

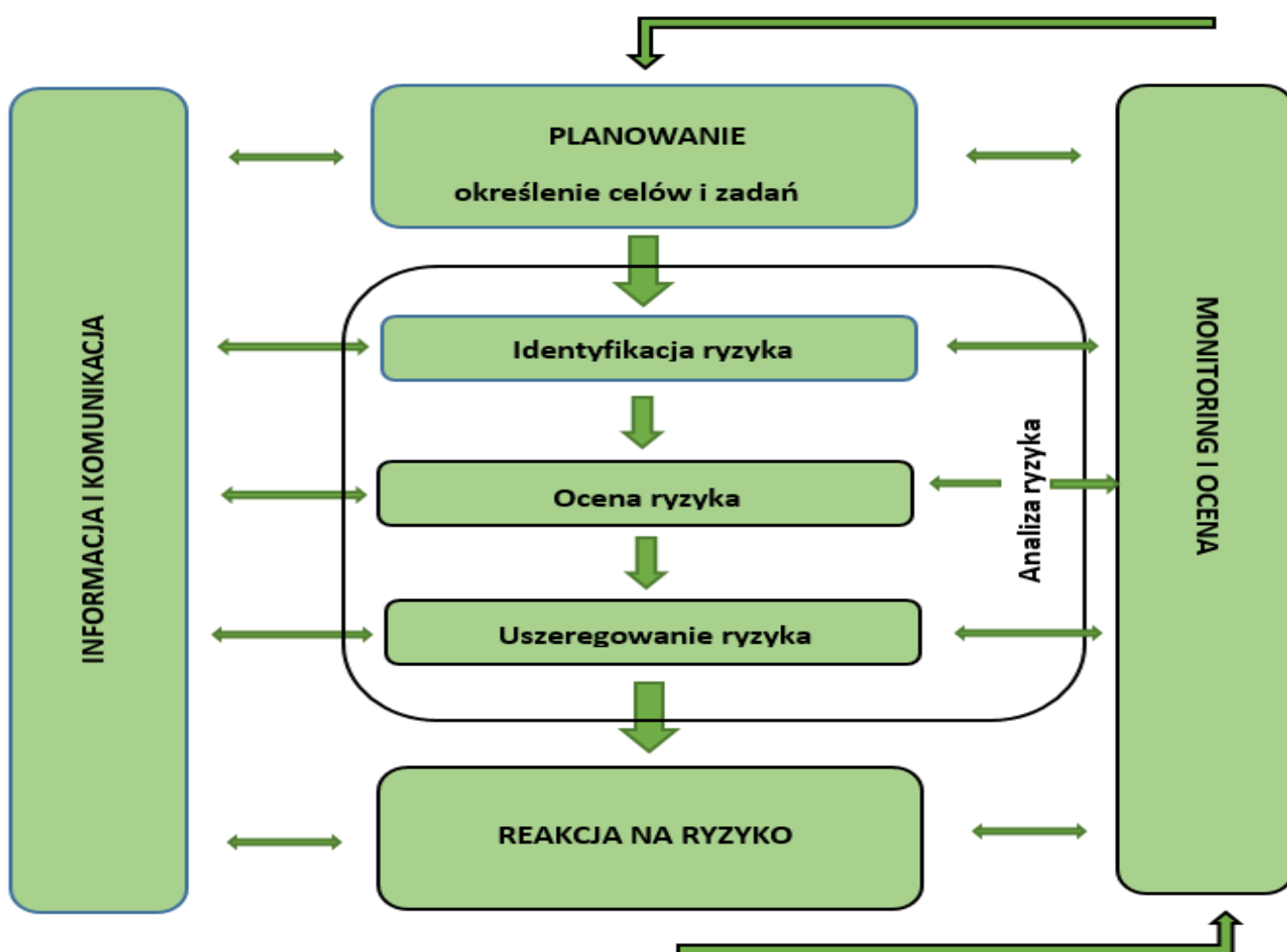
Załącznik nr 1

Zarządzanie ryzykiem oraz reakcja na ryzyko.

Celem zarządzania ryzykiem jest identyfikacja potencjalnych zdarzeń, które mogą wywrzeć wpływ na realizację przez jednostkę w działach jej celów i zadań, utrzymanie ryzyka w ustalonych granicach oraz zapewnienie realizacji celów jednostki.

Ryzykami, które mogą utrudnić lub uniemożliwić realizację celów, należy zarządzać. Warunkiem właściwego zarządzania ryzykiem jest dokładne poznanie i opisanie ryzyka.

Proces zarządzania ryzykiem w działach administracji rządowej energia, klimat i środowisko przedstawiono na poniższym schemacie.



1. Identyfikacja ryzyka

Identyfikacja ryzyka polega na ustaleniu występującego lub możliwego do wystąpienia ryzyka zagrażającego realizacji celów i zadań jednostki w działach. Dla zwiększenia prawdopodobieństwa realizacji celów i zadań kierownik jednostki powinien identyfikować wszystkie zagrożenia związane z realizacją poszczególnych celów i zadań. Ryzyka identyfikowane są przez poszczególnych kierowników jednostek w ramach podległych im obszarów, z uwzględnieniem zagrożeń w jednostkach im podległych lub przez nich nadzorowanych. Każdy właściciel ryzyka prowadzi własny rejestr ryzyk w formie udokumentowanej (np. w formie elektronicznej z możliwością wydruku i podpisania), przy czym obowiązek ten może delegować na wyznaczonego przez siebie koordynatora do spraw ryzyka. Podstawą do budowania rejestru ryzyk są cele określone w planie działalności jednostki w działach.

Identyfikując ryzyka należy:

- 1) określić nazwę ryzyka;
- 2) opisać ryzyko;
- 3) skategoryzować ryzyko – należy przypisać ryzyko do jednej z kategorii zgodnie z załącznikiem nr 2 do komunikatu;
- 4) opisać potencjalne przyczyny wystąpienia ryzyka (wewnętrzne oraz zewnętrzne).

Istotne jest, aby zidentyfikowane ryzyka w rzeczywisty sposób opisywały zagrożenia, które mogą wpłynąć na realizację celów i zadań.

Identyfikacja ryzyka powinna być przeprowadzana:

- 1) okresowo, przynajmniej raz w roku w sposób udokumentowany (np. w formie elektronicznej z możliwością wydruku i podpisania przez kierownika jednostki);
- 2) na bieżąco, jako element rutynowego działania pracowników.

Właściwym momentem analizy ryzyka jest czas, kiedy określone są cele i zadania jednostki na rok następný oraz zasoby przeznaczane na realizację tych zamierzeń.

W identyfikację ryzyk powinny być zaangażowane te same osoby, które będą później odpowiedzialne za realizację wyznaczonych celów i zadań jednostki.

Po zakończonej identyfikacji ryzyk może się okazać, że ryzyka będą tworzyć określone grupy, dlatego też wskazane jest ich grupowanie, dzięki czemu zarządzanie ryzykiem zostanie ułatwione i usprawnione.

Ryzyko występuje na wszystkich szczeblach organizacji (osoby zarządzające i pozostali pracownicy), dlatego też identyfikacja ryzyka powinna być przeprowadzana na wszystkich poziomach jednostki.

Ryzyka zidentyfikowane przez pracowników:

- 1) każdy pracownik zobligowany jest do informowania bezpośredniego przełożonego o wszystkich ryzykach przez niego zidentyfikowanych;
- 2) bezpośredni przełożony po przeanalizowaniu zgłoszenia decyduje o konieczności poinformowania koordynatora do spraw ryzyka lub właściciela ryzyka w celu umieszczenia ryzyka w rejestrze ryzyk. Przekazanie informacji na temat ryzyka powinno nastąpić w formie pisemnej (np. e-mailowej) zawierającej szczegółowy opis ryzyka obejmujący przynajmniej nazwę ryzyka oraz potencjalne przyczyny wystąpienia ryzyka;
- 3) właściciel ryzyka decyduje o umieszczeniu nowego ryzyka w rejestrze ryzyk.

2. Ocena ryzyka

Ocena ryzyka powinna być dokonywana w terminach uwzględniających termin opracowania planu działalności jednostki w działach oraz termin okresowej sprawozdawczości z wykonania planu działalności jednostki.

Dokonując oceny ryzyka właściciel ryzyka powinien określić:

- 1) prawdopodobieństwo wystąpienia ryzyka – zgodnie z częścią A załącznika nr 3 do komunikatu;
- 2) skutki wystąpienia ryzyka – zgodnie z częścią B załącznika nr 3 do komunikatu;

Mechanizmy kontroli powinny stanowić odpowiedź na konkretne ryzyko. Należy stosować takie mechanizmy kontroli, których koszty wdrożenia i stosowania nie przewyższają uzyskanych dzięki nim korzyści.

Kierownicy jednostek podległych lub nadzorowanych powinni przekazać właściwemu członkowi kierownictwa Ministerstwa wyniki oceny ryzyka wraz z:

- 1) projektem planu działalności jednostki;
- 2) okresowymi sprawozdaniami z wykonania planu działalności jednostki.

Ocena ryzyka dostarcza informacji niezbędnych do uszeregowania ryzyk oraz zawiera propozycje postępowania z nimi.

Poziom ryzyka należy określać przyporządkowując im właściwą wartość liczbową, określoną w załączniku nr 3 do komunikatu. Opis dla danej wartości jest pomocniczy i nie w każdym przypadku będzie w pełni adekwatny.

3. Uszeregowanie ryzyka

Każdy właściciel ryzyka w ramach przeprowadzanej oceny ryzyka powinien wskazać ryzyka z grupy ryzyk o najwyższej wartości poziomu ryzyka, które uważa za nieakceptowalne w swojej działalności.

Dla każdego z ryzyk nieakceptowalnych należy zaproponować działania – plan postępowania.

Poprzez uszeregowanie ryzyk zostaną wskazane:

- 1) ryzyka nieakceptowalne, wobec których muszą zostać podjęte dodatkowe działania;
- 2) ryzyka, które wymagają szczególnego monitorowania;
- 3) ryzyka nie niosące istotnego zagrożenia dla realizacji celów i zadań.

4. Reakcja na ryzyko

W celu określenia planu postępowania z ryzykiem należy przeanalizować:

- 1) przyczyny ryzyka i możliwe scenariusze rozwoju;
- 2) skuteczność istniejących mechanizmów kontroli, tj. zakres, w jakim przeciwdziałają one ryzyku.

Aby określić metody postępowania z ryzykiem nieakceptowalnym rekomendowane jest rozpisanie ryzyka zgodnie z załącznikiem nr 4 do komunikatu.

Przyjmuje się, iż w odniesieniu do ryzyk nieakceptowalnych można podjąć następujące działania:

- 1) **unikanie ryzyka** – odejście od działań, które wiążą się z ryzykiem;

- 2) **minimalizacja ryzyka (zapobieganie)** – podjęcie działań mających na celu minimalizację prawdopodobieństwa lub skutków wystąpienia ryzyka lub obu jednocześnie;
- 3) **transfer ryzyka (przeniesienie)** – ograniczenie prawdopodobieństwa i efektu wystąpienia danego zdarzenia poprzez przekazanie w całości lub częściowo innej stronie;
- 4) **akceptacja ryzyka (tolerowanie)** – przyjmuje się, że ryzyka skrajne, nieakceptowalne można zaakceptować w przypadku braku możliwości podjęcia działań ograniczających poziom danego ryzyka.

Dla każdej propozycji postępowania z ryzykiem nieakceptowalnym należy dokonać analizy korzyści i kosztów, zgodnie z załącznikiem nr 5 do komunikatu, a następnie ustalić „budżet na dane ryzyko”. Analiza kosztów i korzyści powinna obejmować porównanie każdego z proponowanych działań w zakresie:

- 1) wpływu na prawdopodobieństwo zaistnienia ryzyka;
- 2) wpływu na skutki wystąpienia ryzyka;
- 3) korzyści (również dodatkowych szans);
- 4) kosztu (nie tylko finansowego);
- 5) możliwego wpływu na inne ryzyka.

Za wdrożenie planów postępowania z ryzykiem odpowiadają właściciele ryzyk.

5. Ryzyka zmaterializowane

Ryzyko zmaterializowane jest to ryzyko, które faktycznie zaistniało i miało wpływ na osiągnięcie celów i zadań jednostki w działach w danym roku.

Właściciel ryzyka przed złożeniem oświadczenia o stanie kontroli zarządczej powinien stworzyć wykaz obrazujący zaistniałe ryzyka w roku poprzednim.

Kierownik jednostki podległej lub nadzorowanej powinien przekazać Ministrowi Klimatu i Środowiska, wraz z oświadczeniem o stanie kontroli zarządczej, wykaz wszystkich ryzyk zmaterializowanych w roku poprzednim, za pośrednictwem właściwej komórki organizacyjnej Ministerstwa Klimatu i Środowiska realizującej zadania z zakresu nadzoru nad daną jednostką na podstawie regulaminu organizacyjnego Ministerstwa Klimatu i Środowiska, w terminie do 15 lutego każdego roku.

Kategorie ryzyk

Wszelkie zidentyfikowane ryzyka przyporządkowywane są do jednego z trzech obszarów ryzyka:

- a) ryzyko strategiczne,
- b) ryzyko finansowe,
- c) ryzyko operacyjne.

Obszar ryzyka	Kategoria	Opis
I. Ryzyko strategiczne Ryzyka związane ze zdarzeniami mającymi bezpośredni wpływ na osiągnięcie celów strategicznych lub ich zaniechanie. Ryzyka w tym obszarze mają charakter długoterminowy.	I.1 Otoczenie polityczne	Ryzyka związane z tworzeniem prawa.
	I.2 Otoczenie społeczne	Ryzyka związane ze społecznym odbiorem działalności jednostki.
II. Ryzyko finansowe Ryzyka związane z finansowaniem działalności jednostki, w tym między innymi zapewnieniem środków na bieżące funkcjonowanie, racjonalnym zarządzaniem wolnymi środkami oraz właściwym rozliczaniem wyniku finansowego.	II.1 Proces inwestycyjny	Ryzyka związane z uczestnictwem w procesach inwestycyjnych.
	II.2 Księgowanie	Ryzyka związane z błędami księgowymi.
	II.3 Sprawozdawczość finansowa	Ryzyka związane z przygotowaniem, przekazaniem sprawozdań finansowych.
	II.4 Pozyskanie środków finansowych	Ryzyka związane z finansowaniem działalności jednostki.
	II.5 Wydatkowanie środków finansowych	Ryzyka związane z wydatkowaniem środków finansowych przez jednostkę.
III. Ryzyko operacyjne Ryzyka związane bezpośrednio z zadaniami realizowanymi przez poszczególne komórki organizacyjne i wynikające z niedoskonałości procesów wewnętrznych, błędów ludzkich, błędów systemów komputerowych oraz zdarzeń zewnętrznych.	III.1 Bezpieczeństwo informacji	Ryzyka związane z utratą poufności, integralności, dostępności informacji.
	III.2 Informatyka	Ryzyka związane z zapewnieniem i wykorzystywaniem zasobów informatycznych.
	III.3 Zasoby ludzkie	Ryzyka związane z zatrudnianiem, szkoleniem zasobów ludzkich.

	III.4 Organizacja	Ryzyka związane bezpośrednio z organizacyjnymi problemami w działalności jednostki.
	III.5 Sprawozdawczość	Ryzyka związane z przygotowaniem, przekazaniem sprawozdań (nie dotyczących strictly finansów).
	III.6 Oszustwo	Ryzyka związane z łamaniem prawa oraz przekraczaniem uprawnień.
	III.7 Współpraca	Ryzyka związane ze współdziałaniem jednostki z innymi jednostkami lub Ministerstwem Klimatu i Środowiska.
	III.8 Bezpieczeństwo i ochrona	Ryzyka związane z bezpieczeństwem i ochroną obiektów jednostki oraz zawartych w nich zasobów.

Skale oceny ryzyka

Część A (prawdopodobieństwo)

Pierwszym kryterium oceny każdego z ryzyk jest prawdopodobieństwo wystąpienia ryzyka na dzień przeprowadzenia oceny.

Prawdopodobieństwo wystąpienia danego ryzyka należy ocenić w pięciostopniowej skali przedstawionej w tabeli poniżej oraz wskazać dodatkowe czynniki mające wpływ na zwiększenie bądź ograniczenie prawdopodobieństwa wystąpienia zdarzenia, tj.:

- 1) dotychczasowe doświadczenia – częstość występowania danego zdarzenia, ryzyka,
- 2) stosowane (bądź nie) na dzień przeprowadzania analizy w odniesieniu do danego ryzyka mechanizmy kontroli oraz ich skuteczność. Przez mechanizmy kontroli należy rozumieć polityki, procedury, techniczne środki zabezpieczeń oraz inne zaprojektowane rozwiązania, jak również rzeczywiste praktyki stosowane w celu prewencji zdarzeń lub redukcji skutków w przypadku zmaterializowania się ryzyka np.: szkolenia, podział odpowiedzialności, listy sprawdzające, stosowanie drugiej pary oczu, monitorowanie, kary umowne, ubezpieczenia,
- 3) w przypadku kolejnych ocen/analiz ryzyka należy uwzględnić działania już podjęte (a wykazane w poprzednim rejestrze ryzyka jako działania niezbędne do podjęcia w odpowiedzi na ryzyko), jako istniejące mechanizmy kontroli,
- 4) dużą liczbę i intensywność działań podejmowanych w ramach procesu, np. obliczenia dokonywane pod presją czasu, przygotowywanie raportów i sprawozdań, wzrost intensywności pracy w pewnych okresach,
- 5) liczbę komórek organizacyjnych i innych podmiotów zaangażowanych w realizację celów, zadań i projektów w danym obszarze – potrzeba współdziałania, współpracy, przepływu informacji,
- 6) zmiany technologiczne, organizacyjne, kadrowe w danym obszarze (ich częstość, zakres, istotność), wchodzące zmiany przepisów prawnych,
- 7) poziom uregulowania prawnego danego obszaru regulacjami o różnym charakterze (ustawy, rozporządzenia, uchwały, zarządzenia),
- 8) inne czynniki mające wpływ na zwiększenie bądź ograniczenie prawdopodobieństwa wystąpienia zdarzenia.

Prawdopodobieństwo	
5	<p>Prawie pewne</p> <p>Zagrożenie jest bardzo wysokie. Od 81 do 100%, że wystąpi regularnie co miesiąc lub częściej. Oczekuje się, że zdarzenie takie nastąpi, dotyczy wszystkich lub prawie wszystkich spraw.</p>
4	<p>Duże</p> <p>Zagrożenie jest wysokie Od 61% do 80%, że wystąpi regularnie, przynajmniej raz w roku. Zaistnienie zdarzenia jest bardzo prawdopodobne, dotyczy większości spraw.</p>
3	<p>Średnie</p> <p>Zagrożenie jest realne. Od 41% do 60%, że wystąpi w przeciągu 3 lat. Zaistnienie zdarzenia jest średnio możliwe, ale w niektórych przypadkach zdarzenie takie może mieć miejsce.</p>

2	Małe	Zagrożenie jest mało realne. Od 21% do 40%, że wystąpi raz na 5 lat. Istnieje małe prawdopodobieństwo zaistnienia tego zdarzenia, może wystąpić kilka razy w okresie 5 lat, dotyczy nielicznych spraw.
1	Bardzo rzadkie lub prawie niemożliwe	Zagrożenie jest raczej nierealne. Od 1% do 20%, że wystąpi raz na 10 lat. Zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach, a najprawdopodobniej w ogóle nie zaistnieje, nie wystąpiło dotychczas, dotyczy jednostkowych spraw.

Część B (skutki)

Dokonując oceny skutku wystąpienia danego ryzyka należy brać pod uwagę najbardziej prawdopodobne konsekwencje spowodowane zmaterializowaniem się ryzyka przede wszystkim w ramach trzech kryteriów: finanse, reputacja oraz realizacja zadań.

Skutek urzeczywistnienia się ryzyka (zagrożającego realizacji celu/zadania/projektu) należy ocenić poprzez wskazanie odpowiedniej wartości na podstawie 5-stopniowej skali skutków wystąpienia ryzyka (opisanej w tabeli poniżej) oraz wskazać dodatkowe czynniki mające wpływ na podjęcie decyzji, w celu ograniczenia skutków wystąpienia ryzyka, tj.:

- 1) skalę potencjalnych strat finansowych (dodatkowych kosztów), zobowiązań finansowych,
- 2) wartość majątku narażonego na utratę bądź uszkodzenie,
- 3) odpowiedzialność prawną wynikającą z niezgodności z przepisami prawa, z postanowieniami umów, istnienie (bądź nie) procedur regulujących dany proces,
- 4) skalę zakłóceń organizacyjnych – wpływ na możliwość realizacji celów, zadań i projektów, np. brak zachowania ciągłości procesów działania, utrzymaniu funkcjonalności systemu niezbędnych do wykonywania podstawowych celów,
- 5) wpływ na wizerunek (np. w kontekście odbioru społecznego, zainteresowania mediów, zasięg oddziaływania tych mediów),
- 6) stosowane (bądź nie) na dzień przeprowadzania analizy w odniesieniu do danego ryzyka mechanizmy kontroli redukujące skutki wystąpienia ryzyka w przypadku zmaterializowania się ryzyka oraz ich skuteczność.

Skutek		
5	Katastrofalny	Brak realizacji celu/zadania/projektu, bardzo poważne i rozległe konsekwencje prawne, wysokie straty finansowe, naruszenie bezpieczeństwa pracowników, utrata dobrego wizerunku Ministerstwa, wielokrotne negatywne informacje w mediach ogólnokrajowych.
4	Poważny	Poważny wpływ na realizację celu/zadania/projektu – zagrożenie terminu jego realizacji i osiągnięcia celu, poważne konsekwencje prawne, poważne straty finansowe, zagrożenie bezpieczeństwa pracowników, poważny wpływ na wizerunek Ministerstwa, jednokrotne negatywne informacje w mediach ogólnokrajowych.
3	Średni	Średni wpływ na realizację celów, zadań i projektów, zakłócenia w działalności, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek Ministerstwa, negatywne informacje w mediach lokalnych.

2	Mały	Mały wpływ na realizację celów, zadań i projektów, niewielkie zakłócenia w działalności, brak skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek Ministerstwa.
1	Nieznacznym	Znikomy wpływ na realizację celów, zadań i projektów, krótkotrwałe zakłócenia w działalności, brak skutków prawnych, nieznacznym skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek Ministerstwa, brak negatywnych informacji w mediach.

Część C (szeregowanie)

Do uszeregowania ryzyk należy posłużyć się mapą ryzyk opierającą się na 5 – stopniowej skali oceny skutku i prawdopodobieństwa wystąpienia ryzyka oraz kryteriami poziomu istotności ryzyka.

Mapa ryzyk:

Skutek (S) Prawdopodobieństwo (P)	Nieznacznym (1)	Mały (2)	Średni (3)	Poważny (4)	Katastrofalny (5)
Bardzo rzadkie lub prawie niemożliwe (1)	1	2	3	4	5
Małe (2)	2	4	6	8	10
Średnie (3)	3	6	9	12	15
Duże (4)	4	8	12	16	20
Prawie pewne (5)	5	10	15	20	25

Kryteria poziomu istotności ryzyka:

Poziom	Ryzyko
1-5	Małe
6-9	Średnie
10-16 oraz gdzie P=1 a S=5	Duże
20-25	Bardzo duże

Następnie należy wskazać działanie, które zostanie podjęte w celu utrzymania zidentyfikowanego ryzyka na akceptowanym poziomie, tj. należy odpowiednio wskazać: akceptacja, minimalizowanie, transfer, unikanie, wg kryteriów zawartych w poniższej tabeli.

Poziom	Ryzyko	Rodzaj reakcji na ryzyko
1-5	Małe	1. Akceptacja
6-9	Średnie	1. Akceptacja 2. Minimalizowanie
10-16 oraz gdzie P=1 a S=5	Duże	1. Minimalizowanie 2. Transfer 3. Akceptacja (wraz z pisemnym uzasadnieniem) 4. Unikanie
20-25	Bardzo duże	1. Minimalizowanie 2. Transfer 3. Akceptacja (wraz z pisemnym uzasadnieniem) 4. Unikanie

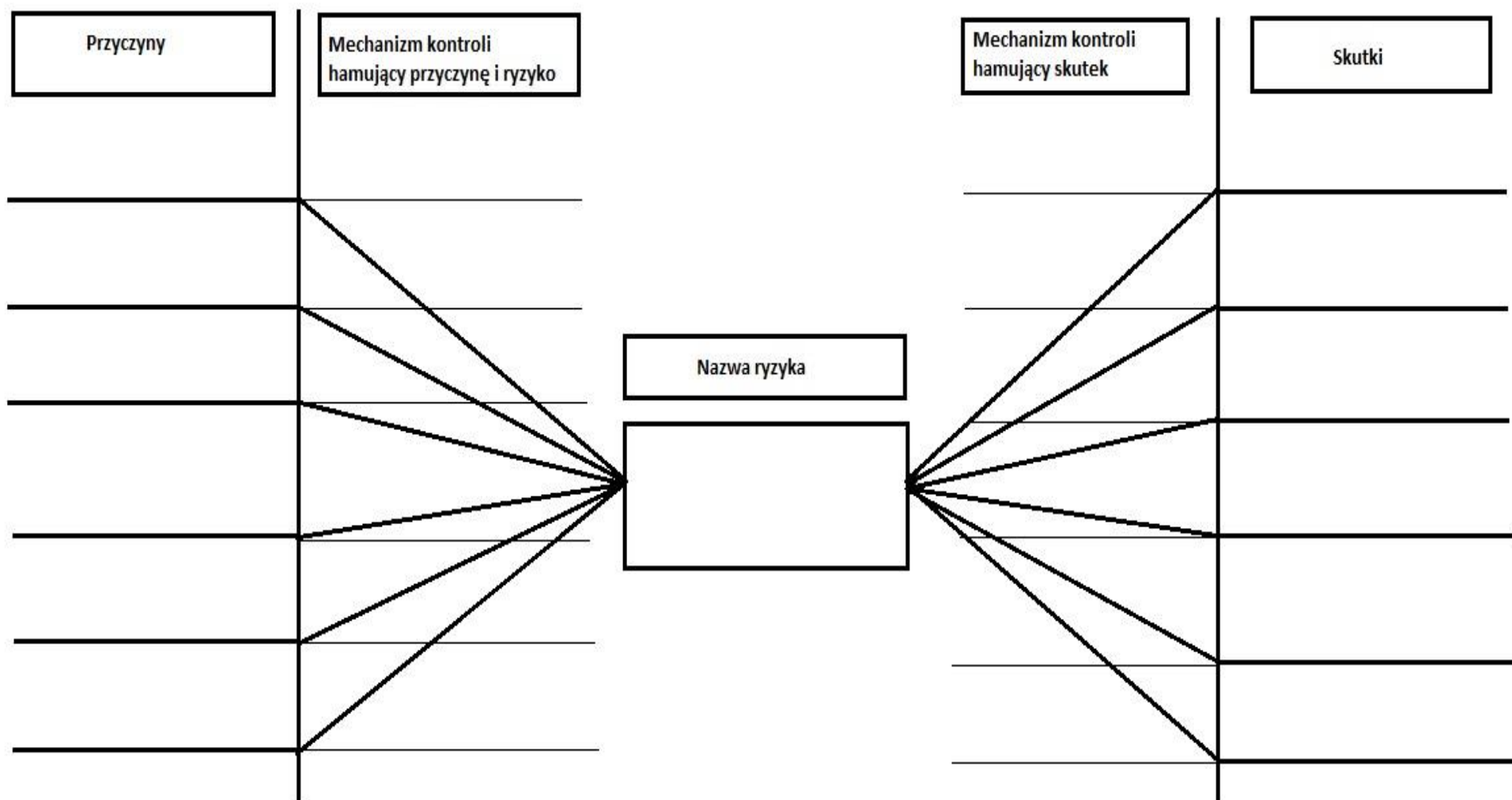


Tabela postępowania z ryzykiem nieakceptowalnym

<i>Liczba porządkowa ryzyka z rejestru ryzyk oraz nazwa ryzyka</i>						
Lp.	Opis działania	Korzyści	Osoba odpowiedzialna	Termin realizacji	Szacowany koszt	Stan realizacji¹⁾
1.						
2.						
3.						

¹⁾ Należy określić stopień realizacji (niezrealizowane; w trakcie realizacji; zrealizowane) wraz z komentarzem/wyjaśnieniem dot. stanu realizacji. Stan realizacji powinien być poddawany bieżącemu monitorowaniu.

Wzór rejestru ryzyk²

Lp.	Cel / zadanie jednostki	Nazwa ryzyka	Opis ryzyka ³	Kategoria ryzyka	Prawdopodobie ństwo (P)		Skutek (S)		Poziom istotności ryzyka (Pi) Pi=P*S	Ryzyko akceptowalne [tak/nie]	Reakcja na ryzyko	Plan postępowania z ryzykiem		
					ocena	opis	ocena	opis				Opis działania	Termin realizacji	Stan realizacji
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1														
2														
3														
...														

² Wzór określa minimum informacji, która ma się znaleźć w rejestrze. Kierownik jednostki może dowolnie rozbudować rejestr ryzyk.

³ Należy opisać m.in. przyczyny wystąpienia ryzyka.