ЗАТВЕРДЖЕНО
Рішення Наглядової ради
Акціонерного товариства
«Фонд декарбонізації
України»
(Протокол
від 29.04.2025 р.
№5/2025)

ПОЛОЖЕННЯ ПРО ОРГАНІЗАЦІЮ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ АКЦІОНЕРНОГО ТОВАРИСТВА «ФОНД ДЕКАРБОНІЗАЦІЇ УКРАЇНИ»

Київ – 2025

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА ТЕРМІНИ

1.1 Положення про організацію системи внутрішнього контролю АКЦІОНЕРНОГО ТОВАРИСТВА «ФОНД ДЕКАРБОНІЗАЦІЇ УКРАЇНИ» (далі – Положення) розроблено відповідно до вимог:

✓ Закону України «Про фінансові послуги та фінансові компанії»;

✓ Положення про авторизацію надавачів фінансових послуг та умови здійснення ними діяльності з надання фінансових послуг, затвердженого Постановою Правління Національного банку України № 199 від 29.12.2023;

✓ Положення про вимоги до системи корпоративного управління та системи внутрішнього контролю фінансової компанії, затвердженого Постановою Правління Національного банку України № 185 від 27.12.2024 року;

✓ Статуту АКЦІОНЕРНОГО ТОВАРИСТВА «ФОНД ДЕКАРБОНІЗАЦІЇ УКРАЇНИ»;

✓ інших законодавчих та нормативних-правових актів, внутрішніх документів Товариства.

1.2 Це Положення визначає основні цілі та принципи організації і функціонування комплексної, адекватної й ефективної системи внутрішнього контролю, які встановлюються та виконуються за всіма напрямами діяльності АКЦІОНЕРНОГО ТОВАРИСТВА «ФОНД ДЕКАРБОНІЗАЦІЇ УКРАЇНИ» (далі – Товариство) на всіх організаційних рівнях, та встановлює мінімальні вимоги щодо організації цієї системи, функціонування якої спрямоване на забезпечення ефективності корпоративного управління в Товаристві.

1.3 В Товаристві система внутрішнього контролю (далі – СВК) інтегрована в систему корпоративного управління шляхом:

1) створення відповідної організаційної структури;

2) визначення у внутрішніх документах (далі – ВД) повноважень, підпорядкованості, підзвітності, опису та розподілу функціональних обов’язків осіб, які задіяні у функціонуванні СВК, їх відповідальності та порядку взаємодії.

1.4. Терміни, що використовуються в цьому Положенні, уживаються в таких значеннях:

1) внутрішній контроль - процес, інтегрований в усі процеси та корпоративне управління Товариства, спрямований на досягнення операційних, інформаційних, комплаєнс-цілей діяльності Товариства;

2) внутрішні документи (ВД) - документи, затверджені органом управління Товариства в межах його компетенції, включаючи політики за окремими напрямами діяльності, положення, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі, з урахуванням вимог законодавства України;

3) інформаційна безпека - комплекс організаційних заходів Товариства, програмно-технічних засобів, що функціонують на всіх організаційних рівнях Товариства та забезпечують захист інформації від випадкових та/або навмисних загроз, наслідком реалізації яких може стати порушення доступності, цілісності, конфіденційності інформації щодо діяльності Товариства або її клієнтів;

4) культура внутрішнього контролю - дотримання визначених принципів, правил, норм, спрямованих на поінформованість працівників Товариства щодо функціонування СВК та участі кожного з працівників у цій діяльності (далі - Культура контролю);

5) контрольне середовище - сукупність суб’єктів СВК, процедур, політик за окремим напрямом діяльності Товариства та інших ВД щодо внутрішнього контролю, а також Культури контролю;

6) періодичні заходи з моніторингу - заходи з моніторингу СВК, що здійснюються на

періодичній основі згідно з окремими процедурами діяльності Товариства;

7) підрозділ - структурний підрозділ Товариства;

8) поточні заходи з моніторингу - заходи з моніторингу СВК, що вбудовані в процеси Товариства та здійснюються на постійній основі;

9) система внутрішнього контролю (СВК) - сукупність організаційної структури Товариства, процедур, заходів з внутрішнього контролю, спрямованих на:

- досягнення Товариством цілей, уключаючи виконання запланованих показників її діяльності, забезпечення ефективності та результативності здійснення Товариством операцій;

- забезпечення ефективності корпоративного управління в Товаристві шляхом функціонування комплексної, ефективної та адекватної системи управління ризиками; забезпечення повноти, своєчасності та достовірності складання і надання фінансової, статистичної, управлінської та іншої звітності; відповідності діяльності Товариства законодавству України, нормативно-правовим актам Національного банку України та ВД;

10) функціональний контроль - контрольна діяльність, яка здійснюється працівниками Товариства, відповідальними за здійснення внутрішнього контролю, на регулярній основі з метою забезпечення контролю за виконанням функціональних обов'язків працівниками відповідно до їх посадових інструкцій.

РОЗДІЛ 2. ОРГАНІЗАЦІЯ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ

2.1. Основна мета СВК - забезпечення органів управління Товариства обґрунтованою впевненістю щодо досягнення загальних цілей і завдань Товариства та забезпечення стабільності, безпеки й результативності операцій і процесів Товариства.

2.2. СВК складається з таких *компонентів*: контрольного середовища, управління ризиками, притаманними діяльності Товариства, контрольної діяльності та контрольних заходів в Товаристві, контролю за інформаційними потоками та комунікаціями, моніторингу ефективності СВК.

2.3. СВК забезпечує досягнення операційних, інформаційних та комплаєнс-цілей діяльності Товариства.

2.4. СВК реалізується на кожному з організаційних рівнів Товариства.

2.5. Завданнями СВК є:

- досягнення Товариством довгострокових цілей його діяльності;
- забезпечення відповідності діяльності Товариства законодавству України та внутрішнім документам Товариства;
- забезпечення здійснення Товариством безперервної діяльності;
- дотримання вимог щодо платоспроможності з урахуванням усіх ризиків, притаманних діяльності Товариства;
- вчасне виконання Товариством своїх зобов'язань;
- належне функціонування системи управління та чіткий розподіл обов'язків, функцій та повноважень між органами управління та структурними підрозділами.

2.6. Комплексна, ефективна та адекватна СВК створюється з дотриманням таких *принципів*:

- *принцип усебічності та комплексності*, що передбачає впровадження у діяльність Товариства кожного з компонентів СВК та забезпечує їх виконання у взаємоінтегрований спосіб, тобто результати виконання такого компонента використовуються під час виконання інших компонентів СВК; процедури з внутрішнього контролю (далі - процедури контролю) вбудовані в процеси на всіх

організаційних рівнях Товариства.

- *принцип ефективності* встановлює, що заходи з внутрішнього контролю (далі - заходи з контролю), що здійснюються в Товаристві, є дієвими та забезпечують досягнення визначених цілей діяльності та обґрунтовану упевненість у тому, що:

1) здійснювані операції є ефективними та відображені коректно в інформаційній системі/системах обліку, реєстрації та звітності;

2) фінансова, статистична, управлінська, податкова та інша звітність є достовірною;

3) Товариство дотримується вимог законодавства, нормативно-правових актів Національного банку України, ВД;

4) працівники володіють необхідною інформацією щодо компонентів СВК та забезпечують виконання цих компонентів у межах компетенції та повноважень, визначених посадовими інструкціями;

5) Товариство забезпечує виявлення та оцінку недоліків СВК та вживає своєчасних, адекватних та достатніх коригуючих заходів з метою виправлення таких недоліків;

- *принцип адекватності* передбачає, що СВК відповідає особливостям діяльності Товариства, уключаючи розмір, бізнес-модель, масштаб діяльності, види, складність операцій, профіль ризику;

- *принцип обачності* встановлює, що забезпечується достатня впевненість органів управління щодо досягнення Товариством цілей його діяльності, виходячи з консервативних припущень та беручи до уваги певну вірогідність помилкових суджень чи рішень керівників та/або працівників;

- *принцип ризик-орієнтованості* передбачає, що забезпечується організація та функціонування СВК, ґрунтуючись на ризик-орієнтованому підході, що передбачає застосування більш поглиблених та частіших заходів з контролю до тих сфер діяльності, яким притаманні більші ризики;

- *принцип інтегрованості* встановлює, що процедури контролю є складовою частиною всіх процесів діяльності та корпоративного управління;

- *принцип завчасності* передбачає, що СВК спроможна забезпечувати виявлення потенційно можливих загроз негативного впливу на діяльність Товариства раніше, ніж такі загрози фактично виникнуть;

- *принцип незалежності* встановлює, що уникаються обставини, що можуть становити загрозу для неупередженого виконання суб'єктами СВК своїх функцій;

- *принцип безперервності* передбачає, що здійснення діяльності з внутрішнього контролю дає змогу на постійній основі та своєчасно попереджати, виявляти та усувати недоліки СВК;

- *принцип конфіденційності* встановлює, що не допускається розголошення інформації особам, у яких відсутні повноваження щодо її отримання.

2.7. СВК забезпечує досягнення наступних *цілей* діяльності Товариства, де:

- *операційні цілі* - це забезпечення спрямованості процедур контролю на ефективність управління активами, зобов'язаннями та позабалансовими позиціями Товариства з метою досягнення прибуткової діяльності, уникаючи або обмежуючи втрати внаслідок впливу негативних внутрішніх та зовнішніх факторів; здійснення систематичного процесу виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення всіх видів ризиків на всіх організаційних рівнях;

- *інформаційні цілі* - це забезпечення цілісності, повноти та достовірності фінансової, управлінської та іншої інформації, що використовується для ухвалення управлінських рішень; створення інформаційних потоків як за вертикаллю, так і за горизонталлю організаційної структури Товариства. Така інформація включає звітність Товариства з фінансових та нефінансових питань, що надається зовнішнім та внутрішнім користувачам;

- *комплаєнс-цілі* - це забезпечення організації діяльності Товариства з метою виявлення та

запобігання ризикам, які можуть виникати під час здійснення Товариством діяльності, передбаченої законом, унаслідок невідповідності такої діяльності вимогам законодавства України та/або іншим вимогам (правилам, стандартам, принципам) щодо здійснення такої діяльності.

2.8. СВК повинна забезпечувати належне функціонування *моделі трьох ліній захисту*, ефективного управління ризиками з чітко визначеними сферами відповідальності за управління ризиками, а саме:

1) перша лінія захисту - складається з бізнес-підрозділів та підрозділів підтримки діяльності Товариства, включаючи їх працівників (суб'єкти першої лінії). Суб'єкти першої лінії ініціюють, здійснюють або відображають господарські операції, приймають ризики в процесі своєї діяльності та відповідають за поточне управління цими ризиками, здійснюють заходи з контролю в межах свої компетенції;

2) друга лінія захисту - складається з головного комплаєнс-менеджеру та головного ризик-менеджеру (суб'єкти другої лінії), які забезпечують ефективність впроваджених першою лінією захисту заходів із контролю та управління ризиками, їх відповідність вимогам законодавства України та ВД;

3) третя лінія захисту - запроваджена в особі внутрішнього аудитора (суб'єкт третьої лінії), який здійснює оцінювання ефективності діяльності першої та другої ліній захисту, загальне оцінювання ефективності системи внутрішнього контролю в межах виконання функції внутрішнього аудиту Товариства.

Функціональний розподіл у рамках моделі трьох ліній захисту забезпечується через виконання таких вимог:

- Підрозділи / працівники першої лінії захисту не можуть поєднувати функції підрозділів / працівників другої та третьої ліній захисту, і навпаки: працівники другої та третьої ліній захисту не можуть поєднувати функції працівників першої лінії захисту.
- Поєднання функцій головного ризик-менеджера (CRO), головного комплаєнс-менеджера (CCO) та внутрішнього аудитора неможливе.

Головний комплаєнс-менеджер (CCO) має право виконувати функції працівника, відповідального за проведення фінансового моніторингу з урахуванням визначених законодавством вимог.

2.9. Процедури та заходи з контролю, які застосовуються підрозділами кожної з трьох ліній захисту, визначаються у ВД, в тому числі:

1) *вертикальної взаємодії*, що застосовується під час здійснення внутрішнього контролю між суб'єктами різних ліній захисту;

2) *горизонтальної взаємодії*, що застосовується в разі здійснення внутрішнього контролю в межах одного підрозділу та/або між суб'єктами однієї лінії захисту.

2.10. *Основні напрями внутрішнього контролю* в Товаристві включають:

1) контроль за досягненням цілей діяльності Товариства, уключаючи цілі, визначені в стратегії та інших ВД Товариства;

2) контроль за забезпеченням ефективності фінансової та господарської діяльності в разі здійснення фінансових та інших операцій;

3) контроль за ефективністю управління активами і пасивами;

4) контроль за збереженням активів;

5) контроль за ефективністю системи управління ризиками;

6) контроль за дотриманням вимог законодавства, нормативно-правових актів Національного банку України, ВД;

7) контроль за достовірністю, повнотою, об’єктивністю і своєчасністю ведення бухгалтерського обліку, складанням та оприлюдненням фінансової та іншої звітності для зовнішніх і внутрішніх користувачів;

8) управління інформаційними потоками, уключаючи отримання і передавання інформації, забезпечення функціонування системи управління інформаційною безпекою.

2.11. *Процедури контролю запроваджуються*:

1) *організаційно* шляхом:

- розподілу в межах організаційної структури Товариства повноважень, обов’язків та відповідальності щодо здійснення внутрішнього контролю між підрозділами, між керівниками та між працівниками Товариства. Підпорядкованість, обов’язки, права та відповідальність працівників визначаються в посадових інструкціях;
- впровадження необхідних контрольних процедур, обмежень, що забезпечують ефективне функціонування СВК;
- опису в положеннях про підрозділи контрольних функцій, що здійснюються кожним з них;
- проведення регулярного оцінювання ризиків Товариства та заходів з контролю Товариства;
- забезпечення інформаційної безпеки та організації належного обміну інформацією;
- проведення моніторингу ефективності СВК, уключаючи оцінку її ефективності шляхом проведення перевірок аудитором внутрішнім;

2) *методологічно* шляхом опису СВК у ВД, уключаючи періодичність та строки виконання заходів з контролю, посадових осіб, на яких покладається контроль;

3) *технологічно* шляхом автоматизації процедур контролю в інформаційній системі / системах обліку, реєстрації та звітності Товариства з урахуванням судження Товариства щодо економічної доцільності автоматизації таких процедур.

РОЗДІЛ 3. КОНТРОЛЬНЕ СЕРЕДОВИЩЕ, УПРАВЛІННЯ РИЗИКАМИ ТА КОНТРОЛЬНА ДІЯЛЬНІСТЬ

3.1. Наглядова рада забезпечує створення та функціонування контрольного середовища як компонента СВК.

3.2. Система управління ризиками є складовою частиною (компонентом) СВК.

3.3. *Суб’єктами СВК* є:

- Наглядова рада;
- Внутрішній аудитор;
- Головний комплаєнс-менеджер та Головний ризик-менеджер;
- керівники та працівники всіх підрозділів, які здійснюють внутрішній контроль відповідно до повноважень, визначених ВД та посадовими інструкціями.

Функції суб’єктів внутрішнього контролю, їх повноваження, відповідальність та порядок взаємодії визначаються Статутом, положеннями, посадовими інструкціями та іншими ВД.

3.4. Органи управління та підрозділи Товариства в межах моніторингу та оцінки СВК здійснюють наступні *функції*:

Наглядова рада

- відповідає за організацію, впровадження та підтримку функціонування адекватної та ефективної

СВК;

- розподіляє функції, повноваження та відповідальність за здійснення внутрішнього контролю між підрозділами та між працівниками;
- забезпечує функціонування та контроль за ефективністю системи управління ризиками;
- затверджує організаційну структуру Товариства;
- затверджує вимоги щодо здійснення моніторингу СВК та звітування;
- затверджує ВД з організації та функціонування СВК;
- розглядає питання організації внутрішнього контролю та заходів щодо підвищення його ефективності;
- розглядає та аналізує оцінку ефективності СВК, проведеної внутрішнім аудитором;
- розглядає результати моніторингу ефективності СВК, викладені у звітах головного комплаєнс-менеджера та головного ризик-менеджера.

Суб'єкт третьої лінії захисту

- здійснює оцінку ефективності діяльності першої та другої ліній захисту та загальну оцінку ефективності системи внутрішнього контролю;
- надає пропозиції з питань розроблення / перегляду процесу здійснення заходів з контролю та/або окремих процедур внутрішнього контролю.

Внутрішній аудитор як суб'єкт третьої лінії захисту

- оцінює ефективність, комплексність та адекватність системи управління ризиками;
- оцінює ефективність, комплексність та адекватність СВК;
- оцінює відповідність СВК видам та обсягам здійснюваних Товариством операцій, змінам у бізнес-моделі Товариства;
- здійснює при проведенні кожної перевірк
- и оцінку системи внутрішнього контролю;
- при здійсненні оцінки ефективності СВК, визначає зміст, процедуру, метод та критерії такої оцінки;
- оцінює ефективність СВК додатково в разі настання або високої ймовірності настання подій, що мають/можуть мати істотний вплив на діяльність Товариства (змін у бізнес-моделі, організаційній структурі Товариства, тощо).

Суб'єкти другої лінії захисту в межах повноважень під час виконання функцій з контролю за дотриманням норм (комплаєнс) та функції з управління ризиками

- надають пропозиції щодо вибору та визначення органом управління Товариства видів контрольної діяльності;
- консультують Правління з питань розроблення / перегляду внутрішніх документів, які визначають процес здійснення кожного з видів діяльності в межах системи внутрішнього контролю, та окремих процедур внутрішнього контролю;
- забезпечують організацію виявлення, моніторинг та контроль суттєвих ризиків, вимірювання ризиків та складання (обчислення) профілю ризиків, здійснюють контроль та моніторинг упровадження внутрішніх документів, включаючи документи з питань культури управління ризиками, та виконання суб'єктами першої лінії захисту покладених на них функцій, включаючи виконання заходів з контролю;
- здійснюють контроль за виявленням та своєчасним інформуванням про виявлені ризики, пов'язані з їх діяльністю;

- контролюють дотримання лімітів ризиків (якісних та/або кількісних, єдиним значенням або діапазоном чи межами), установлених для окремих підрозділів / відповідальних працівників Товариства та в межах таких підрозділів, лімітів ризику концентрації, лімітів дотримання повноважень, лімітів щодо продуктів та сервісів, інших лімітів, установлених внутрішніми документами Товариства;
- забезпечують складання висновків щодо ризиків, притаманних діяльності Товариства, включаючи висновки щодо ризиків, що виникають під час запровадження нових продуктів / послуг;
- ураховують у процесі прийняття рішень інформацію, отриману в межах системи управління ризиками;
- забезпечують складання та своєчасне звітування, підготовка якого належить до компетенції відповідного підрозділу / відповідального працівника, включаючи звітування щодо ризиків, притаманних діяльності Товариства, висновки щодо ризиків, що виникають під час запровадження нових продуктів / послуг);
- здійснюють контроль за дотриманням прав клієнтів Товариства , внутрішніх документів та процесів;
- здійснюють контрольну діяльність за інформаційною системою / системами обліку, реєстрації та звітності й технологіями, надають рекомендації щодо їх удосконалення, усунення виявлених недоліків у їх роботі виконавчому органу Товариства;
- перевіряють відповідність внутрішніх документів Товариства законодавству України, забезпечують здійснення моніторингу змін у законодавстві України та здійснюють оцінку впливу таких змін на процеси та процедури, запроваджені в Товаристві, а також забезпечують контроль за імплементацією відповідних змін у внутрішні документи;
- перевіряють відповідність здійснюваних суб'єктами першої лінії захисту заходів із контролю внутрішнім документам Товариства;
- забезпечують управління ризиками, пов'язаними з конфліктом інтересів, що можуть виникати на всіх рівнях організаційної структури Товариства;
- забезпечують організацію контролю за захистом і обробкою персональних даних та іншої інформації, що підлягає захисту відповідно до законодавства України;
- відповідають за належне та своєчасне інформування суб'єктів внутрішнього контролю щодо внутрішніх документів та внесених до них змін, які визначають процедури здійснення кожного з видів контрольної діяльності та окремих процедур внутрішнього контролю;
- складають звіти в межах компетенції щодо реалізації контрольної діяльності / моніторингу, які мають бути подані для оцінки та розгляду Наглядовій раді Товариства.

Головний комплаєнс-менеджер як суб'єкт другої лінії захисту

- координує організацію СВК в межах Товариства;
- здійснює моніторинг ефективності процедур контролю на першій лінії захисту;
- забезпечує організацію контролю за відповідністю діяльності Товариства вимогам законодавства, нормативно-правовим актам Національного банку України, ВД;
- здійснює узагальнюючий аналіз повноти імплементації змін до законодавства та нормативно – правових актів Національного банку України у ВД Товариства;
- проводить перевірки дотримання лімітів комплаєнс-ризику, обмежень, що передбачені чинним законодавством (за необхідності);
- надає керівникам підрозділів пропозиції щодо підвищення ефективності внутрішнього контролю та здійснення коригуючих дій;

- здійснює контроль за якістю усунення недоліків в сфері комплаєнсу та виконання коригуючих дій підрозділами;
- здійснює допомогу при розробці нових процесів або внесення змін в існуючі;
- сприяє в оцінці та відслідковуванні комплаєнс- ризиків.

Головний ризик-менеджер як суб'єкт другої лінії захисту

- забезпечує створення та функціонування комплексної, ефективної та адекватної системи управління ризиками;
- на всіх організаційних рівнях (уключаючи Товариство в цілому, підрозділи та працівників) виявляє ризики, притаманні діяльності Товариства, та визначає заходи щодо управління такими ризиками;
- здійснює моніторинг ефективності процедур контролю на першій лінії захисту відповідно до вимог ВД, які регламентують процес управління ризиками;
- відповідає за якість виконання заходів із моніторингу СВК.

Суб'єкти першої лінії захисту в межах компетенції

- здійснюють виконання покладених на них обов'язків та повноважень відповідно до внутрішніх документів Товариства, забезпечують дотримання вимог, визначених внутрішніми документами;
- постійно здійснюють заходи з контролю, періодичність та обов'язок із виконання яких визначаються у внутрішніх документах Товариства, та відповідають за їх належне і своєчасне виконання;
- здійснюють заходи з виявлення та інформування про ризики, пов'язані з діяльністю суб'єктів першої лінії захисту, відповідно до вимог цього Положення;
- мають право ініціювати / брати участь у періодичному перегляді / розробленні заходів процесу внутрішнього контролю.

Правління, Керівники підрозділів як суб'єкти першої лінії захисту

- забезпечують організацію, упровадження та належне здійснення контролю за компетенціями;
- проводять попередній, поточний і подальший контроль якості/ефективності роботи підлеглих на предмет наявності помилок і мотивують працівників проводити якісний самоконтроль;
- виконують рішення та рекомендації Наглядової ради та Правління, а також допомагають впроваджувати конкретні заходи мінімізації та контролю з недопущення виникнення ризику, також допомагають оцінити ефективність проведених заходів;
- здійснюють оцінки ризиків відповідно до своєї компетенції;
- відповідають за дотримання всіх вимог ВД, що відносяться до їх сфери діяльності;
- проводять постійний моніторинг усіх процесів та ВД з метою їх своєчасного оновлення;
- забезпечують своєчасне виконання контролів у підрозділі;
- здійснюють коригуючі дії у разі виявлення недоліків у СВК;
- розробляють заходи у разі недостатнього внутрішнього контролю у підрозділі;
- забезпечують своєчасне та повне виконання розроблених заходів.

Працівники підрозділів як суб'єкти першої лінії захисту

- здійснюють контроль в межах своїх посадових обов'язків;
- негайно інформують безпосереднього керівника про важливість та тип виявлених недоліків;
- надають пропозиції щодо покращення/оптимізації процесів та контролів;
- беруть участь у заходах, що мають на меті виправлення недоліків.

3.5. В Товаристві забезпечується безперервність виконання функцій управління ризиками, забезпечення відповідності законодавству та здійснення внутрішнього аудиту.

У разі тимчасової відсутності (відпустка, тимчасова непрацездатність, відрядження тощо) головного ризик-менеджера, головного комплаєнс-менеджера та внутрішнього аудитора їхні обов'язки покладаються на іншого компетентного співробітника Товариства.

Рішення про покладення обов'язків на час тимчасової відсутності приймається Наглядовою радою Товариства. При покладенні обов'язків враховується:

- ✓ Наявність у співробітника необхідних знань, досвіду та кваліфікації для виконання відповідних функцій.
- ✓ Відповідність кваліфікаційним вимогам, встановленим законодавством України, нормативно-правовими актами НБУ та внутрішніми документами Товариства.
- ✓ Рівень відповідальності та самостійності, необхідний для виконання обов'язків.

Покладення обов'язків оформлюється відповідним рішенням Наглядової ради Товариства.

Співробітник, на якого тимчасово покладаються обов'язки головного ризик-менеджера, головного комплаєнс-менеджера або внутрішнього аудитора, несе повну відповідальність за належне виконання цих обов'язків протягом визначеного терміну. Після повернення основного співробітника, співробітник, який тимчасово виконував його обов'язки, передає всі необхідні документи та інформацію.

3.6. Компонент «Контрольне середовище» складається з методологічних та організаційних засад функціонування СВК (процедур, політик та інших внутрішніх документів щодо внутрішнього контролю, а також культури контролю).

Товариство визначає у внутрішніх документах чіткий опис процесів, які забезпечують внутрішній контроль.

Товариство визначає у внутрішніх документах процедури та заходи з контролю, які застосовуються підрозділами кожної з трьох ліній захисту.

Товариство доводить до відома працівників внутрішні документи, які містять інформацію, необхідну для належного виконання такими працівниками своїх повноважень, включаючи повноваження щодо здійснення внутрішнього контролю.

Товариство письмово фіксує кожний факт ознайомлення працівника / працівників із відповідними документами шляхом отримання підпису ознайомленого працівника та уповноваженої особи, яка забезпечила проведення ознайомлення.

Уповноважена особа, яка забезпечує проведення ознайомлення, провадить ознайомлення з відповідними документами працівників Товариства (залежно від їхніх посадових обов'язків) у випадку:

1) приймання працівника на роботу - до початку виконання таким працівником посадових обов'язків;

2) затвердження або внесення змін до відповідних документів - не пізніше 3 робочих днів із дня затвердження, внесення змін (крім працівників, які протягом цього періоду перебували у відпустці, на лікарняному, у відрядженні, які ознайомлюються не пізніше двох робочих днів з дня виходу на роботу).

3.7. СВК забезпечує наявність системи управління ризиками Товариства та проведення постійного контролю за її розвитком і функціонуванням.

Товариство створює та забезпечує функціонування системи управління ризиками, що забезпечує виявлення, вимірювання (оцінку), моніторинг, контроль, звітування та пом'якшення (зниження до контрольованого рівня) всіх суттєвих ризиків, визначених в Стратегії управління

ризиками, на всіх організаційних рівнях.

Управління ризиками поділяється на 4 групи, відповідальними за якими є відповідні посадові особи:

- Управління кредитним ризиком – Головний ризик-менеджер;
- Управління операційним ризиком – Головний ризик-менеджер;
- Управління комплаєнс-ризиками – Головний комплаєнс-менеджер;
- Управління ризиком ліквідності – Головний ризик-менеджер.

Система управління ризиками повинна забезпечувати:

- оцінку зовнішніх факторів;
- розгляд внутрішніх факторів;
- оцінку ризиків, що підлягають кількісному вимірюванню, і тих, які не підлягають кількісному вимірюванню;
- визначення ризиків, які можуть виникнути в діяльності Товариства, щодо яких воно може ухвалити рішення стосовно їх прийняття, враховуючи можливість негативного впливу таких ризиків на досягнення цілей Товариства.

Цілі СВК в частині контролю систем управління ризиками досягаються за допомогою:

- перевірки правильності використання наданих доступів та дозволів;
- контролю за періодичністю, повнотою та якістю проведення перевірки дотримання лімітів, обов'язкових умов, а також їхнього моніторингу;
- перевірки проведення оновлень внутрішніх документів у частині управління ризиками;
- перевірки послідовності виконання етапів процесів і в разі необхідності оптимізації/актуалізації процесу управління ризиками.

3.8. Товариство здійснює контрольну діяльність з метою надання достатньої впевненості органам управління щодо досягнення Товариством цілей його діяльності шляхом:

- запровадження та виконання заходів з контролю щодо усіх процесів та на всіх організаційних рівнях;
- розгляду звітів, підготовлених за результатами здійснення контрольних заходів (заходів з контролю).

Заходи з контролю повинні відповідати таким *критеріям*:

1) *достовірність та своєчасність* - фінансові операції та дії в межах інших процесів діяльності Товариства відображаються в інформаційних та інших системах коректно та своєчасно на кожному етапі здійснення/оброблення;

2*) повнота* - усі виконані операції та дії в межах інших процесів діяльності Товариства відображаються в інформаційних та інших системах в повному обсязі;

3) *дійсність* - операції та дії в межах інших процесів Товариства є подіями, які фактично відбулися та виконані відповідно до встановлених процедур.

Заходи з контролю впроваджуються на кожному з організаційних рівнів.

Метою застосування заходів з контролю є:

1) запобігання порушень - шляхом запобігання недоліків/невідповідностей/порушень (уключаючи визначення правил авторизації операцій чи контролю за наданням доступу);

2) виявлення порушень - шляхом виявлення недоліків/невідповідностей/порушень (уключаючи подвійний або автоматизований контроль, самоконтроль /самооцінку);

3) виправлення порушень - шляхом виправлення недоліків/невідповідностей/порушень (уключаючи забезпечення автоматичного виправлення помилок в інформаційних системах Товариства).

Заходи з контролю передбачають такі *етапи*:

1) визначення процедур, видів контролю у ВД;

2) виконання функцій/процесів працівниками Товариства, що включають визначені процедури, види контролю;

3) аналіз та контроль виконання функцій/процесів працівниками Товариства.

Процедури контролю *передбачають* такий *контроль*:

1) що здійснюється керівниками Товариства та включає аналіз звітності, яка надається на регулярній основі або запитується згідно з окремо встановленими процедурами, про результати діяльності підрозділів з метою аналізу відповідності цих результатів установленим цілям діяльності Товариства;

2) що здійснюється керівниками підрозділів та включає аналіз звітів про результати діяльності відповідних підрозділів;

3) за наданням доступу, що включає обмеження доступу до приміщень Товариства, розподіл відповідальності за зберігання і використання цінностей, забезпечення охорони приміщень, проведення періодичних інвентаризацій, обмеження доступу до інформаційних систем, уключаючи санкціонування допуску до комп'ютерних програм та даних;

4) за дотриманням установлених лімітів на здійснення фінансових операцій та інших угод, що виконується шляхом отримання відповідних звітів та/або звіряння з даними первинних документів, інформаційних та інших систем Товариства;

5) за наданням дозволів та підтверджень на здійснення операцій, що включає встановлення порядку розподілу повноважень під час здійснення фінансових операцій та виконання інших угод;

6) за відповідністю відображення операцій, що включає контроль за дотриманням порядку здійснення фінансових операцій та виконанням інших угод, їх належним відображенням у бухгалтерському обліку, фінансовій та статистичній звітності, інформуванням керівників Товариства відповідного рівня про виявлені порушення, помилки і недоліки.

Здійснення процедур контролю забезпечується *шляхом*:

1) *розмежування функцій* - працівники, відповідальні за укладання угод, не повинні здійснювати бухгалтерський облік операцій, що виконуються за такими угодами. В одному підрозділі не може бути зосереджено проведення операції, починаючи з її ініціювання до відображення в регістрах бухгалтерського обліку Товариства, крім операцій з установленим механізмом контролю з використанням відповідного програмного забезпечення;

2) *контролю за введенням даних в системи обліку, реєстрації та звітності* - введення інформації/операції одним працівником (виконавцем) має бути перевірено іншим працівником (контролером), крім операцій з установленим механізмом контролю з використанням відповідного програмного забезпечення;

3) *звіряння даних* - звіряння даних повинно відбуватися між різними системами (*обліку, реєстрації та звітності*), а також на різних етапах оброблення даних, що реалізується шляхом порівняння детальної інформації та/або кінцевих даних;

4) *контролю за виправленнями* - унесення будь-яких виправлень до вхідної інформації у системах Товариства має бути додатково проконтрольовано (санкціоновано) іншим працівником (який не є виконавцем).

Розподіл обов'язків між працівниками Товариства здійснюється в такий спосіб, що забезпечує захист від ризику несанкціонованих операцій, шахрайських дій та маніпулювання даними для приховування фінансових збитків або порушень законодавства, нормативно-правових актів Національного банку України, ВД.

З метою досягнення цілей СВК, для виконання функцій та обов'язків, залучаються компетентні особи, забезпечується наявність *належного рівня кваліфікації* працівників на всіх організаційних рівнях Товариства, створюються умови, що сприяють розвитку працівників. Розробляються та впроваджуються заходи щодо підтримки на належному рівні актуальних знань та навичок у працівників з метою підвищення ефективності діяльності Товариства. Уповноважені працівники Товариства мають постійно оцінювати достатність кваліфікації працівників та потребу в їх регулярному навчанні.

З метою досягнення цілей діяльності Товариства, уключаючи цілі СВК, розвивається, підтримується та оцінюється компетентність працівників.

СВК включає такі *види контролів*:

1) залежно від моменту здійснення контролю:

попередній - передує виконанню дії або операції;

поточний - здійснюється під час виконання дії або операції;

подальший - здійснюється після виконання дії або операцій та спрямований на виявлення недоліків, виправлення допущених помилок.

Товариство забезпечує послідовне поєднання попереднього, поточного і подальшого контролів з метою підвищення дієвості та ефективності контролю;

2) залежно від призначення контролю:

превентивний - спрямований на попередження порушень та ризиків;

виявляючий - спрямований на виявлення ризиків;

коригуючий - спрямований на уникнення/пом'якшення реалізованих ризиків;

3) залежно від суб'єкта контролю:

самостійний контроль - здійснюється працівником самостійно;

подвійний контроль - здійснюється двома (або більше) працівниками (принцип "двох пар очей");

колегіальний контроль - здійснюється колегіальним органом;

автоматизований контроль - здійснюється автоматизованою системою;

4) залежно від періодичності здійснення:

функціональний (постійний) - проводиться на регулярній основі;

періодичний - проводиться згідно з установленою у ВД періодичністю;

5) залежно від обсягів контролю:

повний - охоплює весь обсяг відповідного процесу Товариства;

портфельний - проводиться за групами функцій, операцій, договорів;

вибірковий - проводиться за окремими відібраними елементами відповідного процесу Товариства.

З метою забезпечення надійного та безперервного функціонування Товариства, обираються та впроваджуються *заходи з контролю за системами (обліку, реєстрації та звітності)* та технологіями, що використовуються в Товаристві. Такі заходи включають в себе:

1) контроль за технологічною інфраструктурою: застосовується до інфраструктурних об'єктів Товариства, уключаючи мережі зв'язку, живлення, робочі станції; здійснюється з метою забезпечення повноти, доступності, цілісності інформації, що використовується в діяльності, та передбачає необхідні коригуючі дії під час виявлення недоліків функціонування систем, уключаючи процедури резервування (копіювання) даних, відновлення функцій систем унаслідок форс-мажорних обставин або технічних збоїв;

2) управління доступами: уключає процедури контролю за доступом до систем обліку,

реєстрації та звітності та охоплює права доступу до виконання фінансових операцій, а також до інших даних, операційних систем (системне програмне забезпечення), мереж, програмних додатків. Ці заходи здійснюються з метою захисту від несанкціонованого використання та зловживань;

3) контроль за системами обліку, реєстрації та звітності та технологіями Товариства під час їх придбання, розроблення або супроводження: упроваджується з метою забезпечення відповідних процедур, що регламентують придбання, розроблення та супроводження систем і їх компонентів та технологічних рішень, вимоги до їх документації, їх тестування та подальше технічне обслуговування. Ці процедури забезпечують контроль за змінами в системах та технологіях та можуть передбачати необхідність авторизації запитів на зміни, узгоджень і результатів тестування.

Системи обліку, реєстрації та звітності забезпечує виконання Товариством процедур та заходів з контролю, уключаючи:

1) виявлення та відстеження помилок, суперечностей і підозрілих операцій;

2) виправлення помилок, суперечностей і неточностей під час відображення операцій в обліку або звітності.

Товариство забезпечує дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем.

Контроль доступу до інформаційних систем включає:

1) перевірку наявності у користувача дозволу керівництва на такий доступ;

2) перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень;

3) періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки.

Заходи контролю інформаційних систем включать:

- захист інформації від витоку;
- надання диференційованого доступу працівникам для здійснення конкретних операцій (створення, читання, запис, модифікація, видалення) за допомогою програмно-технічних засобів, а також розмежування доступу користувачів до даних в системах та комп'ютерних мережах;
- ідентифікація користувачів та здійснюваних ними процесів в системах та комп'ютерних мережах на основі використання паролів, ключів, цифрового підпису тощо;
- попередження передачі інформації з обмеженим доступом по незахищених лініях зв'язку;
- запобігання впровадженню в інформаційно-комунікаційні системи програм-вірусів;
- регулярна перевірка технічних засобів і приміщень для виявлення наявності в них пристроїв несанкціонованого доступу до інформації.

РОЗДІЛ 4. КОНТРОЛЬ ЗА ІНФОРМАЦІЙНИМИ ПОТОКАМИ ТА КОМУНІКАЦІЯМИ

4.1. Якість інформації ґрунтується на *принципах*:

- *наявність та доступність* - інформацію легко отримати тим, хто її потребує для виконання своїх посадових/функціональних обов'язків. Користувачі ознайомлені з переліком доступної їм інформації та процедурою доступу до інформаційних систем Товариства;

- *коректність* - інформація є достовірною та повною. Інформаційні системи забезпечують проведення перевірок достовірності і повноти даних;

- *актуальність* - зібрана інформація є актуальною та оновлюється з необхідною частотою, уключаючи періодичність, визначену законодавством України, нормативно-правовими актами Національного банку України, ВД;

- *цілісність* - інформація є захищеною від несанкціонованого спотворення, руйнування або знищення. Товариство забезпечує класифікацію інформації (наприклад, загальнодоступна, з обмеженим доступом, таємниця фінансових послуг) та інші процедури захисту інформації;

- *збереження* - інформація доступна протягом термінів, визначених законодавством України, нормативно-правовими актами Національного банку України, ВД;

- *достатність* - рівень деталізації інформації відповідає потребам внутрішніх та зовнішніх користувачів;

- *дійсність* - інформація, отримана відповідно до затверджених процедур, і, за винятком гіпотетичних припущень, є даними про події, які фактично відбулися;

- *підтверджуваність* - інформація підтверджується доказами з відповідного джерела.

4.2. Товариство забезпечує використання якісної інформації на всіх її організаційних рівнях з метою досягнення цілей діяльності та своєчасного реагування на виявлені недоліки СВК.

Форма та періодичність надання інформації визначається з урахуванням потреб та вимог внутрішніх та зовнішніх користувачів.

Контроль за дотриманням процедур СВК здійснює Головний комплаєнс-менеджер.

4.3. Контроль за інформаційними потоками та комунікаціями (обміном інформацією) здійснюється *з метою*:

- надання та отримання якісної інформації внутрішніми та зовнішніми користувачами з метою прийняття обґрунтованих суджень, своєчасних та адекватних управлінських рішень;

- створення та функціонування інформаційної системи, що забезпечує здійснення внутрішніх та зовнішніх комунікацій.

4.4. Обмін інформацією стосовно внутрішнього контролю здійснюється на всіх організаційних рівнях, що включає інформацію щодо:

- цілей СВК, важливості та переваг наявності ефективної СВК;

- політики та процедур, що визначають функціональні обов'язки керівників та працівників щодо виконання заходів з контролю;

- ролей, повноважень та обов'язків керівників та інших працівників щодо виконання заходів з контролю;

- суттєвих питань щодо організації та функціонування СВК, уключаючи інформацію щодо недоліків та невідповідностей у СВК.

4.5. *Внутрішні комунікації* здійснюються *за різними напрямами*, а саме:

- вертикально (знизу - вгору) - інформація щодо ризиків та інших питань діяльності доводиться до відома Наглядової ради з метою прийняття відповідних управлінських рішень;

- вертикально (зверху - вниз) - інформація про стратегічний план розвитку Товариства доводиться до відома керівників усіх рівнів, ключових осіб та інших працівників;

- горизонтально - інформація, якою володіє один підрозділ, надається іншому підрозділу, якому вона необхідна для виконання своїх функцій.

4.6. *Працівникам* відповідно до їх функціональних обов'язків *надають* якісну інформацію, зокрема щодо:

1) стратегічних, поточних цілей та планів Товариства, стану їх виконання;

2) змін у ВД, уключаючи документи щодо здійснення внутрішнього контролю;

3) культури контролю;

4) розпоряджень керівників Товариства та підрозділів, уключаючи розпорядження щодо здійснення заходів з контролю;

5) правил техніки безпеки та охорони праці;

6) порядку користування, передавання, збереження документів та інших носіїв інформації, що становить комерційну таємницю, таємницю фінансової послуги або містить іншу охоронювану законом інформацію;

7) процедур щодо дотримання вимог з інформаційної та кібербезпеки;

8) відповідальності (дисциплінарної, адміністративної, кримінальної) за вчинення порушень.

4.7. Перевірці якості інформації підлягає вся інформація, що використовується в діяльності Товариства, включаючи:

✓ Фінансова звітність.

✓ Управлінська звітність.

✓ Операційні дані.

✓ Юридична документація.

✓ Інформація про клієнтів.

✓ Дані систем обліку, реєстрації та звітності.

✓ Зовнішня інформація (ринкові дані, регуляторні звіти тощо).

✓ Будь-яка інша інформація, що впливає на прийняття рішень або відображає діяльність Товариства.

4.8. Відповідальність за забезпечення якості інформації несуть:

✓ Перша лінія захисту: Відповідають за якість інформації, що генерується та використовується в їхній діяльності.

✓ Друга лінія захисту: Здійснюють нагляд та контроль за якістю інформації в межах своїх функцій.

✓ Третя лінія захисту: Проводить незалежну оцінку якості інформації в рамках аудиторських перевірок.

4.9. Перевірка якості інформації може здійснюватися на регулярній основі або за потреби та включає наступні етапи:

1) Визначення об'єкта та мети перевірки: Визначається конкретна інформація або система чи її складова, що підлягає перевірці. Формулюється мета перевірки (наприклад, оцінка відповідності принципам якості, перевірка достовірності джерела).

2) Вибір методів перевірки. Залежно від об'єкта та мети перевірки можуть застосовуватися наступні методи:

✓ Порівняння: Зіставлення інформації з іншими джерелами (внутрішніми та зовнішніми), попередніми періодами, плановими показниками.

✓ Аналіз первинних документів: Перевірка відповідності інформації документам, що стосуються операції (договори, звіти, квитанції тощо).

✓ Перевірка розрахунків: Контроль правильності математичних розрахунків та алгоритмів.

✓ Інтерв'ю та опитування: Отримання пояснень від осіб, відповідальних за підготовку та використання інформації.

✓ Тестування систем обліку, реєстрації та звітності: Перевірка логіки обробки даних, контролів вводу та виводу інформації.

✓ Аналіз метаданих: Перевірка інформації про походження, дату створення та зміни даних.

✓ Зовнішнє підтвердження: Отримання підтвердження інформації від зовнішніх джерел (наприклад, контрагентів, регуляторів).

✓ Візуальний огляд: Перевірка фізичного стану документів або записів.

3) Проведення перевірки: Здійснюється збір та аналіз необхідної інформації з використанням обраних методів. Фіксуються виявлені невідповідності, помилки або ознаки недостовірності.

4) Оцінка результатів перевірки: Оцінюється суттєвість виявлених недоліків та їхній потенційний вплив на діяльність Товариства. Визначаються причини виникнення недоліків.

5) Підготовка звіту про результати перевірки. Звіт повинен містити:

- ✓ Мету та об'єкт перевірки.
- ✓ Перелік застосованих методів.
- ✓ Опис виявлених недоліків та невідповідностей.
- ✓ Оцінку суттєвості виявлених недоліків.
- ✓ Висновки щодо якості перевіреної інформації.
- ✓ Рекомендації щодо усунення виявлених недоліків та запобігання їхньому повторенню.
- ✓ Інформацію про відповідальних осіб та терміни виконання рекомендацій.

6) Доведення результатів перевірки до відома відповідальних осіб: Звіт про результати перевірки надається керівництву відповідних структурних підрозділів та іншим зацікавленим особам.

7) Контроль за виконанням рекомендацій. Здійснюється моніторинг виконання розроблених рекомендацій та оцінка ефективності вжитих заходів.

4.9.1. Перевірка достовірності джерела походження інформації додатково може включати:

- ✓ Ідентифікацію джерела: Визначення особи або системи, що є першоджерелом інформації.
- ✓ Оцінку надійності джерела: Аналіз репутації, компетентності та незалежності джерела.
- ✓ Перевірку каналів передачі інформації: Оцінка безпеки та цілісності каналів, через які надходить інформація.
- ✓ Підтвердження інформації з інших незалежних джерел (за можливості).
- ✓ Аналіз контролів за вводом та обробкою даних у системах обліку, реєстрації та звітності.

4.10. Під час комунікації *з зовнішніми користувачами* розробляються та впроваджуються заходи з контролю. Такі заходи включають отримання інформації від зовнішніх користувачів та передавання цієї інформації в межах організаційної структури Товариства, що дає змогу Товариству визначати тенденції, події або обставини, які можуть вплинути на досягнення цілей Товариства.

Здійснюючи комунікацію із зовнішніми користувачами, забезпечується:

- надання актуальної та своєчасної інформації щодо діяльності Товариства зовнішнім користувачам, уключаючи учасника, партнерів, клієнтів, наглядові, контролюючі, правоохоронні органи;

- отримання інформації щодо функціонування СВК від зовнішніх аудиторів, наглядових органів, інших зовнішніх користувачів з метою ухвалення адекватних управлінських рішень.

4.11. Від зовнішніх користувачів отримується інформація про функціонування СВК про:

- оцінку СВК зовнішніми аудиторами та наглядовими (контролюючими) органами;

- відгуки клієнтів стосовно якості надання фінансових послуг;

- публікації про Товариство у засобах масової інформації, на інформаційних сайтах, у зовнішніх інформаційних системах.

Отримана інформація передається до того структурного підрозділу або конкретної посадової особи, до компетенції якої належить її розгляд та подальша обробка.

4.11.1. Забезпечення конфіденційності та захисту даних: Передавання, обробка та збереження інформації, що містить персональні дані або іншу конфіденційну інформацію, здійснюється із вживанням необхідних технічних і організаційних заходів, із забезпеченням контролю умов використання інформації.

4.12. Заходи контролю під час здійснення зовнішньої комунікації включають:

- ✓ Визначення уповноважених осіб: Чітке визначення кола осіб, уповноважених здійснювати зовнішню комунікацію від імені Товариства за різними каналами (офіційні листи, електронна пошта,

телефонні розмови, соціальні мережі, веб-сайт тощо).

- ✓ Відповідність затвердженим стандартів комунікації, включаючи:
  - Формати офіційних документів.
  - Шаблони стандартних відповідей на типові запити.
  - Правила ведення телефонних розмов.
  - Порядок розміщення інформації на веб-сайті та в соціальних мережах.
- ✓ Погодження важливої інформації: Встановлення процедури обов'язкового погодження важливої інформації, що надається зовнішнім користувачам (наприклад, офіційні заяви, фінансова звітність, роз'яснення щодо послуг).
- ✓ Ведення обліку зовнішньої комунікації: Забезпечення обліку важливої зовнішньої комунікації (реєстрація вихідної кореспонденції, телефонограм, договорів тощо з подальшим їх збереженням до закінчення строку зберігання та знищення у встановленому законодавством порядку).
- ✓ Навчання персоналу: Проведення регулярного навчання персоналу з питань стандартів зовнішньої комунікації, етики спілкування та вимог щодо захисту інформації.
- ✓ Моніторинг зовнішніх комунікацій: Здійснення періодичного моніторингу зовнішніх комунікацій для виявлення та усунення можливих порушень стандартів.
- ✓ Контроль за актуальністю інформації на веб-сайті та в інших публічних джерелах: Забезпечення регулярного оновлення та перевірки актуальності інформації, розміщеної на офіційних ресурсах Товариства.

4.13. Перевірка інформації від зовнішніх користувачів здійснюється з метою встановлення її достовірності, повноти та відповідності вимогам законодавства та внутрішнім процедурам. Порядок перевірки може включати:

✓ Перевірка ідентифікації особи: У випадках, передбачених законодавством або ВД, здійснюється перевірка ідентифікації особи, яка надала інформацію (перевірка документів, що посвідчують особу).

✓ Перевірка достовірності документів: У разі отримання документів від зовнішніх користувачів, здійснюється їхня первинна перевірка на наявність ознак підробки, пошкоджень, відповідність встановленим формам та вимогам.

✓ Верифікація інформації: Здійснення верифікації наданої інформації шляхом її порівняння з іншими доступними джерелами (внутрішні бази даних, зовнішні реєстри, публічна інформація).

✓ Запит додаткової інформації: У разі необхідності, для підтвердження або уточнення отриманої інформації, здійснюється запит додаткових даних у зовнішнього користувача.

✓ Консультації з профільними фахівцями: У складних або нестандартних випадках, для перевірки отриманої інформації може залучатися працівник юридичного управління або іншого компетентного підрозділу Товариства.

РОЗДІЛ 5. МОНІТОРИНГ ЕФЕКТИВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ

5.1. Моніторинг СВК здійснюється в Товариства з метою:

- визначення здатності СВК забезпечити досягнення цілей діяльності Товариства;
- оцінки якості СВК у визначений період часу;
- визначення ймовірності виникнення недоліків, що впливають на досягнення цілей Товариства;
- оцінки суттєвості цих недоліків;
- розробки заходів з метою вдосконалення СВК.

5.2. Види заходів з моніторингу СВК обираються як комбінація поточних та періодичних заходів контролю з урахуванням встановлених цілей діяльності Товариства, характеру, обсягу та складності операцій, кількості та складності видів контролю, ризику виникнення недоліків, а також кваліфікації та досвіду працівників Товариства. Відповідальність за проведення таких заходів у межах визначених Товариством повноважень несуть:

- головний комплаєнс- менеджер та головний ризик-менеджер – за моніторинг ефективності процедур контролю на першій лінії захисту в межах виконання функцій незалежного контролю другої лінії захисту;

- внутрішній аудитор - за оцінку ефективності СВК Товариства в цілому.

5.3. СВК включає в себе заходи моніторингу всіх процесів/функцій Товариства та зосереджена на організаційних питаннях і механізмах контролю.

5.4. Усі ВД регулярно переглядаються на предмет відповідності нормам чинного законодавства та нормативно – правових актів, в тому числі перегляду підлягають процедури внутрішнього контролю.

Всі учасники процесів зобов`язані у своїй роботі суворо дотримуватись затверджених ВД.

5.5. З метою оперативного виявлення та усунення недоліків, всі працівники Товариства, в ході виконання своїх посадових обов'язків/ проведення щоденних операцій, дотримуючись вимог ВД Товариства, здійснюють самостійний превентивний попередній/поточний контроль.

З метою виявлення недоліків після факту події, керівниками відповідних підрозділів або особами, визначеними посадовими інструкціями, здійснюється подальший виявляючий/коригуючий, постійний/періодичний, повний/портфельний/вибірковий контроль.

5.6. Періодичні заходи з моніторингу СВК здійснюються з урахуванням:

- характеру та обсягу питань з урахуванням складності операцій, ризику порушень та випадків виникнення порушень у СВК в минулому;

- частоти моніторингу питань з урахуванням обсягу та складності операцій, основних видів контролю, частоти і характеру змін, що відбуваються в операційному середовищі;

- тривалості проведення заходів з моніторингу;

- достатності та рівня кваліфікації працівників, відповідальних за проведення заходів, та наданих цим працівникам повноважень;

- порядку підготовки звітів щодо результатів моніторингу СВК, обговорення та затвердження цих звітів;

- достатності та повноти необхідної інформації щодо проведення заходів з моніторингу.

5.7. Керівники підрозділів самостійно визначають ділянки процесів/функцій, які підлягають внутрішньому контролю.

5.8. Головний комплаєнс-менеджер та головний ризик-менеджер також можуть ініціювати створення нових контролів як на етапі створення нового процесу, так і на етапі роботи вже існуючого. Причиною створення додаткових контролів можуть бути виявлення нових операційних ризиків, зауваження аудиту, контролюючих органів та ін. Впровадження таких контролів здійснюється шляхом внесення змін до ВД.

5.9. Товариство здійснює обов'язкові поточні та періодичні заходи з моніторингу ефективності СВК у наступному порядку:

Критерій	Поточні заходи моніторингу СВК	Періодичні заходи моніторингу СВК
Періодичність	1 раз на квартал	1 раз на рік

Відповідальні виконавці	Суб'єкти першої та другої ліній захисту	Суб'єкт третьої лінії захисту
Мета	Оперативне виявлення та усунення недоліків СВК	Оцінка ефективності СВК в цілому з метою виявлення недоліків після факту події

5.10. Товариство установлює розподіл відповідальності за ефективність СВК наступним чином:

Суб'єкти СВК	**Відповідальність у межах СВК**
Наглядова рада	відповідальність за ефективність СВК в межах Товариства
Виконавчий орган-Правління	в межах своїх повноважень забезпечує виконання рішень відповідального органу фінансової компанії щодо забезпечення організації та функціонування системи внутрішнього контролю фінансової компанії
Суб'єкти першої лінії захисту	безпосередня відповідальність за виконання заходів щодо виправлення недоліків СВК
Головний ризик-менеджер, головний комплаєнс-менеджер	відповідальність за якість виконання заходів із моніторингу СВК (за винятком оцінки ефективності СВК)
Внутрішній аудитор	відповідальність за якість оцінки ефективності СВК

5.11. Вимоги до здійснення моніторингу ефективності СВК включають наступне:

• Наглядова рада забезпечує здійснення щорічної оцінки ефективності СВК внутрішнім аудитором. Відповідальний за консолідацію щорічного звіту - Внутрішній аудитор.

• Наглядова рада забезпечує здійснення суб'єктами другої лінії захисту квартального моніторингу якості виконання заходів з контролю СВК. Відповідальний за консолідацію квартального звіту - Головний комплаєнс-менеджер. Після розгляду звіту Головний комплаєнс-менеджер надає керівникам підрозділів пропозиції щодо підвищення ефективності внутрішнього контролю та здійснення коригуючих дій (внесення змін в наявні ВД, створення нових, при необхідності - посилення існуючих засобів контролю або запровадження нових тощо).

РОЗДІЛ 6. ПРОЦЕДУРА ВИПРАВЛЕННЯ НЕДОЛІКІВ ФУНКЦІОНУВАННЯ СВК

6.1. Недоліки в СВК можуть бути виявлені на усіх трьох лініях захисту.

6.2. Недоліки у функціонуванні СВК можуть бути виявлені через наступні джерела:

✓ Результати виконання контрольних процедур: Виявлені відхилення, помилки, невідповідності під час здійснення щоденних, періодичних та спеціальних контрольних процедур, передбачених цим Положенням.

✓ Звіти про виявлені порушення та інциденти: Інформація про факти порушень внутрішніх регламентів, законодавства та інші інциденти, що свідчать про неефективність окремих елементів СВК.

✓ Зворотний зв'язок від співробітників: Повідомлення, пропозиції та зауваження співробітників щодо проблемних аспектів функціонування СВК, виявлених ними в процесі роботи.

✓ Результати самооцінки контролів: Оцінки ефективності контролів, що проводяться керівниками та співробітниками структурних підрозділів.

✓ Звіти внутрішнього аудитора: Висновки та рекомендації внутрішніх аудиторів, отримані в результаті проведення незалежних аудитів окремих процесів та СВК в цілому.

✓ Звіти зовнішніх аудиторів та регуляторних органів: Зауваження, рекомендації та вимоги зовнішніх аудиторів та регуляторних органів щодо вдосконалення СВК.

✓ Аналіз скарг клієнтів: Скарги клієнтів, що свідчать про недостатність або неефективність внутрішніх процесів та контролів.

6.3. Діяльність підрозділів / працівників першої лінії захисту в межах СВК спрямована на виявлення інцидентів операційного ризику чи комплаєнс-ризику будь-яким працівником Товариства.

У разі недосконалості процесу або неякісного існуючого контролю керівник підрозділу першої лінії захисту може зробити висновок про необхідність здійснення коригувальних заходів для усунення виявлених недоліків процесів.

6.4. Суб'єкти другої лінії захисту:

- забезпечують належне здійснення підрозділами / працівниками першої лінії захисту реалізації на практиці компонентів СВК;
- забезпечують своєчасне повідомлення виконавчого органу та Наглядової ради про виявлені недоліки СВК та/або допущені підрозділами / працівниками першої лінії захисту порушення та причини їх вчинення;
- визначають відповідальних за прийняття рішення про здійснення коригувальних заходів, усунення порушення та/або внесення змін до внутрішніх документів.

6.5. Недоліки і порушення виявляються суб'єктами другої лінії захисту під час управління інцидентами операційного ризику чи комплаєнс-ризику та при здійсненні власних контрольних процедур. Коригувальні заходи проводяться в межах прийняття рішення щодо управлінням ризиком: «мінімізувати» ризик або «уникнути/передати» ризик.

Суб'єкти другої лінії захисту надають на квартальній основі в межах системи управління ризиками звітність по напрямках ризиків та, у разі необхідності, вказують проведені коригувальні заходи щодо виправлення виявлених недоліків СВК.

6.6. Процес виправлення недоліків СВК базується на наступних принципах:

✓ **Оперативність:** Вжиття заходів щодо усунення виявлених недоліків у найкоротші терміни.

✓ **Адекватність:** Розробка та впровадження коригувальних дій, що є адекватними характеру та значущості виявленого недоліку.

✓ **Системність:** Усунення не лише наслідків недоліку, але й його першопричин для запобігання повторенню.

✓ **Відповідальність:** Чітке визначення відповідальних осіб за розробку, затвердження та виконання коригувальних дій.

✓ **Контроль:** Забезпечення контролю за процесом виконання коригувальних дій та оцінка їхньої ефективності.

✓ **Документування:** Фіксація виявлених недоліків, розроблених коригувальних дій, стану їх виконання та результатів оцінки ефективності.

6.7. Порядок виправлення недоліків, виявлених суб'єктами першої лінії захисту

При виявленні недоліків СВК суб'єктами першої лінії захисту (керівниками та співробітниками структурних підрозділів) застосовується наступний порядок:

- **Негайне інформування:** Негайне інформування безпосереднього керівника про виявлений недолік.
- **Первинна оцінка та локалізація:** Безпосередній керівник проводить первинну оцінку значущості недоліку та вживає оперативних заходів для його локалізації та мінімізації негативного впливу в межах своєї компетенції.

- **Розробка та впровадження коригувальних дій:** Керівник структурного підрозділу відповідає за розробку та впровадження простих та оперативних коригувальних дій для усунення недоліку в межах компетенції підрозділу.
- **Інформування другої лінії захисту (за потреби):** Якщо виявлений недолік є значним, має системний характер або потребує координації з іншими підрозділами, інформація ескалюється до відповідного суб'єкта другої лінії захисту.
- **Звітування:** Інформація про виявлені та усунені недоліки включається до звітності підрозділу.

6.8. Порядок виправлення недоліків, виявлених суб'єктами другої лінії захисту

При виявленні недоліків СВК суб'єктами другої лінії захисту застосовується наступний порядок:

- **Документування недоліку:** Детальне документування виявленого недоліку, включаючи його опис, потенційний вплив та рекомендації щодо усунення.
- **Інформування першої лінії захисту:** Надання інформації про виявлений недолік керівнику відповідного структурного підрозділу першої лінії захисту для розробки та впровадження коригувальних дій.
- **Узгодження плану коригувальних дій:** Участь у розробці плану коригувальних дій, забезпечення його адекватності та встановлення термінів виконання.
- **Моніторинг виконання плану коригувальних дій:** Здійснення контролю за своєчасним та якісним виконанням запланованих коригувальних дій.
- **Оцінка ефективності коригувальних дій:** Оцінка ефективності впроваджених заходів щодо усунення недоліку та запобігання його повторенню.
- **Ескалація інформації (за потреби):** У разі невиконання плану коригувальних дій у встановлені терміни або виявлення неефективності вжитих заходів, інформація ескалюється на вищий рівень управління (керівництву Товариства).
- **Звітування:** Інформація про виявлені недоліки та стан їх виправлення включається до регулярної звітності другої лінії захисту.

6.9. Порядок виправлення недоліків, виявлених суб'єктом третьої лінії захисту

При виявленні недоліків СВК Внутрішнім аудитором застосовується наступний порядок:

- **Оформлення аудиторського звіту:** Детальне відображення виявлених недоліків, оцінка їхнього впливу та надання рекомендацій щодо усунення в аудиторському звіті.
- **Доведення звіту до відома керівництва:** Надання аудиторського звіту Наглядовій раді Органу управління, та керівникам відповідних структурних підрозділів першої та суб'єктам другої ліній захисту.
- **Розробка плану коригувальних дій:** Керівники відповідних структурних підрозділів розробляють план коригувальних дій на основі рекомендацій внутрішнього аудиту та надають його на затвердження керівництву Товариства.
- **Затвердження плану коригувальних дій:** План коригувальних дій затверджується Наглядовою радою із зазначенням термінів виконання та відповідальних осіб.
- **Моніторинг виконання плану коригувальних дій:** Внутрішній аудитор здійснює моніторинг виконання затвердженого плану коригувальних дій.
- **Верифікація усунення недоліків:** Після завершення термінів виконання, Внутрішній аудитор проводить верифікацію фактичного усунення виявлених недоліків та оцінює ефективність вжитих заходів.

- **Звітування:** Результати моніторингу та верифікації виконання планів коригувальних дій відображаються у звітах внутрішнього аудиту, що надаються органу управління Товариства.

6.10. Порядок виправлення недоліків, виявлених зовнішніми аудиторами

При виявленні недоліків СВК зовнішніми аудиторами застосовується наступний порядок:

- **Аналіз звіту зовнішнього аудитора:** Керівництво Товариства та відповідні структурні підрозділи проводять детальний аналіз звіту зовнішнього аудитора та виявлених недоліків.
- **Розробка плану коригувальних дій:** На основі рекомендацій зовнішнього аудитора розробляється план коригувальних дій із зазначенням конкретних заходів, термінів виконання та відповідальних осіб.
- **Затвердження плану коригувальних дій:** План коригувальних дій затверджується Наглядовою радою.
- **Впровадження коригувальних дій:** Відповідальні особи забезпечують своєчасне та якісне впровадження запланованих коригувальних дій.
- **Звітування перед зовнішнім аудитором (за потреби):** Надання інформації зовнішнім аудиторам про стан виконання плану коригувальних дій у встановлені терміни.
- **Внутрішній контроль за виконанням:** Внутрішній аудитор (або інший визначений підрозділ) здійснює контроль за виконанням плану коригувальних дій.

6.11. Порядок виправлення недоліків відповідно до рішення НБУ про застосування коригувальних заходів

При отриманні рішення НБУ про застосування коригувальних заходів щодо СВК застосовується наступний порядок:

- **Детальне вивчення рішення НБУ:** Керівництво Товариства та відповідні структурні підрозділи проводять детальне вивчення рішення НБУ та визначених недоліків.
- **Розробка плану заходів щодо усунення порушень:** На основі вимог НБУ розробляється детальний план заходів щодо усунення виявлених порушень та недоліків із зазначенням конкретних дій, термінів виконання та відповідальних осіб.
- **Затвердження плану заходів:** План заходів затверджується Наглядовою радою.
- **Погодження плану заходів з НБУ (за потреби):** У випадках, передбачених рішенням НБУ, розроблений план заходів погоджується з НБУ.
- **Виконання плану заходів:** Відповідальні особи забезпечують своєчасне та повне виконання запланованих заходів.
- **Звітування перед НБУ:** Надання звітності до НБУ про стан виконання плану заходів у встановлені терміни.
- **Внутрішній контроль за виконанням:** Внутрішній аудитор здійснює контроль за виконанням плану заходів та оцінює ефективність вжитих заходів.

РОЗДІЛ 7. ОРГАНІЗАЦІЯ ЗВІТУВАННЯ ЩОДО ФУНКЦІОНУВАННЯ СВК

7.1. Метою звітування є забезпечення Органу управління, керівництва та інших зацікавлених осіб своєчасною, повною та достовірною інформацією про стан внутрішнього контролю, виявлені недоліки, ризики та ефективність вжитих заходів для прийняття обґрунтованих управлінських рішень та постійного вдосконалення системи внутрішнього контролю.

7.2. В рамках системи внутрішнього контролю Товариства формуються наступні основні види звітів:

Вид звіту	Періодичність	Виконавець звіту	Орган (суб'єкт), якому надається	Зміст
Звіти про результати контрольних процедур	щоквартально	Працівники/керівники структурних підрозділів	Керівник структурного підрозділу, внутрішній аудитор	Відображають результати виконання конкретних контрольних процедур, спрямованих на виявлення та запобігання помилкам, шахрайству та неефективності в окремих бізнес-процесах або сферах діяльності Товариства.
Звіти про виявлені порушення та інциденти	Негайно після виявлення	Співробітник, який виявив порушення/керівник структурного підрозділу	Керівник структурного підрозділу, CRO/CCO	Містять інформацію про факти виявлених порушень внутрішніх політик, процедур, законодавства, а також про операційні інциденти (збої, помилки, втрати), шахрайські дії та інші нештатні події, що мали або могли мати негативний вплив на СВК Товариства
Звіти про оцінку ризиків та контролів	Щоквартально	Керівники структурних підрозділів	CRO, CCO	Відображають результати періодичної або спеціальної оцінки ідентифікованих ризиків, їхньої ймовірності та потенційного впливу, а також оцінку адекватності та ефективності існуючих контрольних заходів, спрямованих на управління цими ризиками.
Звіти про виконання планів коригувальних дій	Відповідно до строку реалізації коригувальних дій	Відповідальні співробітники/керівники структурних підрозділів, CRO, CCO	Наглядова рада, внутрішній аудитор (за потреби)	Надають інформацію про стан виконання планів коригувальних дій, розроблених для усунення виявлених недоліків, порушень або для вдосконалення системи контролів.
Звіти служби внутрішнього аудиту	Відповідно до плану аудиту	Внутрішній аудитор	Наглядова рада, Правління (вище керівництво)	Відображають результати незалежних внутрішніх аудитів окремих бізнес-процесів, структурних підрозділів або СВК в цілому. Містять незалежну оцінку адекватності та ефективності системи управління ризиками, контролю та корпоративного управління.
Спеціальні звіти	За потреби	Визначається залежно від теми (потреби) звіту	Визначається залежно від адресата запиту або теми звіту	Готуються за вимогою Наглядової ради/CRO CCO/Внутрішнього аудитора для розгляду конкретних питань, пов'язаних з внутрішнім контролем, управлінням ризиками або корпоративним управлінням.

7.3. Порядку розгляду звітів:

7.3.1. Звіти про результати контрольних процедур

✓ Керівник структурного підрозділу: Отримує звіт, вивчає виявлені відхилення, аналізує причини їх виникнення. Приймає оперативні рішення щодо усунення недоліків у межах своєї компетенції та вживає заходів для запобігання їхньому повторенню.

✓ Внутрішній аудитор (за потреби): Отримує звіт для моніторингу загальних тенденцій, виявлення системних проблем та оцінки ефективності контрольних процедур на рівні Товариства. Може ініціювати додаткові перевірки або рекомендувати зміни до контрольних процедур.

7.3.2. Звіти про виявлені порушення та інциденти

✓ Керівник структурного підрозділу: Негайно розглядає звіт, оцінює серйозність порушення/інциденту, вживає першочергових заходів для локалізації наслідків та інформує вище керівництво та відповідних працівників (CRO/CCO).

✓ Головний комплаєнс-менеджер: Розглядає звіт з точки зору дотримання законодавства та внутрішніх нормативних документів, проводить розслідування (за потреби), визначає необхідні коригувальні та дисциплінарні заходи.

✓ Головний ризик-менеджер: Аналізує звіт для оцінки операційних ризиків, потенційного впливу на діяльність Товариства, а також для виявлення слабких місць у системі внутрішнього контролю, що могли призвести до порушення/інциденту.

✓ Керівництво Товариства: Отримує інформацію про значні порушення та інциденти, приймає рішення щодо подальших дій, контролює процес розслідування та вжиття заходів.

7.3.3. Звіти про оцінку ризиків та контролів

✓ Головний ризик-менеджер: Аналізує звіт, узагальнює результати оцінки, визначає пріоритетні ризики та недостатні контролі. Оцінює загальний рівень ризиків та ефективність системи контролів на рівні Товариства, затверджує плани дій щодо вдосконалення контролів. Розробляє рекомендації щодо вдосконалення контрольних заходів.

✓ Керівники структурних підрозділів: Розглядають звіт щодо ризиків та контролів у своїх підрозділах, оцінюють адекватність існуючих контролів та розробляють плани дій щодо впровадження рекомендованих заходів.

✓ Правління: Отримує інформацію про ключові ризики та стан контрольного середовища, контролює виконання планів дій.

7.3.4. Звіти про виконання планів коригувальних дій

✓ Головний ризик-менеджер: Отримує та аналізує звіт, відстежує прогрес у виконанні планів коригувальних дій, оцінює ефективність вжитих заходів. Інформує керівництво про стан виконання.

✓ Керівники структурних підрозділів: Розглядають звіт щодо виконання планів у своїх підрозділах, вживають заходів для забезпечення своєчасного та якісного виконання.

✓ Внутрішній аудитор (за потреби): Може використовувати ці звіти для моніторингу виконання аудиторських рекомендацій.

✓ Керівництво Товариства: Контролює загальний прогрес у виконанні планів коригувальних дій та вживає заходів у разі виявлення затримок або неефективності.

7.3.5. Звіти внутрішнього аудитора

Суб’єкт третьої лінії захисту за результатами здійснення моніторингу ефективності СВК складає звіти, що надаються на розгляд Наглядовій раді. Ці звіти мають містити інформацію про виявлені недоліки СВК та порушення, аналіз причин їх виникнення, ймовірні наслідки, до яких можуть призвести ці недоліки, рекомендації/пропозиції щодо підвищення ефективності функціонування системи внутрішнього контролю, процес контролю за станом виконання рекомендацій/пропозицій, затверджених раніше. В аудиторському звіті викладаються виявлені недоліки в діяльності Товариства,

порушення Товариством вимог законодавства України, причини, що зумовили такі недоліки та/або порушення, а також пропозиції щодо їх усунення.

✓ Наглядова рада: Є основним органом, що розглядає звіти внутрішнього аудиту, оцінює незалежність та об'єктивність, розглядає виявлені недоліки та рекомендації. Отримує інформацію про результати внутрішніх аудитів та ключові висновки, здійснює нагляд за функціонуванням СВК та діями керівництва щодо реагування на аудиторські рекомендації.

✓ Правління: Розглядає звіти внутрішнього аудиту, розробляє та впроваджує плани коригувальних дій у відповідь на аудиторські рекомендації.

✓ Внутрішній аудитор повинен відслідковувати й фіксувати фактичне здійснення необхідних заходів з виправлення недоліків, виявлених під час аудиту, а також виконання рекомендацій шляхом відповідного аудиторського спостереження.

7.3.6. Спеціальні звіти

✓ Визначається в кожному конкретному випадку залежно від теми та адресата звіту. Як правило, звіт розглядається тим органом або посадовою особою, за чиєю вимогою він був підготовлений. Може передбачати обговорення, прийняття рішень та розробку планів дій щодо вирішення порушеного питання.

РОЗДІЛ 8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

8.1. Положення вступає в силу з дня його затвердження Наглядовою радою Товариства. Зміни та доповнення до Положення набирають чинності з дня їх затвердження Наглядовою радою Товариства. В разі викладення змін та доповнень у вигляді нової редакції Положення, попередня редакція Положення втрачає чинність з дня набрання чинності нової редакції.

8.2. Перегляд на предмет необхідності актуалізації Положення здійснюється не рідше одного разу на три роки. Причинами внесення змін до Положення можуть бути зміни в організаційній структурі Товариства, зміни в законодавчих, регуляторних та інших нормах.

8.3. У разі невідповідності будь-якої частини Положення чинному законодавству України або нормативно-правовим актам, у тому числі у зв'язку з прийняттям нових актів законодавства України або нових нормативно-правових актів, це Положення буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України або нормативно-правовим актам.

8.4. Положення є обов'язковим до виконання всіма працівниками Товариства, у межах їх посадових обов'язків.