ЗАТВЕРДЖЕНО
Рішення Наглядової ради
АТ «Оператор ринку»
від «30» серпня 2023 року
Протокол № 12

СТРАТЕГІЯ ТА ПОЛІТИКА УПРАВЛІННЯ РИЗИКАМИ АТ «ОПЕРАТОР РИНКУ»

Київ 2023

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Стратегія та Політика управління ризиками АТ «Оператор ринку» (далі – Стратегія) регламентує процес управління ризиками, визначає перелік суттєвих видів ризиків, що притаманні діяльності АТ «Оператор ринку» (далі – Товариство), принципи та порядок організації управління ризиками в Товаристві, порядок, строки та періодичність надання звітів Наглядовій раді Товариства, Комітету наглядової ради АТ «Оператор ринку» з питань аудиту, управління ризиками та комплаєнсу.

1.2. Стратегія розроблена відповідно до:

Закону України «Про ринок електричної енергії» (із змінами та доповненнями);

Постанови НКРЕКП від 27 грудня 2017 року N 1466 «Про затвердження Ліцензійних умов провадження господарської діяльності зі здійснення функцій оператора ринку»;

Статуту Товариства

Кодексу корпоративної етики АТ «Оператор ринку»;

Положення про організацію системи внутрішнього контролю (комплаєнсу) затвердженого Наглядовою радою 24 квітня 2023 року.;

Положення про організацію системи управління ризиками затвердженого Наглядовою радою 21липня 2023 року;

Порядку запобігання виникнення та врегулювання конфлікту інтересів затвердженого Наглядовою радою 24 квітня 2023 року;

1.3. Метою Стратегії є забезпечення:

захисту інтересів Товариства від можливих загроз та небезпек, які можуть виникнути в процесі діяльності

стабільності фінансового стану та операційної діяльності Товариства, зменшення коливань та ризиків, що можуть впливати на роботу;

аналізу і визначення важливості ризиків з точки зору ймовірності виникнення та впливу на діяльність Товариства;

визначення планів дій, які дозволять зменшити або контролювати ризики;

впровадження ефективної системи управління ризиками, що дозволяє ідентифікувати, відслідковувати та контролювати ризики на всіх рівнях діяльності Товариства;

постійного спостереження за ситуацією та оцінка ефективності заходів з управління ризиками.

1.4. Реалізація мети Стратегії здійснюється шляхом виконання наступних завдань:

проведення комплексного аналізу потенційних ризиків, що можуть впливати на діяльність Товариства. Це включає ідентифікацію зовнішніх та внутрішніх ризиків, оцінку їхнього впливу та ймовірності виникнення;

розробка, на основі аналізу ризиків, конкретних стратегій та планів дій для зменшення впливу ризиків;

впровадження контрольних процедур та стандартів, з метою забезпечення дотримання стратегій управління ризиками та своєчасну реакцію на зміни у ризиковому середовищі;

підготовка персоналу до реагування на ризики;

постійний моніторинг і оновлення стратегій управління ризиками з метою адаптації до нових загроз і забезпечити актуальність процесів управління ризиками;

розвиток культури управління ризиками в Товариства на всіх рівнях управління, визначених цією Стратегією.

1.5. Ці підходи можуть варіюватися залежно від специфіки діяльності та цілей Товариства.

1.6. У разі невідповідності окремих положень Стратегії нормам чинного законодавства України до моменту внесення змін до цієї Стратегії застосовуються норми чинного законодавства України.

2. ТЕРМІНИ, СКОРОЧЕННЯ ТА ЇХ ВИЗНАЧЕННЯ.

2.1. Терміни та скорочення використовуються в цій Стратегії у такому значенні:

звітування – підготовка та надання управлінської звітності про стан та результати діяльності Товариства, яка використовується керівником Товариства для планування, моніторингу, контролю та прийняття відповідних управлінських і економічних рішень, з метою забезпечення оперативного та ефективного управління ресурсами Товариства, оцінки ризиків, на які наражається Товариство, та їх мінімізації;

ідентифікація ризиків – пошук, визначення та опис ризиків, які можуть допомагати або перешкодити Товариству у досягненні її цілей. Ідентифікація ризиків проводиться за категоріями та видами;

культура управління ризиками – дотримання визначених Товариством принципів, правил, норм, спрямованих на поінформованість усіх працівників Товариства щодо прийняття ризиків та управління ризиками;

ліквідність Товариства – спроможність Товариства фінансувати зростання своїх активів та виконувати свої зобов’язання у належні строки, не зазнаючи при цьому неприйнятних втрат;

моніторинг ризиків – систематичний збір та обробка інформації про ризики, направлені на забезпечення ефективного контролю за рівнем (величиною) ризиків, з метою інформування структурних підрозділів та керівника Товариства про ризики та поліпшення процесу прийняття рішень щодо управління ризиками;

оцінка ризиків – визначення величини (рівня) ризиків за допомогою кількісних та якісних показників для формування мотивованого судження Товариства щодо рівня ризиків;

внутрішній аудитор – постійно діючий працівник, який є складовою системи внутрішнього контролю, підпорядкованим та підзвітним безпосередньо

члену Наглядової ради – голові комітету з питань аудиту, управління ризиками та комплаєнсу;

менеджер з управління ризиками – постійно діючий працівник, що обирається та призначається рішенням Наглядової ради Товариства, та який виконує функції з управління ризиками Товариства та відповідає за розроблення, впровадження внутрішніх положень (локальних нормативно-правових актів) і процедур управління ризиками відповідно до визначеної Товариством стратегії та політики управління ризиками;

реєстр ідентифікованих ризиків – інструмент управління ризиками, який використовується для документування, організації та моніторингу ризиків, які були ідентифіковані в рамках діяльності Товариства. Його основною метою є забезпечення систематичного підходу до управління ризиками і забезпечення належної уваги до потенційних загроз і можливостей.

ризик – можливість настання події, що матиме негативний вплив на здатність Товариства ефективно виконувати завдання і функції та досягати визначеної мети, стратегічних та інших цілей діяльності;

ризик-апетит – сукупна величина ризику, яку Товариство може приймати в процесі діяльності з метою забезпечення отримання прибутку або досягнення інших цілей, передбачених стратегією та бізнес-планом розвитку Товариства;

система управління ризиками – сукупність дій та політик, методик і процедур управління ризиками, за допомогою яких Товариство здійснює систематичний процес виявлення, ідентифікації, оцінки, моніторингу, контролю, звітування та мінімізації всіх видів ризиків на всіх організаційних рівнях, з метою оцінки достатності внутрішнього капіталу Товариства для покриття всіх видів ризиків, рівня ліквідності Товариства, з урахуванням профілю ризиків, ринкових і макроекономічних умов, взаємозв'язків між різними видами ризиків та забезпечення належного звітування щодо управління ризиками;

управлінські рішення – результат вибору методів і способу дій, здійснений керівником, що спрямований на досягнення результатів відповідно до законодавчо визначених функцій та завдань, мети стратегічних та інших цілей, планів щодо діяльності Товариства;

фішингова атака – це спроба отримати конфіденційну інформацію Товариства оманливим шляхом.

2.2. Інші терміни, які вживаються в цьому Положенні, використовуються в значеннях, визначених законами України та іншими нормативно-правовими актами України.

3. ПРИНЦИПИ ТА ПОРЯДОК ОРГАНІЗАЦІЇ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ТОВАРИСТВА.

3.1. Система управління ризиками відповідає таким принципам:

дієвість та ефективність – забезпечення об’єктивної оцінки розміру ризиків Товариства та повноти заходів щодо управління ризиками з оптимальним

використанням фінансових ресурсів, персоналу та інформаційних систем щодо управління ризиками Товариства;

розподіл обов'язків – забезпечення уникнення ситуації, за якої одна особа здійснює повний контроль над функцією чи видом діяльності Товариства;

усебічність та комплексність – охоплення всіх видів діяльності Товариства та його структурних підрозділів;

своєчасність – забезпечення своєчасного (на ранній стадії) виявлення, вимірювання, моніторингу, контролю, звітування та пом'якшення всіх видів ризиків на всіх організаційних рівнях;

незалежність – відокремлення функції оцінки ефективності системи управління ризиками від функцій її організації і здійснення;

конфіденційність – збереження та захист інформації від несанкціонованого доступу, розголошення або використання третіми особами;

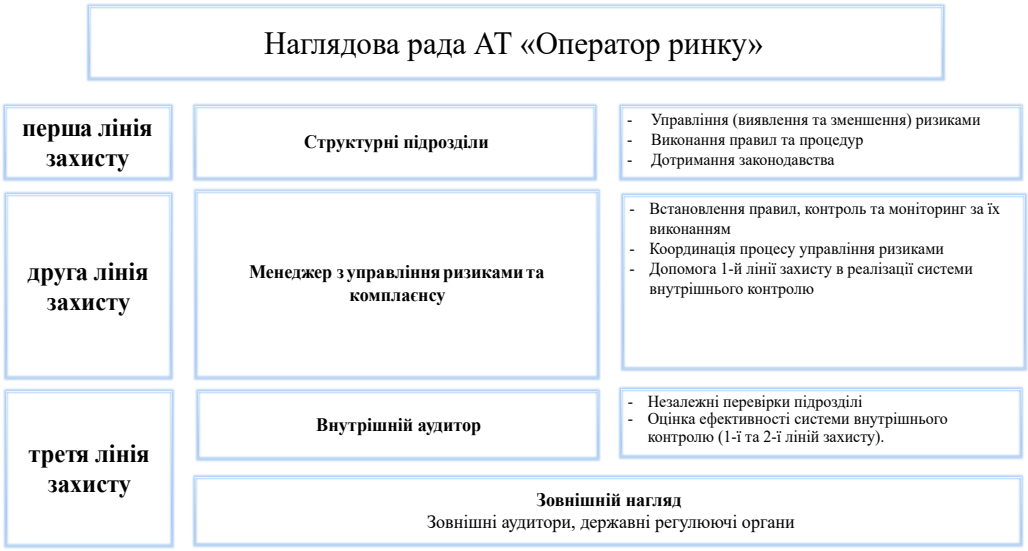
пропорційність – застосування методів та процедур для створення комплексної та ефективної системи управління ризиками, які відповідають рівням складності операцій, що здійснюються Товариством, та його профілю ризиків;

прозорість – оприлюднення Товариством інформації про управління ризиками;

обізнаність – сприяння розвитку культури управління ризиками щодо повного усвідомлення ризиків, притаманних діяльності Товариства, шляхом забезпечення своєчасного та повного розкриття інформації щодо наявних ризиків для їх всебічної оцінки та прийняття своєчасних та адекватних управлінських рішень

3.2. Процес управління ризиками в Товаристві передбачає налагодження процесів та чіткий розподіл обов'язків між підрозділами Товариства із застосуванням моделі трьох ліній захисту:

Рівні внутрішнього контролю АТ «Оператор ринку»



3.3. Ключові ролі та обов'язки суб'єктів системи управління ризиками Товариства:

	Організаційна структура	Основні завдання і функції
1	Наглядова рада	Затверджує стратегію та політику управління ризиками, процедури управління ними, а також перелік видів ризиків.
		Контролює ефективність функціонування системи управління ризиками.
		Забезпечує створення та дотримання культури управління ризиками.
		Призначає та звільняє менеджера з управління ризиками.
		Контролює виконання розроблених Товариством заходів щодо усунення недоліків у функціонуванні системи управління ризиками.
		Забезпечує безперервне функціонування системи управління ризиками.
		Сприяє уникненню будь-якого конфлікту інтересів Товариства.
2	Комітет з питань аудиту, управління ризиками та комплаєнсу	Забезпечує виконання функцій та повноважень, визначених Наглядовою радою.
		Здійснює моніторинг та контроль за виконанням стратегії та політики управління ризиками.
		Визначає перелік, формат і частоту отримання інформації про ризики, на які наражається Товариство.
		Організовує та проводить регулярні зустрічі, наради з метою загального спрямування процесу управління ризиками, у тому числі за результатами розгляду звітів, підготовлених менеджером з управління ризиками.
		Контролює розробку внутрішніх документів Товариства з питань управління ризиками.
		Контролює стан виконання заходів щодо оперативного усунення недоліків у функціонуванні системи управління ризиками.
		Контролює стан виконання заходів, розроблених з метою уникнення конфлікту інтересів у Товаристві.
3		Бере участь у розробці та впроваджені стратегії, політики та інших внутрішніх документів з питань управління ризиками.

	Менеджер з управління ризиками та комплаєнсу	Забезпечує функціонування системи управління ризиками шляхом здійснення своєчасного виявлення, ідентифікації, оцінки, моніторингу, контролю, звітування та мінімізації усіх видів ризиків.
		Узагальнює інформацію про ідентифікацію та оцінку ризиків, отриману від структурних підрозділів.
		Здійснює звітування щодо функціонування системи управління ризиками шляхом регулярної підготовки та надання звітів з питань управління ризиками Наглядовій раді, Комітету Наглядової ради з питань аудиту, управління ризиками та комплаєнсу.
		Забезпечує постійний аналіз всіх видів ризиків, на які наражається Товариство у процесі діяльності.
		Забезпечує оперативну підготовку та надання інформації з питань управління ризиками Наглядовій раді, Комітету Наглядової ради з питань аудиту, управління ризиками та комплаєнсу.
		Забезпечує координацію роботи з питань управління ризиками з іншими структурними підрозділами Товариства.
4	Генеральний директор	Забезпечує розроблення та реалізацію затверджених Наглядовою радою стратегії, політики та інших внутрішніх документів Товариства з питань управління ризиками.
		Формує визначену Наглядовою радою організаційну структуру Товариства, у тому числі обов'язки, повноваження, відповідальність, порядок підпорядкування працівників Товариства.
		Здійснює безперервний процес управління ризиками шляхом забезпечення розроблення та застосування ефективних процедур контролю за всіма видами ризиків.
		Забезпечує здійснення оцінки ефективності функціонування системи управління ризиками на всіх організаційних рівнях Товариства.
		Забезпечує підготовку та надання Наглядовій раді своєчасних та змістовних звітів.
		Забезпечує розроблення політики захисту інформаційних систем та контролює її дотримання.
		Приймає участь у розробці заходів щодо оперативного усунення недоліків у функціонуванні системи управління ризиками.
5	Заступники генерального директора	Приймають участь у реалізації затверджених Наглядовою радою стратегії, політики та інших внутрішніх документів Товариства з питань управління ризиками.
		Приймають участь у контролю за доведенням до відома відповідних структурних підрозділів та працівників Товариства інформації про внесені зміни до стратегії, політики та інших внутрішніх документів з питань управління ризиками.
		Відповідають за координацію різних структурних підрозділів та структурних одиниць, що мають відношення до управління ризиками.
		Приймають участь у розробці заходів щодо оперативного усунення недоліків у функціонуванні системи управління ризиками.
6	Головний бухгалтер	Бере участь у виконані фінансового аналізу для оцінки фінансової стійкості Товариства, аналізує фінансові показники, такі як показники рентабельності, ліквідності та платоспроможності, для виявлення можливих ризиків і прогнозування фінансової стабільності.
		Бере участь у плануванні тарифу Товариства та фінансового плану на рік допомагає установити фінансові цілі, визначити прибуткові та витратні статті.
		Аналізує фінансові звіти, баланси, звіти про прибутки та збитки, а також інші фінансові дані для виявлення тенденцій, показників та потенційних фінансових ризиків.
		Співпрацює зі зовнішніми та внутрішніми аудиторами для здійснення фінансових перевірок та оцінки ефективності системи управління ризиками.

7	Структурні підрозділи	Забезпечують, в межах компетенції, постійний аналіз ризиків, на які наражається Товариство у процесі діяльності.
		Проводять кількісну та якісну оцінку ризиків.
		Готують та надають менеджеру з управляння ризиками реєстр ідентифікованих ризиків Товариства, який включає ідентифікацію та оцінку ризиків.
		Взаємодіяють з менеджером з управління ризиками, іншими органами Товариства, які залучені до процесу управління ризиками.

3.4. З організаційної точки зору управління ризиками відбувається на всіх рівнях Товариства:

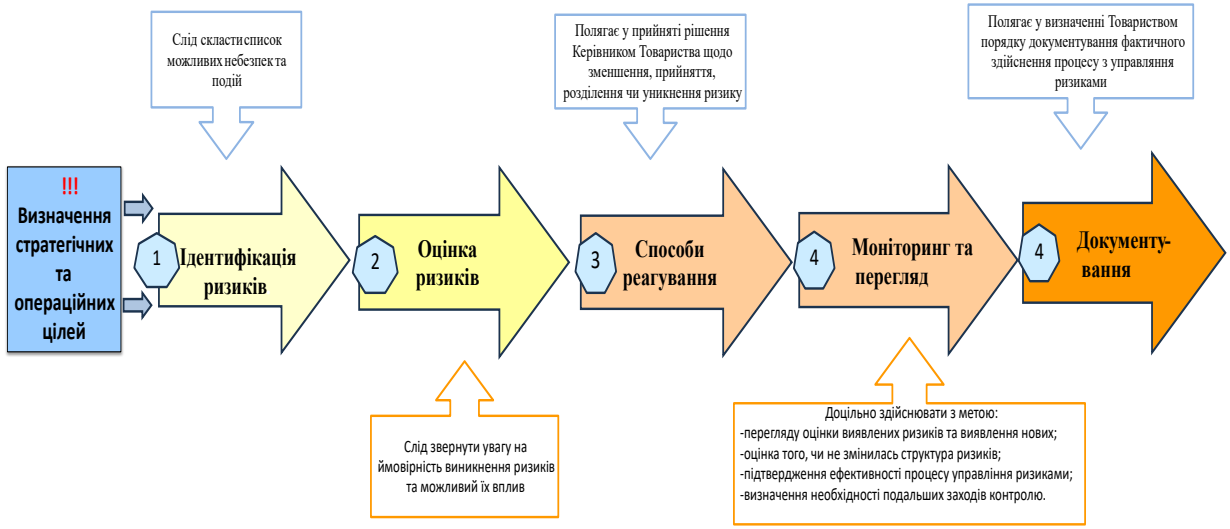
3.4.1. Організаційна структура управління ризиками передбачає чіткий розподіл функцій, обов'язків і повноважень з управління ризиками між усіма суб'єктами системи управління ризиками та працівниками Товариства, а також їх відповідальність згідно з таким розподілом.

3.4.2.Товариство враховує необхідність забезпечення взаємозаміни працівників з метою уникнення негативного впливу на ефективність функціонування системи управління ризиками у разі тимчасової відсутності працівника або його звільнення.

3.4.3. Товариство забезпечує наявність належної кількості кваліфікованих і досвідчених працівників, виходячи з потреб організаційної структури системи управління ризиками.

4. ПОСЛІДОВНІ ЕТАПИ ЗАПРОВАДЖЕННЯ СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ.

4.1. Стратегія з управління ризиками в Товаристві складається з наступних послідовних кроків, які забезпечують успішне впровадження та виконання Стратегії управління ризиками



4.2. Ідентифікація ризиків – визначення ймовірних подій, ситуацій або факторів, які впливатимуть на здатність Товариства виконувати завдання і функції для досягнення встановлених мети (місії) та цілей.

Важливим аспектом під час діяльності Товариства є виявлення та реагування на проблеми/проблемні питання, проте такі дії не розглядаються у контексті управління ризиками, тобто, ризик виникає в майбутньому, несе певну невизначеність та може відбутися/або не відбутися в якийсь час. Важлива відмінність полягає в тому, що управління ризиками спрямоване на систематичний попередній аналіз та планування для зменшення можливих негативних наслідків.

Ідентифікація ризиків здійснюється у кожному структурному підрозділі Товариства шляхом класифікації ризику відповідно до його категорії та виду.

4.2.1. Класифікація ризику відповідно до категорії.

Внутрішні – події, ймовірність виникнення яких пов'язана з безпосереднім досягненням встановлених мети (місії), цілей та завдань, виконанням Товариством та його працівниками відповідних планів, обов'язків, функцій, процесів та операцій. Ризики, на які Товариство має вплив та може вживати відповідні заходи контролю.

Зовнішні – події, які є зовнішніми по відношенню до Товариства та ймовірність виникнення яких не пов'язана з досягненням встановлених мети (місії), цілей та завдань, виконанням Товариством та її працівниками відповідних планів, функцій, процесів та операцій. Тобто ризики, які пов'язані з великою кількістю зовнішніх подій/загроз. Оскільки таких подій може бути багато, основна проблема полягає у визначенні, яка саме подія чи загроза призведе до негативних наслідків в Товаристві.

4.2.2. Класифікація ризику відповідно до його виду.

Перелік суттєвих ризиків із зазначенням видів операцій, які генерують ці ризики:

	Ризик	**Види операцій, які генерують ризик**
1	Нормативно-правові ризики	Зміни в енергетичному законодавстві
		Зміни в політиці регуляторних органів, зокрема НКРЕКП
		Невиконання умов договорів з партнерами
		Недотримання вимог щодо збереження ліцензій
2	Операційні ризики	Ризик недостатньої ефективності та недієвості процесів, які використовуються для виконання операційних функцій
		Ризик помилок у виконанні операцій, включаючи втрату даних, неправильну обробку транзакцій, затримки у виконанні завдань
		Ризик недостатньої надійності постачальників та партнерів, що може вплинути на виконання операційних завдань
		Ризик недостатньої гнучкості та адаптивності до змін у ринкових умовах, технологічних новаціях, вимогах клієнтів
		Ризик втрати конкурентоспроможності через нездатність адаптуватись до нових трендів та вимог ринку

3	Програмно-технічні ризики	Недоліки у програмному забезпеченні можуть призводити до некоректної роботи систем, втрати даних або навіть створення потенційних точок входу для кібератак
		Технічні неполадки або відмови у роботі серверів, баз даних, мережевого обладнання або інших компонентів інфраструктури можуть призвести до перерв у роботі та втрати доступності систем
		Недоцільне розміщення ресурсів або недостатня масштабованість систем може призвести до недостатньої продуктивності під час пікових навантажень або збоїв
		Взаємодія різних програм та систем може призвести до конфліктів, що спричиняють несправність або некоректну роботу
		Напади на інформаційні системи АТ "Оператор ринку" з метою крадіжки даних, впровадження шкідливих програм або навіть блокування роботи можуть створювати серйозні технічні ризики
		Неправильне впровадження оновлень або недостатнє оновлення програмного забезпечення може зробити систему вразливою до атак
		Помилки або збоїв у роботі фізичного обладнання, такого як сервери, мережеве обладнання або сховища даних, можуть призвести до недоступності або втрати даних
4	Кадрові ризики	Несвоєчасне навчання та недостатні знання можуть спричинити некоректні дії або помилки у виконанні робочих обов'язків
		Постійні втрати співробітників та нестабільність складу персоналу можуть негативно позначитися на діяльності компанії і призвести до втрати досвіду та знань
		Конфлікти між співробітниками або між співробітниками та керівництвом можуть призвести до недружньої атмосфери та зниження продуктивності
		Недостатня мотивація працівників може призвести до зниження якості роботи і недосягнення поставлених цілей
		Відсутність внутрішньої спілкування, етики або несвоєчасне вжиття заходів зі зміцнення корпоративної культури можуть призвести до ризиків для репутації компанії
		Втрата ключових талантів може призвести до проблем у здійсненні бізнес-процесів та негативно вплинути на діяльність компанії
		Недоцільний підбір кандидатів на роботу може призвести до зайняття неадекватних або несумісних з посадою співробітників
5	Ризики інформаційної безпеки	Кібератаки: Це можуть бути спроби несанкціонованого доступу до систем, використання шкідливих програм, фішингові атаки, DDoS-атаки тощо
		Втрата даних: Невідповідне зберігання, передача або обробка даних може призвести до їх втрати або пошкодження
		Внутрішні загрози: Співробітники АТ "Оператор ринку" можуть становити потенційну загрозу інформаційній безпеці, особливо якщо вони мають несанкціонований доступ до конфіденційної інформації
		Соціальний інжиніринг: Це включає маніпуляцію людьми для отримання конфіденційної інформації або отримання несанкціонованого доступу до систем
		Несанкціонований доступ до систем: Це може бути результатом слабких аутентифікаційних механізмів, недостатньої захисту мережі або недостатніх правил контролю доступу
6	Репутаційні ризики	Випадки маніпулювання цінами, що може призвести до втрати довіри влади та інвесторів
		Порушення законодавства або етичних стандартів ведення бізнесу, яке може призвести до погіршення іміджу компанії
		Конфлікти інтересів або неправомірні дії керівництва, що можуть спричинити сумніви щодо ділової практики компанії
		Порушення конфіденційності або витік важливої інформації, що може підірвати довіру клієнтів та партнерів

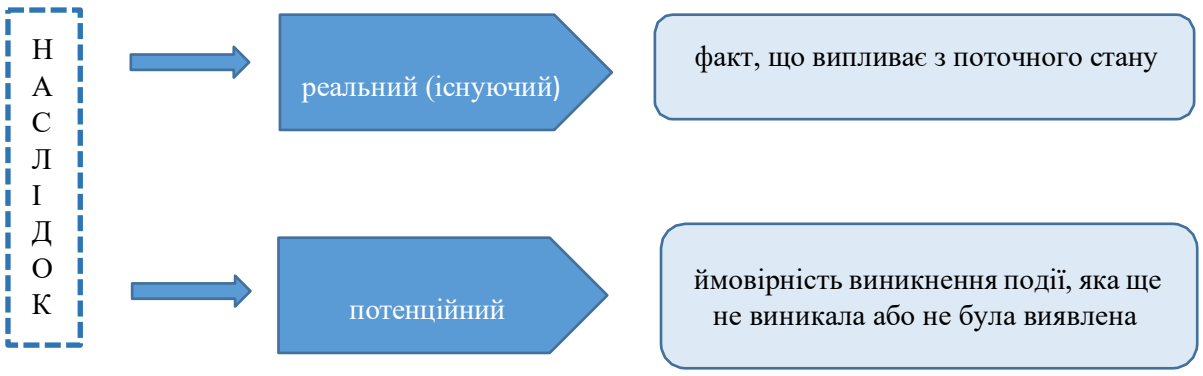
		Проблеми з якістю послуг, що можуть спричинити незадоволення клієнтів і погіршення репутації компанії
7	Фінансові ризики	Ризики зміни попиту: Зміни в ринковому попиті на послуги, що надає АТ "Оператор ринку", можуть впливати на його доходи та прибутковість.
		Ризики конкуренції: За наявності конкурентів на ринку АТ "Оператор ринку" зіткнеться з ризиком втрати своєї частки ринку або зниження цін на послуги
		Фінансові ризики: Сюди входять ризики, пов'язані з управлінням фінансами компанії, такі як недостатня ліквідність, неправильне управління оборотними коштами, зміни вартості активів та пасивів, недоліки у фінансовому плануванні та прогнозуванні
		Ризики залежності від контрагента: Якщо АТ "Оператор ринку" залежить від певних послуг, ризик може полягати у зміні цін, надійності або доступності постачальників
		Ризики змін законодавства та регулювання: Зміни в правовому середовищі, такі як нові податкові закони чи зміни умов ліцензування, можуть мати фінансовий вплив на АТ "Оператор ринку". Компанія повинна відстежувати такі зміни та враховувати їх в своїй стратегії та фінансовому плануванні
		Ризики технологічних змін: Зміни в технологіях та інноваціях можуть вплинути на конкурентоспроможність АТ "Оператор ринку".

4.3. Ідентифікація ризиків здійснюється через визначення причин та наслідків у чіткому їх зв’язку:

Причина – явище чи процес, що вже в міру свого існування викликає певні зміни в середовищі. Причина характеризується тим, що завжди передує результату, при цьому результатом її дії є наслідок. Це свого роду «показники» того, що щось відбувається «не так» та які можна перевірити.

Наслідки – це те, в чому виявляються безпосередні результати певної проблеми. Важливо зазначити, що іноді декілька причин зумовлюють один загальний наслідок. У той же час одна причина може проявитися у безлічі наслідків. Наслідки можуть бути реальними чи потенційними.

Схематично поняття причинно-наслідковий зв’язок відображається наступним чином:



Здійснення заходів з усунення наслідків не усуне самої причини виникнення ризику та не призведе до вдосконалення існуючих процесів в Товаристві, покращення внутрішнього контролю та відповідно управління ризиками. Повністю чи частково уникнення від повторення небажаної події можливо лише через виявлення і усунення безпосередньо її причини.

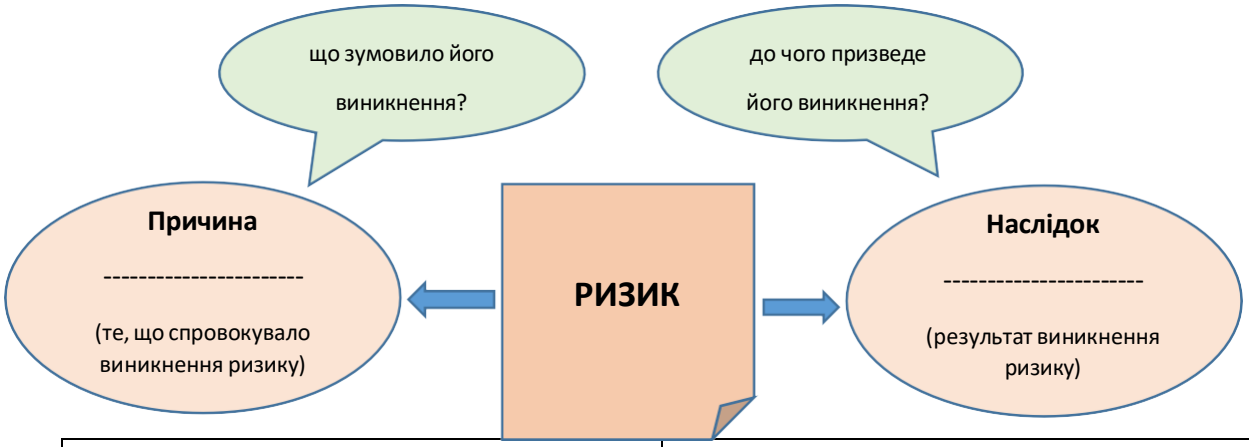
4.4. Оцінка ризиків.

Наступним кроком Стратегії з управління ризиками є оцінка ризиків. Поняття «оцінка ризиків» іноді застосовується в розумінні одноразової дії, однак в контексті розуміння такої оцінки у діяльності Товариства – такий процес є триваючим і повторюваним, який відбувається на всіх рівнях.

Метою оцінки ризиків є визначення, які з подій (ідентифікованих ризиків) є досить важливими та суттєвими, щоб вони були розглянуті керівництвом Товариства.

Оцінка ризиків здійснюється за такими критеріями, як рівень ймовірності виникнення та рівень їх впливу на здатність Товариства виконувати функції для досягнення встановленої мети (місії), цілей та завдань.

Наприклад, оцінка може здійснюватися у такому форматі:



За впливом ризиків на здатність Товариства виконувати функції для досягнення встановленої мети (місії), цілей та завдань		**За ймовірністю виникнення ризику**		
Критерій ризику	Числове значення	Низька ймовірність	Середня ймовірність	Висока ймовірність
		1	**2**	**3**
Низький рівень впливу	**1**	**1 (1 х 1)** (зелена зона)	**2 (1 х 2)** (зелена зона)	**3 (1 х 3)** (жовта зона)
Середній рівень впливу	**2**	**2 (2 х 1)** (зелена зона)	**4 (2 х 2)** (жовта зона)	**6 (2 х 3)** (червона зона)
Високий рівень впливу	**3**	**3 (3 х 1)** (жовта зона)	**6 (3 х 2)** (червона зона)	**9 (3 х 3)** (червона зона)

Завданням оцінки ризиків є визначення ризикових сфер діяльності Товариства та надання відповідної інформації керівнику Товариства для прийняття ним управлінських рішень стосовно тих «ключових» ризиків, що впливають на здатність Товариства виконувати плани, вимоги щодо діяльності, основні функції, процеси та операції для досягнення визначених мети (місії), цілей діяльності та завдань.

4.5. Способи реагування.

4.5.1. Враховуючи результати проведеної оцінки ризиків, в Товаристві приймається рішення щодо вибору форми реагування на них.

Визначення та обрання способів реагування ідентифіковані та оцінені ризики здійснюється шляхом прийняття Керівником Товариства рішення щодо **зменшення, прийняття, розділення чи уникнення ризику** на підставі проведеної оцінки ймовірності виникнення та рівня їх впливу з урахуванням існуючого рівня «ризик-апетиту».

4.5.2. Для прийняття відповідного рішення, оцінюються можливі витрати, пов'язані з реагуванням на ризик, порівняно з очікуваним отриманням майбутньої вигоди від його уникнення або зменшення та здійсненими заходами контролю для запобігання або зменшення його негативного впливу на досягнення визначеної мети (місії), цілей та завдань Товариства (далі – рішення про способи реагування).

1) Зменшення ризику – безсумнівно, що дана форма реагування на ризики є найбільш поширеною та здійснюється через вжиття певних заходів, які сприяють зменшенню або повному усуненню ймовірності їх виникнення та/або впливу (зокрема шляхом прийняття щоденних управлінських рішень під час повсякденної діяльності Товариства).

2) Прийняття ризику передбачає відсутність заходів реагування в Товаристві щодо такого ризику, тобто жодних дій до нього не застосовується. Такий спосіб реагування використовується у випадках, якщо:

за результатами оцінки ризику встановлено, що його вплив на діяльність буде мінімальним і суттєво не позначиться на досягненні встановленої мети (місії), цілей та завдань Товариства, ризик знаходиться в межах допустимого (прийнятного) його рівня;

обсяг витрат на заходи контролю будуть перевищувати вигоди від вжиття певних заходів, спрямованих на зменшення ризику, чи які спричинять виникненню нових негативних наслідків;

застосування способів реагування створить додаткові ризики з високим/середнім значенням;

Товариство не може вплинути на ризик та відсутні заходи контролю щодо запобігання настанню відповідної негативної події.

3) Розділення (розподіл, передача) ризику передбачає зменшення ймовірності виникнення або впливу ризику шляхом його перенесення або розподілу (поділу) частини цього ризику з іншими заінтересованими сторонами/учасниками (наприклад, страхування діяльності). Зазначений варіант є особливо корисним при скороченні фінансових ризиків, ризиків для майна.

4) Уникнення ризику здійснюється шляхом припинення/призупинення діяльності (функції, процесу, операції), яка призводить до підвищення значення ризику. Проте уникнення ризику може бути ефективним способом реагування, якщо необхідно прийняти рішення про прийнятність нового порядку/механізму надання публічних послуг або доцільності продовження реалізації певного проекту.

4.5.3. Рішення про обрані способи реагування приймається з урахуванням допустимого (прийнятного) рівня ризику, який Товариство може прийняти не вживаючи жодних заходів контролю.

4.5.4. Визначення допустимого (прийнятного) рівня ризику є суб'єктивним процесом та здійснюється керівництвом Товариства, керуючись власним досвідом, обраними та впровадженими відповідними механізмами, застосованими інструментами та методами управління.

4.5.5. Під час прийняття рішення щодо способу реагування на ризик враховуються:

результати оцінки ймовірності його виникнення та впливу, тобто його значення (високе, середнє або низьке);

витрати, пов'язані із заходами реагування, порівняно з отриманою вигодою від його зменшення;

що обраний спосіб реагування може спричинити виникнення додаткових ризиків.

4.5.6. У разі наявності залишкових/остаточних ризиків, в Товаристві здійснюється оцінка їх можливого впливу порівняно з допустимим (прийнятним) рівнем ризику й обираються шляхи управління ними, тобто вжиття інших заходів для зменшення рівня їх впливу на здатність Товариства виконувати функції, процеси та операції, для досягнення встановлених мети (місії), цілей та завдань або прийняття таких ризиків.

4.6. Моніторинг та перегляд

4.6.1. Процес з управління ризиками є динамічним, ітеративним і гнучким до змін. У міру зміни пріоритетів, заходи з управління ризиками мають контролюватися та переглядатися.

4.6.2. Моніторинг – це постійний процес проведення оцінки якості функціонування системи внутрішнього контролю та/або окремих його елементів (у тому числі управління ризиками) у часі.

4.6.3. Здійснення моніторингу спрямовано на своєчасне запобігання неефективності, недоцільності та безрезультативності впроваджених механізмів та інструментів внутрішнього контролю і може здійснюватися через організацію відповідних заходів: постійного (безперервного) моніторингу та періодичних оцінок.

4.6.4. Ефективна та результативна система моніторингу у комплексі зі звітуванням охоплює всі складові структури управління ризиками та передбачає здійснення керівниками самостійних структурних підрозділів таких кроків:

1) пріоритезація ризиків залежно від цілей (можливо використання системи пріоритетності ризиків, як при їх оцінюванні);

2) визначення заходів контролю, які стосуються цих «ключових» ризиків (заходи контролю допомагають впевнитись у тому, що Товариство спрямовує ресурси на найбільш важливі напрями своєї діяльності);

3) запровадження інформаційно-комунікаційного обміну про хід досягнення встановлених мети (місії), цілей та завдань (підтвердження ефективності реалізації заходів контролю. Інформація може вказувати на те, що

діяльність з управління ризиками функціонує належним чином, а також на можливість неефективних, недієвих або неактуальних здійснюваних заходів контролю);

4) перегляд впроваджених політик, правил, заходів та їх корегування (за необхідності).

4.6.5. Ефективна система управління ризиками включає застосування відповідних механізмів моніторингу та звітування у щоденній діяльності. Здійснення моніторингу структури управління ризиками включає:

дослідження стану зовнішнього середовища з метою виявлення змін, які можуть вплинути на досягнення встановлених мети (місії), цілей та виконання завдань Товариства;

оцінку ефективності заходів контролю для реагування на «ключові» ризики;

виявлення змін в ідентифікованих та оцінених ризиків у разі змін пріоритетів діяльності Товариства;

виявлення нових «ключових» ризиків.

4.6.6. Перегляд діяльності з управління ризиками доцільно здійснювати з метою:

оцінки того, чи не змінилось їх значення;

визначення необхідності подальших заходів реагування;

підтвердження її ефективності та результативності.

4.6.7. Будь-який процес перегляду має визначати, чи вжиті заходи контролю:

призвели до бажаних результатів;

допомогли у підвищенні поінформованості, що запроваджена діяльність з управління ризиками сприяла прийняттю кращих управлінських рішень, засвоєнню і використанню набутих знань та уроків для удосконалення діяльності з управління ризиками.

4.6.8. Моніторинг передбачає проведення аналізу наслідків реалізації управлінських рішень і оцінку їх доцільності з позиції вже здійснених заходів контролю щодо «ключових» ризиків у залежності від досягнутих результатів.

4.6.9. Моніторинг, як і інші кроки діяльності з управління ризиками, є безперервним процесом, що відбувається протягом усієї такої діяльності.

4.7. Документування управління ризиками.

4.7.1. Діяльність з управління ризиками може документуватися з метою:

1) обміну інформацією про таку діяльність;

2) прийняття відповідних управлінських рішень;

3) її удосконалення;

4)сприяння взаємодії із зацікавленими сторонами, у тому числі відповідальними за здійснення заходів контролю та їх результати.

4.7.2. Документування способів управління ризиками в Товаристві здійснюється через складання відповідних реєстрів, таблиць, матриць ризиків, визначених для конкретних функцій, процесів та операцій, що спрямовані на досягнення її мети (місії), цілей, завдань, із зазначенням заходів контролю, відповідальних виконавців, строків та індикаторів виконання таких заходів

тощо.

5. ПРИНЦИПИ ТА ПЕРІОДИЧНІСТЬ ПОДАННЯ ЗВІТНОСТІ ПРО РИЗИКИ.

5.1. Управлінська звітність про ризики має бути точною, вивіреною, відображати рівень прийнятого Товариством ризику та формується з дотриманням наступних принципів:

комплексність – управлінська звітність про ризики має охоплювати розгляд ризиків як інтегрованої та всебічної системи, яка охоплює всі аспекти діяльності Товариства. Цей принцип допомагає забезпечити ефективне та цілісне управління ризиками, уникнути їх фрагментації та виявлення взаємодій між різними ризиками.

безперервність – надання звітності має охоплювати все Товариство і повинно проводитися безперервно відповідно зі встановленими термінами;

достовірність – відображає необхідність надання об'єктивної, точної та достовірної інформації про ризики організації. Цей принцип покликаний забезпечити, що інформація про ризики викладена без перекручень, приховувань або маніпуляцій, що дозволяє керівництву та зацікавленим сторонам розуміти потенційні небезпеки та приймати обґрунтовані рішення з управління ризиками.;

чіткість та інформативність – управлінська звітність про ризики має надавати чітку та однозначну інформацію та бути достатньо вичерпною для прийняття своєчасних та адекватних управлінських рішень;

періодичність надання – інформація має надаватись періодично, у встановлений термін, а також у випадках, визначених цією Стратегією з управління ризиками;

конфіденційність – управлінська звітність про ризики містить конфіденційний характер та має поширюватися серед користувачів такої звітності із дотриманням заходів конфіденційності.

5.2. Терміни подання звітності:

5.2.1. Структурні підрозділи (не рідше одного разу на квартал, не пізніше за 7 число місяця, що настає за звітним кварталом) надають менеджеру з управління ризиками, опрацьовану, проаналізовану інформацію про ідентифікацію та оцінку ризиків у реєстрі ідентифікованих ризиків.

5.2.2. Менеджер з управління ризиками узагальнює інформацію, отриману від структурних підрозділів, формує узагальнений реєстр ідентифікованих ризиків та звітує щодо функціонування системи управління ризиками, шляхом регулярної підготовки та надання звітів з питань управління ризиками (не рідше одного разу на квартал, не пізніше за 10 число місяця, що настає за звітним кварталом) Наглядовій раді, Комітету Наглядової ради з питань аудиту, управління ризиками та комплаєнсу та Генеральному директору Товариства;

5.2.3. Товариство щороку до 31 жовтня звітує до Міністерства енергетики України щодо запровадженої в Товаристві системи управління ризиками згідно із встановленими формами;

5.2.4. Звітність повинна формуватися із заданою періодичністю і зміст звітів повинен подаватися в структурованому вигляді.

6. ПОРЯДОК ПЕРЕГЛЯДУ ДОКУМЕНТУ

6.1. Ця Стратегія підлягає плановому перегляду та актуалізації не рідше 1 разу на рік.

6.2. Перегляд та оновлення (актуалізація) Стратегії здійснюється шляхом затвердження нової редакції Стратегії або прийняття рішення про дію Стратегії на наступний період до її чергового перегляду за попереднім схваленням та рекомендацією Комітету з питань аудиту, управління ризиками та комплаєнсу.

6.3. Перегляд та оновлення (актуалізація) Стратегії здійснюється з урахуванням змін у законодавстві.

Менеджер з управління
ризиками та комплаєнсу Олена КАРАТУМАНОВА