

АТ "УОП"



3355273

Додаток №5 до протоколу №9
засідання наглядової ради АТ «УОП» від 30.05.2024

22.07.2024

ЗАТВЕРДЖЕНО

Протоколом Наглядової ради 529
Акціонерного Товариства
«Українська оборонна
промисловість»

СТРАТЕГІЯ
управління ризиками
Акціонерного Товариства
«Українська оборонна промисловість»

Київ – 2024

1

№ В-77 від 06.06.2024

АТ "УОП"



3348920

Зміст

I. ВСТУП	3
II. СФЕРА ЗАСТОСУВАННЯ	3
III. ЗАГАЛЬНІ ПОЛОЖЕННЯ	4
IV. ВИЗНАЧЕННЯ ОСНОВНИХ ВИДІВ РИЗИКІВ	5
V. ОСНОВНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ	
Глава 1. Базові інструменти оцінки ризиків	10
Глава 2. Цільове управління стратегічними ризиками	12
Глава 3. Цільове управління операційними ризиками	13
Глава 4. Цільове управління фінансовими ризиками	14
Глава 5. Цільове управління комплаєнс-ризиками	15
Глава 6. Цільовий підхід до оцінки ризиків	15
Глава 7. Мінімізація ризиків	19
Глава 8. Моніторинг і контроль рівня ризиків	19
VI. РИЗИК АПЕТИТ	20
VII. ЗВІТУВАННЯ	21
VIII. КОНТАКТИ ТА ІНФОРМАЦІЯ	21

I. ВСТУП

1.1. Ключовою складовою будь-якої господарської діяльності в умовах мінливості економічного середовища є ризики – потенційні несприятливі внутрішні чи зовнішні події чи процеси, виникнення яких може призвести до фінансових втрат чи неможливості здійснювати діяльність. У відповідності до Закону України від 22.02.2024 № 3587-ІХ «Про внесення змін до деяких законодавчих актів України щодо вдосконалення корпоративного управління» Державне унітарне підприємство, господарське товариство, у статутному капіталі якого більше 50 відсотків акцій (часток) належать державі повинно створити комплексну, адекватну та ефективну систему управління ризиками.

1.2. Створення системи управління ризиками в Акціонерного Товариства «Українська оборонна промисловість» є складовою моделі корпоративного управління об'єктами державної власності в оборонно-промисловому комплексі України відповідно до рекомендацій з корпоративного управління суб'єктами господарювання Організації економічного співробітництва та розвитку.

II. СФЕРА ЗАСТОСУВАННЯ

2.1 Ця Стратегія визначає базові принципи та методики згідно з якими запроваджується та діє система управління ризиками у Акціонерному Товаристві «Українська оборонна промисловість» та на Підприємствах.

2.2 Стратегія управління ризиками розроблена з метою є сприяння досягненню стратегічних цілей Товариства шляхом впровадження та ефективного функціонування комплексної системи управління ризиками, що відповідає міжнародним стандартам та практикам, та передбачає:

- впровадження ризик-орієнтованого підходу в процеси Акціонерного Товариства «Українська оборонна промисловість» (далі АТ «УОП», Товариство) та державних підприємств (у тому числі казенних підприємств), щодо яких АТ «УОП» є уповноваженим суб'єктом управління об'єктами державної власності, а також господарських товариств, 100% акцій (часток у статутному капіталі) яких належить або перебуває в управлінні АТ «УОП» (належали або перебували в управлінні Державного концерну «Укроборонпром» на момент припинення Концерну) (надалі – Підприємство / Підприємства);
- високий рівень залученості власників ризиків до управління ризиками;

- дотримання рівнів ризиків в межах лімітів ризиків визначених в декларації схильності до ризиків.

2.3 Стратегія управління ризиками (далі Стратегія) визначає ключовий напрям розбудови комплексної системи управління ризиками в Товаристві, формалізує ключові підходи до ідентифікації, аналізу та оцінки, мінімізації, впровадження заходів мінімізації, моніторингу та контролю ризиків.

2.4 Стратегія визначає основні види ризиків, якими Товариство управляє в своїй діяльності та визначає цільові підходи до управління основними видами ризиків.

2.5 Стратегія є внутрішнім документом Акціонерного Товариства «Українська оборонна промисловість» і розроблена відповідно до:

- Статуту Акціонерного Товариства «Українська оборонна промисловість»;
- Стратегії розвитку оборонно-промислового комплексу України, затвердженого рішенням Ради національної безпеки і оборони України від 18 червня 2021 року;
- Політики управління ризиками Акціонерного Товариства «Українська оборонна промисловість»;
- Положення про Департамент з питань комплаєнсу та управління ризиками Акціонерного Товариства «Українська оборонна промисловість»;
- Закону України «Про особливості реформування підприємств оборонно-промислового комплексу державної форми власності»;
- Закону України «Про внесення змін до деяких законодавчих актів України щодо вдосконалення корпоративного управління»;
- міжнародних стандартів з управління ризиками, зокрема стандарті ISO 31000:2018 «Менеджмент ризиків» та методології COSO (Committee of Sponsoring Organizations of the Treadway Commission), які передбачають рекомендації щодо впровадження ефективної системи управління ризиками та організацію внутрішнього контролю;
- інших нормативних документів Товариства.

2.6 Органи управління Акціонерного Товариства «Українська оборонна промисловість», усі працівники і посадові особи АТ «УОП» та Підприємств, повинні знати та дотримуватись у своїй діяльності вимог цієї Стратегії.

2.7 Стратегія є обов'язковою до виконання та поширюється на органи управління АТ «УОП та Підприємств та підлягає застосуванню як у внутрішній діяльності, так і у відносинах з діловими партнерами, контрагентами, органами державної влади та органами місцевого самоврядування.

2.8 Ця Стратегія може бути застосована в господарських товариств, 50% і більше акцій яких перебуває в управлінні АТ «УОП», якщо таке рішення буде прийнято відповідним органом управління такого господарського товариства.

ІІІ. ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1 Ця Стратегія формалізує та визначає основні положення функціонування системи управління ризиками в Товаристві та на Підприємствах, а саме:

- визначити та чітко формулює ризики якими управляє Товариство та Підприємства;
- визначає рівні ймовірності реалізації ризиків та вплив в разі реалізації ризиків;
- формує підходи до визначення рівнів ризиків, з метою визначення рівнів ризиків, які відповідно до Декларації схильності до ризиків Товариство / Підприємства, планують прийняти або уникнути;
- формує цільові підходи до управління основними видами ризиків;
- посилення ефективності діяльності Товариства та Підприємств шляхом аналізу та оцінки існуючих ризиків;

3.2 Система управління ризиками АТ «УОП» та взаємодія її суб'єктів побудована на розподілі обов'язків із застосуванням моделі трьох ліній захисту відповідно до Політики управління ризиками.

3.3 Система управління ризиками націлена на послідовну, ефективну та своєчасну ідентифікацію, оцінку, мінімізацію, моніторинг та контроль, і звітування про ризики, які виникають в процесі діяльності Товариства та Підприємств.

3.4 З метою управління ризиками, Товариство / Підприємства застосовують такі підходи:

- ризик-орієнтований підхід який забезпечує організацію та функціонування системи управління ризиками, фокусуючи більше зусиль та заходів до тих напрямків діяльності, яким притаманні більші ризики;
- процесний підхід, який полягає в організації функціонування системи управління ризиками, як системи взаємодіючих процесів, що виконуються всередині функціональної структури і реалізують мету діяльності;
- системний підхід який полягає в тому, що система управління ризиками охоплює всі види діяльності враховуючи, адміністративні та допоміжні функції на всіх організаційних рівнях Товариства та Підприємств, маючи на меті як мінімізацію наслідків реалізації ризиків та і їх запобігання;

3.5 Система управління ризиками Товариства та Підприємств заснована на принципах сформованих в Політиці управління ризиками АТ «УОП».

IV. ВИЗНАЧЕННЯ ОСНОВНИХ ВИДІВ РИЗИКІВ

4.1 Відповідно до Політики управління ризиками, Товариство визначає та управляє наступними основними видами ризиків:

4.1.1 Стратегічний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок неправильних

управлінських рішень та/або неадекватного реагування на зміни в бізнес-середовищі; стратегічний ризик, характеризується неспроможністю Товариства досягти своїх стратегічних цілей.

Стратегічний ризик включає наступні ризики 2-го рівня:

- ризик недосягнення стратегічних цілей – відсутність та/або невірні управлінські рішення, відхилення в процесі реалізації управлінських рішень та/або їх не виконання, що позначається на можливості Товариства забезпечувати обсяги виробництва, займати долю ринку, генерувати дохід / прибуток, контролювати / обмежувати витрати, здобувати та підтримувати конкурентні переваги тощо;
- ризик невиконання / некоректної імплементації стратегічних документів - відхилення в процесі реалізації стратегічних документів, що позначається на можливості Товариства забезпечувати цілі визначені такими документами;
- ризик недосконалого корпоративного управління – сукупність відхилень або окремі відхилення, що негативно впливають на корпоративні відносини між керівництвом Товариства, Наглядовою радою, акціонерами, керівництвом підприємств та іншими зацікавленими сторонами, які складають основу корпоративної структури Товариства. Такі відхилення негативно впливають на досягнення цілей Товариства, шляхом негативного впливу на засоби досягнення таких цілей та/або на результати моніторингу діяльності Товариства та/або на структуру розподілу повноважень та відповідальності та/або та на спосіб прийняття корпоративних рішень;
- ризик неузгодженості з ключовими партнерами (НАТО / ЄС / ОБСЄ / компанії оборонно-промислового комплексу) – розходження між керівництвом Товариства та ключовими партнерами, щодо стратегічних та оперативних цілей, шляхів та методів їх досягнення, управлінських рішень, організації структури управління та розподілу повноважень, тощо що можуть призвести до зменшення обсягу (припинення) співпраці та/або строках досягнення визначених цілей партнерства;
- ризик країни – ризик можливості реалізації зовнішніх подій на рівні держави, інших країн та/або міжнародних організацій, які виникають під тиском на суверенітет країни, можуть проявлятися в війнах, зокрема торгівельних, несприятливих рішеннях інших країн, організацій, засобах тиску на керівництво держави та/або Товариство іншими країнами, організаціями; зовнішній примус до певних рішень тощо;

- ризик політичного впливу – визначається здатністю окремих осіб та/або груп осіб та/або публічних діячів (в тому числі іноземних) формувати або впливати на управлінські рішення, які приймаються Товариством та/або Підприємствами Товариства.

4.1.2 Операційний ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників або інших осіб, збоїв у роботі систем або внаслідок впливу зовнішніх факторів.

Операційний ризик включає наступні ризики 2-го рівня:

- внутрішнє шахрайство – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок шахрайських дій, незаконного привласнення майна або навмисного порушення норм законодавства України або внутрішніх нормативних документів, здійснених працівниками Підприємства / Товариства;
- зовнішнє шахрайство – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок шахрайських дій, незаконного привласнення майна або навмисного порушення норм законодавства України або внутрішніх нормативних документів, здійснених іншими особами (не працівниками Підприємства / Товариства);
- недосконалі процеси – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок розладу, збоїв процесів Підприємства / Товариства та / або неналежного виконання контрагентами та постачальниками своїх зобов'язань що призвели до збоїв процесів Підприємства / Товариства;
- управління персоналом – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок дій, що не відповідають законодавству або помилок в рамках здійснення оптимізації, реорганізації, ліквідації, підбору персоналу, відсутність або прорахунки в кадровій стратегії, системі винагород, в питаннях соціального забезпечення та взаємодії з профспілками;
- взаємовідносини з контрагентами – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок неумисного або недбалого ставлення до професійних обов'язків перед клієнтами включаючи неналежну якість та/або в результаті недосконалих практик ведення співпраці та/або некомпетентності осіб Підприємства / Товариства відповідальних за співпрацю з контрагентами;
- ризик інформаційних технологій – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів

унаслідок несправності та/або невідповідності інформаційних технологій потребам Підприємства / Товариства, що може призвести до порушення їх сталого функціонування, або недоліків в організації управління такими технологіями; ризик інформаційної безпеки - імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик;

- пошкодження активів – ризик збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок пошкодження або знищення активів Підприємства / Товариства через природні або інші події військового, руйнівного характеру та/або непереборної сили;
- юридичні ризик – імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок неочікуваного застосування норм законодавства через можливість їх неоднозначного тлумачення або унаслідок визнання недійсними умов договору у зв'язку з їх невідповідністю вимогам законодавства України;
- репутаційний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок несприятливого сприйняття іміджу Товариства / Підприємства клієнтами, контрагентами, акціонерами, наглядовими та контролюючими органами та іншими зацікавленими сторонами;
- технологічний ризик – ризик пов'язані з суто технічними факторами та характеристиками складних механізмів, окремих елементів механізмів, конструкцій та/або обумовлені неможливістю / обмеженими можливостями використання певних механізмів чи технічних рішень, як в комплексі, так і окремо;

4.1.3 Фінансовий ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів, втрати капіталу в процесі функціонування Підприємства / Товариства. Фінансовий ризик включає наступні ризики 2-го рівня:

- ціновий ризик – це потенційний вплив зміни (зростання або зниження ціни) вартості товарів/робіт/послуг, які використовуються Підприємством / Товариством в діяльності;
- ризик ліквідності - імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок неспроможності Підприємства / Товариства забезпечувати

фінансування поточної діяльності та/або інвестицій та/або виконання своїх зобов'язань у належні строки;

- кредитний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок невиконання Підприємством/ Товариством та/або боржником/контрагентом узятих на себе зобов'язань;
- процентний ризик - імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок впливу несприятливих змін процентних ставок як в частині активів так і зобов'язань;
- валютний ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів, який виникає через несприятливі коливання курсів іноземних валют, що впливають на вартість/ціну активів/зобов'язань Підприємства / Товариства.

4.1.4 Комплаєнс-ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів, імовірність накладення санкцій, внаслідок невиконання Товариством / Підприємством вимог законодавства, нормативно-правових актів, ринкових стандартів, правил добросовісної конкуренції, правил корпоративної етики, виникнення конфлікту інтересів, а також внутрішніх нормативних документів Товариства / Підприємства.

Комплаєнс-ризик включає наступні ризики 2-го рівня:

- корупційний ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів через вчинення корупційного або пов'язаного з корупцією правопорушення, що негативно вплине на діяльність організації;
- регуляторний ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів через недотримання регуляторних вимог, зокрема, нормативних документів, законів, міжнародних стандартів, тощо;
- ризик внутрішніх невідповідностей (internal non-compliance risk) – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів через відхилення від встановлених стандартів, правил та вимог визначених внутрішніми нормативними документами, корпоративними правилами, корпоративною культурою Товариства / Підприємства.
- санкційний ризик – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів, або втрати репутації, обмеження господарської діяльності, значний час і витрати на проведення внутрішніх розслідувань та/або захист від

розслідувань та примусових заходів в результаті недотримання санкцій;

- ризик конфлікту інтересів – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів в разі (потенційної) ситуації, за якої приватний інтерес (зацікавленість) працівника чи пов'язаних з ним осіб впливає або може вплинути на належне виконання ним посадових (трудових) обов'язків та його об'єктивність або неупередженість при прийнятті рішень, вчинення чи невчинення дій під час виконання посадових (трудових) обов'язків. В результаті конфлікту інтересів виникає суперечність між приватним інтересом (зацікавленістю) працівника та/чи пов'язаних з ним осіб та правами і законними інтересами Підприємства або АТ «УОП»;
- ризик неетичної (ділової) поведінки – це імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів через порушення норм ділової культури та поведінки, заснованих на принципах прийнятих в Товаристві / Підприємствах та моральних засадах, який включає недобросовісні методи та прийоми ведення ділових взаємовідносин;
- штрафи / стягнення – ризик накладення на Підприємство / Товариство штрафів / стягнень / заборон / інших обмежень;
- ризик корпоративної, соціальної, екологічної відповідальності (ESG ризик) – це ризик негативного впливу на навколишнє середовище (забруднення та безвідповідальне ресурсокористування, зміна клімату, біорізноманіття тощо), ризик у сфері охорони праці та промислової безпеки, ризик негативного впливу на суспільство (здоров'я та безпека працівників та клієнтів, негативний вплив на регіони присутності тощо).

V. ОСНОВНІ ПІДХОДИ ДО УПРАВЛІННЯ РИЗИКАМИ

Глава 1. Базові інструменти оцінки ризиків

5.1.1 З метою здійснення ідентифікації, якісної та кількісної оцінки, аналізу основних видів ризиків можливо застосування наступних інструментів ідентифікації та оцінки ризиків:

- проведення мозкового штурму, що полягає у відкритому зборі й обговоренні думок та ідей заінтересованих сторін - учасників мозкового штурму;
- анкетування / опитування, що полягає у зборі думок та ідей за допомогою набору послідовних питань шляхом незалежного та анонімного висловлення думок, у тому числі за допомогою електронних засобів комунікації;

- метод експертних оцінок (метод Делфі), що полягає у зборі бачення, оцінок, причинно-наслідкових зв'язків, практичних та теоретичних знань щодо (потенційних) ризиків, їх причин та наслідків, від осіб, які володіють високою експертизою та компетенцією щодо питання, яке оцінюється;
- метод «Що - якщо», що полягає у проведенні аналізу з метою пошуку (моделюванні) відповідей на питання «Що може відбутися, якщо...?», «Яким чином ...?»;
- моделювання дерева рішень - метод відпрацювання оптимальних рішень, шляхом пошуку найкращих рішень для кожного кроку (етапу), які мінімізують ризики або дозволяють їх уникати;
- моделювання дерева відмов - метод відпрацювання оптимальних рішень, шляхом постановки (потенційних) ризиків / «відмов» та пошуку рішень для пошуку найкращих рішень для кожного кроку (етапу), які мінімізують такі ризики / «відмови» або дозволяють їх уникати;
- сценарний аналіз, що полягає у моделюванні правдоподібних сценаріїв реалізації ризику;
- стрес-тестування - метод вимірювання ризику, через моделювання стрес-сценарію(їв), що дає змогу оцінити потенційні несприятливі результати впливу ризиків. Такий результат виражається через величину потенційних збитків, що можуть стати наслідком шоккових змін різних факторів ризиків, які відповідають виключним (екстремальним), але ймовірним подіям;
- SWOT аналіз, що передбачає ідентифікацію та оцінку сильних (strengths) та слабких (weaknesses) сторін суб'єкту оцінки, а також можливостей (opportunities) та загроз (threats). Такий аналіз дозволяє визначити найбільш значущі ризики суб'єкта оцінки та розробити плани для їх мінімізації.
- метод екстраполяції, що передбачає перенесення висновків, отриманих зі спостережень за одним суб'єктом або його складовою та перенесення таких висновків на інші подібні суб'єкти та/або частини суб'єкту;
- встановлення критеріїв якісної та/або кількісної оцінки, згруповані в систему рейтингування;

5.1.2 Вказаний в п.5.1.1 перелік інструментів є базовим та не є вичерпним і може бути доповненим. Даний перелік дозволяє здійснити ідентифікацію, аналіз та оцінку ризиків. З метою більш глибокої ідентифікації ризиків їх детального аналізу та оцінки доцільно використовувати поєднання вказаних методів, а також застосування цільових інструментів оцінки кожного виду ризиків. Координацію конкретного методу оцінки ризику здійснює Департамент з питань комплаєнсу та управління ризиками на кожному відповідному етапі впровадження системи управління ризиками.

Глава 2. Цільове управління стратегічними ризиками

5.2.1 Ідентифікація та оцінка стратегічних ризиків ґрунтується на:

- аналізі ключових та/або стратегічних документів Товариства / Підприємства, зокрема стратегії Товариства, плану щодо її реалізації;
- планах вдосконалення системи корпоративного управління відповідно стандартів Організації економічного співробітництва та розвитку, тощо;
- фінансовому плані;
- інвестиційному плані;
- плану перетворень / злиття / поглинання;
- Законів України, документів на рівні центральних органів виконавчої влади, актів національних державних органів;
- інших стратегічних документів, концепцій, тощо.

5.2.2 Управління стратегічними ризиками передбачає:

- розробку стратегічних / концептуальних документів щодо окремих напрямків діяльності Товариства / Підприємства та алгоритмів реагування на ризики;
- виконання розрахунків вигоди та економічного ефекту для Товариства / Підприємства при розгляді нових проєктів, стратегічних, організаційних змін тощо;
- аналіз макроекономічного середовища, його вплив на стратегічні цілі й відповідна адаптація стратегії Товариства / Підприємства;
- застосування підходів проєктного менеджменту;
- визначення індикаторів досягнення стратегічних цілей;
- каскадування стратегічних цілей Товариства на операційну діяльність;
- розробку, регламентацію та впровадження циклічного процесу стратегічного планування;
- посилення роботи з пріоритизації інтересів Товариства на державному рівні – на рівні державних органів виконавчої влади, на рівні Кабінету Міністрів України, на рівні Верховної Ради України, на рівні Президента України;
- упровадження ключових індикаторів ризику та їх послідуочий аналіз;
- здійснення тематичних перевірок окремих процесів;
- аналіз ризиків для інвестиційних проєктів, враховуючи (але не виключно) показники чистої теперешньої вартості, дисконтування, норм рентабельності, строків окупності, аналіз впливу на бізнес-процеси;

5.2.3 Перелік інструментів вказаний в п.5.2.2 є цільовим для управління стратегічними ризиками та не є вичерпним і може бути доповненим. Координацію конкретного методу оцінки ризику здійснює Департамент з питань комплаєнсу та управління ризиками АТ «УОП» на кожному відповідному етапі впровадження системи управління ризиками.

5.2.4 Результатом ідентифікації, оцінки та аналізу стратегічних ризиків є висновок з оцінки ризиків та/або відповідна інформація в загальному реєстрі ризиків Товариства та/або Підприємства. Загальний реєстр ризиків АТ «УОП» та Підприємства ведеться та актуалізується ризик-координатором АТ «УОП» та Підприємств і періодично агрегується на рівні Товариства, в Департаменті з питань комплаєнсу та управління ризиками.

5.2.5 Визначення та встановлення лімітів стратегічних ризиків здійснюється в рамках Декларації схильності до ризиків.

Глава 3. Цільове управління операційними ризиками

5.3.1 Ідентифікація та оцінка операційних ризиків ґрунтується на аналізі процесів діяльності Товариства / Підприємства, взаємодії з партнерами, персоналом, а також аналізу впливу зовнішніх подій на діяльність Товариства / Підприємства.

5.3.2 Управління операційними ризиками передбачає:

- здійснення самооцінки ризиків, шляхом створення робочих груп та проведення опитування власників ризиків;
- створення та накопичення бази суттєвих подій;
- створення та ведення реєстру ризиків;
- створення та ведення реєстру планів заходів, аналіз ефективності їх виконання;
- проведення стрес-тестування операційного ризику або окремо операційних ризиків 2-го рівня;
- упровадження ключових індикаторів ризику та їх послідуочий аналіз;
- проведення регулярної оцінки внутрішніх нормативних документів Товариства / Підприємства;
- здійснення тематичних перевірок окремих процесів Товариства / Підприємства.

5.3.3 Перелік інструментів вказаний в п.5.3.2 є цільовим для управління операційними ризиками та не є вичерпним і може бути доповненим. Координацію конкретного методу оцінки ризику здійснює Департамент з питань комплаєнсу та управління ризиками АТ «УОП» на кожному відповідному етапі впровадження системи управління ризиками.

5.3.4 Результатом ідентифікації, оцінки та аналізу операційних ризиків є висновок з оцінки ризиків та/або відповідна інформація в загальному реєстрі ризиків Товариства та/або Підприємства. Загальний реєстр ризиків АТ «УОП» та Підприємства ведеться та актуалізується ризик-координатором АТ «УОП» та Підприємств і періодично агрегується на рівні Товариства, в Департаменті з питань комплаєнсу та управління ризиками.

5.3.5 Визначення та встановлення лімітів операційних ризиків здійснюється в рамках Декларації схильності до ризиків.

Глава 4. Управління фінансовими ризиками

5.4.1 Управління фінансовим ризиком передбачає:

- здійснення на постійній основі вибіркового контролю за цінами на основні товари та послуги, що закуповуються та реалізуються Підприємствами / Товариством, на усіх етапах проведення процедур закупівлі;
- встановлення прямих контрактів з виробниками (у разі такої можливості);
- прогноз вільних грошових коштів, у тому числі за методом ролінгу;
- аналіз розривів ліквідності;
- впровадження порядку пріоритизації платежів у разі кризи ліквідності (нестачі коштів для своєчасного виконання всіх зобов'язань);
- лімітування витрат в разі загрози кризи ліквідності;
- упровадження Плану дій в умовах кризи ліквідності на Товаристві / на Підприємстві;
- централізоване управління вільною ліквідністю;
- автоматизація процесу управління ліквідністю;
- хеджування валютних ризиків, мінімізації кредитного ризику шляхом застосування банківських інструментів;
- удосконалення підходів щодо формування резервів під очікувані збитки в разі несвоєчасно погашення дебіторської заборгованості;
- забезпечення участі Товариства в процесах погодження значних правочинів Підприємств;
- здійснення регулярного моніторингу рівнів процентних ставок на ринку, порівняльний аналіз умов фінансування, що пропонуються банками та аналіз ринкових тенденцій;
- упровадження системи внутрішніх нормативних документів, що регламентують процеси аналізу та управління фінансовими ризиками, зокрема, взаємодії з контрагентами; роботи з фінансовими установами щодо розміщення вільних коштів та послуг щодо покриття ризиків взаємодії з контрагентами; процедур відбору банків; процесів роботи з простроченою заборгованістю; тощо;
- проведення стрес-тестування фінансового ризику або окремо фінансових ризиків 2-го рівня;
- упровадження ключових індикаторів ризику та їх послідуєчий аналіз;
- здійснення тематичних перевірок окремих процесів;

5.4.2 Перелік інструментів вказаний в п.5.4.1 є цільовим для управління фінансовими ризиками та не є вичерпним і може бути доповненим. Координацію конкретного методу оцінки ризику здійснює Департамент з питань комплаєнсу та управління ризиками АТ «УОП» на кожному відповідному етапі впровадження системи управління ризиками.

5.4.3 Результатом ідентифікації, оцінки та аналізу операційних ризиків є висновок з оцінки ризиків та/або відповідна інформація в загальному реєстрі ризиків Товариства та/або Підприємства. Загальний реєстр ризиків АТ «УОП» та Підприємства ведеться та актуалізується ризик-координатором АТ «УОП»

та Підприємств і періодично агрегується на рівні Товариства, в Департаменті з питань комплаєнсу та управління ризиками.

5.4.4 Визначення та встановлення лімітів фінансових ризиків здійснюється в рамках Декларації схильності до ризиків.

Глава 5. Управління комплаєнс-ризиками

5.5.1 Управління комплаєнс-ризи́ком передбачає:

- проведення оцінювання корупційних ризиків Товариства та Підприємств;
- впровадження принципу tone at the top;
- впровадження принципів доброчесності та етики;
- створення комунікаційного каналу для звернень;
- створення каналу комунікації з керівником комплаєнсу;
- впровадження механізму захисту прав викривачів;
- створення системи каналів повідомлень;
- побудову діалогу з зовнішніми стейкхолдерами;
- проведення опитувань;
- проведення навчання;
- управління конфліктом інтересів;
- впровадження ключових індикаторів ризику та їх послідовний аналіз;
- здійснення тематичних перевірок окремих процесів;

5.5.2 Перелік інструментів вказаний в п.5.5.1 є цільовим для управління комплаєнс ризиками та не є вичерпним і може бути доповненим. Координацію конкретного методу оцінки ризику здійснює Департамент з питань комплаєнсу та управління ризиками АТ «УОП» на кожному відповідному етапі впровадження системи управління ризиками.

5.5.3 Результатом ідентифікації, оцінки та аналізу комплаєнс ризиків є висновок з оцінки ризиків та/або відповідна інформація в загальному реєстрі ризиків Товариства та/або Підприємства. Загальний реєстр ризиків АТ «УОП» та Підприємства ведеться та актуалізується ризик-координатором АТ «УОП» та Підприємств і періодично агрегується на рівні Товариства, в Департаменті з питань комплаєнсу та управління ризиками.

5.5.4 Визначення та встановлення лімітів комплаєнс ризиків здійснюється в рамках Декларації схильності до ризиків.

Глава 6. Цільовий підхід до оцінки ризиків

5.6.1 Відповідно до Політики управління ризиками АТ «УОП» для аналізу ризиків використовується шкала, яка складається з 4х рівнів - «низький», «середній», «високий», «дуже високий».

5.6.2 Аналіз ризиків полягає в визначенні:

- а/ ймовірності реалізації ризику, яка визначається на основі 4-х бальної шкали, що формалізована у вигляді Таблиці 1 для визначення рівня ймовірності реалізації ризику

Таблиця 1. Визначення рівня ймовірності реалізації ризику

Рівень імовірності і значення	Скорінг	Визначення
Дуже високий	4 бали	Ризик може бути реалізований із частотою - 1 раз та більше, протягом 6 місяців та/або ризик реалізовувався протягом минулих 6 місяців
Високий	3 бали	Реалізація ризику із частотою - 1 раз та більше є можливою у діапазоні від 6 до 12 місяців та/або ризик реалізовувався протягом минулих 12 місяців
Середній	2 бали	Реалізація ризику із частотою - 1 раз та більше є можливою у діапазоні від 1 до 3 років та/або ризик реалізовувався протягом минулих 1-3 роки
Низький	1 бал	Реалізація ризику із частотою - 1 раз та більше є можливою у діапазоні від 3х років та/або ризик не реалізовувався в минулому

б/ визначені впливу ризику. Вплив визначається на основі 5 бальної шкали окремо за рівнем фінансового (кількісного) впливу, що формалізовано в формі Таблиці 2 та окремо за рівнем не фінансового (якісного) впливу - Таблиця 3:

Таблиця 2 Визначення рівня фінансового (кількісного) впливу

Рівень фінансового впливу	Скорінг	Загальна сума втрат від ризику для підприємств <u>річний дохід до 300*</u>	Загальна сума втрат від ризику для підприємств <u>річний дохід від 300 до 1000*</u>	Загальна сума втрат від ризику для підприємств <u>річний дохід від 1000*</u>
		* - річний рівень доходу в млн грн (в еквіваленті)		
Критичний	5 балів	перевищує 10% загальних активів або річного доходу підприємства		
Дуже високий	4 бали	перевищує 1% річного доходу підприємства		
Високий	3 бали	від 300 тис. грн. до 1% річного доходу	від 1 млн грн до 1% річного доходу	від 5 млн грн до 1% річного доходу

Середній	2 бали	від 50 тис. грн. до 300 тис. грн	від 300 тис. грн. до 1 млн грн	від 1 до 5 млн грн
Низький	1 бал	менше або дорівнює 50 тис. грн.	Менше або дорівнює 300 тис. грн.	менше або дорівнює 1 млн грн

Таблиця 3 Визначення рівня нефінансового (якісного) впливу

Рівень нефінансового / якісного впливу	скорінг	Визначення
Критичний	5 балів	Загибель працівників Серйозна шкода навколишньому середовищу Пошкодження будівель/виробничої лінії, що призвело до зупинки більш ніж на 72 години
Дуже високий	4 бали	Критично для діяльності підприємства – зупинка, унеможливлення функціонування підприємства або критичних процесів (наприклад виробництва)
Високий	3 бали	Вплив на діяльність підприємства високий, зміни в діяльності підприємства є необхідними, високий вплив на цільову діяльність підприємства та/або реалізацію стратегічних планів, цільових стратегій, фінансового плану, тощо
Середній	2 бали	Вплив на діяльність підприємства присутній, потрібні мінімальні зміни в діяльності підприємства, які не матимуть впливу на цільову діяльність підприємства (наприклад виробництво)
Низький	1 бал	Вплив на діяльність підприємства відсутній або мінімальний (не спричинить жодних змін в діяльності підприємства)

5.6.3 В процесі аналізу ризиків визначається:

- рівень ймовірності (значення від 1-го до 4-х балів, яке відповідає рівню ймовірності відповідно «низький», «середній», «високий», «дуже високий»)(Таблиця 1);
- рівень впливу, значення від 1-го до 5 балів яке відповідає рівню впливу відповідно «низький», «середній», «високий», «дуже високий»,

«критичний». Рівень впливу визначається окремо для фінансового (кількісного) впливу та/або не фінансового (якісного) впливу. Рівень впливу визначається як найбільше значення (бал) з поміж фінансового та або якісного впливу.

5.6.4 Для аналізу ризиків можуть використовуватись наступні дані:

- періодичних звітів для внутрішнього користування, в тому числі інформаційно-аналітичні матеріали Товариства;
- дані (інформаційних) систем Підприємства / Товариства;
- загальні дані щодо діяльності Підприємства / Товариства та ринку, в тому числі з інтернет-ресурсів;
- дані управлінського / бухгалтерського / фінансового / складського / інших видів обліку прийнятих на Підприємстві / Товаристві;
- дані щодо ризиків, отриманими від Департаменту з питань комплаєнсу та управління ризиками, ризик-координаторів, інших джерел;

5.6.5 Після визначення рівня ймовірності та рівня впливу визначається профіль ризику. Профіль ризику є результатом оцінки рівня ризиків на певну дату до врахування заходів для мінімізації ризиків.

5.6.6 Профіль ризику визначається як добуток балів рівня ймовірності реалізації ризику та рівня впливу (фінансового або якісного залежно від того яке значення є більшим) від реалізації ризику згідно наступної матриці ризиків (таблиця 4):

Таблиця 4

Ймовірність							
4	дуже високий						
3	високий						
2	середній						
1	низький						
Матриця ризиків		низький	середній	високий	дуже високий	критичний	вплив
		1	2	3	4	5	

Профіль ризику:

Критичний дорівнює значенню = 5 / 10 /15 /20 балів

Дуже високий = 12 / 16 балів;

Високий = 6 / 8 / 9 балів;

Середній = 3 / 4 бали;

Низький = 1 / 2 бали.

5.6.7 В результаті проведення етапу аналізу та оцінки ризиків - визначений рівень ризику та опис з обґрунтування рівня ймовірності та рівня впливу зазначається в реєстрі ризиків.

5.6.8 Реєстр ризиків - реєстр в форматі ексел-таблиці в якому відображено опис ідентифікованих ризиків, середовища організації, визначення та опис ймовірності та впливу ризиків, визначено рівень ризиків та відповідні заходи мінімізації ризиків. На Підприємствах ризик-координатор створює та підтримує в актуальному стані реєстр ризиків. В Товаристві ведення реєстру ризиків (за ризиками ідентифікованими в Товаристві) здійснює Департамент з питань комплаєнсу та управління ризиками.

Глава 7. Мінімізація ризиків

5.7.1 Мінімізація ризику - включає в себе визначення стратегії мінімізації ризику відповідно до Політики управління ризиками АТ «УОП» та розробку плану дій (планів заходів) щодо мінімізації ризиків.

5.7.2 План мінімізації ризику (план дій / захід) має відповідати 5 компонентам, а саме:

- захід є конкретним, що означає, що захід має бути точно визначений та сформульований;
- захід є вимірювальним, що означає, що захід можливо виміряти та досягнути;
- захід є досяжний, що означає, що захід можливо досягти;
- захід є релевантний, що означає, що захід має бути направлений саме на проблемний процес, на джерело ризику, а реалізація заходу змінить рівень ризику в сторону його зменшення;
- захід є визначений в часі, що захід повинен мати кінцевий термін для виконання заходу;

5.7.4 Плани мінімізації ризиків розробляються з урахуванням наступних принципів:

- усебічності та комплексності
- ефективності
- адекватності
- обачності
- ризик-орієнтованого підходу
- інтегрованості
- завчасності

5.7.5 На Підприємствах ризик-координатор створює та підтримує в актуальному стані базу планів заходів. В Товаристві ведення реєстру планів заходів (за заходами впровадженими в Товаристві) здійснює Департамент з питань комплаєнсу та управління ризиками.

5.7.6 База планів заходів – ексель реєстр в якому відображена вся сукупність планів заходів, спрямованих на мінімізацію ризиків, ідентифікованих в рамках системи управління ризиками.

Глава 8. Моніторинг і контроль рівня ризиків

5.8.1 Моніторинг рівня ризику - дія, яка полягає в оцінці ризику в процесі спостереження за рівнем ризиком та тренду зміни рівня ризику.

5.8.2 Після первинної ідентифікації ризику та реалізації планів мінімізації ризику (в разі їх вжиття) здійснюється повторний вимір рівня ризику за шкалою ймовірності та шкалою впливу та співставлення отриманих значень з попередньою (попередніми) оцінкою ризику.

5.8.3 В разі знижувального тренду рівня ризику, а саме зміни рівня ризику з «критичного», «дуже високого» або «високого» до «низького» або «середнього» здійснюється подальший моніторинг рівня ризику.

5.8.4 В разі висхідного тренду рівня ризику, а саме якщо в процесі моніторингу рівня ризику повторно отримано значення «критичний», «дуже високий» або «високий», або рівень ризику зріс з «низького» або «середнього» до «високий», «дуже високий» або «критичний» - впроваджується новий / уточнений план заходів та відповідно подальший моніторинг.

5.8.5 В разі перманентно низького тренду моніторингу рівня ризику, а саме отримання значення «низький» протягом декількох періодів спостережень, в подальшому можливо не здійснювати моніторинг рівня ризику, якщо він не є характерним для Підприємства або можливо змінити періодичність проведення спостережень за ризиком в бік зменшення частоти спостереження. Дані щодо такого ризику та результати моніторингу можливо використовувати в діяльності щодо управління ризиками.

VI. РИЗИК АПЕТИТ

6.1 Товариство / Підприємства виражають ризик-апетит в кількісному та якісному вимірі з встановленими лімітами та рівнями раннього виявлення, які є інструментом моніторингу профілю ризику для суб'єктів системи управління ризиками.

6.2 У разі наближення або перевищення кількісних лімітів чи відхилення від якісних критеріїв ризик-координатор здійснює звітування про такі факти в межах щоквартального звітування;

6.3 Перегляд кількісних та якісних показників основних ризиків, в тому числі критеріїв та лімітів ризику, здійснюється на щорічній основі або у разі потреби за умови суттєвих внутрішніх чи зовнішніх змін та/або змін нормативно-правової бази.

6.4 Перегляд критеріїв та лімітів основних видів ризику враховує стратегічні напрямки діяльності та відображає стратегічну візію Наглядової ради АТ «УОП».

6.5 Ключовим завданням процесу визначення та моніторингу профілю ризику Товариства / Підприємства є виявлення сфер діяльності, які мають найбільшу концентрацію ризику, з метою прийняття подальших обґрунтованих управлінських рішень щодо розробки й застосування інструментів і заходів мінімізації виявлених ризиків.

6.6 Моніторинг та контроль профілю основних видів ризику забезпечується шляхом впровадження відповідних механізмів, процедур і процесів інформування та агрегування даних щодо профілю ризиків (результати самооцінки ризику, фактичні події ризику, звітування про суттєві події, оцінка ризиків в процесах, інші зовнішні та/або внутрішні оцінки ризиків та їх наслідки тощо).

6.7 Значення ризик-апетиту Товариства / Підприємств щодо основних видів ризиків визначається в декларації схильності до ризиків Товариства.

6.8 Декларація схильності до ризиків Товариства та Підприємств затверджується Наглядовою Радою АТ «УОП» за поданням Департаменту з питань комплаєнсу та управління ризиками.

VII. ЗВІТУВАННЯ

7.1 З метою управління ризиками, Департамент з питань комплаєнсу та управління ризиками регулярно здійснює збір та агрегування інформації з АТ «УОП» та Підприємств щодо рівня ризиків, а саме:

- інформації щодо суттєвих подій;
- регулярної оцінки ризиків;
- самооцінки як окремих процесів;
- комплексної оцінки ризиків Підприємства;
- оцінки ризиків «нової діяльності»;
- результатів моніторингу ключових індикаторів ризику;
- стану впровадження планів заходів та їх ефективності;
- інші питання відповідно до документів, що регулюють діяльність системи управління ризиками;

7.2 Департамент з питань комплаєнсу та управління ризиками агрегує, аналізує та пріоритизує інформацію вказану в п.7.1 з метою подання управлінської звітності щодо рівня ризиків на які наражається АТ «УОП» та Підприємства.

7.3 Звітування Департаменту з питань комплаєнсу та управління ризиками здійснюється в рамках положень визначених в Політиці управління ризиками.

**Директор департаменту з питань
комплаєнсу та управління ризиками**

Олена КОВАЛЬОВА