ТЕМА 6. КОРПОРАТИВНЕ УПРАВЛІННЯ РИЗИКАМИ ТА ВАРТІСТЬ ФІРМИ. КОМПЛАЙЄНС-КОНТРОЛЬ

7.1 Вибір стратегії управління ризиками.

Неодмінною умовою успішного функціонування підприємства є побудова ефективної стратегії управління, формування якої залежить від особливостей організації.

Стратегія управління ризиком – це мистецтво управління діяльністю підприємством у невизначеній господарській ситуації, засноване на прогнозуванні ризику і прийомах його зниження.

Управління ризиком це специфічна галузь менеджменту, яка вимагає знань предметної діяльності фірми, страхової справи, аналізу господарської діяльності підприємства, математичних методів оптимізації економічних завдань.

Виокремлюють чотири основні принципи, яких необхідно дотримуватись при виборі тієї чи іншої стратегії менеджменту в конкретній ситуації:

– необхідно передавати ризик третій стороні (страхувати) в тих ситуаціях, коли можливі збитки внаслідок несприятливих подій досить суттєві, а ймовірність їх настання невелика;

– потрібно уникати ризику в ситуаціях, коли збитки внаслідок несприятливих подій значимі, а ймовірність їх настання невелика;

– доцільно ризикувати в тих випадках, коли збитки внаслідок настання несприятливих подій незначні, а ймовірність їх настання невелика.

Для можливих варіантів стратегії підприємства по управлінню ризиками необхідно мати довідкову інформацію за граничним значенням витрат, прийнятим підприємством по кожній із процедур управління ризиками.

Результати етапу "Уточнення стратегії підприємства по управлінню ризиками і вибору процедур управління ними" представлено в табл. 1.

Управління ризиками сьогодні – один із видів професійної діяльності, що динамічно розвивається. Ризик-менеджер поряд із відповідними фахівцями приймає участь у прийнятті ризикованих рішень (наприклад, видача кредиту чи вибір об'єкту інвестування) і шукає способи того, як уникнути небажаних ризиків. Ці дії названі системою управління ризиками.

Таблиця 1 - Результати етапу "Уточнення стратегії підприємства щодо управління ризиками та вибір процедур управління ними"

Результати етапу	Примітки
Уточнена стратегія підприємства щодо управління ризиками	Можливий вибір однієї з наступних стратегій: ризикована; зважена; обережна
Процедури управління ризиками, пріоритетні для обраних стратегій управління	Для ризикованої стратегії: прийняття ризиків на себе; передача ризиків Для зваженої стратегії: прийняття ризиків на себе; передача ризиків; відмовлення від ризиків Для обережної стратегії: відмовлення від ризиків; передача ризиків

Управління ризиками вимагає знань в області теорії фірми, страхової справи, аналізу господарської діяльності підприємства і т. ін. Діяльність підприємства в цій області спрямована на захист своєї фірми від дій ризиків, що загрожують її прибутковості, і сприяє рішенню основної задачі підприємництва: у залежності від ситуації вибрати з декількох проектів оптимальний, з огляду при цьому на те, що чим прибутковіше проект, тим вище ступінь ризику для фірми. Якісне управління ризиком підвищує шанси підприємницької фірми домогтися успіху в довгостроковій перспективі і зменшує небезпеку погіршення її фінансового положення.

У силу того, що в ринковій економіці господарські ризики неминучі, перше правило в управлінні ризиком наголошує: "не уникати ризику, а передбачати його, прагнучи знизити до можливо низького рівня".

2.Загальна схема процесу управління ризиками.

Організацію ризик-менеджменту можна розглядати як єдину технологію процесу управління ризиком (рис. 1)

Рисунок 1 - Схема управління ризиком

Перший крок - визначення цілі ризику і цілі ризикованих вкладень капіталу. Ціль ризику - це результат, який необхідно одержати. Ним може бути виграш, прибуток, дохід і т.п. Ціль ризикованих вкладень капіталу - одержання максимального прибутку.

Другий крок - одержання інформації про навколишнє середовище, яка необхідна для прийняття рішення. Адже на кожному кроці підприємця підстерігають ситуації, що можуть загрожувати людям, майну, фінансовим результатам господарської діяльності. І підприємцю важливо знати відповідний дійсності ступінь ризику для прийняття рішення. На основі аналізу такої інформації і з урахуванням міри ризику можна правильно визначити ймовірність появи ризикованої події, знайти ступінь ризику й оцінити його вартість.

Під вартістю ризику слід розуміти фактичні збитки підприємця, затрати на зниження величини цих збитків чи затрати по відшкодуванню таких збитків і їх наслідків.

Третій крок - на основі наявної інформації про навколишнє середовище, ймовірність, ступінь і величину ризику розробляються різні варіанти ризикованого вкладення капіталу і проводиться оцінка їх оптимальності шляхом зіставлення очікуваного прибутку і величини ризику.

Четвертий крок - дії, що дозволяють правильно обрати стратегію і прийоми управління ризиком, а також способи зниження ступеня ризику. Тут головна роль належить фінансовому менеджеру, його психологічним якостям, схильності до ризику. Фінансовий менеджер, що займається питаннями ризику

(менеджер по ризику), повинний мати право вибору прийняття рішення і право відповідальності за вибір.

П'ятий крок - розробка програми по зниженню ризику. Тут необхідно враховувати, що прийняття рішень в умовах ризику це психологічний процес. Тому поряд з математичною обґрунтованістю рішень слід враховувати психологічні особливості людини: агресивність, нерішучість, сумніви, самостійність і ін. Адже зрозуміло, що та сама ризикована ситуація сприймається різними людьми по-різному. Тому оцінка ризику і вибір фінансового рішення багато в чому залежать від ОПР. Наприклад, керівники консервативного типу, що несхильні до інновацій, невпевнені у своїй інтуїції й у своєму професіоналізмі, невпевнені у своїх працівниках, звичайно намагаються уникати ризику.

Шостий крок - організація заходів щодо виконання наміченої програми дії. Тобто визначення заходів, обсягів і джерел фінансування цих робіт, конкретних виконавців, термінів виконання і т.п.

Сьомий крок - контроль за виконанням наміченої програми, аналіз і оцінка результатів виконання обраного варіанта ризикованого рішення. Для цього створюються органи управління ризиком на даному суб'єкті господарювання. Органом управління ризиком може бути фінансовий менеджер, менеджер по ризиках, відповідний апарат управління: сектор страхових операцій, сектор венчурних інвестицій, відділ ризикованих вкладень капіталу і т.п.

3.Специфічні особливості венчурного бізнесу.

Венчур – одне з найбільш динамічних і перспективних напрямків інноваційного розвитку. Саме завдяки йому були створені та досягли значних успіхів такі компанії, як Apple, Google, Microsoft; з’явилися абсолютно нові галузі та напрями виробництва (біотехнології, персональні комп’ютери, IT індустрія).

Венчурний бізнес зародився у США в середині 1950-х років та відрізняється від інших видів активної інвестиційної діяльності саме підвищеним ступенем ризику: інвестор не має жодних гарантій щодо повернення вкладених у бізнес-проект коштів. В якості винагороди він, як правило, отримує частку у статутному капіталі нового інноваційного підприємства або пакет акцій. Як стверджує І. І. Родіонов, венчурний бізнес – це ризикований бізнес, що є основною формою технологічних нововведень. Він характерний для умов комерціалізації результатів наукових досліджень у наукомістких галузях, підвищення ступеня ризиків вкладень капіталу в інноваційні сфери. Цим бізнесом, як наголошує вчений, займаються відповідні фірми, які забезпечують створення продукту, займаються пошуком і розробкою наукової чи технічної ідеї, її апробацією, створенням зразків і моделей для їх передачі на стадію

виробництва. У міжнародній практиці по завершенні роботи пов'язаної із створенням продукту, венчурна фірма, як правило, припиняє своє існування.

Процеси інституціоналізації венчурного бізнесу, які почалися у 1950х – 1960х роках XX століття збільшили кількість джерел надходження венчурного капіталу, котрих наразі є понад 500. Більшість інституційних джерел мають форму корпорацій або партнерств (стратегічних альянсів). Великі транснаціональні корпорації (далі – ТНК), як особливі суб'єкти міжнародних економічних відносин, мають цілі підрозділи в межах яких зосереджується венчурний капітал.

Більшість сучасних великих корпорацій мають у своїй структурі окремі підрозділи, котрі займаються венчурною діяльністю, серед них: Siemens, Intel, Dassault, PPR, Air liquide, Dell Computer, Microsoft, Cisco, Apple тощо. Для здійснення венчурного бізнесу іноді створюються спеціальні фонди. Досить часто корпорації делегують управління своїми венчурними фондами саме незалежними венчурним фірмам, які є більш компетентними та обізнаними з тенденціями ринку венчурного капіталу. Жофре та Кеніг, розрізняють чотири форми корпоративної венчурної діяльності в залежності від рівня залучення фінансових та людських ресурсів, це: фінансовий венчур, «живильний» венчур, венчур «проникнення» та кооперaційний венчур. Так, фінансовий венчур визначається як процес простої участі в капіталі малих підприємств. Натомість «живильний» венчур не обмежується фінансовими інвестиціями. Інвестор забезпечує свого партнера підтримкою у сферах торгівлі, маркетингу, виробництва чи НДДКР. При венчурі «проникнення» передбачається, що співробітники підприємства вироблятимуть ідеї або технології, які є побічним продуктом більш важливих проектів. Ці вторинні продукти стануть об'єктом проникнення та сприятимуть створенню окремих бізнес-утворень. Кооперaційний венчур сприяє співробітництву малого та великого підприємства, яке передбачає їх специфічний вклад в окремий проект. Сучасні корпоративні венчурні капіталісти діють по принципу LIFO (останнім ввійшов, першим вийшов) (last in, first out). Під цим досить умовним поняттям, мається на увазі схильність корпорацій до вступу у венчурний бізнес у найвдаліші періоди циклу, коли ще існує можливість отримати прибутки, а можливість втрати залучених коштів найменша.

Виявлено наступні особливості венчурного бізнесу, які найбільш характерно відрізняють його від інших видів інвестиційної діяльності:

- Венчурний капітал зосереджується на невеликих високотехнологічних компаніях, орієнтованих на розробку і випуск наукомісткої продукції;
- Венчурний капітал вкладається у нові високотехногічні компанії на середній і тривалий термін та зазвичай не вилучається

венчурним вкладником за власним бажанням до завершення життєвого циклу компанії;

- Венчурний капітал спрямовується на підтримання нетрадиційних (нових, а іноді й зовсім оригінальних) компаній, що, з одного боку, збільшує ризик, а з іншого – робить можливим отримання надвисоких прибутків;
- Венчурне фінансування – це своєрідне надання компаніям в борг певного обсягу коштів, довгострокового кредиту без отримання відповідних гарантій, але під більш високий, ніж у банках, відсоток;
- Взаємний інтерес засновників компанії та інвесторів в успішному і динамічному розвитку нового бізнесу пов'язаний не тільки з вірогідністю отримання високих доходів, але і з можливістю стати учасником створення нової прогресивної технології, стимулюючої науково-технічний прогрес.

Венчурний бізнес ініціює інноваційний підйом, стимулюючи інвесторів вкладати кошти в ризикові проекти, нові технології, нову продукцію, формування нових видів послуг, які здійснюються малими високотехнологічними підприємствами або спільними підприємствами у разі заснування стратегічних альянсів. Індустрія венчурного бізнесу забезпечує доступ до комерційних банків, розширює сферу консалтингових послуг. Істотно зростає економічна мобільність і гнучкість, підвищується конкурентоспроможність виробництва.

Таким чином, венчурний бізнес є важливою складовою інноваційного розвитку корпорацій. Форма та організація венчурної діяльності окремих компаній зазвичай відповідає цілям, якими мотивуються останні, залежить від спеціалізації їх виробництва, менеджменту (так званої корпоративної ідеології) та інституційного середовища у межах якого працює компанія, її підрозділи.

4.Програма ризик-менеджменту і принципи її складання. Документація: Декларація ризик-менеджменту.

Управління ризиками включає в себе розробку і реалізацію програми ризик-менеджменту, котра забезпечує економічно обґрунтовані для підприємства рекомендації та заходи, спрямовані на зниження загального рівня підприємницького ризику до прийнятного рівня. Програма ризик-менеджменту з управління ризиками підприємницької діяльності включає такі підходи: системний, процесний, ситуаційний, а поряд з застосовуваними у практиці методами, метод аналізу ієрархій. Враховувати всі умови, в яких здійснюють діяльність підприємства, з одночасним впливом щодо зниження ризиків, що не завжди є можливим.

Усі заходи щодо управління ризиком можна поділити на доподійні і післяподійні. Перші, як випливає з назви, планують і здійснюють завчасно, а другі – після того, як непередбачена подія вже відбулася.

До доподійних заходів відносять: страхування, самострахування, попереджувальні організаційно-технічні, юридичні, договірні й інші заходи для передачі ризику.

Післяподійні заходи – це одержання ресурсів на ліквідацію збитків у вигляді фінансової допомоги, позик тощо.

Важливе завдання ризик-менеджера – розробка стратегії і принципів управління ризиком на підприємстві та виклад їх у внутрішніх нормативних документах. Основні з них такі:

• декларація з ризик-менеджменту;
• настанови з ризик-менеджменту;
• програма управління ризиками.

В основі діяльності служби ризик-менеджменту лежать стратегія і програма управління ризиком. Стратегію формулюють письмово і вона приймає вигляд Декларації з ризик-менеджменту. Її затверджує вищий керівник організації. Автором первинного тексту декларації зазвичай є один із заступників її першого керівника, на якого покладають загальне управління ризик-менеджментом. Щоб розробити перший варіант такого документа, на допомогу йому можуть запросити зовнішнього консультанта. На цьому етапі надзвичайно важливий свіжий, всеохопний погляд на організацію, її мету, активи, фактори ризику.

Декларація з ризик-менеджменту містить виклад ключових моментів управлінської стратегії підприємства в певній сфері, зокрема зниження рівня можливих ризиків аварій, створення спеціальних резервних фондів для компенсації можливих збитків чи створення системи страхування.

Декларація виражає філософію компанії стосовно управління ризиком. У ній слід окреслити розмежування повноважень між різними структурними одиницями, зазначити, хто відповідає за певні аспекти управління ризиком тощо.

Наявність чіткої декларації надає компанії такі переваги. По-перше, її розробка фокусує увагу керівництва на питаннях управління ризиками, тому що топ-менеджмент вимушений чітко визначити свою позицію стосовно ризиків, з якими стикається компанія, та донести її до всіх інших працівників.

По-друге, декларація допомагає в підготовці планів, потребуючи внесення в них відомостей про те, як саме (операційно та організаційно) компанія буде реалізовувати поставлені завдання у сфері ризик-менеджменту.

По-третє, декларація закріплює обов’язки щодо управління ризиками за цілком конкретними посадами, що дозволяє уникнути безвідповідальності працівників компанії та налагодити дисципліну.

По-четверте, декларація сприяє обговоренню питань управління ризиками в усіх підрозділах компанії в ході контактів ризик-менеджера з їх працівниками.

Нижче наведено один з можливих варіантів декларації.

Політика компанії АВС і її підрозділів полягає в прийнятті загальної методології управління ризиками. Цей підхід містить у собі чітко виражену стратегію щодо визначення того, які ризики компанія буде брати на себе, а які – ні.

Ми визначаємо ризик так: (наводять визначення).

Він має три аспекти:

• фактор ризику (подія);
• імовірність події;
• наслідки події.

Ризик-менеджмент – це (наводять визначення).

Основою для політики у сфері ризик-менеджменту є наші зобов'язання і бажання захистити:

• наших працівників і клієнтів;
• навколишнє середовище;
• позиції нашої компанії, що надає продукцію і послуги найвищої якості.

Наша політика відповідно до цих сформульованих фундаментальних зобов'язань передбачає виділення відповідних матеріальних, фінансових і людських ресурсів, щоб забезпечити наші стандарти у виготовленні продукції. Жоден з бізнес-пріоритетів не є найважливішим.

Політика ризик-менеджменту виходить також з потреби виправдати сподівання наших акціонерів щодо того, що компанія повинна для досягнення своїх цілей використовувати сприятливі можливості, які відкриваються перед нею, навіть якщо це пов'язано з певним ризиком. Наша політика полягає в тім, щоб з належною увагою ставитися до балансу ризику і відповідної винагороди і максимально можливо оптимізувати прибуток від нашого бізнесу.

За виконання політики у сфері ризик-менеджменту відповідають насамперед рада директорів і правління. Директор компанії та його підлеглі відповідають за реалізацію цієї політики у своїй діяльності.

Ця стратегія спирається на аналітичні методи визначення й оцінки ризику, методи впливу на ризики, процедури комунікації і поліпшення профілю ризику компанії. Цю політику і стратегії, що випливають з неї, щороку аналізує рада директорів для того, щоб ми були впевнені в їх дієвості. Додатково раз на півроку цю політику аналізують також незалежні консультанти.

Наша компанія поділяє філософію ефективного ризик-менеджменту як основи ефективного управління загалом.

Директор (підпис)

Від ради директорів (підпис)

Настанови з ризик-менеджменту складаються з нормативних, інструктивних та робочих матеріалів ризик-менеджера, потрібних для розробки програми управління ризиками. Настанови можуть мати різну форму та структуру, залежно від того, які вони виконують завдання. Так, якщо вони призначені для використання вищим керівництвом компанії, то мають стислий формат і містять тільки загальні положення про політику та методи управління ризиком. До другого типу належать настанови, розраховані на використання працівниками середнього рівня. У цьому разі в них наводять усі відповідні методики компанії в галузі ризик-менеджменту. Є ще варіант, коли до настанов включають і Програму управління ризиками.

Ще раз зауважимо, що не існує якогось обов'язкового стандарту відносно форми настанов та інших документів, які повинна мати компанія для управління ризиками.

Ще один документ, який має розробити компанія, має назву Програма управління ризиками. Вона максимально конкретна й описує виявлені ризики та методи впливу на них.

Програма управління ризиками на підприємстві може мати таку структуру:

- Титульний аркуш.
- Зміст.
- Резюме для вищого керівництва.
- Опис бізнесу компанії.
- Стратегічні і тактичні цілі компанії.
- Виявлені фактори ризику компанії.
- Оцінка ризику: наслідки та ймовірність.
- Карта ризиків.
- Методи впливу на ризики.
- Страхування – як основний метод управління ризиками.
- Додатки.

5. Установлення контексту ризику: визначення стратегічних і тактичних позицій компанії, методи виявлення ризику.

Під контекстом ризик-менеджменту розуміється сукупність внутрішніх і зовнішніх чинників (умов), в рамках яких здійснюється управління ризиками.

Розробка контексту ризик-менеджменту дозволяє встановити основні параметри (межі), в рамках яких необхідно управляти ризиками. Контекст також включає в себе внутрішнє і зовнішнє оточення компанії та мета процесу ризик-менеджменту.

Необхідно стежити за тим, щоб цілі ризик-менеджменту враховували специфіку зовнішнього і внутрішнього оточення компанії.

Розробка контексту пов'язана з визначенням основних ідей компанії, її ризиків, масштабу процесу ризик-менеджменту і з розробкою структури завдань, поставлених перед цим процесом. Ця стадія необхідна щоб:

- Визначити цілі компанії;
- Визначити зовнішні характеристики підприємницького середовища, в рамках функціонування якої необхідно досягти поставлених цілей;
- Конкретизувати масштаб і цілі ризик-менеджменту;
- Визначити межі процесу ризик-менеджменту, а також рівень прийнятного ризику;
- Визначити основні вимоги щодо видів діяльності компанії, на які поширюється процес ризик-менеджменту;
- Визначити перелік основних показників для структурування процесу ідентифікації ризиків і визначення їх параметрів.

Основною метою цієї стадії є здійснення первісної оцінки всіх факторів ризику, які можуть впливати на здатність компанії досягти запланованих цілей. В результаті цього повинна вийти стисла формулювання цілей організації компанії, точних критеріїв успіху, цілей і масштабу ризик-менеджменту і послідовність етапів на стадії ідентифікації ризиків. Особливо важливо, щоб процес мав чіткі межі (область застосування, цілі і завдання, вхідні і вихідні параметри, ресурси та управляючі), що дозволить забезпечити функціонування процесу ризик-менеджменту в керованих умовах.

Як вже розглядалося раніше, ризик являє собою співвідношення ймовірності виникнення ризикової ситуації та її наслідків, яке призводить до відхилення фактичних результатів діяльності від запланованих. За своєю суттю заплановані результати роботи компанії випливають з поставлених цілей - як на стратегічному рівні, так і на рівні функціонування її бізнес-процесів. Тому, щоб забезпечити якісну ідентифікацію всіх значущих ризиків, необхідно знати як цілі діяльності, так і цілі бізнес-процесів. Визначення контексту можна розбити на два основних етапи.

Перший етап визначення контексту - ідентифікувати цілі, завдання та внутрішні параметри компанії, а також зовнішні характеристики підприємницького середовища.

Другий етап - визначити масштаб процесу ризик-менеджменту, основні питання та проблеми, які він ставить перед організацією і взаємовідношення між стратегією організації і запланованими результатами бізнес-процесів.

При визначенні зовнішніх характеристик підприємницького середовища повинні враховуватися такі основні умови:

- Ділове, соціальне, нормативне, культурне, конкурентна, фінансове і політичне оточення організації;
- Слабкі і сильні сторони організації;
- Перспективи компанії і несприятливі фактори, що перешкоджають її розвитку;

- Особливості зовнішніх учасників процесу ризик-менеджменту;
- Ключові фактори економічної діяльності організації.

В ході реалізації другого етапу можна використовувати основоположні документи, такі як стратегічний план, бізнес-плани і бюджети, річні звіти, економічні аналізи і іншу документацію, яка містить зареєстровану інформацію про діяльність організації. Також, в ході визначення контексту ризик-менеджменту необхідно співвіднести заплановані результати бізнес-процесів, ідентифіковані кордону процесу ризик-менеджменту з чинним законодавством.

Встановлення масштабу і меж ризик-менеджменту включає в себе:

- Ідентифікацію процесу, проекту або діяльності і визначення її цілей і завдань;
- Визначення характеру рішень, які необхідно прийняти;
- Визначення масштабу діяльності за проектом або функції за часом і місцем;
- Визначення характеру і масштабу необхідних досліджень, їх цілей і ресурсів;
- Визначення області застосування процесу ризик-менеджменту, включаючи всі винятки;
- Оцінку ролі і відповідальності різних структур організації, що беруть участь в процесі ризик-менеджменту.

Необхідно також відзначити, що процес ризик-менеджменту не буде всеосяжним і повним, якщо не визначені ключові елементи діяльності, щодо якої здійснюється управління ризиками.

Ключові елементи діяльності являють собою сукупність важливих напрямків (пріоритетів діяльності), які повинні бути послідовно опрацьовані в процесі ідентифікації ризиків.

Кожен ключовий елемент діяльності має більш вузьку специфіку, ніж вся діяльність в цілому. Данна обставина дозволяє фахівцям з ідентифікації ризиків здійснити деталізовану опрацювання можливих причин і факторів ризиків. У разі якщо діяльність розглядається, як єдине ціле, здійснити ідентифікацію ризиків на всіх етапах її життєвого циклу вкрай важко. Ретельно розроблений набір ключових елементів буде стимулювати творчу думку і гарантувати повне охоплення всіх важливих тем (пріоритетів діяльності). Коли для ідентифікації ризиків використовується метод «мозкового штурму», ключові елементи формують порядок денний і основні завдання зустрічі.

6.Оцінка ризику (фактор, наслідки, імовірність).

Оцінка допустимого ступеня ризику людини в розвинутих країнах вважається індивідуальним ризиком, який дорівнює 10~6 на рік. Малим вважається індивідуальний ризик загибелі 10~4 на рік. На сьогодні розроблена й існує концепція прийнятого (допустимого) ризику, сутність якої полягає у

прагненні забезпечити такий ступінь безпеки, яку сприймає суспільство у цей час.

Для цього, на основі аналізу й оцінки ризику, потрібно вжити заходів щодо вдосконалення управління системою безпеки. Досвід розвинутих країн свідчить, що саме цей метод дозволяє передбачати і здійснювати ефективні запобіжні заходи щодо ймовірних можливих небезпек. За оцінками експертів, його впровадження дозволяє за рахунок підвищення ефективності заходів у 7—10 разів скоротити витрати на розробку і створення безпечних систем.

У наукових дослідженнях управління ризиком визначається як системне регулярне дослідження виникнення ймовірних ризиків, які загрожують людині, майну, інтересам, діяльності. Дослідження ризику дозволяє заздалегідь передбачати певні тенденції розвитку небезпек, допустимості параметрів їхнього впливу на людину, навколишнє середовище. Зрештою, як зазначають окремі автори, врахування ризику повинно стати невід'ємною складовою всіх сфер життя людини. У словнику ризик визначається як "можливість небезпеки". Людина, якій від народження властивий інстинкт самозбереження, зазвичай схильна уникати ризику залежно від виховання, умов життя, світогляду, досвіду, інформованості, але абсолютна безпека не може бути гарантована жодному індивідууму.

Зауважимо, що управління ризиком широко використовується в багатьох сферах науково-виробничої діяльності (техніка, економіка, екологія, психологія, соціологія та ін.). Щоб чіткіше уявити, як на практиці використовується методика управління ризиком, розглянемо приклад, пов'язаний з ризиком небезпеки під час виконання технологічної операції.

Таблиця 3. - Вимірювання ймовірності ризику на робочому місці.

Тяжкість наслідків	Ймовірність події		
	Висока (А)	Середня (В)	Мала (С)
Великі (І)	(5) Дуже високий ризик, неприпустимий	(4) Високий ризик, неприпустимий	(3) Середній ризик, припустимий
Середні (П)	(4) Високий ризик, неприпустимий	(3) Середній ризик, припустимий	(2) Малий ризик, припустимий

Малі (Ш)	(3) Середній ризик, припустимий	(2) Малий ризик, припустимий	(1) Дуже малий ризик, припустимий

Із табл. 3. видно, що рівень ризику збільшується пропорційно збільшенню ймовірності події і тяжкості наслідків. На підставі цієї таблиці встановлюється категорія ризику, а за необхідності здійснюються запобіжні заходи.

Тяжкість наслідків — середня (П), ймовірність події — висока (А). Із табл. 1.3 визначаємо категорію ризику — (4) — високий ризик, неприпустимий.

У цьому випадку ми маємо високий ризик, неприпустимий, запланована робота не може бути розпочата до встановлення огородження.

Оцінка професійного ризику повинна здійснюватися перед запуском обладнання, робочого місця в експлуатацію, а згодом — у разі впровадження змін у конструкції обладнання, організації праці, технологічному процесі, у випадку аварії чи травми працівника.

Оцінка ризику може здійснюватися різними методами:

1. Інженерний. Базується на використанні теорії надійності матеріалів та передбачає виявлення можливих шляхів виникнення відмов на об'єктах з розрахунком імовірності їх виникнення. При цьому ризик може оцінюватися не тільки за нормальних умов безаварійної експлуатації об'єктів, але й у разі виникнення аварійної ситуації.

2. Експертний. Полягає в проведенні оцінки ризику з залученням експертів (спеціалістів) у тій чи іншій галузі.

3. Статистичний. Дозволяє проводити оцінку ризику небезпеки за допомогою інформаційного матеріалу (звіти про небезпечні ситуації, які траплялися на досліджуваному об'єкті).

4. Аналоговий. Базується на використанні та порівнянні небезпек і факторів ризику, які відбувалися в подібних умовах та ситуаціях.

5. Соціологічний. Здійснюється з метою експертної оцінки можливого виникнення ризику у працівників певних професій, спеціальностей, груп населення.

Важливу роль в управлінні ризиком відіграє так званий людський чинник.

Людський чинник — це причини ризику, що пов'язані з помилкою людини у середовищі, де відбувається її діяльність. Він включає різнобічні елементи. Серед них: поведінка людини та її працездатність, проектування, улаштування засобів виробництва на робочому місці; прийняття рішень на виконання виробничого завдання та інші елементи. Здебільшого причиною аварій, катастроф, нещасних випадків є людський чинник (рис. 1.2):

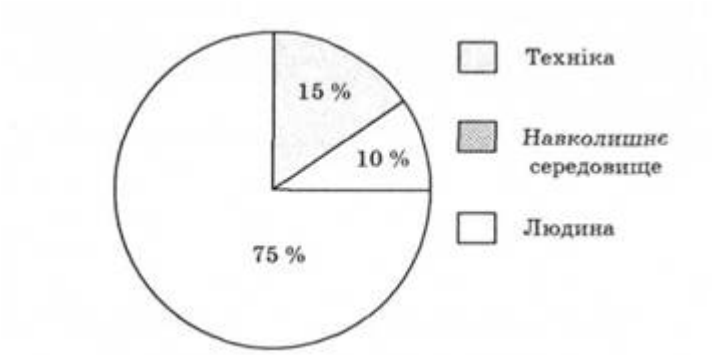

Рис. 2. Розподіл чинника ризику в системі "людина — техніка — середовище"

Таким чином, застосування методики оцінки ризику небезпек дає можливість обґрунтувати раціональні заходи, які дозволяють знизити природні, техногенні, соціальні ризики до мінімально можливого рівня.

Складання карти ризиків.

В ході ідентифікації та оцінки фінансових ризиків застосовуються різні графічні методи, що дають наочне уявлення розподілу ризиків у часі, за видами діяльності, за стадіями бізнес-процесу, в просторі (наприклад по приміщеннях), за розмірами виявленого збитку і т.д. Але самим універсальним інструментом візуалізації інформації, широко використовуваним в ризик-менеджменті, є так звана карта ризиків. Вона будується на основі реєстру ризиків і їх якісних і кількісних характеристик, отриманих в процесі вимірювання. Карту ризиків можна побудувати або для всієї організації, або для будь-якого підрозділу. Крім того, карти ризиків можуть бути складені для напрямки діяльності організації або для окремого проекту, програми.

Карту ризиків будуємо на основі наступних параметрів:

- ймовірність дії ризиків (настання ситуацій ризику);
- частка величини втрат, що виникли у результаті дії ризику по відношенню до планового прибутку по періоду.

У загальному випадку алгоритм процесу картографування ризиків вимагає декілька етапів.

1. Визначається мета і встановлюються межі аналізу, які визначають області картографування ризиків: карта ризиків окремих бізнес-процесів; карта ризиків всього підприємства. При цьому обов’язково враховується доступність і вартість інфляції, необхідної для побудови карти ризиків.

2. Формується команда менеджерів, яка безпосередньо буде займатися складанням карт ризиків (на основі встановлених границь аналізу господарської діяльності і технологічних рішень її здійснення).

3. В межах границь аналізу факторів виявляються всі потенційні ризики конкретного ТП, а також стратегій розвитку його діяльності і сценарії,* що призводять до їх появи.

4. Після встановлення обмеженої кількості сценаріїв здійснюється ранжирування виділених видів ризиків по ступеню їх дії і ймовірності. При цьому можуть використовуватися як якісні, так і кількісні характеристики, як об'єктивні, так і суб'єктивні методи оцінки.

При суб'єктивному підході ймовірність і дія ризику оцінюється за допомогою кількісних і якісних характеристик. Уякісних термінах виділяють наступні ранги дій ризику:

1) катастрофічний;
2) критичний;
3) суттєвий;
4) граничний (допустимий);
5) мінімальний.

Кількісна дія ризику виражається величиною втрат, які в залежності від специфіки ризиків можуть відповідати вартості ресурсів, резервів або визначеній частині втрат у загальній величині прибутку, вартості підприємства і т.ін. ранги ймовірності можуть виражатися у наступних якісних термінах: незначна (майже неможлива), мінімальна, середня, підвищена, висока, реальна.Кількісно ранг ймовірності визначається у процентах (від 0 до 100) або в долях одиниці (від 0 до 1). Результат ідентифікації і ранжування ризиків представляється у вигляді таблиці, в якій показуються джерела або вили ризиків, дія (значимість або величина втрат) і ймовірність ризиків.

5. Перед побудовою карти ризиків визначаються так звані області і границі толерантності до ризику, які відображають терпимість до ризику, т.т. визначення того, наскільки ризик є прийнятним або неприйнятним. Як правило, виділяється дві або три області ризику. Наприклад, зона допустимого ризику (зелена зона), зона помірного або середнього ризику (жовта зона), зона недопустимого ризику (червона зона). Зони помірного і недопустимого ризику, а особливо «червона зона», потребують організації постійного контролю і реалізації активних заходів по зниженню ймовірності і н6. Заключний етап – побудова карти ризиків. При її реалізації ризики розміщуються на карті на основі рангу їх дії і рангу ймовірності. Таким чином, здійснюється свого роду класифікація ризиків по двох параметрахегативної дії ризиків.

8.Комплаєнс ризик

Ведення бізнесу за своєю природою є ризикованим. Будь-яка бізнес-практика, яка не відповідає закону чи галузевим правилам, є ризиком комплаєнсу. Якщо організація не відповідає вимогам, вона ризикує зазнати потенційних фінансових, юридичних та інших втрат. Наприклад, якщо організація не дотримується правил обробки даних, вона може бути

оштрафована або зіткнутися з судовим позовом, якщо кіберзловмисник викраде дані.

Під час створення інфраструктури захист даних має бути головним пріоритетом. Це означає написання правил кодування, розробку баз даних і налаштування процедур застосування, все з урахуванням безпеки даних. Організації зазвичай встановлюють засоби контролю безпеки відповідно до нормативних стандартів HIPAA, PCI-DSS, SOX, GDPR та інших.

Найкращі методи забезпечення цілісності даних є планом безпеки даних. Вони включають правила, наприклад, хто може отримати доступ до даних. Менші організації, які не знайомі з найкращими практиками, повинні звернутися за порадою до експерта.

Що таке комплаєнс-ризик?

Ризик комплаєнсу означає можливу вразливість компанії до фінансових санкцій, юридичних наслідків, репутаційної шкоди та матеріальних втрат через недотримання правових норм, галузевих стандартів або рекомендованих найкращих практик. Кожна організація, державна, приватна, комерційна, благодійна, державна чи федеральна, стикається з таким ризиком.

Види ризику комплаєнс

Існує кілька типів ризиків відповідності вимогам кібербезпеки, з якими організаціям необхідно мати справу, щоб захистити конфіденційні дані та виконати юридичні зобов'язання.

Ось кілька прикладів різних типів ризиків відповідності:

Людська помилка

Люди роблять помилки, що робить соціальну інженерію та фішинг успішними. Ваші дані знаходяться під загрозою, якщо співробітники регулярно не навчаються про поширені кіберзагрози.

Відсутність нагляду

Відстеження даних часто вимагається правилами відповідності. Адміністратори можуть виявляти активні загрози за допомогою моніторингу та отримувати попередження про порушення даних. Обидва вони потенційно можуть знизити серйозність порушення та будь-які наступні наслідки.

Неправильне зберігання

Конфіденційну інформацію слід зберігати в зашифрованому форматі. Якщо є порушення даних, ваша компанія піддається більшому ризику, якщо ви використовуєте формат відкритого тексту.

Порушення даних

Можливість втрати, викрадення або несанкціонованого доступу до конфіденційних даних через недостатні заходи безпеки. Серйозні наслідки витоку даних можуть включати грошові втрати, репутацію та юридичну відповідальність.

Невідповідність нормативним вимогам

Недотримання законів із кібербезпеки та вказівок, встановлених бізнес-асоціаціями чи державними установами, як-от Загальний регламент захисту даних (GDPR), Закон про перенесення та підзвітність медичного страхування (HIPAA), Стандарт безпеки даних платіжних карток (PCI DSS) тощо.

Вразливі місця в ланцюзі поставок

Сучасні ланцюжки постачання взаємопов'язані, що робить їх уразливими до проблем кібербезпеки , якщо злом станеться одним із партнерів чи постачальників.

Як визначати ризик відповідності?

Оцінка можливих областей невідповідності всередині організації вимагає систематичної методології для виявлення ризику відповідності. Розуміння чинних законів і нормативних актів, проведення аналізу прогалин у відповідності, залучення експертів із відповідності, оцінка внутрішніх процесів, моніторинг зовнішнього середовища та проведення оцінки ризиків є частиною виявлення проблем із відповідністю.

Оцінка ризику відповідності залежить від галузі та даних. Наприклад, медичні компанії повинні дотримуватися правил HIPAA. Таким чином, оцінка лікарні завжди посилатиметься на правила HIPPA. Кожна оцінка ризику унікальна.

Організації використовують аудит для оцінки ризиків. Часто ці аудити супроводжуються цифровими рішеннями щодо ризиків відповідності . Ці аудити перевіряють інфраструктуру організації, зокрема:

- Контроль безпеки
- Процедури аварійного відновлення

- Додатки
- Елементи керування авторизацією та автентифікацією
- Сховище та хмарне середовище

Ці аудити визначають, наскільки добре організація дотримується правил зберігання та управління даними.

Концепції оцінки ризиків і вказівки допомагають аудиторам переглядати та ранжувати найбільш ризиковані сфери бізнесу. Ці вказівки також містять дорожню карту для вирішення проблем відповідності. Аудитори також можуть рекомендувати шляхи зменшення порушень.

Ризик ніколи не можна усунути. Але повна оцінка ризику може значно зменшити ризики, якщо вона супроводжується кращими засобами контролю безпеки.

Як оцінити ризики відповідності.

1. Пов’яжіть потенційні ризики з постраждалими сторонами та потенційними результатами

Зіставте ці ризики з їхніми потенційними наслідками та постраждалими сторонами, коли ви ознайомитеся з діяльністю вашої компанії та будь-якими проблемами дотримання або прогалинами, які можуть існувати.

2. Визначте засоби контролю та визначте пріоритетність серйозних ризиків

Впроваджувати програми відповідності або покращувати ті, які у вас уже є, може бути надзвичайно важко. Ми рекомендуємо ранжувати всі виявлені небезпеки відповідно до їх наслідків і спершу зосередитися на найсерйозніших. З’ясуйте, де ваші поточні засоби контролю не справляються з такими загрозами. Що ви можете зробити, щоб це виправити? Також подумайте про те, як ви можете помітити майбутні порушення правил щодо цих серйозних небезпек. Це зменшить будь-які несподівані витрати на недотримання вимог.

3. Впровадження та перевірка засобів контролю

Запровадити засоби контролю, щоб забезпечити відповідність кожному виявленому ризику. Перш ніж переходити до наступного ризику, перевірте ефективність контролю, щоб підтвердити його ефективність. Вивчіть висновки та оцініть, чи контроль функціонує належним чином. За потреби розгорніть додаткові/кращі засоби керування для досягнення бажаної продуктивності.

4. Постійно перевіряйте ризики, оцінюйте засоби контролю та оновлюйте за потреби

Пам’ятайте, що ваша компанія завжди повинна мати корпоративну програму відповідності. Ваші ризики змінюються, коли ваша фірма розширюється. Закони, що стосуються вашої компанії, змінюються з часом.

Періодично перевіряйте елементи керування, оцінюйте їх ефективність і за потреби вносьте зміни в курс.

Як побудувати основу для оцінки комплаєнс ризиків?

Створення організованого підходу до розпізнавання, оцінки та зменшення ризиків відповідності всередині організації є частиною створення структури для оцінки ризиків відповідності. Нижче наведено основні кроки для створення основи для оцінки ризику відповідності:

Крок 1. Встановіть цілі

Постановка цілей завжди має бути першим кроком у будь-якому бізнесі. На що спрямована наша програма управління ризиками? Яким чином наша оцінка ризиків може сприяти досягненню цих цілей? Які елементи має містити оцінка, щоб цього досягти?

Ваша оцінка ризику комплаєнсу в ідеалі має бути спрямована на:

- Узагальніть профіль ризику вашої організації.
- Визначте області для покращення та прогалини в них.
- Визначте тривалість комплаєнс-підходу.
- Зверніть увагу на методологію оцінювання.
- Використовується для розробки пропозицій для вищого керівництва щодо зменшення ризиків для обробки певних небезпек.

Крок 2. Підготуйте

Перш ніж фактично розробляти та використовувати структуру, ви повинні спочатку встановити все інше на місце після того, як ви впевнені у своїх цілях оцінки ризику відповідності.

Спочатку створіть команду, яка відповідатиме за виконання решти кроків. Після цього створіть структуру, методологію, сховище даних, часові рамки та план впровадження. З усіма цими процедурами ви будете готові провести оцінку ризику відповідності за допомогою структури, яку ви створили під час цього процесу.

Крок 3: Підхід до оцінки ризику

Виберіть підхід до оцінки ризику, який підходить для вашої організації. Найпопулярніші методики включають якісні, кількісні та напівкількісні методології. Щоб оцінити серйозність виявлених небезпек, визначте критерії ризику та систему оцінки.

Крок 4: Проведіть оцінку ризику

Тепер ви готові виконати план. Почніть з проведення співбесід, випуску опитувань і анкет, розміщення форумів тощо. Потім зберіть усі ці дані у своєму сховищі даних.

Використовуючи ці дані, ви будете готові перейти до наступного етапу оцінки ризику: оцінки ризику або порівняння ризиків у різних областях і категоріях.

Якщо ваша оцінка ризиків виконала свою роботу правильно, ви зможете визначити пріоритетність ризиків окремо або за категоріями в розумний спосіб. Вирішіть, які ризики потрібно пом’якшити після того, як їх визначили за пріоритетністю, а потім розробіть плани дій для кожного.

Які існують випадки комплаєнс-ризику?

У реальному житті було багато випадків, коли ризики відповідності мали серйозні наслідки для організацій. Ось кілька прикладів:

Скандал із неавторизованими обліковими записами в Wells Fargo:

У 2016 році було виявлено, що працівники відкрили мільйони несанкціонованих рахунків від імені клієнтів без їхнього відома чи згоди, створюючи ризик недотримання вимог для Wells Fargo, важливого банку США. Як наслідок, топ-менеджери покинули компанію, були накладені регуляторні санкції та завдано шкоди репутації. (Джерело)

Порушення даних Equifax:

У 2017 році в компанії Equifax, яка займається звітністю про споживчі кредити, стався серйозний витік даних, у результаті якого були розкриті особисті дані понад 147 мільйонів людей. Порушення сталося в результаті вразливості системи, яку не було виправлено, що представляє ризик відповідності щодо безпеки та конфіденційності даних. У результаті на Equifax були накладені великі грошові штрафи, судові позови та завдано шкоди бренду. (Джерело)

Шахрайські дії Theranos:

Коли було виявлено, що Theranos ввів в оману інвесторів, регулятори та громадськість щодо можливостей їхньої технології тестування крові, бізнес технологій охорони здоров'я наразився на ризики відповідності. Theranos нарешті подав заяву про банкрутство після того, як на нього порушили судові позови та завдали шкоди його репутації. Засновника і топ-менеджерів компанії звинуватили в шахрайстві. (Джерело)