16. За якою формою складається повідомлення про результати ідентифікації ОПН?

17. Який документ повинен бути у суб'єкта господарської діяльності, що свідчить про його турботу за забезпечення безпеки ОПН?

18. Що включають основні напрями механізму реалізації системи управління ризиками на законодавчому рівні?

Тема 3. УПРАВЛІННЯ РИЗИКАМИ. МІЖНАРОДНИЙ СТАНДАРТ ISO 31000:2009

3.1. «П'яти крокова система» оцінки професійних ризиків.

3.2. Міжнародний стандарт ISO 31000:2009.

3.1. **«П'яти крокова система» оцінки професійних ризиків**

У міжнародній практиці поширеним підходом до оцінки професійних ризиків є так звана « П'яти крокова система».

Крок 1. Ідентифікація небезпек, що призводять до ризику. На цьому етапі потрібно розглянути на робочому місці все, що потенційно може спричинити заподіяння шкоди, і визначити працівників, які можуть зазнавати небезпеки.

Крок 2. Оцінювання та «ранжирування» ризиків (їх серйозність, їх імовірність та ін.), розподіл за важливістю.

Крок 3. Визначення превентивних заходів. На цьому етапі необхідно ідентифікувати підходящі заходи для виключення ризиків та управління ними.

Крок 4. Вживання заходів. Реалізація цього кроку полягає у складанні плану реалізації захисних та превентивних заходів (можливо, не всі проблеми можуть бути вирішені негайно), визначенні, хто, що і коли конкретно робить і якими засобами забезпечується виконання запланованих заходів.

Крок 5. Моніторинг та перевірка. Оцінку слід проводити на регулярній основі. Результати оцінки повинні переглядатися при значущих змінах в організації виробництва, а також при нещасних випадках.

Елементи цього підходу містяться в європейських рекомендаціях з оцінки ризику, а також у Методичних вказівках щодо проведення аналізу ризику небезпечних виробничих об'єктів, затверджених постановою Держгіртехнагляду від 10.07.2001 р. № 30.

3.2. Міжнародний стандарт ISO 31000:2009

ISO 31000 призначений для сімейства стандартів, пов'язаних із управлінням ризиками та запропанованих Міжнародною організацією зі стандартизації. Метою ISO 31000:2009 є забезпечення загальних керівних принципів з управління ризиками. ISO 31000 спрямований на забезпечення загальновизнаної парадигми для практиків і компаній, що використовують процеси управління ризиками, щоб замінити безліч існуючих стандартів, методологій та парадигм, які відрізнялися між галузями, з урахуванням питань і регіонів.

У цей час стандарт ISO 31000 включає:

• ISO 31000:2009 – Принципи та Керівництво з впровадження;

• ISO / IEC 31010:2009 – Управління ризиками – методи оцінки ризику[18];

• ISO Guide 73:2009 – Управління ризиками – Словник [19].

ISO 31000 був опублікований як стандарт 13 листопада 2009 р. та надає стандартний підхід щодо здійснення управління ризиками. Переглянуті і узгоджені ISO / IEC Guide 73 було опубліковано в той самий час. Мета ISO 31000:2009 – застосування і адаптація для «будь–яких державних, приватних або громадських підприємств, об'єднань, груп або індивіду».

18. ISO / IEC 31010, Ризик–менеджмент – Техніки оцінки ризику

19. Керівництво ISO 73: 2009, Risk Ризик–менеджмент: Словник

Таким чином, загальна сфера ISO 31000 – в сімействі стандартів управління ризиками – не розроблення для певної групи промисловості системи управління, мається на увазі, швидке забезпечення оптимальної структури практики і керівництва усіх операцій, пов'язаних з управлінням ризиками.

ISO 31000:2009 надає загальні керівні принципи для розробки, впровадження та супроводу процесів управління ризиками у межах всієї організації. Такий підхід до оформлення практики управління ризиками сприятиме найбільш широкому впровадженню компаніями, які вимагають для управління ризиками стандарт, що вміщує декілька систем управління.

У рамках цього підходу до управління ризиками передбачається забезпечення всіх стратегічних, управлінських і оперативних завдань організації на проектах, функцій і процесів, які будуть узгоджені із загальним набором цілей управління ризиками.

Відповідно ISO 31000:2009 призначений для широкої групи зацікавлених осіб, включаючи:

• зацікавлених сторін виконавчого рівня;

• призначенних кураторів групи управління ризиками на підприємстві;

• ризик–аналітиків та співробітників управління;

• лінійних керівників і менеджерів проектів;

• внутрішніх аудиторів;

• незалежних практиків.

Ризик концептуалізації. Однією з ключових змін парадигми є запропонований у ISO 31000 ризик концептуалізації. Відповідно до ISO 31000:2009 і перегляду термінології, поняття «ризик» більше не є «випадковістю або ймовірністю втрати», або «ефектом невизначеності мети». Слово «ризик» тепер може бути використано для позначення як позитивних, так і негативних можливостей.

ISO 31000 – рамковий підхід. Стандарт ISO 31000:2009 був отриманий як заміна існуючому стандарту з управління ризиками – AS/NZS 4360:2004. Стандарт ISO 31000:2009 призначений для системи управління, яка підтримує

розроблення, впровадження, підтримання та покращення процесів управління ризиками.

Здійснення. Мета стандарту ISO 31000 – застосування у рамках існуючих систем управління, формалізація і поліпшення процесів управління ризиками.

Впровадження стандарту ISO 31000 передбачало:

• закриття прогалин при передачі звітності в управлінні ризиками на підприємстві;

• вирівнювання цілей як основ управління з ISO 31000;

• удосконалення механізмів управління системою звітності;

• створення єдиних критеріїв оцінки ризику та методик.

Наслідки. Більшість наслідків прийняття нового стандарту стосуються реорганізації існуючої практики управління згідно з документацією, комунікацією та соціалізацією нової парадигми управління операційних ризиків; на відміну від загальної переорієнтації практики управління в рамках всієї організації. Відповідно, найвищі службові особи управління ризиками організацій, мають бути інформовані про наслідки прийняття стандарту і бути спроможними розробити ефективні стратегії для впровадження стандарту по всьому ланцюжку поставок і комерційних операцій.

Деякі аспекти верхньої підзвітності управління, стратегічного здійснення політики й ефективних структур управління потребують більшої уваги щодо організації, яку раніше використовували як зайве, а тепер – як методологію управління ризиками.

У деяких сферах, що стосуються менеджменту ризиків, зокрема, безпеки та корпоративної соціальної відповідальності, яка може працювати з використанням відносно простих процесів управління ризиками, більше матеріалу необхідно буде змінити, особливо щодо чіткого формулювання політики управління ризиками, формалізації процесів власності ризиків, структурування у рамках процесів і прийняття програми безперервного поліпшення.

Управління ризиками. ISO 31000:2009 передбачає порядок, за яким необхідно працювати із ризиками з урахуванням пріоритетів:

а) уникнення ризиків, вирішивши не починати або не продовжувати діяльність, що призводить до ризику;

б) вилучення або зменшення ризику для того, щоб контролювати можливі наслідки;

в) усунення джерел ризику;

г) зміни ймовірності;

д) зміни наслідків;

е) розподілу ризиків з іншою стороною або сторонами (у тому числі договорів та фінансування ризику);

ж) збереження ризик–обґрунтованого рішення.

Акредитація. ISO 31000 було розроблено з метою сертифікації (2009). Починаючи з березня 2013 року, затверджено тренінги з акредитації та сертифікації щодо ISO 31000. Професійні сертифікати організовані та видаються Академією професійної сертифікації (APC, http://www.apc.org.hk).

Менеджмент ризиків. Впровадження серії стандартів ISO 31000, підготовленої 262 Проектним комітетом «Управління ризиками» Міжнародної організації зі стандартизації (ISO), допоможе виявити і, в умовах повної невизначеності, ефективно управляти ризиками, які впливають на досягнення цілей і діяльність організацій, наприклад, на їх економічну ефективність, ділову репутацію, навколишнє природне середовище, безпеку персоналу і соціальні наслідки. На сьогоднішній день серія ISO 31000 представлена групою стандартів, настановами та технічними звітами, що наведені далі.

ISO 31000:2009 «Менеджмент ризиків. Принципи і керівні вказівки» містить одинадцять принципів і загальні керівні вказівки з ефективного виявлення та управління ризиками, тобто, зовнішніми і внутрішніми факторами і впливами, які додають невизначеності у досягнення цілей організації. Цей стандарт також включає в себе рекомендації з розробки, впровадження та постійного вдосконалення структури, мета якої полягає в інтеграції процесу

управління ризиками в загальну схему управління, формування стратегії, а також планування, управління, процеси, політику, цінності і культуру організації. Положення стандарту ISO 31000: 2009 можуть бути застосовані до будь–якого типу ризику, незалежно від його походження, що має позитивні або негативні наслідки. ISO 31000:2009 може бути використаний в організації в цілому або її окремих частинах і різних видах діяльності, включаючи стратегії і рішення, операції, процеси, функції, проекти, товари, послуги та активи. Сфера застосування стандарту поширюється на будь–які державні та комерційні підприємства, асоціації, групи і фізичні особи. Метою створення ISO 31000: 2009 є гармонізація процесів управління ризиками в існуючих і майбутніх стандартах, а також забезпечення єдиного підходу для підтримки та реалізації вимог стандартів, що стосуються конкретних ризиків і/або галузей промисловості.

ISO Guide 73:2009 «Менеджмент ризиків. Словник» доповнює ICO 31000, забезпечує послідовне розуміння й узгоджений підхід до концепції управління ризиками, містить визначення загальних термінів, пов'язаних з ідентифікацією, аналізом, моніторингом, оцінкою, управлінням ризиком, а також процесами і, власне, менеджментом ризиків. Цей посібник призначено для використання особами, відповідальними за управління ризиками в організаціях, експертів і фахівців, що беруть участь в діяльності ISO і IEC, і розробників національних і галузевих нормативних документів, що стосуються менеджменту ризиків.

ISO/TR31004:2013 «Менеджмент ризиків. Керівництво з впровадження ISO 31000» сприяє ефективному впровадженню ISO 31000 та забезпечує:

- структурований підхід до переходу від існуючої практики управління ризиками до ISO 31000 з гнучкою перспективою адаптації до майбутніх змін;
- роз'яснення базових концепцій ISO 31000 з рекомендаціями та прикладами, адаптованими до індивідуальних потреб користувачів;
- додаткове керівництво за принципами ISO 31000 та основи управління ризиками.

ISO/IEC 31010:2009 «Менеджмент ризиків. Методи оцінки ризиків» був підготовлений 56 Технічним комітетом «Надійність» Міжнародної електротехнічної комісії (IEC) спільно з 262 TC ISO. Цей стандарт доповнює положення ISO 31000.

ISO/IEC 31010 зосереджено на поняттях, процесах і виборі методу оцінки ризиків та забезпечує основу для прийняття рішення про застосування найбільш доцільного підходу для оцінки конкретних ризиків.

У стандарті наведено приклади різних методів оцінки ризику (у тому числі «мозковий штурм», метод Делфі, «попередній аналіз небезпеки», методи HAZOP, HACCP, FMEA, FTA, «дерево прийняття рішень», техніка SWIFT, метод Монте–Карло та ін. – всього 31 метод) і дані посилання на інші міжнародні стандарти, в яких більш докладно описано їх застосування.

Міжнародний стандарт ISO 31000 – Перше видання 2009-11-15.

ISO (International Organization for Standardization – Міжнародна організація зі Стандартизації) є всесвітньою федерацією національних органів по стандартизації (органів-членів ISO). Робота над підготовкою Міжнародних Стандартів виконується, як правило, технічним комітетом ISO. Кожен орган–член ISO, зацікавлений у меті, для якої був створений технічний комітет, має право бути представленим у цьому комітеті. Міжнародні організації, урядові та неурядові, що підтримують зв’язок з ISO, також беруть участь у роботі. ISO також тісно співпрацює з Міжнародною електротехнічною комісією (IEC), ведеться спільна робота з усіх питань електротехнічної стандартизації.

Міжнародні Стандарти складаються відповідно до правил, викладених у Директивах ISO / IEC, Частина 2.

Основною метою технічного комітету є підготовка Міжнародних Стандартів. Проекти Міжнародних Стандартів направляються технічним комітетом органам-членам ISO для голосування. Публікація документа як Міжнародного Стандарту відбувається тільки після схвалення щонайменше 75% голосуючих органів-членів ISO.

Особливу увагу приділено тому, що деякі елементи цього документа можуть бути предметом патентних прав. ISO не повинна бути відповідальною за їх ідентифікацію або всі подібні патентні права.

Стандарт ISO 31000 був підготовлений ISO Technical Management Board Working Group (робочею групою із технічного менеджменту) з управління ризиками.

Організації всіх типів і розмірів стикаються з внутрішніми і зовнішніми чинниками і впливами, через які стає неможливо визначити, як і коли вони досягнуть своїх цілей. Вплив невизначеності на цілі організації визначається як «ризик».

Будь–яка діяльність організації пов’язана з ризиком. Організації управляють ризиком за допомогою його ідентифікації, аналізу та подальшого вирішення щодо обробки з метою задоволення критеріїв ризику. Протягом усього процесу організації здійснючи комунікації та консалтинг із зацікавленими сторонами, управляють та аналізують ризик і засоби управління, які модифікують ризик з метою забезпечення того, що наступна обробка ризику не буде потрібна. Даний Міжнародний Стандарт описує цей систематичний і логічний процес у деталях.

У той час як всі організації управляють ризиком до певної міри, цей Міжнародний Стандарт встановлює деякі принципи, при виконанні яких управління ризиками стає більш ефективним. Міжнародний Стандарт рекомендує організаціям розвивати, впроваджувати та постійно покращувати систему, метою якої є інтеграція процесу з управління ризиками з керівництвом, стратегією і плануванням, управлінням, процесами звітності, політикою, цінностями і культурою.

Ризик-менеджмент можна застосувати до цілої організації, до її майданчиків і рівнів, у будь-який час, а також і до певних функцій, проектів та видів діяльності.

Незважаючи на те що практика ризик-менеджменту розвинулася після тривалого часу і в багатьох галузях для задоволення різних потреб,

впровадження послідовних процесів у рамках всебічної системи може допомогти гарантувати, що ризик управляється ефективно, раціонально і послідовно у всій організації. Загальний підхід, описаний в цьому Стандарті, відбиває принципи та керівництва для управління будь-якою формою ризиків систематичним і прозорим способом для будь-якої галузі і будь-якого контексту.

Кожна певна сфера ризик-менеджменту застосовна до індивідуальних потреб, аудиторії, сприйняття і критеріїв. Тому основною особливістю цього Міжнародного Стандарту є «встановлення контексту» як заходів на початку загального процесу управління ризиками. Встановлення контексту зафіксує цілі організації, умови, за яких вона намагається досягти своїх цілей, зацікавлені сторони і різноманітність критеріїв ризику, кожен з яких допоможе виявити й оцінити природу та складність ризику організації.

Відношення між принципами управління ризиком, системою, в якій воно з'являється і процесом управління ризиками описано в цьому Міжнародному Стандарті, та наведено на рис. 3.1.

Коли система впроваджена і підтримується відповідно до Міжнародного Стандарту, управління ризиками дозволяє організації:

– збільшити ймовірність досягнення цілей;

– підтримувати випереджаюче управління;

– поліпшити фінансову звітність;

– поліпшити обізнаність про необхідність ідентифікувати й обробляти ризик у всій організації;

– поліпшити ідентифікацію можливостей і обробки ризиків;

– відповідати релевантним законодавчим вимогам та регламентам, а також міжнародним нормам;

– поліпшити діяльність управління;

– посилити довіру зацікавлених сторін;

– встановити надійну основу для прийняття рішень і планування;

– поліпшити контроль;

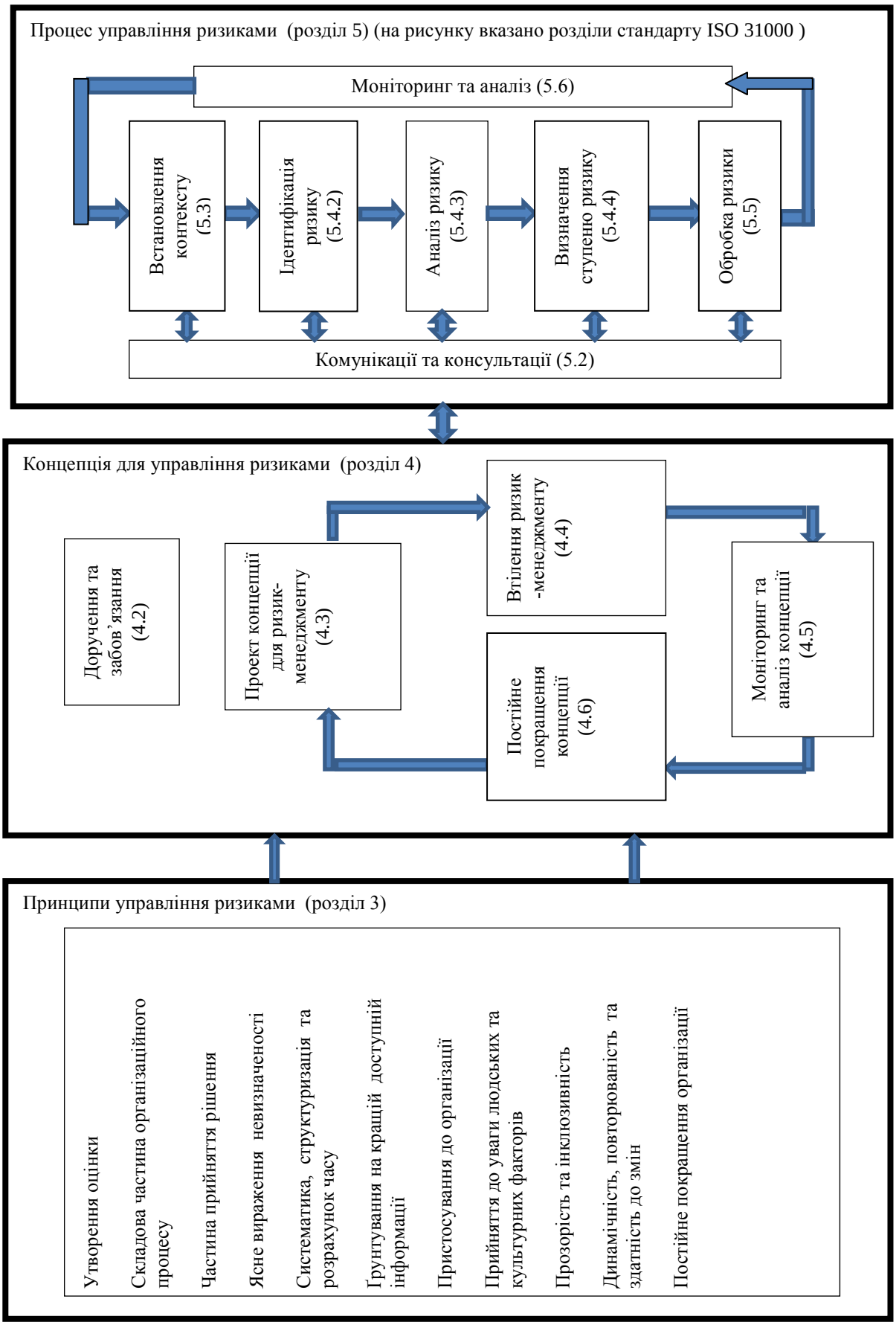

Рисунок 3.1. – Відношення між принципами управління ризиком, системою, в якій воно з'являється і процесом управління ризиками

– ефективно розподілити і використати ресурси для обробки ризику;

– поліпшити оперативну ефективність і результативність;

– поліпшити показники професійної безпеки та здоров'я, а також екологічні показники;

– поліпшити попередження втрат і дії з ліквідації наслідків пригод;

– мінімізувати втрати;

– поліпшити навчання на робочому місці;

– поліпшити працездатність колективу.

Ций Міжнародний Стандарт призначений для задоволення потреб широкого кола зацікавлених сторін, включаючи:

– відповідальних осіб за розвиток політики ризик менеджменту у своїй організації

– відповідальних осіб за забезпечення того, що ризиком ефективно управляють у всій організації або в якійсь певній області, проект або діяльності

– осіб, яким необхідна оцінка продуктивності організації в області управління ризиками

– розробників стандартів, інструкцій, процедур і кодексів правил, які повністю або частково встановлюють, яким чином слід управляти ризиками в контексті даного документа.

Поточні процеси управління багатьох організацій включають компоненти управління ризиками, також багато організацій вже офіційно прийняли формальні процеси управління ризиками для особливих типів ризиків або обставин. У подібних випадках організація може виконувати аналіз існуючих практик і процесів відповідно до цього Міжнародного Стандарту.

У Міжнародному Стандарті використовуються вирази «ризик менеджмент» і «Управління ризиком». Сформульований в загальному сенсі вираз «ризик-менеджмент» належить до «архітектури» (тобто принципів, умов і процесів) ефективного управління ризиками, при цьому вираз «управління ризиком» належить до застосування цієї архітектури до певного ризику. У

стандарті використовуються такі терміни, як прозорість та інклюзивність. Інклюзивність (від лат. Include, що означає включаю, укладаю) – це властивість, пов’язана з включенням живого чи неживого об’єкта в будь-яке явище або їх безліч. Інклюзія означає процес залучення в що–небудь. Синонімом «інклюзивний» є слово «включений», а протилежним за значенням – «ексклюзивний» (або виключений).

Сфера застосування.

Даний Міжнародний Стандарт надає принципи та концептуальні керівництва з управління ризиками, може бути використаний будь–яким державним, приватним чи громадським підприємством, асоціацією, групою компаній або окремою компанією, тому його може офіційно прийняти будь–яка індустрія або сфера діяльності.

Цей Міжнародний Стандарт може бути застосовний протягом всього життєвого циклу організації, а також до широкого спектра діяльності, включаючи стратегії і рішення, операції, процеси, функції, проекти, продукцію, послуги та активи; до будь-якого типу ризиків, незалежно від того, яку природу вони мають, а також позитивні чи негативні наслідки.

Незважуючи на те що цей Міжнародний Стандарт пропонує концептуальні керівні принципи, його метою не є проголошення однаковості ризик-менеджменту у всіх організаціях. При розробці та впровадженні проектів і концепцій ризик-менеджменту потрібно враховувати різні потреби кожної організації, конкретні цілі, контекст, структуру, операції, процеси, функції, проекти, продукцію, послуги та активи, а також практичну роботу.

Передбачається, що цей стандарт буде використовуватися для узгодження процесів з управління ризиками в існуючих і майбутніх стандартах. Він надає загальний підхід сприяння стандартів, в яких йдеться про особливі ризики та/або сфери ризиків, не замінюючи ці стандарти.

Терміни та визначення

Ризик – в*плив невизначеності на цілі*. Вплив розглядається як відхилення від очікуваного – з позитивними або негативними наслідками. Цілі можуть

мати різні аспекти (фінансові; аспекти, що стосуються професійної безпеки та здоров'я; екологічні задачі) і можуть належити до різних рівнів (стратегічний рівень, організаційний, рівень проекту, продукції та процесу).

Невизначеність – це стан, частково відсутність інформації щодо розуміння або знання події, її наслідків або ймовірності.

Ризик-менеджмент – скоординовані дії для того, щоб направляти і контролювати організацію відносно ризиків

Концепція ризик-менеджменту – набір компонентів, що надають основи й організаційні заходи для проектування, впровадження, моніторингу, аналізу і постійного поліпшення ризик-менеджменту у всій організації. Основи включають політику, цілі, доручення і зобов'язання управляти ризиками . Організаційні заходи передбачають планування, відносини, звітність, ресурси, процеси і діяльність. Концепція ризик-менеджменту включена в загальну стратегію організації, оперативну політику і діяльність.

Політика ризик-менеджменту – становище загальних намірів і напрямів організації щодо ризик-менеджменту.

План ризик-менеджменту – схема в складі концепції ризик-менеджменту, що визначає підхід, компоненти менеджменту та ресурси, застосовні до управління ризиками. Компоненти менеджменту зазвичай включають процедури, практики, призначення відповідальних осіб, послідовність і час дій. План ризик-менеджменту може бути застосований до певного продукту, процесу і проекту, а також до частини і цілої організації.

Власник ризику – особа або об'єкт, який несе відповідальні за управління ризиками.

Процес управління ризиками – систематичне застосування політики менеджменту, процедур і практик щодо відношенню щодо комунікації, консалтингу, встановлення контексту, а також ідентифікації, аналізу, оцінки, дослідження, моніторингу та аналізу ризику .

Встановлення контексту – визначення зовнішніх і внутрішніх параметрів, які необхідно взяти до уваги під час управління ризиками, а також встановлення сфери та критеріїв ризику для політики ризик-менеджменту.

Зовнішній контекст – зовнішнє середовище, в якому організація прагне досягти своїх цілей. Зовнішній контекст може включати:

- середовище – культурне, соціальне, політичне, правове, регулятивне, фінансове, технологічне, економічне, природне, конкурентне або міжнародне, національне, регіональне, або локальне;
- ключові рушійні сили і тренди, що впливають на цілі організації;
- відносини із зовнішніми зацікавленими сторонами, їх сприйняття та оцінка.

Внутрішній контекст – внутрішнє середовище, в якому організація прагне досягти своїх цілей. Внутрішній контекст може включати:

- управління, організаційну структуру, ролі та відповідальність;
- політику, цілі, стратегії, що використовуються для досягнення цілей;
- можливості, розуміння у рамках ресурсів та знань (наприклад, фінанси, час, процеси, системи і технології);
- сприйняття та оцінку внутрішніх зацікавлених сторін;
- інформаційні системи, інформаційні потоки, а також процес прийняття рішень (формальних і неформальних);
- відносини з внутрішніми зацікавленими сторонами, їх сприйняття та оцінка;
- культуру організації;
- стандарти, керівництва і моделі, офіційно прийняті організацією;
- форму та обсяг договірних відносин.

Комунікації і консультації – постійний і повторюваний процес, яким управляє організація для того, щоб надати, поділитися або придбати інформацію, а також для того, щоб розпочати діалог із зацікавленими сторонами та іншими щодо управління ризиками. Інформація може стосуватися суті, природи, ймовірності, строгості, оцінки, прийнятності, обробки або інших

аспектів управління ризиками. Консультація – це двосторонній процес інформаційної комунікації між організацією та її зацікавленими сторонами або іншими сторонами з певного питання, прийняття рішення або визначення напряму за конкретною темою. Консультація – це процес, що впливає на рішення краще, ніж повноваження, а також це вхідні дані для прийняття рішення, а не спільне прийняття рішення.

Зацікавлена сторона – особа або організація, яка може вплинути (або на неї можна вплинути, а також відчувати себе під впливом) на рішення або діяльність. Особа, що приймає рішення, може бути зацікавленою стороною.

Оцінка ризику – загальний процес ідентифікації ризику, аналіз ризику і визначення ступеня ризику.

Ідентифікація ризику – процес знаходження, розпізнавання й опису ризику. Ідентифікація ризику включає ідентифікацію джерел ризику, подій, їх причин і потенційних наслідків. Ідентифікація ризику може включати історичні дані, теоретичний аналіз, інформаційні та експертні опції і потреби зацікавлених сторін.

Джерело ризику – елемент, який сам по собі або в комбінації з іншими має внутрішній потенціал для виникнення ризику. Джерело ризику може бути матеріальним або нематеріальним.

Подія – поява або зміна певних обставин. Подія може являти собою одну або багато обставин і може мати декілька причин. Подія може складатися з того, що не відбувається. Іноді подія може належати до термінів «Інцидент» або «Випадковість». Подія без наслідків також може належати до термінів «часткова удача», «випадок», «загроза події», «небезпечне становище».

Наслідок – результат події, що впливає на цілі. Подія може привести до ряду наслідків. Наслідок може бути визначеним або невизначеним і мати позитивний або негативний вплив на цілі. Наслідки можуть бути виражені якісно і кількісно. Початкові наслідки можуть спричинити за собою більш серйозні.

Ймовірність – можливість того, що щось станеться. В термінології ризик-менеджменту слово «ймовірність» використовується для посилання на можливість, що щось станеться, вимірюється і визначається об'єктивно і суб'єктивно, кількісно та якісно, й описується за допомогою загальних термінів або математично (наприклад, ймовірність або частота в цей період часу). Англійський термін «ймовірність» у багатьох мовах не має прямого еквівалента, в той час як термін «можливість» часто використовується. Незважаючи на це в англійській мові «ймовірність» часто інтерпретується як математичний термін. Отже, у термінології ризик-менеджменту використовується «ймовірність», тому цей термін має більш широку інтерпретацію, ніж «можливість».

Структура ризику – **о**пис будь-якої групи ризиків. Група ризиків може містити такі ризики, які належать до цілої організації, частини організації або інших компонентів.

Аналіз ризику – процес розуміння природи ризику і визначення рівня ризику. Аналіз ризику надає основу для визначення ступеня ризику і для вирішення обробки ризику. Аналіз ризику включає оцінку ризику.

Критерії ризику – дані, за якими оцінюється значущість ризику. Критерії ризику засновані на цілях організації, її зовнішньому і внутрішньому контексті. Критерії ризику можуть бути похідними від стандартів, законів, політики та інших вимог.

Рівень ризику – величина ризику, виражена в рамках комбінації наслідків та їх ймовірностей.

Визначення ступеня ризику – процес порівняння результатів аналізу ризику з критеріями ризику для визначення того, чи можна прийняти величину ризику. Визначення ступеня ризику сприяє обробці ризику.

Обробка ризику – процес модифікації ризику. Обробка ризику може включати: обхідний шлях ризику за допомогою рішення не починати або не продовжувати діяльність, яка провокує появу ризику; збереження або збільшення ризику з метою дослідити обставини; видалення джерела ризику;

зміну ймовірності; зміну наслідків; поділ ризику з іншою стороною або сторонами (включаючи контракти і фінансування ризику); збереження ризику при наявності повної інформації. Обробки ризиків, які мають справу з негативними наслідками, іноді приводять до «зменшення ризиків», «усунення ризиків», «уникнення ризиків» і «редукції ризиків». Обробка ризику може створити нові ризики або модифікувати вже існуючі.

Контроль – вимірювання, здатне змінити ризик. Контроль включає будь–який процес, політику, приладу, практика або інші дії, що модифікують ризик. Контроль не завжди впливає на очікуваний або передбачуваний модифікуючий ефект.

Залишковий ризик – ризик, який залишається після обробки ризику. Залишковий ризик може містити в собі не ідентифікований ризик. Залишковий ризик може також називатися «збережений ризик».

Моніторинг – постійна перевірка, нагляд, критичне спостереження або визначення статусу ідентифікації зміни показників та очікуваних результатів. Моніторинг може бути застосований до концепції ризик-менеджменту, процесу ризик-менеджменту, ризику або контролю.

Аналіз – процес для визначення придатності, адекватності та ефективності виконаних дій для досягнення встановлених цілей. Аналіз може бути застосований до концепції ризик-менеджменту, процесу ризик-менеджменту, ризику або контролю.

Принципи ризик-менеджменту.

Для того щоб управління ризиками було ефективним, організація повинна на всіх рівнях відповідати принципам, перерахованим нижче.

а) *Ризик-менеджмент створює і захищає оцінки.*

Ризик-менеджмент сприяє очевидному досягненню цілей і поліпшенню показників, наприклад, здоров’я та безпеки людини, захисту, відповідності законодавству та регламенту, публічного визнання, захисту навколишнього середовища, якості продуктів, проектного управління, ефективності діяльності, керівництва та репутації.

б) *Ризик-менеджмент – це складова частина всіх організаційних процесів.*

Ризик-менеджмент – є не автономною діяльністю, вона не відокремлена від основної діяльності та процесів організації. Ризик-менеджмент – це частина відповідальності управління і складова частина всіх організаційних процесів, включаючи стратегічне планування та управління процесами проектів і змін.

в) *Ризик-менеджмент є частиною прийняття рішення.*

Ризик-менеджмент допомагає особам, які приймають рішення, зробити правильний вибір, розставити пріоритети і визначити альтернативні курси дій.

г) *Ризик-менеджмент ясно відображає невизначеність*

Ризик-менеджмент враховує невизначеність, природу цієї невизначеності та спосіб їх вираження.

д) *Ризик-менеджмент систематизований, структурований і погоджений за часом.*

Систематичний, структурований і погоджений за часом підхід до ризик-менеджменту сприяє ефективності, а також послідовним, порівняльним достовірним результатам.

е) *Ризик-менеджмент заснований на кращій доступній інформації.*

Вхідні дані для процесу управління ризиками засновані на інформаційних ресурсах, таких, як історичні дані, досвід, зворотний зв’язок зацікавлених сторін, спостереження, прогнози і вислови експертів. Однак особи, які приймають рішення, повинні бути інформовані і брати до уваги будь–які обмеження в даних або використанні моделювання, а також можливість розбіжності думок експертів.

ж) *Ризик-менеджмент особливий для кожної організації.*

Ризик-менеджмент сконцентрований на зовнішньому і внутрішньому контексті організації та структурі ризику.

и) *Ризик-менеджмент враховує людські та культурні фактори.*

Ризик менеджмент розпізнає потенціал, сприйняття та наміри зовнішніх і внутрішніх зацікавлених сторін, які можуть сприяти або заважати досягненню цілей організації.

к) *Ризик-менеджмент володіє транспарентністю та інклюзивністю.*

Відповідне і правильне за часом залучення зацікавлених сторін, зокрема, осіб, які повинні приймати рішення на всіх рівнях організації, гарантує, що ризик-менеджмент залишається релевантним і оновленим. Залучення також дозволяє зацікавленим сторонам бути відповідно представлено й усвідомлювати, що їхні погляди прийняті до уваги при визначенні критеріїв ризику.

л) *Ризик-менеджмент – це динамічний, повторюваний і здатний до змін процес процес де* трапляються внутрішні і зовнішні події, змінюється контекст і знання, мають місце моніторинг та аналіз, виникають нові ризики, отже щось змінюється, а інше зникає. Тому ризик-менеджмент реагує на зміни.

м) *Ризик-менеджмент сприяє постійному поліпшенню організації.*

Організації повинні розвивати і впроваджувати стратегії для поліпшення розвитку їх ризик-менеджменту на ряду з іншими аспектами організації.
Додаток А стандарту ISO 31000 пропонує подальші поради організації з метою зробити управління ризиками більш ефективним.

Концепція

Загальні положення. Успіх менеджменту ризиків залежатиме від ефективності управлінської концепції, що надає основи й угоди, які впроваджуються в організацію на всіх її рівнях. Концепція робить внесок в ефективний ризик–менеджмент шляхом застосування його процесів на різних рівнях і в певних контекстах всередині організації. Така система дає гарантію того, що про інформацію, зібрану під час реалізації процесів ризик-менеджменту, був зроблений доцільний звіт, її покладено в основу прийняття рішень, і це на неї спираються на всіх відповідних організаційних рівнях. Цей

пункт описує невід'ємні компоненти ризик-менеджменту, і те, як вони взаємодіють у повторюваному середовищі, як це показано в рис. 3.2.

Рисунок 3.2. – Взаємозв'язки між компонентами концепції ризик-менеджменту

Мета цієї концепції – не припис до системи менеджменту, а скоріше допомога організації у процесі інтеграції ризик-менеджменту в загальну систему менеджменту.

Таким чином, організації повинні освоїти компоненти концепції для власних потреб. Якщо існуючі практики і процеси управління всередині організації включають компоненти ризик-менеджменту, або якщо організація вже застосовує формальні процеси ризик-менеджменту для певних типів

ризику, все це має бути проаналізовано з критичної точки зору й оцінено щодо цього Міжнародного Стандарту, включаючи інформацію яка міститься у його Додатку А, щоб переконатися в їх доцільності та ефективності.

Доручення та зобов'язання

Введення в ризик-менеджмент і безперервна гарантія його ефективності потребують сильної і виправданої прихильності з боку керівництва організації, а також: доручень та зобов'язань; розробки системи для ризик-менеджменту; розуміння організації та контексту, в якому вона функціонує; встановлення політики ризик-менеджменту; звітності; інтеграції в процеси організації; ресурсів; встановлення внутрішньої комунікації та механізму звітності; встановлення зовнішньої комунікації та механізму звітності; постійного поліпшення концепції; застосування ризик-менеджменту на практиці; застосування системи ризик-менеджменту на практиці; застосування на практиці процесів ризик-менеджменту; моніторингу та оцінки концепції ризик-менеджменту; стратегічного і ретельного планування для досягнення прихильності на всіх рівнях. Керівництву необхідно:

- визначити та затвердити політику ризик-менеджменту;
- бути впевненим у тому, що рівень культури всередині організації та політики ризик-менеджменту відповідають один одному;
- визначити показники ефективності ризик-менеджменту, що відповідають показниками ефективності організації;
- порівняти цілі ризик-менеджменту з цілями і стратегіями організації;
- бути впевненим у своєму відповідно до юридичних та нормативних питань;
- розподілити відповідальності й обов'язок на всіх рівнях організації;
- дати гарантію того, що ресурси, необхідні для ризик-менеджменту, були розподілені;
- донести до всіх зацікавлених сторін переваги ризик-менеджменту;

- бути впевненим у тому, що концепція ризик-менеджменту і раніше залишається доцільною.

Проект концепції ризик-менеджменту

Розуміння організації та її контексту. Перед початком розробки і впровадження концепції ризик-менеджменту важливо оцінити й зрозуміти як зовнішній, так і внутрішній контекст організації, оскільки вони можуть значною мірою вплинути на розробку концепції. Оцінка зовнішнього контексту організації може включати (але не обмежуватися):

а) соціальне і культурне, політичне, законодавче, нормативне, фінансове, технологічне, економічне, природне і конкурентне середовище, як міжнародне, так і національне, регіональне та місцеве;

б) ключові рушійні сили і напрями, що впливають на цілі організації;

в) відносини із зовнішніми зацікавленими сторонами, їх перспективи та цінності.

Оцінка внутрішнього контексту організації передбачає (але не обмежується):

- правління, організаційну структуру, посади та обов'язки;
- політику, цілі та стратегії, яких необхідно досягти;
- можливості – ресурси та знання (наприклад капітал, час, людські ресурси, процеси, системи і технології);
- інформаційні системи, інформаційні потоки і процеси прийняття рішень (формальні і неформальні);
- відносини з внутрішніми зацікавленими сторонами, їх перспективи та цінності;
- культуру всередині організації;
- стандарти, керівництва та моделі, прийняті всередині організації;
- форму й об'єм контрактних відносин.

Встановлення політики ризик-менеджменту. Політика ризик-менеджменту повинна ясно відображати цілі та прихильність організації щодо ризик-менеджменту і відповідати таким критеріям:

- прагненню організації до обробки ризиків;
- зв’язків між цілями організації і політиками, в тому числі політиці ризик-менеджменту;
- відповідальності і обов’язків з обробки ризиків;
- способу, до якого вдаються у вирішенні конфлікту інтересів;
- зобов’язань щодо забезпечення необхідними ресурсами того, хто відповідає за управління ризиками;
- тому, як буде вимірюватися і підтверджуватися ефективність ризик-менеджменту;
- зобов’язань щодо постійної оцінки та поліпшення політики ризик-менеджменту і концепції, або внаслідок якої-небудь події, а також під час зміни якихось обставин, тому що політика ризик-менеджменту повинна управлятися належно.

Відповідальність. Організація повинна дати гарантію того, що існує відповідальність, уповноважені та належний рівень компетенції для управління ризиками, включаючи впровадження та підтримку процесів ризик-менеджменту, а також гарантію доцільності, ефективності та достатності будь-яких методів управління. Цьому може сприяти:

- ідентифікація власників ризику, які відповідальні та уповноважені управляти ризиками;
- ідентифікація осіб, відповідальних за розвиток, застосування і підтримання концепції управління ризиками;
- ідентифікація інших відповідальностей щодо процесів ризик-менеджменту, покладених на персонал усіх рівнів всередині організації ризик-менеджменту;
- встановлення заходів ефективності, а також зовнішніх та/або внутрішніх процесів підтвердження та розгляду керівництвом;
- гарантія визнання на всіх відповідних рівнях.

Інтеграція в процеси організації. Ризик-менеджмент має бути впроваджений у всі практики організації доти, доки він має доречний, ефективний і достатній характер. Процеси ризик-менеджменту повинні стати частиною процесів організації, а ніяк не стояти осторонь від них. Зокрема, ризик-менеджмент має бути впроваджений у політику розвитку, оцінку бізнес- і стратегічного планування, а також у процеси управління змінами.

У всій організації повинен існувати план ризик-менеджменту з метою гарантії того, що політика ризик-менеджменту застосовується до всіх процесів і практик цієї організації. План ризик-менеджменту може бути інтегрований в інші плани організації, наприклад, у стратегічний план.

Ресурси. Організація повинна розподілити необхідні для ризик-менеджменту ресурси. Мають бути розглянуті такі аспекти:

- людські ресурси, навички, досвід і конкурентоспроможність;
- ресурси, необхідні для кожного кроку процесу ризик-менеджменту;
- процеси організації, методи і засоби обробки ризиків;
- документовані процеси та процедури;
- системи менеджменту інформації та знань;
- навчальні програми.

Встановлення внутрішньої комунікації і звітного механізму. Організація повинна встановити внутрішню комунікацію і механізми звітності, для того щоб підтримати процеси контролю і володіння ризиками. Ці механізми повинні давати такі гарантії:

- ключові компоненти концепції ризик-менеджменту і будь-яких подальших модифікацій управляються належно;
- існує зрозуміла система внутрішньої звітності щодо концепції, її ефективності та результатів;
- необхідна інформація, отримана під час застосування ризик-менеджменту, доступна в будь-який час і на відповідних рівнях;
- існують процеси консультації з внутрішніми зацікавленими сторонами.

Механізми повинні, там де необхідно, включати процеси щодо об’єднання інформації за ризиками з безлічі ресурсів, а також враховувати секретність такої інформації.

Встановлення зовнішньої комунікації і звітного механізму. Організація повинна розробити та впровадити план того, як буде відбуватися комунікація із зовнішніми зацікавленими сторонами. Він повинен включати:

- залучення відповідних зовнішніх зацікавлених сторін і гарантію ефективного обміну інформацією;
- систему зовнішньої звітності, щоб відповідати юридичним, нормативним і урядовим вимогам;
- надання відгуків з комунікацій та консалтингу;
- використання комунікації як методу створення атмосфери довіри всередині організації;
- комунікацію із зацікавленими сторонами в разі виникнення кризи або нештатної ситуації.

Механізми повинні, включати процеси щодо об’єднання інформації за ризиками з безлічі ресурсів, як і внутрішніх комунікаціях, а також брати до уваги секретність такої інформації.

Впровадження ризик-менеджменту

Впровадження концепції для управління ризиками. В процесі впровадження концепції організації з управління ризиками ця організація повинна:

- визначити відповідні часові рамки і стратегії для впровадження концепції;
- застосовувати політику ризик-менеджменту і його процеси до процесів всередині організації;
- відповідати юридичним і нормативним вимогам;
- дати гарантію того, що процес прийняття рішень, включаючи розробку та постановку цілей, відповідає результатам процесів ризик-менеджменту;
- проводити ознайомлювальні та навчальні семінари;

- повідомляти зацікавленим сторонам, що концепція ризик-менеджменту залишається доцільною.

Впровадження процесів з управління ризиками. Ризик-менеджмент має бути впроваджений при повній гарантії того, що його процеси, застосовуються відповідно до плану ризик-менеджменту на всіх відповідних рівнях і позиціях організації як частина його практик і процесів.

Моніторинг та аналіз концепції

Для того щоб дати гарантію, що ризик-менеджмент ефективний і продовжує підтримувати продуктивність організації, така організація повинна:

- Вимірювати ефективність ризик-менеджменту щодо показників, які періодично аналізуються на відповідність вимогам;
- Час від часу вимірювати зріст відносно і окремо від плану ризик-менеджменту;
- Періодично з'ясовувати, чи відповідають по колишньому концепція, політика і план ризик-менеджменту вимогам, враховуючи внутрішній і зовнішній контекст організації;
- Вести звіт про ризики і зростанні відповідно до плану ризик-менеджменту, а також про тому, як дотримується політика ризик-менеджменту;
- Аналізувати ефективність концепції ризик-менеджменту.

Постійне поліпшення концепції. Засновані на результатах моніторингу та оцінки повинні прийматися рішення щодо поліпшення концепції ризик-менеджменту, його політики та плану. Такі рішення повинні привести до поліпшення управління ризиками всередині організації та загальної культури управління ризиками.

Процес

Загальні положення. Процеси ризик-менеджменту мають бути:

– невід'ємною частиною менеджменту;
– впроваджено в культуру і практику;
– пристосовані до бізнес–процесів організації.

Процес ризик-менеджменту показаний на рис. 3.3.

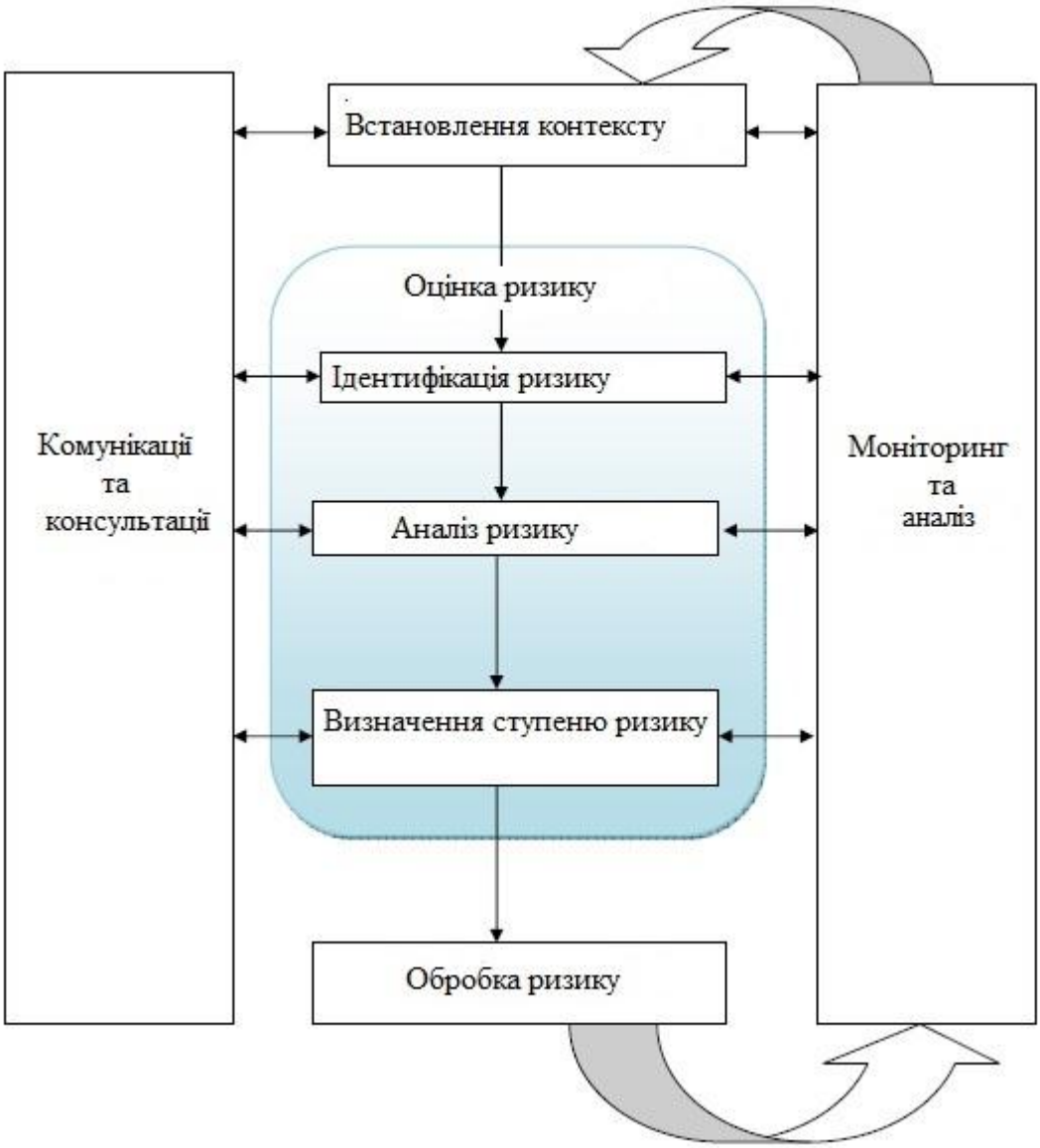

Рисунок 3.3 – Процес ризик-менеджменту

Комунікації та консультації. Комунікації і консультації із зовнішніми і внутрішніми зацікавленими сторонами повинні відбуватися на всіх стадіях процесу управління ризиками. Тому плани щодо комунікації та консультації мають бути розроблені ще в початковій стадії. Вони повинні висвітлювати питання, що стосуються ризиків безпосередньо, їх причин, наслідків (якщо такі відомі), і заходів, яких було вжито з метою обробки такого ризику. Ефективні зовнішні та внутрішні комунікації і консультації повинні давати гарантію що ті, хто відповідальні за процес управління ризиком, і зацікавлені сторони

усвідомлюють підстави для прийняття рішень і причини, того, чому потрібні певні дії.

Консультаційний підхід всередині команди передбачає:

- комунікації і консультації; моніторинг та аналіз;
- оцінку ризику;
- встановлення контексту;
- визначення ступеня ризику;
- аналіз ризику;
- ідентифікацію ризику;
- обробку ризику;
- допомогти в належному встановленні контексту;
- гарантувати, що інтереси зацікавлених сторін зрозумілі і що з ними рахуються;
- гарантувати, що ризики належним чином ідентифіковані;
- зводити різні сфери експертних знань воєдино для аналізу ризиків;
- гарантувати те, що при визначенні критеріїв ризику та їх оціненні, розглядаються різні точки зору;
- забезпечити підтвердження і підтримку плану обробки;
- підвищити доцільність управління змінами під час процесу ризик-менеджменту;
- розробити доцільний план внутрішньої і зовнішньої комунікації.

Комунікації і консультації із зацікавленими сторонами важливі, оскільки вони дають судження про ризик, засновані на їх власному сприйнятті ризику. Ці сприйняття можуть змінитися через різницю в цінностях, потребах, припущеннях, поняттях і очікуваннях зацікавлених сторін. Оскільки їхні погляди можуть істотно вплинути на прийняті рішення, сприйняття зацікавлених сторін, повинно бути ідентифіковано, документовано, і повинно прийматися до уваги при прийнятті рішень.

Комунікації і консультації повинні сприяти обміну достовірною, важливою, точною і зрозумілою інформацією, враховуючи конфіденційні та особисті аспекти її цілісності.

Встановлення контексту

Загальні положення. Встановлюючи контекст, організація ясно формулює свої цілі, визначає зовнішні і внутрішні параметри, які будуть прийняті до уваги при управлінні ризиками, а також встановлює сферу розповсюдження і критерії ризиків для решти процесів. У той час як багато з цих параметрів подібні до тих, які були розглянуті при розробці концепції ризик-менеджменту при встановленні контексту для процесу управління ризиками вони повинні бути розглянуті детально, оскільки належать до процесу управління в сфері конкретного ризику.

Встановлення зовнішнього контексту. Зовнішній контекст – це зовнішнє середовище, в якому організація прагне досягти своїх цілей.

Розуміння зовнішнього контексту важливо для гарантії того, що цілі та очікування зовнішніх зацікавлених сторін будуть розглянуті при розробці критеріїв ризику. Він заснований на контексті всієї організації, але з певними тонкощами у вигляді юридичних і нормативних вимог, сприйняттях зацікавлених сторін та інших аспектах ризику, природних для сфери застосування процесів ризик-менеджменту.

Зовнішній контекст може включати але не бути обмеженим (див. стор.131).

Встановлення внутрішнього контексту. Внутрішній контекст – це внутрішнє середовище, в якому організація прагне досягти своїх цілей.

Процес ризик-менеджменту повинен відповідати культурі, процесам, структурі та стратегіям організації. Внутрішній контекст це щось, що може вплинути зсередини на те, як організація буде управляти ризиками. Він повинен бути встановлений, оскільки:

а) ризик-менеджмент поданий у контексті цілей організації;

б) цілі та критерії певного проекту, процесу або діяльності повинні

розглядатися у світлі цілей організації загалом;

в) деякі організації не можуть визначити можливості для досягнення їх стратегічних, проектних або бізнес-цілей, і це не якнайкраще відбивається на активності, довірі, надійності та цінності організації.

Необхідно розуміти, що таке внутрішній контекст (див. стор. 131).

Встановлення контексту процесу управління ризиками. Повинні бути встановлені цілі, стратегії, сфера застосування і параметри діяльності організації, або тих частин організації, в яких застосовується процес ризик-менеджменту. Менеджмент ризиків повинен проводитися з розглядом необхідності узгодження ресурсної бази, що використовується при обробці ризику.

Необхідні ресурси, обов'язки та уповноважені, записи, які повинні вестися, також необхідно визначити. Контекст процесу ризик-менеджменту буде різнитися зважаючи на потреби організації. Він може включати (але не бути обмеженим):

- визначення цілей і завдань заходів з ризик-менеджменту;
- визначення відповідальностей щодо процесу в ході заходів ризик-менеджменту;
- визначення області застосування, так само як і глибини і ширини заходів щодо ризик-менеджменту, в тому числі необхідні включення і виключення;
- визначення заходів, процесів, функцій, проектів, продукції, послуг або активів щодо часу і розташування;
- визначення взаємовідносин між певним проектом, процесом або діяльністю та іншими проектами, процесу або діями організації;
- визначення методологій оцінки ризиків;
- визначення методу, яким буде оцінюватися ефективність управління ризиком;
- ідентифікацію та встановлення рішень, які необхідно прийняти;

- ідентифікацію, визначення сфери застосування, або складання необхідних досліджень і ресурсів, необхідних для таких досліджень.

Увага до тих чи інших факторів може гарантувати, що застосовуваний процес ризик-менеджменту відповідає обставинам, що склалися, організації і ризикам, що гальмують здійснення організацією її цілей.

Визначення критеріїв ризику. Організація повинна визначити критерії для використання в процесі оцінки значущості ризику. Критерії повинні відображати цінності, цілі і ресурси організації. Деякі критерії можуть бути введені або витягнуті з юридичних і нормативних або ж інших вимог, яких дотримується організація.

Критерії ризиків повинні відповідати політиці ризик-менеджменту організації, мають бути визначені на початку процесу ризик-менеджменту і постійно оновлюватися.

При визначенні критеріїв ризику необхідно розглянути такі фактори:

- природу і тип причин та наслідків, які можуть виникнути, і те, як вони вимірюватимуться;
- як буде визначена ймовірність;
- часові рамки ймовірності та / або наслідків;
- як буде визначено рівень ризику;
- погляди зацікавлених сторін;
- рівень, на якому ризик стає допустимим або прийнятним;
- чи повинні розглядатися комбінації множинних ризиків, і якщо так, то як і які комбінації мають бути розглянуті.

Оцінка ризику

Загальні положення. Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ступеня ризику. ISO/IEC 31010 надає керівництво з техніки оцінення ризику.

Ідентифікація ризику. Організація повинна визначити джерело ризику, сфери його впливу, ризикові випадки (включаючи зміну обставин), їх причини, а також їх потенційні наслідки.

Мета цього кроку – скласти вичерпний список ризиків, заснований на тих ризикових випадках, які можуть створити підґрунтя для збільшення можливостей, запобігання, погіршення, скорочення досягнення цілей.

Важливо ідентифікувати ризики, пов'язані з втраченою можливістю. Вичерпна ідентифікація критично важлива, оскільки ризик, який не був ідентифікований на цій стадії, не буде включений у подальший аналіз.

Ідентифікація повинна охоплювати всі ризики (незалежно від того, чи знаходиться їх джерело під контролем організації, чи ні), навіть якщо джерело ризику або його причина неочевидні.

Ідентифікація ризику повинна включати перевірку ланцюгової реакції деяких визначених наслідків, включаючи каскадний ефект і сумарні дії. Вона також має розглядати широкий спектр наслідків, навіть якщо джерело ризику або його причина неясні. Поряд з ідентифікацією можливих наслідків необхідно розглядати можливі причини і сценарії, які можуть вказати на приблизні наслідки. Усі значущі причини мають бути прийняті до уваги.

Організація повинна застосовувати інструменти і техніки ідентифікації ризиків, які відповідають її цілям і можливостям, а також ризикам, з якими вона зіткнулася.

Відповідна та актуальна інформація дуже важлива при ідентифікації ризиків. Вона по можливості повинна включати в себе і загальну інформацію. Працівники, які володіють відповідними знаннями, повинні бути залучені до процесу ідентифікації ризиків.

Аналіз ризику. Щоб проаналізувати ризик, необхідно прийти до його розуміння. Аналіз ризику надає входи для оцінки ступеня ризику й обговорень з питань необхідності проведення обробки ризику, а також стратегій і методів його обробки. Аналіз ризику може також надавати входи для прийняття рішень щодо ризиків різних типів і рівнів, особливо тих, де стоїть вибір.

Аналіз ризиків включає в себе розгляд причин і джерел ризику, його позитивних і негативних наслідків та ймовірності виникнення цих наслідків. Фактори, що впливають на наслідки та ймовірність, й повинні бути визначені. Ризик аналізується шляхом визначення наслідків та їх ймовірності, а також інших супутніх ризику характеристик. Ризиковий випадок може спричинити множинні наслідки і відбитися на безлічі цілей.

Існуючі методи управління, їх ефективність і достатність також необхідно врахувати.

Те, як відбиваються наслідки і ймовірність і те, як вони комбінуються при визначенні рівня ризику, – має відображати тип ризику, доступну інформацію і мету, для якої використовується вихід процесу обробки ризику. Все це повинно відповідати критеріям ризику. Також важливо враховувати незалежність різних ризиків і їх джерел.

Достовірність при визначенні рівня ризику та його чутливості за попередніми умовами і припущеннями повинна бути невід'ємною частиною аналізу і доводитися до відомості тих, хто приймає рішення і, відповідно, зацікавлених осіб. Такі фактори, як розбіжності в думках експертів, невпевненості, доступність, якість, кількість і постійна актуальність інформації, чи обмеження при моделюванні повинні бути чітко сформульовані і виведені на перший план.

Аналіз ризику може бути зроблений з різними видами деталей, залежно від ризику, мети аналізу, та інформації, даних і доступних ресурсів. Аналіз може бути якісним, наполовину кількісним або кількісним, або їх поєднанням, залежно від обставин.

Наслідки і ймовірність їх виникнення можуть бути визначені шляхом моделювання результатів події або набором подій, або екстраполяцією від експериментальних досліджень або на основі наявних даних.

Наслідки можуть бути виражені у вигляді матеріальних і нематеріальних наслідків. У деяких випадках, більш ніж однієї числової величини або дескриптора, обов'язково зазначати наслідки і ймовірність їх для різних часів,

місць, груп або ситуацій. Наслідки і їх вірогідність можуть бути визначені моделюванням результатів ризикового випадку або випадків, або екстраполяцією експериментальних досліджень або доступних даних.

Визначення ступеня ризику. Мета визначення ступеня ризику полягає у прийнятті рішень з його аналізу, заснованого на тому, які ризики необхідно обробити, і пріоритетності у застосуванні обробки.

Визначення ступеня ризику передбачає порівняння рівня, виявленого в процесі аналізу ризику, з критеріями ризику, визначеними при встановленні контексту.

Необхідність обробки розглядається на підставі такого порівняння. Рішення повинні враховувати більш широкий контекст ризику і включати в себе розгляд поміркованості ризику, що має відношення до сторін, за винятком тих організацій, які від ризику тільки виграють. Рішення повинні прийматися відповідно до законодавчих, нормативних та інших вимог.

У деяких обставинах оцінка ступеня ризику може призвести до того, що буде необхідний додатковий аналіз. Також оцінка ступеня ризику може привести до рішення не обробляти ризик, а підтримувати його в існуючому стані.

На таке рішення може вплинути ставлення організації до ризиків та встановленя для нього критеріїв.

Обробка ризику

Загальні положення. Обробка ризику включає в себе одну або більше позицій модифікації ризиків і застосування таких модифікацій.

Як тільки вони були застосовані, методи обробки надають або модифікують способи управління.

Обробка ризику включає циклічний процес:

- оцінки обробки ризику;
- прийняття рішення про допустимість існуючого ризику;
- генерації нового способу обробки, якщо ризик недопустимий;

- оцінки ефективності обробки.

Способи обробки ризику необов’язково виключають один одного і необов’язково доречні за всіх обставин.

Способи можуть включати:

а) уникнення ризику шляхом рішення не починати або не продовжувати діяльність, що призвела до ризику;

б) взяття на себе ризику або підвищення його рівня, щоб використати можливість;

в) знищення джерела ризику;

г) зміну ймовірності;

д) зміну наслідків;

е) розподіл ризику з іншою стороною або сторонами (включаючи контракти і фінансування ризику);

ж) обґрунтоване рішення прийняття на себе страхового ризику.

Вибір опцій обробки ризику. Вибір найбільш доцільної опції обробки ризику передбачає балансування цін і спроб впровадження щодо вигод, згідно з юридичними, нормативними та іншими вимогами, такими як соціальна відповідальність і захист навколишнього середовища. Рішення повинні також врахувати ризики, пов’язані з такою оборобкою, яка не буде виправдана з економічної точки зору, наприклад важкі ризики (що спричиняють вкрай негативні наслідки), але рідкісні (з низькою ймовірністю).

Деякі опції обробки можуть бути прийняті до уваги і здійсненні спільно або окремо. Організація, як правило, може отримати вигоду при застосуванні сукупності опцій обробки ризиків.

При виборі опції обробки ризику організація має враховувати цінності та сприйняття зацікавлених сторін, і найбільш відповідні способи комунікації з ними. Там, де опції обробки ризику можуть вплинути на ризики поза організацією або у відносинах із зацікавленими сторонами, це також потрібно враховувати. І хоча опції обробки ризику однаково ефективні, деякі з них можуть бути більш допустимими для деяких зацікавлених сторін, ніж інші.

План з обробки ризиків повинен ясно ідентифікувати пріоритетний порядок, в якому застосовуватимуться окремі опції обробки ризику.

Обробка ризику сама по собі може спричиняти ризик. Значним ризиком може бути помилка або неефективність заходів обробки ризиків. Моніторинг має бути невід'ємною частиною плану з обробки ризику як гарантія того, що вживаються ефективні заходи.

Обробка ризику може спричинити вторинні ризики, які також необхідно розглядати, обробляти, за якими необхідно стежити й аналізувати. Такі вторинні ризики повинні бути включені в той самий план з обробки ризиків, як і початкові ризики, таким чином немає ніякої необхідності в обробці такого ризику як нового. Зв'язок між двома ризиками необхідно ідентифікувати і підтримувати.

Підготовка і впровадження планів обробки ризику. Мета планів з обробки ризику – документувати те, як вибрана опція обробки ризику буде застосована.

Інформація, яка надається в планах з обробки має включати:

- причини вибору опцій обробки, включаючи очікувані вигоди;
- тих, хто несе відповідальність за ствердження плану, і тих, хто відповідальний за впровадження такого плану;
- пропоновані дії;
- ресурсні вимоги, включаючи нештатні ситуації;
- заходи ефективності та обмеження;
- вимоги щодо звітності та моніторингу;
- часові рамки і плани–графіки.

Плани обробки повинні бути інтегровані з процесами управління всередині організації і мають обговорюватися з зацікавленими сторонами.

Ті, хто приймають рішення, і зацікавлені сторони повинні усвідомлювати природу і ступінь залишкового ризику після його обробки. Залишковий ризик повинен бути документований. До такого ризику має бути застосований моніторинг, оцінка, і, якщо необхідно, додаткова обробка.

Моніторинг та аналіз

Моніторинг, а також оцінка повинні бути сплановані під час процесу ризик-менеджменту і мають підлягати регулярній перевірці та нагляду. Вони можуть мати як періодичний, так і ситуативний характер.

Відповідальності з моніторингу та аналізу мають бути чітко визначені. Процеси організації з моніторингу та аналізу повинні включати всі аспекти процесу ризик-менеджменту з метою:

- гарантії того, що методи управління ефективні і достатні як при розробці, так і при функціонуванні;
- придбання додаткової інформації з метою поліпшення оцінки ризику;
- аналізу та засвоєння уроків із ризикових випадків (включаючи інциденти, зміни, успіхи і провали);
- виявлення змін у зовнішньому і внутрішньому контексті, включаючи зміни в умовах ризику і сам ризик, який може спричинити перевірку обробки ризику і пріоритетів;
- ідентифікації появи ризиків.

Прогрес у застосуванні планів з обробки ризиків є мірою ефективності. Результат може бути включений у загальний менеджмент ефективності всередині організації, вимірювання, зовнішні і внутрішні звітні заходи.

Результати моніторингу та аналізу повинні бути записано і належно доведені до відома зовнішніх і внутрішніх зацікавлених сторін, а також мають бути використані як вхідні для аналізу концепції ризик-менеджменту.

Запис процесів ризик-менеджменту

Заходи з ризик-менеджменту повинні бути доступні для аналізу. У процесі ризик-менеджменту записи є основою поліпшення методів та інструментів, а також процесу в цілому.

Рішення, що стосуються створення записів мають враховувати:

- потреби організації в безперервному навчанні;
- переваги від повторного використання інформації в управлінських цілях;
- витрати і спроби створення та підтримки записів;
- юридичні, нормативні та операційні потреби записів;
- метод оцінки, доступність вилучення та способи зберігання;
- період зберігання;
- конфіденційність інформації.

Властивості поліпшеного ризик-менеджменту [20]

Загальні положення. Всі організації повинні прагнути до високого рівня ефективності концепції ризик-менеджменту, це узгоджується з прийнятими рішеннями. Нижче наведено список ознак високого рівня ефективності в управлінні ризиками. Щоб допомогти організаціям у вимірі їх ефективності щодо цих критеріїв нижче наведені принципові індикатори кожної ознаки.

Ключові виходи. Організація володіє актуальним, правильним і вичерпним розумінням ризиків. Ризики організації відповідають її критеріям ризиків.

Ознаки. Постійне поліпшення. Наголос робиться на постійне поліпшення ризик-менеджменту, шляхом постановки цілей організації, вимірювань, аналізу та подальшої модернізації процесів, систем, ресурсів, можливостей і навичок.

Все це може бути підкреслено існуванням відкритих цілей у сфері продуктивності, що вимірюється в індивідуальній продуктивності організації та окремих її менеджерів. Продуктивність організації може бути виміряна і доведена до відома зацікавлених осіб. Зазвичай аналіз продуктивності має проводитись принаймні раз на рік, а потім відбувається перевірка процесів, постановка перевірених цілей у сфері продуктивності на наступний період.

20. Додаток А стандарту ISO 31000. Свойства улучшенного риск менеджмента. ISO 31000:2009 Международный Стандарт ISO 31000 Первое издание 2009-11-15. Риск Менеджмент – Принципы и руководства.

Така оцінка ефективності ризик-менеджменту – невід'ємна частина всієї оцінки продуктивності організації та системи вимірювань відділів та окремих співробітників.

Повна відповідальність за ризики. Покращений ризик–менеджмент включає всеосяжну, повністю визначену допустиму відповідальність за ризики, методи управління і завдання з обробки ризиків. Уповноважені працівники повною мірою беруть відповідальність, вони володіють достатніми навичками і мають доречні ресурси для перевірки систем управління, моніторингу ризиків, поліпшення управління, а також здатні ефективно доводити ризики до відома внутрішніх і зовнішніх сторін.

Все це може бути відзначено всіма членами організації за умови, що вони повністю обізнані про ризики, методи управління і завдання, за якими вони несуть відповідальність. Зазвичай це записується в посадових інструкціях, базах даних або інформаційних системах. Визначення ролей ризик-менеджменту, обов'язків і відповідальностей має бути частиною програм із уведення посад в організації.

Організація дає гарантію того, що ті, хто несуть відповідальність, повністю забезпечені повноваженнями, часом, навчанням, ресурсами та навичками, достатніми для виконання їх зобов'язань.

Впровадження ризик-менеджменту в процес прийняття рішень. Всі рішення, прийняті всередині організації, незалежно від рівня значущості та важливості, потребують відкритого розгляду ризиків і застосування ризик-менеджменту до певного необхідного ступеня.

Це може бути зазначено записами нарад і рішень з метою показу того, що відкриті обговорення за ризиками були. Більш того, має бути присутня можливість побачити, що всі компоненти ризик-менеджменту подано відповідно до ключових процесів прийняття рішень в організації, наприклад обговорення з приводу розподілу капіталу за головним проектом, за реструктуризацією і змінами всередині організації.

З цих причин науково-методологічний ризик-менеджмент постає в межах організації як основа ефективного управління.

Постійні комунікації. Покращений ризик-менеджмент включає постійні комунікації із зовнішніми і внутрішніми зацікавленими сторонами, включаючи всеосяжне і часте надання звітів з ефективності ризик-менеджменту як частини належного управління.

Це може бути зазначено комунікацією із зацікавленими сторонами як невід'ємна і природна частина ризик-менеджменту. Комунікація постає як двосторонній процес, так, щоб належно поінформовані рішення могли бути прийняті відповідно до рівня ризику та необхідності його обробки щодо встановлених сучасних критеріїв ризику.

Вичерпна і регулярна внутрішня та зовнішня звітність і за значними ризиками, і за ефективністю ризик-менеджменту робить внесок в ефективне управління всередині організації.

Повна інтеграція у структуру управління організації. Ризик–менеджмент розглядається як центральний процес управління в організації, такий, при якому ризики розглядаються у світлі впливу невідповідностей на цілі.

Структура управління та процес засновані на управлінні ризиками. Ефективний ризик-менеджмент вважається керівниками природним засобом досягнення цілей організації. Це підтверджується мовою керівників і важливими письмовими матеріалами організації, що використовує термін «неясності» стосовно до ризиків. Ця ознака також відбивається в політиці організації, особливо тієї, що належить до ризик-менеджменту. Як правило, ця ознака верифікується шляхом проведення інтерв'ю з керівниками та шляхом огляду з дій і тверджень.

Запитання для самоконтролю

1. Які етапи включено до міжнародної системи «Пяти крокова система» оцінки професійних ризиків?