



Кафедра менеджменту інновацій

Управління інноваційними проєктами

Кубарева Ірина

к.е.н., доцент, проєктний менеджер

КАУ

Управління ризиками: сутність та документи у PM2

Ризик — це невизначена подія або набір подій (позитивних чи негативних), які, якщо вони відбудуться, вплинуть на досягнення цілей проекту. Ризик, як правило, вимірюється поєднанням ймовірності (ймовірності виникнення ризику) та розміру впливу на проект.

Схильність до ризику (Ризик-апетит) описує рівень ризику, який організація готова прийняти для досягнення своїх цілей.

Оцінка ризику – це оцінка, яка виконується шляхом аналізу ймовірності настання визначеної події та впливу на цілі проекту, якщо ця подія станеться, разом із схильністю до ризику та наявними вразливими місцями проекту/організації. Рівні ризику розраховуються для кожної події, а потім ризики визначаються за пріоритетністю.

Чому ризики особливо критичні в наукових проектах

- **Унікальні фактори наукових R&D-проектів:**
- **Висока технологічна невизначеність** (TRL 1–6)
- **Залежність від обладнання, лабораторій, реактивів**
- **Дефіцит кадрів з потрібними компетенціями**
- **Залежність від зовнішніх партнерів** (університети, інститути, постачальники)
- **Ризики етичних комітетів, дозволів, сертифікацій**
- **Ризики публікацій** (затримка рецензії, відмова журналу)

Типові ризики наукових проєктів (класифікація)

1. Технічні:

- невідтворюваність результатів
- несправність обладнання
- відсутність необхідних реактивів чи їх дефіцит

2. Організаційні:

- відсутність ключових експертів
- зміна пріоритетів інституту

3. Регуляторні:

- затримки дозволів, етичних погоджень
- зміна вимог

4. Фінансові:

- зміна курсу валюти
- підвищення цін на реактиви

5. Наукові ризики:

- гіпотеза не підтвердилась
- низька кількість даних / мала вибірка

Ризики наукової доброчесності

- Ризики недотримання FAIR принципів
- Ризики некоректного зберігання даних
- Ризики дублювання даних або плагіату
- Ризики втрати доступу до сирих даних
- Вимога до **Data Management Plan**

1. Ризики недотримання FAIR принципів

FAIR = Findable, Accessible, Interoperable, Reusable.

Тобто дані повинні бути:

- знайденими,
- доступними,
- сумісними,
- повторно використаними.

Порушення FAIR = ризик, що дані будуть непридатні для перевірки чи повторення експериментів.

Приклади ризиків:

- дані зберігаються у різних форматах,
- не підписані набори даних,
- неможливо зрозуміти, як отримані результати.

2. Ризики некоректного зберігання даних

Це стосується того, як команда зберігає лабораторні журнали, файли з даними, фото результатів, параметри експериментів.

Приклади ризиків:

- файли зберігаються лише на особистому ноутбукі → втрата даних при поломці;
- відсутні резервні копії;
- неправильні назви файлів;
- немає єдиного сховища (Google Drive, GitLab, ELN тощо).
- Це одна з найчастіших причин **втрати відтворюваності результатів**.

3. Ризики дублювання даних або плагіату

Цей ризик стосується як неетичної поведінки, так і технічних помилок.

Приклади ризиків:

- повторне використання одного й того ж набору даних як різних;
- випадкове дублювання результатів;
- використання чужих даних без відповідного цитування;
- використання текстів/картинок без посилань.
- Це може призвести до:
- відмови журналу у публікації,
- відкликання статті,
- порушення грантових умов.

4. Ризики втрати доступу до сирих даних

Сирі дані (raw data) — це основа наукової роботи.

- Якщо вони втрачені:
- неможливо повторити експеримент;
- неможливо довести, що результати справжні;
- не можна подати статтю в престижний журнал.

Типові причини:

- зміна робочих комп'ютерів;
- відсутність політики backup;
- відсутність контролю доступу при зміні членів команди.

5. Вимога до Data Management Plan (DMP)

DMP — це документ, який визначає:

- де зберігаються дані,
- як вони документуються,
- хто має доступ,
- як вони резервуються,
- як передаються та архівуються.

Відсутність або слабкий DMP = ризик для грантів, публікацій, аудиту.

Багато програм ЄС (Horizon Europe, ERA, EIT) вимагають DMP як обов'язковий артефакт.

Вторинні та залишкові ризики (PM²)

- (на основі PM2 Guide 3.0, стор. Secondary/Residual risks)
- **Вторинні ризики:** з'являються після впровадження певної відповіді на ризик
- **Залишкові:** ті, що залишаються після всіх заходів
- **Приклад:**
 - Встановили UPS для серверів → зменшили ризик відключень → **вторинний ризик:** потрібне обслуговування UPS → **залишковий ризик:** UPS теж може вийти з ладу

Ієрархічна та функціональна ескалація ризику (PM²)

- (на основі RMP – розділ 6.1, PM2 Guide, Escalation)
- **Функціональна:**
потрібна експертиза (звертаємось до відділу, експерта, лабораторії)
- **Ієрархічна:**
ризик впливає на строки / бюджет → повідомляємо PO → PSC
- **Приклади ескалації в науковому проєкті:**
- затримка дозволу етичного комітету >14 днів → ескалація PO
- критичний ризик з обладнанням → ескалація на рівень адміністрації інституту

Де ризики з'являються у WBS

WBS → основа для пошуку ризиків

- На кожен елемент WBS ставимо питання:
- Що може піти не так під час виконання цього пакета робіт?
- Які зовнішні залежності?
- Які припущення можуть не спрацювати?

У PM2: ризики, пов'язані з роботою, відображаються у **Risk Log** та у **Work Plan** (дії з реакції додаються в план).

Ризики і розклад (Schedule)

Ризики створюють:

- затримки (delay risk)
- залежності, що можуть бути порушені
- потребу в буферах

У розкладі відображаємо:

- резерв часу (contingency buffer)
- завдання реагування на ризик
- критичні точки контролю (milestones)

Ризики і ресурси проєкту

Ризики впливають на:

- доступність фахівців
- навантаження
- доступ до обладнання / приміщення

У плані ресурсів відображаємо:

- резерви персоналу
- альтернативні ресурси
- критичні компетенції

Ризики і бюджет проєкту

якщо створюємо резерв коштів — він має з'явитися у бюджеті!

Показуємо у:

- Contingency Reserve (Резерв на відомі ризики)
- Management Reserve (Резерв на непередбачені події)

Ризики і бюджет проєкту

1. Contingency Reserve (Резерв на відомі ризики)

- Створюється **лише на ті ризики, які ідентифіковані у Risk Log.**
Розраховується на основі $L \times I$ та вартості реагування.

Приклади contingency reserve:

- Резерв на закупівлю матеріалів у разі затримки постачання
- Резерв на ремонт обладнання у разі поломки (ризик у реєстрі!)
- Резерв на консультацію експерта, якщо дані будуть неповні
- Резерв часу: +1–2 тижні до критично ризикового пакета робіт

Ризики і бюджет проєкту

2. Management Reserve (Резерв на непередбачені події)

- Формує керівництво / організація для покриття **невідомих ризиків (unknown unknowns)**.

Приклади management reserve:

- Підвищення цін через інфляцію (якщо не було визнано як ризик)
- Несподівана зміна нормативних вимог
- Аварійні ситуації, яких не можна було передбачити

Відмінності між резервами

Характеристика	Contingency reserve	Management reserve
На що	Відомі ризики	Невідомі ризики
Де відображається	WBS, Budget, Risk Log	Бюджет (верхній рівень)
Хто контролює	PM (Project Manager)	Керівництво / PO (Project Office)
Приклад	ремонт обладнання після поломки	несподівана заміна приладу

Мапа відображення ризиків у проєктних документах (PM²)

PM2 документ	Як відобрааються ризики
Project Charter	ключові ризики верхнього рівня
Business Case	ризики рішення, припущення
Stakeholder Matrix	ризик-апетит
Work Plan	дії з реагування, резерви
Risk Log	повний перелік ризиків
RMP (Risk Management Plan)	процеси, ескалація, шкали

Характеристики Ризику проекту (РМВОК)

Організації сприймають ризик як вплив невизначеності щодо проектів та організаційних цілей. Організації та зацікавлені сторони готові прийняти різну ступінь ризику залежно від їхнього ризику.

На ставлення до ризику як організації, так і зацікавлених сторін може впливати ряд факторів, які в основному класифікуються на три групи:

Схильність до ризику - це ступінь невизначеності, який суб'єкт господарювання готовий взяти на себе в очікуванні винагороди.

Толерантність до ризику - це ступінь, розмір чи обсяг ризику, який приймає організація чи людина.

Поріг ризику, який стосується заходів, що відповідають рівню невизначеності або рівня впливу, при якому зацікавлена сторона може мати певний інтерес. Нижче цього порогу ризику організація прийме ризик. Вище за цей поріг ризику організація не потерпить ризику.

Вторинний ризик / Secondary risk

Залишковий ризик / Residual Risk

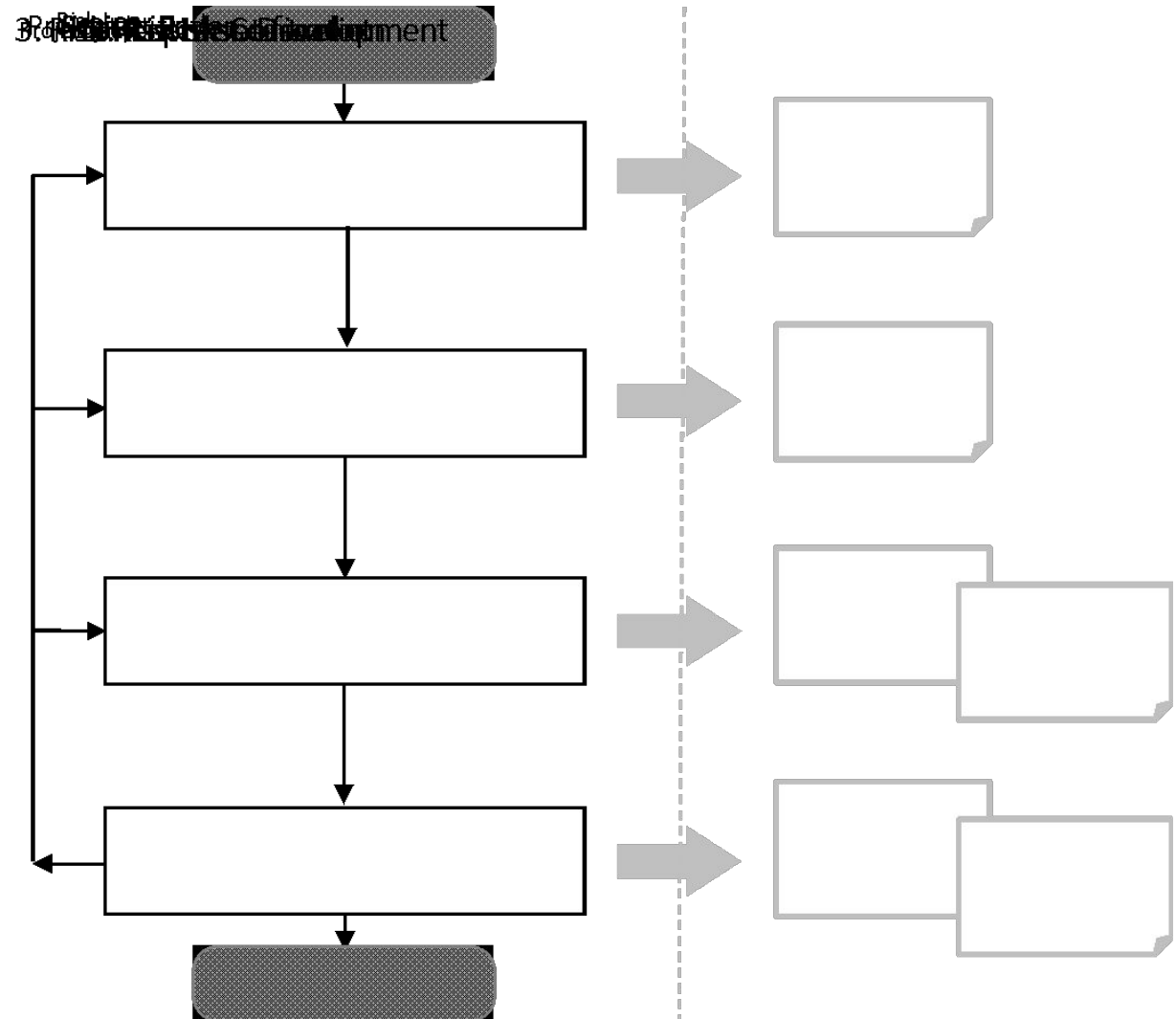
- **Вторинний ризик / Secondary risk** – це той, який залишається після впровадження стратегії реагування на ризик. Потім оцінюється новий ризик і, якщо необхідно, може бути визначена нова стратегія реагування.
- **Залишковий ризик / Residual Risk** — це незначний прийнятний ризик, який залишається після впровадження стратегії реагування на ризик або після розгляду існуючих засобів контролю.

Хто такий власник в РМ2? Власник ризику

Власник (Owner) - це особа/організація, яка в кінцевому рахунку відповідає за щось: проєкт, результат (deliverable), процес, дії, ризик, складне питання (issue) чи рішення.

Власник ризику (Risk Owner) - це особа, відповідальна за управління та моніторинг конкретного ризику.

Управління ризиками: дії і документи



Журнал або Реєстр ризиків / Risk Log

Журнал ризиків є центральним сховищем усіх ризиків, виявлених проектом або організацією.

Журнал ризиків містить інформацію для кожного ризику, таку як: ймовірність, вплив, рівень, стратегії реагування на ризик і власник ризику.

Журнал ризиків також можна назвати Реєстром ризиків (Risk Register) або Списком ризиків (Risk List).

Ідентифікація ризиків (PMBOK)

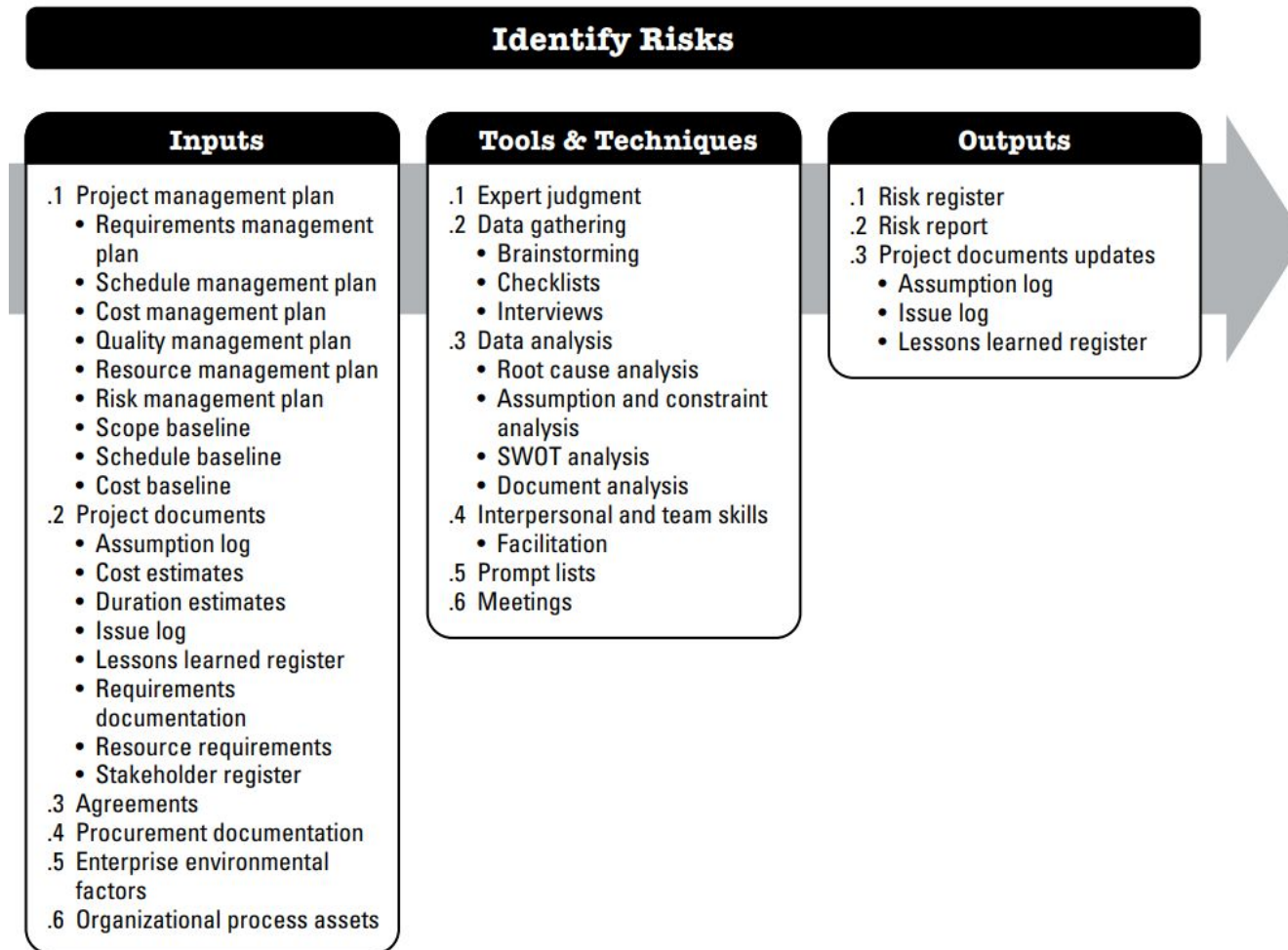


Figure 11-6. Identify Risks: Inputs, Tools & Techniques, and Outputs

Оцінка ризику / Risk Assessment

Оцінка ризику – це оцінка, яка виконується шляхом аналізу ймовірності настання визначеної події та впливу на цілі проекту, якщо ця подія станеться, разом із схильністю до ризику та наявними вразливими місцями проекту/організації.

Рівні ризику розраховуються для кожної події, а потім ризики визначаються за пріоритетністю.

Матриця оцінки ризиків / Risk Assessment (Likelihood/Impact) Matrix

Матриця оцінки ризиків показує різні **комбінації ймовірності та впливу** ризиків проекту та визначає діапазони рівня ризику, яким пропонують стратегії реагування на ризик.

Вплив ризику / Risk Impact (I) описує потенційні наслідки, які ризик матиме на цілі проекту, якщо він матеріалізується. Вплив може мати як кількісний, так і якісний характер. Зазвичай він виражається за шкалою від 1 до 5.

Ймовірність ризику / Risk Likelihood (L) виражає ймовірність того, що ризик може виникнути. Зазвичай він виражається за шкалою від 1 до 5 (також можна виразити через фактичні ймовірності, наприклад, 10%-30%-50%-70%-90%).

Рівень ризику / Risk Level (RL) є результатом комбінації ймовірності (L) виникнення ризику та його впливу (I), якщо він відбудеться. **($RL=L*I$)**.

Матриця ймовірності та впливу ризику (PM2 приклад) джерело: Артефакт «План управління ризиками»

Зелений: рівень ризику ≤ 2 ;
Жовтий: рівень ризику ≥ 3 та ≤ 16 ;
Червоний: рівень ризику ≥ 20 .

		Impact				
		1=Very low	2=Low	3=Medium	4=High	5=Very high
Likelihood	5=Very high	5	10	15	20	25
	4=High	4	8	12	16	20
	3=Medium	3	6	9	12	15
	2=Low	2	4	6	8	10
	1=Very low	1	2	3	4	5

Legend:

	Risks can be <u>accepted</u> , contingency plans may be developed.
	Risks cannot be accepted, a risk response strategy should be developed (avoid, reduce, transfer/ share)
	Unacceptable – immediate risk reduction or avoidance response
- - - -	Risk appetite

Figure 1: Risk Likelihood/Impact matrix.

Please customize the above matrix as per your project's or/and organization's needs.>

Шкали рівня ризику для Матриці ймовірності та впливу ризику (PM2 приклад) джерело: Артефакт «План управління ризиками» PM2

Ймовірність	Вплив
Дуже низька: менше ніж 5% зміни виникнення;	Дуже низький: зачіпає менше 1% бюджету проекту, або/та інші базові показники проекту майже не зазнають впливу, або/і зачіпає небагато осіб (лише всередині команди проекту), або/і не впливає на репутацію, або/і легко та швидко здатність відреагувати та вирішити проблему.
Низька: від 5% до 10% шансів виникнення;	Низький: від 1% до 2% бюджету проекту зазнає впливу, або/і низький вплив на інші базові показники проекту, або/і зачеплено лише одну віху, або/і зацікавлені сторони проекту можуть зазнати впливу, або/і вплив на репутацію в організації чи підрозділі або/та достатні проектні компетенції для вирішення проблеми (якщо виникає ризик).
Середня: від 10% до 25% ймовірності виникнення;	Середній: вплив від 2% до 5% бюджету проекту, або/і середній вплив на інші базові показники проекту, або/і вплив на один або більше етапів, або/і зацікавлені сторони проекту певною мірою постраждають, або/і цілі проекту можуть або/та репутаційний вплив серед технічного персоналу в інших організаціях або підрозділах, або/та офіційні скарги, або/і обмежені компетенції проекту для вирішення проблеми (якщо виникає ризик).
Висока: ймовірність виникнення від 25% до 50%;	Високий: від 5% до 10% бюджету проекту є під впливом, або/та значний вплив на інші базові лінії проекту, або/і є під впливом на кілька етапів, або/і зацікавлені сторони проекту постраждають/занепокоєні, або/і цілі проекту вплинуть, або/і вплив на репутацію в кількох організаціях або підрозділах, або/і офіційні та юридичні скарги, або/і недостатня внутрішня компетентність проекту для вирішення проблеми (якщо виникає ризик).
Дуже висока: ймовірність появи понад 50%.	Дуже високий: понад 10% бюджету проекту зазнає впливу, або/і дуже значний вплив на інші базові лінії проекту, або/і зачеплено кілька етапів, або/і зацікавлені сторони проекту будуть сильно зачеплені/стурбовані, або/і загальний проект буде зазнати впливу, або/і зовнішній репутаційний вплив, або/і значні формальні та юридичні скарги, або/або зовнішні компетенції необхідні для вирішення проблеми (якщо виникає ризик).

Управління ризиками: стратегії реагування на ризики

Стратегія реагування на ризик / Risk-Response Strategy описує спосіб управління ризиком

Стратегії реагування на ризик створені для того, щоб мати можливість протистояти як **позитивним ризикам (можливості)**, так і **негативним ризикам (загрози)**

Стратегії згруповані таким чином:

для загроз (негативних ризиків) : уникнути, зменшити, прийняти, передати/поділитися

для можливостей (позитивних ризиків)*: використовувати, покращувати, приймати, ділитися

Можливість*/Opportunity — це сприятлива умова, яку можна використати, щоб призвести до позитивних змін або покращення середовища проєкту.

Сценарії для обрання Стратегії реагування на ризики

Сценарій	Стратегія реагування/відповіді на ризик
Дуже великий вплив і висока або дуже висока ймовірність або високий або дуже великий вплив і дуже висока ймовірність	Уникайте або запровадьте негайне скорочення
Дуже сильний вплив і дуже низька ймовірність	Передача/Поділ
Всі інші рівні ризику	Зменшити
Низька або дуже низька ймовірність і дуже низький вплив або дуже низька ймовірність і низький вплив	Прийняти (моніторинг і планування непередбачених ситуацій, якщо це буде необхідно)

Стратегії реагування на ризики

- **Avoid (risk response strategy) / Уникнення** — це стратегія реагування на ризик, яка полягає у зміні умов проекту, планів, заходів або навіть масштабів, щоб зробити ризик невідповідним для проекту (тобто Вплив=0 та/або Ймовірність=0%)
- **Reduce (risk response strategy) Зменшення** — це стратегія реагування на ризик, спрямована на **пом'якшення*** впливу та/або ймовірності ризику шляхом проактивного впровадження заходів зі зменшення ризику (наприклад, заходів контролю) до рівня, коли можна прийняти залишковий ризик
- ***Mitigation / Пом'якшення** — це дія, яка виконується для: (1) зниження ймовірності виникнення ризику та (2) зменшення впливу ризику на проект шляхом мінімізації його впливу, якщо він має місце. (Див. також Зменшення, стратегія реагування на ризик)

Стратегії реагування на ризики

- **Accept (risk-response strategy) Прийняття** — це стратегія реагування на ризик, яка застосовна як для негативних (загрози), так і для позитивних (можливості) ризиків. У випадку загроз є дві можливі реакції, тобто пасивне прийняття (особливих дій не планується, просто продовжуйте стежити за ризиком) або активне прийняття, що передбачає розробку плану на випадок непередбачених обставин. Що стосується можливостей, то ніяких конкретних дій щодо їх реалізації не робиться. Ми просто виграємо від них у разі їх виникнення.
- **Transfer/Share (risk-response strategy) Передача** — це стратегія реагування на ризик, яка полягає в передачі ризику третій стороні (наприклад, через страхування або аутсорсинг). Ця стратегія не звільняє організацію від ризику, але вона може зменшити ймовірність (наприклад, передаючи діяльність спеціалізованій стороні) та/або вплив у разі виникнення ризику. Завжди існує рівень вторинного та/або залишкового ризику, оскільки остаточною відповідальністю за ризики проекту залишається за організацією.

Стратегії реагування на ризики

- **Exploit (risk response strategy) Експлуатування (Використання)** — це стратегія реагування на ризик, яка полягає у зміні умов проекту, планів, заходів або навіть масштабів, **щоб гарантувати виникнення позитивного ризику (можливості) (з ймовірністю=100%)**
- **Enhance (risk response strategy) Посилення/Збільшення** — це стратегія реагування на ризик, спрямована на підвищення ймовірності та/або впливу позитивного ризику (можливості). Вона суттєво відрізняється від стратегії реагування на ризики Exploit, оскільки **не забезпечує реалізації можливості**.

Структура ризиків (РМВОК)

RBS LEVEL 0	RBS LEVEL 1	RBS LEVEL 2
0. ALL SOURCES OF PROJECT RISK	1. TECHNICAL RISK	1.1 Scope definition
		1.2 Requirements definition
		1.3 Estimates, assumptions, and constraints
		1.4 Technical processes
		1.5 Technology
		1.6 Technical interfaces
		Etc.
	2. MANAGEMENT RISK	2.1 Project management
		2.2 Program/portfolio management
		2.3 Operations management
		2.4 Organization
		2.5 Resourcing
		2.6 Communication
		Etc.
	3. COMMERCIAL RISK	3.1 Contractual terms and conditions
		3.2 Internal procurement
		3.3 Suppliers and vendors
		3.4 Subcontracts
		3.5 Client/customer stability
		3.6 Partnerships and joint ventures
		Etc.
	4. EXTERNAL RISK	4.1 Legislation
		4.2 Exchange rates
		4.3 Site/facilities
		4.4 Environmental/weather
		4.5 Competition
		4.6 Regulatory
		Etc.

Категорії Ризиків (за РМ2)

- **Бізнес:** стосується політичних рішень, стратегії та бізнес-процесів і послуг;
- **ІТ:** пов'язані з інфраструктурою, розвитком системи, безпекою, безперервністю бізнесу та доступністю ІТ-послуг;
- **Люди та організація:** пов'язані з персоналом проекту, компетенціями та координацією між командами;
- **Зовнішній:** пов'язаний з аутсорсингом діяльності, зовнішніми партнерами та макросередовищем;
- **Юридичні:** пов'язані із законами, постановами та правилами;
- **Комунікація та інформація:** стосується методів і каналів комунікації, а також якості та своєчасності інформації.

Управління ризиками: сутність та документи у PM2

Управління ризиками – це систематичний безперервний процес ідентифікації, оцінки та управління ризиками, щоб вони відповідали прийнятому ставленню організації до ризику.

Управління ризиками підвищує впевненість команди проекту шляхом проактивного управління будь-якими потенційними подіями, які можуть мати позитивний або негативний вплив на цілі проекту

Процес управління ризиками можна адаптувати та налаштувати відповідно до потреб проекту та **задокументувати в Плані управління ризиками (Risk Management Plan) або в Посібнику з проекту (Project Handbook).**

Журнал ризиків (Risk Log) використовується для документування та передачі інформації про ризики та відповідні дії та обов'язки щодо реагування на ризик

Управління ризиками проєкту: вхідні дані

Входи:

Бізнес-кейс (Business Case)

Статут проєкту (Project Charter)

Процеси управління ризиками (Risk Management Process)

Реєстр ризиків (Risk Log)

Управління ризиками проєкту: кроки

1. **Визначити ризики:** Мета цього - визначити та задокументувати ризики, які можуть мати вплив на цілі проєкту. Нові ризики можуть виникати в будь-який момент під час проєкту та їх слід додати до журналу ризику для подальшого аналізу/дії.
2. **Провести оцінку ризику:** Метою цього кроку є оцінка ймовірності кожного ризику та тяжкості його впливу на цілі проєкту. Ця оцінка необхідна перед плануванням реагування на ризик. Ризики середнього та високого рівня вирішуються на більш високому рівні пріоритету.
3. **Розробити стратегію реагування на ризик:** Мета цього кроку - вибрати найбільш доцільну стратегію для реагування на визначений ризик та планування дій, необхідних для реалізації цієї стратегії.
4. **Контроль діяльності з відповіді на ризик:** Метою цього кроку є моніторинг та контроль впровадження діяльності з відповіді на ризик та перегляду/оновлення журналу ризиків на основі регулярної переоцінки.
5. **Занесення у документ/Запис:** Оновлення плану роботи проєкту за допомогою чітких завдань щодо відповіді на ризик, коли це вважається необхідним.
6. **Звітування:** регулярно інформувати керівний комітет проєкту (PSC) про діяльність, пов'язану з ризиком.

Управління ризиками проєкту: ключові учасники

Ключові учасники

Менеджер Проєкту (Project Manager - PM) Здійснює моніторинг і контроль ризиків.

Інші стейкхолдери проєкту (Other project stakeholders)
Поінформовані про критичні ризики.

Основна команда проєкту (Project Core Team – PCT)
Залучена до процесу виявлення ризиків і реагування на них.

Керівний комітет проекту (Project Steering Committee - PSC)
Здійснює моніторинг проектів з високим рівнем ризику.

Інші стейкхолдери Визначають та повідомляють про ризики у своїх сферах компетенції

Управління ризиками проєкту: учасники і артефакти

RAM (RASCI)	AGB	PSC	PO	BM	BIG	SP	PM	PCT
Manage Risks	I	C	A	S/C	C	I	R	C

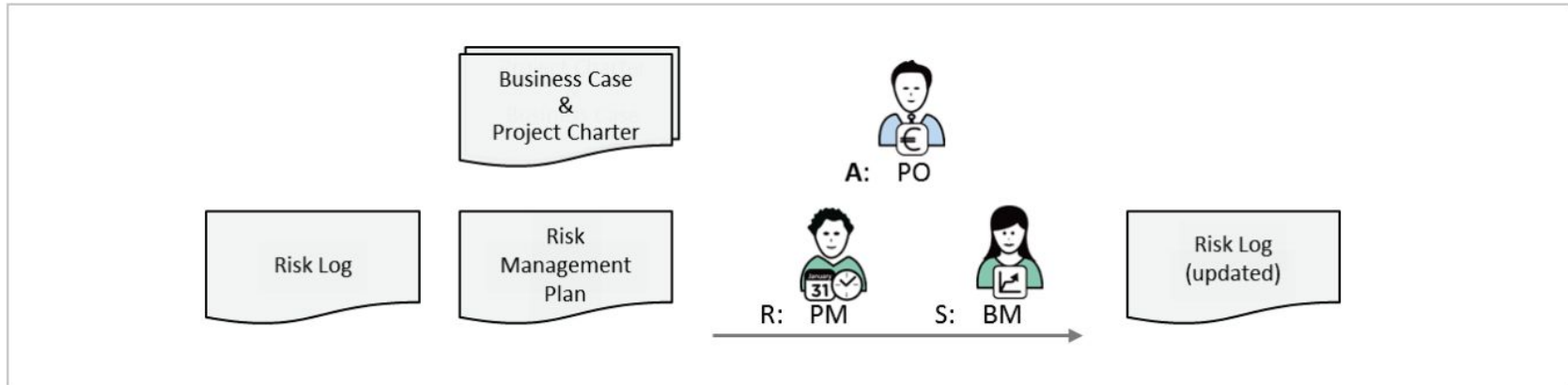


Fig 9.8: Manage Risk inputs/outputs and main roles

Related Artefacts	Initiating	Planning	Executing	Monitor & Control	Closing
Risk Management	Project Charter	Risk Management Plan	Project Reports	Project Logs Project Work Plan	Project-End Report

Outputs

- Risk Log (updated)

PM² Template?



Поняття «Ескалація / Escalation» в PM2

Ескалація / Escalation — стосується діяльності, яка потребує додаткових ресурсів для досягнення результату/виходу.

Існує два типи ескалації:

Функціональна ескалація - якщо потрібні додаткові компетенції/вищий рівень досвіду

Ієрархічна ескалація - коли необхідно залучити вищі (більш високого статусу) рівні прийняття рішень

Ескалація ризиків описується у Плані управління ризиками (артефакт Risk Management Plan) – розділ 6, пункт 6.1 (див. артефакт PM2)

Ключові учасники для Плану управління ризиками і Процесу управління ризиками

Керівник проекту (PM) несе відповідальність за виявлення, оцінку, управління та моніторинг ризиків проекту, консультування команди проекту та інших зацікавлених сторін, якщо це необхідно (наприклад, Керівний комітет проекту (PSC), власник проекту (PO), бізнес-менеджер (BM), постачальник рішень (SP) і представники користувачів (UR)). Керівник проекту (PM) також відповідає за розподіл ресурсів для процесу управління ризиками за погодженням з власником проекту (PO).

Планування діяльності з управління ризиками виконується керівником проекту (PM) і документується в Плані управління ризиками.

Нові ризики та пов'язані з ними дії, а також зміни до виявлених ризиків і дій затверджуються Власником проекту (PO) і повідомляються Керівному комітету проекту (PSC) відповідно до процедури ескалації.

Ризики та відповідні дії будуть передані іншим керівним органам, коли це буде доречно. Керівний комітет проекту (PSC) та інші керівні органи перевірятимуть ідентифіковані ризики та дії, а також плануватимуть інші дії, якщо вони доцільні.

Контактні дані кожної із зазначених зацікавлених сторін задокументовано в матриці зацікавлених сторін проекту (Project Stakeholder Matrix).

RAM (RASCI)	AGB*	PSC	PO	BM	UR	SP	PM	PCT
Risk Management Plan	I	C	A	C	I	I	R	I
Manage Risks	I	C	A	S/C	C	I	R	C

Ініціація проєкту: які документи стосуються ризиків

Інформація про ризики міститься в таких документах:

Бізнес-кейс (Business Case) - ключові ризики запропонованого рішення, які спочатку були визначені за допомогою відповідної стратегії пом'якшення, якщо така існує

Запит на ініціацію проєкту (Project Initiation Request) - ризик верхнього рівня без деталізації, акцент на бізнес-ризиках)

Довідник проєкту (Project Handbook) - високорівневий опис процесу управління ризиками, який буде використовуватися, який може бути налаштований відповідно до конкретного проєкту та організаційного контексту, якщо необхідно

Статут проєкту (Project Charter) – початкова оцінка ризиків, має висвітлити ключові ризики проєкту, які визначені на цьому початковому етапі, і запропонувати відповідні стратегії управління ризиками

Матриця стейкхолдерів (Stakeholders Matrix) – визначає ризик-апетит (ставлення до ризику, міру прийняття ризику стейкхолдерами проєкту)

План робіт проєкту (Project Work Plan) – в частині визначення непередбачуваних ресурсів та відповідних резервів

Планування проєкту. План Управління ризиками проєкту

План управління ризиками:

Визначає та документує **процес управління ризиками** для проєкту

Описує, як будуть **ідентифікуватися та оцінюватися** ризики

Описує, які **інструменти та методи** можна використовувати, які шкали оцінювання та допуски

Описує відповідні **ролі та обов'язки**

Описує, як часто потрібно переглядати ризики тощо.

Визначає **процес моніторингу та ескалації** ризиків

Визначає **структуру журналу/реєстру ризиків**, який використовується для документування та передачі інформації про ризики та дії щодо реагування на них.

Артефакт План управління ризиками проєкту (Risk Management Plan)

Містить:

- ✓ Ролі та обов'язки управління ризиками
- ✓ Інструменти та техніки управління ризиками (Реєстр ризиків, Матриця Ймовірність/Вплив)
- ✓ Активності з ідентифікації ризиків
- ✓ Підхід до оцінювання ризиків
- ✓ Стратегії реагування на ризики
- ✓ Активності з контролю ризиків
- ✓ Пов'язані РМ2 плани

План Управління ризиками проєкту: значення, вхідні та вихідні документи

Управління ризиками забезпечує видимість ризиків і підзвітність щодо того, як вони обробляються, а також гарантує, що ризики проєкту проактивно розглядаються, регулярно відстежуються та контролюються.

Входи: Бізнес-кейс (Business Case) і Статут проєкту (Project Charter), Довідник проєкту (Project Handbook), План робіт проєкту (Project Work Plan)

Виходи: Реєстр ризиків (Risk Log), План управління ризиками (Risk Management Plan)

(див. Артефакти Risk Log, Risk Management Plan)

План Управління ризиками проєкту: кроки створення

1. Перевірте, чи існує вже процес управління ризиками на рівні організації.
2. Адаптуйте план управління ризиками до потреб проєкту (наприклад, видаліть/додайте кроки чи дії, змініть опис діяльності або відповідні обов'язки тощо). Створіть його як окремий документ або як розділ у Довіднику проєкту.
3. Переконайтеся, що немає дублювання інформації, що міститься в інших планах управління або Довіднику проєкту (наприклад, процедура ескалації).
4. Визначте інструменти та методи, які будуть використовуватися для виявлення, оцінки та моніторингу ризиків (наприклад, мозковий штурм, база даних ризиків, структура розподілу ризиків, матриця ймовірності й впливу, дерево рішень, журнал ризиків тощо).
5. Налаштуйте шкали, які використовуються для оцінки ризиків (тобто ймовірності, впливу та загального рівня ризику).

План Управління ризиками проєкту: кроки створення

6. Визначити (із залученням ключових стейкхолдерів) ризик-апетит проекту (обсяг ризику, який зацікавлені сторони готові прийняти)
7. Вирішіть, як часто слід переглядати журнал ризиків, враховуючи як проект, так і організаційні умови та політики.
8. Вкажіть процедури ескалації та комунікації про ризики, які потребують особливої уваги (тобто, які зацікавлені сторони проекту повинні бути проінформовані, якщо спрацьовують критичні ризики).
9. Визначте відповідні стратегії реагування на ризик як для ідентифікованих загроз, так і для можливостей (тобто: уникати, передавати/ділитися, зменшувати, приймати або використовувати, покращувати, ділитися та приймати відповідно).
10. Визначте рівень деталізації, з яким дії реагування на ризик повинні бути описані в журналі ризиків (наприклад, опис дії, власник дії, запланована робота тощо). Зауважте, що дії, які потребують значних зусиль, мають бути включені у план робіт проєкту (Project Work Plan).
11. Переконайтеся, що процес управління ризиками доведений до команди проекту та зацікавлених сторін

Планування Управління ризиками проєкту

RAM (RASCI)	AGB	PSC	PO	BM	BIG	SP	PM	PCT
Risk Management Plan	I	C	A	C	I	I	R	I

Related Artefacts	Initiating	Planning	Executing	Monitor & Control	Closing
Risk Management	Project Charter	Project Handbook Risk Management Plan	Project Reports	Risk Log Project Logs	Project-End Report

Artefact

- Risk Management Plan
- Risk Log

PM² Template?



Джерело: PM² Project Management Methodology, Guide 3.0

Причини і Наслідки Ризиків проекту. Окремий і загальний ризик.

- **Ризик може мати одну або більше причин, і якщо він виникає, він може мати один або більше наслідків.** Причиною може бути дана або потенційна вимога, припущення, обмеження або умова, що створює можливість негативних чи позитивних результатів.
- **Окремі ризики проекту відрізняються від загального ризику проекту.** Загальний ризик проекту являє собою вплив невизначеності для проекту в цілому. Це більше, ніж сума окремих ризиків в рамках проекту, оскільки включає всі джерела невизначеності проекту. Він представляє схильність зацікавлених сторін до наслідків варіацій результатів проекту, як позитивних, так і негативних.

Інструменти збору інформації про ризики (РМВОК)

Data-gathering techniques that can be used for this process include but are not limited to:

- ◆ **Brainstorming.** The goal of brainstorming (see Section 4.1.2.2) is to obtain a comprehensive list of individual project risks and sources of overall project risk. The project team usually performs brainstorming, often with a multidisciplinary set of experts who are not part of the team. Ideas are generated under the guidance of a facilitator, either in a free-form brainstorm session or one that uses more structured techniques. Categories of risk, such as in a risk breakdown structure, can be used as a framework. Particular attention should be paid to ensuring that risks identified through brainstorming are clearly described, since the technique can result in ideas that are not fully formed.
- ◆ **Checklists.** A checklist is a list of items, actions, or points to be considered. It is often used as a reminder. Risk checklists are developed based on historical information and knowledge that has been accumulated from similar projects and from other sources of information. They are an effective way to capture lessons learned from similar completed projects, listing specific individual project risks that have occurred previously and that may be relevant to this project. The organization may maintain a risk checklist based on its own completed projects or may use generic risk checklists from the industry. While a checklist may be quick and simple to use, it is impossible to build an exhaustive one, and care should be taken to ensure the checklist is not used to avoid the effort of proper risk identification. The project team should also explore items that do not appear on the checklist. Additionally, the checklist should be reviewed from time to time to update new information as well as remove or archive obsolete information.
- ◆ **Interviews.** Individual project risks and sources of overall project risk can be identified by interviewing experienced project participants, stakeholders, and subject matter experts. Interviews (see Section 5.2.2.2) should be conducted in an environment of trust and confidentiality to encourage honest and unbiased contributions.

Інструменти аналізу ризиків (РМВОК)

Data analysis techniques that can be used for this process include but are not limited to:

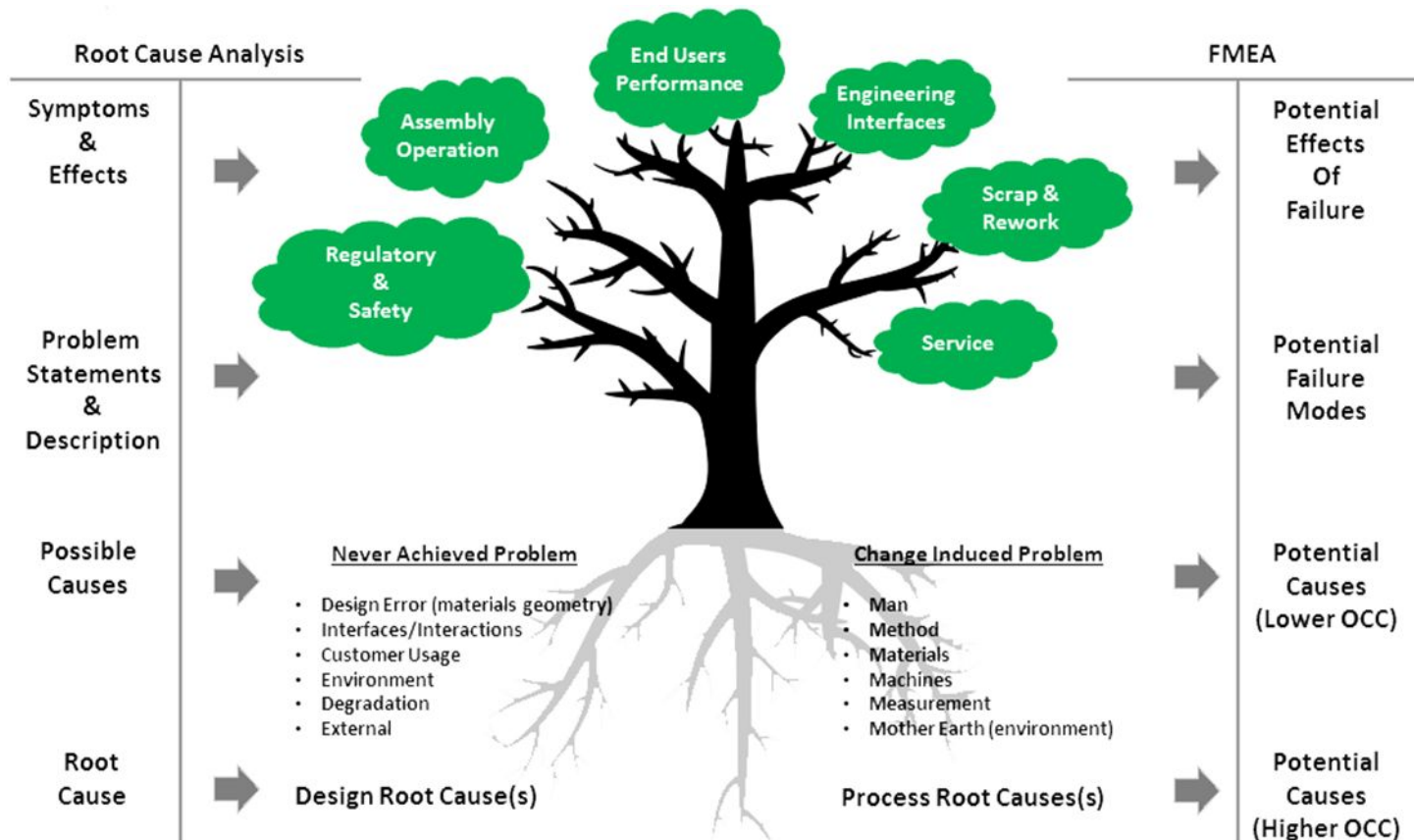
- ◆ **Root cause analysis.** Root cause analysis (see Section 8.2.2.2) is typically used to discover the underlying causes that lead to a problem, and develop preventive action. It can be used to identify threats by starting with a problem statement (for example, the project might be delayed or over budget) and exploring which threats might result in that problem occurring. The same technique can be used to find opportunities by starting with a benefit statement (for example, early delivery or under budget) and exploring which opportunities might result in that benefit being realized.
- ◆ **Assumption and constraint analysis.** Every project and its project management plan are conceived and developed based on a set of assumptions and within a series of constraints. These are often already incorporated in the scope baseline and project estimates. Assumption and constraint analysis explores the validity of assumptions and constraints to determine which pose a risk to the project. Threats may be identified from the inaccuracy, instability, inconsistency, or incompleteness of assumptions. Constraints may give rise to opportunities through removing or relaxing a limiting factor that affects the execution of a project or process.
- ◆ **SWOT analysis.** This technique examines the project from each of the strengths, weaknesses, opportunities, and threats (SWOT) perspectives. For risk identification, it is used to increase the breadth of identified risks by including internally generated risks. The technique starts with the identification of strengths and weaknesses of the organization, focusing on either the project, organization, or the business area in general. SWOT analysis then identifies any opportunities for the project that may arise from strengths, and any threats resulting from weaknesses. The analysis also examines the degree to which organizational strengths may offset threats and determines if weaknesses might hinder opportunities.
- ◆ **Document analysis.** Described in Section 5.2.2.3. Risks may be identified from a structured review of project documents, including, but not limited to, plans, assumptions, constraints, previous project files, contracts, agreements, and technical documentation. Uncertainty or ambiguity in project documents, as well as inconsistencies within a document or between different documents, may be indicators of risk on the project.

Причинно-наслідкова діаграма у аналізі причин ризиків

Коренева причина / Root Cause описує вихідну/основну причину проблеми чи ризику

Визначення кореневої причини ризику можливе за допомогою процесу Root Cause Analysis (аналіз кореневих причин) або інша назва Діаграма Ішикави

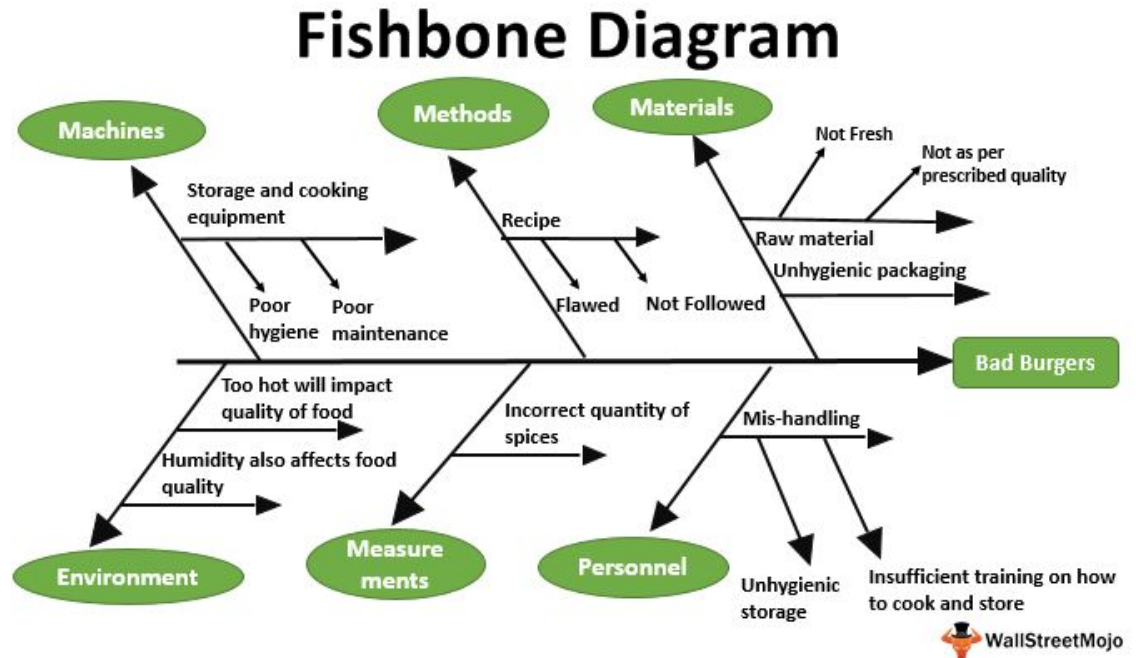
Причинно-наслідкова діаграма у аналізі причин ризиків



Причинно-наслідкова діаграма у аналізі причин ризиків

Діаграма Ішикави
або діаграми
причинно-
наслідкових зв'язків

(так звані діаграми
риб'ячої кістки,
оскільки вони
виглядають як
кістки риби)
визначають
потенційні причини
певних проблем (в
тому числі і ризиків)



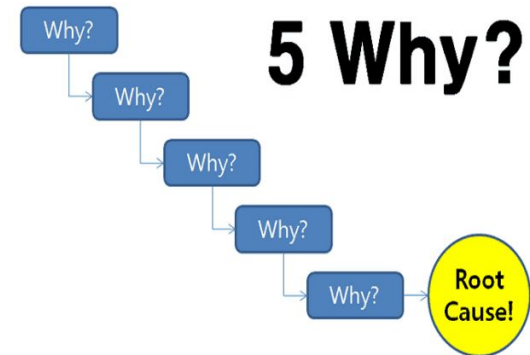
Підхід 5 ЧОМУ у аналізі причин ризиків

5 WHYS / 5 ЧОМУ - візуальний інструмент, який зазвичай використовується на засіданнях робочих груп для виявлення першопричини проблеми.

Ведучий зустрічі записує на аркуші запитання, наприклад, «Чому цей документ не запобіг дефекту?» Робоча група відповідає, а модератор продовжує задавати питання «Чому?» до тих пір, поки не стане очевидною першопричина.

В цьому випадку не потрібно задавати питання 5 разів: це може бути 3 або 7 разів, тобто стільки, скільки необхідно для отримання першопричини

Результати обговорення зазвичай фіксуються на причинно-наслідковій діаграмі (діаграма Ішикави).



- ✓ П'ять чому (або 5 чому) — це ітеративна опитувальна техніка, яка використовується для дослідження причинно-наслідкових зв'язків, що лежать в основі певної проблеми
- ✓ Основна мета методики – визначити першопричину (наприклад, ризику) чи проблеми шляхом повторення запитання «Чому?». Кожна відповідь є основою для наступного запитання. «П'ять» у назві походить від спостереження щодо кількості ітерацій, необхідних для вирішення проблеми.
- ✓ Не всі проблеми мають одну першопричину. Якщо хтось хоче виявити кілька основних причин, цей метод потрібно повторювати, ставлячи щоразу іншу послідовність питань.
- ✓ Метод не передбачає жорстких і швидких правил щодо того, які рядки запитань досліджувати або як довго продовжувати пошук додаткових першопричин. Таким чином, навіть якщо метод ретельно дотримується, результат все одно залежить від знань і наполегливості залучених людей.

Аналіз Парето / Pareto Analysis у аналізі причин ризиків

Аналіз Парето — це формальна техніка для виявлення складних питань (issues), які викликають більшість проблем у проекті.

Принцип Парето стверджує, що, як правило, **80% наслідків походять від 20% причин** (наприклад, 80% витрат можуть бути віднесені до 20% діяльності або **80% наслідків ризику можуть виникати лише через 20% ідентифікованих ризиків**).

Зосереджуючись на цих основних проблемах (20%), аналіз Парето може бути корисним для управління ризиками або якістю, оскільки він допомагає зосередитися на тих ризиках або проблемах якості, які мають найбільший вплив на проект, тому сприяє визначенню пріоритетності необхідних дій щодо пом'якшення або надзвичайних (contingency) заходів.

Методи збору та аналізу інформації про ризик

Збір інформації

Мозковий штурм. Мета мозкового штурму - отримати вичерпний перелік проектних ризиків. Ідеї щодо проектного ризику формуються під керівництвом фасилітатора, або в рамках традиційного сеансу мозкового штурму у вільній формі, або в структурованих методах масового інтерв'ю.

Техніка Delphi. Техніка Delphi - це спосіб досягти консенсусу експертів. Експерти з проектних ризиків беруть участь у цій методиці анонімно. Фасилітатор використовує анкету, щоб отримати ідеї про важливі ризики проекту. Відповіді підсумовуються і потім повторно передаються експертам для подальшого коментаря.

Інтерв'ю. Опитування досвідчених учасників проекту, зацікавлених сторін та експертів з предметів допомагає виявити ризики.

Аналіз інформації

Аналіз кореневих причин. Аналіз кореневих причин - це специфічна методика, яка використовується для виявлення проблеми, виявлення основних причин, що призводять до неї, та розробки профілактичних дій.

SWOT-аналіз ризиків. Ця методика вивчає проект з позицій сильних, слабких сторін, можливостей та загроз (SWOT), щоб збільшити широту виявлених ризиків, включаючи внутрішньо генеровані ризики. Методика починається з виявлення сильних і слабких сторін організації, орієнтуючись або на проект, організацію, або бізнес-сферу загалом. Потім SWOT-аналіз визначає будь-які можливості для проекту, які впливають із організаційних сильних сторін, та будь-які загрози, що виникають внаслідок організаційних слабкостей. Аналіз також вивчає ступінь, якою організаційні сильні сторони компенсують загрози, а також виявлення можливостей, які можуть послужити подоланню слабких місць.

Ризик – менеджмент: наради

- ✓ складаються високорівневі плани дій з управління ризиками
- ✓ розробляються елементи вартості та операції розкладу для управління ризиками, які включаються відповідно до бюджету і розклад проекту
- ✓ встановлюються або переглядаються підходи до використання резервів та можливі втрати від ризиків
- ✓ призначаються сфери відповідальності з управління ризиками
- ✓ наявні в організації загальні шаблони, що стосуються категорій ризиків і визначень термінів (наприклад, матриця ймовірності і впливу), адаптуються до конкретного проекту з урахуванням його специфіки
- ✓ якщо шаблонів для інших кроків процесу не існує, вони можуть бути створені в ході даних нарад