МІНІСТЕРСТВО
ФІНАНСІВ
УКРАЇНИ

Ідентифікація та оцінка ризиків, визначення способів реагування на них (третій – п`ятий елемент внутрішнього контролю за моделлю COSO)

тренінг з внутрішнього контролю та внутрішнього аудиту для внутрішніх аудиторів системи міністерств, інших центральних органів виконавчої влади

18 вересня 2017 року

МОДЕЛЬ COSO


Мета діяльності
Стратегічні цілі
Операційні цілі
Цілі звітування і відповідності
Внутрішнє середовище
Формулювання цілей
Ідентифікація ризиків
Оцінка ризиків
Способи реагування на ризики, управління ними
Механізми контролю (контрольні заходи)
Організація інформаційногота комунікаційного обміну
Здійснення моніторингу системи внутрішнього контролю та відслідковування результатів реалізації контрольних заходів
Організація
Структурний підрозділ
Функції
Процеси і операції

Ідентифікація ризиків (І)

Ризики – це потенційні події, поява яких може негативно вплинути на успішність реалізації стратегії діяльності установи та досягнення визначених установою цілей

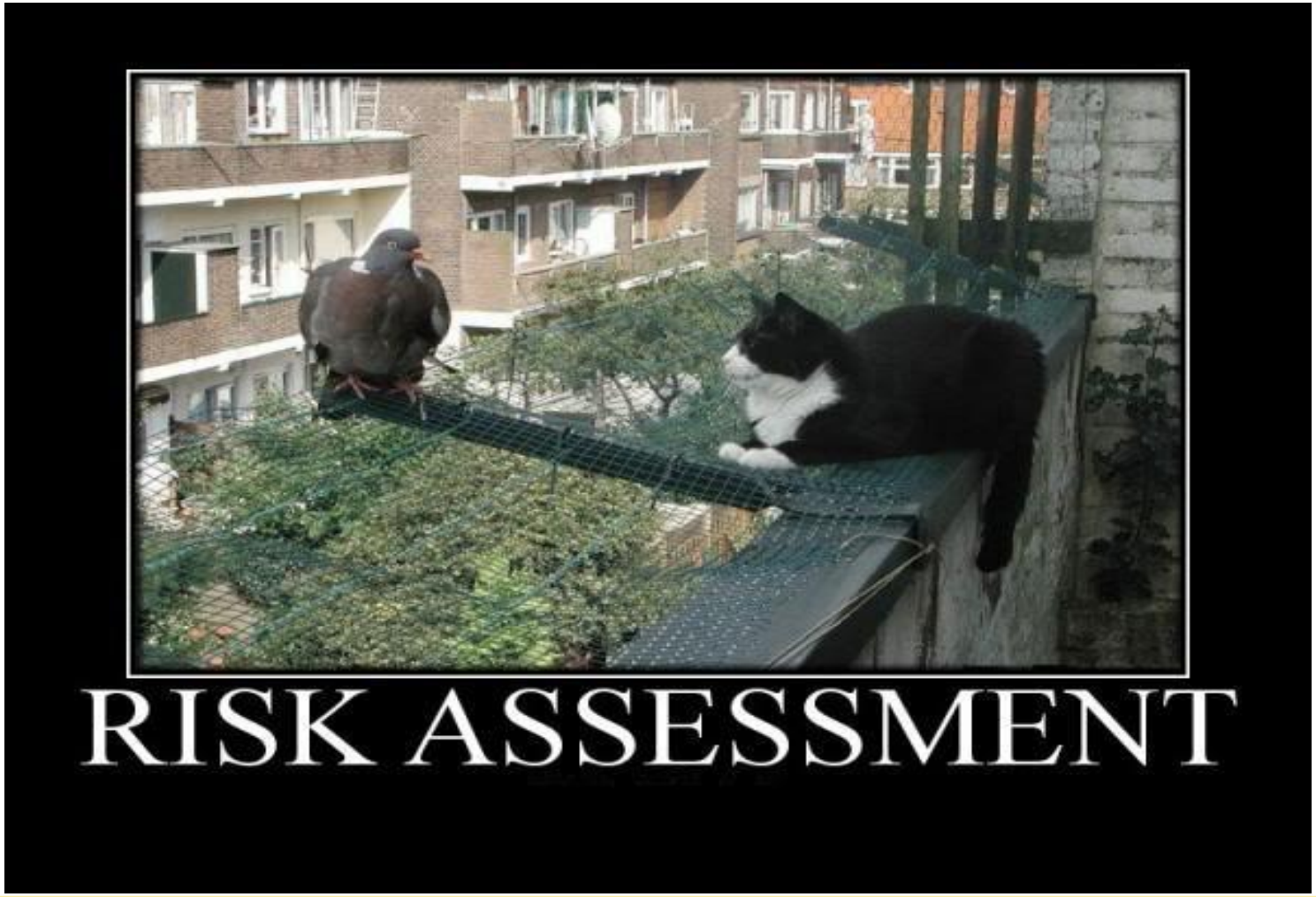
Новий погляд на ризики:
ризик – не лише загроза, а й **нові можливості**

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

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 (ІІ)

Ідентифікація ризиків передбачає визначення та класифікацію ризиків за категоріями та видами

За категоріями ризики можуть бути:

- **зовнішні** - це події, які є зовнішніми по відношенню до установи та ймовірність виникнення яких не пов’язана з виконанням структурними підрозділами установи процесів та операцій;
- **внутрішні** - це події, ймовірність виникнення яких безпосередньо пов’язана з виконанням структурними підрозділами та працівниками установи відповідних процесів та операцій

Ідентифікація ризиків (ІІІ)

Ризики поділяються на:

- ***законодавчі*** – ризики, ймовірність виникнення яких пов'язана із відсутністю, суперечністю або нечіткою регламентацію виконання операції у відповідних нормативно-правових актах, законодавчими змінами тощо;
- ***операційно-технологічні*** – ризики, ймовірність виникнення яких пов'язана із порушенням визначеного порядку виконання операції, зокрема термінів та формату подання документів, розподілу повноважень з виконання операції тощо;
- ***репутаційні*** – дії або події, які можуть негативно вплинути на репутацію установи чи її керівника;
- ***програмно-технічні*** – ризики, ймовірність виникнення яких пов'язана із відсутністю прикладного програмного забезпечення або змін до нього відповідно до діючої нормативно-правової бази, неналежною роботою або відсутністю необхідних технічних засобів тощо;
- ***кадрові*** – ризики, ймовірність виникнення яких пов'язана із неналежною професійною підготовкою працівників установи, неналежного виконання ними посадових інструкцій тощо;
- ***фінансово-господарські*** – ризики, ймовірність виникнення яких пов'язана із фінансово-господарським станом установи, зокрема, неналежним ресурсним, матеріальним забезпеченням тощо
- ***інші***

Ідентифікація ризиків (IV)

Ідентифікація ризиків
має здійснюватися у чіткому

причинно-наслідковому зв'язку

Основним повідомленням є –

усуньте подію, що призводить до цієї проблеми!!!

Ідентифікація ризиків (V)

Систематичний перегляд ідентифікованих ризиків здійснюється з метою виявлення нових та таких, що зазнали змін

Методи ідентифікації ризиків:

- ***"згори донизу" (на рівні 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 напрямами/сферами діяльності установи

Оцінка ризиків

Оцінювання ризиків – серйозна справа……

Оцінка ризиків (І)

Оцінка ризиків може здійснюватися за критеріями ймовірності виникнення ідентифікованих ризиків та суттєвості їх впливу на здатність установи виконувати визначені актами законодавства завдання і функції для досягнення нею мети та стратегічних цілей

Оцінка ризиків здійснюється за критеріями:

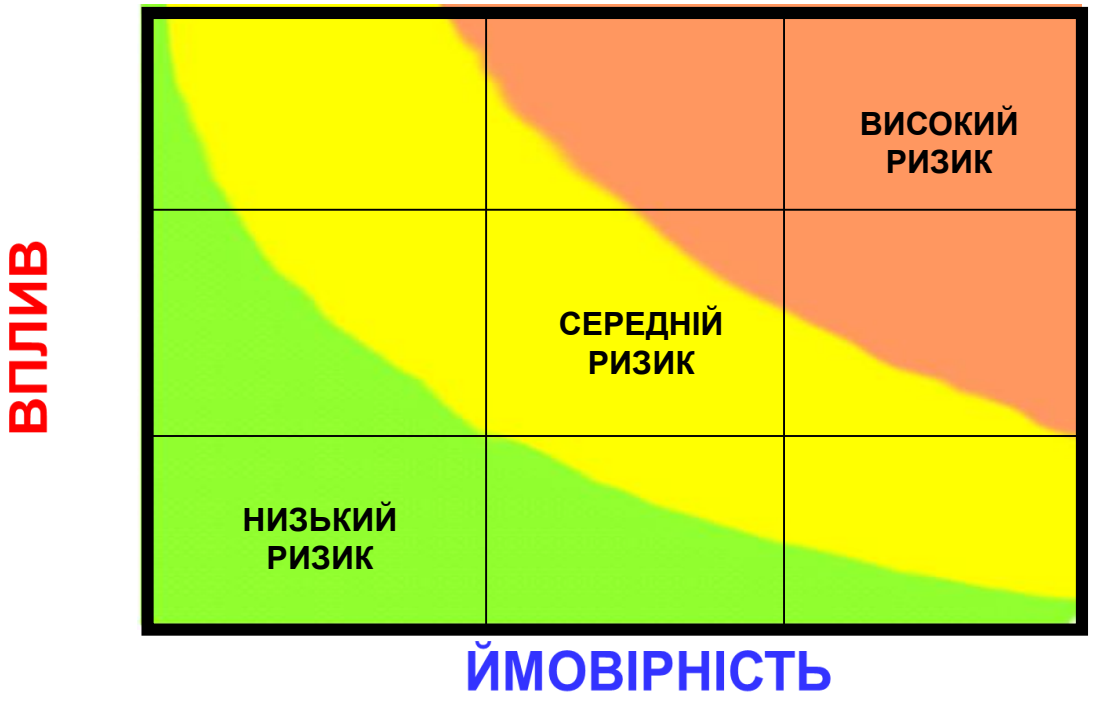
- ***ймовірності***, *що* означає вірогідність, можливість виникнення того чи іншого ризику у певний проміжок часу;
- ***впливу***, *який* представляє собою суттєвість із якою ризик може вплинути на спроможність установи досягати поставлені цілі

Оцінка ризиків (II)

Відповідно до критеріїв ймовірності виникнення та суттєвості їх впливу ризикам присвоюються значення:

- "високий"
- "середній"
- "низький"

МАТРИЦЯ РИЗИКІВ



Оцінка ризиків (ІІІ)

Керівництво установи інформується щодо сфер діяльності установи з "високою" ймовірністю виникнення ризиків та їх "високим" ступенем впливу (пріоритетні/ключові)

Рішення щодо способів реагування на ризики з меншою ймовірністю та ступенем впливу, а також вжиття заходів по їх зменшенню можуть прийматися керівниками структурних підрозділів установи в межах їх повноважень та компетенції з подальшим інформуванням керівництва установи про прийняті рішення у разі потреби

Способи реагування на ризики (І)

Визначення способів реагування на ризики полягає у прийняті рішення керівництвом установи щодо зменшення, прийняття, розділення чи уникнення ризику

Рішення щодо реагування на ризики приймаються разом із визначенням допустимого рівня ризику, який установа може прийняти, не вживаючи заходів контролю

Способи реагування на ризики (II)

Чотири способи реагування на ризики:

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

Залишкові ризики – це ризики, які залишаються після вжитих керівництвом установи заходів щодо зменшення впливу ризиків та ймовірності настання негативних подій, у тому числі після здійснення заходів контролю щодо ризиків

Способи реагування на ризики (III)

Важливим аспектом визначення форми реагування на ризик є ставлення установи до ризиків – **"ризиковий апетит"** (або апетит на ризики), який стосується рівня ризиків, які установа готова прийняти, та ризиків, на які будуть розроблятися відповідні заходи

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

Способи реагування на ризики (IV)

При прийнятті рішення щодо способу реагування на ризик звертається увага на:

- оцінку ймовірності та впливу ризику;
- витрати, пов’язані з реагуванням на ризик, порівняно з отриманою вигодою від його зменшення;
- те, чи не створює обраний спосіб реагування на ризик додаткових ризиків

Приклад управління ризиками

(для підрозділу внутрішнього аудиту)

Ціль – збільшити питому вагу впроваджених рекомендацій до 75 % від їх загальної кількості станом на 31.12.2017

Ризик 1 – неякісне здійснення моніторингу внаслідок відсутності регламенту (за категорією ризик внутрішній, за видом – нормативно-правовий, ймовірність – висока, вплив – високий, загальна оцінка – висока);

Ризик 2 – недотримання затвердженого порядку здійснення моніторингу (за категорією ризик внутрішній, за видом – операційно-технологічний, ймовірність – низька, вплив – високий, загальна оцінка ризику – середній);

Ризик 3 – неможливість впровадження рекомендацій внаслідок їх неналежної якості (за категорією ризик внутрішній, за видом – кадровий, ймовірність – середній, вплив – середній, загальна оцінка ризику – середній)

Спосіб реагування – зменшити

Документування діяльності з управління ризиками (І)

Керівник визначає відповідальних за забезпечення:

- документування ризиків та способів реагування на них;
- визначення та провадження на практиці ефективних способів реагування на ризики;
- перегляд на регулярній основі оцінки ризиків і врахування відповідних змін та обставин

Документування діяльності з управління ризиками (II)

Установа самостійно розробляє форми документів, у яких відображається діяльність щодо управління ризиками

Складання і затвердження плану заходів щодо управління ризиками у вигляді таблиці (матриці) щодо:

- класифікованих та оцінених за критеріями ймовірності та впливу ризиків (визначених для конкретних функцій),

- заходів контролю по зменшенню ризиків (із зазначенням відповідальних виконавців, термінів та індикаторів (показників) виконання таких заходів)

Роль внутрішнього аудиту при оцінці елементу внутрішнього контролю – управління ризиками (І)

У тих випадках, коли діяльність з управління ризиками в установі вже існує, внутрішньому аудитору залишається:

- дослідити наявність внутрішніх документів з управління ризиками, їх дотримання, своєчасність надання керівництву та працівникам установи інформації з питань управління ризиками;
- проаналізувати реєстр ризиків для формування власного бачення щодо повноти переліку ідентифікованих ризиків та об’єктивність їх оцінки;

Роль внутрішнього аудиту при оцінці елементу внутрішнього контролю – управління ризиками (II)

- зрозуміти «апетит на ризик» керівництва та оцінити заходи контролю, запроваджені для реагування на відповідні ризики;
- проаналізувати ефективність запроваджених заходів контролю та оцінити залишкові ризики;
- визначити ризики найвищого пріоритету з урахуванням остаточної оцінки залишкових ризиків

Роль внутрішнього аудиту при оцінці елементу внутрішнього контролю – управління ризиками (ІІІ)

У тих випадках, коли діяльність з управління ризиками в установі відсутня внутрішньому аудиту доведеться самостійно визначати та оцінювати ризики

Працівник підрозділу внутрішнього аудиту застосовує власне судження про ризики в діяльності установи після консультацій, проведених з керівництвом та посадовими особами установи, які безпосередньо відповідають за функції, процеси, що охоплюються внутрішнім аудитом

Під час самостійної оцінки ризиків корисно врахувати позицію керівництва та посадових осіб установи, які безпосередньо відповідають за функції, процеси

Роль внутрішнього аудиту при оцінці елементу внутрішнього контролю – управління ризиками (IV)

Внутрішній аудитор <u>не несе відповідальність!!!</u> за заходи, що здійснюються керівником установи для забезпечення створення та функціонування системи внутрішнього контролю, розробку та впровадження контрольних процедур, заходів контролю з метою впливу на ризики

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

МІНІСТЕРСТВО
ФІНАНСІВ
УКРАЇНИ

Заходи контролю (шостий елемент внутрішнього контролю за моделлю COSO)

тренінг з внутрішнього контролю та внутрішнього аудиту для внутрішніх аудиторів системи міністерств, інших центральних органів виконавчої влади

19 вересня 2017 року

Модель COSO


Мета діяльності
Стратегічні цілі
Операційні цілі
Цілі звітування і відповідності
Внутрішнє середовище
Формулювання цілей
Ідентифікація ризиків
Оцінка ризиків
Способи реагування на ризики, управління ними
Механізми контролю (контрольні заходи)
Організація інформаційногота комунікаційного обміну
Здійснення моніторингу системи внутрішнього контролю та відслідковування результатів реалізації контрольних заходів
Організація
Структурний підрозділ
Функції
Процеси і операції

Заходи контролю

Заходи контролю

Заходи контролю

Заходи контролю –

сукупність запроваджених в установі управлінських дій, які здійснюються керівництвом усіх рівнів та працівниками для впливу на ризики з метою досягнення мети та стратегічних цілей установи

Заходи контролю здійснюються на всіх рівнях діяльності установи та щодо усіх функцій і завдань та включають відповідні правила і процедури

Заходи контролю

Для того, щоб бути ефективними, заходи контролю

повинні бути:

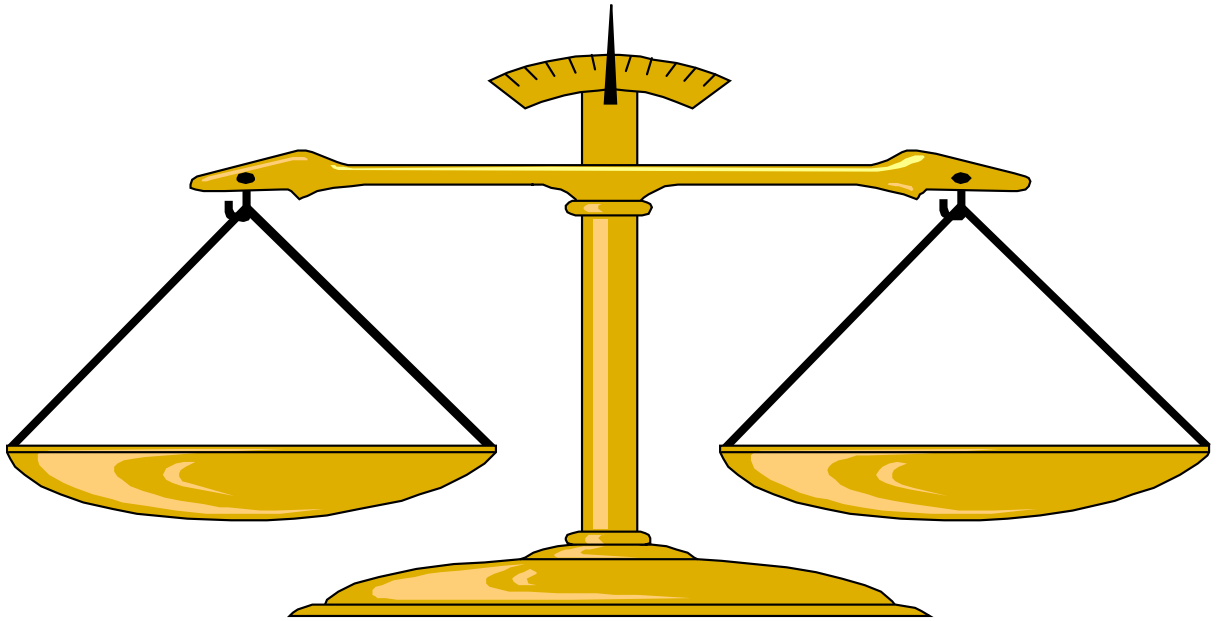
- Доцільними;
- Послідовними та періодичними;
- Економними;
- Повними, обґрунтованими та безпосередньо стосуватись цілей діяльності установи

Заходи контролю

Заходи контролю

Висока свідомість контролю функцій

Ризик



Вартість

Користь

Вартість на внутрішній контроль не повинна перевищувати користь від нього

Види заходів контролю

Централізований контроль

Попереджувальний контроль

Виявляючий контроль

Коригуючий контроль

Типові заходи контролю (І)

(1) авторизація та підтвердження здійснюється шляхом отримання дозволу відповідальних осіб на виконання операцій через процедуру візування, погодження та затвердження

(2) розподіл обов'язків та повноважень, ротація персоналу, що зменшує кількість ризиків помилок чи втрат;

(3) контроль за доступом до ресурсів та облікових записів, а також закріплення відповідальності за збереження і використання ресурсів, що зменшує ризик їх втрати чи неправильного використання;

(4) контроль за достовірністю проведених операцій, перевірка процесів та операцій до та після їх проведення, звірка облікових даних з фактичними;

Типові заходи контролю (II)

(5) оцінка загальних результатів діяльності установи, окремих функцій та завдань шляхом оцінювання їх ходу та результатів на предмет ефективності та результативності, відповідності нормативно-правовим актам та внутрішнім регламентам, правилам та процедурам установи;

(6) систематичний перегляд роботи кожного працівника установи (нагляд);

(7) інші правила та процедури, в тому числі визначені регламентом установи, внутрішніми документами про систему контролю за виконанням документів, правила внутрішнього трудового розпорядку працівників установи тощо

Заходи контролю

Більшість заходів контролю здійснюється відповідно до законодавства (наприклад, інвентаризації, подвійний підпис на фінансових документах, правова та антикорупційна експертиза, перевірки якості товарів, робіт та послуг, контроль виконавської дисципліни тощо)

Решта заходів контролю, залежно від обраних способів реагування на ризики, запроваджується керівником установи

Здійснення заходів контролю має бути підтверджено документально і в подальшому досліджується під час проведення внутрішніх аудитів

Документування заходів контролю

Формування карти ризиків - кінцевий результат даного етапу побудови системи внутрішнього контролю

До карти ризиків заносяться:

- заходи контролю;
- відповідальні виконавці;
- терміни виконання;
- очікувані результати від реалізації заходів контролю;
- тощо (перелік може бути розширений відповідно до організаційних вимог та специфіки діяльності установи)

МІНІСТЕРСТВО
ФІНАНСІВ
УКРАЇНИ

Інформація та комунікація (сьомий елемент внутрішнього контролю за моделлю COSO)

тренінг з внутрішнього контролю та внутрішнього аудиту для внутрішніх аудиторів системи міністерств, інших центральних органів виконавчої влади

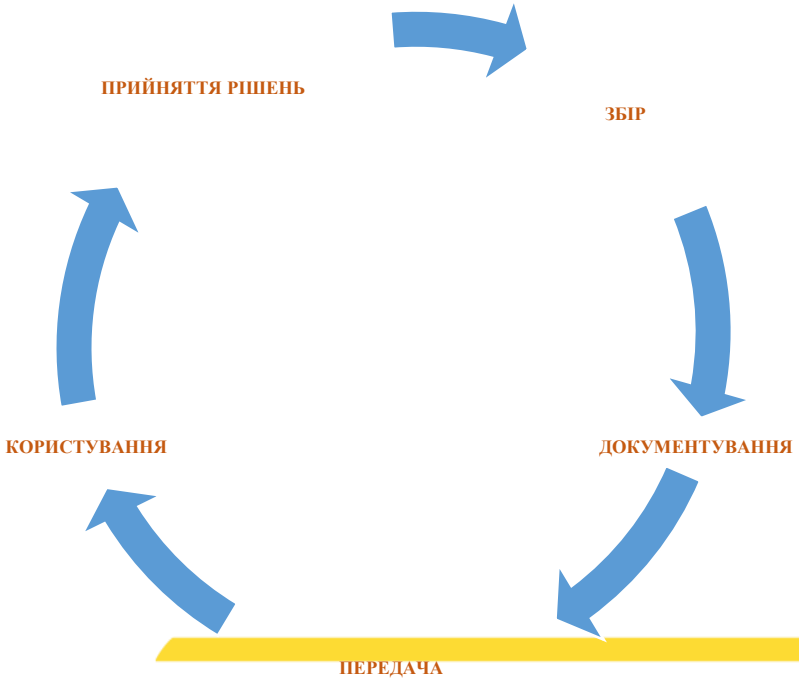
19 вересня 2017 року

Модель COSO


Мета діяльності
Стратегічні цілі
Операційні цілі
Цілі звітування і відповідності
Внутрішнє середовище
Формулювання цілей
Ідентифікація ризиків
Оцінка ризиків
Способи реагування на ризики, управління ними
Механізми контролю (контрольні заходи)
Організація інформаційногота комунікаційного обміну
Здійснення моніторингу системи внутрішнього контролю та відслідковування результатів реалізації контрольних заходів
Організація
Структурний підрозділ
Функції
Процеси і операції

Інформація та комунікація

Інформаційний та комунікаційний обмін в установі передбачає збір, документування, передачу інформації та користування нею керівництвом та працівниками установи для належного виконання і оцінювання функцій та завдань



Інформація та комунікація

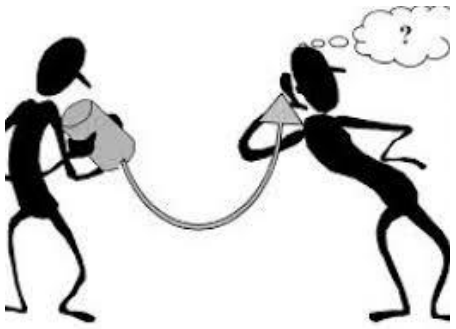
Інформація, що повинна бути:

- Доцільною (чи наявна необхідна інформація?);
- Своєчасною (чи є вона тоді, коли необхідна?);
- Актуальною (чи є це остання інформація?);
- Чіткою (чи є вона вірною?);
- Доступною (чи можуть відповідні учасники процесу її легко отримати?)

Інформація та комунікація

(1) Інформація необхідна для виконання зобов'язань
- Інформація **від** Керівництва і **для** Керівництва

(2) Необхідний результативний обмін інформацією
- Більше ніж потоки інформації
- Основне – це розуміння повідомлення



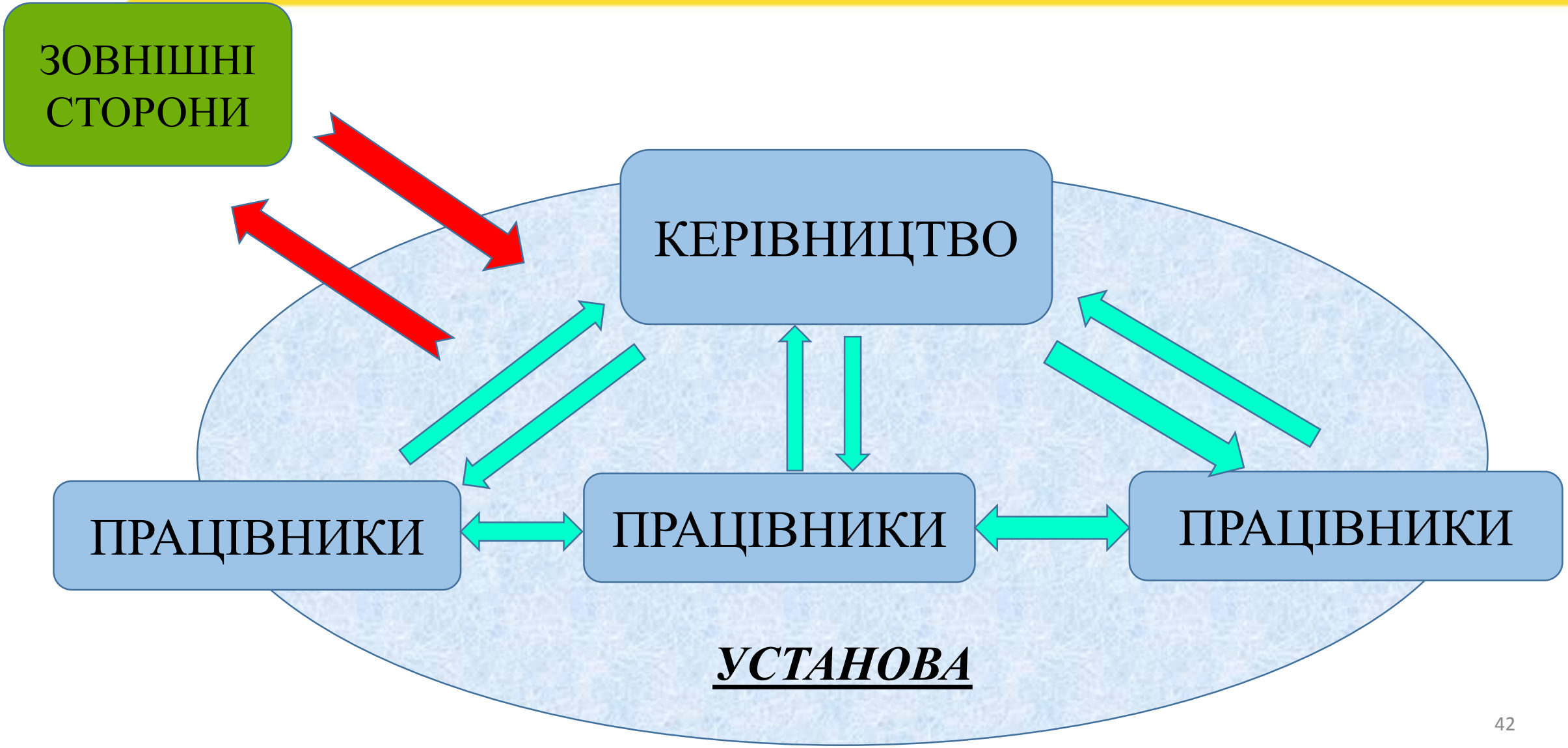
Інформація та комунікація

- Ключові елементи – **система повинна**
  - Ідентифікувати
  - Фіксувати
  - Опрацьовувати
  - Передавати

- Інформація базується на
  - Внутрішніх та зовнішніх джерелах
  - Операційна інформація розробляє фінансову інформацію

Керівництво визначає, фіксує та доносить відповідну інформацію у формі та у відповідний час, що дозволяє персоналу виконувати покладені обов'язки

Інформація та комунікація



Інформація та комунікація

Ефективному виконанню завдань і функцій (з метою досягнення мети та цілей) **сприяють:**

- ❖ налагодження інформаційного та комунікаційного обміну із зовнішніми сторонами;
- ❖ оприлюднення інформації про діяльність

Документування інформації та комунікація

Систему інформаційного та комунікаційного обміну формують:

- **порядки обміну інформацією**, що містять процедури, форми, обсяги, терміни, перелік надавачів та отримувачів інформації (наприклад, регламенти щодо доступу до публічної інформації);
- **графіки документообігу;**
- **графіки складання і подання звітності;**
- **схеми інформаційних потоків;**
- **комп'ютеризовані інформаційно-аналітичні системи тощо**

МІНІСТЕРСТВО
ФІНАНСІВ
УКРАЇНИ

Моніторинг (восьмий елемент внутрішнього контролю за моделлю COSO)

тренінг з внутрішнього контролю та внутрішнього аудиту для внутрішніх аудиторів системи міністерств, інших центральних органів виконавчої влади

19 вересня 2017 року

Модель COSO

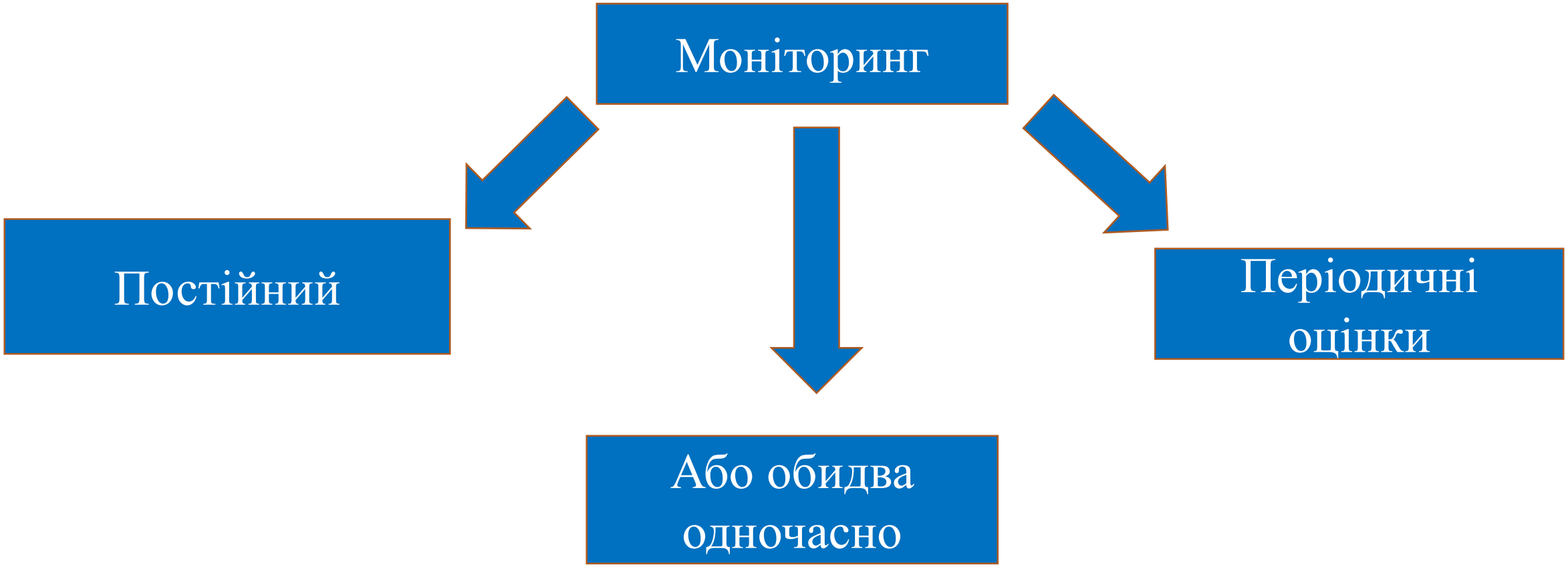

Мета діяльності
Стратегічні цілі
Операційні цілі
Цілі звітування і відповідності
Внутрішнє середовище
Формулювання цілей
Ідентифікація ризиків
Оцінка ризиків
Способи реагування на ризики, управління ними
Механізми контролю (контрольні заходи)
Організація інформаційногота комунікаційного обміну
Здійснення моніторингу системи внутрішнього контролю та відслідковування результатів реалізації контрольних заходів
Організація
Структурний підрозділ
Функції
Процеси і операції

Моніторинг

Моніторинг – це постійний процес проведення оцінки якості функціонування системи внутрішнього контролю у часі

Моніторинг повинен забезпечити адекватне та невідкладне запровадження рекомендацій і пропозицій для усунення наявних та попередження можливих недоліків системи внутрішнього контролю

Моніторинг


Моніторинг
Постійний
Або обидва одночасно
Періодичні оцінки

Моніторинг

Постійний моніторинг

здійснюється у ході щоденної/поточної діяльності установи та передбачає управлінські, наглядові та інші дії керівників усіх рівнів та працівників установи при виконанні ними своїх обов'язків з метою визначення та коригування відхилень

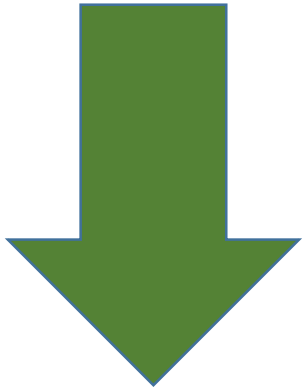
Моніторинг

Періодичні оцінки

передбачають проведення оцінки виконання окремих функцій, завдань на періодичній основі та здійснюються працівниками, які не несуть відповідальності за їх реалізацію, та/або підрозділом внутрішнього аудиту установи для більш об'єктивного аналізу результативності системи внутрішнього контролю

Моніторинг

Функція ВА



може відігравати
роль моніторингу

Моніторинг

Керівник установи повинен:

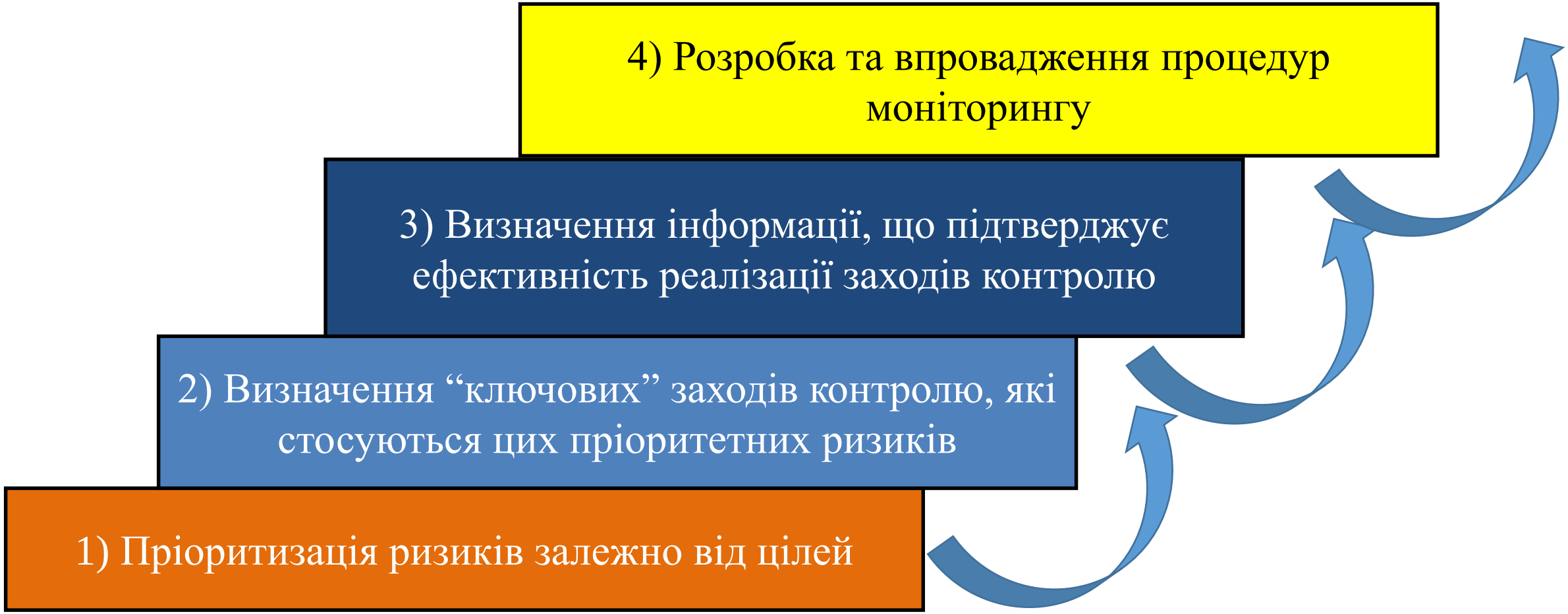
- брати до уваги та оцінювати знахідки аудитів та інших перевірок, включаючи ті, що виявляють недоліки;

- адекватно реагувати на знахідки та рекомендації;

- своєчасно вживати заходи, що коригують порушені аудиторами питання

Моніторинг

Кроки для запровадження ефективної системи моніторингу в установі



Процес документування внутрішнього контролю в установі

- структура установи, правові підстави її діяльності, внутрішні нормативно-правові акти;
- мета та основні стратегічні і операційні цілі установи;
- стратегічний план діяльності установи на період 3 – 5 років;
- для кожної діяльності/функції перелік процесів, операцій, блок-схем і описів процесів);
- визначені ризики, їх оцінка та запропоновані способи управління ними;
- опис заходів контролю та відповідальних за кожен захід осіб;
- ризики, що залишилися після запровадження заходів контролю;
- опис системи відслідковування результатів реалізації заходів контролю

Критичні фактори успіху

- Чіткі цілі;
- Достатні знання та досвід у роботі із управлінням ризиками, внутрішній контроль;
- Зовнішні рушійні сили;
- Достатні можливості;
- Відповідність вже використовуваним (планування та контроль) методам;
- Існування інструментів та допоміжних можливостей.

ТА…. Позитивні, стимулюючі дії керівництва.