Ministry of Finance

УПРАВЛІННЯ РИЗИКАМИ

Застосування моделей та технік Управління Ризиками (COSO, ISO, COBID тощо), а також їх практичне впровадження *(сесії із управління ризиками, роль ВА тощо)*

Руслана Рудніцька

Київ, 1-2 березня, 2023

Структура теми:

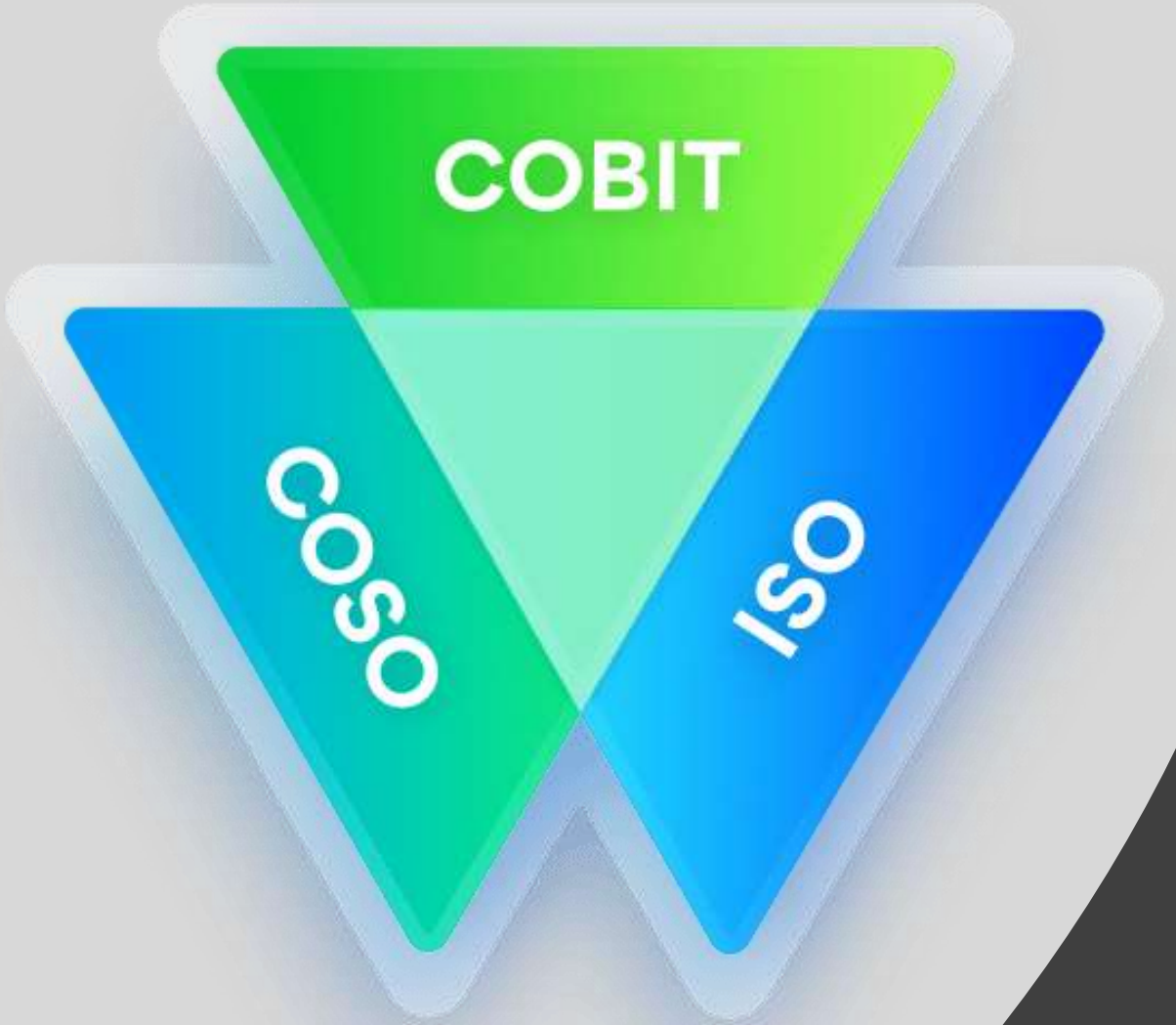
- Модель COSO та її особливості
- Стандарти ISO та їх застосування
- Стандарти COBIT, їх доцільність для різних зацікавлених сторін
- Роль та місце BA в процесах розбудови системи управління ризиками в установі

Управління ризиками

Метою управління ризиками є забезпечення того, щоб невизначеність ніколи не відволікала зусилля від досягнення встановлених цілей.

УР - це процес, який включає ідентифікацію, оцінку та встановлення пріоритетів ризику для контролю ймовірності впливу.

Тепер, коли ви знаєте теорію управління ризиками, наступне запитання, яке слід поставити: «Які існують **моделі та техніки** управління ризиками?»



Найбільш поширені моделі організації системи контролю

- **Керівництво використовує ту чи іншу модель розбудови системи контролю, залежно від призначення та потреби в організації системи управління ризиками**

Модель COSO

- **Модель COSO** є одним із найбільш поширених підходів до управління ризиками, який використовується організаціями державного сектору для допомоги в управлінні ризиками
- **Модель COSO** описує процес управління ризиками та надає покрокову інструкцію з визначення, оцінки та управління ризиками.
- **Модель COSO** – інструмент керівника, який він може застосовувати на стратегічному, операційному, програмному, процесному або проектному рівнях.

Складові Моделі COSO

Середовище контролю	1. Демонструє відданість чесності та етичним цінностям 2. Здійснює нагляд за відповідальністю 3. Встановлює структуру, повноваження та відповідальність 4. Демонструє прагнення до компетентності 5. Забезпечує відповідальність
Оцінка ризиків	6. Визначає відповідні цілі 7. Визначає та аналізує ризики 8. Оцінює ризик шахрайства 9. Визначає та аналізує значні зміни
Заходи контролю	10. Добирає та розробляє контрольні заходи 11. Вибирає та розробляє загальні контрольні заходи над технологіями 12. Здійснює вплив за допомогою політик і процедур
Інформація та комунікація	13. Використовує актуальну інформацію 14. Спілкується внутрі організації 15. Комунікує назовні
Заходи моніторингу	16. Проводить поточні та/або окремі оцінки 17. Оцінює та повідомляє про недоліки

Практичне застосування Моделі COSO

- Модель COSO може бути використана як основа:

- для підготовки внутрішнього нормативно-розпорядчого документу (наприклад, Методики оцінки ризиків в установі);
- для пілотування діяльності/заходів із управління ризиками;
- для аналізу та оцінки стану внутрішнього контролю та управління ризиками в установі.

Оцінка ризиків може проводитися на різних рівнях організації:

-Оцінка стратегічного ризику: стратегічні сесії із оцінки ризиків, пов'язаних із місією та стратегічними цілями організації;

- Оцінка операційного ризику: стратегічні сесії із оцінки ризиків

на операційному рівні (включаючи ризики для фінансових результатів і стану).

!!!Державним організаціям рекомендується використовувати підхід до управління ризиками «зверху вниз»!!!

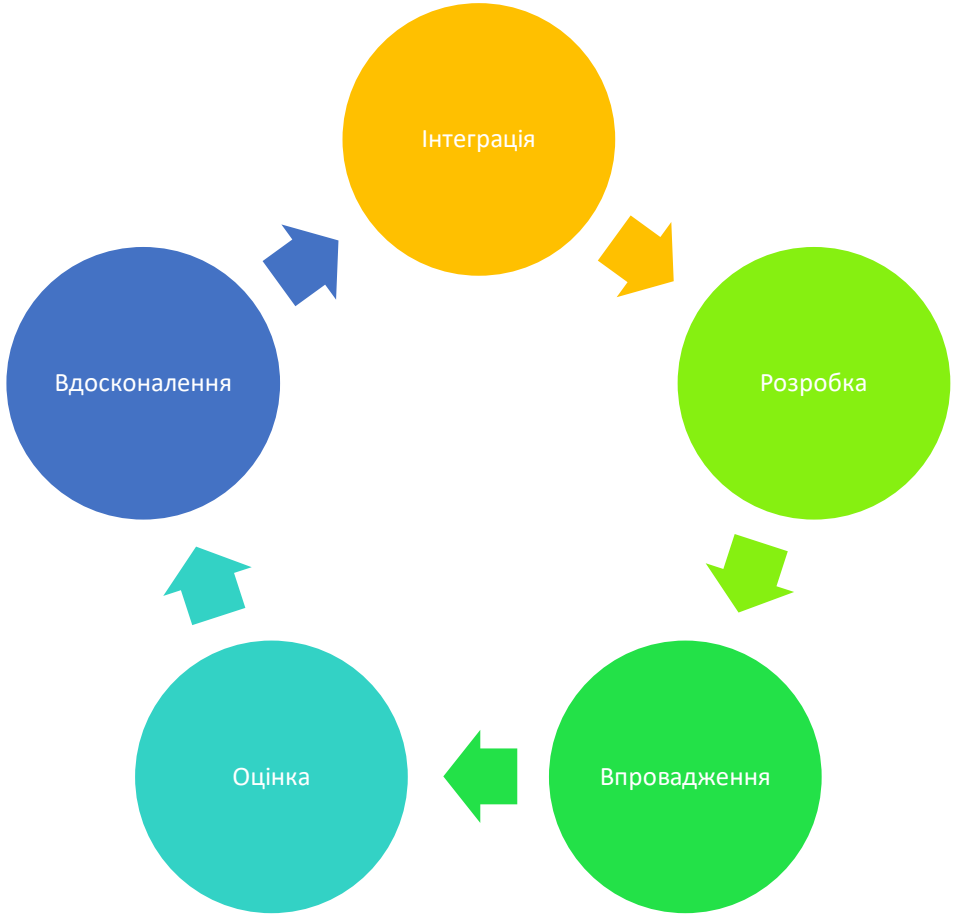
Стандарт з Управління Ризиками ISO 31 000 (1)

- ISO 31000 це міжнародний стандарт, який містить принципи та вказівки щодо ефективного управління ризиками;
- Стандарт є універсальним для будь-якого типу організацій, галузі чи сектору та призначений для задоволення потреб організації, не залежно від її розмірів;
- ISO 31000 Управління ризиками містить 11 принципів та загальні керівні вказівки щодо ефективного виявлення та управління ризиками, тобто, зовнішніми та внутрішніми факторами та впливами, які вносять невизначеність у досягнення цілей організації.

Стандарт з Управління Ризиками ISO 31 000 (2)

- Управління ризиками створює цінність
- **Управління ризиками є невід'ємною частиною бізнес-процесів**
- **Управління ризиками є частиною процесу прийняття рішень**
- Управління ризиками чітко визначає небезпеку
- **Управління ризиками систематично, структуровано і запрограмовано**
- Управління ризиками базується на найкращій доступній інформації
- **Управління ризиками, адаптоване**
- Управління ризиками розглядає людські та культурні фактори
- Управління ризиками є прозорим і всеохоплюючим
- Управління ризиками є динамічним, повторюваним і чутливим до змін
- Управління ризиками сприяє постійному вдосконаленню

Загальною метою системи ISO 31000 є розробка культури управління ризиками, в якій співробітники та зацікавлені сторони усвідомлюють важливість моніторингу та управління ризиками.



Стандарти COBIT

COBIT - це скорочення від Control Objectives for Information and Related Technology («Завдання інформаційних і суміжних технологій»);

COBIT - це пакет документів, близько 40 міжнародних і національних стандартів та настанов в області управління IT, аудиту та IT-безпеки;

COBIT є інструментарієм, який дозволяє керівникам підприємств усунути недоліки системи управління з урахуванням вимог контролю та бізнес-ризиків, а також продемонструвати рівень контролю зацікавленим сторонам;

COBIT, завдяки єдиній термінології, служить своєрідною платформою-буфером для конструктивного діалогу між усіма учасниками бізнесу: вищим керівництвом, керівниками середньої ланки (IT-директором, начальниками відділів), безпосередніми виконавцями (інженерами, програмістами і т. Д.), аудиторами.

Цільова аудиторія COBIT

Користувачі	Використання COBIT
Вище керівництво	Для контролю віддачі від інвестицій в IT, врівноваження ризиків і управління інвестиціями в сфері IT
Керівництво середньої організації	Для впевненості в належному управлінні і контролі над IT процесами
IT-менеджмент	Для надання IT послуг, необхідних департаментам/підрозділам і реалізації єдиної «організаційної стратегії» в контрольованих і керованих умовах
Аудитори	Для обгрунтування своїх висновків і / або консультування керівництва з питань внутрішнього контролю

Роль внутрішнього аудиту (ВА)

- З одного боку, ВА використовує результати процесу оцінки ризиків керівництва як вхідні дані для своїх планів і роботи, з іншого боку, ВА проводить власний незалежний аналіз ризиків.
- ВА також як і керівництво органу/установи може використовувати кожну із цих моделей/стандартів, залежно від мети аудиту

Роль та місце ВА в процесі управління ризиками

Внутрішній аудит (ВА) забезпечує об’єктивну оцінку відповідності та ефективності процесів контролю для вищого керівництва шляхом застосування систематичного професійного підходу до оцінки та надання рекомендацій.

ВА може виконувати консультативну/дорадчу роль у розвитку УР в установі:

- Допомога у ідентифікації та оцінці ризиків;

- Навчання керівництва з питань УР;

- Координація діяльності з управління ризиками (на початкових етапах);

- Надання рекомендацій (за результатами аудитів) щодо розвитку системи УР;

- Стимулювання створення системи УР;

- Розробка стратегії УР.