик-координатори (далі – ризик-координатори), є головними суб'єктами, які забезпечують організацію та контроль за належним дотриманням законодавства та внутрішніх процедур та ефективністю управління операційним ризиком Банківської Групи, забезпечують інтегрованість управління операційним ризиком в загальну систему управління ризиками Банківської Групи.

2.3. Відповідальність за загальний контроль при управлінні операційним ризиком БГ покладається на Наглядову раду Відповідальної особи. Наглядова рада Відповідальної особи затверджує це Положення, принаймні щороку оцінює ефективність дотримання законодавства України на рівні Банківської Групи та розглядає визначення та оцінки основних операційних ризиків Банківської Групи.

2.4. Відповідальність за організацію операційного контролю та ефективне управління операційним ризиком покладається на Правління Відповідальної особи, в т.ч. прийняття і доведення до працівників БГ внутрішніх нормативних документів щодо операційних ризиків, забезпечення їх дотримання та сприяння складанню звітності перед Наглядовою радою з управління операційним ризиком.

2.5. Служба управління ризиками Відповідальної особи здійснює загальну координацію щодо управління операційним ризиком, функціонально забезпечує процес управління ризиком, виконує обов'язки в сприянні керівним органам в ефективному управлінні операційними ризиками, визначає та здійснює періодичну оцінку, моніторинг, контроль операційного ризику, консультує керівників та ризик-координаторів БГ з питань операційних ризиків, складає та подає управлінську звітність керівництву щодо операційного ризику. Відповідальність за безперервне функціонування системи операційний-контролю.

2.6. Управління операційним ризиком є невід'ємною частиною корпоративної культури в діяльності Банківської Групи. Виявлення, оцінка і управління операційним ризиком супроводжує кожний процес діяльності БГ.

2.7. Дотримання принципів управління операційними ризиками є обов'язком кожного працівника БГ.
2.8. Кожний учасник Банківської групи в межах цього Положення має право впроваджувати власні політики, положення, порядки щодо управління операційним ризиком відповідно до законодавчо визначених вимог для кожного учасника БГ відповідно до виду діяльності такого учасника.
2.9. Правління Відповідальної особи та керівники інших учасників Банківської Групи відповідають за безпосереднє забезпечення дотримання законодавства, стандартів та внутрішніх процедур, реалізацію порядку управління операційним ризиком, забезпечення впровадження процедур виявлення, оцінки, контролю та моніторингу операційних ризиків Банківської Групи.
2.10. У разі недотримання цього Положення Правління Відповідальної Особи має забезпечити вжиття запобіжних або дисциплінарних заходів та доведення до керівників учасників Банківської Групи інформації щодо вжиття запобіжних або дисциплінарних заходів.
2.11. Служба управління ризиками Відповідальної особи в цілях оцінки операційного ризику Банківської Групи:
2.11.1 визначає щоквартальну оцінку основних операційних ризиків з врахуванням операційних ризиків кожного учасника Банківської Групи, результатів стрес-тестування, розрахунку профіль ризику та дотримання ризик -апетиту до операційного ризику;
2.11.2 негайно доповідає Наглядовій раді про істотні операційні події/інциденти.
2.12. Поточні обов'язки з управління ризиками, в тому числі операційними ризиками на рівні Банківської Групи виконуються:
2.12.1 Службою управлінням ризиків Відповідальної особи в частині впровадження ефективної системи управління ризиками;
2.12.2 Службою управління ризиками Відповідальної особи в частині визначення, оцінки, контролю та моніторингу операційних ризиків учасників Банківської групи, звітування Наглядовій раді та Правлінню Відповідальної особи з питань управління та оцінки операційних ризиків Банківської Групи;
2.12.3 Юридичним управлінням Відповідальної особи в частині надання консультаційної допомоги з правових питань учасникам Банківської Групи;
2.12.4 Управлінням інформаційних технологій та Управлінням інформаційною безпекою Відповідальної особи в частині забезпечення управління інформаційною системою та управління інформаційною безпекою інформаційної системи Банківської Групи;
2.13. Головним бухгалтером Відповідальної особи в частині складання та подання консолідованої звітності Банківської Групи.
2.14. Між керівниками/ризик-координаторами учасників Банківської Групи і керівником кожного з цих підрозділів та між цими підрозділами мають бути налагоджені зв'язки (у тому числі з питань надання консультацій та обміну необхідною інформацією), достатні для ефективного функціонування системи управління операційними ризиками на рівні Банківської Групи. Учасники Банківської Групи мають співпрацювати з Службою управління ризиками Відповідальної особи в наданні інформації, допомагати виявляти операційні ризики та управляти ними на ранньому етапі їх виникнення.
2.15. Служба внутрішнього аудиту здійснює перевірку та оцінку ефективності системи управління операційними ризиками в БГ та інформує Наглядову раду щодо результатів перевірки стану ефективності управління операційним ризиком в БГ. Результати перевірки доводяться керівництву БГ та керівникам учасників БГ, діяльність яких перевірялась разом із рекомендаціями для усунення зауважень, виявлених в результаті перевірки.

3. ОСНОВНІ ПРИНЦИПИ ВЗАЄМОДІЇ МІЖ УЧАСНИКАМИ БАНКІВСЬКОЇ ГРУПИ З ПИТАНЬ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ

3.1. Ефективне функціонування системи управління операційним ризиком вимагає надійного зберігання та чіткий і оперативний обмін інформацією між Службою управління ризиками, ризик-координаторами та керівництвом Банку, БГ і Службою внутрішнього аудиту.
3.2. З метою організації системи оперативного пошуку та обміну інформацією у БГ використовуються всі можливі канали комунікації – письмові звіти, електронна пошта Банку, система електронного документообігу, внутрішній Веб-портал, зовнішній сайт Банку тощо. Працівниками /ризик -

координаторами БГ вживаються всі заходи для усунення блокування й викривлення інформації, що використовується в процесі управління операційним ризиком.

3.3. Основні принципи взаємодії між учасниками Банківської Групи з питань здійснення управління операційними ризиками:

3.3.1. працівники всіх учасників Банківської Групи відповідають за дотримання законодавства України, нормативів, правил, внутрішніх політик, стандартів і кодексів, що стосуються їх діяльності;

3.3.2. працівники всіх учасників Банківської Групи приймають участь в виявленні операційних ризиків БГ (подій/інцидентів);

3.3.3. працівники всіх учасників Банківської Групи негайно доповідають своєму безпосередньому керівнику про суттєві операційні події/інциденти або мають право інформувати безпосередньо керівника Служби управління ризиками Відповідальної особи;

3.3.4. працівники Служби управління ризиками Відповідальної особи мають право за своєю ініціативою контактувати з усіма керівниками/працівниками БГ, отримувати доступ до документів та архівів, необхідними для виконання своїх обов'язків.

4. ВИЗНАЧЕННЯ ОПЕРАЦІЙНОГО РИЗИКУ, ІДЕНТИФІКАТОРИ/ДЖЕРЕЛА/ФАКТОРИ РИЗИКУ

4.1. Класифікація операційних ризиків здійснюється згідно з рекомендаціями Базельського комітету з банківського нагляду та передбачає наступні загальні категорії:

	Категорія (1 рівень деталізації)	Характеристика категорії (2 рівень деталізації)
1	**Персонал та робоче середовище/ Управління персоналом та охорона праці /**	*Збитки в результаті дій, які не відповідають законодавству в сфері охорони праці (виплати персоналу у зв'язку з виробничими травмами, втратою здоров'я)* Втрати, які виникають внаслідок дій Банку, що суперечать укладеним кодексам, домовленостям (договорам) з працівниками, трудовому законодавству України, вимогам безпеки праці та протипожежної безпеки, а також відшкодування, виплачені за отримання виробничих травм. Ця категорія включає події, що стосуються взаємовідносин із працівниками, безпечного робочого середовища та дискримінації за різними ознаками.
2	**Внутрішнє шахрайство.**	*Збитки в результаті дій шахрайства, незаконного привласнення майна або **навмисного** порушення норм законодавства, інших нормативно правових актів або внутрішніх нормативних та/або організаційно розпорядчих документів, здійснених працівниками Банку* Втрати внаслідок умисних обманних дій, привласнення активів, ухилення від виконання/дотримання вимог законодавства України чи внутрішніх нормативних та/або організаційно-розпорядчих документів Банку за участю працівників Банку, несанкціоновані дії, крадіжка чи шахрайство за участі як мінімум однієї внутрішньої сторони/працівника Банку.

3	**Клієнти, продукти і норми ділової практики /стандарти ведення бізнесу.**	*Збитки в результаті неумисного або недбалого відношення до професійних зобов'язань перед клієнтами (включаючи неналежну якість рекомендацій) або в результаті недосконалості продуктів/послуг Банку.* Втрати, що виникають внаслідок халатності чи помилок під час виконання професійних обов'язків з обслуговування та супроводу клієнта, а також втрати, причиною яких є природа або властивості, банківського продукту/послуги/операції. Операційні ризики, що належать до цієї категорії, виникають унаслідок невиконання зобов'язань перед клієнтом, а також через характер або конструкції банківського продукту/послуги/операції
4	**Виконання операцій та управління процесами/ бізнес-процесами. //Виконавча дисципліна, процесний менеджмент**	*Збитки в результаті розладу, збоїв у процесі обробки транзакцій Банком або неналежного виконання контрагентами та постачальниками Банку своїх зобов'язань.* *Порушення у процесах банківської діяльності і надання послуг* Втрати, що виникають внаслідок помилок під час виконання операцій або управління процесами, а також помилок в управлінні відносинами з контрагентами та постачальниками. Ця категорія охоплює ризикові події, пов'язані з обробкою операцій або управлінням процесами, взаємовідносинами з торговими контрагентами і постачальниками.
5	**Порушення безперервної діяльності та збої в роботі/функціонуванні систем /порушення звичного режиму ведення бізнесу та відмови (негаразди, збої) систем. Технологічні збої та інфраструктура. Унеможливлення діяльності та функціонування систем**	Витрати що виникають внаслідок збоїв у роботі Банку або внаслідок несправності систем, неефективної організаційної структури, викривленої звітності. *Збитки в результаті збоїв у бізнес-процесах та системах*
6	**Зовнішнє шахрайство.**	*Збитки в результаті шахрайства, незаконного* ***привласнення*** *майна або* ***навмисного порушення*** *норм законодавства, інших нормативно правових актів або* ***внутрішніх нормативних та/або організаційно-розпорядчих документів, здійснених третіми особами****.* Втрати внаслідок умисних обманних дій, привласнення активів, ухилення від вимог законодавства України, що вчинені сторонніми для Банку особами (включаючи агентів та посередників), розкрадання або шахрайство, здійснене третьою, зовнішньою щодо Банку стороною.
7	**Пошкодження або знищення активів /заподіяння шкоди фізичним активам./ Стихійні лиха, безпека**	***Збитки в результаті пошкодження або знищення активів через природну катастрофу або інші події*** *Втрати, що виникають внаслідок знищення або пошкодження активів через стихійні лиха або дії інших чинників.* Ця категорія охоплює ризики втрат у результаті: катастроф, тероризму, вандалізму та третіх осіб.

4.2. На операційний ризик суттєво впливають юридичний ризик та комплаєнс-ризик, що визначається як негативні наслідки для надходжень та капіталу, які виникають через порушення або недотримання Банком вимог законів, нормативно-правових актів, угод, прийнятої практики або етичних норм, встановлених правил Банку, а також через можливість двозначного тлумачення діючих законів або правил.

4.3. **ФАКТОРИ ОПЕРАЦІЙНОГО РИЗИКУ:**

4.3.1 Для ідентифікації операційного ризику Банк визначає основні джерела / ідентифікатори/фактори (далі – фактори) операційних ризиків, які можуть призвести до збитків, виникнення додаткових витрат Банку або недоотримання запланованих доходів, а саме:

- **персонал;**
- **процеси;**
- **інформаційні технології та безпека;**
- **зовнішні події.**

4.3.2 Такі фактори є як зовнішніми, так і внутрішніми.

4.3.3 Банк та БГ визначають наступні особливості операцій, що є потенційними джерелами/факторами операційного ризику:

• операції, які вимагають високої кваліфікації, залежать від окремих працівників, їх знань та кваліфікації;

• процеси проведення операцій не формалізовані і не прозорі, при проведенні операцій велику роль грають «експертні» оцінки і суб'єктивні дані;

• системи, у яких проводяться операції, працюють з близькими до граничного або неадекватним навантаженням;

• операції, що проводяться, є технологічно складні;

• результат операції залежить у великій мірі від ефективності роботи персоналу;

• персонал низького рівня (кваліфікація, посада тощо) при проведенні операцій володіє високими повноваженнями за визначенням характеру операцій (в залежності від виду операції/бізнес-процесу/продукту/послуги);

• ефективність і ризиковість операцій, що проводяться, не піддаються оцінці в поточному режимі.

4.4. Розширена класифікація операційних ризиків з видами потенційних ідентифікаторів/джерел/ факторів приведена в **Додатку 1** до цього Положення.

4.5. Операційний ризик є складовою частиною всіх ризиків, на які наражається Банк та БГ. Управління операційними ризиками здійснюється, як окремо, так і в комплексі, спільно з іншими видами ризиків.

4.6. У разі наявності операційних ризиків, пов'язаних з кредитними/активними операціями, Банк такі ризики, в залежності від їх виду та впливу на процес, може розглядати їх як у складі операційних ризиків так і кредитних ризиків. При цьому до операційного ризику не включаються (не вичерпний перелік):

• судові справи, які є звичайною практикою;

• судові витрати і оплату по юридичних та інших послугах за ведення кредитних справ/справ пов'язаних із поверненням проблемної заборгованості або інших спорів, які не включають події операційного ризику;

• використання послуг зовнішніх юридичних консультантів/адвокатів з метою отримання консультацій, підготовки або перевірки документів, здійснення представництва тощо, пов'язаних з кредитними/активними операціями.

4.7. Банк та БГ чітко розмежовує функції управління операційним ризиком та комплаєнс-ризиком з метою уникнення їх дублювання.

5. УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ.

5.1. Ефективне управління операційним ризиком є необхідним для досягнення основних бізнес – цілей Банку та БГ, виконання законодавства України та регулятивних вимог Національного банку України:

5.2. Ефективне управління операційним ризиком забезпечує наступні переваги для діяльності Банку та БГ:

• зниження операційних втрат;

- раннє виявлення неправомірної діяльності;
- зменшення витрат на аудит;
- зменшення впливу майбутніх операційних ризиків;
- покращення розподілу капіталу.

5.3. Банк виходить з тих принципів, що рівень витрат на зменшення ризиків має бути дешевшим за той ефект, який можуть принести встановлені контрольні процедури за зменшенням ризиків та дії на фактори операційного ризику.

5.4. При управлінні операційним ризиком Банк застосовує циклічний підхід:

5.5. Для зменшення величини операційного ризику/залишкової величини операційного ризику Банк та БГ використовують наступні основні заходи та процедури:

5.5.1 Оптимізація організаційної структури Банку/БГ та системи внутрішнього контролю, внутрішніх правил та процедур здійснення банківських операцій, облікової політики, функціонування технічних, інформаційних та інших систем Банку та БГ;

5.5.2 відбір персоналу, доведення до персоналу його обов'язків, періодичні перевірки відповідності кваліфікації посаді, проведення навчання та перепідготовки працівників, контроль за діяльністю персоналу;

5.5.3 продуманий розподіл повноважень та підзвітності по банківських бізнес-процесах, операціях, додаткове підтвердження операцій, побудову адекватної системи внутрішнього контролю;

5.5.4 внутрішні контрольні процедури для мінімізації ризиків, документальний контроль, контроль за виконанням встановлених лімітів по банківських операціях тощо;

5.5.5 подвійне введення та регулярна звірка первинних документів та рахунків по банківських операціях;

5.5.6 виконання встановленого порядку доступу до інформації та матеріальних активів Банку та БГ;

5.5.7 розвиток автоматизації, банківських технологій та захисту інформації;

5.5.8 вивчення керівниками підрозділів системних помилок та здійснення заходів для подальшого їх усунення;

5.5.9 розробку системи заходів по забезпеченню безперебійності фінансово-господарської діяльності Банку та БГ, в тому числі забезпечення безперебійності функціонування операційних систем, дублювання та відновлення інформації, створення резервних систем;

5.5.10 розробку технологічних карт/регламентів бізнес – процесів / продуктів/послуг, видів діяльності Банку та БГ, аналіз і усунення слабких місць процесів, що підтримуються в постійно актуальному стані;

5.5.11 запровадження процедур раннього реагування на ймовірні операційні ризики, а саме визначення ключових індикаторів операційних ризиків ризику (KRI, KRI_ST), сценарний аналіз стрес-тестування операційних ризиків, встановлення обмежень/лімітів ризику, визначення ризик-апетиту до операційного ризику;

5.5.12 запровадження повного і своєчасного збору та внесення та аналіз інформації про події операційного ризику до бази внутрішніх подій операційного ризику та контроль за якістю і повнотою внесеної інформації;

5.5.13 постійний моніторинг та перегляд системи управління операційним ризиком;

5.5.14 розробку Службою управління ризиками системи звітності керівництву Банку та БГ для виявлення потенційних проблем та стимулювання управління операційним ризиком;

5.5.15 прив'язку матеріальної винагороди працівникам до якості управління операційним ризиком у підрозділах Банку;

5.5.16 розробку та контроль планів заходів щодо мінімізації, зменшення, пом'якшення операційного ризику;

5.5.17 використання передачі ризику (аутсорсинг);

5.5.18 зменшення фінансових наслідків операційного ризику (страхування та перестрахування);

5.5.19 визначення необхідного капіталу під операційний ризик;

5.5.20 впровадження ефективної системи внутрішнього контролю та її вдосконалення в подальшому.

6. ЕТАПИ ПРОЦЕСУ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ

Етапами процесу управління операційним ризиком є ідентифікація, оцінка ймовірності настання ризикової події, оцінювання ризику, моніторинг ризику, контроль ризику, мінімізація (нейтралізація) ризику.

6.1. ВИЯВЛЕННЯ/ІДЕНТИФІКАЦІЯ ОПЕРАЦІЙНОГО РИЗИКУ.

6.1.1 Виявлення операційного ризику – належне виявлення ризику - це, в першу чергу, визнання та розуміння наявних операційних ризиків або ризиків, що можуть виникнути у зв'язку з новими діловими ініціативами.

6.1.2 Виявлення операційного ризику має бути постійним процесом, що має здійснюватися як на рівні окремої операції, так і на рівні портфелів, це процес, згідно якого визначаються сфери, в яких виникає або може виникати операційний ризик, а також визначаються джерела/фактори, що можуть призвести до операційних втрат.

6.1.3 В процесі виявлення операційних ризиків задіяні усі працівники Банку виконання встановленого порядку доступу до інформації та матеріальних активів Банку та БГ, в межах сфер відповідальності їх підрозділів.

6.1.4 Основним інструментом виявлення операційних ризиків за окремим бізнес-процесом/банківським продуктом/послугою є аналіз Технологічних карт/регламентів бізнес-процесів/операцій, Паспортів банківських продуктів та Карт оцінки операційних ризиків бізнес-процесів (далі - Карта оцінки ОР), оформлених за формою, визначеною Додатком до діючої Методики оцінки операційних ризиків. Такі Карти оцінок ОР акумулюються та зберігаються в Службі управління ризиками. Метою створення Технологічних карт/регламентів бізнес-процесів/операцій є опис етапів бізнес-процесів, видів діяльності та розподіл організаційних функцій, а також визначення операційних та інших ризиків, що притаманні бізнес-процесам. В процесі створення Технологічних карт/регламентів бізнес-процесів виявляються його ключові первинні операційні ризики, взаємозв'язок з іншими ризиками, наявні контролі. Результатом виявлення операційних ризиків є впровадження, за необхідності, заходів з метою зниження залишкового ризику бізнес-процесу до рівня, що знаходиться в рамках встановленого Банком рівня ризик-апетиту до операційного ризику.

6.1.5 В ході виявлення операційних ризиків працівники Банку, в межах відповідальності своїх підрозділів повинні:

- виявляти загальні операційні ризики, які визначені в Технологічних картах/регламентах бізнес-процесів операцій, Паспортах банківських продуктів, Картах оцінок ОР.
- виявляти інші специфічні ризики та забезпечити їх належну класифікацію до загальних видів;
- забезпечити належне документування виявлених операційних ризиків, надавати звітність про інциденти операційних ризиків та вказувати виявлені операційні ризики в процесі здійснення подальшого внутрішнього контролю (ПВК) при складанні Довідок ПВК;
- на регулярній основі здійснювати перегляд виявлених операційних ризиків;
- надавати Голові Правління Банку, керівництву БГ та Службі управління ризиками інформацію про стан індикаторів раннього попередження операційного ризику - **Ключових індикаторів операційних ризиків (KRI);**

6.1.6 Для виявлення операційних ризиків Службою управлінням ризиками та керівниками підрозділів також використовується інформація, що отримана в процесі моніторингу операційних ризиків, а саме:

- класифікація бізнес-процесів;
- дані про операційні випадки/втрати/інциденти;
- результати розслідування операційних випадків/інцидентів;
- результати аналізу Ключових індикаторів операційного ризику (KRI);
- дані про результати проведеного подальшого внутрішнього контролю;
- результати стрес-тестування операційних ризиків, сценарний аналіз;
- проведення самостійної оцінки операційних ризиків та видів/засобів контролю;
- збір і аналіз даних щодо понесених Банком або БГ збитків, в т.ч. штрафів, даних ревізій кас та інвентаризацій;
- збір і аналіз зовнішніх даних про збитки;
- збір і аналіз даних щодо скарг клієнтів;
- показники ефективності діяльності, що є статистичними даними та даними управлінської звітності;
- порівняльний аналіз;
- участь Служби управління ризиками в розробці внутрішніх нормативних документів, які стосуються змін в процесах та стратегії роботи Банку та БГ;
- дані внутрішнього або зовнішнього аудиту, інших контролюючих органів;
- інша інформація, що може бути передбачена діючою методикою про збір даних про операційні випадки (інциденти), моніторинг та оцінку операційних ризиків.

6.1.7 Виявлення операційних ризиків повинно охоплювати ризики, які виникають як в існуючих бізнес-процесах, продуктах/послугах та інформаційних системах, так і ризики, які виникають на етапі впровадження нових банківських продуктів/послуг, інформаційних систем або змін в перебігу бізнес-процесів. Процедуру виявлення операційних ризиків в нових банківських продуктах регламентовано в діючих ВНД про розробку та узгодження нових продуктів Банку та значних змінах в діяльності Банку.

6.1.8 Результатом роботи по виявленню операційних ризиків є заповнена інформація в окремому розділі Технологічних карт/регламентів бізнес-процесів /операцій «Система внутрішнього контролю», передбачена політиками щодо внутрішнього контролю Банку в якому передбачається опис сфери відповідальності підрозділів під час виконання процесу та опис (ідентифікація) ризиків, способи їх мінімізації та види контролю/контрольних процедур для мінімізації таких ризиків, в розрізі контролів першої та другої лінії захисту. Оцінка ризиків проводиться в Картах оцінки ОР, які повинні містити такі поля: процес який оцінюється, ідентифікований операційний ризик та існуючий контроль.

6.2. ВИМІРЮВАННЯ. ОЦІНКА ЙМОВІРНОСТІ НАСТАННЯ РИЗИКОВИХ ПОДІЙ. ОЦІНЮВАННЯ РИЗИКУ

6.2.1 Оцінка/вимірювання ризиків - визначення величини (рівня) ризиків за допомогою кількісних та якісних показників для формування мотивованого судження щодо рівня операційного ризику. Процес оцінки операційних ризиків полягає в визначенні потенційних

втрат (як фінансових, так і не фінансових), до яких може призвести реалізація операційного ризику.

6.2.2 Для визначення процесу та критеріїв оцінки операційного ризику Службою управління ризиками розробляється відповідна **методика оцінки операційного ризику**.

6.2.3 Оцінка проводиться для усіх бізнес-процесів/нових продуктів та усіх виявлених в ході попереднього аналізу операційних ризиків.

6.2.4 Оцінку операційних ризиків (бізнес-процесів/банківських продуктів) проводять уповноважені особи, або керівники підрозділів в межах відповідальності їх підрозділів.

6.2.5 Управління ризиків контролює процес оцінки, та надає інформаційну/методологічну підтримку підрозділам, узгоджує визначені оцінки рівня ризику.

6.2.6 Оцінка операційних ризиків охоплює три стадії:

- **Оцінка можливих втрат** в разі реалізації операційного ризику зважаючи на ймовірність настання та величину впливу;
- **Оцінка ефективності контрольних процедур**, які запобігають реалізації операційного ризику, або попереджують втрати в разі його реалізації;
- **Оцінка залишкового рівня ризику** (рівень ризику з урахуванням ефективності контрольних процедур).

При цьому, для визначення результату оцінки залишкового рівня ризику, Банк приводить оцінку можливих втрат та оцінку ефективності контрольних процедур до єдиних порівнюваних значень показників вимірів (застосовує бальні величини).

6.2.7 В ході оцінки операційних ризиків працівники Банку та/або БГ, в межах відповідальності своїх підрозділів повинні:

- проводити оцінку виявлених операційних ризиків, та забезпечити перегляд цієї оцінки на щорічній основі;
- забезпечити належне документування результатів оцінки операційних ризиків;

6.2.8 Працівники Банку та/або БГ -власники процесів повинні виявляти/ідентифікувати та оцінювати операційні ризики та контролі в Технологічних картах/регламентах бізнес-процесів, операцій, паспортах банківських продуктів та Картах оцінки ОР/ висновках щодо нових банківських продуктів відповідно до внутрішніх нормативних документів Банку.

6.2.9 Для оцінки операційних ризиків додатково можуть використовуватися:

- дані про операційні інциденти/втрати, дані оцінки фінансового впливу реалізації операційного ризику;
- дані про динаміку показників індикаторів операційного ризику;
- дані сценарного аналізу операційних ризиків, для оцінки операційних випадків з низькою ймовірністю та значним впливом.

6.2.10 Для оцінки операційних ризиків розробляються методики на основі бальних методів, а також сценарний аналіз.

6.2.11 В процесі оцінки можуть використовуватися, як кількісні підходи, що базуються на статистичних даних, даних про втрати, так і якісні підходи, що базуються на самооцінці операційних ризиків підрозділами Банку /метод оціночних карт/ та визначення ключових показників/індикаторів операційних ризиків.

6.2.12 Служба управління ризиками на підставі отриманих результатів внутрішнього контролю, інцидентів операційних ризиків, інформації щодо індикаторів операційного ризику, результатів самооцінки операційного ризику щоквартально здійснює загальну оцінку операційного ризику та складає Карту загальної оцінки операційного ризику відповідно до методики про збір даних про операційні випадки (інциденти), моніторинг та оцінку операційних ризиків.

6.2.13 **Оцінка ризиків** - визначення величини (рівня) ризиків за допомогою кількісних та якісних показників для формування мотивованого судження Банку щодо рівня операційного ризику. Процес оцінки операційного ризику полягає в визначенні потенційних втрат (як фінансових, так і не фінансових), до яких може призвести реалізація операційного ризику .

6.2.14 Для визначення процесу та критеріїв оцінки операційного ризику Правління Банку забезпечує розроблення відповідної методики.

При цьому Банк та/або БГ застосовують бальну оцінку ризику та визначає наступні оцінки операційного ризику:

Бали рівня ризику		Опис ризику
До «1» включно	ризик низький	У діяльності Банку та/або БГ відсутні суттєві невідповідності щодо управління ризиками. *Незначний рівень ризику, не потребує виконання додаткових заходів, на розсуд керівників (члени Правління – куратори напрямку, начальник департаменту, управлінь/служб)*
Від 1 до «2» включно	помірний ризик	У діяльності Банку та/або БГ є певні невідповідності щодо управління ризиками, які не становлять загрозу інтересам вкладників та інших кредиторів Банку. *Помірний рівень ризику, управляється на рівні керівників (члени Правління – куратори напрямку, директори, начальники департаменту, управлінь/служб*)
Від 2 до «3» включно	підвищений ризик	У діяльності Банку та/або БГ є невідповідності щодо управління ризиками, які, у разі їх не усунення, можуть створити загрозу інтересам вкладників та інших кредиторів Банку. *Підвищений рівень ризику, вимагає прийняття необхідних управлінських рішень Правлінням Банку* та/або керівництвом БГ *в прийнятні для Банку/БГ терміни*
Від 3 до «4» включно	високий ризик	У діяльності Банку та/або БГ є суттєві невідповідності щодо управління ризиками, що створює загрозу інтересам вкладників та інших кредиторів Банку. Значний рівень ризику, вимагає прийняття негайних необхідних управлінських рішень Наглядової ради/комітетів ради за поданням Правління Банку або Служби управління ризиками
Від 4 до 5 - «F»	«F» безпосередній ризик для життєздатності Банку	Характеризує безпосередній ризик для життєздатності Банку БГ, у тому числі в разі, якщо є обґрунтовані підстави для віднесення Банку до категорії проблемних, неплатоспроможних або ліквідації.

6.2.15 Для визначення оцінки операційного ризику Служба управління ризиками, за кожною окремою подією/ інцидентом операційного ризику може використовувати якісну оцінку яка визначається працівником служби ризиків на підставі суб'єктивного погляду у залежності від виду та впливу події/інциденту операційного ризику на діяльність Банку. На підставі визначеної якісної оцінки Служба управління ризиками має право як погіршити оцінку операційного ризику на 1-2 пункти, так і покращити її на 1 пункт.

6.2.16 По операційних ризиках бізнес-процесів, які згідно розробленої методики оцінки операційного ризику, оцінено як «підвищений» та «високий», розробляється план заходів зниження операційних ризиків (далі - План заходів) за формою, встановленою відповідним додатком до діючої методики оцінки операційного ризику.

6.2.17 По значних змінах в діяльності /нових банківських продуктах на підставі розгляду застережень, наданих Службою управління ризиками щодо операційного ризику, Наглядова рада/Правління Банку приймає управлінські рішення щодо пом'якшення/зниження рівня /мінімізації операційного ризику, при цьому підрозділами Банку можуть бути складені відповідні Плани заходів для мінімізації/зниження рівня операційного ризику у бізнес – процесі /продукті, за формою, встановленою відповідним додатком до діючої методики оцінки операційного ризику.

6.2.18 План заходів як правило затверджується Правлінням Банку. При розгляді звітності по операційних ризиках, наряду з прийнятими управлінськими рішеннями, План заходів може затверджуватись Наглядовою радою Банку.

6.2.19 У разі, якщо між підрозділами Банку та Службою управління ризиками досягнуто компромісне рішення, затвердження Плану заходів може не виноситися на розгляд Правління, а підтверджуватись внутрішньою перепискою між підрозділами Банку та Службою управління ризиками. Таке врегулювання питань відбувається при незначних ризиках, або коли недоліки уже виправлені.

6.2.20 План заходів, що запропонований підрозділами, погоджений з СУР та затверджений Правлінням Банку та /або Наглядовою радою є обов'язковим до виконання.

6.2.21 Служба управління ризиками доводить інформацію до відома Правління Банку про заходи, що були затверджені Наглядовою радою Банку.

6.2.22 План заходів повинен обов'язково містити:

- опис заходів, які необхідно вжити для зменшення рівня операційних ризиків,
- відповідальний за виконання підрозділ Банку,
- призначеного відповідального працівника підрозділу,
- контролера підрозділу відповідального за виконання заходу
- очікувані терміни виконання.

6.2.23 Результатом оцінки операційних ризиків є заповнені:

- Карта оцінки ОР по бізнес-процесу/або критичному процесу
- Карта загальної оцінки операційного ризику,
- Висновки підрозділів з оцінками ризиків по значних змінах діяльності/нових банківських продуктах,
- застереження Служби управління ризиками щодо нових банківських продуктів де для операційного ризику проставлена величина ризику (бальна оцінка, визначення категорії ризику), та у разі необхідності План заходів. При затвердженні нових банківських продуктів відповідні оцінки рівня операційного ризику зазначаються у спеціальних висновках підрозділів – власників бізнес-процесів та підрозділів, що супроводжують/контролюють банківський продукт .

6.2.24 Необхідність розробки Плану заходів по кожному оціненому ризику визначається Службою управління ризиками після аналізу результатів оцінки.

6.2.25 Крім того, як альтернатива Планам заходів, може бути наступна процедура реагування на операційні ризики при їх оцінці:

- Банк свідомо та об'єктивно може приймати ризики за умови, що вони чітко задовольняють політику Банку та критерії прийняття ризиків,

або

- Банк може уникнути операційних ризиків (наприклад: відмовляється від проведення окремих операцій тощо);

або

- Банк переносить відповідні операційні ризики на інші сторони, наприклад: страхувальників, постачальників, аутсорсерів.

6.3. МОНІТОРИНГ ОПЕРАЦІЙНОГО РИЗИКУ.

Моніторинг операційного ризику полягає в спостереженні за змінами в процесах Банку, БГ за допомогою інструментів, що показують рівень операційного ризику.

Основними інструментами моніторингу операційних ризиків є:

1) **Ключові індикатори операційного ризику** (KRI). KRI є кількісним показником, який динамічне змінюється в часі та відображає зміну характеру операційного ризику. KRI використовується банком для раннього виявлення негативних тенденцій/явищ, пов'язаних з підвищенням операційного ризику, що притаманні процесам. KRI є кількісним показником, який динамічне змінюється в часі та відображає зміну характеру операційного ризику. KRI використовується банком для раннього виявлення негативних тенденцій/явищ, пов'язаних з підвищенням операційного ризику, що притаманні процесам. Банк визначає перелік показників KRI, порядок їх розрахунку та граничні значення, які забезпечують своєчасне та найбільш повне виявлення факторів операційного ризику з метою застосування своєчасних заходів щодо управління ними. Банк розраховує показники KRI з періодичністю раз на три місяці. Ключовий індикатор операційного ризику (KRI) розробляється Службою управління ризиками спільно з уповноваженою

особою підрозділів Банку (ризик-координатором) та ризик-координаторами БГ, або з робочими групами.

2) **Аналіз результатів перевірок, здійснених підрозділом внутрішнього аудиту та зовнішнім аудитором.** Здійснюється аналіз щоквартальної інформації від Служби внутрішнього аудиту з метою виявлення операційних ризиків та занесення подій операційного ризику до Бази подій операційного ризику.

3) **Створення та ведення бази внутрішніх подій** операційного ризику та аналіз накопиченої в ній інформації з урахуванням наступних принципів:

- точність і цілісність,
- повнота даних,
- своєчасність,
- адаптивність

Банк уносить операційні події в базу внутрішніх подій операційного ризику з урахуванням визначених банком критеріїв звітування.

4) **Самооцінка операційного ризику**. У рамках самооцінки операційного ризику не рідше ніж один раз на рік проводиться аналіз бізнес-процесів банку з урахуванням інформації щодо можливих загроз і вразливостей та оцінюють можливі втрати від них, оцінюються ризики бізнес-процесів банку (до впровадження або перегляду контролів), ефективність контрольного середовища (запроваджених контролів) та залишкові ризики (з урахуванням запроваджених або переглянутих контролів.

5)**Сценарний аналіз**. Цей інструмент застосовується шляхом формування судження працівниками підрозділу з управління ризиками та підрозділів першої лінії захисту щодо визначення можливих малоймовірних подій операційного ризику з суттєвими наслідками для банку та їх кількісної оцінки. Сценарний аналіз є методом стрес-тестування операційного ризику для різних короткострокових і довгострокових стрес-сценаріїв, що можуть реалізуватися як для банку, так і для ринку в цілому, з метою виявлення причин можливих втрат внаслідок реалізації операційного ризику та оцінки відповідності результатів здійснення стрес-тестування встановленому рівню ризик-апетиту до операційного ризику. Банк проводить сценарний аналіз, базуючись на судженнях працівників підрозділів першої лінії захисту та працівників Служби управління ризиками щодо:

- імовірного збільшення частоти (кількості) подій та/або обсягу операційних збитків порівняно зі статистикою, що міститься в базі внутрішніх подій операційного ризику;

- виникнення нових подій операційного ризику внаслідок впровадження нових або внесення значних змін у діючі процеси;

- виникнення подій операційного ризику зі значним рівнем втрат та низькою імовірністю настання. В процесі моніторингу за операційним ризиком відповідальні підрозділи повинні здійснювати моніторинг операційного ризику на постійній основі з метою виявлення будь яких змін щодо рівня операційного ризику, на який наражається Банк.

6.3.1 Для моніторингу операційних ризиків використовується База подій операційного ризику, яка ведеться Службою управління ризиками на внутрішньому ВЕБ порталі Банку.

6.3.2 Для ефективного ведення такої інформаційної бази даних Банком розробляється:

1) Методика про збір даних про операційні випадки (інциденти), моніторинг та оцінку операційних ризиків, яка в тому числі передбачає процедури контролю за повнотою та якістю даних про події операційного ризику, а зокрема:
    - розподіл обов'язків та відповідальності між підрозділами банку щодо контролю за повнотою та якістю даних про події операційного ризику банку під час їх збору, унесення до бази внутрішніх подій операційного ризику та подальшої перевірки;
    - **заходи поточного** (під час збору та внесення даних до бази внутрішніх подій операційного ризику) **та подальшого контролю за повнотою та якістю даних про події операційного ризику**, уключаючи автоматизовані та/або ручні перевірки щодо

відсутності помилок та суперечливості даних, відповідності обліковим, фінансовим, статистичним даним та даним управлінської звітності банку.

2) Інструкція по роботі в інтерактивному веб-сервісі реєстрації та обробки повідомлень про події операційного ризику.

6.3.3 Служба управління ризиками проводить класифікацію кожного виявленого операційного випадку згідно із діючою Методикою про збір даних про операційні події (інциденти), моніторинг та оцінку операційних ризиків.

6.3.4 По всіх операційних подіях (інцидентах) встановлюються причини виникнення та наслідки їх реалізації, а також, у разі необхідності (якщо випадок визначено як суттєвий), розробляється План заходів, який формалізує внесення змін у процес для недопущення реалізації подібних випадків у майбутньому.

6.3.5 Процедура реагування регламентується окремим розділом діючої Методики про збір даних про операційні події (інциденти), моніторинг та оцінку операційних ризиків.

6.3.6 У разі необхідності проводяться наступні процедури реагування на операційна подія (інцидент) або виявлений ідентифікований операційний ризик, а саме:

- У разі виявлення значних подій операційного ризику складається відповідний План заходів щодо пом'якшення чи уникнення ризиків;
- Банк та/або БГ свідомо та об'єктивно приймає ризики за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;
- Банк та/або БГ уникає операційних ризиків (наприклад, відмовляється від проведення окремих операцій тощо);
- Банк/БГ може здійснювати передавання своєї відповідальності за ризик іншим особам за винагороду зі збереженням наявного рівня ризику наприклад, страхувальникам, постачальникам, аутсорсерам.

6.3.7 У разі необхідності встановлення додаткових причин реалізації операційного ризику, або розробки Плану заходів для недопущення їх виникнення у майбутньому наказом Голови Правління може бути створена робоча група.

6.3.8 Служба управління ризиками також використовує результати подальшого внутрішнього контролю для виявлення та аналізу операційного ризику.

6.4. УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ, ЩО ВЛАСТИВИЙ ПРОЦЕСУ СПІВПРАЦІ З АУТСОРСЕРАМИ.

6.4.1 Управління операційним ризиком, що властивий процесу співпраці з аутсорсерами відбувається у відповідності до даного Положення, а також у відповідності до внутрішнього документу Банку, що визначає порядок роботи із аутсорсерами-постачальниками послуг під час передачі деяких функцій Банку для виконання третіми особами. Мета такого документу є встановлення належного управління ризиками, що пов'язані з передаванням функцій на аутсорсинг та виконанням аутсорсером таких функцій.

6.4.2 Під час передавання функцій на аутсорсинг основними критеріями щодо прийняття відповідного рішення є:

- обґрунтованої доцільності передавання функцій на аутсорсинг;
- забезпечення збереження банківської та комерційної таємниці в разі передавання функцій на аутсорсинг;
- подальшого належного управління ризиками, що пов'язані з передаванням функцій на аутсорсинг та виконанням аутсорсером таких функцій.

6.4.3 Банк не має права передавати на аутсорсинг функції щодо:

- здійснення банківської діяльності, на яку він отримав банківську ліцензію;
- управління ризиками, крім випадків, передбачених Положенням про організацію системи управління ризиками в банках України та банківських групах, затвердженою Постановою НБУ №64 від 11.06.2018р., зі змінами.

6.4.4 Банк не має враховувати як аутсорсинг таке:

- послуги зовнішнього аудитора та інші послуги, що відповідно до законодавства України надаються визначеними постачальниками послуг;
- послуги агентств Bloomberg, Moody's, Standard & Poor's, Fitch;
- послуги платіжних систем Visa, MasterCard;
- послуги клірингу;
- послуги Товариства всесвітніх міжбанківських фінансових телекомунікацій SWIFT;
- послуги банків-кореспондентів;
- придбання послуг, які в іншому випадку не здійснювалися б банком (ураховуючи юридичні, медичні, туристичні послуги; послуги з прибирання, озеленення та обслуговування приміщень, службових автомобілів банку, громадського харчування; послуги архітектора, торгових автоматів, пошти, секретарів та операторів розподільних щитів, комутаторів); послуги з виробництва товарів (ураховуючи пластикові картки, карт-рідери, канцелярське приладдя, персональні комп'ютери, меблі) та комунальні послуги (ураховуючи електропостачання, газопостачання, водопостачання, телефонний та інтернет-зв'язок).

6.4.5 Банк повинен під час прийняття рішення про відбір аутсорсеру та надалі на щомісячні основі дотримуватися контрольних процедур щодо аналізу та контролю ефективності співпраці з аутсорсером, що визначені у внутрішнього документу Банку, що визначає порядок роботи із аутсорсерами-постачальниками послуг під час передачі деяких функцій Банку для виконання третіми особами

6.5. ЗВІТНІСТЬ

6.5.1 Служба управління ризиками повинна підсумовувати результати моніторингу операційних ризиків та **щоквартально** готувати управлінську звітність для Правління Банку та Наглядової ради Банку.

6.5.2 Служба управління ризиками **щоквартально** здійснює моніторинг та складає звіти Правлінню та Наглядовій раді :

- внутрішніх даних про операційні втрати чи наслідки операційних випадків;
- показників Ключових індикаторів операційних ризиків (KRI),
- реалізації Планів заходів для зменшення/пом’якшення або перенесення операційного ризику (у разі наявності);
- ефективності функціонування контрольних механізмів за операційними ризиками.

6.5.3 Частота проведення моніторингу повинна зростати одночасно із частотою змін в операційному середовищі Банку та/або БГ.

6.6. КОНТРОЛЬ ЗА РІВНЕМ ОПЕРАЦІЙНОГО РИЗИКУ. МІНІМІЗАЦІЯ (НЕЙТРАЛІЗАЦІЯ) РИЗИКУ

6.6.1 Організація внутрішнього контролю операційного ризику в Банку будується наступним чином:

- Підрозділи, в особі керівника підрозділу(ризик-координатора), здійснюють безпосередній контроль управління операційним ризиком;
- організація контролю операційного ризику здійснюється Службою управління ризиками;
- Служба внутрішнього аудиту забезпечує незалежну оцінку управління операційним ризиком.

6.6.2 Основні види внутрішніх контролів/контрольних процедур за операційним ризиком передбачаються у внутрішніх нормативних документах (Технологічних картах/регламентах бізнес-процесів/банківських продуктах чи послуг) в частині опису основних ризиків та контрольних процедур, Картах оцінок ОР в полі «Оцінка ВК», в Графіках подальшого внутрішнього контролю Банку.

6.6.3 Процес контролю за операційним ризиком та реагування на нього полягає **в прийнятті, ухиленні, перенесені або зменшені рівня ризику:**

- операційні ризики можуть бути прийняті, якщо вони не впливають на результати діяльності Банку/БГ, або їх вплив не призводить до значних наслідків;

- зменшення операційних ризиків полягає у зменшенні рівня їх впливу на Банк/БГ шляхом впроваджені контрольних процедур/ додаткових контрольних механізмів або зменшення обсягів операційної діяльності;
- ухилення від ризиків може здійснюватися шляхом відмови від певного виду діяльності;
- перенесення операційного ризику може здійснюватися шляхом страхування наслідків його реалізації, аутсорсингу.

Рішення про прийняття, ухилення, перенесення або зменшення (мінімізацію) рівня операційного ризику приймається Правлінням Банку та Наглядовою радою Банку.

6.6.4 Банк/БГ встановлює наступні основні методи обмеження рівня операційного ризику, через впровадження контрольних процедур:

- розподіл функцій та повноважень;
- обмеження доступу, в т.ч. фізичного доступу,
- моніторинг, управлінська звітність,
- звірка даних;
- затвердження документів,
- контроль керівника,
- подвійне введення даних;
- контроль виправлень;
- додаткове підтвердження операцій;
- персоналізація відповідальності за кожну операцію;
- заходи підвищення надійності інформаційних систем:
- використання резервного сервера;
- архівування документів,
- централізоване збереження даних на резервних зовнішніх магнітних носіях;
- шифрування, тощо

В залежності від розвитку Банку/БГ, IT систем та змін бізнес-процесів контрольні процедури можуть оновлюватись, появлятись нові.

6.6.5 Додатково, для мінімізації операційних ризиків, можуть використовуватися інші заходи, наприклад: перебудова бізнес-процесів, автоматизація процесів тощо.

6.6.6 Суттєвим впливом на зменшення рівня операційних ризиків є наявність ефективного та цілісного комплексного Плану забезпечення безперервної діяльності (BCP - Business Continuity Plan), який уключає:

1) стратегічні цілі та пріоритети банку щодо забезпечення безперервної діяльності в розрізі процесів Банку/БГ;
2) процедури та заходи реагування на інциденти порушення безперервності діяльності;
3) заходи у разі порушення безперервної діяльності щодо внутрішніх комунікацій, а також зовнішніх комунікацій банку з клієнтами, контрагентами банку, Національним банком, іншими регуляторними, контролюючими органами та органами державної влади;
4) заходи відновлення діяльності для критичних процесів банку;
5) заходи відновлення інформаційних систем після збоїв.

6.6.7 В процесі контролю за операційними ризиками відповідальні підрозділи повинні:

- забезпечити належний контроль за виявленими операційними ризиками (переконатися, що рівень кожного операційного ризику не перевищує рівень схильності Банку до цього ризику);
- проводити періодичну оцінку витрат для підтримки інструментів контролю за операційними ризиками;
- дотримуватися політики управління ризиками, визначеної Наглядовою радою Банку;
- забезпечити впровадження та підтримку ефективної системи внутрішнього контролю;
- забезпечити належне утримання величини операційного ризику на прийнятному для Банку/БГ рівні;
- призначити у Планах заходів відповідального за усунення наслідків реалізації операційних ризиків, а також вживати заходи необхідні для попередження подібних випадків у майбутньому;

6.6.8 Виконання Плану заходів є інструментом контролю за рівнем операційних ризиків. СУР централізовано підсумовує результати виконання Планів заходів.

6.6.9 Відповідальні за виконання Плану заходів повинні щоквартально протягом перших 15 днів наступного місяця за звітним кварталом, або за окремими запитами Служби управління ризиками, надавати інформацію щодо результатів виконання Планів заходів зниження операційного ризику у відповідному бізнес-процесі/банківському продукті чи послузі до Служби управління ризиками засобами електронної пошти. Надана інформація повинна обов'язково містити:

- у разі виконання: дату впровадження, опис того, що було виконано, а також підтверджуючий документ;
- у разі невиконання: причини затримки та новий очікуваний термін виконання або обґрунтування причин в разі недоцільності виконання відповідного заходу.

6.6.10 Щоквартально Служба управління ризиками надає управлінську звітність щодо результатів моніторингу Планів заходів Правлінню Банку та Наглядовій раді Банку. Такий звіт містить інформацію про заходи, які було виконано, прострочене (із зазначенням причин затримок та нових термінів виконання), а також інформацію про заходи, терміни яких ще не наступили та рекомендації.

7. КЛЮЧОВІ ПОКАЗНИКИ ОПЕРАЦІЙНОГО РИЗИКУ / ІНДИКАТОРИ ОПЕРАЦІЙНИХ РИЗИКІВ (KRI)

7.1. В цьому розділі Положення визначається методологія стосовно ідентифікації, вибору, управління, моніторингу і звітування щодо Ключових індикаторів операційних ризиків (KRI) у межах Банку та визначено різні типи Ключових індикаторів операційних ризиків (KRI), ролі і відповідальність, підходи до вибору індикаторів, характеристики ефективних індикаторів, процеси управління і моніторингу, а також звітування про результати моніторингу індикаторів.

7.2. До категорії індикатор ризику Банк відносить критерії із заданими наперед параметрами, використання яких дає можливість здійснювати вибір об'єкта контролю, що становить ризик.

7.3. Показники Ключових індикаторів операційних ризиків (KRI) використовуються Банком при формуванні звітності про потенційний, поточний стан або тенденцію схильності до операційного ризику, що дає можливість розробити заходи з його попередження.

7.4. Банк впроваджує ключові показники операційного ризику – Ключові індикатори операційного ризику (KRI – Key Risk Indicators).

Індикатор ризику стає «ключовим», коли він відстежує важливу загрозу ризику (ключовий ризик) або він робить це особливо добре (ключовий індикатор), або ж виконує обидві функції.

Прикладом індикатору ризику може бути плинність кадрів, цей індикатор може показувати збільшену можливість шахрайства, нестачу кадрів і помилки процесу.

Ключові індикатори операційного ризику (KRI) є інструментом для моніторингу бізнес-процесів, операцій, що потенційно генерують операційні збитки, а також якості операційних процесів, яка, в свою чергу, може свідчити про їх недосконаліть, порушення та можливі операційні збитки.

7.5. Ключові індикатори операційного ризику (KRI) є елементом системи раннього попередження операційних ризиків. Ключові індикатори операційного ризику (KRI) дозволяють оцінити поточний статус основних ризиків, перевірити, чи знаходяться ризики у встановлених межах, виділити слабкі місця, які потребують залучення додаткових ресурсів для їх зниження. Вони є показниками, які використовуються для постійного моніторингу загрози реалізації інцидентів операційних ризиків з метою попередження відповідальних осіб про те, що індикатор перевищив/впав нижче визначених порогових значень і необхідним є вжиття заходів з мінімізації операційного ризику.

7.6. Банк впроваджує ключові індикатори операційного ризику (KRI) з метою попередження керівництва Банку про те, що рівень загрози реалізації інциденту операційного ризику в Банку зростає і, можливо, необхідним є перевірка таких індикаторів та вжиття відповідних заходів з мінімізації операційних ризиків.

7.7. 5.6. Ключові індикатори операційного ризику (KRI), як індикатори раннього попередження операційних ризиків – це система показників, які відображають статус операційного ризику у визначений період часу. СУР використовує ці показники для про активного моніторингу процесів діяльності Банку з метою виявлення потенційних операційних ризиків, що можуть на них вплинути, до їх реалізації, визначеної схильності до ризику протягом певного періоду часу. Таким чином, будь-які величини, які можуть виконувати цю функцію, можуть вважатися індикаторами.

7.8. Ключові індикатори операційного ризику (KRI) можуть ділитись на типи:

- Індикатори ризику: прогнозний, поточний, ретроспективний.
- Індикатори контролю.
- Індикатори виконання.

7.9. В рамках системи управління операційним ризиком індикатором ризику є показник, який надає інформацію про рівень загрози операційного ризику у визначений час. Необхідно, щоб індикатор ризику мав взаємозв'язок із ризиком, загрозу по якому він представляє.

7.10. Існують три основних індикатори ризику:

- прогнозні,
- поточні,
- ретроспективні.

7.11. Індикатор вважається прогнозним, якщо він відображає очікувану зміну рівня ризику. Ці типи індикаторів можуть попереджати Службу управління ризиками та керівництво Банку про потенційне зростання операційного ризику, дозволяючи їм приймати попереджуючі заходи/заходи з мінімізації операційних ризиків до реалізації подій чи інцидентів операційного ризику. З точки зору управління, це найбільш прийнятний тип індикатору, наприклад, при розрахунках: непідтверджені транзакції при розрахунках швидше за все призведуть до помилок або заборгованості;

7.12. Поточний індикатор забезпечує моментальний знімок середовища загрози на поточний момент. Таким чином, він дозволяє вжити заходи для зменшення/мінімізації підвищеної загрози реалізації події операційного ризику.

7.13. Ретроспективний індикатор відображає історичну тенденцію втрат або збільшення схильності до ризику, що спостерігалася у минулих періодах. При належному застосуванні такі індикатори можуть допомогти ідентифікувати «приховані» втрати і надати контекстуальну інформацію щодо існуючих тенденцій схильності до ризику.

7.14. Індикатори контролю.

Індикатор ефективності контролю надає інформацію про рівень, до якого даний контроль зменшує / мінімізує певний ризик. Він може використовуватися для виміру ефективності певних контролів у певному проміжку часу. Індикатор ефективності контролю повинен мати сильний кореляційний зв'язок як з контролем, так і з ризиком, для зменшення/мінімізації якого було впроваджено контроль. **наприклад**, при підтвердженні: цей індикатор є мірою контролю (ефективності), який представляє собою кількість транзакцій, які не були підтверджені і потребують подальших дій.

7.15. Індикатори виконання. Індикатор виконання є показником, який вимірює результат діяльності.

Загалом індикатори виконання більше стосуються інших сфер бізнесу, вони стосуються операційного ризику, коли вимірюють досягнення особливих цілей, таких як зменшення загрози реалізації події операційного ризику, та визначення Банком якості управління своїми операційними ризиками. **наприклад,** при угодах: це індикатор представляє собою кількість помилок в процесі укладання угод.

7.16. Ідентифікація і вибір Ключових індикаторів операційного ризику (KRI).

Загальна цінність Ключових індикаторів операційного ризику (KRI), залежить від їх можливості порівнювати та інтерпретувати результати моніторингу. Ця мета досягається у разі наявності достатнього рівня стандартизації процесу ідентифікації та розробки Ключових індикаторів операційного ризику (KRI). Нижченаведені кроки є обов'язковими для Банку

під час процесу ідентифікації, вибору, розробки, моніторингу і перегляду своїх Ключових індикаторів операційного ризику (KRI).

7.17. При виборі Ключових індикаторів операційного ризику (KRI) необхідно обов'язково приймати до уваги наступні критерії:

- відображення схильності до операційного ризику на рівні Банку. При їх виборі враховується стратегія управління ризиками Банку,
- сприяння агрегуванню даних по відповідних продуктах/послугах з метою визначення.

7.18. При виборі Ключових індикаторів операційного ризику (KRI) необхідно враховувати:

- результати аналізу ризиків, тобто забезпечити, щоб обрані індикатори сприяли безперервному моніторингу ідентифікованих ризиків;
- результати перевірок регуляторних органів/висновків аудиту, тобто обрані індикатори зможуть закрити виявлені недоліки в системі контролів або моніторингу;
- ризики, які ідентифіковані в процесі розгляду нового продукту;
- будь-яку інформацію, отриману в результаті нещодавніх інцидентів ОР;
- зовнішні індикатори, такі як зміни у економічному середовищі (наприклад, індикатори ризику шахрайства);
- планові показники для систем, продуктів і працівників.

Все вищезазначене вважається потенційною відправною точкою для вибору/ідентифікації індикаторів.

7.19. При виборі Ключових індикаторів операційних ризиків (KRI) Банк застосовує також наступні критерії:

- Доречність. Індикатор повинен мати взаємозв'язок з тим, що він відслідковує. Це означає, що індикатор ризику повинен давати можливість здійснювати моніторинг рівня схильності до ризику, тоді як індикатор контролю повинен давати можливість відслідковувати ефективність контролю.
- Вимірюваність. Індикатори повинні підлягати вимірюванню, мати високий рівень достовірності і збиратися на регулярній основі. Це означає, що індикатори повинні мати числові значення (кількість, грошова вартість, відсотки, коефіцієнти, визначені відхилення тощо) і бути зрозумілими без додаткового (суб'єктивного) аналізу. Текстові індикатори є чутливими до порушень і неправильного трактування; тому задля уникнення таких проблем Банк їх не використовує.
- Простота моніторингу. Індикатори повинні бути простими і економічно ефективними (для збору, забезпечення якості і розподілу), зрозумілими та простими для моніторингу. Процес збору даних не повинен бути обтяжливим; дані мають бути доступними, з мінімальним робочим навантаженням щодо прийняття/обробки існуючих показників. Цикл збору індикаторів повинен бути чітко визначеним і прозорим, що дозволить забезпечити належну якість процесу.
- Можливість порівняння. Усі індикатори повинні порівнюватися з встановленими по відношенню до них показниками (лімітами/порогами), які надають їм належного значення і можливість подальшої ескалації. Індикатори повинні ґрунтуватися на статистичній інформації, зібраній за певний (тривалий) періоду часу. Це дасть можливість Банку отримати певну базову інформацію щодо рівня ризику по певному процесу для подальшого встановлених лімітів і порогових значень, на основі яких будуть впроваджуватися заходи з ескалації.
- Можливість аудиту Індикатори повинні бути прозорими і придатними для аналізу. Ефективний процес управління є основою ризик-менеджменту, тому незалежний аудит процесу вибору індикаторів і самого процесу є обов'язковим.

7.20. Наглядова рада Банку щороку в першому місяці звітного року затверджує перелік Ключових індикаторів операційних ризиків (KRI) та визначає їх граничні значення, які забезпечують своєчасне та найбільш повне виявлення факторів операційного ризику з метою вжиття своєчасних заходів щодо управління ними.

7.21. Протягом року, в залежності від схильності Банку до операційного ризику, такий перелік Ключових індикаторів операційних ризиків (KRI), може доповнюватись, переглядатись на підставі

управлінської звітності за показниками, іншою звітністю за операційним ризиком, в т.ч. за поданням рекомендацій від Правління Банку, Служби управління ризиками.

7.22. Оскільки значимість Ключових індикаторів операційних ризиків (KRI) з часом може змінюватись через виникнення нових, мінімізацію існуючих загроз або їх неактуальність, встановлений перелік Ключових індикаторів операційних ризиків (KRI) повинен постійно переглядатися на щорічній основі.

7.23. Процес впровадження/зміни індикаторів не відрізняється від процесу їх початкового вибору і повинен здійснюватися відповідно до вимог цього розділу Положення. Будь-які зміни до Ключового індикатора операційних ризиків (KRI), включаючи видалення Ключового індикатора операційних ризиків (KRI), що слідують за цим періодом, повинні погоджуватися Службою управління ризиками. Якщо Ключовий індикатор операційних ризиків (KRI) визначено як більше недоречний для Банку, Служба управління ризиками, Правління Банку можуть запропонувати Наглядовій раді Банку вилучити такий індикатор із затвердженого переліку. Після рішення Наглядової ради Банку відповідний Ключовий індикатор операційних ризиків (KRI) виключається з переліку та по ньому не здійснюється розрахунок.

7.24. Перелік Ключових індикаторів операційних ризиків (KRI) складається за формою Додатку 2 до цього Положення та має включати наступні показники та вимоги:

- Назву Ключового індикатора операційних ризиків (KRI);
- Період вимірювання;
- Частоту збору даних;
- Функцію вимірювання;
- Граничне значення /ліміт/ порогове значення індикатору (trigger);
- Аналітичну модель розрахунку;
- Критерії прийняття рішень;
- Інтерпретації індикатору;
- Частоту аналізу та звітності;
- Перегляд індикатора.

7.25. **Встановлення лімітів і порогових значень.**

Ліміти і порогові значення є границями, які використовуються в якості інструментів моніторингу індикаторів ризику. Вони встановлюються на визначених рівнях і існують як система попередження про операційні ризики для Банку. Наприклад, збільшилася схильність до ризику і виникає потреба у вжитті заходів з її мінімізації. Перевищення кожного ліміту/порогового значення подає сигнал власнику ризику про необхідність перевірки ситуації та, у разі необхідності, вжиття заходів з мінімізації/пом'якшення ризику.

7.26. Банк застосовує три стандартні типи порогових значень:

7.26.1 одностороннє високе (верхня межа): ескалація/потреба у вирішенні питання, прийняття заходу / вступає в силу, коли індикатор перевищує/дорівнює пороговому значенню;

7.26.2 одностороннє низьке (нижня межа): ескалація вступає в силу, коли індикатор знижується нижче/дорівнює пороговому значенню;

7.26.3 двостороннє (визначені нижня і верхня межі): ескалація вступає в силу, коли індикатор більше не знаходиться у межах визначеної області.

7.27. Встановлення порогових значень і лімітів без повного розуміння індикатору та його діапазону значень не надає операційної цінності. Таким чином, для встановлення порогових значень і лімітів індикаторів, необхідно зібрати дані за період, який становить хоча б 6 (шість) місяців, а краще – 1 (один) рік. Після визначення Службою управління ризиками лімітів і порогових значень Ключових індикаторів операційних ризиків (KRI), вони мають бути погоджені Правлінням Банку та затвердженні Наглядовою радою Банку, та відображати погоджений ризик-апетит по операційних ризиках. Після погодження лімітів і порогових значень будь-які зміни до них мають погоджуватись з Службою управління ризиками та затверджуватись Наглядовою радою Банку.

7.28. Тригери ескалації та мінімізація ризиків. Банк впроваджує систему тригерів для ескалації (керівник Служби управління ризиками, члени Правління, Наглядова рада Банку) у випадку порушення ліміту/порогового значення індикатора.

Тригери для ескалації є першим кроком процесу мінімізації операційного ризику, коли відповідальний працівник Служби управління ризиками має перевірити індикатор, встановити причини порушення ліміту / порогового значення. Якщо причини не суттєві (помилковий сигнал, вже вирішена проблема тощо), відповідальний працівник Служби управління ризиками має переглянути заходи з мінімізації операційних ризиків та забезпечити аналіз рентабельності потенційних заходів з мінімізації операційних ризиків, що потрібні для приведення відповідного ризику до прийнятного рівня (прийняття ризику також є способом мінімізації операційних ризиків). Якщо причини є суттєвими, інформація для прийняття рішень надається вищому керівництву.

7.29. Для визначення показників ключових індикаторів операційних ризиків (KRI), застосовується наступна процедура :

7.30. **Наглядова рада Банку:**

7.30.1 Затверджує показники Ключових індикаторів операційних ризиків (KRI).

7.30.2 Забезпечує, що встановлені в Банку ключові індикатори операційних ризиків (KRI) відповідають його бізнес-процесам.

7.30.3 Регулярно (щорічно) переглядає ключові індикатори операційних ризиків (KRI) для забезпечення їх актуальності, достовірності та своєчасності.

7.30.4 Затверджує зміни щодо впроваджених індикаторів, включаючи їх порогові значення і ліміти.

7.30.5 Щоквартально розглядає управлінську звітність по розрахунках ключових індикаторів операційних ризиків (KRI).

7.30.6 Приймає рішення щодо ескалації питань, пов'язаних з тривалим порушенням лімітів/порогових значень.

7.31. **Правління Банку :**

7.31.1 Переглядає і погоджує ключові індикатори операційних ризиків (KRI) перед їх поданням на розгляд Наглядової ради Банку.

7.31.2 Розглядає і аналізує управлінську звітність про ключові індикатори операційних ризиків (KRI), впроваджує дієві механізми контролю для зниження та упередження підвищення рівня операційного ризику, застосовує механізми альтернативних заходів для зниження операційних ризиків,

7.31.3 Переглядає та погоджує ліміти і порогові значення Ключових індикаторів операційних ризиків (KRI),

7.31.4 Впроваджує в дію заходи з мінімізації операційних ризиків, прийнятих за результатами аналізу Ключових індикаторів операційних ризиків (KRI).

7.31.5 У випадку порушення лімітів/порогових значень Ключових індикаторів операційних ризиків (KRI) забезпечує прийняття попередньо визначених заходів щодо ескалації причин порушення.

7.32. **Служба управління ризиками:**

7.32.1 Має повноваження розробляти, підтримувати і забезпечувати організацію процесу визначення, затвердження та моніторингу Ключових індикаторів операційних ризиків (KRI) для Банку.

7.32.2 Методологічно супроводжує процес впровадження та дії Ключових індикаторів операційних ризиків (KRI), надання інструкцій, навчальних матеріалів, консультацій.

7.32.3 За результатами аналізу інцидентів операційного ризику, самооцінки операційних ризиків, проведення стрес-тестування/сценарного аналізу операційних ризиків, матеріалів оцінки операційних ризиків при впровадження нових банківських процесів/продуктів, іншої доступної інформації разом з підрозділами-власниками процесів, які генерують найбільш критичні операційні ризики (ризики з оцінкою рівня «критичний», «високий», та «підвищений», у разі значної кількості такого ризику щодо всіх бізнес-процесів Банку), готує пропозиції для Спостережної ради Банку щодо вибору Ключових індикаторів операційних ризиків (KRI).

7.32.4 Щоквартально збирає дані, що необхідні для розрахунків Ключових індикаторів операційних ризиків (KRI), забезпечує впровадження процесу збору даних для вибраних індикаторів.

7.32.5 Аналізує зібрані дані з метою надання пропозицій щодо встановлення лімітів і порогових значень для кожного індикатора.

7.32.6 Щоквартально аналізує і готує, акумулює управлінську звітність про Ключові індикатори операційних ризиків (KRI), на агрегованій основі.

7.32.7 Першого місяця за звітним кварталом надає Звіт про стан Ключових індикаторів операційних ризиків (KRI) Наглядовій раді Банку та Правлінню Банку.

7.32.8 За результатами щоквартальних розрахунків показників Ключових індикаторів операційних ризиків (KRI) готує пропозиції Правлінню Банку та Наглядовій раді Банку щодо заходів з мінімізації операційних ризиків.

7.32.9 Здійснює моніторинг виконання заходів з мінімізації/пом'якшення операційних ризиків.

7.33. **Керівники підрозділів першої лінії захисту:**

7.33.1 Приймають участь у виборі індикаторів, визначають індикатори, надають пропозиції Службі управління ризиками щодо формування Ключових індикаторів операційних ризиків (KRI),

7.33.2 Надають періодичну звітність, агреговану інформацію, оперативні дані Службі управління ризиками щодо розрахунків Ключових індикаторів операційних ризиків (KRI) .

7.33.3 Банк розраховує показники Ключових індикаторів операційних ризиків (KRI) з періодичністю не рідшою ніж 1 (один) раз на квартал. Банк порівнює поточні значення Ключових індикаторів операційних ризиків (KRI) з результатами Банку за попередній період.

8. СТРЕС-ТЕСТУВАННЯ ОПЕРАЦІЙНОГО РИЗИКУ.

8.1. Для визначення потенційних втрат від реалізації операційних ризиків Банк використовує стрес тестування, а саме метод сценаріїв у відповідності до внутрішнього положення Банку, що регулює дане питання.

8.2. **Метою стрес-тестування,** що проводиться в Банку є оцінка можливості Банку компенсувати можливі критичні збитки та визначення комплексу дій, які має здійснити Банк для зниження рівня операційного ризику. Метою сценарного аналізу є забезпечення перспективного методу збору малоймовірних подій, які, можливо, не відбувались в Банку та підвищення обізнаності шляхом надання перспектив по різних типах операційного ризику та керування заходами з мінімізації /пом'якшення операційного ризику та можливого подальшого інвестування.

8.3. **Основним завданням за результатами стрес-тестування** є підготовка упереджувальних стратегічних і тактичних заходів Банку, які дозволять врегулювати проблемні або напружені ситуації, що можуть виникнути в майбутньому, та послабити вплив операційного ризику на діяльність Банку.

8.4. Проведення стрес-тестування операційного ризику має забезпечувати **досягнення таких цілей**:

8.4.1 визначення прийнятного рівня ризику, який може брати на себе Банк для забезпечення безперервної діяльності Банку та підтримання фінансової стабільності, у тому числі в довгостроковій перспективі;

8.4.2 визначення ефективності та адекватності внутрішньобанківських документів з питань управління операційним ризиком;

8.4.3 визначення розміру збитків Банку в цілому та за окремими видами операцій у разі реалізації стрес-сценаріїв, а також оцінку потенційних можливостей покрити такі збитки;

8.4.4 оцінка впливу реалізації стрес-сценаріїв на дотриманням Банком граничних значень нормативів, встановлених Національним банком України;

8.4.5 порівняння отриманих результатів з встановленим рівнем ризик-апетиту до операційного ризику;

8.4.6 визначення ступеня залежності основних типів/видів операційного ризику від окремих факторів, які обмежують або посилюють їх дію;

8.4.7 мінімізація впливу операційних ризиків на діяльність Банку шляхом розробки упереджувальних заходів для врегулювання стресових ситуацій, що можуть виникнути в майбутньому;

8.4.8 оцінка ефективності системи управління ризиками.

8.5. Фактори ризику, які використовуються при проведенні аналізу сценаріїв, базуються на історичних або гіпотетичних даних.

8.6. Стрес-тестування операційного ризику проводиться не рідше одного разу на рік. Затверджений Наглядовою радою **Перелік сценаріїв** стрес-тестування операційних ризиків ведеться, зберігається та підтримується в актуальному стані СУР.

8.7. Банк для підвищення ефективності здійснення стрес-тестування забезпечує регулярний і систематичний (**не рідше одного разу на рік**) перегляд (удосконалення) процедур проведення стрес-тестування операційного ризику, зокрема методів та стрес-сценаріїв. Банк **щорічно** виконує процедури визначення **і вибору обов'язкових сценаріїв операційного ризику.**

8.8. Управлінська звітність за сценарним аналізом стрес-тестування операційного ризику, аналізу впливу операційного ризику на капітал Банку за результатами стрес–тестування та результатів виконання запланованих заходів по результатах стрес-тестування надаються Службою управління ризиками Правлінню Банку і Наглядовій раді Банку для розроблення та вжиття відповідних заходів та прийняття управлінських рішень, щодо зменшення впливу потенційних операційних ризиків та уникнення/мінімізації втрат/фінансових, матеріальних, інтелектуальних, кадрових, збільшення капіталу Банку тощо.

9. РИЗИК-АПЕТИТ ДО ОПЕРАЦІЙНОГО РИЗИКУ.

9.1. Ризик-апетит до операційного ризику - це зміни в результатах діяльності Банку, **які Банк готовий прийняти** відповідно до його бізнес моделі та стратегічних цілей, це обмеження щодо операційного ризику, згідно з якими Банк має діяти під час впровадження своєї діяльності та стратегії, кількісний показник ризик-апетиту до операційного ризику за своє суттю визначає максимальний обсяг збитків від подій операційного ризику протягом наступних 12 місяців.

9.2. Впровадження ризик-апетиту операційного ризику є важливим кроком в організації щоденного процесу управління операційного ризику.

9.3. Розмір Ризик- апетиту операційного ризику розраховується в залежності від величини мінімального розміру операційного ризику, стратегічних цілей Банку, показників бюджету та інформації щодо історичних середньорічних втрат від інцидентів операційного ризику за попередніх 12 кварталів та результати стрес-тестування операційних ризиків.

9.4. Банк визначає загальний рівень Ризик апетиту до операційного ризику як комбінацію кількісних та якісних показників.

9.4.1 До кількісних показників Банк відносить :

- розмір Ризик-апетиту до операційного ризику визначений у тисячах гривень (заокруглюється до цілого числа) в межах 10 % показника мінімального розміру операційного ризику. При цьому розмір розрахованого показника Ризик-апетиту до операційного ризику може коригуватись в сторону збільшення на величину втрат від інцидентів операційного ризику (середній річний показник розрахований за показниками 12 попередніх кварталів на дату затвердження Ризик-апетиту) та/або розрахункову величину прогнозних втрат від реалізації всіх затверджених сценаріїв операційного ризику (станом на дату затвердження Ризик- апетиту).
- Розрахунковий розмір Ризик-апетиту може збільшуватись на суму перевищення розміру Ризик апетиту :
- Середнього показника втрат від інцидентів операційного ризику
- 20 % суми прогнозних втрат від реалізації всіх затверджених сценаріїв операційного ризику.

При цьому за рішенням Наглядової ради при коригуванні може обиратись один або два коригуючих показника.

9.4.2 До якісних показників Ризик-апетиту до операційного ризику Банк відносить:

- повноту внутрішніх документів з управління ризиками, які відповідають бізнес-моделі та стратегії Банку;

- наявності опису процесів Банку, що визначають ключові точки, в яких Банк може наражатися на суттєві операційні ризики;
- достатнього рівня кваліфікації персоналу Банку, що забезпечують виконання процесів з управління ризиками;
- достатність та належне функціонування інформаційних систем Банку щодо управління операційними ризиками, необхідних для підтримки процесів;
- наявність в інформаційних системах щодо управління операційними ризиками Банку повних та якісних даних, що забезпечують належну оцінку величини ризиків.
- наявності контролю за дотриманням норм (комплаєнс), кодексу поведінки (етики), запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

9.4.3 Оцінку якісних показників ризик-апетиту до операційного ризику Банк розраховує із застосуванням критеріїв оцінки, яка визначається у балах та розраховується відповідно Додатку 3 до цього Положення.

9.4.4 Розрахунок дотримання ризик-апетиту операційного ризику по якісних показниках здійснюється Службою управління ризиками шляхом оцінки кожного з якісних показників ризик - апетиту до операційного ризику (Додаток) застосовуючи професійне мотивоване судження щодо рівня операційного ризику.

9.4.5 До кожної оцінки якісного показника застосовується ваговий показник (Wi) впливу для узагальнення результатів та визначення загальної оцінки якісних показників ризик апетиту:

№	Якісний показник	Оцінка якісного показника ризик апетиту /бали	Питома вага показника (Wi)	Результат дотримання якісних показників ризик апетиту (с.3*с.4)/бали
1	**2**	**3**	**4**	**5**
1	повнота внутрішньобанківських документів з управління ризиками, які відповідають бізнес моделі банку	Від 1 до 5	15%	
2	наявність опису процесів банку, що визначають ключові точки, в яких банк може наражатися на суттєві ризики	Від 1 до 5	15%	
3	достатність рівня кваліфікації персоналу банку, що забезпечують виконання процесів з управління ризиками	Від 1 до 5	15%	
4	достатність та належного функціонування інформаційних систем банку щодо управління ризиками, необхідних для підтримки процесів	Від 1 до 5	10%	
5	наявність в інформаційних системах щодо управління ризиками банку повних та якісних даних, що забезпечують належну оцінку величини ризиків	Від 1 до 5	20%	
6	наявність контролю за дотриманням норм (комплаєнс), кодексу поведінки (етики), запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення	Від 1 до 5	25%	

Разом загальна оцінка якісних показників ризик апетиту до ОР		100%	

В результаті Загальна оцінка якісних показників ризик-апетиту до операційного ризику визначається за наступними параметрами:

До 1 балу включно	**Якісні показники з низьким ризиком**
вище 1 балу до 2 включно	**Якісні показники з помірним ризиком**
вище 2 балів до 3 включно	**Якісні показники з підвищеним ризиком**
вище 3 балів до 4 включно	**Якісні показники з високим ризиком**
Більше 4-х балів	**Якісні показники в критичному стані ризику**

9.5. Ризик-апетит до операційного ризику є основою для встановлення лімітів щодо кожного виду/типу операційного ризику. Банк встановлює ліміти до 1-ї та 2 –ї категорії деталізації видів операційного ризику, які Банк вважає для себе значними та у межах ризик – апетиту. Кількісні показники лімітів операційного ризику визначають максимальний обсяг збитків від подій операційного ризику протягом наступних 12 місяців.

Збір даних для розрахунку лімітів операційного ризику здійснює Служба управління ризиками.

При затвердженні лімітів операційного ризику можуть визначатися підрозділи Банку, що мають їх контролювати. Загальний контроль за дотриманням лімітів здійснює Служба управління ризиками.

Наглядова рада може делегувати Голові Правління Банку повноваження щодо погодження авторизованих перевищень лімітів операційного ризику, при цьому запроваджується періодична звітність про випадки дотримання та перевищення встановлених лімітів.

9.6. Банк здійснює регулярний перегляд величини Ризик-апетиту та лімітів щодо кожного виду/типу операційного ризику не рідше одного разу на рік, у строк до 01 червня звітного року паралельно з розрахунком показника мінімального розміру операційного ризику.

За поданням Служби управління ризиками (**Додаток 4** до цього Положення) Ризик -апетит до операційного ризику та розмір лімітів операційного ризику затверджується Наглядовою радою Банку після погодження Правлінням Банку.

9.7. У разі суттєвих змін у діяльності /стратегії Банку, появи нових продуктів протягом звітного року Служба управління ризиками може ініціювати питання коригування величини Ризик апетиту операційного ризику.

9.8. Правління Банку, Служба управління ризиками та керівники підрозділів забезпечують належний контроль дотримання розміру Ризик – апетиту до операційного ризику, контроль дотримання лімітів операційного ризику. Для обмеження впливу операційних ризиків на діяльність Банку та дотримання Ризик- апетиту Банком впроваджуються Ключові індикатори операційного ризику.

9.9. СУР періодично щоквартально готує управлінську звітність Наглядовій раді та Правлінню Банку щодо результатів контролю дотримання розміру Ризик-апетиту операційного ризику та лімітів операційного ризику, при цьому при аналізі ризик-профілю Банку (аналізуються матеріали внутрішнього подальшого контролю, результати інцидентів операційного ризику, результати сценарного аналізу операційних ризиків, тощо) здійснюється експертиза дотримання Ризик-апетиту до операційного ризику.

9.10. При впровадженні нових продуктів висновок Служби управління ризиками має включати інформацію про те, чи знаходиться новий продукт в межах затвердженого Ризик-апетиту до операційних ризиків.

9.11. 7.12. Наглядова рада та Правління Банку за результатами розгляду управлінської звітності приймають відповідні управлінські рішення, в т.ч. щодо прийняття відповідних заходів для мінімізації ризиків, зміни технологій, дисциплінарного характеру тощо.

9.12. 7.13. Контроль за виконанням рішень керівних органів, щодо Ризик –апетиту та лімітів операційного ризику покладається на Службу управління ризиками за загальними процедурами, передбаченими цим Положенням.

9.13.

10. РОЗРАХУНОК МІНІМАЛЬНОГО РОЗМІРУ ОПЕРАЦІЙНОГО РИЗИКУ

10.1. Мінімальний розмір операційного ризику повинен забезпечуватися відповідним рівнем капіталу.

10.2. Банк розраховує мінімальний розмір операційного ризику станом на перше січня кожного року не пізніше останнього робочого дня травня поточного року на підставі даних річної фінансової звітності, перевіреної та підтвердженої аудитором.

10.3. Банк здійснює розрахунок за такою формулою:

ОР = КБІ·ВМЗ, де ОР – розмір операційного ризику;

КБІ – компонент бізнес-індикатора;

ВМЗ – внутрішній мультиплікатор збитків (втрат) від подій операційного ризику. Банк для розрахунку мінімального розміру операційного ризику застосовує значення ВМЗ, що дорівнює 1, при цьому показник ВМЗ може переглядатися Національним банком України з урахуванням результатів банківського нагляду щодо перевірки повноти та якості накопичених банками статистичних даних про збитки (втрати) від подій операційного ризику.

10.4. Банк розраховує КБІ за такою формулою: КБІ = БІ·α,

де БІ – бізнес-індикатор;

α – граничний коефіцієнт зважування. Для розрахунку КБІ банк застосовує значення α, що дорівнює 0,15.

10.5. Банк розраховує значення БІ за такою формулою: БІ = КПД/В + СК + ФК,

де КПД/В – компонент чистих процентних доходів/витрат та доходу у вигляді дивідендів;

СК – сервісний компонент;

ФК – фінансовий компонент.

10.6. Банк уключає до розрахунку КПД/В, СК, ФК доходи та витрати банку за складовими, визначеними у таблиці:

Складові компонентів КПД/В, СК, ФК

№ з/п	Код рядка	Компонент	Показник	Залишки за балансовим рахунком/групою/розділом
1	2	3	4	5
1	1	Компонент чистих процентних доходів/витрат та доходу у вигляді дивідендів (далі - КПД/В)		
2	1.1		Процентні доходи (далі - ПД)	1. Група 600 Процентні доходи за коштами, що розміщені в Національному банку України 2. Група 601 Процентні доходи за коштами, що розміщені в інших банках 3. Група 602 Процентні доходи за кредитами, що надані суб'єктам господарювання, які обліковуються за амортизованою собівартістю 4. Група 603 Процентні доходи за придбаними (створеними) знеціненими кредитами, що надані суб'єктам господарювання, які обліковуються за амортизованою собівартістю 5. Група 604 Процентні доходи за кредитами, що надані органам державної влади та органам місцевого

				самоврядування, які обліковуються за амортизованою собівартістю 6. Група 605 Процентні доходи за кредитами, що надані фізичним особам, які обліковуються за амортизованою собівартістю 7. Група 606 Процентні доходи за придбаними (створеними) знеціненими кредитами, що надані фізичним особам, які обліковуються за амортизованою собівартістю 8. Група 607 Процентні доходи за кредитами, що надані суб'єктам господарювання, які обліковуються за справедливою вартістю через інший сукупний дохід 9. Група 608 Процентні доходи за кредитами, що надані органам державної влади, які обліковуються за справедливою вартістю через інший сукупний дохід 10. Група 609 Процентні доходи за кредитами, що надані суб'єктам господарювання та органам влади, які обліковуються за справедливою вартістю через прибутки/збитки 11. Група 610 Процентні доходи за кредитами, що надані фізичним особам, які обліковуються за справедливою вартістю через інший сукупний дохід 12. Група 611 Процентні доходи за кредитами, що надані фізичним особам, які обліковуються за справедливою вартістю через прибутки/збитки 13. Група 612 Процентні доходи за операціями з цінними паперами 14. Група 614 Інші процентні доходи 15. Рахунок 6395П Дохід від оперативного лізингу (оренди)
3.	1.2		Процентні витрати (далі - ПВ)	1. Група 700 Процентні витрати за коштами, що отримані від Національного банку України 2. Група 701 Процентні витрати за коштами, що отримані від інших банків 3. Група 702 Процентні витрати за операціями із суб'єктами господарювання, які обліковуються за амортизованою собівартістю 4. Група 703 Процентні витрати за коштами бюджету та позабюджетних фондів України 5. Група 704 Процентні витрати за операціями з фізичними особами 6. Група 706 Процентні витрати за кредитами, що отримані від міжнародних та інших організацій 7. Група 707 Процентні витрати за операціями з небанківськими фінансовими установами 8. Група 712 Процентні витрати за цінними паперами власного боргу 9. Група 714 Інші процентні витрати Рахунок 7395А Витрати на оперативний лізинг (оренду)

4	1.3		Дохід у вигляді дивідендів (далі - ДД)	Група 630 Дохід у вигляді дивідендів
5	2	Сервісний компонент (далі - СК)		
6	2.1		Комісійні доходи (далі - КД)	1. Група 650 Комісійні доходи за операціями з банками 2. Група 651 Комісійні доходи за операціями з клієнтами
7	2.2		Комісійні витрати (далі - КВ)	Група 750 Комісійні витрати
8	2.3		Інші операційні доходи(далі - ІОД)	Група 631 Дохід від інвестицій в асоційовані і дочірні компанії Група 633 Дохід від модифікації фінансових зобов'язань Група 634 Дохід від припинення визнання фінансових активів Група 635 Дохід від припинення визнання фінансових зобов'язань Група 639 Інші операційні доходи за виключенням рахунку 6395П Дохід від оперативного лізингу (оренди) 6. Рахунок 6490П Позитивний результат від продажу нематеріальних активів та основних засобів
9	2.4		Інші операційні витрати (далі - ІОВ)	1. Група 730 Витрати на телекомунікації 2. Група 731 Витрати від інвестицій в асоційовані і дочірні компанії 3. Група 733 Витрати від модифікації фінансових зобов'язань 4. Група 734 Витрати від припинення визнання фінансових активів 5. Група 735 Витрати від припинення визнання фінансових зобов'язань 6. Група 739 Інші операційні витрати за виключенням рахунку 7395А Витрати на оперативний лізинг (оренду) Рахунок 7706АП Відрахування в банківські резерви на покриття ризиків і втрат (в частині покриття операційних ризиків)
10	3	Фінансовий компонент (далі - ФК)		
11	3.1		Чистий прибуток/збиток за торговою книгою (далі - ЧТК)	Розділ 62 Результат від переоцінки та від операцій купівлі-продажу

12	3.2		Чистий прибуток/збиток за банківською книгою (далі - ЧБК)	Розділ 62 Результат від переоцінки та від операцій купівлі-продажу

Пояснення до таблиці:

У колонці 5 таблиці зазначено залишки за балансовим рахунком/групою/розділом Плану рахунків бухгалтерського обліку банків України, затвердженого постановою Правління Національного банку України від 11 вересня 2017 року № 89 (зі змінами).

Банк здійснює розподіл результату від переоцінки та від операцій купівлі-продажу між торговою (код рядка 3.1 таблиці) та банківською (код рядка 3.2 таблиці) книгами відповідно до вимог Положення № 64 та внутрішньобанківських документів.

10.7. Банк розраховує розмір операційного ризику на підставі річних даних файлу А4Х "Дані про коригуючі обороти за результатами звітного періоду, року та залишки на рахунках" (далі – файл А4Х), що складається та подається до Національного банку відповідно до Правил організації статистичної звітності, що подається до Національного банку України, затверджених постановою Правління Національного банку України від 13 листопада 2018 року № 120 (зі змінами).

10.8. Банк розраховує розмір операційного ризику на підставі річних даних файлів А4Х за три останні звітні роки.

10.9. Банк розраховує КПД/В за такою формулою:

$$\text{КПД/В} = \frac{\sum_{i=1}^{n}[|\text{ПД} - \text{ПВ}|]_i}{n} + \frac{\sum_{i=1}^{n}\text{ДД}_i}{n},$$

де $[|\text{ПД}- \text{ПВ}|]_i$ - абсолютна величина різниці процентних доходів та процентних витрат за *i*-й звітний рік (без врахування знака);

ДД_i - дохід у вигляді дивідендів за *i*-й звітний рік; n - кількість років, за які здійснюється розрахунок.

10.10. Банк розраховує СК за такою формулою:

$$\text{СК} = \max\left(\frac{\sum_{i=1}^{n}\text{КД}_i}{n}; \frac{\sum_{i=1}^{n}\text{КВ}_i}{n}\right) + \max\left(\frac{\sum_{i=1}^{n}\text{ІОД}_i}{n}; \frac{\sum_{i=1}^{n}\text{ІОВ}_i}{n}\right),$$

де

КД_i - комісійні доходи за *i*-й звітний рік;

КВ_i - комісійні витрати за *i*-й звітний рік; ІОД_i - інші операційні доходи за *i*-й звітний рік; ІОВ_i - інші операційні витрати за *i*-й звітний рік.

10.11. Банк розраховує ФК за такою формулою:

$$\text{ФК} = \frac{\sum_{i=1}^{n}|\text{ЧТК}|_i}{n} + \frac{\sum_{i=1}^{n}|\text{ЧБК}|_i}{n}.$$

де $|\text{ЧТК}|_i$ - абсолютна величина чистого прибутку/збитку за торговою книгою за *i*-й звітний рік (без врахування знака); $|\text{ЧБК}|_i$ - абсолютна величина чистого прибутку/збитку за банківською книгою за *i*-й звітний рік (без врахування знака).

10.12. **Щороку, не пізніше 31 травня** Служба управління ризиками надає на погодження Правлінню та затвердження Наглядовій раді розрахунок показника мінімального рівня операційного ризику та інформацію щодо впливу операційного ризику на капітал Банку.

11. ІНФОРМАЦІЙНІ СИСТЕМИ (БАЗИ) ДЛЯ НАКОПИЧЕННЯ, ЗБЕРІГАННЯ ТА ОБРОБЛЕННЯ ДАНИХ

11.1. Банк створює інформаційні системи, які мають бути адекватними для вимірювання, оцінки та звітування про розмір, структуру та якість здійснюваних Банком операцій у розрізі видів операційних ризиків, продуктів та контрагентів.

З метою забезпечення ефективності та адекватності функціонування системи управління ризиками інформаційні системи Банку мають щонайменше забезпечувати ідентифікацію, оцінку, моніторинг та контроль операційних ризиків на всіх організаційних рівнях.

11.2. В Банку впроваджується система накопичення, зберігання, оцінки, вимірювання і управління операційним ризиком.

11.3. Інформаційне забезпечення операційної діяльності Банку включає програмно-технічні комплекси автоматизації банківської діяльності, взаємозв'язки для обміну інформацією між ними, телекомунікаційну інфраструктуру, внутрішні нормативні документи та інструкції щодо їх застосування.

11.4. Відповідальним підрозділом за інформаційне забезпечення діяльності Банку є Управління інформаційних технологій.

11.5. Одним із основних засобів програмно-технічного комплексу за допомогою якого здійснюється операційна діяльність Банку є програмно-технічний комплекс автоматизації банківської діяльності – система автоматизації Банку "Б-2" (далі - САБ Б2), яка відповідає функціональним, технологічним вимогам НБУ, а також вимогам щодо інформаційної безпеки та забезпечує основні вимоги, зокрема:

11.5.1 можливість детального аналізу всієї вхідної інформації до часу її відображення в регістрах бухгалтерського обліку;

11.5.2 можливість перегляду етапів проходження операції в такому порядку:

- регістри аналітичного обліку;
- регістри синтетичного обліку;
- звітність та в зворотному порядку;

11.5.3 надійність та здатність до швидкого відновлення робочого процесу в разі виникнення технічних або програмних збоїв. Наявність резервного накопичення та зберігання всієї інформації для забезпечення відновлення роботи Банку внаслідок виникнення форс мажорних обставин або в разі ліквідації Банку;

11.5.4 автоматизація роботи з електронними архівами системи. Можливість ознайомлення з будь якою потрібною архівною інформацією протягом терміну її зберігання, у тому числі в розрізі підрозділів Банку. У цьому разі виконуються лише операції з перегляду, пошуку та формування вихідних документів;

11.5.5 архівація – регламентна або позапланова (у разі потреби).

11.6. За допомогою САБ Б2 відбувається:

11.6.1 хронологічне та систематичне відображення всіх операцій на аналітичних рахунках бухгалтерського обліку на підставі первинних документів;

11.6.2 своєчасне та повне відображення всіх операцій Банку;

11.6.3 дотримання правил складання і подання фінансової, статистичної, управлінської та податкової (тощо) звітності;

11.6.4 взаємозв'язок даних синтетичного та аналітичного обліку. Банк у разі невідповідності структури рахунків аналітичного і синтетичного обліку забезпечує їх взаємозв'язок за допомогою перехідних таблиць;

11.6.5 накопичення та систематизація даних обліку в розрізі економічних показників, потрібних для складання звітності;

11.6.6 автоматизований розрахунок економічних показників, що визначені відповідними методиками НБУ;

11.6.7 можливість оперативного аналізу фінансової діяльності Банку в розрізі бізнес-напрямків діяльності, структурних/відокремлених підрозділів, продуктів, контрагентів, видів активів, галузей, регіонів тощо;

11.6.8 інтегрованість з електронними системами інформаційного обміну НБУ;

11.6.9 інтегрованість з іншими складовими системи автоматизації Банку, можливість отримувати інформацію про здійснені операції в будь-якому розрізі;

11.6.10 уніфікація програмно-технічних рішень та технологій для структурних підрозділів Банку;

11.6.11 можливість нарощування функціональних характеристик програмного забезпечення, а також його адаптація в разі зміни законодавчої бази щодо облікових операцій.

12. СИСТЕМА УПРАВЛІНСЬКОЇ ІНФОРМАЦІЇ ТА ЗВІТУВАННЯ ЗА ОПЕРАЦІЙНИМИ РИЗИКАМИ.

12.1. **Інформаційні системи Банку мають забезпечувати:**

12.1.1 звітування про розмір операційного ризику, його оцінку, інформацію про втрати від операційного ризику, про величини Ключових індикаторів операційного ризику (KRI), про результати стрес-тестування, про дотримання ризик –апетиту і вплив операційного ризику на капітал Банку шляхом підготовки відповідної звітності;

12.1.2 вчасне та постійне інформування Наглядової ради Банку та Правління Банку, керівників підрозділів про профіль ризику Банку, додаткові потреби у внутрішньому капіталі для його покриття та про додаткові контрольні процедури Банку;

12.1.3 регулярні і зрозумілі процеси щодо обміну та отримання інформації з питань управління операційним ризиком;

12.1.4 участь керівників Банку в процесі прийняття рішень щодо управління операційними ризиками.

12.1.5 10.2. Банк забезпечує належне документування процедур (правил, методик, політик тощо), які встановлюють вимоги до процесів накопичення даних про розміри операційного ризику, на які наражається Банк, і звітування про них.

12.1.6 10.2.1. Усі зацікавлені сторони Банку, що приймають рішення/або мають виконати відповідні заходи з мінімізації операційного ризику (Наглядова рада Банку, Правління Банку, комітети Наглядової ради, Правління, інші колегіальні органи, керівники підрозділів), повинні вчасно і належним чином бути повідомлені про відповідну інформацію, пов'язану з окремими інструментами, які використовуються при управлінні операційним ризиком. Банк визначає форми звітності з питань управління операційним ризиком з урахуванням потреб конкретного користувача: Наглядової ради Банку, Правління Банку, підрозділів, працівників Банку, Служби внутрішнього аудиту, зовнішнього аудиту, наглядових/регуляторних органів тощо.

12.2. 10.3. Банк запроваджує ефективний обмін інформацією за різними напрямами, а саме:

12.2.1 вертикально знизу – вгору, щоб Наглядова рада Банку і Правління Банку знали і усвідомлювали операційні ризики, на які наражається Банк, та адекватно реагували, організовували та контролювали роботу Банку. Такий принцип реалізовано через подання регулярної управлінської інформації про операційний ризик керівництву Банку (Наглядова рада Банку, Правління Банку) від Служби управління ризиками та Служби внутрішнього аудиту в межах планових перевірок.

12.2.2 10.3.2. вертикально згори – вниз, щоб інформація про стратегію та політику Банку з управління операційними ризиками доводилася до відома всіх управлінських рівнів та інших працівників, яких залучено до управління інформаційною безпекою та обміном інформацією. Такий принцип реалізовано через доступ до внутрішньої нормативної бази, розміщеної в діючій системі електронного документообігу та рішень керівних колегіальних органів щодо визначення зобов'язань секретарів таких колегіальних органів (в т.ч. Корпоративного секретаря) доводити інформацію до працівників Банку.

12.2.3 10.3.3. горизонтально, щоб інформація, якою володіє один структурний підрозділ Банку, надавалась іншому структурному підрозділу, якому вона необхідна для виконання своїх функцій. Такий принцип реалізовано через механізм розробки та впровадження внутрішніх нормативних документів (політик, положень, технологічних карт, регламентів), рішень колегіальних органів (Наглядова рада Банку, Правління Банку, КБІТ), де передбачається

порядок надання та отримання інформації, необхідної для вжиття заходів для управління операційним ризиком.

10.4. Процес управління операційними ризиками в Банку здійснюється на підставі сформованої відповідними підрозділами звітності:

№	Назва Звіту	Періодичність подання	Кому подається	Відповідальний орган/ підрозділ
1	Звіт про результати самооцінки операційних ризиків бізнес-процесів	Щорічно 1 кв. року наступного за звітним (протягом 2-х місяців з дати впровадження **нового** бізнес-процесу)	Наглядова рада Банку Правління Банку	Служба управління ризиками
2	Звіт про результати самооцінки операційних ризиків/ Карта оцінки операційного ризику у бізнес – процесі	Щорічно до 15 лютого року наступного за звітним (протягом 45 днів з дати впровадження **нового** бізнес-процесу)	Служба управління ризиками	Структурні підрозділи
3	Узагальнені дані про події операційного ризику, накопичених у базі внутрішніх подій операційного ризику	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
4	Звіт про значні події операційного ризику, результатів дослідження їх причин та заходів щодо запобігання таким подіям у майбутньому	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
5	Звіт про складені плани заходів та про виконання планів заходів по мінімізації /зниженню рівня операційного ризику/ результати моніторингу планів заходів (у разі наявності планів)	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
6	Звіт про виконання планів заходів по мінімізації/зниженню рівня операційного ризику (у разі наявності планів)	Щоквартально до 15 числа місяця наступного за звітним кварталом	Служба управління ризиками	Структурні підрозділи
7	Звіт «Розрахунки Ключових індикаторів операційних ризиків (KRI)	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками

8	Пропозиції для Наглядової ради Банку щодо вибору Ключових індикаторів операційних ризиків (KRI)	Щорічно	Наглядова рада Банку Правління Банку	Служба управління ризиками
9	Розрахунок/Інформація, що необхідна для розрахунків Ключових індикаторів операційних ризиків (KRI)	Щоквартально до 15 числа місяця наступного за звітним кварталом	Служба управління ризиками	Структурні підрозділи
10	План проведення сценарного аналізу операційних ризиків на ____ рік та звіт про методи проведення стрес – тестування регулярний і систематичний перегляд (удосконалення) процедур проведення стрес-тестування операційного ризику, зокрема методів та стрес сценаріїв.	Щорічно	Наглядова рада Банку Правління Банку	Служба управління ризиками
11	Стрес-тестування (сценарний аналіз) операційного ризику за темою____	Щорічно	Наглядова рада Банку Правління Банку	Служба управління ризиками
12	ПЛАН ЗАХОДІВ по мінімізації/зниженню рівня операційного ризику за результатами стрес-тестування операційного ризику	За результатами розгляду сценаріїв операційного ризику	Наглядова рада Банку Правління Банку	Служба управління ризиками
13	ЗВІТ про складені плани заходів та про виконання планів заходів по мінімізації /зниженню рівня операційного ризику/ результати моніторингу планів заходів за результатами стрес-тестування операційного ризику	Щоквартально, протягом кварталу за звітним кварталом	Наглядова рада Банку Правління Банку	Служба управління ризиками
14	Розрахунок **профілю операційного ризику**	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
15	Оцінка операційного ризику - «Карта загальної оцінки операційного ризику / розрахунок профілю ризику	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками

15.1.	Результати контролю дотримання кількісних та якісних показників Ризик-апетиту до операційного ризику та лімітів операційного ризику,	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
15.2.	Інформація щодо впливу операційного ризику на капітал Банку	Щоквартально	Наглядова рада Банку Правління Банку	Служба управління ризиками
15.3.	Розрахунок мінімального розміру операційного ризику та інформація про вплив операційного ризику на капітал Банку та визначення Ризик апетиту до операційного ризику та лімітів щодо кожного виду/типу операційного ризику Банку	Щорічно до 31.05.	Наглядова рада Банку Правління Банку	Служба управління ризиками

13. СИСТЕМА ВНУТРІШНЬОГО КОНТРОЛЮ.

13.1. Система внутрішнього контролю за операційними ризиками будується на впровадженні обов'язкової періодичної звітності за операційними ризиками та чітким розподіленням обов'язків при виявленні, оцінці, моніторингу, контролі, звітуванні за операційним ризиком.

13.2. **Наглядова рада відповідає за здійснення нагляду та оцінкою ефективності системи управління операційним ризиком.**

13.3. **Служба внутрішнього аудиту** відповідає за своєчасне надання Службі управління ризиками Аудиторських звітів за результатами внутрішніх аудиторських перевірок стосовно виявлених операційних ризиків у Банку та незалежну оцінку операційних ризиків Банку.

13.4. **Служба комплаєнсу** відповідає за своєчасне надання Службі управління ризиками звітності за результатами подальшого внутрішнього контролю по виявлених операційних ризиків у Банку, та виявлених операційних ризиків при управління комплаєнс-ризиком.

13.5. **Правління** відповідальне за безпосереднє дотримання законодавства України та внутрішніх процедур Банку, та забезпечує реалізацію цього Положення, сприяє звітуванню перед Наглядовою радою Банку по питаннях управління операційним ризиком, виконує задачі Наглядової ради Банку щодо приведення у відповідність системи управління операційним ризиком за матеріалами проведених перевірок, тощо.

13.6. **Служба управління ризиками** несе функціональну відповідальність за:

- координацію роботи з управління операційним ризиком,
- збір інформації про інциденти та операційні ризики,
- за здійснення оцінки операційного ризику, в т.ч. по нових продуктах,
- моніторинг ризику та контроль за виконанням прийнятих заходів щодо операційного ризику,
- складання адекватної управлінської звітності щодо операційного ризику
- за розробку, підтримку цього Положення та інших документів щодо операційних ризиків в актуальному стані та відповідності їх іншим внутрішнім нормативним документам Банку.

13.7. **Управління інформаційної безпеки** відповідає за своєчасне внесення інформації про інциденти інформаційної безпеки в базу подій/інцидентів операційного ризику

13.8. **Керівники структурних/відокремлених підрозділів** контролюють та відповідають за:

- дотримання норм, правил, процедур, регламентованих правовстановлюючими, внутрішніми нормативними та організаційно - розпорядчими документами Банку;
- за регулярне проведення моніторингу змін законодавства та нормативно – правових актів НБУ, ФГВФО, НКЦПФР, ДПС та інших Регуляторів, що стосуються діяльності очолюваних підрозділів;
- внесення змін до внутрішніх нормативних документів, погодження та затвердження таких змін згідно внутрішніх нормативних документів Банку у встановлені строки відповідно до компетенцій;
- негайне інформування Служби управління ризиками про виявлення операційного ризику або вірогідність настання операційного ризику, надання звітності/інформації передбаченої внутрішніми нормативними документами щодо операційного ризику,
- надання Службі управління ризиками інформації про інциденти операційних ризиків.
- Контроль за правильністю застосування цього Положення покладається на Службу управління ризиками.

13.9. Бази даних інцидентів операційних ризиків, інформація щодо службових перевірок/службових розслідувань носять конфіденційний характер та повинні бути захищені, права доступу до баз даних інцидентів надаються за погодженням Служби управління ризиками.

13.10. Загальний контроль за своєчасним наданням інформації про операційний ризик Службі управління ризиками відповідно до процедур визначених цим Положенням несуть керівники підрозділів відповідних підрозділів.

13.11. Контроль за функціонуванням та оцінкою операційного ризику проводиться згідно нормативних документів, що описують систему управління операційним ризиком.

13.12. Основні види ризиків та контролів, що виникають в процесі управління операційними ризиками зазначені в нижче приведеній таблиці:

№	Вид ризику	Фактор ризику / ідентифікатор ризику/ інформація, що підтверджує настання ризику	Зміст/короткий опис процедур контролю /вид внутрішнього контролю /контрольна процедура*/	Періодичність здійснення процедури контролю	Перший рівень контролю колегіальний орган/ підрозділ / ризик/ комплаєнс-координатор				Другий /третій рівень контролю	Вид контролю
					самостійний контроль	подвійний контроль	автоматизований контроль	колегіальний контроль куратор/член Правління		
1	*Комплаєнс ризик*	Недотримання вимог законодавства України, нормативно-правових актів НБУ щодо наявності внутрішніх нормативних документів, регламентуючих процес та відповідності ВНД законодавству / /невірна/застаріла методологія виконання операції/процесу, недотримання кореляції ВНД між собою	Моніторинг змін законодавства України, нормативно-правових актів НБУ, актуалізація внутрішніх нормативних документів, що регламентують здійснення управління операційним ризиком , не рідше 1 разу на 1 рік відповідно до внутрішніх процедур. Внутрішній контроль за актуалізацією ВНД.	Постійно В межах плану перевірок СВА	Керівники підрозділів власники процесів	Управління методології та процесів		Член Правління Банку	Служба управління ризиками Служба комплаєнсу СВА	Попередній Поточний Подальший
2	*Комплаєнс ризик*	Порушення норм законодавства, регуляторного середовища, правил, внутрішньобанківських документів щодо операційного ризику	Контроль керівника, внутрішня ревізія, Управлінська звітність, відповідальність в посадових інструкціях	Постійно	Керівники підрозділів, члени Правління – /ризик/комплаєнс-координатори			Член Правління Банку	Служба управління ризиками Служба комплаєнсу СВА	Попередній Поточний Подальший

3	*Комплаєнс ризик Операційний ризик*	Порушення вимог законодавства та нормативно правових актів НБУ з питань управління операційним ризиками	Здійснення попереднього, поточного та подальшого контролю відповідно ВНД Контроль керівника	Постійно	Структурні /відокремлені підрозділи Ризик комплаєнс координатори			Член Правління Банку	Служба управління ризиками Служба комплаєнсу	Попередній Поточний Подальший
4	Комплаєнс ризик Операційний ризик	Порушення встановлених термінів подання інформації по операційних ризиках	Контроль керівника, внутрішня ревізія, суцільна та послідовна нумерація створюваних документів	Постійно				Член Правління Банку	Служба управління ризиками Служба комплаєнсу	Попередній Поточний
5	Комплаєнс ризик Операційний ризик	Порушення вимог внутрішніх нормативних документів з питань управління операційним ризиком	Здійснення попереднього, поточного та подальшого контролю відповідно ВНД Навчання персоналу	Постійно	Структурні /відокремлені підрозділи Ризик координатори			Член Правління Банку	Служба управління ризиками Служба комплаєнсу	Попередній Поточний Подальший
7	Комплаєнс ризик	Отримання або провокація хабаря //Хабарі / “відкати”, вимагання	▪Стандартизація продукту, ▪розгляд кредитної пропозиції /продукту різними підрозділами контроль керівника, ▪Впровадження механізму конфіденційного повідомлення про порушення	Постійно	Структурні /відокремлені підрозділи БГ Ризик/комплаєнс -координатори			Член Правління Банку	Служба комплаєнсу	Попередній Поточний Подальший

8	*Комплаєнс ризик*	Не надання інформації про інциденти та випадки шахрайства	Контроль керівника Звірка даних, моніторинг та реєстрація документів у спеціальних журналах	Постійно	Начальники підрозділів /ризик координатори			Член Правління Банку	Служба управління ризиками	Попередній Поточний Подальший
9	*Комплаєнс ризик*	свідомі порушення, заборонені практики, неналежна діяльність, неприйнятна поведінка тощо	Контроль керівника ▪Налагодження процесу перевірки персоналу при прийомі на роботу, ▪Навчання проведення навчання персоналу стосовно виконання кодексів корпоративного управління етики Впровадження механізму конфіденційного повідомлення про порушення впровадження етичних та моральних стандартів	Постійно	Начальники підрозділів /ризик/комплаєнс координатори			Член Правління Банку	Служба комплаєнсу	Поточний Подальший

14. ПРИКІНЦЕВІ ПОЛОЖЕННЯ.

14.1. Це Положення набирає чинності з моменту його затвердження Наглядовою радою Банку та діє до його скасування або прийняття нового внутрішнього нормативного документу, який регулює аналогічні питання, у встановленому законодавством та внутрішніми нормативними документами Банку порядку.

14.2. Зміни та доповнення до цього Положення оформлюються окремим документом або шляхом його викладення у новій редакції. Прийняття нової редакції Положення автоматично призводить до припинення дії попередньої редакції.

14.3. Дія цього Положення припиняється з моменту прийняття відповідного рішення Наглядової ради Банку.

14.4. У разі невідповідності будь-якої частини цього Положення законодавству України, у тому числі у зв'язку з прийняттям нових нормативно-правових актів, це Положення буде діяти лише в тій частині, що не суперечитиме законодавству України.

14.5. Всі питання, не врегульовані цим Положенням, вирішуються у формах, що не суперечать здоровому глузду, в порядку, передбаченому іншими внутрішніми документами Банку та на підставі законодавства України.

14.6. Відповідальність за актуалізацію цього Положення покладається на Службу управління ризиками. У міру необхідності, документ повинен переглядатися як мінімум 1 раз на 1 рік.

14.7. Пропозиції щодо змін та доповнень до цього Положення підрозділи Банку направляють на адресу Служби управління ризиками.

14.8. Це Положення публікується у формі, яка не може бути легко змінена, але до якої має вільний доступ відповідний читач. Документ зберігається і надається таким чином, щоб бути доступним для працівників Банку, які надалі будуть мати право користуватися ним.

14.9. Рекомендується публікувати це Положення в системі електронного документообігу /інших аналогічних системах Банку або в місці, доступному кожному працівнику Банку.

14.10. За консультаціями та / або у випадках інших непорозумінь щодо цього Положення працівники Банку мають звертатися до працівників Служби управління ризиками.

15. ДОДАТКИ

15.1. Додаток 1. Розширена класифікація операційних ризиків АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

15.2. Додаток 2. Ключові показники ризику / ключові індикатори операційного ризику (KRI)

15.3. Додаток 3. Розрахунок загальної оцінки якісних показників ризик-апетиту до операційного ризику АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

15.4. Додаток 4. Розрахунок ризик-апетиту до операційного ризику АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»


Додаток1_Бібліотека КЛ_ОР.xlsx


Додаток2_KRI.xlsx


Додаток3_розрахунок ЯП.xlsx


Додаток4_розрахунок РА.xlsx

ІСТОРІЯ ВНУТРІШНЬОГО ДОКУМЕНТУ
Положення про управління операційним ризиком Банку та Банківської групи
АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

Власник документу	Служба управління ризиками

Розробник	Поточна редакція	Служба управління ризиками
Документ затверджено **Номери параграфів, що були змінені та/або доповнені**		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від 06.03.2025 р., Протокол № 14 Внесені зміни щодо Банківської групи
Розробник	Попередня редакція	Служба управління ризиками
Розробник		Служба управління ризиками
Документ затверджено		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від « 29» серпня 2024 р., Протокол № 46
Номери параграфів, що були змінені та/або доповнені		У новій редакції
Документ затверджено Номери параграфів, що були змінені та/або доповнені		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від «11» квітня 2024 р., Протокол № 18 У новій редакції
Розробник	Попередня редакція	Служба управління ризиками
Документ затверджено **Номери параграфів, що були змінені та/або доповнені**		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від «18» березня 2021 р., Протокол № 22 У новій редакції
Розробник	Попередня редакція	Служба управління ризиками
Документ затверджено **Номери параграфів, що були змінені та/або доповнені**		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від «31» березня 2020 р., Протокол № 20 У новій редакції
Розробник	Попередня редакція	Служба управління ризиками
Документ затверджено		Затверджена рішенням Наглядової ради АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» від «10» жовтня 2019 р., Протокол № 105

Номери параграфів, що були змінені та/або доповнені		Новий документ