ТЕМА 9

СТАНДАРТИ ОРГАНІЗАЦІЇ РИЗИК-МЕНЕДЖМЕНТУ ПІДПРИЄМСТВ

https://images.app.goo.gl/RHLbxvoALv2XnpLn9

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM.

9.2. Основні положення ISO 31000:2018.

9.3. Основні положення COSO ERM.

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM

СІМЕЙСТВО СТАНДАРТІВ ISO 31000 УПРАВЛІННЯ РИЗИКОМ [1]

Сімейство стандартів ISO 31000 розроблено Технічним комітетом №262 «Менеджмент ризику» Міжнародної організації зі стандартизації (ISO)*

У лютому 2018 року вийшла нова версія стандарту (друге видання).

Сімейство охоплює стандарти:

ISO 31000:2018 Управління ризиками – Керівництво (доступно англійською та російською мовами);

ISO 31010:2019 Risk management – Risk assessment techniques (доступно лише англійською мовою).

Українським аналогом ISO 31010 є ДСТУ 31010:2013 Керування ризиком. Методи загального оцінювання ризиків.

* Міжнародна організація по стандартизації (англ. International Organization for Standardization, ISO) – міжнародна організація, що займається розробкою та випуском стандартів.

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM

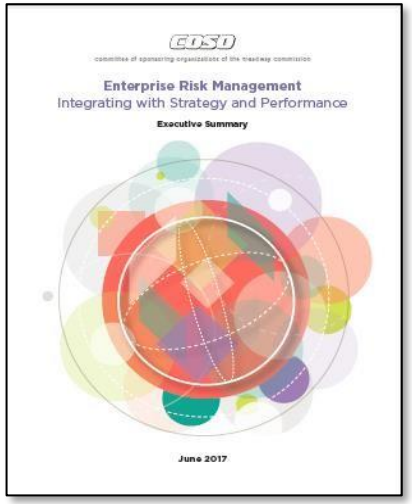
КОНЦЕПТУАЛЬНІ ЗАСАДИ УПРАВЛІННЯ РИЗИКАМИ: Інтеграція зі стратегією управлінням діяльністю

(англ. Enterprise Risk Management Integrated Framework, COSO ERM)

Концептуальні засади управління ризиками COSO ERM розроблені Комітетом організацій-спонсорів Комісії Тредвея**

COSO ERM не є стандартом, а є керівництвом, що концептуально представляє кращі практики з управління ризиками. Першу версію видано у 2004 році, чинну – у 2017 році.

COSO ERM є доступним в англомовній версії.



** Комітет організацій-спонсорів Комісії Тредвея (англ. The Committee of Sponsoring Organizations of the Treadway Commission, COSO) є добровільною приватною організацією, створеною в США. Організація призначена для вироблення відповідних рекомендацій для корпоративного керівництва по найважливішим аспектам організаційного управління, ділової етики, фінансової звітності, внутрішнього контролю, управління ризиками компаній і протидії шахрайству. [1]

1. Enterprise Risk Management — Integrated Framework. URL: https://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Russian.pdf

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM

ВИЗНАЧЕННЯ ТЕРМІНУ «РИЗИК»

РИЗИК — ймовірність виникнення подій, що можуть вплинути на досягнення стратегічних та бізнес цілей. [1]

РИЗИК — вплив невизначеності на цілі. [2]

1. Enterprise Risk Management — Integrated Framework. URL: https://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Russian.pdf
2. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM

ВИЗНАЧЕННЯ ТЕРМІНУ «УПРАВЛІННЯ РИЗИКОМ»

УПРАВЛІННЯ РИЗИКОМ — культура, компетенції та практики, інтегровані з процесом визначення стратегій та управління ефективністю, на які організація спи рається у створенні, збереженні та реалізації вартості.[1]

УПРАВЛІННЯ РИЗИКОМ — скоординовані дії для того, щоб направляти і контролювати організацію щодо ризиків.[2]

1. Enterprise Risk Management — Integrated Framework. URL: https://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Russian.pdf
2. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

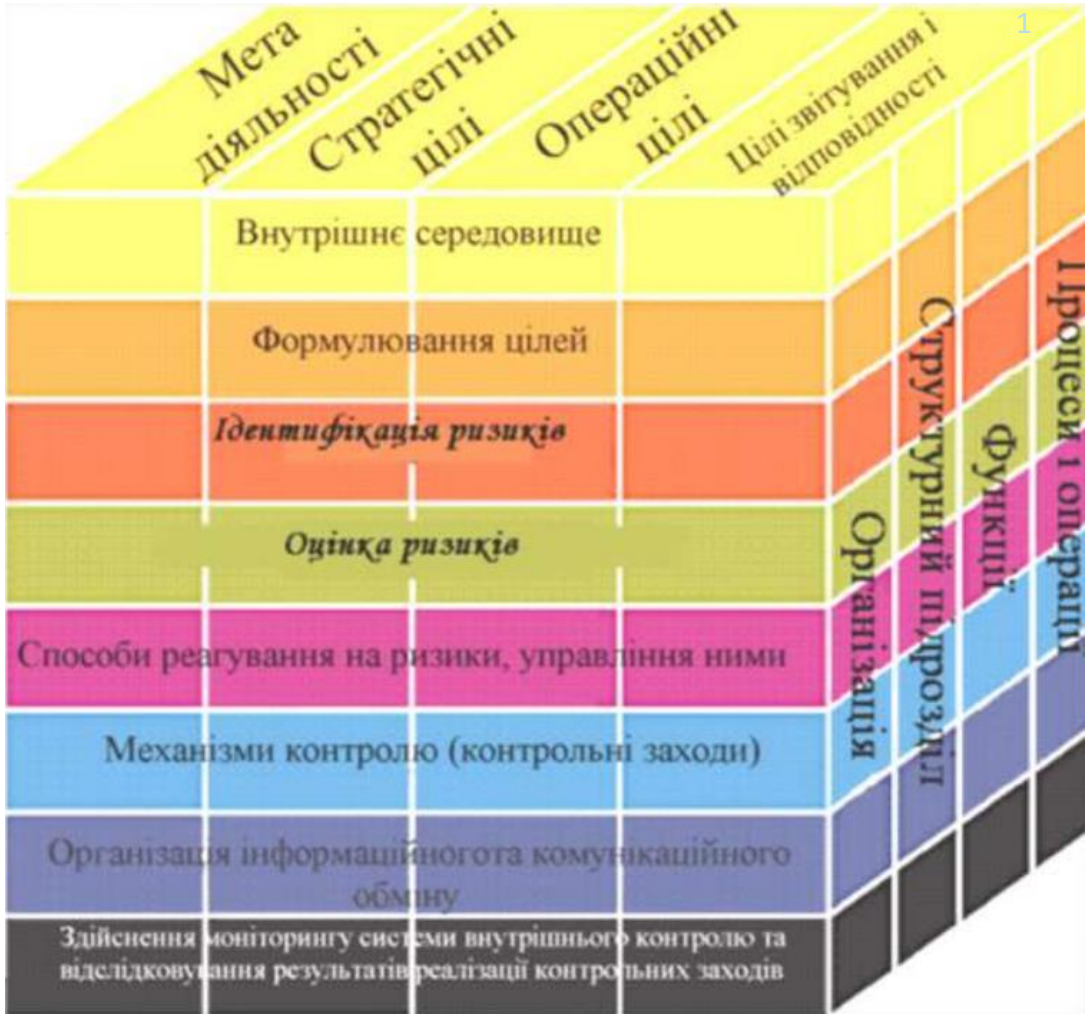
9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM

ПРОЦЕС УПРАВЛІННЯ РИЗИКОМ [1]

(стандарт ISO 31000: 2018)

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.1. Порівняльна характеристика стандартів управління ризиками ISO 31000:2018 та COSO ERM



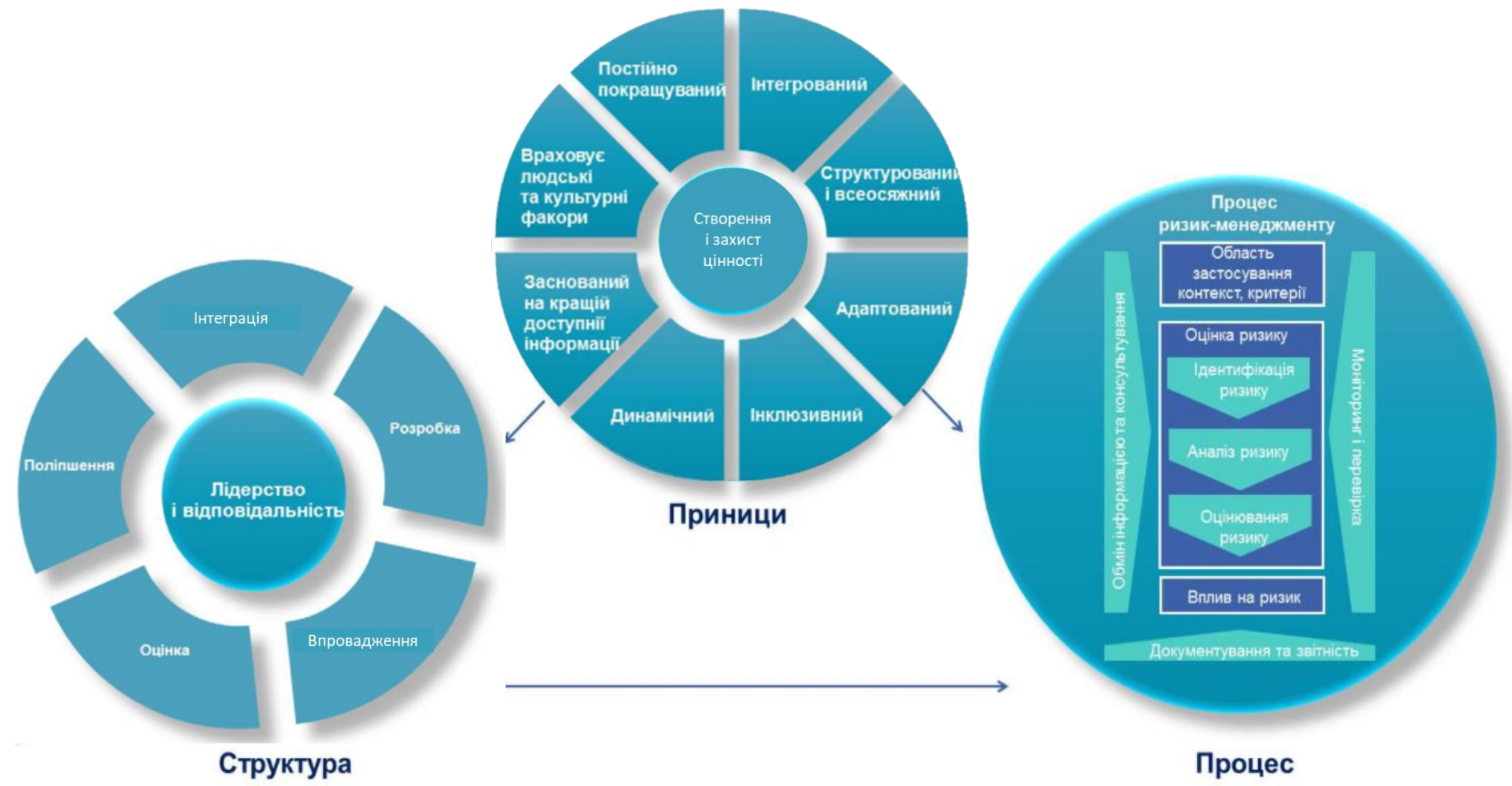
ПРОЦЕС УПРАВЛІННЯ РИЗИКОМ [1]

(стандарт COSO Enterprise Risk Management Integrated Framework)

1. Enterprise Risk Management — Integrated Framework. URL: https://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Russian.pdf

9.2. Основні положення ISO 31000:2018

ВЗАЄМОЗВ'ЯЗОК МІЖ ПРИЦИПАМИ, СТРУКТУРОЮ ТА ПРОЦЕСОМ УПРАВЛІННЯ РИЗИКАМИ В ISO 31000:2018 [1]



1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРИЗНАЧЕННЯ СТАНДАРТУ

- Стандарт призначений для осіб, які створюють і захищають вартість в організації шляхом управління ризиками, прийняття рішень, постановки цілей та забезпечення продуктивності.[1]

- Управління ризиками є частиною корпоративного управління і лідерства та лежить в основі управління організацією на всіх рівнях. Воно сприяє вдосконаленню систем управління.[1]

- Управління ризиками враховує зовнішню і внутрішню ситуацію (контекст) організації, включаючи поведінку та культуру людей.

Стандарт зорієнтований на всі види організацій, всі види процесів, всі рівні організації, всі рівні прийняття рішень. Основний «посил» стандарту в тому, що методологія та ідеологія, які в ньому прописані, можуть бути застосовані для всіх організацій та на всіх рівнях усередині організації.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СФЕРА ЗАСТОСУВАННЯ СТАНДАРТУ

- Стандарт являє собою посібник з управління ризиками, з якими стикається організація. Він може застосовуватися до будь-якої організації та її середовища.[1]
- Стандарт встановлює загальний підхід до управління будь-якими ризиками і не є вузькоспеціалізованим або галузевим.[1]
- Стандарт може використовуватися протягом всіх фаз життєвого циклу організації і щодо всього широкого спектру видів її діяльності, включаючи прийняття рішень на всіх рівнях.

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

МЕТА ТА ПРИНЦИПИ РИЗИК-МЕНЕДЖМЕНТУ

- Мета ризик-менеджменту (РМ) полягає в створенні та захисті вартості. Це сприяє інноваціям, поліпшенню показників та досягненню цілей. [1]
- Принципи дають уявлення про характеристики ефективного управління ризиками, його цінності, а також пояснюють його призначення іта мету. [1]
- Принципи лежать в основі управління ризиками та повинні враховуватися при розробленні структури і процесів РМ в організації . [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРИНЦИПИ РИЗИК-МЕНЕДЖМЕНТУ[1]

- інтегрований – РМ є невід'ємною частиною діяльності організації;
- структурований і всеосяжний – структурований та комплексний підхід до РМ призводить до узгоджених та порівняних результатів;
- адаптований – структура та процес ризик-менеджменту співвідносяться і налаштовуються з урахуванням зовнішнього і внутрішнього контексту організації, пов'язаного з її завданнями;
- інклюзивний – відповідне і своєчасне залучення зацікавлених сторін дозволяє враховувати їх знання, погляди і думки. Це призводить до підвищення обізнаності та обґрунтованості РМ;
- динамічний – ризики можуть виникати, змінюватися або зникати в міру зміни зовнішнього і внутрішнього контексту організації. РМ передбачає, виявляє, визнає і реагує на ці зміни і події відповідним чином і вчасно;[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРИНЦИПИ РИЗИК-МЕНЕДЖМЕНТУ [1] (продовження)

- заснований на найкращій доступній інформації – в якості вхідних даних для процесу РМ застосовуються історичні та фактичні дані, а також прогнозні очікування. РМ явно враховує будь-які обмеження і невизначеності, пов'язані з наявними даними та очікуваннями. Використовувана інформація повинна бути актуальною, ясною і доступною для зацікавлених сторін;
- враховує людські та культурні чинники – людська поведінка і культура суттєво впливають на всі аспекти РМ на кожному рівні та етапі;
- постійно покращуваний – РМ постійно вдосконалюється завдяки навчанню та накопичення досвіду. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

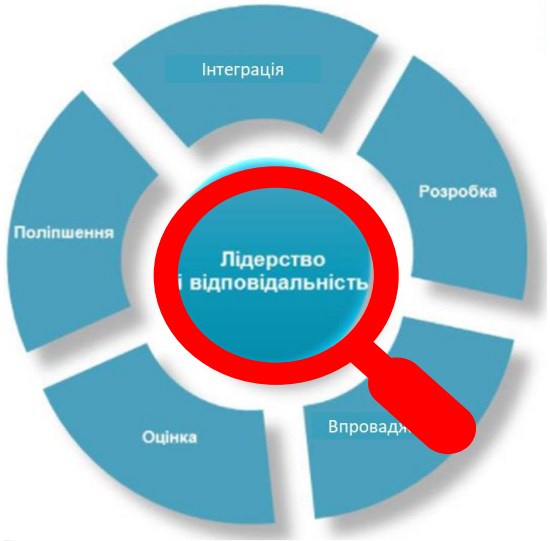
- Структура РМ призначена для сприяння організації у впровадженні РМ в усі сфери її діяльності.[1]
- Ефективність РМ залежить від його інтегрованості в систему управління та всі види діяльності організації, включаючи прийняття рішень. Це вимагає підтримки зацікавлених осіб, зокрема, вищого керівництва.[1]
- Розробка структури включає в себе інтеграцію, проектування, реалізацію, оцінку і поліпшення ризик-менеджменту в організації.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Лідерство та відповідальність



Вище керівництво та наглядові органи забезпечують інтеграцію РМ в усі види діяльності організації та демонструють лідерство і відповідальність шляхом: [1]

- узгодження РМ зі стратегіями, цілями та культурою організації;
- прийняття положення або політики, що встановлює підхід до РМ, план або порядок дій;
- виділення ресурсів для РМ;
- встановлення повноважень, відповідальності і зобов'язань на відповідних рівнях організації;
- виконання всіх вимог та зобов'язань організації;
- встановлення величини та типів припустимих та неприпустимих ризиків, на підставі яких розробляються критерії, і забезпечення того, що відповідна інформація доведена до зацікавлених сторін.
- надання інформації зацікавленим сторонам про переваги РМ;
- забезпечення безперервного моніторингу ризиків;
- забезпечення постійної адекватності структури РМ. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Інтеграція ризик-менеджменту

- Інтеграція РМ заснована на розумінні організаційних структур і контексту. Структури розрізняються залежно від мети, завдань і складності організації. РМ здійснюється в кожному елементі структури. Кожна людина в організації несе відповідальність за РМ.[1]
- Принципи корпоративного управління спрямовують діяльність організації, її зовнішні і внутрішні відносини, визначають правила, процеси і процедури, необхідні для досягнення мети. Структури управління перетворюють принципи в стратегію і цілі, необхідні для досягнення бажаних стійких показників і довгострокової життєздатності.[1]

- Інтеграція РМ в організацію – це динамічний та ітеративний процес, який повинен враховувати потреби і культуру організації. РМ повинен входити в якості складової частини в цілі організації, корпоративне управління, лідерство та відповідальність, стратегії, цілі та діяльність.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Розробка структури ризик-менеджменту

Організації розробляють структуру РМ, що включає:[1]

- Ознайомлення з організацією та зовнішнім і внутрішнім контекстом її діяльності.
- Демонстрація вищим керівництвом і наглядовими органами схильності до РМ. Це може бути реалізовано за допомогою політики, програмної заяви або іншим способом, що чітко відображає цілі і прихильність організації менеджменту ризику.
- Визначення організаційних функцій, відповідальності, обов'язків, наділення повноваженнями щодо УР і доведення їх до відома відповідних осіб в організації.
- Розподіл ресурсів для управління ризиками.
- Встановлення механізмів обміну інформацією та консультування для підтримки структури і сприяння ефективному застосуванню РМ.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Впровадження структури ризик-менеджменту

Організація впроваджує структуру РМ за допомогою:[1]

- розробки відповідного плану з визначенням термінів;
- визначення того, де, коли, як і ким приймаються різні типи рішень щодо організації;
- модифікації застосовуваних процесів прийняття рішень;
- забезпечення розуміння та правильного застосування механізмів управління ризиками організації.

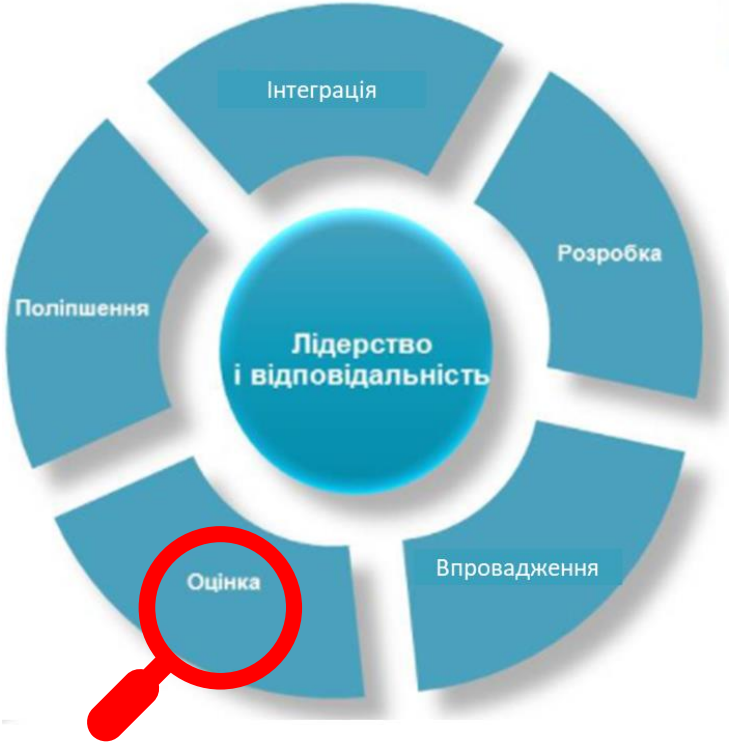
Належним чином спроектована і застосована структура ризик-менеджменту забезпечує його впровадження в усі види діяльності організації, включаючи процес прийняття рішень, а також належний облік змін у зовнішній і внутрішній ситуації. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Оцінка структури ризик-менеджменту



З метою оцінки ефективності структури РМ, організація: [1]

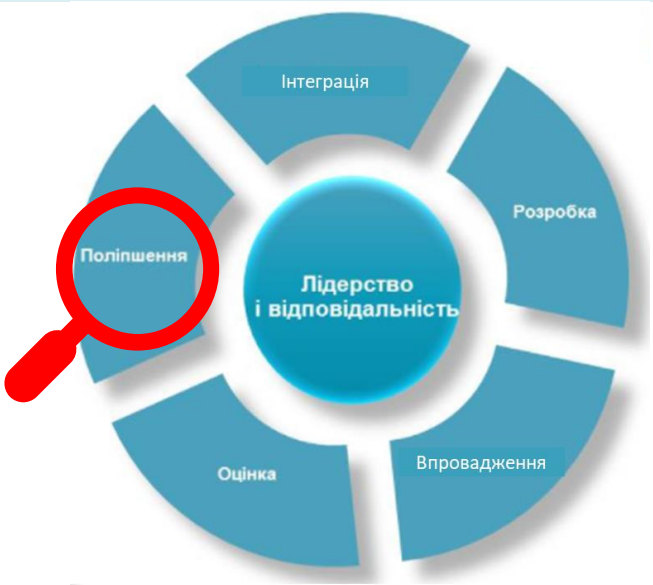
- проводить періодичну оцінку ефективності структури РМ з точки зору її мети, планів реалізації, показників та передбачуваної поведінки.
- визначає, як структура сприяє досягненню цілей організації. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

СТРУКТУРА РИЗИК-МЕНЕДЖМЕНТУ

Покращення структури ризик-менеджменту



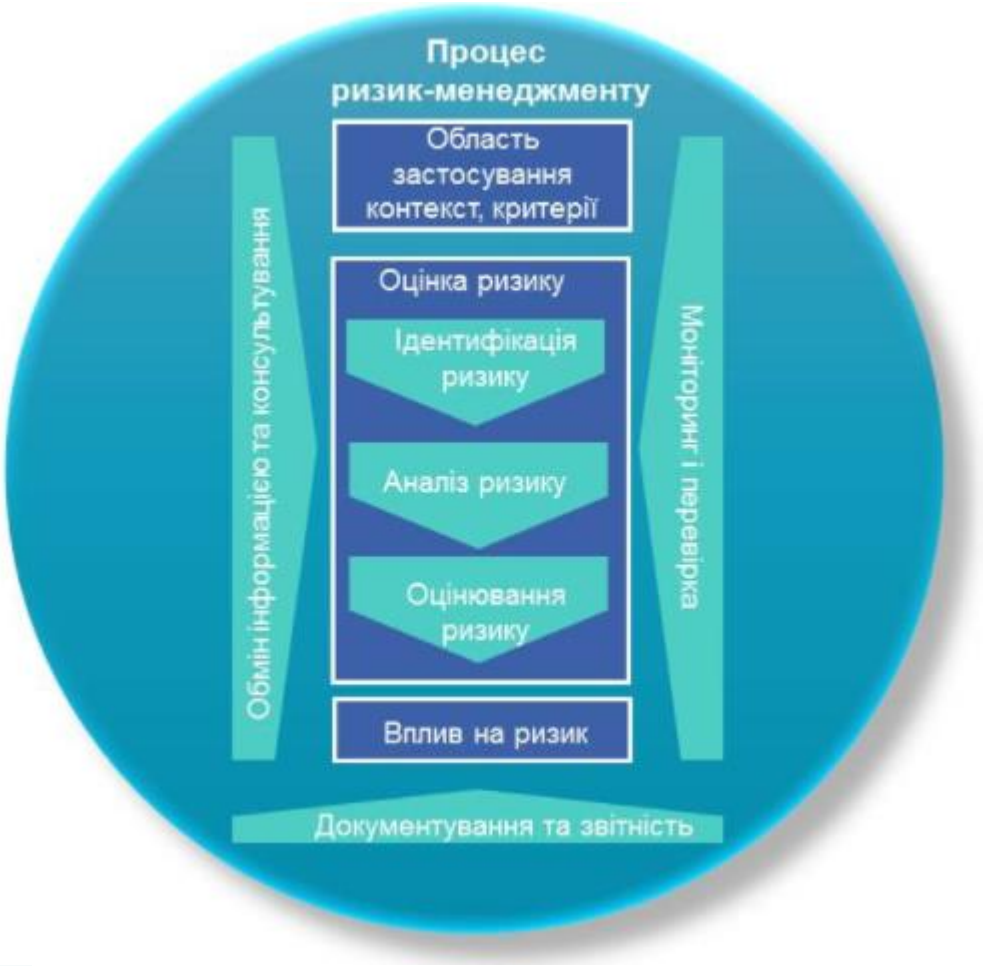
- Організація постійно контролює і адаптує структуру РМ для реагування на зовнішні і внутрішні зміни. Діючи таким чином, організація може поліпшити показники своєї вартості.[1]
- Організація постійно підвищує рівень адекватності, достатності та ефективності структури РМ і покращує способи інтегрування процесу ризик-менеджменту.

У міру виявлення відповідних недоліків або можливостей поліпшення організація розробляє плани та завдання і доручає їх виконання тим, хто відповідає за реалізацію. Після реалізації ці поліпшення сприяють удосконаленню системи РМ.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ



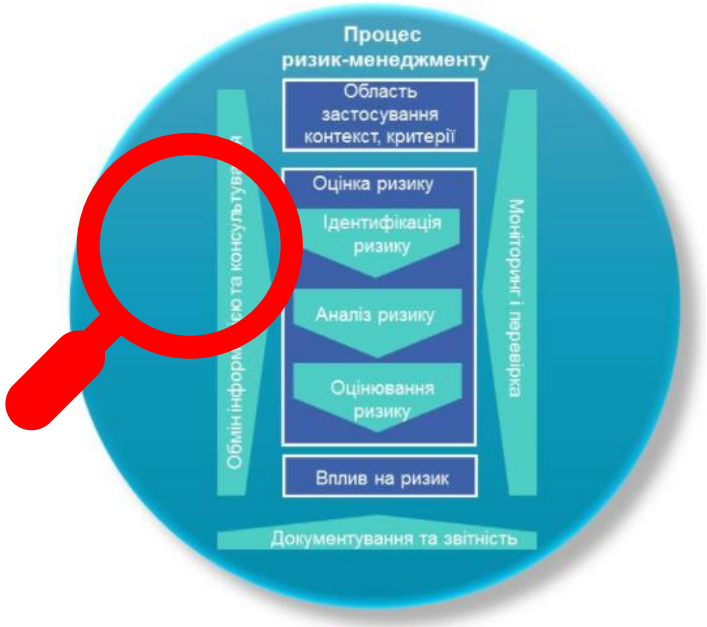
- Процес РМ повинен стати невід'ємною частиною процесів менеджменту та прийняття рішень, інтегрованим в структуру, діяльність і процеси організації.[1]
- Він може застосовуватися на стратегічному, операційному, програмному або проектному рівнях.[1]
- В організації процес РМ, адаптований до зовнішнього та внутрішнього контекстів, може застосовуватися в різних цілях.[1]
- Протягом всього процесу ризик-менеджменту слід враховувати динамічний і мінливий характер поведінки та культури людини.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Коммунікація та консультування



Метою комунікації та консультування є сприяння зацікавленим сторонам в розумінні ризику, формування засад для прийняття рішень і визначення причин, за якими необхідні певні дії. [1]

- Комунікація спрямована на поінформованість та розуміння ризику, а також способів його усунення. [1]
- Консультування включає отримання зворотного зв'язку та інформації в підтримку процесу прийняття рішень.

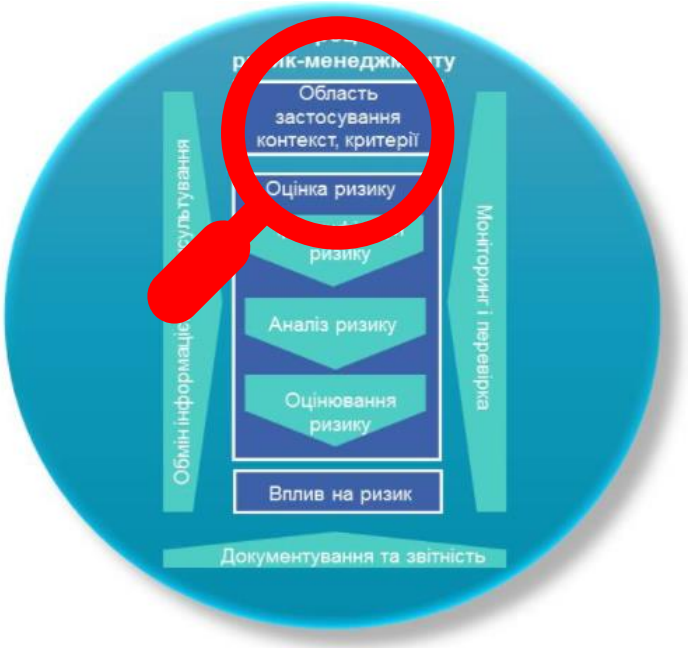
- Тісна взаємодія цих двох процесів має сприяти фактичному, своєчасному, актуальному, точному і зрозумілому обміну інформацією з урахуванням конфіденційності та достовірності інформації. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Визначення ситуації (контексту)



Метою визначення контексту є адаптація процесів оцінки ризиків та відповідного впливу на ризик.[1]

- Визначення контексту включає визначення мети і сфери застосування процесу, досягнення розуміння контексту, планування необхідного підходу та визначення критеріїв оцінки.

- При визначенні контексту необхідно враховувати внутрішній та зовнішній контекст, окреслений в рамках системи РМ.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Оцінка ризику

Оцінка ризику – це сукупний процес ідентифікації, аналізу та оцінювання ризику.[1]

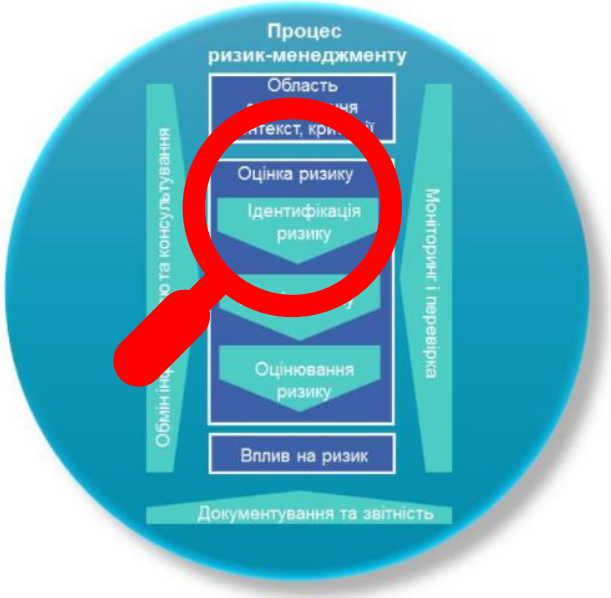
- Оцінка ризику повинна проводитися систематично, ітераційно і спільно, ґрунтуючись на знаннях і думках зацікавлених сторін. Необхідно використовувати всю доступну інформацію, у міру необхідності доповнюючи її новою інформацією.[1]
- Метою ідентифікації ризику є в пошук, визначення та опис ризиків. Для ідентифікації ризику необхідна відповідна і актуальна інформація.
- Мета аналізу ризику полягає в забезпеченні розуміння характеру ризику і його особливостей, в тому числі (коли це необхідно) рівня ризику. Аналіз ризиків включає детальний розгляд невизначеностей, джерел ризику, наслідків, ймовірностей подій, сценаріїв, засобів контролю та їх ефективності. Подія може мати різні причини і наслідки і може впливати на різні цілі.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Оцінка ризиків (продовження)



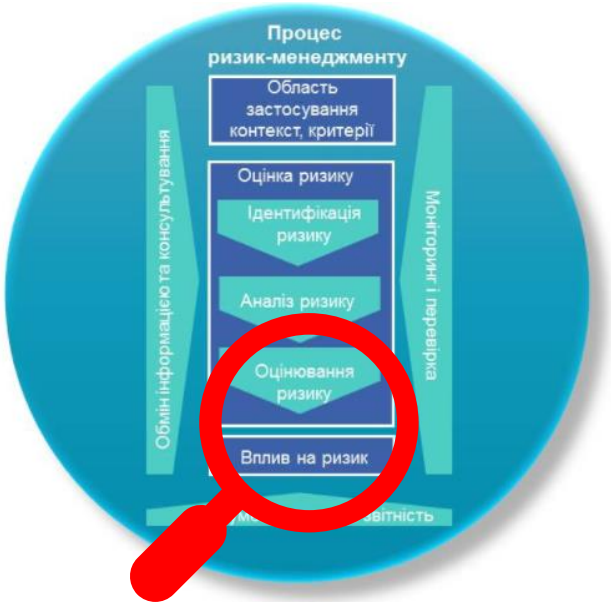
- На аналіз ризиків впливає будь-яка розбіжність думок, необ'єктивність, сприйняття ризику та судження.[1]
- Додатковий вплив має якість використовуваної інформації, припущення та виключення, будь-які обмеження методик та способів їх виконання. Ці фактори необхідно вивчити, документувати і повідомляти особам, відповідальним за прийняття рішень.[1]
- Метою оцінювання ризику є сприяння прийняттю рішень. Оцінювання ризику включає порівняння результатів аналізу ризику та встановлених критеріїв ризику, що здійснюється для визначення його суттєвості.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Обробка ризиків (вплив на ризики)



Вплив на ризик являє собою ітеративний процес відбору та застосування різних способів реагування на ризик і передбачає: [1]

- визначення та вибір варіантів та способів впливу на ризик;
- планування та реалізацію впливу на ризик;
- оцінку ефективності впливу;
- прийняття рішення про прийнятність залишкового ризику;
- подальший вплив в разі, якщо ризик є неприйнятним. [1]

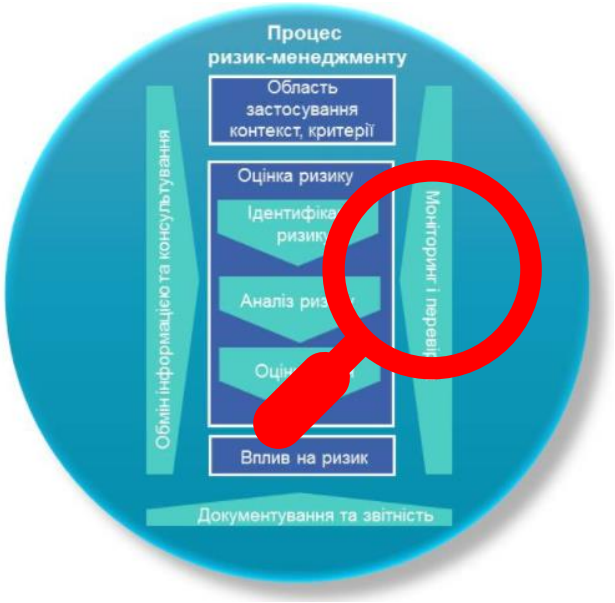
- Вибір найбільш відповідного варіанту (варіантів) впливу на ризик включає зіставлення витрат, зусиль та недоліків реалізації обраного способу впливу з вигодами, які отримуються завдяки досягненню цілей впливу на ризик. [1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

Моніторинг та перевірка



Моніторинг і перевірка спрямовані на забезпечення якості та ефективності реалізації РМ: [1]

- Постійний моніторинг і періодична перевірка процесу управління ризиками та його результатів повинні бути спланованою частиною процесу РМ, щодо якої встановлена чітка відповідальність. [1]
- Моніторинг і перевірка повинні проводитися на всіх етапах процесу і включати планування, збір, аналіз інформації, документування результатів і надання зворотного зв'язку. [1]

- Результати моніторингу та перевірки повинні бути частиною діяльності по загальному управлінню організацією, оцінці ефективності, а також складання звітності.

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.2. Основні положення ISO 31000:2018

ПРОЦЕС РИЗИК-МЕНЕДЖМЕНТУ

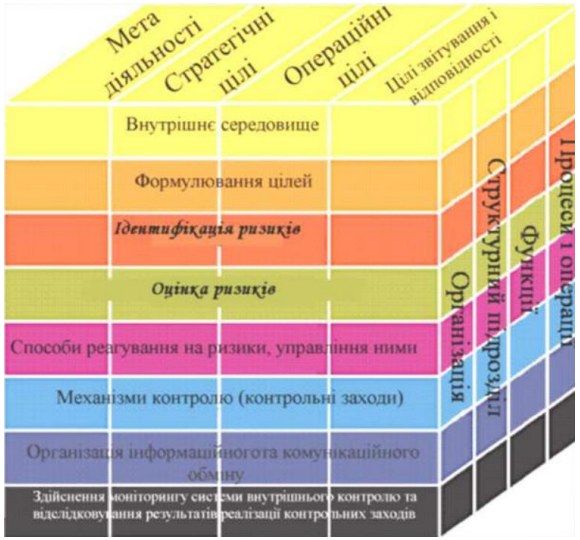
Документування та звітність

- Процес управління ризиками та його результати повинні документуватись та відображатись в звітності за допомогою відповідних механізмів.[1]
- Рішення щодо створення, зберігання та обробки задокументованої інформації повинні прийматись з урахуванням їх використання, конфіденційності інформації, зовнішнього та внутрішнього контекстів.[1]
- Звітність є невід'ємною частиною корпоративного управління та повинна підвищувати якість діалогу з зацікавленими особами, сприяти вищому керівництву і наглядовим органам у виконанні ними своїх обов'язків.[1]

1. ISO 31000:2018. Менеджмент рисков: Принципы и руководящие указания. International Organization for Standardization. URL: https://www.iso.org/ru/iso-31000-risk-management.html

9.3. Основні положення COSO ERM

ПРИНЦИПИ РИЗИК-МЕНЕДЖМЕНТУ



- РМ не є функцією або структурою організації. Це культура, компетенції та практики, які організація інтегрує з процесом розробки стратегії і її реалізації з метою управління ризиками при створенні, збереженні та реалізації вартості. [1]
- РМ не обмежується реєстром ризиків. [1]
- РМ пов'язаний не тільки з внутрішнім контролем, а й зі стратегією, корпоративним управлінням, комунікацією із зацікавленими сторонами і управлінням ефективністю. [1]
- РМ організації не є чек-листом. Він включає принципи, відповідно до яких можуть бути побудовані бізнес-процеси та є системою моніторингу, навчання і поліпшення ефективності діяльності. [1]
- РМ може бути застосованим для всіх організацій незалежно від їх розміру. [1]

1. Enterprise Risk Management — Integrated Framework. URL: https://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Russian.pdf

9.3. Основні положення COSO ERM

СТРУКТУРА КОНЦЕПЦІЇ РИЗИК-МЕНЕДЖМЕНТУ В COSO ERM [1]

Управління та культура	Стратегія і постановка цілей	Ефективність діяльності	Моніторинг і впровадження змін	Інформація, комунікація та звітність
1. Здійснення радою директорів наглядової функції за управлінням ризиками. **2.** Створення операційних структур. **3.** Визначення бажаної культури. **4.** Демонстрація прихильності основним цінностям. **5.** Залучення, розвиток та утримання кваліфікованих фахівців.	**6.** Аналіз умов ведення діяльності. **7.** Визначення ризик-апетиту. **8.** Оцінка стратегічних альтернатив. **9.** Формулювання бізнес-цілей.	**10.** Виявлення ризиків. **11.** Оцінка впливу ризиків. **12.** Пріорітезація ризиків. **13.** Реагування на ризики. **14.** Комплексний погляд на ризики.	**15.** Оцінка істотних змін. **16.** Аналіз ризиків та ефективності діяльності. **17.** Підвищення ефективності системи управління ризиками.	**18.** Використання інформації та технологій. **19.** Поширення інформації про ризики. **20.** Звітність про ризики, корпоративній культурі та ефективності діяльності.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

УПРАВЛІННЯ ТА КУЛЬТУРА[1]

1. Здійснення радою директорів наглядової функції за управлінням ризиками	• Рада директорів несе ключову відповідальність за здійснення нагляду за управлінням ризиками. • Здійснення нагляду за управлінням ризиками вимагає від Ради директорів глибокого розуміння стратегії, галузі та інформованості з поточних питань. • Рада директорів повинна оцінювати ефективність управління ризиками з точки зору його внеску в створення вартості.
2. Створення операційних структур	• Операційна структура організації визначається виходячи з її стратегії та цілей. • Збір інформації щодо ризиків може бути делегований комітетам при Раді директорів. • Ризик-офіцер здійснює роль методологічної підтримки та координації діяльності з управління ризиками.
3. Визначення бажаної культури	• Корпоративна культура впливає на те, яким чином ризики виявляються, оцінюються і управляються в організації з моменту визначення стратегії та до її реалізації. • У ризик-орієнтованої корпоративної культури прийняті рішення та поведінка є чітко окресленими ризик-апетитом організації.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

УПРАВЛІННЯ ТА КУЛЬТУРА[1] (продовження)

4. Демонстрація прихильності основним цінностям	• Розуміння ключових цінностей організації закладає фундамент для інтегрованої системи управління ризиками. • Рада директорів призначає генерального директора відповідальним за управління ризиками для забезпечення досягнення стратегічних і бізнес цілей. • Генеральний директор та інші представники топ-менеджменту несуть відповідальність за всі аспекти розвитку культури і системи управління ризиками.
5. Залучення, розвиток та утримання кваліфікованих фахівців	• Керівництво, при нагляді з боку Ради директорів, визначає потребу в людському капіталі, необхідному для досягнення стратегічних і бізнес цілей. • Система заохочення повинна бути прив'язана до досягнення стратегічних і бізнес цілей організації, що також вимагає відповідну оцінку, пріоритизації ризиків і план заходів по їх управлінню.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

Зауваження 1

- У багатьох компаніях Рада директорів формально виконує наглядові функції в частині управління ризиками, але не проявляє реального інтересу в розвитку РМ і його інтеграції з бізнесом. Перед ризик-менеджерами стоїть завдання підвищення інтересу до управління ризиками з боку Ради директорів і керівництва за допомогою розробки і впровад-ження підходів, при яких взаємозв'язок між управлінням ризиками і створенням вартості буде більш очевидним.[1]

- Існують практики, при яких ризик-офіцер розглядається як співробітник, який несе відповідальність за ризики. COSO ERM однозначно підкреслює, що роль ризик-офіцера полягає в методологічній підтримці і координації діяльності з управління ризиками. Проте, необхідно розуміти ситуації, при яких роль ризик-офіцера може бути більш розширеною.[1]

- У багатьох компаніях організаційна структура та кадрова політика сформовані історично і не завжди відображають стратегічні ініціативи. Реструктуризація може вимагати істотних ресурсів і зіткнутися з опором з боку керівництва.[1]

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

СТРАТЕГІЯ І ПОСТАНОВКА ЦІЛЕЙ[1]

6. Аналіз умов ведення діяльності	• Організація розглядає умови (зовнішні / внутрішні) ведення бізнесу в процесі розробки стратегії для реалізації своєї місії, бачення і ключових цінностей. • Вплив умов ведення бізнесу на профіль ризику може розглядатися в перспективи минулих, поточних і майбутніх подій.
7. Визначення ризик-апетиту	• Рішення пов'язані з вибором стратегії і визначенням ризик-апетиту не пов'язані лінійними відносинами, коли одне передує іншому. • Підходи до визначення ризик-апетиту визначаються організаціями виходячи зі специфіки їх діяльності. • Кращим підходом вважається визначення ризик-апетиту в контексті ризик профілю та ємності ризику.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

СТРАТЕГІЯ І ПОСТАНОВКА ЦІЛЕЙ (продовження)[1]

8. Оцінка стратегічних альтернатив	• Організація повинна проводити аналіз альтернативних стратегій і оцінювати ризики і можливості кожної з альтернатив. • Керівництво та Рада директорів повинні враховувати профіль ризику і ризик-апетит при виборі стратегії.
9. Визначення бажаної культури	• Цілі визначаються на різних рівнях, але повинні бути прив'язані до стратегії організації. • Толерантність відображає прийнятне відхилення від поставлених цілей. • Відповідно, толерантність визначається в відносин цілей і ефективності, а не конкретних ризиків. • Ступінь ефективності досягнення цілей визначається межами толерантності.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

Зауваження 2

- Ризик-апетит є невід'ємною частиною інтеграції управління ризиками зі стратегічним плануванням. Оскільки COSO ERM залишає розробку підходів до визначення ризик-апетиту на розсуд організацій, перед зацікавленими сторонами стоїть завдання щодо такого впровадження концепції ризик-апетиту, що буде використовуватися як реальний діючий інструмент при прийнятті рішень, а не залишатися формальним.[1]

- У багатьох бізнес-практиках концепція толерантності до ризиків вже застосовується в процесах планування та реалізації господарської діяльності. Виникає питання щодо взаємної ув’язки толерантності до ризиків з ризик-апетитом організації.[1]

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

ЕФЕКТИВНІСТЬ ДІЛЬНОСТІ [1]

10. Виявлення ризиків	• Організація виявляє ризики, пов'язані з досягненням стратегічних і бізнес цілей. • Спочатку організація формує загальну базу даних за ризиками (risk inventory) і в подальшому визначає, які ризики є актуальними. • Ризики можуть бути структуровані за окремими категоріями, які організація визначає на власний розсуд. • Ризики визначаються на всіх рівнях бізнес-процесів і функцій.
11. Оцінка впливу ризиків	• Ризики оцінюються за впливом та ймовірністю. Вплив ризику вимірюється щодо мети, на яку він впливає. • Імовірність ризику може бути виражена експертною, кількісною оцінкою або статистичною частотою. • Опис ризику включає опис ризикових факторів і їх наслідків. • Оцінка ризиків може бути кількісною та якісною. • В процесі оцінки ризиків керівництво бере до уваги властивий ризик, цільовий та фактичний залишковий ризик. • Карта ризиків (heat map) використовується як інструмент графічної візуалізації суттєвості ризиків. • При оцінці ризиків керівництво повинно брати до уваги та знижувати ефект упередженості.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

ЕФЕКТИВНІСТЬ ДІЛЬНОСТІ [1] (продовження)

12. Пріоритезація ризиків	• Організація пріоритезує ризики для вибору адекватної стратегії реагування на ризики та розподілу ресурсів. • При пріоритезації ризиків необхідно враховувати ризик-апетит. Підвищений пріоритет отримують ризики, вплив яких може привести до перевищення ризик-апетиту. • Пріоритетність ризиків визначається за встановленими критеріями (наприклад, складність, швидкість, стійкість впливу ризику, адаптивність до ризику, відновлення після нього).
13. Реагування на ризики	• Виділяються 5 стратегій реагування на ризик (ухилення, прийняття, розподіл, попередження, зниження ризику). • Ці стратегії застосовуються в рамках існуючих умов діяльності, прийнятих цілей та ризик-апетиту. У випадках, коли рівень ризику виявляється занадто високим, а стратегії реагування на нього – неприйнятними, організація може переглянути свої стратегічні та операційні цілі. • Вибір стратегії здійснюється з урахуванням умов бізнесу, співвідношення вигод та витрат, зобов'язань і очікувань, пріоритезації ризиків, ризик-апетиту і суттєвості ризику.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

ЕФЕКТИВНІСТЬ ДІЛЬНОСТІ (продовження)[1]

14. Комплексний погляд на ризики

- Комплексний погляд на ризики дозволяє організації визначити наскільки залишковий профіль ризику відповідає встановленому ризик-апетиту.
- Виділяються кілька підходів до портфельного аналізу ризиків в залежності від ступеня інтеграції РМ з бізнесом:
  - ✓ Мінімальна інтеграція (фокус лише на істотні ризики) – організація виявляє і оцінює ризики дискретно, фокусуючись на подіях, а не на цілях.
  - ✓ Обмежена інтеграція (фокус на певних категоріях ризиків) – організація формує базу даних за ризиками, структурованими за категоріями. Портфель ризиків являє перелік ризиків, згрупованих за категоріями.
  - ✓ Часткова інтеграція (фокус на профілі ризику) – організація переносить фокус на бізнес-цілі та ризики, пов'язані з їх досягненням.
  - ✓ Повна інтеграція (комплексний погляд на ризики) – організація фокусується на стратегії і бізнес-цілях. Ризики визначаються на всіх рівнях прийняття рішень.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

Зауваження 3

- Створення і ведення бази даних ризиків може потребувати багато ресурсів. Не завжди є можливим обґрунтування доцільності цього процесу в точки зору створення вартості.[1]
- Концепція COSO ERM встановлює основні метрики для оцінки ризиків (ймовірність / вплив). Тим не менш, в ній не зазначається, що для певних ризиків більш доцільним є визначення ймовірного розподілу впливу.[1]
- Карта ризиків залишається основним інструментом візуалізації ризиків. При цьому не зазначється можливість застосування альтернативних інструментів (наприклад, діаграми-торнадо).[1]
- У багатьох організаціях концепція толерантності до ризиків вже застосовується в процесах планування та здійснення діяльності. Виникає питання щодо взаємоузгодження толерантності до ризиків з ризик-апетитом організації.[1]

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

МОНІТОРИНГ І ВПРОВАДЖЕННЯ ЗМІН [1]

15. Оцінка істотних змін	• Організація, як правило, розглядає потенційні зміни в процесі визначення стратегії і установки цілей, але, тим не менш, їй необхідно здійснювати моніторинг змін в поточній діяльності і оцінювати їх вплив на стратегію і профіль ризику.
16. Аналіз ризиків та ефективності діяльності	• Аналіз ризиків та ефективності діяльності повинен бути інтегрований в діяльність організації. Ключовими питаннями є: ✓ Чи досягла організація цілей з очікуваною ефективністю? ✓ Які ризики реалізовуються і можуть вплинути на ефективність? ✓ Чи є достатнім рівень ризику для досягнення цілей компанії? ✓ Чи правильно було оцінено ризик? • У разі істотних відхилень від цілей, організація може переглянути бізнес-цілі, стратегію, корпоративну культуру, цільові показники ефективності діяльності, оцінку ризиків, стратегії реагування на ризики, ризик-апетит.
17. Підвищення ефективності системи РМ	• Організація повинна прагнути до постійного підвищення ефективності управління ризиками на всіх рівнях управління.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html

9.3. Основні положення COSO ERM

ІНФОРМАЦІЯ, КОМУНІКАЦІЯ І ЗВІТНІСТЬ [1]

18. Використання інформації та технологій	• Побудова інформаційної інфраструктури має враховувати забезпечення гнучкості в прийнятті рішень. • Необхідно брати до уваги розвиток технологій з аналізу даних, які дозволяють охопити великі обсяги даних та приймати більш обґрунтовані рішення.
19. Поширення інформації про ризики	• Комунікація інформації за ризиками повинна стати невід'ємною частиною комунікації стратегії і бізнес-цілей. • Необхідно визначити ролі та обов'язки між радою директорів і керівництвом в частині підготовки та використання інформації за ризиками. • Обговорення ризик-апетиту між радою директорів і керівництвом повинно проходити на постійній основі.
20. Звітність про ризики, корпоративній культурі та ефективності діяльності	• Звітність за ризиками може готуватися на всіх рівнях управління. • На рівні ради директорів звітність повинна бути сфокусована на взаємозв'язку між стратегією, бізнес-цілей, ризиками і ефективністю діяльності. • Частота та якість звітності визначається керівництвом виходячи із специфіки і бізнес-необхідності.

1. Управление рисками. Правила игры меняются. Делойт. 30.01.2018. URL: https://www2.deloitte.com/ru/ru/pages/risk/events/risk-management-business-breakfast.html