



Міністерство
фінансів
України

Управління ризиками: рамкові основи та практичне застосування

Цілі установи



- ❑ **Стратегічні цілі** являють собою завдання вищого порядку, досягнення яких повинно сприяти меті діяльності установи. Керівництво визначає стратегічні цілі, формулює стратегію, після чого на їх основі розробляються операційні цілі.
- ❑ **Операційні цілі** – показники які розкривають стратегічні цілі на короткостроковий період, стосуються ефективності та результативності операційної діяльності установи, включаючи виконання завдань і захист ресурсів від втрат.

Кожна ціль (незалежно від рівня) може бути стартовою точкою для управління ризиками, оскільки як самі ризики, так і способи реагування на них напряду залежать від визначених цілей і змінюються у разі коригування цілей.





Ідентифікація ризиків неможлива без визначення стратегічних та операційних цілей!!!

Цілі повинні бути чітко визначені та відповідати критеріям SMART:

- | | | |
|----------|--|-------------------------------------|
| S | - <u>Конкретні</u> (англ. <i>specific</i>) | Що ви хочете зробити? |
| M | - <u>Вимірювані</u> (англ. <i>measurable</i>) | Як ви дізнаєтесь, що досягли цього? |
| A | - <u>Досяжні</u> (англ. <i>achievable</i>) | Чи у ваших силах це зробити? |
| R | - <u>Реалістичні</u> (англ. <i>realistic</i>) | Чи можете ви реально досягти цього? |
| T | - <u>Визначені у часі</u> (англ. <i>timely</i>) | Коли саме ви хочете цього досягти? |

Що таке ризик?



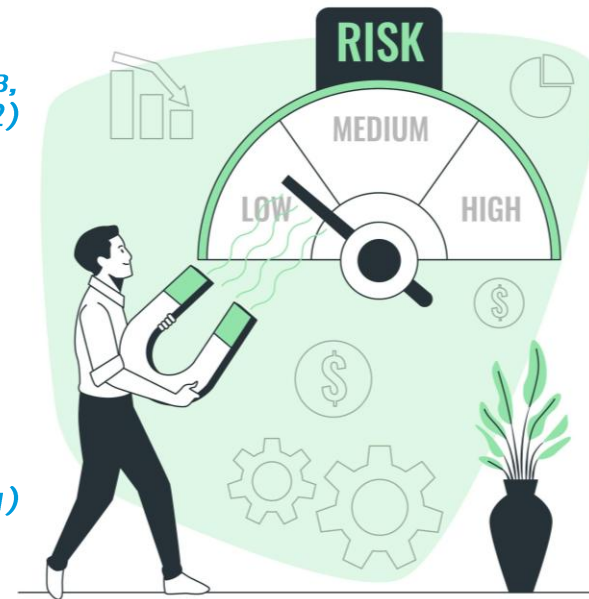
Ризик – можливість настання події, обставини або їх сукупність, що матиме вплив на здатність установи виконувати завдання і функції, цільове, ефективне управління бюджетними коштами, у тому числі такими, що спрямовуються на підготовку та реалізацію публічних інвестиційних проектів, об'єктами державної (комунальної) власності та іншими ресурсами, функціонування інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем, функціонування внутрішнього контролю та досягати визначених мети (місії), стратегічних та інших цілей діяльності установи, зокрема може спричинити або допустити виникнення відхилень, корупційних ризиків, шахрайства або зловживань службовим становищем

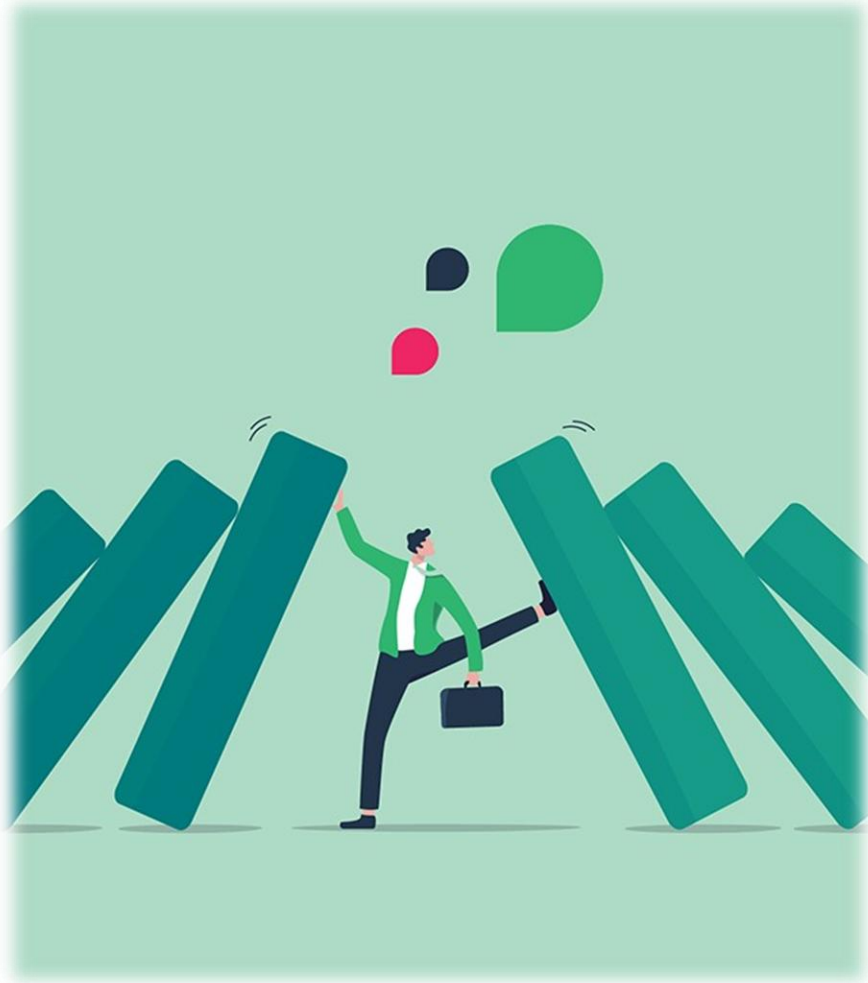
(Основні засади здійснення внутрішнього контролю розпорядниками бюджетних коштів, затверджені постановою Кабінету Міністрів України від 12.12.2018 № 1062)

Ризик – вплив невизначеності на цілі. Тобто це відхилення від того, що очікується. Цей вплив може бути позитивним та/або негативним, і може сприяти реалізації можливостей та усуненню загроз, створювати або призводити до виникнення можливостей і загроз

(ISO 31000:2018 – Управління ризиками)

Ризик – це не лише загроза, а нові можливості для установи.





Управління ризиками – діяльність керівництва та працівників установи з ідентифікації ризиків, проведення їх оцінки, визначення способів реагування на ідентифіковані та оцінені ризики, здійснення перегляду ідентифікованих та оцінених ризиків для виявлення нових та таких, що зазнали змін.

(Основні засади здійснення внутрішнього контролю розпорядниками бюджетних коштів, затверджені постановою Кабінету Міністрів України від 12.12.2018 № 1062)

Ідентифікація ризиків



Ідентифікація ризиків – визначення ризиків за категоріями (зовнішні та внутрішні) та видами (нормативно-правові, операційно-технологічні, програмно-технічні, фінансово-господарські тощо).

Тобто, Ідентифікація ризиків – визначення ймовірних подій, які негативно впливають/вплинуть на здатність установи виконувати визначені актами законодавства завдання і функції для досягнення мети та стратегічних цілей.



Визначаючи ризики, корисно задавати питання **«що може відбутися не так?»**

Ідентифікація ризиків



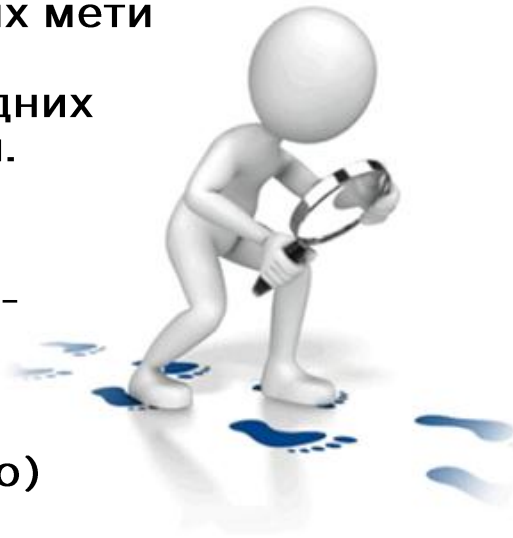
Ідентифікація ризиків передбачає їх визначення та класифікацію за категоріями:

Зовнішні

Події, які є зовнішніми по відношенню до установи та ймовірність виникнення яких не пов'язана з досягненням встановлених мети (місії), цілей та завдань, виконанням установою та її працівниками відповідних планів, функцій, процесів та операцій.

Причини виникнення:

- Обставини непереборної сили (форс-мажорні обставини)
- Природні явища
- Кібератаки (фішинг, DDoS-атаки тощо)



Внутрішні

Події, ймовірність виникнення яких пов'язана з безпосереднім досягненням встановлених мети (місії), цілей та завдань, виконанням установою та її працівниками відповідних планів, функцій, процесів та операцій.

Причини виникнення:

- Шахрайство
- Використання неперевіреного програмного забезпечення (ПЗ)
- Відвідування небажаних web-ресурсів
- Втрата електронного цифрового підпису (ЕЦП), паролю/логіну тощо

Ідентифікація ризиків



Ідентифікація ризиків передбачає їх визначення та класифікацію за видами:

нормативно-правові (законодавчі) – суперечність або нечітка регламентація виконання повноважень у відповідних нормативно-правових актах, що виникла із законодавчими змінами тощо;

операційно-технологічні – недотримання/порушення визначеного порядку виконання процесу, зокрема строків та формату подання документів, наявністю недоліків або помилок в установі відповідних внутрішніх процесів тощо;

кадрові – недостатність персоналу, його неналежна професійна підготовка та/або неналежне виконання посадових обов'язків тощо;

фінансово-господарські – пов'язані зі станом фінансово-господарської діяльності установи, матеріально-технічним забезпеченням тощо;

програмно-технічні – відсутність прикладного програмного забезпечення або його адаптації відповідно до вимог нормативно-правових актів, відсутність необхідних технічних засобів тощо;

репутаційні – дії або події, які можуть негативно вплинути на репутацію установи чи її керівництва;

корупційні – недоброчесність працівників, виникнення конфлікту інтересів, безконтрольність з боку керівництва, наявність дискреційних повноважень та інші чинники, які сприяють або не запобігають виникненню корупції.



Методи ідентифікації ризиків



Карта перевірки (чек-лист) - використання певного сформованого переліку питань, для перевірки стану виконання процесу

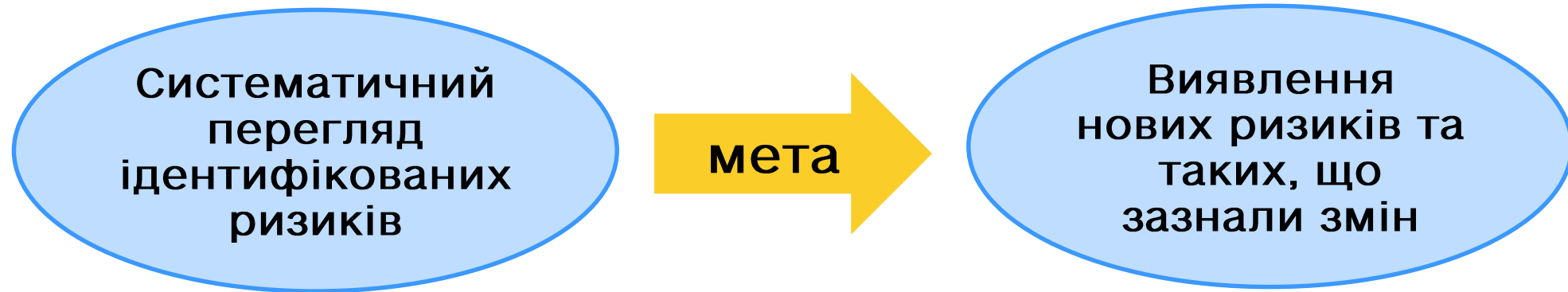
Аналіз блок-схем - послідовний аналіз виконуваного процесу, послідовність виконання якого відображено у графічний спосіб

Порівняння з еталонними критеріями (бенчмаркінг) - систематичний пошук і впровадження найкращих практик для покращення діяльності установи. Дієвий інструмент для порівняння стану функціонування установи з іншими, подібними за розмірами та/або сферою діяльності

Сценарне планування - дослідження зовнішнього середовища, що впливає на діяльність установи, для формулювання альтернативних сценаріїв майбутнього



Способи ідентифікації ризиків



Способи ідентифікації ризиків:

- "згори донизу" (на рівні структури установи);
- "знизу догори" (на рівні конкретних операцій/ділянок роботи)



Бажаним є поєднання цих двох методів, що забезпечує одночасне покриття установи в цілому та розподіл ризиків за різними напрямками/сферами її діяльності



Під час ідентифікації ризиків необхідно свідомо уникати:

- включення ризиків, які не впливають на досягнення цілей;
- включення наслідків/проблем/недоліків, які можна прийняти за ризики;
- зворотного формулювання цілей.

Ідентифікація ризиків - приклад



□ **Операційна ціль Установи X** – До кінця 2026 року населення має доступ до безкоштовних навчальних ресурсів, направлених на розвиток цифрових навичок.

Які ризики можуть вплинути на досягнення зазначеної операційної цілі?

Ідентифікація ризиків - приклад



Ідентифікація ризиків здійснюється у причинно-наслідковому зв'язку



Оцінка ризиків здійснюється за критеріями ймовірності виникнення ідентифікованих ризиків та суттєвості їх впливу на здатність установи виконувати визначені завдання та функції для досягнення нею мети та стратегічних цілей.



Оцінка ризиків здійснюється за критеріями:

Ймовірності – вірогідності, можливості виникнення того чи іншого ризику у певний проміжок часу

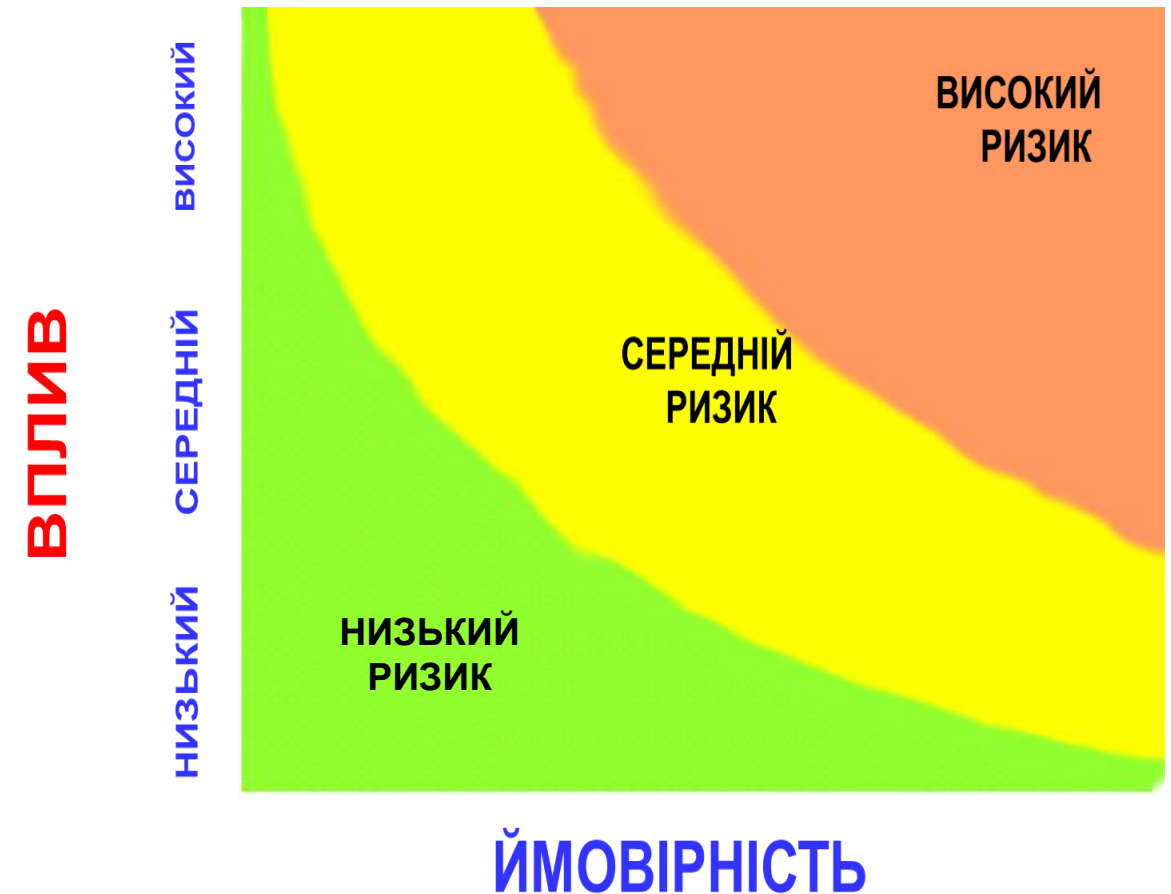
Впливу – суттєвості, із якою ризик може вплинути на спроможність установи досягати поставлених цілей

Матриця оцінки ризиків







Відповідно до критеріїв ймовірності виникнення та суттєвості впливу ризикам можуть присвоюватися такі значення:

- ✓ **ВИСОКИЙ**
- ✓ **середній**
- ✓ **НИЗЬКИЙ**



Способи реагування на ризики



-  • **Прийняття** – жодних дій відносно ризику не здійснюється
-  • **Зменшення** – вжиття тих заходів, які сприяють зменшенню або повному усуненню ймовірності виникнення ризиків та/або їх впливу
-  • **Розділення (передача)** – зменшити ймовірність або вплив ризику шляхом поділу цього ризику із іншими зацікавленими сторонами, або перенесення частини ризику
-  • **Уникнення** – призупинення (припинення) діяльності (функції, процесу, операції), що призводить до підвищення ризику

Залишкові ризики – ті, що залишаються після вжитих заходів щодо зменшення впливу ризиків, у тому числі після здійснення заходів контролю щодо ризиків.

Способи реагування на ризики



Під час прийняття рішення про спосіб реагування на ризик звертається увага на:

- Оцінку ймовірності та впливу ризику;
- Витрати, пов'язані з реагуванням на ризик, у порівнянні з отриманою вигодою від його зменшення;
- Те, чи не створює обраний спосіб реагування додаткових ризиків.



Ставлення установи до ризиків – **«ризиковий апетит»** (або апетит на ризики), стосується рівня ризиків, які установа готова прийняти, та ризиків, на які будуть розроблятися відповідні заходи.

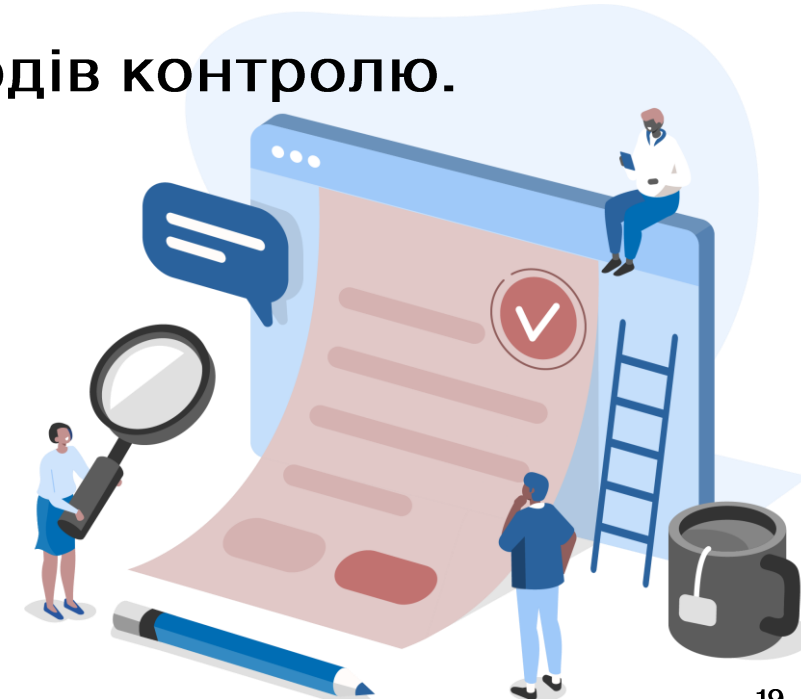
Визначення допустимого рівня ризику в установі є суб'єктивним процесом, однак залишається важливим аспектом діяльності управління ризиками.

Перегляд діяльності з управління ризиками доцільно здійснювати з метою:

- оцінки того, чи не змінилася структура ризиків;
- підтвердження ефективності управління ризиками;
- визначення необхідності подальших заходів контролю.



Перегляд має підтверджувати наявність необхідного контролю за функціями установи, а також усвідомленням і виконанням процедур



Інформаційні дані щодо ризиків



Основне призначення інформації щодо ризиків

– це доведення узагальнених результатів аналізу ризиків до керівництва з метою реагування, ухвалення відповідних рішень та вдосконалення процесів управління в установі

Для дієвості (практичної цінності) та забезпечення здійснення ефективного управління ризиками необхідно періодично переглядати зведену інформацію по ризиках



Роль внутрішнього аудиту



Внутрішній аудитор:

- проводить оцінку ефективності діяльності з управління ризиками та надає рекомендації керівнику щодо удосконалення зазначеної діяльності;
- бере до уваги систему управління ризиками, що функціонує в установі, під час планування діяльності з внутрішнього аудиту та при проведенні аудиторських досліджень.



Внутрішній аудитор **не несе відповідальність!!!** за заходи, що здійснюються керівником установи для організації внутрішнього контролю та забезпечення його функціонування в установі, розробку та впровадження заходів контролю з метою впливу на ризики.

Отже, при оцінці діяльності з управління ризиками внутрішні аудитори **повинні утримуватись** від прийняття на себе управлінських обов'язків, тобто від фактичного управління ризиками.

Рекомендації



Інтегрувати УР **у процеси планування** діяльності установи на усіх рівнях з метою встановлення досяжних пріоритетних цілей

Визначати **чіткі цілі**, що дозволяє точно ідентифікувати ризики та їх вплив на конкретний робочий процес

Ідентифікація ризиків має здійснюватися через визначення відповідних причин та наслідків **у чіткому причинно-наслідковому зв'язку**

Перед початком ідентифікації ризиків доцільно зрозуміти їх значення та вплив на конкретну ціль. Практичне формулювання ризиків забезпечить більш тісний зв'язок процесу управління ризиками із заходами контролю





Чи можна підготуватися до
всіх глобальних ризиків?

⇒ **НІ**



Неможливо бути готовим до всіх ризиків:
мати готові рішення питань від всього і
відразу.

АЛЕ, варто готуватись!

У разі виявлення ризиків, що будуть
впливати на діяльність установи,
потрібно розуміти як діяти і для чого.

**Це основа мінімізації їхніх негативних
наслідків.**