ISO 31000 Менеджмент ризиків. Керівництво

Перекладач Єгоров А.

Передмова
ISO (Міжнародна організація зі стандартизації) є всесвітньою федерацією національних органів стандартизації (органів-членів ISO). Робота з підготовки міжнародних стандартів, як правило, здійснюється через технічні комітети ISO. Кожен орган-член, зацікавлений у суб'єкті, для якого створено технічний комітет, має право бути представленим у цьому комітеті. У роботі також беруть участь міжнародні організації, урядові та неурядові, які підтримують зв'язок з ISO. ISO тісно співпрацює з Міжнародною електротехнічною комісією (IEC) з усіх питань електротехнічної стандартизації.

Процедури, що використовуються для розробки цього документа, та ті, що призначені для його подальшого обслуговування, описані в Директивах ISO/IEC, частина 1. Зокрема, слід зазначити різні критерії затвердження, необхідні для різних типів документів ISO. Цей документ був розроблений відповідно до редакційних правил Директив ISO/IEC, частина 2 (див.www.iso.org/directives).

Звертається увага на можливість того, що деякі елементи цього документа можуть бути об'єктом патентних прав. ISO не несе відповідальності за ідентифікацію будь-яких або всіх таких патентних прав. Деталі будь-яких патентних прав, виявлених під час розробки документа, будуть у Вступі та/або в ISO переліку отриманих патентних декларацій (див.www.iso.org/patents).

Будь-яке комерційне найменування, що використовується в цьому документі, є інформацією, наданою для зручності користувачів, і не є схваленням.

Пояснення щодо добровільного характеру стандартів, значення специфічних термінів та виразів ISO, пов'язаних з оцінкою відповідності, а також інформацію про дотримання ISO принципів Світової організації торгівлі (СОТ) у Технічних бар'єрах у торгівлі (ТВТ) можна знайти в наступному URL:www.iso.org/iso/foreword.html.

Даний документ підготовлений Технічним комітетом ISO/TC 262,Управління *ризиками*.

Це друге видання скасовує та замінює перше видання (ISO 31000:2009), яке було технічно переглянуто.

Основні зміни в порівнянні з попередньою редакцією наступні:

- —розгляд принципів управління ризиками, які є ключовими критеріями його успішності;
- —виділення лідерства вищим керівництвом та інтеграція управління ризиками, починаючи з управління організацією;
- —більший акцент на ітераційному характері управління ризиками, відзначаючи, що новий досвід, знання та аналіз можуть призвести до перегляду елементів процесу, дій та засобів контролю на кожному етапі процесу;

- — упорядкування вмісту з більшою увагою до підтримки моделі відкритих систем відповідно до різних потреб і контекстів.

Введення

Цей документ призначений для використання людьми, які створюють і захищають цінність в організаціях шляхом управління ризиками, прийняття рішень, встановлення та досягнення цілей та підвищення ефективності.

Організації всіх типів і розмірів стикаються із зовнішніми і внутрішніми факторами і впливами, які роблять невизначеним, чи досягнуть вони своїх цілей.

Управління ризиками є ітераційним і допомагає організаціям у визначенні стратегії, досягненні цілей та прийнятті обґрунтованих рішень.

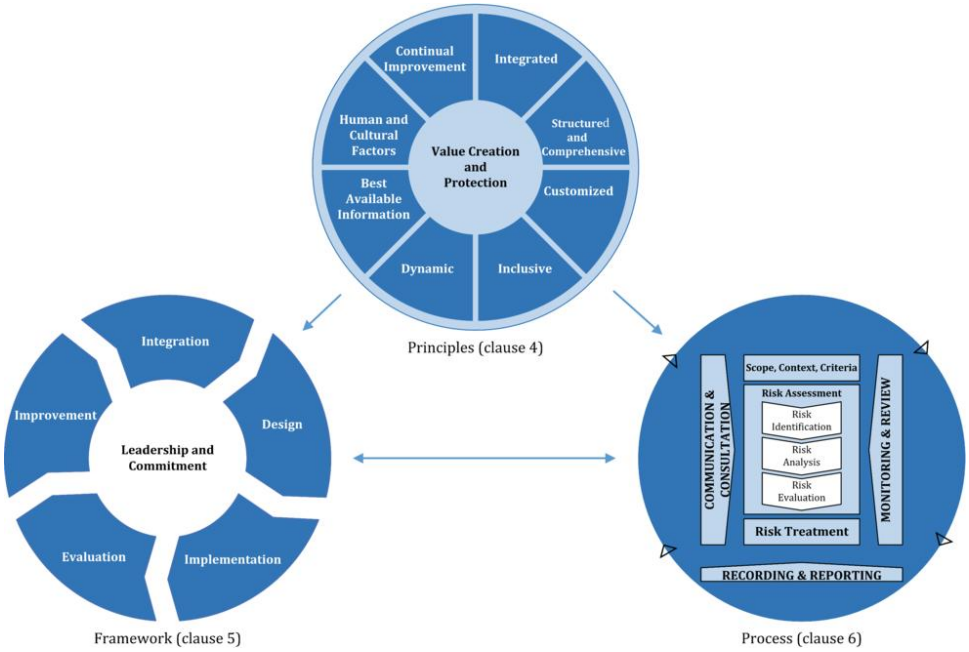
Управління ризиками є частиною управління та лідерства і є основоположним для того, як організація управляється на всіх рівнях. Вона сприяє вдосконаленню систем управління.

Управління ризиками є частиною всіх видів діяльності, пов'язаних з організацією і включає в себе взаємодію зі стейкхолдерами.

Управління ризиками враховує зовнішній і внутрішній контекст організації, включаючи поведінку людини і культурні чинники.

Управління ризиками базується на принципах, структурі та процесах, викладених у цьому документі, як проілюстровано нарисунку 1. Ці компоненти вже можуть існувати повністю або частково в організації, однак, можливо, їх потрібно буде адаптувати або вдосконалити, щоб управління ризиками було ефективним, ефективним і послідовним.

Рисунок 1 — Принципи, рамки та процес



1 Сфера застосування

Цей документ містить керівні принципи щодо управління ризиками, з якими стикаються організації. Застосування цих керівних принципів можна налаштувати під будь-яку організацію та її контекст.

Цей документ забезпечує загальний підхід до управління будь-яким видом ризиків і не є специфічним для галузі чи сектору.

Цей документ може використовуватися протягом усього життя організації і може застосовуватися до будь-якої діяльності, включаючи прийняття рішень на всіх рівнях.

2 Нормативні посилання

Нормативних посилань в цьому документі немає.

3 Терміни та визначення

Для цілей цього документа застосовуються такі терміни та визначення.

ISO та IEC ведуть термінологічні бази даних для використання в стандартизації за наступними адресами:

- — Платформа перегляду ISO в Інтернеті: доступна заадресою http://www.iso.org/obp
- — IEC Electropedia: доступний заадресою http://www.electropedia.org

3.1

ризик

вплив невизначеності на цілі

Примітка 1 до запису: Ефект - це відхилення від очікуваного. Він може бути позитивним, негативним або обома, а також може вирішувати, створювати або призводити до можливостей і загроз.

Примітка 2 до запису: Цілі можуть мати різні аспекти та категорії, і можуть застосовуватися на різних рівнях.

Примітка 3 до запису: Ризик, як правило, виражається в термінах джерел ризику(3.4), потенційних подій(3.5), їх наслідків(3.6)і їх**ймовірності**(3.7).

3.2

управління ризиками

скоординована діяльність щодо спрямування та контролю організації щодо**ризику**(3.1)

3.3

Зацікавлена сторона

особа чи організація, які можуть впливати на рішення чи діяльність, впливати на них або сприймати себе як такі, що впливають на них

Примітка 1 до запису: Термін «зацікавлена сторона» може використовуватися як альтернатива «зацікавленій стороні».

3.4

джерело ризику

елемент, який окремо або в поєднанні може призвести до**ризику**(3.1)

3.5

подія

виникнення або зміна певного збігу обставин

Примітка 1 до запису: Подія може мати одне або кілька подій, а може мати кілька причин і кількА**наслідків**(3.6).

Примітка 2 до запису: Подія також може бути чимось, що очікується, що не відбувається, або чимось, що не очікується, що все-таки станеться.

Примітка 3 до запису: Подія може бути джерелом ризику.

3.6

наслідок

результат**події**(3.5)що впливає на цілі

Примітка 1 до запису: Наслідок може бути певним або невизначеним і може мати позитивний або негативний прямий або непрямий вплив на цілі.

Примітка 2 до запису: Наслідки можуть бути виражені якісно або кількісно.

Примітка 3 до запису: Будь-який наслідок може загостритися за допомогою каскадних і кумулятивних ефектів.

3.7

Ймовірність

ймовірність того, що щось трапиться

Примітка 1 до запису: У термінології**управління** ризиками(3.2)слово «ймовірність» використовується для позначення ймовірності того, що щось станеться, незалежно від того, чи визначається, вимірюється або визначається об'єктивно чи суб'єктивно, якісно чи кількісно, і описується за допомогою загальних термінів або математично (наприклад, ймовірність або частота протягом певного періоду часу).

Примітка 2 до запису: Англійський термін "ймовірність" не має прямого еквівалента в деяких мовах; Замість нього часто використовується еквівалент терміна «ймовірність». Однак в англійській мові «імовірність» часто вузько трактується як математичний термін. Тому в термінології управління ризиками «ймовірність» використовується з наміром, що вона повинна мати таке ж широке тлумачення, як і термін «ймовірність» у багатьох мовах, крім англійської.

3.8

контроль

міра, яка підтримує та/або змінює**ризик**(3.1)

Примітка 1 до запису: Засоби контролю включають, серед іншого, будь-який процес, політику, пристрій, практику або інші умови та/або дії, які підтримують та/або змінюють ризик.

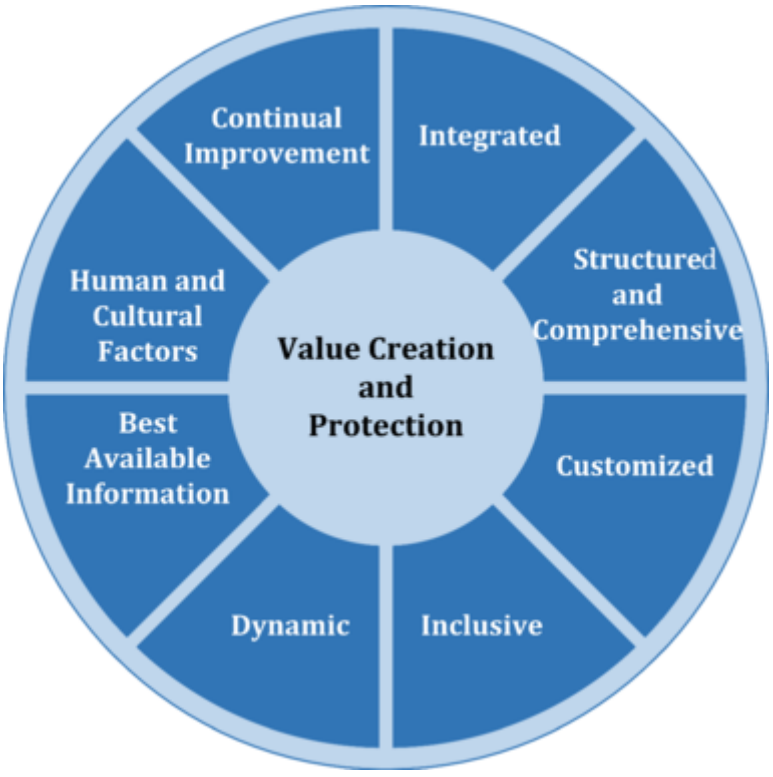
Примітка 2 до запису: Елементи керування не завжди можуть надавати передбачуваний або передбачуваний модифікуючий ефект.

4 Принципи

Метою управління ризиками є створення і захист цінності. Це підвищує продуктивність, заохочує інновації та підтримує досягнення цілей.

Принципи, викладені нарисунку 2, дають орієнтири щодо особливостей ефективного та результативного управління ризиками, повідомлення про його цінність та пояснення його наміру та призначення. Принципи є основою управління ризиками і повинні враховуватися при встановленні структури і процесів управління ризиками організації. Ці принципи повинні дозволяти організації управляти наслідками невизначеності для своїх цілей.

Рисунок 2 — Принципи



Ефективне управління ризиками вимагає елементіврисунка 2і може бути додатково пояснено наступним чином.

- а) Інтегрована
- Управління ризиками є невід'ємною частиною всіх організаційних заходів.
- б) Структурований і всеосяжний

- Структурований і комплексний підхід до управління ризиками сприяє досягненню послідовних і порівнянних результатів.
- в) Налаштувати
- Структура та процес управління ризиками налаштовані та пропорційні зовнішньому та внутрішньому контексту організації, пов'язаному з її цілями.
- г) Включно
- Належне та своєчасне залучення зацікавлених сторін дозволяє враховувати їхні знання, погляди та сприйняття. Це призводить до підвищення обізнаності та інформованого управління ризиками.
- д) Динамічний
- Ризики можуть виникати, змінюватися або зникати в міру зміни зовнішнього і внутрішнього контексту організації. Управління ризиками передбачає, виявляє, визнає та реагує на ці зміни та події належним та своєчасним чином.
- е) Найкраща доступна інформація
- Вхідні дані в управління ризиками базуються на історичній та поточній інформації, а також на майбутніх очікуваннях. Управління ризиками явно враховує будь-які обмеження і невизначеності, пов'язані з такою інформацією і очікуваннями. Інформація повинна бути своєчасною, чіткою та доступною для відповідних зацікавлених сторін.
- ж) Людські та культурні чинники
- Поведінка і культура людини істотно впливають на всі аспекти управління ризиками на кожному рівні і етапі.
- є) Постійне вдосконалення
- Управління ризиками постійно вдосконалюється завдяки навчанню та досвіду.

5 Фреймворк

5.1 Загальні положення

Метою системи управління ризиками є надання допомоги організації в інтеграції управління ризиками в значущі види діяльності і функції. Ефективність управління ризиками буде залежати від його інтеграції в управління організацією, включаючи прийняття рішень. Для цього потрібна підтримка зацікавлених сторін, зокрема топ-менеджменту.

Розробка фреймворку охоплює інтеграцію, проектування, впровадження, оцінку та вдосконалення управління ризиками в організації. Рисунок 3ілюструє компоненти фреймворку.

Рисунок 3 — Фреймворк

Організація повинна оцінити свої існуючі практики та процеси управління ризиками, оцінити будь-які прогалини та усунути ці прогалини в рамках.

Компоненти фреймворку та спосіб їх спільної роботи повинні бути адаптовані до потреб організації.

5.2 Лідерство та відданість справі
Вищі органи управління та нагляду, у відповідних випадках, повинні забезпечити, щоб управління ризиками було інтегровано в усі організаційні заходи та демонструвало лідерство та відданість шляхом:

- — налаштування та реалізація всіх компонентів фреймворку;
- — видання заяви або політики, яка встановлює підхід до управління ризиками, план або порядок дій;
- — забезпечення виділення необхідних ресурсів для управління ризиками;
- —присвоєння повноважень, відповідальності та підзвітності на відповідних рівнях всередині організації.
- Це допоможе організації:
- — привести управління ризиками у відповідність до його цілей, стратегії та культури;
- —визнавати і вирішувати всі зобов'язання, а також свої добровільні зобов'язання;
- —встановити розмір і вид ризику, які можуть бути прийняті або не прийняті для керівництва розробкою критеріїв ризику, забезпечення їх доведення до організації та її зацікавлених сторін;
- —донести цінність управління ризиками до організації та її зацікавлених сторін;
- —сприяти системному моніторингу ризиків;

- —забезпечити, щоб структура управління ризиками залишалася відповідною контексту організації.

Вище керівництво несе відповідальність за управління ризиками, тоді як органи нагляду несуть відповідальність за нагляд за управлінням ризиками. Органи нагляду часто очікуються або зобов'язані:

- —забезпечити адекватне врахування ризиків при постановці цілей організації;
- —розуміти ризики, що стоять перед організацією в досягненні її цілей;
- — забезпечити впровадження та ефективну роботу систем управління такими ризиками;
- —переконатися, що такі ризики є доцільними в контексті цілей організації;
- —забезпечити належне донесення інформації про такі ризики та управління ними.

5.3 Інтеграція

Інтеграція управління ризиками спирається на розуміння організаційних структур і контексту. Структури відрізняються в залежності від мети, цілей і складності організації. Управління ризиком здійснюється в кожній частині структури організації. Кожен в організації несе відповідальність за управління ризиками.

Управління керує ходом організації, її зовнішніми і внутрішніми відносинами, а також правилами, процесами і практиками, необхідними для досягнення її мети. Управлінські структури переводять напрямок управління в стратегію і пов'язані з нею цілі, необхідні для досягнення бажаних рівнів стійкої ефективності і довгострокової життєздатності. Визначення підзвітності управління ризиками та наглядових ролей в організації є невід'ємними частинами управління організацією.

Інтеграція управління ризиками в організацію є динамічним та ітераційним процесом, і його слід налаштувати відповідно до потреб та культури організації. Управління ризиками має бути частиною, а не окремою від організаційної мети, управління, лідерства та зобов'язань, стратегії, цілей та операцій.

5.4 Дизайн

5.4.1 Розуміння організації та її контексту

При розробці структури управління ризиками організація повинна вивчити і зрозуміти її зовнішній і внутрішній контекст.

Вивчення зовнішнього контексту організації може включати, але не обмежується:

- — соціальні, культурні, політичні, правові, нормативні, фінансові, технологічні, економічні та екологічні фактори, будь то міжнародні, національні, регіональні чи місцеві;
- —ключові рушії та тенденції, що впливають на цілі організації;
- — взаємозв'язки, сприйняття, цінності, потреби та очікування зовнішніх стейкхолдерів;
- —договірні відносини та зобов'язання;
- —складність мереж і залежностей.

Вивчення внутрішнього контексту організації може включати, але не обмежується:

- —бачення, місія та цінності;
- — управління, організаційна структура, ролі та підзвітність;
- —стратегія, цілі та політика;
- —культура організації;
- —стандарти, керівні принципи та моделі, прийняті організацією;
- —можливості, що розуміються з точки зору ресурсів і знань (наприклад, капітал, час, люди, інтелектуальна власність, процеси, системи і технології);
- —дані, інформаційні системи та інформаційні потоки;
- —взаємовідносини з внутрішніми стейкхолдерами з урахуванням їх сприйняття та цінностей;
- —договірні відносини та зобов'язання;
- —взаємозалежності та взаємозв'язки.

5.4.2 Формулювання зобов'язань з управління ризиками
Вищі органи управління та нагляду, де це можливо, повинні продемонструвати та сформулювати свою постійну прихильність до управління ризиками за допомогою політики, заяви або інших форм, які чітко передають цілі організації та її прихильність до управління ризиками. Зобов'язання повинно включати, але не обмежується:

- —мета організації в управлінні ризиками та зв'язки з її цілями та іншими політиками;
- —посилення необхідності інтеграції управління ризиками в загальну культуру організації;
- — керівництво інтеграцією управління ризиками в основні види діяльності та прийняття рішень;
- —повноваження, обов'язки та відповідальність;
- —надання необхідних ресурсів;
- —спосіб вирішення суперечливих цілей;
- —вимірювання та звітність у межах показників діяльності організації;
- —перегляд і вдосконалення.

Зобов'язання щодо управління ризиками повинні бути повідомлені в організації та зацікавленим сторонам, якщо це доречно.

5.4.3 Призначення організаційних ролей, повноважень, обов'язків та підзвітності
Вищі органи управління та нагляду, у відповідних випадках, повинні забезпечити, щоб органи, обов'язки та відповідальність за відповідні ролі щодо управління ризиками були призначені та повідомлені на всіх рівнях організації, і повинні:

- — підкреслити, що управління ризиками є основним обов'язком;
- —визначити осіб, які мають підзвітність та повноваження щодо управління ризиками (власники ризиків).

5.4.4 Розподіл ресурсів
Вищі органи управління та нагляду, у відповідних випадках, повинні забезпечити розподіл відповідних ресурсів для управління ризиками, які можуть включати, але не обмежуються ними:

- —люди, навички, досвід і компетентність;
- — процеси, методи та інструменти організації, які будуть використовуватися для управління ризиками;
- —задокументовані процеси та процедури;
- — системи управління інформацією та знаннями;
- —потреби у професійному розвитку та навчанні.

Організація повинна враховувати можливості та обмеження існуючих ресурсів.

5.4.5 Налагодження комунікації та консультацій
Організація повинна встановити затверджений підхід до комунікації та консультацій з метою підтримки рамок та сприяння ефективному застосуванню управління ризиками. Комунікація передбачає обмін інформацією з цільовими аудиторіями. Консультації також включають в себе надання учасниками зворотного зв'язку з розрахунком на те, що він буде сприяти і формувати рішення або інші заходи. Методи та зміст комунікації та консультацій повинні відображати очікування зацікавлених сторін, де це доречно.

Комунікація та консультації повинні бути своєчасними та забезпечувати збір, узагальнення, узагальнення та обмін відповідною інформацією, якщо це доречно, а також надання зворотного зв'язку та вдосконалення.

5.5 Реалізація
Організація повинна впровадити систему управління ризиками шляхом:

- — розробка відповідного плану з урахуванням часу та ресурсів;
- —визначення того, де, коли і як приймаються різні типи рішень в організації, і ким;
- — модифікація відповідних процесів прийняття рішень, де це необхідно;
- — забезпечення чіткого розуміння та практики організації щодо управління ризиками.

Успішна реалізація фреймворку вимагає залучення та обізнаності зацікавлених сторін. Це дозволяє організаціям чітко вирішувати невизначеність у прийнятті рішень, а також гарантувати, що будь-яка нова або подальша невизначеність може бути врахована в міру її виникнення.

Правильно розроблена та впроваджена структура управління ризиками забезпечить, щоб процес управління ризиками був частиною всієї діяльності в усій організації, включаючи прийняття рішень, і що зміни у зовнішньому та внутрішньому контекстах будуть адекватно зафіксовані.

5.6 Оцінка
Для того щоб оцінити ефективність системи управління ризиками, організація повинна:

- — періодично вимірювати ефективність системи управління ризиками відповідно до її мети, планів реалізації, показників та очікуваної поведінки;
- —визначити, чи залишається вона придатною для підтримки досягнення цілей організації.

5.7 Удосконалення

5.7.1 Адаптація

Організація повинна постійно контролювати та адаптувати структуру управління ризиками для вирішення зовнішніх та внутрішніх змін. При цьому організація може підвищити свою цінність.

5.7.2 Постійне вдосконалення

Організація повинна постійно вдосконалювати придатність, адекватність та ефективність системи управління ризиками та спосіб інтеграції процесу управління ризиками.

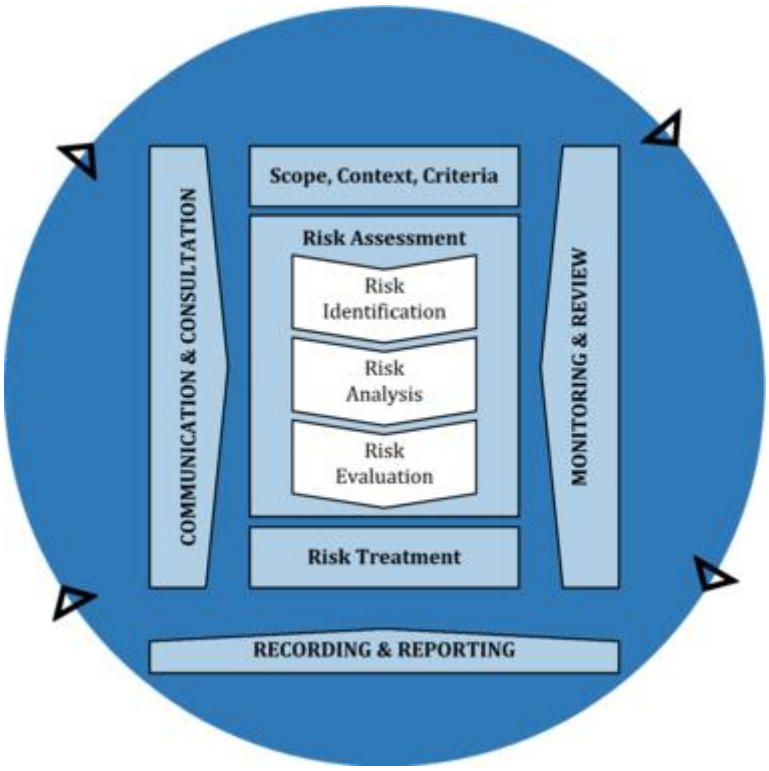
У міру виявлення відповідних прогалин або можливостей поліпшення організація повинна розробляти плани і завдання і призначати їх відповідальним за реалізацію. Після впровадження ці вдосконалення повинні сприяти вдосконаленню управління ризиками.

6 Процес

6.1 Загальні положення

Процес управління ризиками передбачає систематичне застосування політик, процедур і практик до діяльності з комунікації та консультування, встановлення контексту і оцінки, обробки, моніторингу, огляду, реєстрації та звітності про ризики. Цей процес проілюстровано нарисунку 4.

Рисунок 4 — Процес



Процес управління ризиками повинен бути невід'ємною частиною управління і прийняття рішень і інтегрований в структуру, операції і процеси організації. Він може

бути застосований на стратегічному, операційному, програмному або проектному рівнях.

В організації може бути багато застосувань процесу управління ризиками, налаштованих для досягнення цілей та відповідно до зовнішнього та внутрішнього контексту, в якому вони застосовуються.

Динамічний і мінливий характер людської поведінки і культури слід розглядати протягом усього процесу управління ризиками.

Хоча процес управління ризиками часто представляється як послідовний, на практиці він носить ітераційний характер.

6.2 Спілкування та консультації

Метою комунікації та консультацій є допомога відповідним зацікавленим сторонам у розумінні ризику, основи, на якій приймаються рішення, та причин, чому потрібні ті чи інші дії. Комунікація спрямована на підвищення обізнаності та розуміння ризику, тоді як консультація передбачає отримання зворотного зв'язку та інформації для підтримки прийняття рішень. Тісна координація між ними повинна сприяти фактичному, своєчасному, актуальному, точному та зрозумілому обміну інформацією з урахуванням конфіденційності та цілісності інформації, а також прав на конфіденційність фізичних осіб.

Комунікація та консультації з відповідними зовнішніми та внутрішніми зацікавленими сторонами повинні відбуватися в межах та на всіх етапах процесу управління ризиками.

Комунікація та консультації спрямовані на:

- — об'єднати різні галузі знань для кожного етапу процесу управління ризиками;
- —забезпечити належне врахування різних поглядів при визначенні критеріїв ризику та при оцінці ризиків;
- — надавати достатню інформацію для сприяння нагляду за ризиками та прийняттю рішень;
- —формувати почуття інклюзивності та власності серед тих, хто постраждав від ризику.

6.3 Сфера застосування, контекст і критерії

6.3.1 Загальні положення

Метою встановлення обсягу, контексту та критеріїв є налаштування процесу управління ризиками, що дозволяє ефективно оцінювати ризики та адекватно ставитися до ризиків. Сфера застосування, контекст і критерії передбачають визначення масштабів процесу, а також розуміння зовнішнього і внутрішнього контексту.

6.3.2 Визначення сфери застосування

Організація повинна визначити сферу своєї діяльності з управління ризиками.

Оскільки процес управління ризиками може застосовуватися на різних рівнях (наприклад, стратегічному, операційному, програмному, проектному або іншому виді

діяльності), важливо чітко розуміти обсяг, що розглядається, відповідні цілі, які необхідно розглянути, і їх відповідність організаційним цілям.

При плануванні підходу міркування включають:

- —цілі та рішення, які необхідно прийняти;
- —результати, очікувані від кроків, які необхідно зробити в процесі;
- —час, місце розташування, конкретні включення та виключення;
- — відповідні інструменти та методи оцінки ризиків;
- — необхідні ресурси, обов'язки та записи, які потрібно вести;
- —зв'язки з іншими проектами, процесами та видами діяльності.

6.3.3 Зовнішній і внутрішній контекст
Зовнішній і внутрішній контекст - це середовище, в якому організація прагне визначити і досягти своїх цілей.

Контекст процесу управління ризиками повинен встановлюватися з розуміння зовнішнього і внутрішнього середовища, в якій функціонує організація, і повинен відображати конкретне середовище діяльності, до якої повинен бути застосований процес управління ризиками.

Розуміння контексту важливо, тому що:

- —управління ризиками відбувається в контексті цілей і напрямків діяльності організації;
- —джерелом ризику можуть бути організаційні чинники;
- —мета і обсяг процесу управління ризиками можуть бути взаємопов'язані з цілями організації в цілому.

Організація повинна встановити зовнішній і внутрішній контекст процесу управління ризиками шляхом розгляду факторів, зазначених в5.4.1.

6.3.4 Визначення критеріїв ризику
Організація повинна вказати суму і вид ризику, який вона може прийняти, а може і не прийняти, щодо цілей. Він також повинен визначити критерії для оцінки значущості ризику та підтримки процесів прийняття рішень. Критерії ризику повинні бути узгоджені з рамками управління ризиками і налаштовані під конкретну мету і сферу даної діяльності. Критерії ризику повинні відображати цінності, цілі та ресурси організації та узгоджуватися з політикою та заявами щодо управління ризиками. Критерії повинні визначатися з урахуванням зобов'язань організації та думки зацікавлених сторін.

Хоча критерії ризику повинні бути встановлені на початку процесу оцінки ризику, вони є динамічними і повинні постійно переглядатися і змінюватися, якщо це необхідно.

Для встановлення критеріїв ризику слід враховувати наступне:

- —характер і тип невизначеностей, які можуть вплинути на результати і цілі (як матеріальні, так і нематеріальні);

- —як будуть визначені та виміряні наслідки (як позитивні, так і негативні) та ймовірність;
- —фактори, пов'язані з часом;
- —послідовність у використанні вимірювань;
- —як визначається рівень ризику;
- —як будуть враховуватися комбінації та послідовності множинних ризиків;
- —спроможність організації.

6.4 Оцінка ризиків

6.4.1 Загальні положення

Оцінка ризиків - це загальний процес ідентифікації ризиків, аналізу ризиків та оцінки ризиків.

Оцінка ризиків повинна проводитися систематично, ітераційно та спільно, спираючись на знання та погляди зацікавлених сторін. Він повинен використовувати найкращу доступну інформацію, доповнену подальшим запитом у разі потреби.

6.4.2 Ідентифікація ризиків

Метою ідентифікації ризиків є пошук, розпізнавання та опис ризиків, які можуть допомогти або перешкодити організації досягти своїх цілей. Актуальна, доречна та актуальна інформація важлива при виявленні ризиків.

Організація може використовувати цілий ряд методів виявлення невизначеностей, які можуть вплинути на одну або кілька цілей. Слід враховувати наступні фактори, а також взаємозв'язок між цими факторами:

- —матеріальні та нематеріальні джерела ризику;
- —причини і події;
- —загрози та можливості;
- — вразливості та можливості;
- —зміни зовнішнього і внутрішнього контексту;
- —індикатори ризиків, що виникають;
- —сутність і вартість активів і ресурсів;
- —наслідки та їх вплив на цілі;
- —обмеження знань і достовірності інформації;
- —фактори, пов'язані з часом;
- —упередження, припущення та переконання причетних.

Організація повинна виявляти ризики, незалежно від того, знаходяться їх джерела під її контролем чи ні. Слід враховувати, що може бути більше одного типу результатів, які можуть призвести до різноманітних матеріальних або нематеріальних наслідків.

6.4.3 Аналіз ризиків

Метою аналізу ризику є осмислення сутності ризику та його характеристик, включаючи, де це доречно, рівень ризику. Аналіз ризиків передбачає детальний розгляд невизначеностей, джерел ризику, наслідків, ймовірності, подій, сценаріїв, засобів контролю та їх ефективності. Подія може мати кілька причин і наслідків і може вплинути на кілька цілей.

Аналіз ризиків може проводитися з різним ступенем деталізації і складності, в залежності від мети аналізу, наявності і достовірності інформації, наявних ресурсів. Методики аналізу можуть бути якісними, кількісними або їх сукупністю, в залежності від обставин і передбачуваного використання.

Аналіз ризиків повинен враховувати такі фактори, як:

- —ймовірність подій і наслідків;
- —характер і масштаби наслідків;
- —складність і зв'язність;
- —фактори, пов'язані з часом, і волатильність;
- —ефективність існуючих засобів контролю;
- —рівень чутливості та впевненості.

На аналіз ризиків може впливати будь-яка розбіжність думок, упереджень, уявлень про ризик і судженнях. Додатковими впливами є якість використовуваної інформації, зроблені припущення та виключення, будь-які обмеження методів та спосіб їх виконання. Ці впливи повинні бути розглянуті, задокументовані та доведені до осіб, які приймають рішення.

Дуже невизначені події може бути важко оцінити кількісно. Це може бути проблемою при аналізі подій з важкими наслідками. У таких випадках використання комбінації методів, як правило, забезпечує більшу проникливість.

Аналіз ризиків забезпечує внесок в оцінку ризику, в рішення про те, чи потрібно і як лікувати ризик, а також про найбільш відповідну стратегію і методи лікування ризиків. Результати дають уявлення про рішення, де робиться вибір, а варіанти включають різні типи та рівні ризику.

6.4.4 Оцінка ризиків

Метою оцінки ризиків є підтримка прийнятих рішень. Оцінка ризиків передбачає зіставлення результатів аналізу ризиків з встановленими критеріями ризику для визначення того, де потрібні додаткові дії. Це може привести до прийняття рішення про:

- —далі нічого не робити;
- —розглянути варіанти лікування ризиків;
- —провести подальший аналіз, щоб краще зрозуміти ризик;
- —підтримувати існуючі органи управління;
- —переглянути цілі.

Рішення повинні враховувати ширший контекст та фактичні та уявні наслідки для зовнішніх та внутрішніх зацікавлених сторін.

Результат оцінки ризиків повинен бути зафіксований, повідомлений, а потім підтверджений на відповідних рівнях організації.

6.5 Лікування ризиків

6.5.1 Загальні положення

Метою лікування ризиків є вибір і реалізація варіантів усунення ризику.

Лікування ризику включає в себе ітераційний процес:

- — формулювання та вибір варіантів лікування ризиків;
- — планування та впровадження лікування ризиків;
- —оцінка ефективності такого лікування;
- — прийняття рішення про те, чи прийнятний ризик, що залишився;
- —якщо це не прийнятно, приймаючи подальше лікування.

6.5.2 Вибір варіантів лікування ризику

Вибір найбільш відповідного варіанту(ів) лікування ризику передбачає збалансування потенційних вигод, отриманих у зв'язку з досягненням цілей, проти витрат, зусиль або недоліків реалізації.

Варіанти лікування ризику не обов'язково є взаємовиключними або доцільними за будь-яких обставин. Варіанти лікування ризику можуть включати один або кілька з наступних:

- —уникнення ризику шляхом прийняття рішення не починати і не продовжувати діяльність, яка породжує ризик;
- —прийняття або збільшення ризику з метою реалізації можливості;
- —усунення джерела ризику;
- —зміна ймовірності;
- —зміна наслідків;
- —розподіл ризику (наприклад, через договори, купівлю страховки);
- —збереження ризику обґрунтованим рішенням.

Обґрунтування поводження з ризиками є ширшим, ніж виключно економічні міркування, і має враховувати всі зобов'язання організації, добровільні зобов'язання та погляди зацікавлених сторін. Вибір варіантів лікування ризиків повинен проводитися відповідно до цілей організації, критеріями ризику і наявними ресурсами.

При виборі варіантів лікування ризиків організація повинна враховувати цінності, сприйняття та потенційне залучення зацікавлених сторін та найбільш відповідні способи комунікації та консультацій з ними. Хоча вони однаково ефективні, деякі методи лікування ризику можуть бути більш прийнятними для деяких зацікавлених сторін, ніж для інших.

Лікування ризиків, навіть якщо воно ретельно розроблене та впроваджене, може не призвести до очікуваних результатів і може призвести до непередбачених наслідків. Моніторинг та огляд повинні бути невід'ємною частиною впровадження лікування ризиків, щоб забезпечити впевненість у тому, що різні форми лікування стають і залишаються ефективними.

Лікування ризиків також може призвести до нових ризиків, якими необхідно керувати.

Якщо немає доступних варіантів лікування або якщо варіанти лікування недостатньо змінюють ризик, ризик повинен бути зареєстрований і зберігатися під постійним оглядом.

Особи, які приймають рішення, та інші зацікавлені сторони повинні знати про характер і ступінь ризику, що залишився після лікування ризиком. Решта ризику повинна бути задокументована та піддана моніторингу, перегляду та, у відповідних випадках, подальшому лікуванню.

6.5.3 Підготовка та впровадження планів лікування ризиків

Мета планів лікування ризику полягає в тому, щоб вказати, як будуть реалізовані обрані варіанти лікування, щоб домовленості були зрозумілі залученим особам, а прогрес у виконанні плану можна було контролювати. План лікування повинен чітко визначати порядок, в якому слід застосовувати лікування ризику.

Плани лікування повинні бути інтегровані в плани управління і процеси організації, в консультації з відповідними зацікавленими сторонами.

Інформація, надана в плані лікування, повинна включати:

- —обґрунтування вибору варіантів лікування, включаючи очікувані вигоди, які необхідно отримати;
- —ті, хто підзвітний і відповідальний за затвердження і виконання плану;
- —запропоновані дії;
- —необхідні ресурси, включаючи непередбачені обставини;
- —показники ефективності;
- —обмеження;
- —необхідна звітність і моніторинг;
- —коли очікується, що дії будуть здійснені і завершені.

6.6 Моніторинг та огляд

Метою моніторингу та огляду є забезпечення та підвищення якості та ефективності проектування, впровадження та результатів процесів. Постійний моніторинг і періодичний перегляд процесу управління ризиками і його результатів повинні бути запланованою частиною процесу управління ризиками, з чітко визначеними обов'язками.

Моніторинг і огляд повинні проходити на всіх етапах процесу. Моніторинг та огляд включає планування, збір та аналіз інформації, запис результатів та надання зворотного зв'язку.

Результати моніторингу та огляду повинні бути включені до всієї діяльності з управління ефективністю, вимірювання та звітності організації.

6.7 Запис і звітність

Процес управління ризиками та його результати повинні бути задокументовані та повідомлені за допомогою відповідних механізмів. Запис і звітність має на меті:

- — повідомляти про діяльність з управління ризиками та результати в організації;
- —надавати інформацію для прийняття рішень;
- — удосконалювати діяльність з управління ризиками;
- — сприяти взаємодії із зацікавленими сторонами, включаючи тих, хто несе відповідальність та відповідальність за діяльність з управління ризиками.

Рішення, що стосуються створення, збереження та обробки документованої інформації, повинні враховувати, але не обмежуватися ними: їх використання, чутливість до інформації та зовнішній і внутрішній контекст.

Звітність є невід'ємною частиною управління організацією і повинна підвищувати якість діалогу із зацікавленими сторонами та підтримувати вище керівництво та органи нагляду у виконанні їхніх обов'язків. Фактори, які слід враховувати для звітності, включають, але не обмежуються ними:

- — різні зацікавлені сторони та їхні конкретні інформаційні потреби та вимоги;
- —вартість, періодичність і своєчасність складання звітності;
- —спосіб складання звітності;
- —відповідність інформації цілям організації та прийняттю рішень.

Бібліографія

[1]	IEC 31010, *Управління ризиками — Методи оцінки ризиків*