ГРОМАДСЬКА СПІЛКА
МЕРЕЖА ПРАВОВОГО РОЗВИТКУ

ГРОМАДСЬКА СПІЛКА
«МЕРЕЖА ПРАВОВОГО РОЗВИТКУ»
LEGAL DEVELOPMENT NETWORK

ldn.org.ua
office@ldn.org.ua
facebook.com/legaldnetwork

ЗАТВЕРДЖЕНО
Рішенням Правління
Громадської спілки
«Мережа правового розвитку»
Протокол
№ 1 від «20» січня 2025 року

ПОЛОЖЕННЯ ПРО УПРАВЛІННЯ РИЗИКАМИ

ТЕРМІНОЛОГІЯ

Організаційний процес - сукупність взаємопов'язаних або взаємодіючих видів діяльності, спрямованих на
створення певного продукту або послуги в Мережі.
Інформаційний ризик/ризик інформаційної безпеки - ймовірність виникнення збитків або додаткових втрат (витрат) внаслідок виникнення внутрішніх і зовнішніх подій щодо інформаційних
систем Мережі та інших інформаційних ресурсів, на яких зберігається інформація щодо усіх видів діяльності Мережі, що використовуються для досягнення цілей Мережі, і який виник в результаті недостатності
внутрішнього контролю чи недостатніх або помилкових внутрішніх процесів управління.
Інформаційний ризик є складовою операційного ризику, однак виділений окремо як суттєвий ризик
для Мережі.
Операційний ризик - ймовірність виникнення збитків або додаткових втрат (витрат) внаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників Мережі або інших осіб, збоїв у роботі управлінських систем Мережі або внаслідок впливу зовнішніх факторів.
Операційний ризик включає корупційний, репутаційний, стратегічний, юридичний чи інші ризики,
однак ними не обмежується.
Пом'якшення ризиків - комплекс заходів, спрямованих на зменшення ймовірності виникнення ризику та/або зменшення впливу ризику на результати діяльності Мережі.
Прийняття ризиків - утримання ризиків на рівні, що перебуває в межах визначеної Мережею схильності до ризиків та не створює загрози для інтересів донорів, партнерів, бенефіціарів, членів Мережі.
Ризик-координатор - керівник/призначені працівники Мережі, що є відповідальними за внутрішній контроль ризиків, які виникають у сфері їх компетенції та відповідають за виявлення та оцінювання ризиків, вжиття управлінських заходів та звітування щодо таких ризиків на всіх рівнях.
Стрес-сценарій - 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, але ймовірним подіям.
Уникнення ризику - припинення здійснення операцій, що з високою ймовірністю настання призводять до значних збитків.
Система управління операційним ризиком - сукупність належним чином задокументованих і затверджених політики, методик і процедур управління операційним ризиком, які визначають порядок дій, спрямованих на здійснення систематичного процесу виявлення,
вимірювання, моніторингу, контролю, звітування щодо операційних ризиків на всіх організаційних рівнях.

Юридичний ризик - ймовірність виникнення збитків або додаткових втрат (витрат) внаслідок неочікуваного застосування норм законодавства через можливість їх неоднозначного тлумачення або внаслідок визнання недійсними умов щодо їх невідповідності вимогам законодавства України.
Оцінка ризиків - визначення величини (рівня) ризиків за допомогою кількісних та якісних показників для формування мотивованого судження щодо рівня операційного ризику. Процес оцінки операційного ризику полягає в визначенні потенційних втрат (як фінансових, так і не фінансових), до яких може призвести реалізація операційного ризику.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про управління ризиками Громадської спілки "Мережа правового розвитку" (далі – Положення) є внутрішнім нормативним документом Мережі, що регламентує процес управління операційним та іншими ризиками, ідентифікації, оцінки, моніторингу та контролю за ризиками у Мережі.
1.2. Система управління операційним ризиком інтегрується в загальну систему управління ризиками Мережі.
1.3. Система управління операційним ризиком носить децентралізований характер, тобто в процес управління операційним ризиком задіяні всі підрозділи Мережі, органи Мережі, працівники, найняті особи.
1.4. Необхідність управління операційним ризиком визначається значним розміром можливих втрат (витрат) Мережі, пов'язаних з реалізацією подій операційного ризику, що створює загрозу фінансовій стабільності Мережі, іміджу і репутації.
1.5. Це Положення поширюється на членів Правління, Ревізійної комісії, Виконавчого директора, співробітників, підрядників, партнерів, стейкхолдерів, бенефіціарів, осіб, закріплених контрактами та третіх осіб, які співпрацюють із Мережею.

2. ІНДИКАТОРИ ОПЕРАЦІЙНОГО РИЗИКУ, ІДЕНТИФІКАТОРИ/ДЖЕРЕЛА/ФАКТОРИ РИЗИКУ

2.1. Класифікація операційних ризиків
Категорія

2.1.1. Персонал та робоче середовище/Управління персоналом та охорона праці
Характеристика категорії:

- збитки в результаті дій, які не відповідають законодавству в сфері охорони праці (виплати персоналу у зв'язку з виробничими травмами, втратою здоров'я;
- втрати, які виникають внаслідок дій, що суперечать укладеним кодексам, домовленостям (договорам) з працівниками, трудовому законодавству України, вимогам безпеки праці та протипожежної безпеки, а також відшкодування, виплачені за отримання виробничих травм;
- витрати, які виникають у результаті порушення взаємовідносин із працівниками, безпечного робочого середовища та дискримінації за різними ознаками.

2.1.2. Внутрішнє шахрайство.
Характеристика категорії:

- збитки в результаті дій шахрайства, незаконного привласнення майна або навмисного порушення норм законодавства, інших нормативно- правових актів або внутрішніх нормативних та/або організаційно- розпорядчих документів, здійснених працівниками чи найманими особами Мережі;
- втрати внаслідок умисних обманних дій, привласнення активів, ухилення від виконання/дотримання вимог законодавства України чи внутрішніх нормативних та/або організаційно- розпорядчих документів за участю працівників чи найманих осіб, несанкціоновані дії, крадіжка чи шахрайство.

2.1.3. Продукти і норми ділової практики /стандарти надання правничої допомоги
Характеристика категорії:

- збитки в результаті неумисного або недбалого відношення до професійних зобов'язань в результаті недосконалості продуктів чи надання послуг Мережею;
- втрати, що виникають внаслідок халатності чи помилок під час виконання професійних обов'язків з обслуговування та супроводу бенефіціарів
- ризики, що належать до цієї категорії, виникають внаслідок невиконання зобов'язань перед партнерами, бенефіциарами тощо.

2.1.4. Виконання операцій та управління процесами / Виконавча дисципліна, процесний менеджмент

Характеристика категорії:

- збитки в результаті розладу, збоїв або неналежного виконання контрагентами та постачальниками Мережі своїх зобов'язань;
- порушення у процесах діяльності і надання послуг;
- втрати, що виникають внаслідок помилок під час виконання операцій або управління процесами, а також помилок в управлінні відносинами з контрагентами та постачальниками.

2.1.5. Зовнішнє шахрайство.

Характеристика категорії:

- збитки в результаті шахрайства, незаконного привласнення майна або навмисного порушення норм законодавства, інших нормативно-правових актів або внутрішніх нормативних та/або організаційно-розпорядчих документів, здійснених третіми особами;
- втрати внаслідок умисних обманних дій, привласнення активів, ухилення від вимог законодавства України, що вчинені сторонніми для Мережі особами , розкрадання або шахрайство, здійснене третьою, зовнішньою щодо Мережі.

2.1.6. Пошкодження або знищення активів / Заподіяння шкоди фізичним активам / Стихійні лиха, безпека

Характеристика категорії:

- збитки в результаті пошкодження або знищення активів через природну катастрофу або інші події;
- втрати, що виникають внаслідок знищення або пошкодження активів через стихійні лиха або дії інших чинників.

2.2. Ця категорія охоплює ризики втрат у результаті: катастроф, тероризму, вандалізму, бойових дій та дій третіх осіб.

3. ФАКТОРИ ОПЕРАЦІЙНОГО РИЗИКУ

3.1. Для ідентифікації операційного ризику Мережа визначає основні джерела/ідентифікатори/фактори операційних ризиків, які можуть призвести до збитків, виникнення додаткових витрат або недоотримання запланованих доходів, а саме:

- персонал;
- організаційні процеси;
- наймані особи;
- інформаційні технології та безпека;
- зовнішні події.

3.2. Такі фактори є як зовнішніми, так і внутрішніми.

3.3. Мережа визначає наступні особливості операцій, що є потенційними джерелами/факторами операційного ризику:

- операції, які вимагають високої кваліфікації, залежать від окремих працівників, їх знань та кваліфікації;
- процеси проведення операцій не формалізовані і не прозорі, при проведенні операцій велику роль грають «експертні» оцінки і суб'єктивні дані;
- операції, що проводяться, є технологічно складні;
- результат операції залежить у великій мірі від ефективності роботи персоналу;
- персонал низького рівня (кваліфікація, посада тощо) при проведенні операцій володіє високими повноваженнями за визначенням характеру операцій (в залежності від виду операції/бізнес- процесу/продукту/послуги);
- ефективність і ризиковість операцій, що проводяться, не піддаються оцінці в поточному режимі.

4. УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ

4.1. Ефективне управління операційним ризиком є необхідним для досягнення основної місії Мережі, виконання законодавства України:

4.2. Ефективне управління операційним ризиком забезпечує наступні переваги для діяльності:

- зниження потенційних втрат (витрат);
- раннє виявлення неправомірної діяльності;
- зменшення впливу майбутніх операційних ризиків на діяльність;
- покращення ефективності виконання проектів.

4.3. Для зменшення операційного ризику Мережа використовує наступні основні заходи та процедури:

4.3.1. Оптимізація організаційної структури Мережі, систем внутрішнього контролю та моніторингу, внутрішніх правил та процедур здійснення статутної діяльності, банківських операцій, облікової політики, функціонування технічних, інформаційних та інших систем Мережі;

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

4.3.3. продуманий розподіл повноважень та підзвітності по організаційних процесах;

4.3.4. внутрішні контрольні процедури для мінімізації ризиків, документальний контроль тощо;

4.3.5. належне введення та регулярна звірка первинних документів та рахунків по банківських операціях;

4.3.6. виконання встановленого порядку доступу до інформації Мережі;

4.3.7. розвиток та автоматизація процесів, захист інформації;

4.3.8. вивчення системних помилок та здійснення заходів для подальшого їх усунення;

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

4.3.10. аналіз і усунення слабких місць та процесів, що підтримуються в постійно актуальному стані;

4.3.11. запровадження процедур раннього реагування на ймовірні операційні ризики, а саме визначення ключових індикаторів операційних ризиків та моделювання потенційних ризикових сценаріїв; аналіз стрес-тестування операційних ризиків;

4.3.12. постійний моніторинг та перегляд правил і процедур;

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

4.3.14. зменшення фінансових наслідків операційного ризику;

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

5. ЕТАПИ ПРОЦЕСУ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ

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

5.1. ВИЯВЛЕННЯ/ІДЕНТИФІКАЦІЯ ОПЕРАЦІЙНОГО РИЗИКУ.

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

5.1.2. В процесі виявлення операційних ризиків задіяні усі працівники Мережі, в межах сфер їх відповідальності.

5.1.3. В ході виявлення операційних ризиків працівники Мережі, в межах відповідальності своїх підрозділів повинні:

- виявляти загальні операційні ризики.
- забезпечити належне документування виявлених операційних ризиків, надавати звітність про інциденти операційних ризиків та вказувати виявлені операційні ризики в процесі здійснення подальшого внутрішнього контролю;
- на регулярній основі здійснювати перегляд виявлених операційних ризиків;
- надавати виконавчому директору інформацію про стан індикаторів раннього попередження операційного ризику

5.1.4. Виявлення операційних ризиків повинно охоплювати ризики, які виникають як в існуючих бізнес-процесах, продуктах/послугах та інформаційних системах, так і ризики, які виникають на етапі впровадження діяльності Мережі.

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

5.2.1. Для визначення процесу та критеріїв оцінки операційного ризику може розроблятися відповідна методика оцінки операційного ризику.

5.2.2. Оцінка проводиться для усіх процесів, господарської діяльності Мережі та усіх виявлених в ході попереднього аналізу операційних ризиків.

5.2.3. Оцінку операційних ризиків проводять уповноважені особи, в межах їх відповідальності.

5.2.4. Оцінка операційних ризиків включає:

- Оцінку можливих втрат;
- Оцінка ефективності чинних процедур;
- Оцінка рівня ризику в поточній діяльності.

5.2.5. В ході оцінки операційних ризиків працівники в межах відповідальності своїх підрозділів повинні:

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

5.2.6. Для оцінки операційних ризиків додатково можуть використовуватися:

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

5.2.7. Для оцінки операційних ризиків можуть розроблятися окремі методики.

5.2.8. У випадку необхідності план заходів мінімізації ризиків розробляється виконавчим директором та затверджується Правлінням Мережі.

5.2.9. План заходів мінімізації ризиків є обов’язковим до виконання.

5.2.10. План заходів мінімізації ризиків повинен обов’язково містити:

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

5.3. МОНІТОРИНГ ОПЕРАЦІЙНОГО РИЗИКУ.

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

5.3.2.Основними інструментами моніторингу операційних ризиків є:

- Визначення ключових індикаторів операційного ризику. Використовується для раннього виявлення негативних тенденцій/явищ, пов'язаних з підвищенням операційного ризику, що притаманні виробничим процесам.
- Аналіз результатів перевірок, здійснення внутрішнього аудиту та за необхідності, зовнішнього аудиту. Здійснюється аналіз щоквартальної інформації від з метою виявлення операційних ризиків.
- Створення та ведення бази внутрішніх подій операційного ризику за їх наявності.
- Самооцінка операційного ризику. У рамках самооцінки операційного ризику не рідше ніж один раз на рік проводиться аналіз бізнес-процесів з урахуванням інформації щодо можливих загроз і вразливостей та оцінюють можливі втрати від них, оцінюються ризики бізнес-процесів, ефективність контрольного середовища.

5.3.3. Сценарний аналіз. Цей інструмент застосовується шляхом формування судження щодо управління ризиками для визначення можливих малоймовірних подій операційного ризику з суттєвими наслідками для Мережі. Сценарний аналіз є методом стрес-тестування операційного ризику для різних короткострокових і довгострокових стрес-сценаріїв.

5.3.4. Для моніторингу операційних ризиків може створюватися база подій операційного ризику, яка ведеться виконавчим директором.

5.3.5. Виконавчий директор проводить ідентифікацію кожного виявленого операційного випадку та моніторингу операційних ризиків.

5.3.6. По всіх операційних випадках (інцидентах) встановлюються причини виникнення та

наслідки їх реалізації, а також, у разі необхідності (якщо випадок визначено як суттєвий), розробляється План заходів, який формалізує внесення змін у процес для недопущення реалізації подібних випадків у майбутньому.

5.4.УНИКНЕННЯ ОПЕРАЦІЙНИХ РИЗИКІВ

5.4.1. Мережа уникає операційних ризиків та може переносити відповідні операційні ризики на інші сторони, наприклад: страхувальників, постачальників, аутсорсерів.

5.4.2. У разі необхідності встановлення додаткових причин реалізації операційного ризику, або розробки Плану заходів для недопущення їх виникнення у майбутньому наказом виконавчого директора може бути створена окрема робоча група.

5.4.3. Процес контролю за операційним ризиком та реагування на нього полягає в прийнятті, ухиленні, перенесені або зменшенню рівня ризику:

- операційні ризики можуть бути прийняті, якщо вони не впливають на результати діяльності Мережі, або їх вплив не призводить до значних наслідків;
- зменшення операційних ризиків полягає у зменшенні рівня їх впливу на Мережу шляхом впроваджені контрольних процедур/додаткових контрольних механізмів або зменшення обсягів операційної діяльності;
- ухилення від ризиків може здійснюватися шляхом відмови від певного виду діяльності;
- перенесення операційного ризику може здійснюватись шляхом страхування наслідків його реалізації, аутсорсингу. Рішення про прийняття, ухилення, перенесення або зменшення (мінімізацію) рівня операційного ризику приймається Правлінням за пропозицією виконавчого директора.

5.4.4. Додатково, для мінімізації операційних ризиків, можуть використовуватися інші заходи, наприклад: перебудова організаційних процесів, автоматизація процесів тощо.

5.4.5. Суттєвим впливом на зменшення рівня операційних ризиків є можливість розроблення ефективного та цілісного комплексного Плану забезпечення безперервної діяльності, який включає:

- стратегічні цілі та пріоритети банку забезпечення безперервної діяльності в розрізі процесів Мережі;
- процедури та заходи реагування на випадки порушення безперервності діяльності;
- заходи відновлення діяльності для важливих процесів життєзабезпечення Мережі;
- заходи відновлення організаційних процесів.

5.4.6. Повідомити про порушення можна на електронну адресу office@ldn.org.ua чи у інший доступний спосіб.