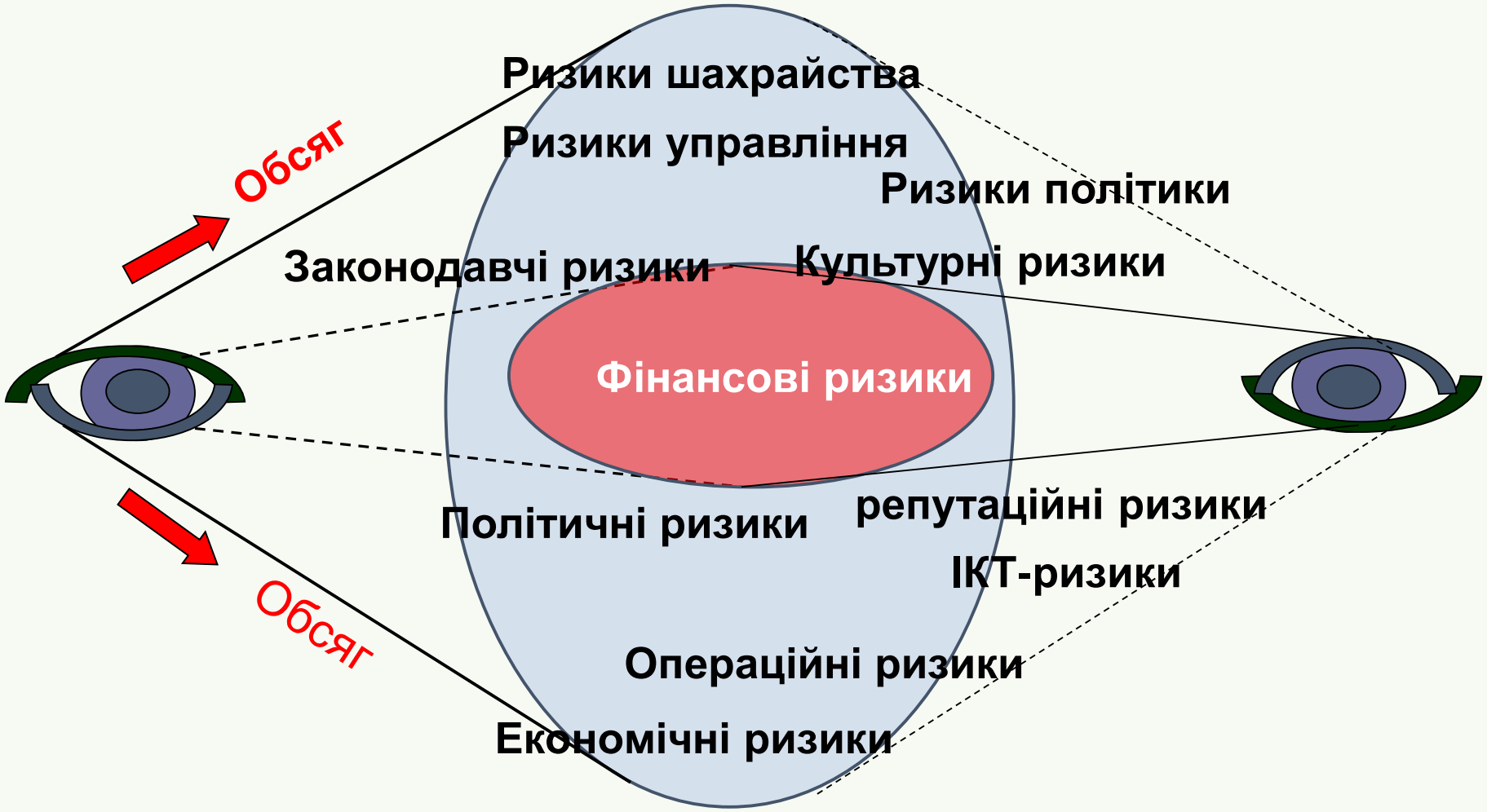
Ministry of Finance

УПРАВЛІННЯ РИЗИКАМИ В КОНКРЕТНИХ КАТЕГОРІЯХ

Манфред ван Кестерен
01/03/2023

Широкий погляд на ризики з боку керівництва та внутрішнього аудиту



Ризики викликаються різними факторами

- **Зовнішні фактори** можуть включати, але не обмежуються змінами в політичному середовищі, законодавстві та нормативних актах, бюджетах, зовнішніх зацікавлених сторонах, форс-мажорних обставинах, соціальному та технологічному середовищі та економічних питаннях, що впливають на організацію.
- **Внутрішні фактори** виникають внаслідок вибору, який керівництво робить щодо внутрішньої організації. Сюди можна віднести інфраструктуру організації, кількість локацій, на яких вона працює, навички та компетентність персоналу, а також те, як працюють бізнес-інформаційні системи.

Управління ризиками на різних рівнях

Стратегічні ризики - це небажані події, які можуть мати негативний вплив на реалізацію довгострокових та середньострокових цілей, стратегічних пріоритетів установи, національних та/або місцевих пріоритетів, пріоритетів окремих державних функцій або секторів (наприклад, охорона здоров'я, навколишнє середовище, правосуддя, стабільність державних фінансів, безпека тощо). Стратегічні ризики зосереджені на більш широких групах інтересів, громадянах, кінцевих споживачах послуг тощо.

Управління стратегічними ризиками належить до компетенції керівника установи, який повинен тісно співпрацювати з найвищим рівнем керівництва установи та установами, що входять до її складу, з метою управління стратегічними ризиками. Управління стратегічними ризиками має бути розроблене як компонент процесів стратегічного планування та ухвалення ключових рішень на найвищому управлінському рівні.

Управління ризиками на різних рівнях

Операційні ризики - це небажані події, які можуть мати негативний вплив на виконання функцій, видів діяльності та процесів у встановлені строки, на рівень якості послуг, помилки у виконанні законів та процедур. Необхідно враховувати, що кумулятивний ефект операційних ризиків може також впливати і загрожувати реалізації деяких стратегічних цілей, і таким чином операційні ризики можуть також спричиняти стратегічні ризики.

Управління операційними ризиками є обов'язком керівників, відповідальних за процеси/діяльність, тобто керівників структурних підрозділів, в яких ці процеси/діяльність реалізуються.

Групування ризиків: стратегічний рівень

Політичні	ризики, пов'язані з неможливістю досягнення поставлених політичних цілей, політичних програм уряду, місцевої громади тощо.
Фінансові/економічні	ризики, які можуть мати негативний вплив на довгострокову фінансову стійкість та стабільність установи
Форс-мажорні	ризики, які можуть мати негативний вплив на здатність органів державного управління реагувати на неочікувані зовнішні значні події (війна, пандемія тощо)
Технологічні	ризики, пов'язані з тим, як органи державного управління реагують на технологічні зміни
Законодавчі	ризики, пов'язані зі змінами в законодавстві, які впливають на зміни в діяльності установ, можуть мати вплив на збільшення витрат на діяльність, на зміну джерел фінансування тощо.
Екологічні/зміна клімату	ризики, пов'язані зі змінами в навколишньому середовищі, зміною клімату та їхнім впливом на якість життя громадян та економіку

Групування ризиків: операційний рівень

Професіоналізм і компетенція співробітників	ризики, пов'язані з непрофесійною поведінкою працівників, що може бути особливо вираженою проблемою, якщо працівники безпосередньо контактують з кінцевими споживачами послуг
Фінансові	ризики, пов'язані з помилками у фінансовій діяльності, бюджетному плануванні та виконанні бюджету, процедурах державних закупівель та укладанні договорів
Регуляторні	ризики, пов'язані з недотриманням або частковим дотриманням правил і процедур у діяльності, що може призвести до негативного висновку зовнішнього аудиту, результатів перевірок, можливих судових позовів, судових розглядів тощо.
Захист людей/майна та інших ресурсів	ризики, пов'язані з безпекою працівників, користувачів послуг, ризики, пов'язані із захистом майна від крадіжок, незаконної конфіскації, пожеж, нераціонального поводження тощо.
Постачальники/зовнішні партнери	ризики, пов'язані зі здатністю постачальників надавати послуги/товари/роботи вчасно та відповідно до контрактної ціни, кількості, якості, наданих гарантій тощо.
Технологічні	ризики, пов'язані з IT-системами, обладнанням, технікою тощо.
Ризики порушень та шахрайства	Ці ризики можуть бути спровоковані, наприклад, відсутністю розподілу обов'язків у важливих фінансових процесах та/або слабким внутрішнім контролем за запобіганням та виявленням шахрайства

Три ключові сфери ризику для фокусування:

- Управління ризиками, пов'язаними з шахрайством та корупцією
- Управління ризиками, пов'язаними з (кібер)безпекою
- Управління ризиками, пов'язаними з форс-мажорними обставинами (стійкість)

Управління ризиками, пов'язаними з шахрайством та корупцією

Забезпечує наявність в організації відповідної політики запобігання шахрайству та корупції

Забезпечує повну обізнаність організації з поточними ризиками шахрайства та корупції, з якими зустрічається установа

Забезпечує наявність в організації належних заходів контролю для усунення/зниження виявлених ризиків шахрайства та корупції - як превентивного, так і виявляючого контролю.

Управління ризиками, пов'язаними з (кібер)безпекою

Оцінка ризиків кібербезпеки - це процес, який допомагає організаціям визначити ключові бізнес-цілі, а потім визначити відповідні IT-активи, необхідні для реалізації цих цілей.

Це передбачає виявлення потенційних кібератак, які можуть негативно вплинути на ці IT-активи. Організація повинна визначити ймовірність виникнення цих атак і визначити вплив, який може спричинити кожна з них.

Оцінка ризиків кібербезпеки повинна відображати все середовище загроз і те, як воно може вплинути на бізнес-цілі організації.

Результат оцінки має допомогти групам з питань безпеки та відповідним зацікавленим сторонам в ухваленні обґрунтованих рішень щодо впровадження заходів безпеки, які пом'якшують ці ризики.

Управління ризиками, пов'язаними з форс-мажорними обставинами (стійкість)

- **Проактивне вжиття поміркованих заходів для пом'якшення** наслідків форс-мажорних обставин. Це може включати рішення про те, як найкраще розподілити обмежену кількість товарів або розглянути можливість заміни.
- **Ведення документального обліку** різних розглянутих варіантів пом'якшення наслідків і кроків, які необхідно вжити. Опрацювання різних сценаріїв.
- **Налагодження процесу постійного аналізу та оцінки потенційних кроків для пом'якшення** наслідків форс-мажорних обставин.