ЗАТВЕРДЖЕНО
Рішенням Наглядової ради
АТ "Укрпошта" від «28» березня 2025 р.,
протокол засідання №4

ПОЛІТИКА
управління ризиками АТ "Укрпошта"

ЗМІСТ

І. ВСТУП

1.1 Політика управління ризиками АТ «Укрпошта» (далі – **Політика**) визначає цілі, завдання та принципи системи управління ризиками АТ «Укрпошта» (далі – **Товариство**), структуру управління ризиками, основні етапи процесу управління ризиками, інструменти оцінки та управління ризиками, встановлює системний підхід до управління ризиками Товариства.
1.2 Політика розроблена з урахуванням найкращих міжнародних практик і стандартів: ISO 31000:2018 «Менеджмент ризиків», ДСТУ IES/ISO 31010:2014, методології COSO ERM Framework (Committee of Sponsoring Organizations of the Treadway Commission), FERMA (Стандарт Асоціацій Ризик Менеджерів), регулятивних норм Національного банку України (далі – **НБУ**) та Міністерства розвитку громад та територій України (далі – **Міністерство**).
1.3 Метою впровадження комплексної системи управління ризиками в Товаристві є організація чіткого процесу з ефективного управління ризиками та сприяння досягненню стратегічних цілей Товариством шляхом своєчасної та повної ідентифікації ризиків та можливостей, забезпечення їх всебічного аналізу, проведення оцінки ризиків та можливостей, розробка заходів з мінімізації ризиків та дотримання і контроль за прийнятним для Товариства рівнем ризику.
1.4 Управління ризиками є невід'ємною складовою ефективного корпоративного управління, процесів планування та прийняття рішень, відповідно управління ризиками інтегровано в усі процеси Товариства та сприяє наданню гарантій зацікавленим сторонам в прийнятті зважених та ефективних рішень.

ІІ. СФЕРА ЗАСТОСУВАННЯ

2.1 Дія Політики розповсюджується на всі процеси та діяльність всіх працівників та всі структурні підрозділи Товариства.
2.2 Політика є частиною внутрішнього трудового розпорядку Товариства та є обов'язковою для ознайомлення і використання для всіх співробітників Товариства. При виконанні функціональних обов'язків і реалізації поставлених завдань, якщо це пов'язано з управлінням ризиками Товариства, кожен співробітник Товариства керується пунктами Політики.
2.3 Кожен керівник структурного підрозділу Товариства несе відповідальність за дотримання вимог даної Політики співробітниками відповідного структурного підрозділу.
2.4 Політика затверджується рішенням Наглядової ради. Перегляд Політики здійснюється за рішенням Наглядової ради, але не рідше ніж раз на два роки.
2.5 Генеральний директор Товариства (далі – **керівник Товариства**) відповідає за реалізацію даної Політики.

ІІІ. ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

3.1 В Політиці використовується такі поняття та терміни:

- ССО (Chief Compliance Officer – Директор з комплаєнсу) – головна посадова особа Товариства, відповідальна за здійснення контролю за дотриманням норм (комплаєнс), яка виконує функції головного комплаєнс-менеджеру в Товаристві.

- CRO (Chief Risk Officer – Директор з управління ризиками) – головна посадова особа Товариства, відповідальна за управління ризиками.
- Cost-benefit analysis (аналіз витрат і вигод) під час інвестиційного аналізу – це метод оцінки ефективності потенційних інвестицій, що полягає у порівнянні очікуваних загальних витрат із можливими вигодами від інвестиційного проекту. Основна мета цього аналізу полягає у прийнятті обґрунтованого рішення щодо того, чи перевищують очікувані вигоди асоційовані з проектом витрати.
- ESG-принципи (Environmental, Social and Governance) – це набір стандартів, які використовуються для оцінки діяльності Товариства з точки зору її впливу на довкілля, соціальну сферу та корпоративне управління.
- ESG-ризики (Environmental, Social and Governance) – ризики пов'язані з екологічними чинниками, соціальним розвитком, рівнем корпоративного управління.
- Risk Universe («довгий список» ризиків) – це загальний класифікований список ризиків, які можуть бути характерними для Товариства. «Довгий список» використовується для подальшого аналізу ризиків на предмет відповідності для Товариства, процесів чи функцій Товариства.
- Власник ризику – особа (працівник / структурний підрозділ / колегіальний орган) Товариства, на яку покладено відповідальність за реалізацію заходів з управління ризиком, і яка володіє достатніми повноваженнями для реалізації заходів з управління ризиком.
- Внутрішній контроль – комплекс заходів, що застосовується для забезпечення дотримання законності та ефективності використання коштів, досягнення результатів відповідно до встановленої мети, завдань, планів і вимог щодо діяльності.
- Вплив ризику – розмір втрат та/або потенційних втрат, які можуть бути понесені Товариством в результаті реалізації ризику.
- Граничні значення KRI – можливі значення (або діапазон значень) KRI, які сигналізують про таку зміну рівня ризику, що може спричинити недосягнення цілей. Граничні значення є інструментом контролю та моніторингу стану ризикоутворюючих факторів, перевищення яких є сигналом Власнику ризику для прийняття відповідних рішень щодо управління ризиками.
- Декларація схильності до ризику (RAS - Risk Appetite Statement) – внутрішній документ, який визначає сукупну величину ризик-апетиту, види ризиків, які Товариство прийматиме або уникатиме з метою досягнення його бізнес-цілей, та рівень ризик-апетиту щодо кожного з них (індивідуальний рівень).
- Джерело ризику – елемент, який сам по собі, чи в комбінації з іншими, може призвести до виникнення ризику.
- Ескалація – порядок звітування про суттєві (критичні) події на рівень Наглядової ради.
- Залишковий ризик – це ризик, що залишився після виконаних дій по зниженню притаманного ризику.
- Ймовірність – можливість того, що певна подія відбудеться.
- Карта ризиків (Risk Heat Map) – інструмент узагальнення інформації про топ-ризики Товариства, графічне зображення оцінки ризику, побудоване на основі двох параметрів: ймовірності реалізації ризику та рівня впливу ризику на діяльність Товариства.

- Ключові індикатори ризику (Key Risk Indicators – KRI) – показники, які дозволяють судити про рівень ризику і динаміку цього рівня в часі. KRI є інструментом моніторингу та використовується для раннього сповіщення про зміну рівня ризику, ефективність заходів (в т.ч. контролю) з управління ризиком.
- Комплаєнс-ризик – ризик невідповідності діяльності Товариства вимогам законодавства, регуляторним нормам, внутрішнім політикам, а також етичним вимогам, що можуть нести за собою правові, репутаційні та інші наслідки.
- Культура ризиків (Risk Culture) – принципи, правила, норми поведінки працівників, пов'язані з поінформованістю щодо ризиків, прийняттям ризиків та управлінням ризиками, а також засоби управління, які формують рішення щодо ризиків. Є складовою загальної корпоративної культури Товариства та сприяє формуванню достатнього рівня обізнаності всіх працівників щодо важливості та правил функціонування системи управління ризиками та залученості всіх працівників до процесу управління ризиками.
- Ліміт ризику – обмеження, установлені Товариством для контролю величини ризиків, на які наражається Товариство протягом своєї діяльності.
- Мінімізація ризику – процес модифікації ризику, що має за мету зменшення або усунення негативного впливу.
- Модель Трьох ліній захисту – модель, розроблена Інститутом внутрішніх аудиторів, яка пов'язує між собою усі рівні управління: операційний менеджмент (перша лінія), контрольні функції (друга лінія), незалежна контрольна функція – внутрішній аудит (третя лінія).
- Перша лінія захисту – на рівні структурних підрозділів Товариства, що безпосередньо пов'язані з наданням товарів/послуг клієнтам, а також підрозділів, що забезпечують діяльність Товариства. Ці підрозділи приймають ризики в процесі своєї діяльності та несуть відповідальність за поточне управління цими ризиками, здійснюють заходи з контролю.
- Друга лінія захисту – на рівні CRO/Управління з менеджменту ризиків, ССО/Підрозділу комплаєнсу, Служби із запобігання та виявлення корупції, Управління фінансового моніторингу. Ці підрозділи забезпечують впевненість органів Товариства, що впроваджені першою лінією захисту заходи з контролю та управління ризиками були розроблені та функціонують належним чином.
- Третя лінія захисту – на рівні Департаменту внутрішнього аудиту, який здійснює незалежну оцінку ефективності діяльності першої та другої ліній захисту та загальну оцінку ефективності системи управління ризиками та внутрішнього контролю.
- Можливість – вплив невизначеності на цілі, що виражається через співвідношення рівня ймовірності та розміру позитивного впливу від наслідків настання подій та дій, які викликають невизначеність в досягненні цілей Товариства.
- Моніторинг ризиків – це процес періодичного розгляду визначених ризиків та контролю реалізації заходів щодо їх зменшення, за допомогою спеціальної звітності.
- Наслідки – результат події, що впливає на цілі.
- Обробка ризиків – процес модифікації ризику, що має за мету зменшення або усунення негативного впливу.
- Операційний інцидент – це подія, які призводять до реалізації операційного ризику.

- Оцінка ризику – процес, що поєднує ідентифікацію, аналіз та порівняльну оцінку ризику на предмет ймовірності настання та розміру впливу. Ризик може бути оцінений для всього Товариства, його структурних підрозділів, окремих проєктів або окремої події. Оцінка ризику здійснюється з метою прийняття рішень для ефективного управління ризиком, що впливають на досягнення поставлених цілей.
- Подія – це виникнення або зміна певної сукупності обставин. Подія 1) може мати одне або декілька проявів, мати декілька причин і декілька наслідків, 2) може бути чимось очікуваним, що не відбувається, або чимось неочікуваним, що відбувається і 3) може бути джерелом ризику.
- Притаманний ризик – це ризик, оцінений без врахування будь-яких дій, вжитих Товариством, з метою змінити вірогідність реалізації ризику чи його впливу.
- Реєстр ризиків (Risk Register) – це база даних ідентифікованих ризиків та можливостей з визначеною оцінкою ризиків, яка містить всю інформацію про ризики Товариства, зокрема: опис та класифікацію ризиків, оцінку з рівнем впливу та ймовірності, грошову оцінку, стратегію реагування на ризик, відповідальних за заходи мінімізації та іншу інформацію, пов’язану з ризиками. Реєстр є робочим інструментом, який має оновлюватись по мірі актуалізації ризиків. Реєстр є джерелом аналітики про ризики організації.
- Рівень ризику – величина, яка виражена в рамках комбінації наслідків та їх ймовірності.
- Ризик – потенційна подія, що може призвести до негативних наслідків для Товариства.
- Ризик-координатор – співробітник структурного підрозділу Товариства, відповідальний за виявлення, самооцінку ризику, вжиття управлінських заходів та звітування щодо таких подій, а також за внутрішній контроль у Товаристві в межах своїх повноважень.
- Система управління ризиками – сукупність належним чином задокументованих і затверджених політики, методик і процедур управління ризиками, які визначають порядок дій, спрямованих на здійснення систематичного процесу виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення всіх видів ризиків на всіх організаційних рівнях.
- Спеціалізовані підрозділи – підрозділи Товариства, що виконують функцію управління ризиками.
- 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, які відповідають виключним (екстремальним), але ймовірним подіям.
- Суттєвий ризик – ризик, реалізація якого в прогнозному періоді призведе до відхилення ключового показника діяльності (ефективності) Товариства на величину, що перевищує затверджений рівень схильності до ризику. Істотний ризик визначається на основі карти ризиків.
- Схильність до ризику (Risk Appetite) – це сукупна величина за всіма видами ризиків та окремо за кожним із ризиків, визначених наперед та в межах допустимого рівня ризику, щодо яких Товариство прийняло рішення про доцільність/необхідність їх утримання з метою досягнення його стратегічних цілей та виконання бізнес-плану. Схильність до ризику закріплюється Декларацією схильності до ризику.

- Толерантність до ризику - це здатність приймати ризики в процесі діяльності Товариства. Це визначається не лише готовністю до прийняття ризикованих рішень, але і здатністю ефективно керувати цими ризиками та забезпечити стійкість Товариства до можливих негативних наслідків.
- Управління ризиками (ризик-менеджмент) – це безперервний процес виявлення, аналізу, оцінки, обробки, розробки заходів для зменшення збитків, моніторингу та контролю ризиків і фінансових ресурсів для зменшення несприятливих наслідків ризиків. Ефективна система управління ризиками та внутрішнього контролю допомагає Товариству досягати поставлених цілей.

IV. ЦІЛІ І ЗАВДАННЯ ПОЛІТИКИ З УПРАВЛІННЯ РИЗИКАМИ

4.1 Основними цілями Політики є:

4.1.1 Створення ефективної системи та структури управління і контролю за ризиками, розвитку можливостей, що включає ідентифікацію (виявлення), аналіз, оцінку, обробку, розробку заходів, контроль та моніторинг, звітування і подальший контроль заходів, що сприятиме керівництву Товариства, керівникам структурних підрозділів в досягненні стратегічних цілей Товариства, підвищенню ефективності корпоративного управління.

4.1.2 Забезпечення цілісності, повноти та достовірності інформації щодо управління ризиками, яка використовується для ухвалення управлінських рішень; створення інформаційних потоків як за вертикаллю, так і за горизонталлю організаційної структури Товариства; забезпечення керівництва та зацікавлених сторін достовірною звітністю.

4.1.3 Впровадження та формалізація уніфікованих підходів до управління ризиками в Товаристві з метою обмеження негативних наслідків, ефективного використання ресурсів та оптимізації процесів.

4.1.4 Визначення чіткої структури відповідальності в рамках системи управління ризиками.

4.1.5 Сприяння безперервності операційної діяльності Товариства.

4.1.6 Забезпечення ефективного розподілу ресурсів на основі рейтингу впливу ризику та схильності до ризику.

4.1.7 Впровадження практики управління ризиками в ділову культуру Товариства.

4.1.8 Сприяння сталому розвитку Товариства з урахуванням принципів ESG.

4.1.9 Забезпечення зростання довіри інвесторів за рахунок створення прозорої системи управління ризиками та можливостями та ефективності її впровадження.

4.1.10 Забезпечення дотримання вимог законодавства України, нормативно-правових актів Міністерства, НБУ, внутрішніх документів, стандартів професійних об’єднань, дія яких поширюється на Товариство.

4.2 Політика направлена на реалізацію таких завдань:

4.2.1 Впровадження структури управління ризиками в управлінський процес і процеси планування, що дозволить покращити якість прийнятих рішень, складання та затвердження довгострокових стратегій і планів Товариства з урахуванням ризиків та утримувати ризики, що вносять невизначеність в досягнення стратегічних цілей і ключових показників ефективності Товариства, на допустимому рівні.

4.2.2 Забезпечення функціонування комплексної та адекватної системи управління ризиками, що враховує специфіку роботи Товариства та встановлені НБУ та Міністерством вимоги щодо управління ризиками.

4.2.3 Опис методологічного супроводу процесів управління ризиками в Товаристві.

4.2.4 Опис підходів до визначення схильності до ризику, а також забезпечення ефективного управління суттєвими для Товариства ризиками.

4.2.5 Забезпечення безперервного процесу управління ризиками, що базується на своєчасному виявлені, оцінці, аналізі, обробці та моніторингу ризиків.

4.2.6 Визначення основних ризиків, притаманних діяльності Товариства.

4.2.7 Запобігання прямим і непрямим втратам, які є результатом реалізації ризиків та збереження активів Товариства.

4.2.8 Моніторинг та попередження порушень граничних показників та внутрішніх лімітів ризику, ескалація виявлених порушень.

4.2.9 Визначення основних вимог до організації діяльності ризик-координаторів.

4.2.10 Розвиток культури управління ризиками в Товаристві на всіх рівнях управління.

4.2.11 Забезпечення захисту інтересів акціонера, клієнтів, кредиторів та інших осіб, зацікавлених в стійкій роботі Товариства.

4.3 Основними принципами процесу управління ризиками Товариства є:

4.3.1 Інтегрованість. Управління ризиками має бути інтегроване в загальне управління Товариством, процеси прийняття рішень та операційну діяльність. Управління ризиками - це не окрема або ізольована функція, а невіддільна частина діяльності Товариства.

4.3.2 Структурованість та комплексний підхід. Структурований та комплексний підхід до управління ризиками сприяє отриманню послідовних і порівнянних результатів ідентифікації, аналізу, оцінки, обробки, моніторингу і контролю ризиків.

4.3.3 Зв’язок з цілями Товариства. Управління ризиками направлене на досягнення стратегічних і операційних цілей Товариства з урахуванням зовнішнього та внутрішнього середовища та сприяє постійному покращенню діяльності та виявленню можливостей для розвитку.

4.3.4 Превентивність. Управління ризиками носить превентивний характер та спрямовано на зменшення ймовірності реалізації ризиків та/або наслідків їх реалізації.

4.3.5 Адаптивність до змін. Ризики можуть виникати, змінюватися або зникати в міру того, як змінюється зовнішнє і внутрішнє середовище Товариства, його стратегічні та операційні цілі. Управління ризиками передбачає, виявляє, визнає та реагує на ці зміни та події належним чином та своєчасно.

4.3.6 Комунікація та залучення. Належне та своєчасне залучення та комунікація з зацікавленими сторонами дозволяє врахувати їх досвід, погляди та сприйняття. Це сприятиме обґрунтованому управлінню ризиками.

4.3.7 Постійне вдосконалення. Управління ризиками постійно вдосконалюється завдяки навчанню та досвіду, та дотримується циклу Плануй-Роби-Перевіряй-Дій (Plan-Do-Check-Act).

4.3.8 Найкраща доступна інформація. Вхідні дані для управління ризиками базуються на історичній та поточній інформації, а також на майбутніх очікуваннях. Управління ризиками

чітко враховує будь-які обмеження та невизначеності, пов'язані з такою інформацією та очікуваннями. Інформація повинна бути своєчасною, чіткою та доступною для відповідних зацікавлених сторін.

4.3.9 Забезпечення «трьох ліній захисту». В процесі здійснення діяльності по управлінню ризиками забезпечується залучення всіх структурних підрозділів Товариства до проведення оцінки, прийняття та контролю ризиків.

4.3.10 Обмеження рівня прийнятих ризиків. Визначення ризик-апетиту та його транслювання в систему обмежень дозволяє забезпечити прийнятний рівень ризиків, прозорий розподіл загального ліміту ризику за напрямками діяльності Товариства. Система управління ризиками забезпечує контроль за виконанням ризик-апетиту Товариства.

V. РОЛІ, ПОВНОВАЖЕННЯ ТА ВІДПОВІДАЛЬНІСТЬ УЧАСНИКІВ

5.1 Система управління ризиками Товариства реалізується через модель Трьох ліній захисту і передбачає участь у процесах ідентифікації, оцінки, аналізу, обробки і моніторингу ризиків усіх підрозділів Товариства (Рис. 1).

Рис. 1. Ілюстративне відображення моделі Трьох ліній захисту для АТ «Укрпошта»

5.2 Суб'єктами системи управління ризиками Товариства є:

- Наглядова рада Товариства;
- Комітет з питань аудиту при Наглядовій раді;

- Генеральний директор Товариства;
- CRO;
- Управління з менеджменту ризиків;
- ССО/ Підрозділ комплаєнсу;
- Служба із запобігання та виявлення корупції;
- Управління фінансового моніторингу;
- Департамент внутрішнього аудиту;
- Бізнес-підрозділи та підрозділи підтримки, що знаходяться на першій лінії захисту, - власники ризиків;
- Ризик-координатори.

5.3 Незалежність підрозділів з управління ризиками та комплаєнсу забезпечуються зі сторони Наглядової ради наступним чином:

- підпорядкування Управління з менеджменту ризиків CRO, CRO – Наглядовій раді, підпорядкування Підрозділу комплаєнсу ССО, ССО – Наглядовій раді;
- звітування CRO та ССО перед Наглядовою радою та Комітет з питань аудиту при Наглядовій ради;
- надання CRO/ Управлінню з менеджменту ризиків, ССО/Підрозділу комплаєнсу прямої можливості обговорення питань щодо ризиків безпосередньо з Наглядовою радою без необхідності (обов'язку) інформування про це Керівника Товариства;
- організаційного та функціонального відокремлення CRO/ Управлінню з менеджменту ризиків, ССО/Підрозділу комплаєнсу від підрозділів (керівників підрозділів) першої та третьої ліній захисту;
- забезпечення достатньої чисельності працівників цих підрозділів і рівня їх кваліфікації для досягнення цілей і завдань, поставлених перед ними;
- гарантування доступу CRO/ Управлінню з менеджменту ризиків, ССО/Підрозділу комплаєнсу до інформації, необхідної для їх ефективної роботи. Керівники та персонал Товариства мають сприяти в наданні такої інформації;
- недопущення працівників CRO/ Управлінню з менеджменту ризиків, ССО/Підрозділу комплаєнсу до здійснення функцій контролю за тими операціями, за які вони раніше безпосередньо несли відповідальність або стосовно яких раніше ухвалювали рішення на першій лінії захисту, з метою запобігання конфлікту інтересів.

5.4 Вищі органи управління Товариства встановлюють напрямок діяльності Товариства, визначають бачення, місію, цінності і схильність до ризиків Товариства. Вищі органи організовують систему управління ризиками та делегують повноваження і відповідальність за досягнення цілей системи управління ризиками. Відповідальність та функції вищих органів управління в системі управління ризиками розподіляється таким чином:

5.4.1 Наглядова Рада:

- несе відповідальність за створення комплексної, адекватної та ефективної системи управління ризиками, на які наражається Товариство в своїй діяльності;
- здійснює нагляд за функціонуванням належної, ефективної та безперервної системи управління ризиками та формуванням культури управління ризиками;

- затверджує загальний рівень схильності (апетиту) до ризиків Товариства та в розрізі основних типів ризиків;
- затверджує та здійснює нагляд за впровадженням, дотриманням і своєчасним оновленням (актуалізацією) документів з питань управління ризиками;
- здійснює розгляд та затвердження звітів з управління ризиками та питань з управління ризиками, що мають найвищий ступінь важливості для Товариства;
- на основі інформації, наданої CRO, CCO, оцінює ризики, пов'язані зі стратегічними ініціативами, ймовірність і потенційний вплив цих ризиків, а також приймає рішення щодо їх прийняття, мінімізації або уникнення;
- забезпечує виділення та доступ до ресурсів (фінансових (у межах фінансового плану), людських, інформаційних) для виконання покладених на Управління завдань з урахуванням можливостей Товариства;
- забезпечує просування відповідального ставлення з боку керівництва (tone from the top) стосовно важливості принципів управління ризиками та впровадження процесів з управління ризиками;
- здійснює розгляд результатів оцінки системи управління ризиками.

5.4.2 Комітет з питань аудиту при Наглядовій раді:

- здійснює розгляд та затвердження результатів незалежної оцінки системи управління ризиками та відповідних контролів, проведеної Департаментом внутрішнього аудиту;
- здійснює попередній розгляд внутрішніх документів з питань управління ризиками;
- здійснює розгляд звітів з управління ризиками, в тому числі звітів про періодичну оцінку ризиків та ризиків за настання події;
- здійснює розгляд річного плану здійснення оцінки ризиків;
- бере участь в розробці стратегії Товариства для забезпечення коректного врахування ризиків;
- надає консультації Наглядовій Ради з питань управління ризиками при визначенні Декларації схильності до ризику;
- забезпечує підтримку Наглядової Ради та, за необхідності, залучення зовнішніх експертів з питань управління ризиками.

5.4.3 Генеральний директор Товариства:

- забезпечує реалізацію затверджених Наглядовою радою політик та інших внутрішніх документів з питань управління ризиками;
- здійснює погодження внутрішніх документів з питань управління ризиками, надає рекомендації щодо їх покращення;
- здійснює інтеграцію управління ризиками в систему управління діяльністю Товариства через врахування оцінки ризиків при прийнятті стратегічних, інвестиційних, бюджетних та інших управлінських рішень;
- здійснює контроль ключових ризиків, показників схильності до ризику, встановлення лімітів;
- здійснює розгляд та прийняття рішення щодо ризиків та операційних інцидентів з істотним впливом на Товариство;

- забезпечує та сприяє впровадженню планів заходів, рекомендацій та інших нормативних документів, направлених на виконання заходів з обробки ризиків, впровадження системи управління ризиками та внутрішнього контролю Товариства;
- здійснює розгляд та погодження звітів щодо управління ризиками та результатів оцінки ризиків Товариства;
- здійснює погодження ключових цілей управління ризиками;
- забезпечує відповідність законодавчим, регуляторним та етичним вимогам;
- здійснює розгляд та погодження результатів оцінки системи управління ризиками;
- забезпечує виділення достатніх ресурсів для ефективного функціонування заходів, передбачених даною Політикою, та доступ працівників Управління та Підрозділу комплаєнсу та ризик-координаторів до інформації, необхідної для їх ефективної роботи;
- своїми управлінськими рішеннями та розпорядчими документами сприяє підвищенню рівня культури управління ризиками у Товаристві;
- забезпечує обізнаність працівників Товариства про ризики, пов'язані з їхніми посадовими обов'язками, а також проходження ними регулярних тренінгів та сертифікацій на знання ризиків, апетитів та внутрішніх політик.

5.5 Учасниками першої лінії є підрозділи, що безпосередньо пов’язані з постачанням товарів/наданням послуг клієнтам, а також підрозділи, що забезпечують ефективність діяльності Товариства. Відповідальність та функції першої лінії в системі управління ризиками розподіляється таким чином:

5.5.1 Структурні підрозділи Товариства – власники ризиків:

- несуть відповідальність за щоденне управління ризиками в межах сфери своєї діяльності та обов’язків, що передбачають ідентифікацію ризиків, їх оцінку, аналіз, розробку та впровадження заходів з мінімізації;
- забезпечують дотримання положень даної Політики та інших документів, що регламентують функціонування системи управління ризиками;
- подають інформацію про ризики в межах своєї компетенції CRO/Управлінню, ССО/Підрозділу комплаєнсу (в т.ч. Службі із запобігання та виявлення корупції), Управлінню фінансового моніторингу;
- оптимізують процеси Товариства з метою зменшення рівня ризиків та їх наслідків;
- беруть участь у розробці ключових індикаторів ризиків;
- беруть участь у формуванні планів дій щодо зменшення ризиків;
- повідомляють ризик-координаторів / працівників Управління з менеджменту ризиків про випадки збитків або інцидентів, які могли призвести до них.

5.5.2 Ризик-координатори. На першій лінії захисту, в рамках підрозділів та їх функціональних обов’язків, здійснюється призначення відповідальних за ідентифікацію ризиків та відображення в базі подій операційного ризику інцидентів, пов’язаних з операційною діяльністю – ризик-координаторів, які:

- взаємодіють з Управлінням з менеджменту ризиків щодо координації своєї роботи з управління ризиками;
- несуть відповідальність за регулярну роботу з ідентифікації можливих ризиків, їх аналіз, оцінку та обробку;

- звітують про реалізовані ризики (події) та регулярно здійснюють їх аналіз;
- координують діяльність підрозділу в сфері управління ризиками та впроваджують культуру управління ризиками в своїх підрозділах;
- ескалюють питання щодо прийняття управлінських рішень на рівень керівництва структурного підрозділу – власника ризиків з використанням знань системи управління ризиками;
- проходять навчання з питань управління ризиками та внутрішнього контролю.

Ризик-координатори призначаються рішенням Керівника Товариства з числа працівників структурних підрозділів рівня не нижче заступника керівника кожного окремого підрозділу. Відповідний функціонал відображається в посадових інструкціях зазначених працівників.
Права і обов'язки ризик-координаторів наведено в Додатку 1.

5.6 Друга лінія Системи управління ризиками забезпечує додаткову експертизу, підтримку, моніторинг і вирішення проблем, пов'язаних з управлінням ризиками. Відповідальність та функції другої лінії в системі управління ризиками розподіляються таким чином:

5.6.1 CRO:

- здійснює впровадження системи управління ризиками та нагляд за її функціонуванням;
- забезпечує координацію роботи з питань управління ризиками між структурними підрозділами Товариства та щодо побудови ефективної системи внутрішнього контролю;
- здійснює проведення ідентифікації, аналізу, оцінки, моніторингу, запобігання та зменшення ризиків;
- здійснює розгляд та прийняття рішень з питань управління ризиками;
- здійснює розробку та затвердження ключових індикаторів ризиків;
- здійснює розробку та затвердження планів дій щодо зменшення ризиків;
- здійснює розробку та затвердження системи внутрішнього контролю;
- здійснює звітування щодо ризиків Керівнику Товариства та Наглядовій Раді, в тому числі на квартальній та річній основі;
- розробляє та готує пропозиції щодо затвердження, впровадження, внесення змін або скасування розпорядчих, нормативних, методичних та інших внутрішніх документів Товариства з питань управління ризиками;
- здійснює розробку Декларації схильності до ризиків та подає її на розгляд і затвердження Керівнику Товариства та Наглядовій Раді;
- надає пропозиції Наглядовій раді, Керівнику Товариства щодо необхідних заходів з пом'якшення впливу ризиків, включаючи ініціювання встановлення лімітів ризиків та/або перегляду їх значень
- впроваджує практики управління ризиками в ділову культуру Товариства;
- контролює дотримання вимог даної Політики в Товаристві.

5.6.2 Управління з менеджменту ризиків:

- безпосередньо здійснює координацію процесу управління ризиками Товариства в співпраці з вищими органами управління, першою, другою та третьою лініями;
- розробку та впровадження системи управління ризиками;
- здійснює оцінку ризиків, їх аналіз та моніторинг дотримання лімітів;

- здійснює розробку, удосконалення, впровадження та супроводження внутрішніх нормативних документів Товариства з питань управління ризиками;
- здійснює моніторинг виконання вимог Політики та впровадження відповідних нормативних документів (процедур) з управління ризиками;
- бере участь у процесах оцінки, обробки та моніторингу ризиків в Товаристві;
- сприяє розробці ключових індикаторів ризиків;
- допомагає у формуванні планів дій щодо зменшення ризиків;бере участь у розробці системи внутрішнього контролю;
- сприяє спільному вирішенню проблем у робочих групах шляхом проведення інтерв'ю, опитувань та групових сесій для виявлення та оцінки ризиків у підрозділах Товариства;
- здійснює підготовку річного плану здійснення оцінки ризиків, звітів про оцінку ризиків;
- здійснює проведення самооцінки системи управління ризиками і винесення її результатів на затвердження CRO;
- сприяє підвищенню рівня культури управління ризиками та обізнаності щодо важливості її впровадження шляхом проведення інформаційних кампаній, підготовки методологічних матеріалів та навчань для працівників Товариства;
- надає роз’яснення та консультації працівникам Товариства щодо застосування внутрішніх документів з питань управління ризиками;
- здійснює координацію діяльності ризик-координаторів;
- співпрацює з підрозділом управління персоналом щодо організації курсів та тренінгів для першої лінії захисту, гарантуючи, що співробітники Товариства навчаються за найвищими стандартами управління ризиками, з контролем проходження навчання колегами.

5.6.3 ССО/ Підрозділ комплаєнсу (у взаємодії зі Службою із запобігання та виявлення корупції):

- бере участь в управлінні комплаєнс-ризиками, зокрема пов’язаними із дотриманням вимог антикорупційного законодавства та законодавства щодо врегулювання конфлікту інтересів;
- забезпечує організацію контролю за дотриманням норм законодавства, внутрішніх документів і відповідних стандартів професійних об'єднань, дія яких поширюється на Товариство;
- здійснює управління комплаєнс-ризиками, пов'язаними з конфліктом інтересів, які можуть виникати на усіх рівнях організаційної структури Товариства, прозорість реалізації процесів Товариства, в т.ч. контроль процедур обов'язкового декларування зовнішньої діяльності персоналу, вручення і отримання подарунків і запрошень, розгляд звернень відносно ситуацій спільної роботи родичів;
- здійснює ведення бази подій (інцидентів) комплаєнс-ризику в загальній базі подій операційного і комплаєнс-ризику;
- здійснює інформування Управління з менеджменту ризиків про події та операційні інциденти, виявлені під час виконання функцій підрозділу, які можуть вплинути на оцінку та обробку ризику;

- забезпечує функціонування системи управління ризиками шляхом здійснення своєчасного виявлення, виміру, моніторингу, контролю, звітності і надання рекомендацій відносно пом'якшення комплаєнс-ризику;
- вживає усі можливі заходи з метою відвертання ухвалення рішень, які піддають Товариство значному комплаєнс-ризику, і здійснює належне інформування Керівника Товариства, Наглядову раду;
- здійснює ознайомлення зі звітністю щодо управління ризиками та результатами оцінки системи управління ризиками.

5.6.4 Управління фінансового моніторингу:

- забезпечує належну організацію системи запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму;
- забезпечує організацію дотримання вимог законодавства України у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму;
- забезпечує здійснення моніторингу валютних операцій клієнтів на їх відповідність вимогам валютного законодавства України;
- управляє ризиками легалізації кримінальних доходів/фінансування тероризму у сфері фінансового моніторингу з метою зменшення їх до прийнятного рівня;
- забезпечує виявлення ризикових фінансових операцій, визначає наявність або відсутність ознак того що фінансові операції клієнтів направлені на використання послуг Товариства з метою легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, вчиняє відповідні дії щодо операцій, які містять ознаки ризиковості;
- виконує контролі другого рівня за виконанням вимог з легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму на першій лінії захисту;
- залучається до ідентифікації, оцінки та зниження ризиків легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму згідно ризик-орієнтованого підходу Товариства;
- приймає участь у розробленні внутрішніх документів, які регламентують питання управління ризиками згідно вимог з легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму.

5.7 До третьої лінії належить Департамент внутрішнього аудиту, який регулярно, відповідно до плану аудиту, оцінює ефективність функціонування системи управління ризиками та внутрішнього контролю структурних підрозділів Товариства, виявляє в ній слабкі місця та надає рекомендації щодо її покращення. Інформація про виявлені ризики, недоліки, порушення та рекомендації надається Наглядовій раді, Генеральному директору, CRO та CCO з метою внесення змін та покращення системи управління ризиками та внутрішнього контролю Товариства.

VI. ПРОЦЕСИ УПРАВЛІННЯ РИЗИКАМИ

6.1 Управління ризиками в Товаристві є постійним, динамічним і безперервним процесом і складається з наступних етапів:

- ідентифікація ризиків;
- оцінка ризиків;
- обробка ризиків;
- моніторинг та контроль ризиків.

6.2 **Ідентифікація ризиків** (Risk Identification) – це процес визначення елементів ризику, складання їх переліку та опис кожного з елементів ризику. Ціллю процесу ідентифікації ризиків є побудова «Довгого списку» ризиків (Risk Universe), що включає ризики, які можуть вплинути на досягнення цілей Товариства і ключових показників ефективності.

6.2.1 Товариство прагне до комплексної ідентифікації ризиків, виходячи з принципу максимально широкого охоплення областей виникнення ризиків по кожній цілі Товариства та показнику розвитку.

6.2.2 Для виявлення ризиків використовуються різні комбінації методик та інструментів, таких як виявлення ризиків на основі поставлених цілей і завдань, галузевих і міжнародних порівнянь, семінарів і обговорень, проведення інтерв'ю, бази даних подій, що відбулися в Товаристві і на ринку.

6.2.3 Зокрема методи ідентифікації ризику можуть включати:

- методи, що базуються на минулих фактах (наприклад, аналіз бази подій ризиків);
- емпіричні методи, включаючи тестування та моделювання для визначення того, що може статися за конкретних обставин;
- методи, в яких предмет, що розглядається, поділяється на менші елементи, кожен з яких, у свою чергу, розглядається за допомогою методів, які ставлять питання "що якщо";
- методи заохочення образного мислення про можливості майбутнього, такі як аналіз сценаріїв;
- метод «мозкового штурму».

6.2.4 Виявлені події систематизуються в формі Risk Universe. Відповідальність за побудову Risk Universe несе Управління з менеджменту ризиків у співпраці з ключовими учасниками першої та другої лінії. Risk Universe доповнюється структурними підрозділами Товариства на постійній основі при виявленні нових ризиків.

6.2.5 Систематизація виявлених ризиків у вигляді Risk Universe забезпечує:

- послідовність класифікації і оцінки ризиків, яка сприяє покращенню порівняння профілю ризиків (за бізнес-процесами, структурними підрозділами, проєктами тощо);
- платформу для побудови покращених методик і технологій оцінки ризиків;
- узгоджене управління та контроль ризиків Товариства.

6.3 **Оцінка ризиків** (Risk Assessment) – процес, що поєднує аналіз та порівняльну оцінку ризику та передбачає детальний розгляд невизначеностей, джерел ризику, наслідків, ймовірності, подій, сценаріїв, засобів контролю та їхньої ефективності. Подія може мати декілька причин і наслідків і впливати на декілька цілей. Ризик може бути оцінений для всього Товариства, його підрозділів, окремих проєктів або окремої події.

6.3.1 Аналіз ризиків є основою для оцінки ризиків – визначення прийнятності рівня ризику, прийняття рішень про необхідність управляти визначеними ризиками та в який спосіб, а також про найбільш прийнятну стратегію і методи управління ризиками.

6.3.2 Аналіз ризику передбачає аналіз ймовірності реалізації ризику та впливу ідентифікованих небезпечних подій з урахуванням наявності та ефективності способів управління ризиками, що вже використовуються. Дані про ймовірність подій та їх наслідки використовуються для визначення рівня ризику.

6.3.3 Аналіз ризиків здійснюється з метою виділення найбільш суттєвих ризиків, які можуть негативно впливати на діяльність Товариства, досягнення його стратегічних цілей і завдань. Визначені суттєві ризики виносяться на розгляд Керівнику Товариства, який приймає рішення щодо їх управління та мінімізації, з подальшим затвердженням Наглядовою радою.

6.3.4 В межах проведення аналізу ризиків в Товаристві можуть використовуватися якісна та кількісна оцінка або їх поєднання.

6.3.4.1 Якісна оцінка передбачає встановлення орієнтиру в якісному вираженні. Підставою для віднесення до тієї чи іншої групи виступає наперед визначена система параметрів, а основним методом оцінки – експертний метод. Якісна оцінка проводиться в разі неможливості використання математичного підходу.

6.3.4.2 Кількісна оцінка передбачає присвоєння кількісного параметра якісному. Проміжним етапом розрахунку можуть виступати показники та коефіцієнти, що мають різні одиниці виміру, проте кінцевим результатом кількісної оцінки є розмір збитків в грошовому вираженні. Кількісна оцінка дозволяє порівнювати усі види ризиків та оцінювати їх вплив на діяльність Товариства.

6.3.5 Процес оцінки ризиків передбачає періодичну самооцінку ризиків, здійснення оцінки ризиків за настання події, збір даних про операційні інциденти, консолідацію даних щодо оцінки ризиків від структурних підрозділів, які виконують функцію управління ризиками.

6.3.6 Оцінка ризиків здійснюється Управлінням з менеджменту ризиків у співпраці з ключовими учасниками першої та другої лінії щорічно, щоквартально або у випадку зміни внутрішніх та зовнішніх факторів, що впливають на бізнес-процеси Товариства.

6.3.7 Для оцінки ризиків Управління з менеджменту ризиків може запитувати інформацію, яка стосується ризиків та подій, що впливають на ймовірність і рівень впливу ризиків на досягнення стратегічних цілей, у структурних підрозділів Товариства.

6.3.8 Збір даних про операційні інциденти здійснюється у випадку виникнення операційних інцидентів та складається з:

- виявлення операційного інциденту;
- інформування ризик-координатора про виявлення інциденту;
- повідомлення про інцидент працівників Управління з менеджменту ризиків;
- внесення повідомлення про операційний інцидент до бази подій операційного ризику (інцидентів) Управлінням з менеджменту ризиків;
- інформування уповноважених органів та підрозділів про настання інциденту згідно відповідного регламенту взаємодії структурних підрозділів Товариства в процесі управління ризиками.

6.3.9 Для кожного ризику визначається дві оцінки рівня ризику – притаманний (найгірший сценарій реалізації) та залишковий ризик (оцінка сценарію після впровадження заходів по обробці ризику).

6.3.10 Визначені на етапі оцінки суттєві ризики відображаються в Декларації схильності до ризиків.

6.4 **Карта ризиків** (Risk Heat Map). Результати оцінки ризиків графічно відображаються з використанням карти ризиків – графічного і текстового опису ризиків, релевантних для Товариства, розміщених в прямокутній таблиці, по одній осі якої вказана ймовірність реалізації ризику, а по іншій – рівень впливу ризику на діяльність Товариства. Карта ризиків дозволяє оцінити відносну значимість кожного ризику для Товариства за 5-бальною шкалою, а також виділити ризики, які є ключовими і потребують розробки механізмів управління ними.

6.4.1 Розгляд ймовірності виникнення ризику визначається як ймовірність одиничної події із значним впливом або декількох подій, пов'язаних з одним ризиком, що агреговано матимуть значний вплив на діяльність Товариства.

6.4.2 При оцінці ймовірності ризику Товариство дотримується наступних принципів:

6.4.2.1 За наявності даних щодо реалізації ризику у базі операційних інцидентів для обґрунтування ймовірності використовуються історичні дані про операційні інциденти.

6.4.2.2 За наявності історичних даних щодо реалізації ризику в інших джерелах (зовнішні бази даних операційних інцидентів, дані інших організацій, підприємств, країн, нормативні значення, дані з фінансової чи управлінської звітності, інша внутрішня) для обґрунтування ймовірності використовуються дані з інших джерел історичних даних.

6.4.2.3 За наявності історичних даних щодо зміни фактору, що призводить до реалізації ризику, використовуються історичні дані щодо зміни фактору ризику.

6.4.2.4 За відсутності історичних даних щодо реалізації ризику використовуються оцінки експертів (експертні судження).

6.4.3 Оцінка ймовірності реалізації ризику наведена в таблиці:

Бал	Оцінка ймовірності реалізації ризику	Ймовірність реалізації ризику	Частота виходячи з історичних даних
5	Критичний	80%< *** <=100%	Частіше, ніж один раз на рік
4	Високий	60%< *** <=80%	Раз в 1 – 2 роки
3	Середній	40%< *** <=60%	Раз в 2 – 3 роки
2	Низький	20%< *** <=40%	Раз в 3 – 5 роки
1	Незначний	0%<= *** <=20%	Раз в 5 років або рідше

6.4.4 При оцінці впливу ризику Товариство дотримується наступних принципів:

6.4.4.1 Рівень значущості впливу ризику повинен визначатися впливом реалізації ризику на досягнення стратегічних цілей у перспективі 1 рік.

6.4.4.2 Аналіз впливу повинен включати кількісні та якісні оцінки значущості впливу ризику із застосуванням планових фінансових показників із фінансового плану Товариства на поточний рік в якості спільного знаменника.

6.4.4.3 Ризики повинні бути оцінені з урахуванням найвищого потенційного впливу.

6.4.4.4 Під час оцінки впливу ризику слід враховувати можливі кумулятивні ефекти, що пов’язані з реалізацією ризиків. У разі якщо збитки від реалізації ризику можуть

накопичуватися протягом кількох років, необхідно оцінювати сумарний вплив ризику протягом відповідного часового горизонту.

6.4.4.5 Оцінку впливу слід проводити в контексті стратегічних цілей та операційних планів діяльності..

6.4.5 Ранжування оцінки рівня впливу від реалізації ризику здійснюється за тією ж шкалою, що й оцінка ймовірності ризику, від "критичного" до "незначного", що забезпечує послідовність в оцінці ризиків:

Бал	Оцінка рівня впливу ризику
5	Критичний
4	Високий
3	Середній
2	Низький
1	Незначний

6.4.6 Оцінка рівня впливу ризику здійснюється з урахуванням наступних аспектів:

- фінансовий аспект – відображає вплив реалізації ризику на фінансові результати;
- вплив на операційну діяльність – аналізуються потенційні порушення у виробничому процесі, які завдають шкоди функціонуванню Товариства, здійсненню основних процесів і поставки продукції;
- нормативно-правовий аспект – аналізується потенційна відповідальність відповідно до чинного законодавства в разі матеріалізації ризику;
- стратегічний аспект – аналізуються наслідки реалізації ризиків для досягнення стратегічних цілей;
- вплив на здоров'я та безпеку – визначається вплив події на здоров'я і безпеку працівників;
- аспект репутації та соціальної відповідальності – аналізується сприйняття події засобами масової інформації та масштабу поширення негативної інформації (на національному / міжнародному рівні).
- екологічний аспект – аналізується вплив на екологію, біорізноманіття та викиди парникових газів.

6.4.7 На основі оцінок ймовірності реалізації ризику та рівня впливу ризику визначається рівень ризику як добуток значень отриманих оцінок:

Рівень ризику						
Вплив	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ймовірність				

6.4.8 Опис рівнів ризику

Бал	Рівень ризику	Опис
16-25	Критичний	Реалізація ризиків може призвести до критичних наслідків, включаючи припинення діяльності, значні фінансові втрати або серйозну шкоду репутації.
12-15	Високий	Суттєвий негативний вплив на діяльність Товариства; значні відхилення від планів, значні фінансові втрати або серйозні порушення у процесах. Вимагають негайних заходів для їх пом'якшення.
8-10	Середній	Відчутний помірний вплив на окремі аспекти діяльності Товариства; можливі затримки, підвищення витрат або зниження якості. Потребують уваги та планування для мінімізації їх наслідків.
4-6	Низький	Невеликий вплив на процеси або результати; можливі незначні затримки чи додаткові витрати, але їх вплив легко контролюється та не потребує значних ресурсів для вирішення.
1-3	Незначний	Мінімальний або відсутній вплив на діяльність Товариства; незначні відхилення від планових показників, відсутність суттєвих фінансових втрат або порушень у процесах.

6.4.9 Рівень ризику розраховується в національній валюті шляхом оцінки потенційного впливу ризику / можливості на EBITDA, операційний прибуток, потоку грошових коштів (free cash flow – FCF). У випадку неможливості грошової оцінки застосовується бальна шкала оцінки на основі експертної думки оцінювачів.

6.5 **Обробка ризиків** (Risk Treatment) – процес вибору, розробки і реалізації заходів, що дозволяють зменшити негативний ефект і ймовірність збитків, пов’язаних з ризиками діяльності Товариства, та здійснюються з метою недопущення порушення визначених рівнів схильності до ризику Товариства.

6.5.1 Варіанти обробки ризиків не обов'язково є взаємовиключними або доречними за будь-яких обставин. Варіанти реагування на ризик можуть включати один або декілька з наступних способів:

6.5.1.1 Прийняття ризику. Товариство приймає ризик без застосування заходів впливу, наприклад, коли відсутні можливості впливати на ризик, чи вартість заходів впливу суттєво перевищує потенційні збитки від реалізації ризику. Також ризик приймається у випадку його не суттєвості, в межах ризик-апетиту.

6.5.1.2 Уникнення ризику. Товариство не готове приймати такий ризик, навіть застосовуючи заходи з мінімізації, тобто уникає будь-яких дій чи рішень, що можуть бути пов’язані з таким ризиком. Захід доцільно (за можливості), але не виключно, застосовувати до ризиків, які мають критичний рівень.

6.5.1.3 Передача ризику (розділення). Товариство передає ризик (частину ризику) зовнішнім контрагентам або передає функції/процеси зовнішнім постачальникам (аутсорсинг). Такий

захід можливо, але не виключно, доцільно застосовувати до ризиків, якими Товариство не має змоги ефективно управляти або впливати на джерело такого ризику.

6.5.1.4 Мінімізація ризику. Товариство зменшує потенційний вплив або ймовірність реалізації ризику через здійснення певних заходів з мінімізації впливу чи ймовірності, або одночасно заходи направляються на зменшення й впливу й ймовірності. Зокрема шляхом покращення (впровадження додаткових) коригуючих та/або контролюючих процедур.

6.5.1.5 Створення запасного плану. Товариство розробляє план дій, на випадок настання певних подій ризику, надзвичайних обставин та ситуацій. План містить алгоритм дій, ролі персоналу, ресурси, які необхідно виконати/залучити у випадку реалізації подій ризику. Зазвичай така стратегія використовується для операційних ризиків, що пов'язані з перебоями у діяльності.

6.5.1.6 Посилення внутрішнього контролю. Товариство забезпечує впровадження (посилення існуючих) превентивних контрольних процедур, в разі якщо вони є ефективними, та/або впровадження нових/додаткових пост-фактум контрольних процедур.

6.5.1.7 Використання можливостей. Товариство активно використовує можливості, які виникають внаслідок подій ризику, з метою отримання додаткової вигоди.

6.5.2 Вибір найбільш прийнятного варіанту (варіантів) обробки ризиків передбачає збалансування потенційних вигод, отриманих у зв'язку з досягненням цілей, з витратами, зусиллями або недоліками, пов'язаними з їх реалізацією.

6.5.3 Прийняті рішення з обробки ризиків розглядаються і затверджуються Директором з управління ризиками, Керівником Товариства в міру необхідності прийняття таких рішень, і є обов'язковими для виконання всіма структурними підрозділами Товариства.

6.5.4 Відповідальність за реалізацію затверджених заходів із обробки ризику несуть власники ризику.

6.6 **Моніторинг та контроль ризиків** (Risk Monitoring and Control). Моніторинг та контроль ризиків є ключовою частиною процесу управління ризиками.

6.6.1 Моніторинг ризику передбачає розрахунок його поточної величини, вивчення її динаміки в часі, аналіз причин зміни та розробка превентивних заходів для її нормалізації в разі наявності негативних тенденцій. Моніторинг полягає в побудові керованого процесу впливу на розмір прийнятого ризику та його динаміку з боку Товариства.

6.6.2 Метою контролю є відповідність прийнятого рівня ризику встановленому рівню ризик-апетиту.

6.6.3 Основними складовими процесу моніторингу ризиків є:

6.6.3.1 Встановлення системи моніторингу, що включає розроблення системи або процедур для моніторингу ризиків: визначення KRI, інструментів та процесів, які будуть використовуватися для виявлення та відстеження ризиків.

6.6.3.2 Встановлення ключових індикаторів ризику та граничних значень з метою відслідковування зміни в рівні ризиків.

6.6.3.3 Встановлення періодичності регулярних оглядів в залежності від динаміки та важливості ризиків.

6.6.3.4 Аналіз даних – зібрані від Власників ризиків дані аналізуються Управлінням з менеджменту ризиків з метою оцінки поточного стану портфелю ризиків, його динаміки.

6.6.3.5 Забезпечення регулярної звітності про стан портфелю ризиків, включаючи інформацію про ті ризики, які перевищують встановлені граничні значення, та ефективність існуючих заходів контролю.
6.6.3.6 Забезпечення комунікації з зацікавленими сторонами з метою повного та своєчасного інформування про стан ризиків і вжиті заходи.
6.6.3.7 Перегляд заходів контролю у випадку, якщо наявні заходи обробки ризиків не дають своїх результатів, або KRI мають негативну динаміку.
6.6.4 Контроль за ризиком включає:
- контроль за агрегованими ризиками Товариства;
- контроль за окремими ризиками;
- контроль за дотриманням встановлених лімітів;
- систему розподілення повноважень в управлінні ризиками та процесі контролю;
- внутрішній контроль;
- внутрішній та зовнішній аудит.

VII. КЛАСИФІКАЦІЯ РИЗИКІВ

7.1 В Товаристві визначено наступні групи суттєвих ризиків:
- стратегічні ризики;
- операційні ризики;
- комплаєнс-ризики;
- фінансові-ризики.

7.2 Стратегічний ризик – ризик виникнення збитків внаслідок змін або помилок при визначенні і реалізації стратегії діяльності і розвитку Товариства, а також зовнішніх системних факторів, таких як:
- зміни політичного середовища;
- регіональні ринкові тенденції;
- ринкові спади;
- інші зовнішні системні фактори.

7.3 Операційний ризик – ризик виникнення збитків або додаткових втрат, чи недоотримання запланованих доходів внаслідок:
- недоліків або помилок у внутрішніх процесах;
- навмисних або ненавмисних дій працівників або третіх осіб;
- збоїв в роботі інформаційних систем;

7.4 внаслідок впливу зовнішніх деструктивних факторів, що впливають на повсякденну діяльність компанії. Включає в себе такі складові, як кіберризики та ризики інформаційної безпеки.Комплаєнс-ризик – ризик невідповідності діяльності Товариства:
- вимогам законодавства;
- регуляторним нормам;
- ринковим стандартам;
- політиці корпоративної етики;
- політиці щодо конфлікту інтересів;

- антикорупційного законодавства;
- санкційних обмежень;
- зобов'язань щодо фінансового моніторингу.

Управління комплаєнс-ризиками здійснюється ССО/ Підрозділом комплаєнсу, Службою із запобігання та виявлення корупції, Управлінням фінансового моніторингу, та регулюється окремими внутрішніми документами.

7.5 Фінансовий ризик – це ризик виникнення події, яка може прямо чи опосередковано призвести до фінансових втрат Товариства. До фінансових ризиків зокрема належать:

- ризик ліквідності та платоспроможності;
- інвестиційний ризик;
- валютний ризик та
- ризики контрагентів.

7.6 Вище зазначені ризики не є взаємовиключними, і, зазвичай, подія або низка подій призводитимуть до виникнення декількох ризиків.

7.7 Більш деталізована класифікація вищезазначених груп суттєвих ризиків наводиться в Реєстрі ризиків та окремих внутрішніх документах, що регламентують управління окремими ризиками.

7.8 Управління з менеджменту ризиків розробляє та підтримує в актуальному стані Реєстр ризиків, який містить невичерпний перелік всіх ризиків, з якими стикається Товариство в своїй діяльності.

7.9 Реєстр ризиків Товариства використовується як основа для ідентифікації ризиків та оновлюється у разі потреби, але не рідше ніж раз на рік.

7.10 Ідентифікація ризиків для нових послуг, продуктів і процесів здійснюється в обов'язковому порядку до їх впровадження.

7.11 Управління з менеджменту ризиків підтримує в актуальному стані Базу подій ризиків, яка наповнюється на основі щоквартальних звітів від підрозділів (ризик-координаторів) про події ризиків.

7.12 Ведення та наповнення Бази подій ризиків регламентується окремим внутрішнім нормативним документом.

VIII. ПІДХІД ДО ВИЗНАЧЕННЯ СХИЛЬНОСТІ ДО РИЗИКУ

8.1 Цілі і завдання Товариства повинні бути узгоджені з затвердженою схильністю до ризику. Схильність до ризику відображає прийнятний рівень невизначеності в досягненні стратегічних цілей.

8.2 Основою для визначення схильності до ризику є ключові показники діяльності (EBITDA, операційний прибуток, потоку грошових коштів тощо).

8.3 Товариство переглядає рівень схильності до ризику в разі зміни стратегічних цілей, а також рівня ризику, який Товариство готове прийняти для досягнення таких цілей.

IX. ОРГАНІЗАЦІЯ СИСТЕМИ ЗВІТНОСТІ ТА ЕСКАЛАЦІЇ

9.1 Ефективна взаємодія між суб'єктами системи управління ризиками реалізовується шляхом організації регулярної та прозорої системи звітності.

9.2 Звітність про ризики має:

- надавати чітку та однозначну інформацію та бути достатньо вичерпною для прийняття своєчасних та адекватних управлінських рішень;
- бути точною, вивіреною та достовірно відображати рівень прийнятого Товариством ризику;
- охоплювати всі суттєві види ризиків Товариства, містити інформацію про концентрацію ризиків, дотримання встановленого розміру ризик-апетиту.

9.3 Наглядова рада та Комітет з питань аудиту не менш ніж раз на квартал отримують звітність від Управління з менеджменту ризиків щодо загального стану системи управління ризиками з описом найбільш значних ризиків та планів їх мінімізації.

9.4 Керівник Товариства не менш ніж раз у квартал отримує інформацію від Управління з менеджменту ризиків щодо результатів ідентифікації та оброблення ризиків.

9.5 Управління з менеджменту ризиків на регулярній основі (не рідше ніж раз на квартал) отримує інформацію від всіх підрозділів Товариства щодо потенційних та реалізованих ризиків.

9.6 Звітність з управління ризиками складається з:

- консолідованого річного звіту про оцінку ризиків Товариства;
- квартального звіту щодо управління ризиками.

9.7 Консолідований річний звіт про оцінку ризиків Товариства містить:

- карту ризиків, де виділені суттєві ризики Товариства;
- таблиці про проведені оцінки ризиків у розрізі видів діяльності;
- виявлені події та інциденти за рік;
- виконання планів з обробки ризиків;
- інформацію про розвиток системи управління ризиками.

9.8 Квартальний звіт щодо управління ризиками містить:

- Карту ризиків із виділеними суттєвими ризиками;
- ключові індикатори ризиків;
- виявлені ризики та інциденти за квартал;
- виконання планів обробки ризиків;
- динаміку ключових індикаторів ризиків за період;
- поточні завдання Управління з менеджменту ризиків.

9.9 Консолідовані звіти щодо оцінки ризиків формуються Управлінням з менеджменту ризиків на основі інформації, отриманої від структурних підрозділів.

9.10 Звіти виносяться на розгляд Керівника Товариства, Комітету з питань аудиту та затвердження Наглядової ради.

9.11 Система звітності з управління ризиками має відповідати наступним принципам:

Раціональності: при формуванні звітності Товариство фокусується на максимізації економічності системи звітності, забезпечуючи наявність всієї необхідної інформації, яка відповідає вимогам регулятора і дозволяє приймати управлінські рішення.

Зрозумілості: звітність повинна бути зрозуміла цільовій аудиторії з точки зору рівня деталізації і обсягу, який містить інформацію.
Прозорості: звітність щодо ризиків повинна мати коректні і точні дані, які можна порівняти.
Повноти: звітність повинна містити інформацію з усіх суттєвих ризиків. Звіти повинні містити порівняння величин прийнятого ризику з доступними фінансовими ресурсами на покриття прийнятих ризиків.
Порівнянності: формат звітності повинен дозволяти агрегувати інформацію з різних видів суттєвих ризиків підрозділами бізнесу для забезпечення повноти подачі і структури ризику.
Єдності термінології: організація системи звітності повинна проводитися таким чином, щоб у разі кризових умов можна було переключитися на оперативне надання даних про фактичні і цільові рівні і структури ризиків для своєчасного прийняття управлінських заходів.
Цілісності: звітність повинна формуватися із заданою періодичністю і зміст звітів повинен подаватися в структурованому вигляді.

X. КУЛЬТУРА РИЗИКІВ

10.1 Культура управління ризиками є складовою загальної корпоративної культури Товариства та сприяє формуванню достатнього рівня обізнаності всіх працівників щодо важливості та правил функціонування системи управління ризиками. Розвиток культури управління ризиками здійснюється шляхом проведення навчань, тематичних зустрічей фокус-груп з метою популяризації процесу управління ризиками та максимальної залученості працівників до цього процесу.
10.2 Культура управління ризиками в Товаристві сприяє підвищенню обізнаності працівників:
- важливості управління ризиками;
- функціонування системи управління ризиками.

10.3 Розвиток культури ризику досягається через:
- навчальні програми;
- обговорень у фокус-групах;
- ініціативи із залученням працівників.

10.4 Мета впровадження культури ризиків полягає в тому, щоб керівництво і працівники Товариства приймали рішення та здійснювали операційну діяльність, обираючи оптимальне співвідношення ризиків і можливостей. Зокрема, це означає:
- відмову від рішень, що призводять до невиправдано високих ризиків;
- вжиття заходів для зменшення впливу ризиків;
- усвідомлення важливості управління ризиками на всіх рівнях.

XI. ОЦІНКА СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ

11.1 Оцінка системи управління ризиками здійснюється на основі міжнародних стандартів (ISO 31000, COSO) та включає аналіз рівня зрілості, самооцінку підрозділів, моніторинг ключових показників ризиків (KRI), аналіз ризикових подій та сценарне моделювання.
11.2 Оцінка системи управління ризиками здійснюється на регулярній основі з метою визначення її зрілості, ефективності та відповідності стратегічним цілям Товариства. Це

дозволяє керівникам структурних підрозділів та Управлінню з менеджменту ризиків отримати об'єктивну картину поточного стану та інструменти для вдосконалення ризик-менеджменту.

11.3 Завдання оцінки системи управління ризиками:

- визначення рівня зрілості системи управління ризиками відповідно до міжнародних стандартів ISO 31000, COSO;
- оцінка ефективності процесів управління ризиками;
- виявлення зон для покращення та усунення слабких місць;
- розробка та імплементація заходів для підвищення ефективності ризик-менеджменту.

11.4 Оцінка базується на ключових показниках ефективності, згрупованих за такими напрямами:

- інтеграція ризик-менеджменту в операційну діяльність, управлінські рішення;
- включення ризиків у процеси стратегічного планування та бюджетування;
- діяльність відповідального підрозділу щодо розвитку культури ризик-менеджменту в Товаристві;
- оптимізація підходів до управління ризиками та їх адаптація до змін середовища;
- розподіл відповідальності за управління ризиками між керівниками та співробітниками;
- рівень компетенцій персоналу у сфері ризик-менеджменту;
- управління ключовими ризиками.

11.5 Оцінка системи управління ризиками використовує наступні методи:

- аналіз рівня зрілості ризик-менеджменту - оцінка ефектності системи управління ризиками та її інтегрованості в діяльність організації, наскільки вона відповідає міжнародним стандартам та які механізми контролю і вдосконалення в ній застосовуються;
- анкетування структурних підрозділів;
- моніторинг ключових ризикових індикаторів (KRI);
- використання матриці ризиків та сценарного аналізу тощо.

11.6 Департаменту внутрішнього аудиту оцінює та надає висновки та рекомендації щодо ефективності системи управління ризиками.

XII. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

12.1 Всі співробітники Товариства несуть відповідальність за невиконання вимог цієї Політики. Приховування, несвоєчасне розкриття інформації, надання недостовірної інформації про конфлікт інтересів або порушення інших вимог цієї Політики є підставою для застосування 'дисциплінарних заходів впливу, в тому числі розривання трудових відносин, притягнення до адміністративної та кримінальної відповідальності відповідно до законодавства України.

ДОДАТОК 1. Функції, права та вимоги до ризик-координаторів Товариства

1. До функцій ризик-координаторів належать:

1.1 Участь у підтвердженні оцінок ймовірності та впливу ризиків, надання підтримки підрозділам у застосуванні методології.

1.2 Участь у розробці планів зменшення ризиків.

1.3 Своєчасне винесення на розгляд Управління з менеджменту ризиків звітів про оцінку ризиків та пропозицій щодо способів обробки ризиків та інцидентів ризику.

1.4 Запровадження культури управління ризиками у Товаристві.

1.5 Інформування Управління з менеджменту ризиків про результати оцінки ризиків структурних підрозділів Товариства.

2. Ризик-координатори з метою реалізації основних функцій в установленому порядку мають право:

2.1 Взаємодіяти зі працівниками Товариства з питань управління ризиками.

2.2 Мати доступ до всієї необхідної документації та іншої інформації щодо джерел виникнення ризику, у випадку вирішення питань, що входять до сфери їх компетенції та в межах своїх повноважень.

2.3 Надавати запити та отримувати від працівників відповідних підрозділів інформацію щодо ідентифікованих ризиків та результатів їх оцінки, операційних інцидентів та результатів службових розслідувань.

2.4 Вносити пропозиції Директору з управління ризиками та Керівнику Товариства щодо заходів оцінки та обробки ризиків та інших питань, які належать до компетенції ризик-координатора.

2.5 Надавати структурним підрозділам Товариства, задіяним в процесах управління ризиками, методичні рекомендації, експертні поради з питань ідентифікації, аналізу, оцінки, обробки та моніторингу ризиків.

2.6 Брати участь у нарадах, семінарах, конференціях, що стосуються питань управління ризиками.

2.7 Планувати та узгоджувати ресурси для виконання своїх функцій.

2.8 Ініціювати розгляд питань, що стосуються управління ризиками, керівником відповідного підрозділу та Керівником Товариства.

3. Ризик-координатори повинні відповідати таким кваліфікаційним вимогам:

3.1 Знання процесів, притаманних компаніям поштового зв’язку.

3.2 Знання ринку поштового зв’язку.

3.3 Знання нормативно-правових актів, що регулюють галузь поштового зв’язку.

3.4 Здатність до аналізу економічних процесів.

3.5 Вміння організовувати та проводити структуровані зустрічі, працювати самостійно та в команді, вміти організовувати роботу.

3.6 Аналітичне мислення, вміння формулювати висновки.

4. **Ефективність роботи ризик-координаторів оцінюється Директором з управління ризиками враховуючи такі показники (КПЕ)**:

4.1 Своєчасне інформування Управління з менеджменту ризиків про ризики та інциденти, виявлені в межах діяльності підрозділу.

4.2 Своєчасне виконання річного плану оцінки ризиків, виявлених в межах діяльності підрозділу.

4.3 Своєчасне оновлення реєстру ризиків, що притаманні діяльності підрозділу.

4.4 Своєчасне оновлення бази операційних ризиків (інцидентів), виявлених в межах діяльності підрозділу.

4.5 Розрахунок ключових індикаторів ризиків, визначених в межах діяльності підрозділу, у встановлені внутрішніми процедурами строки.