

ZAMÓWIENIA PUBLICZNE AGENCJI UNII EUROPEJSKIEJ

Aneta Wilk-Łyś

26.07.2023 r.

Film szkoleniowy został realizowany przez Polską Agencję Rozwoju Przedsiębiorczości,
w ramach projektu Centrum Rozwoju Małych i Średnich Przedsiębiorstw.



Plan prezentacji:

1. Wprowadzenie – ryzyka w działalności przedsiębiorstwa

- Cechy charakterystyczne mające wpływ na profil ryzyka w małych i średnich przedsiębiorstwach
- Ryzyka w biznesie
- Zarządzanie ryzykiem w małym i średnim przedsiębiorstwie

2. Analiza i ocena ryzyka

- Strategia przedsiębiorstwa, cele strategiczne i operacyjne
- Analiza kluczowych procesów i kontroli
- Mapa ryzyk

3. Reakcja na ryzyko

- Proces zarządzania ryzykiem
- Koncepcja trzech linii obrony, w tym rola audytu wewnętrznego
- Ryzyko informatyczne



Rozdział 1

Wprowadzenie do zarządzania ryzykiem



Cechy charakterystyczne mające wpływ na profil ryzyka w małych i średnich przedsiębiorstwach

- Dominujący wpływ niewielkiej grupy osób na działalność firmy. Przykład: Pan Jan prowadzi niewielki zakład mechaniki samochodowej. Zatrudnia trzy osoby. Pan Jan samodzielnie zarządza przedsiębiorstwem. Czasami pomaga mu jego żona. Pan Jan nie ma zaufania do nikogo innego.
- Ograniczony, w porównaniu do dużych podmiotów, dostęp do finansowania. Przykład: Pan Jan chciałby rozszerzyć działalność o diagnostykę samochodową. W tym celu potrzebuje dobudować jedno skrzydło do obecnego warsztatu. Pan Jan zwrócił się do banku o kredyt. Niestety jako mały przedsiębiorca został uznany przez bank za klienta o wyższym ryzyku i bank zażądał dodatkowego zabezpieczenia. Ustanowiono hipotekę na nieruchomości należącej do pana Jana, co z jego punktu widzenia podwyższyło ryzyko działalności (w razie problemów może stracić główne aktywo).
- Ograniczony dostęp do innych zasobów takich, jak wysoko wykwalifikowany personel, nowoczesne technologie. Przykład: Pan Jan chciałby zatrudnić nowego kierownika do nowej części zakładu. Zauważył, że nie jest wcale łatwo znaleźć dobrze wykwalifikowaną osobę, która chciałaby przyjść do pracy w niewielkim zakładzie. Inną kwestią jest też to, że pan Jan niechętnie dzieli się obowiązkami. Woli mieć sam „na wszystko oko”. Niestety ten brak zaufania do pracowników często spowalnia rozwój firmy.
- Zasięg działania relatywnie ograniczony do lokalnego rynku.



Cechy charakterystyczne mające wpływ na profil ryzyka w małych i średnich przedsiębiorstwach

- Zasięg działania relatywnie ograniczony do lokalnego rynku. Przykład: Pan Jan woli działać na lokalnym rynku, który jest mu znany. Czuje się pewniej działając w mniejszej skali. Stawarza to dodatkowe ryzyko w przypadku wejścia na rynek dużego konkurenta. Koncentracja może kosztować firmę nawet bankructwo.
- Brak możliwości skorzystania z korzyści skali, przez co koszty jednostkowe są stosunkowo wyższe niż w dużych firmach. Przykład: Pan Jan oferuje w zakładzie mechanicznym drobne naprawy. Niestety konkurencja jest wysoka, co często wiąże się z koniecznością obniżki cen. Brak odpowiedniej skali działania powoduje, że często pan Jan musi myśleć jak wiązać koniec z końcem.
- Brak rozbudowanej struktury organizacyjnej (struktura raczej płaska), przewaga nieformalnych, rodzinnych relacji. Przykład: Pan Jan sam zarządza swoim zakładem. Nie ma rozbudowanej struktury organizacyjnej, jak to ma miejsce na przykład w jednej z francuskich sieci zakładów autonapraw. Pan Jan nie ma do nikogo zaufania. Sam zarządza wszystkim i wykonuje różne obowiązki. To niestety stwarza spore ryzyko błędów. Pan Jan zatrudnia głównie osoby z rodziny (lub inne osoby zaprzyjaźnione). Niestety czasem wiąże się to z kłopotami, ponieważ więzi rodzinne biorą górę nad kompetencjami.



Cechy charakterystyczne mające wpływ na profil ryzyka w małych i średnich przedsiębiorstwach

- Duża elastyczność działania umożliwiającą szybsze reakcje na zmieniające się warunki gospodarcze. Przykład: Pan Jan zauważył, że mała działalność ma swoje plusy. Ponieważ nie ma tutaj mowy o rozbudowanej ścieżce decyzyjnej, to łatwiej jest podejmować decyzje, w tym te dotyczące rozwoju firmy. Jednak rozwój oznacza pojawienie się większych ryzyk, a te wymagają uporządkowania i dobrej organizacji pracy.
- Brak formalnych procedur. Przykład: Pan Jan nie lubi wprowadzać żadnych formalnych procedur. Jest zdania, że lepiej poświęcić czas na bieżącą działalność i zarabianie pieniędzy. Niestety brak procedur oznacza zwiększone ryzyko. Często firmy, które nie dbają o tę sferę padają ofiarą oszustw i nadużyć



Ryzyka w biznesie

Ryzyko gospodarcze:

- kluczowe ryzyko w działalności przedsiębiorstwa,
- możliwość zaistnienia zdarzeń, które mogą negatywnie wpływać na zdolność firmy do osiągnięcia celów i realizowania swoich strategii lub na niewłaściwe określenie celów i strategii (np. utrata rynku zbytu, utrata kluczowego personelu, utrata dostępu do surowców, zmiany preferencji klientów, bez możliwości sprostania nowym wymaganiom).



Ryzyko gospodarcze

1. Ryzyko finansowe:

- ryzyko kursowe,
- ryzyko płynności,
- ryzyko stóp procentowych,
- ryzyko kredytowe,
- ryzyko cenowe.

2. Ryzyko operacyjne (związane z działalnością bieżącą), w tym ryzyko defraudacji.

3. Ryzyko braku zgodności z obowiązującymi przepisami.



Ryzyko finansowe

Ryzyko kursowe	Ryzyko płynności	Ryzyko stóp procentowych	Ryzyko kredytowe	Ryzyko cenowe
<p>To ryzyko związane z prowadzeniem działalności całkowicie lub częściowo w walucie obcej (np. wystawiamy lub otrzymujemy faktury w EUR z terminem płatności 30 dni – co oznacza, że przez te 30 dni zmiana w kursie EUR wpływa w sposób niekontrolowany na nasze należności lub zobowiązania).</p>	<p>To ryzyko związane z możliwością utraty płynności (czyli brakiem możliwości zaspokojenia zobowiązań bieżących). Zarządzanie tym ryzykiem, to na przykład umiejętne ustalanie terminów płatności należności (biorąc pod uwagę terminy płatności zobowiązań), polityka sprzedaży gotówkowej, korzystanie z szybkich linii kredytowych wspomagających bieżącą działalność i umożliwiającą bieżącą obsługę zobowiązań w oczekiwaniu na spływ środków z należności.</p>	<p>To ryzyko związane z wpływem zmian stóp procentowych na naszą działalność (np. jeśli korzystamy z kredytu o zmiennym oprocentowaniu).</p>	<p>To ryzyko związane na przykład z korzystaniem przez firmę z usług jednego banku w ramach wszystkich transakcji – co w sytuacji trudności tego banku stwarza zagrożenie dla naszej działalności.</p>	<p>Firmy narażone są na ryzyko cenowe związane ze wzrostem cen najczęściej kupowanych materiałów, surowców, towarów, cen usług świadczonych przez podwykonawców itp.</p>



Ryzyko operacyjne

- Ryzyko wyczerpania się zapasów i braku możliwości realizacji zamówień (Pani Joanna, prowadząca sklep z żywnością ekologiczną korzysta z wielu sprawdzonych źródeł dostaw, poza tym na wypadek awaryjnej sytuacji dysponuje także własną uprawą ekologiczną, która pozwoli jej przetrwać pierwsze trudne chwile).
- Utrata kluczowych pracowników (np. zespołu utalentowanych kucharzy, dietetyków – kluczowych dla funkcjonowania firmy).
- Niewłaściwe zarządzanie (na przykład zbyt duża koncentracja na jednym kontrahencie, brak dywersyfikacji dostaw, nierespektowanie potrzeb pracowników).
- Źle kojarząca się marka (np. ryzyko pojawienia się negatywnych komentarzy dotyczących jakości jednej z serwowanych potraw, co ma implikacje dla wszystkich produktów oznaczonych tą marką).
- Utrata zamówień (np. w wyniku wejścia na rynek konkurencji z lepszym i tańszym odpowiednikiem naszego produktu).



Ryzyko braku zgodności z przepisami

Brak znajomości przepisów może narazić przedsiębiorcę na przykre konsekwencje, np.:

- brak znajomości przepisów podatkowych naraża firmę na różnego rodzaju sankcje, w tym kary pieniężne;
- brak znajomości przepisów branżowych może spowodować utratę pozwoleń (np. koncesji),
- brak znajomości przepisów dotyczących sprawozdawczości finansowej może doprowadzić do sporządzania niezetelnych sprawozdań finansowych.



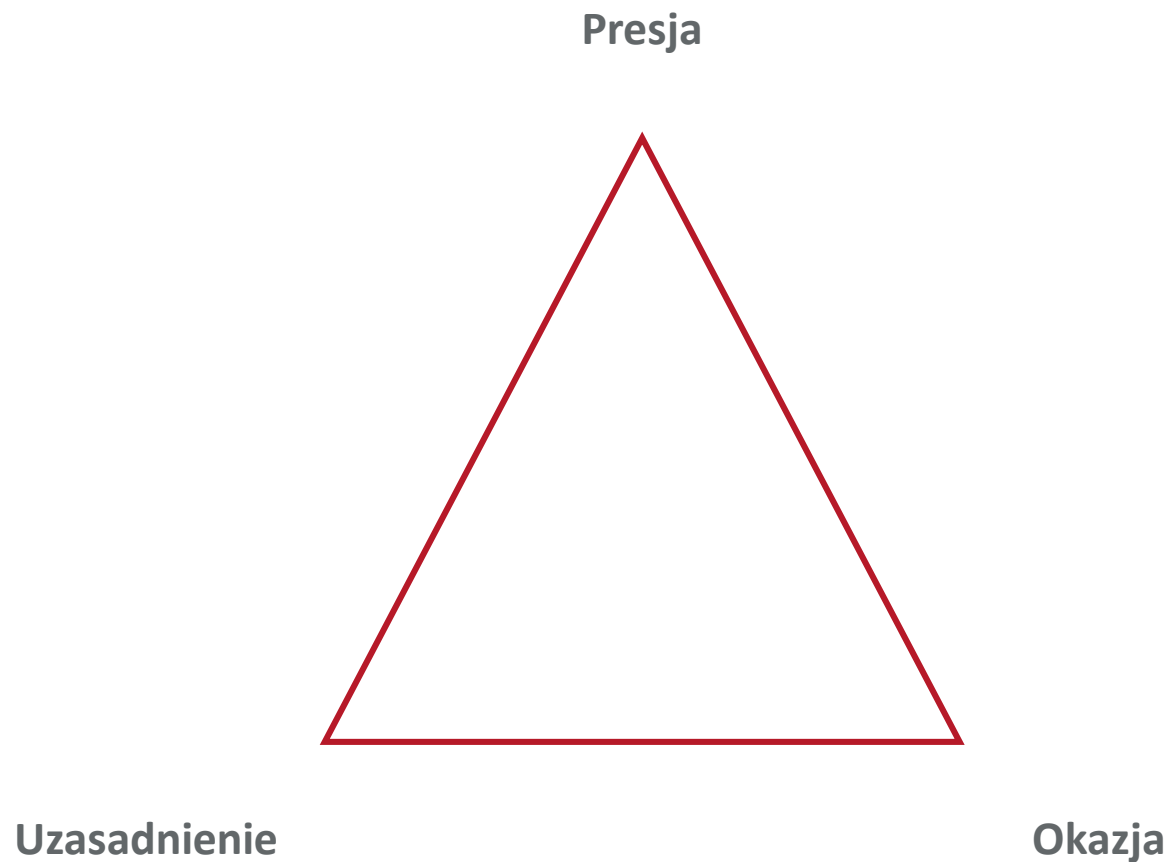
Ryzyko defraudacji

Oszustwo to zamierzone działanie podjęte przez jednego lub kilku członków kierownictwa, właścicieli, członków rady nadzorczej, pracowników lub stronę trzecią (na przykład klienta, dostawcę itp.), przy wykorzystaniu kłamstwa, w celu uzyskania nieuzasadnionej lub niezgodnej z prawem korzyści.

Prawdopodobieństwo wystąpienia defraudacji jest wysokie, jeśli wystąpi tzw. „trójkąt oszustwa”, czyli równocześnie dojdzie do wystąpienia: presji, okazji i uzasadnienia.



Ryzyko defraudacji – trójkąt oszustw



Ryzyko defraudacji – trójkąt oszustw - presja

- Stabilność finansowa lub rentowność firmy są zagrożone.
- Nadmierne naciski wywierane na kierownictwo, aby sprostało oczekiwaniom.
- Osobista sytuacja finansowa kierownictwa jest zagrożona przez finansowe wyniki działalności (np. członkowie zarządu mają kredyty do spłacenia, a jak w firmie będzie się źle działo to mogą stracić pracę, albo występuje pilna potrzeba w związku z chorobą w rodzinie, ale też może być to hazard i potrzeba zaspokojenia długów).
- Niskie morale pracowników i zarządu (np. podwójne życie, hazard).
- Brak poszanowania podstawowych zasad etycznych (np. wykorzystywanie samochodu służbowego do celów prywatnych bez zgody pracodawcy).



Ryzyko defraudacji – trójkąt oszustw - okazja

- Znaczna ilość trudnych pozycji bilansowych wymagających dokonywania częstych szacunków wartości „tylko pani Krysia to rozumie”, czyli nikt nie kontroluje pani Krysi.
- Niekompetentni pracownicy, w tym zarząd (np. zarząd z ambicjami dotyczącymi dużych inwestycji, a mający ograniczoną wiedzę w temacie – błędne rozumienie zdania „kto nie ryzykuje, ten nie pije szampana”).
- Niezainteresowany właściciel np. właściciel to inżynier, wizjoner i sprawy przyziemne, a księgi go nie interesują.
- Duża rotacja personelu (ponieważ oszustwo wtedy łatwiej ukryć).
- Brak procedur, podziału obowiązków (np. księgową, która jako jedyna sporządza deklaracje ZUS, PIT itp. i jednocześnie ma pełne uprawnienia do wykonywania przelewów), słaba kontrola wewnętrzna, brak odpowiedniego personelu.
- Nadmierne skupienie obowiązków i autoryzacji w rękach jednej osoby np. jednego członka zarządu („wie wszystko”, „jest niezastąpiony”).



Ryzyko defraudacji – trójkąt oszustw - uzasadnienie

Przykładowe wyjaśnienia „winowajców”:

- „chciałam/em pożyczyć i zamierzam oddać”,
- „inni też tak robią”,
- „należy mi się”,
- „fałszujemy wyniki finansowe dla dobra firmy, żeby nie doszło do ogłoszenia upadłości”,
- „to zemsta za potraktowanie mnie niesprawiedliwie”.



Zarządzanie ryzykiem w małym i średnim przedsiębiorstwie

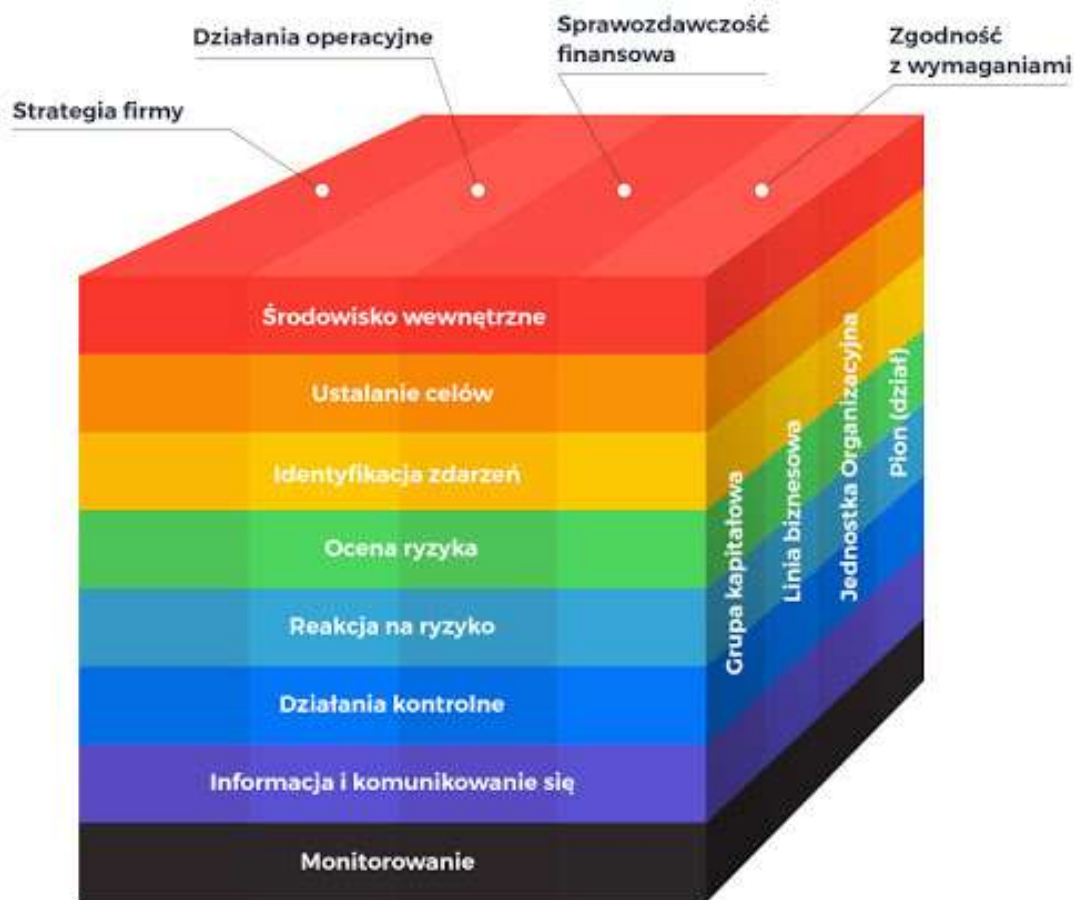
Zarządzanie ryzykiem to cały proces i element strategii firmy.

Celem zarządzania ryzykiem jest identyfikacja potencjalnych zdarzeń (ryzyk), które mogą wywrzeć wpływ na firmę i na realizację jej celów, a następnie utrzymanie ryzyka w ustalonych granicach, tak aby założone cele zostały osiągnięte.

Jest to proces, w którym można wyodrębnić elementy, które są wspólne dla podmiotów różnego typu.



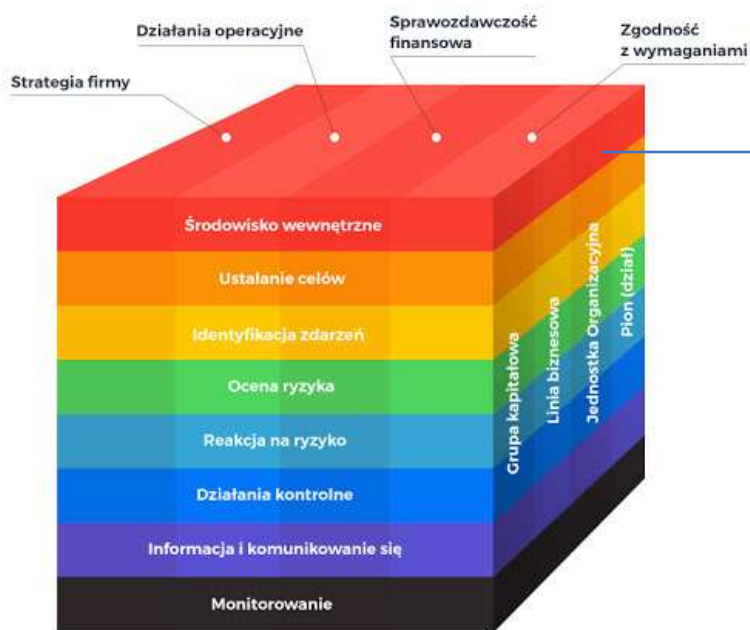
Model COSO – kompleksowy model zarządzania ryzykiem



Schemat przedstawia elementy, jakie składają się na skuteczny mechanizm zarządzania ryzykiem w przedsiębiorstwie.



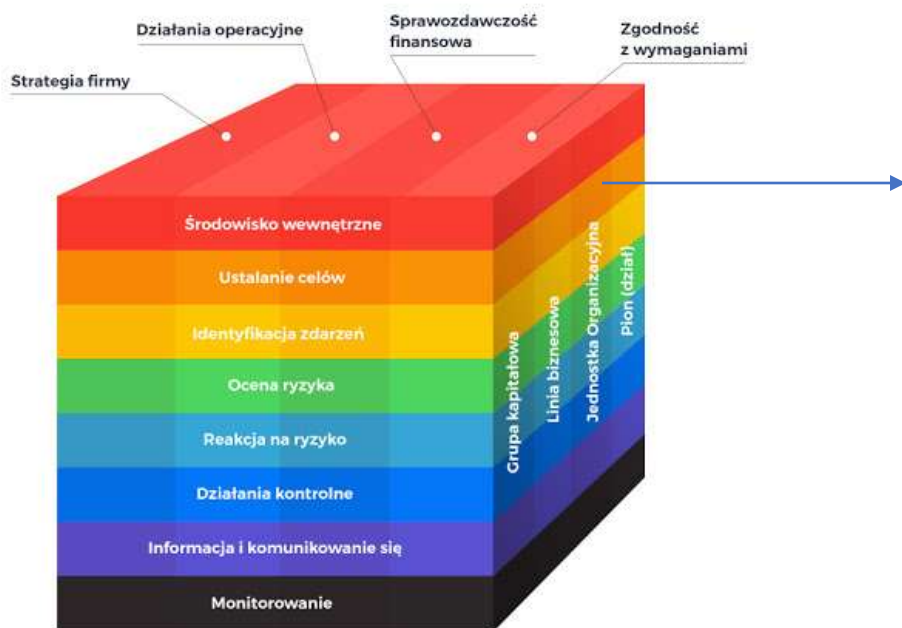
Model COSO – kompleksowy model zarządzania ryzykiem



Środowisko wewnętrzne obejmuje charakter organizacji i klimat w niej panujący. Jest podstawą postrzegania ryzyka przez pracowników i ich reagowaniu na ryzyko. Środowisko wewnętrzne to także filozofia zarządzania ryzykiem oraz określony przez kierownictwo akceptowalny poziom ryzyka, a także uczciwość i wartości etyczne oraz środowisko do pracy.



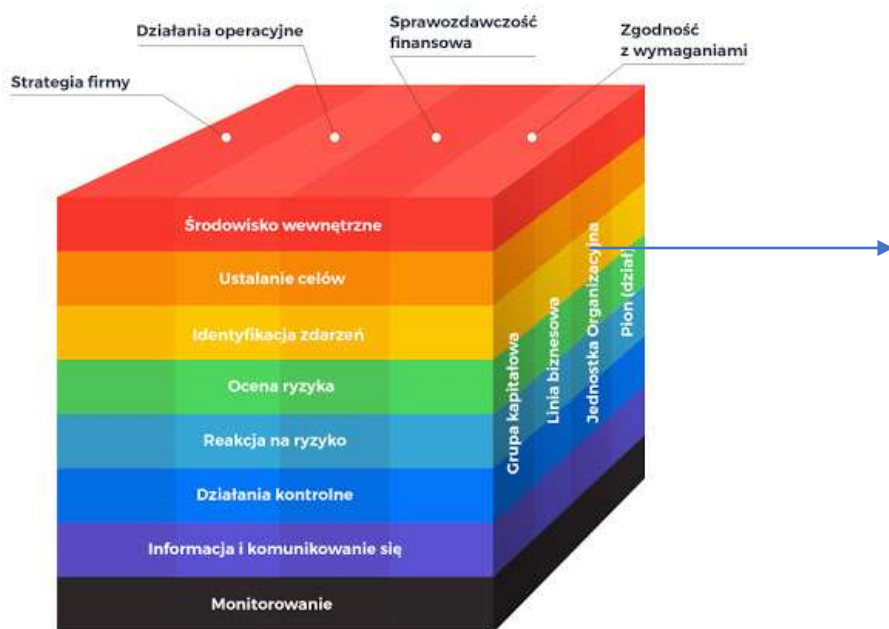
Model COSO – kompleksowy model zarządzania ryzykiem



Ustalenie celów jest kluczowym czynnikiem stabilnego rozwoju firmy. Po ustaleniu celów kierownictwo identyfikuje potencjalne zdarzenia, które mogą mieć negatywny wpływ na ich osiągnięcie. Cele muszą odwoływać się do misji firmy i jej wizji. W ich ustaleniu uwzględniany jest także zaakceptowany wcześniej poziom dopuszczalnego ryzyka.



Model COSO – kompleksowy model zarządzania ryzykiem



Identyfikacja zdarzeń to element, który polega na stworzeniu listy zdarzeń (wewnętrznych i zewnętrznych), które mają wpływ na osiągnięcie celów przez firmę. Są to zdarzenia stanowiące zarówno zagrożenia, jak i szanse, które mają wpływ na realizację przyjętej strategii.



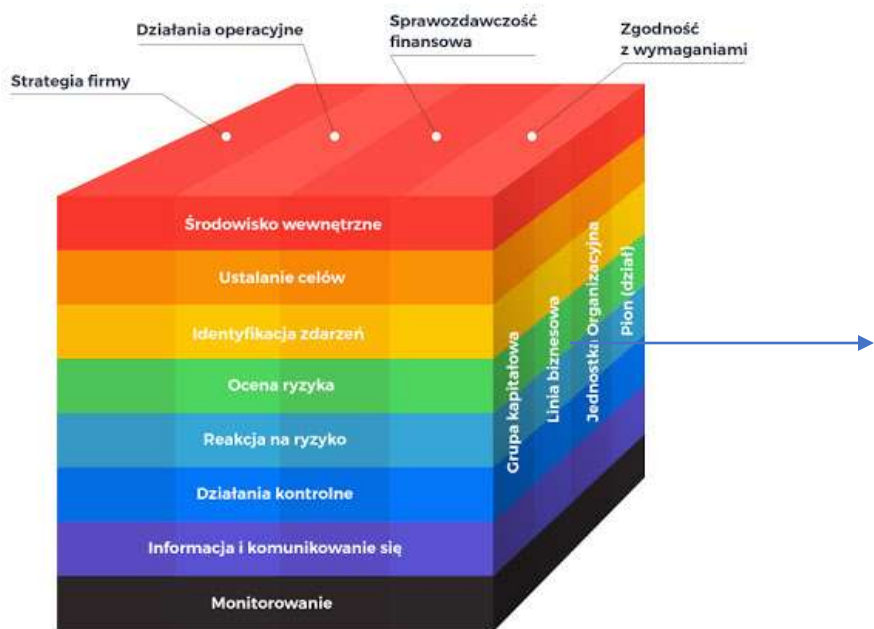
Model COSO – kompleksowy model zarządzania ryzykiem

Przykład: przedsiębiorca odzieżowy

Cel strategiczny: w ciągu trzech lat stać się najbardziej rozpoznawalną ekskluzywną marką odzieżową w Polsce.	
Cele operacyjne:	Przykładowe zdarzenia wpływające na realizację celu:
Zatrudnić dwóch projektantów w ciągu najbliższych 6 miesięcy.	brak pracowników na lokalnym rynku, zbyt wygórowane żądania co do wynagrodzeń, brak środków na realizację celu (np. otrzymanie negatywnej decyzji w sprawie dotacji, kredytu lub brak wypracowanych własnych środków), pojawienie się zdolnych studentów ASP na rynku pracy (szansa na „taniego” projektanta, który nie wymaga wysokiego wynagrodzenia, ale zyskuje doświadczenie)
Zatrudnić trzy krawcowe w ciągu najbliższego miesiąca.	brak wykwalifikowanych krawcowych na rynku, zbyt wysokie wymagania co do wynagrodzeń, brak środków pieniężnych
W ciągu najbliższego roku podjąć współpracę ze znajomymi aktorami (kolegami z czasów licealnych), którzy w zamian za ubrania, będą je odpowiednio reklamowali.	Niechęć aktorów do takiego koleżeńskiego rozwiązania – konieczność zapłaty honorarium. Konieczność szukania alternatywnego rozwiązania umożliwiającego reklamę.



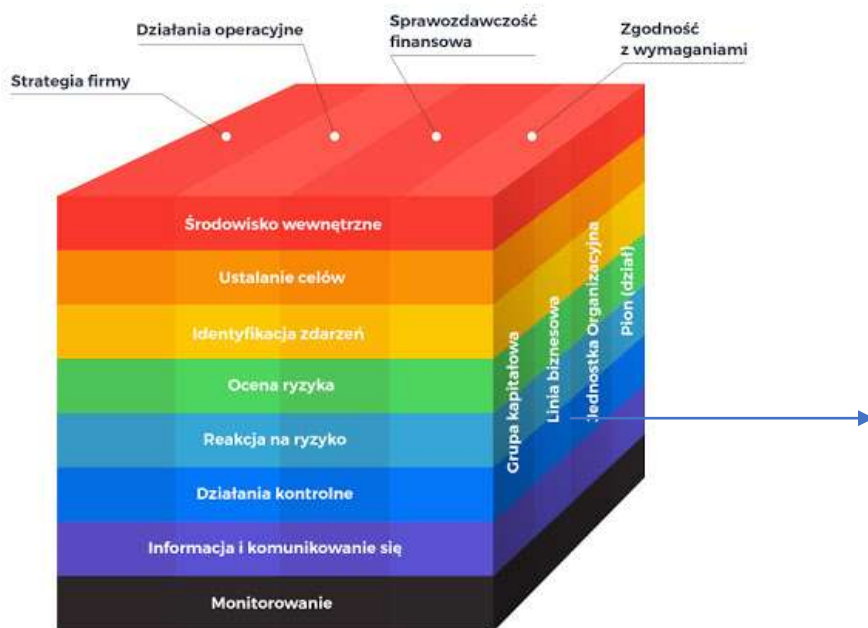
Model COSO – kompleksowy model zarządzania ryzykiem



Ocena ryzyka polega na analizie możliwych skutków niepożądanych zdarzeń, jak również prawdopodobieństwa ich wystąpienia.



Model COSO – kompleksowy model zarządzania ryzykiem

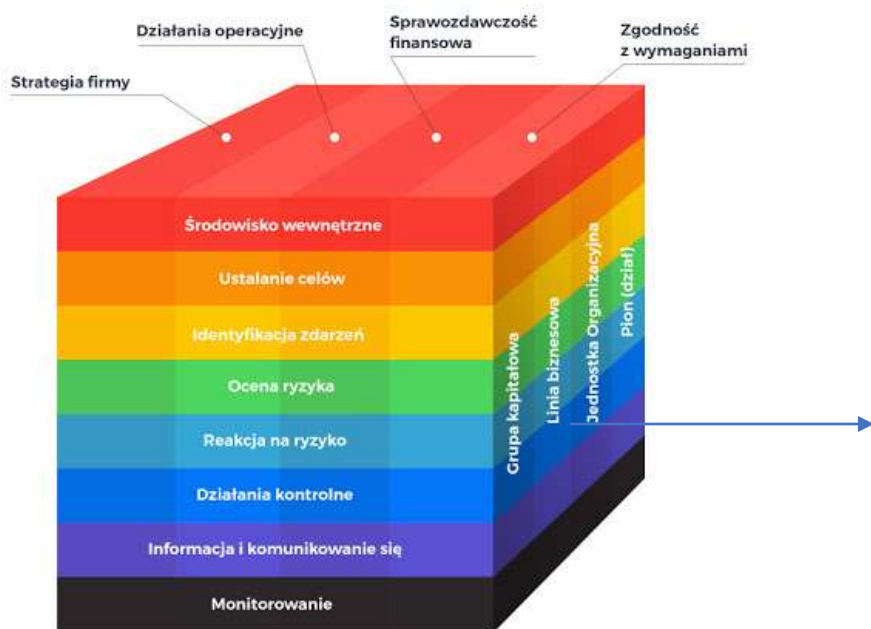


Reakcja na wystąpienie ryzyka może obejmować na przykład: unikanie, akceptację, ograniczanie lub dzielenie się ryzykiem, by w dalszej kolejności opracować plan powiązania ryzyk z działaniami, które doprowadzą ryzyka do akceptowalnego poziomu.

Działania takie mają na celu również ograniczenie niespodzianek i strat operacyjnych firmy, opracowanie w dalszej kolejności rozwiązań pozwalających zarządzać wieloma rodzajami ryzyk, a także wykorzystanie różnych możliwości i szans.



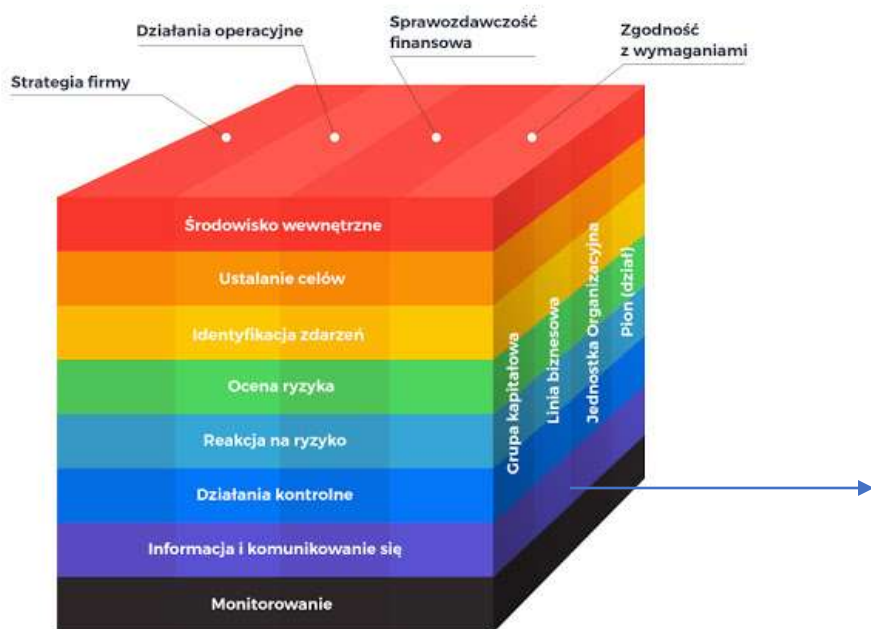
Model COSO – kompleksowy model zarządzania ryzykiem



Działania kontrolne to różne procedury ustalone i przestrzegane w firmie. Są one efektem określonej reakcji na ustalone wcześniej ryzyka. Kontrola wewnętrzna jest integralną częścią procesu zarządzania ryzykiem, ponieważ pozwoli zminimalizować pojawiające się błędy (zarówno wynikające z błędów ludzkich, jak i ze zmieniających się okoliczności).



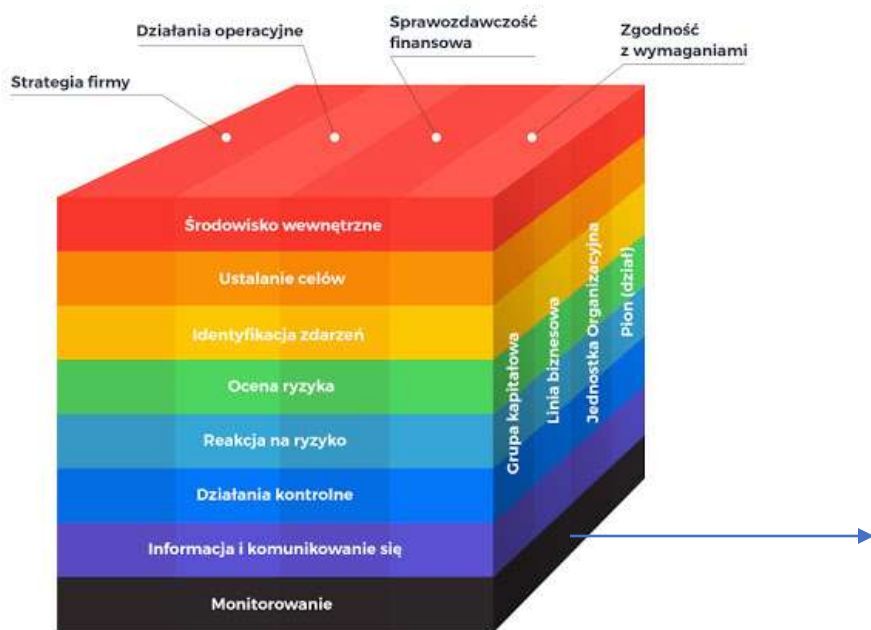
Model COSO – kompleksowy model zarządzania ryzykiem



Informacja i komunikowanie się to element nieodzowny w każdym procesie zarządzania ryzykiem. Nawet najlepsze analizy i ustalone procedury nie będą dobrze funkcjonować, jeśli nie zostaną odpowiednio zakomunikowane. Odpowiednia komunikacja to taka, która dotrze do odpowiednich odbiorców we właściwym czasie i umożliwi im reakcję. Skuteczna komunikacja działa w obrębie całej firmy w każdą stronę struktury organizacyjnej. Ponoszą za nią odpowiedzialność wszyscy pracownicy, ponieważ każdy z nich może przekazać swoim przełożonym cenne informacje o problemach operacyjnych, nieprzestrzeganiu kodeksu etyki lub o innych niepokojących działaniach.



Model COSO – kompleksowy model zarządzania ryzykiem



Monitorowanie jest dopełnieniem procesu. Jest ono realizowane poprzez stałe aktywności kierownictwa i personelu, które mają na celu bieżącą analizę funkcjonowania ustalonych wcześniej zasad. Może obejmować raportowanie, okresowe kontrole, zlecenie niezależnych ocen itp.

Realizacja powyższych zadań musi odbywać się w każdym z następujących obszarów: strategicznym, działalności operacyjnej (bieżącej), sprawozdawczości finansowej i przestrzegania prawa.

Co więcej proces musi przebiegać zarówno na poziomie samego przedsiębiorstwa i wyodrębnionych w nim działów, pionów, linii biznesowych, jak na poziomie i całej grupy kapitałowej. I właśnie to zostało przedstawione powyżej w formie kostki.



[Powrót do spisu treści](#)

Rozdział 2

Analiza i ocena ryzyka



Strategia przedsiębiorstwa

Strategia przedsiębiorstwa jest kluczowa dla prawidłowego funkcjonowania firmy i powinna zawierać co najmniej:

- misję,
- długoterminowe (w tym strategiczne) cele,
- określenie rynków działania,
- oferty produktowej,
- struktury geograficznej działalności,
- sposobu konkutowania na rynku,
- określenie modelu biznesowego,
- inne elementy.



Strategia przedsiębiorstwa – misja i cele strategiczne

Ujęta w strategii **misja** to kierunek, w którym podąża firma. To także ważne wartości, jak również najważniejsze elementy jej działania: co produkuje, co sprzedaje, kto jest jej klientem, jakie są plany na przyszłość.

Przykładową misją firmy szkoleniowej może być na przykład zdanie: „**chcemy motywować naszych studentów, inspirować ich do realizacji pomysłów oraz do ciągłego rozwoju**”.

W ramach przyjętych misji i wizji opracowuje się **cele do realizacji**. **Cele długoterminowe to cele strategiczne, które doprecyzowują misję i wizję**, które wybiegają w przyszłość na kilka lat (np. 3-5 lat). Stanowią one podstawę do stworzenia celów krótkoterminowych.



Cele strategiczne przedsiębiorstwa a ryzyka

Powiązanie celów strategicznych z ryzykami, a następnie z kontrolą wewnętrzną:

- ustalenie celów mniejszej wagi w ramach celów głównych,
- dokładne przeanalizowanie procesów w ramach tych obszarów,
- przygotowanie listy ryzyk poprzez uzyskanie odpowiedzi na pytanie „co może pójść nie tak”,
- zaplanowanie działań kontrolnych (kontroli wewnętrznych), które zapobiegą ryzykom zdefiniowanym w kroku trzecim.



Powiązanie celów strategicznych z ryzykami, a następnie z kontrolą wewnętrzną – **przykład**.

Przedsiębiorca odzieżowy wyznaczył cel strategiczny swojej firmie: „zwiększenie zysku na sprzedaży o 15% w stosunku do ubiegłego roku”. Następnie wykonał analizę czterech kroków:

1. Ustalił cele mniejszej wagi: zwiększenie przychodów ze sprzedaży ubrań o 30%, sprzedaż nowego modelu garnituru dziewczęcego i osiągnięcie przez niego 10% udziału w wolumenie sprzedaży, ograniczenie kosztów zmiennych produkcji o 10%.
2. Przeanalizował procesy w obszarze sprzedaży tak, żeby móc wyselekcjonować kluczowe czynniki sukcesu, które pozwolą osiągnąć cele (np. programy lojalnościowe dla klientów, reklama i rozwój nowych kanałów sprzedaży itd.)
3. Zadał sobie pytanie „co może pójść nie tak”. Odpowiedzi: podchwycenie pomysłu przez konkurencję, wzrost cen materiałów i innych surowców do produkcji ubrań, brak/utrata kompetentnych projektantów i krawcowych, rynek pracownika – rosnące wynagrodzenia, brak dostępu do kapitału.
4. Za planował listę działań które zapobiegą ryzykom zidentyfikowanym w punkcie trzecim. Pan Franciszek określił również poziom ryzyka, który istnieje bez względu na wprowadzone środki zaradcze i przyjął również określony poziom apetytu na ryzyko (czyli poziom ryzyka akceptowalnego). Przyjął na przykład, że przyjmuje jako akceptowalny wzrost cen surowców o 2%, co jest naturalnym poziomem, który nie zaburzy realizacji celów. Przyjął także, że akceptowalnym poziomem rotacji wśród krawcowych jest 5% (poziom normalny na tym rynku).



Środowisko wewnętrzne – fundament procesu zarządzania ryzykiem

Środowisko wewnętrzne stanowi fundament pozostałych elementów kontroli wewnętrznej i zarządzania ryzykiem. Główne elementy środowiska wewnętrznego można przedstawić następująco:

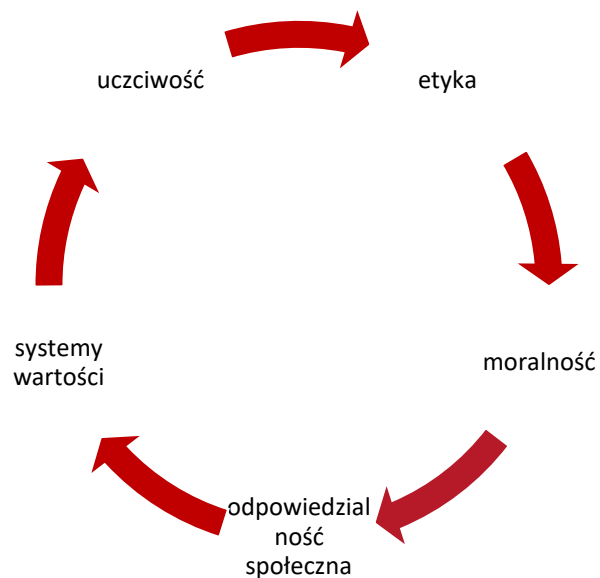


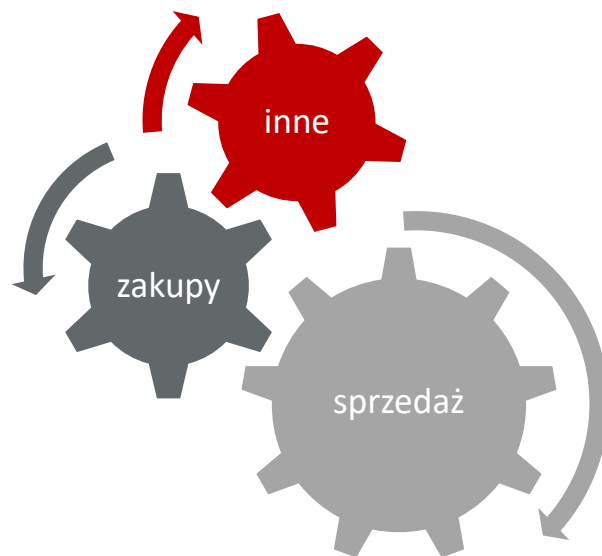
Diagram przedstawia kluczowe elementy składające się na środowisko wewnętrzne przedsiębiorstwa.



Analiza kluczowych procesów i kontroli

Przedsiębiorstwo – jako sprawny organizm, w którym funkcjonują różne wzajemnie ze sobą powiązane obszary, procesy (tzw. cykle), na przykład:

- cykl zakupów,
- cykl sprzedaży,
- cykl produkcji,
- cykl obrotu gotówką,
- sprawozdawczość.



Schemat przedstawia trzy zazębiające się koła, z których każde symbolizuje jeden obszar działalności przedsiębiorstwa: sprzedaż, zakupy, inne



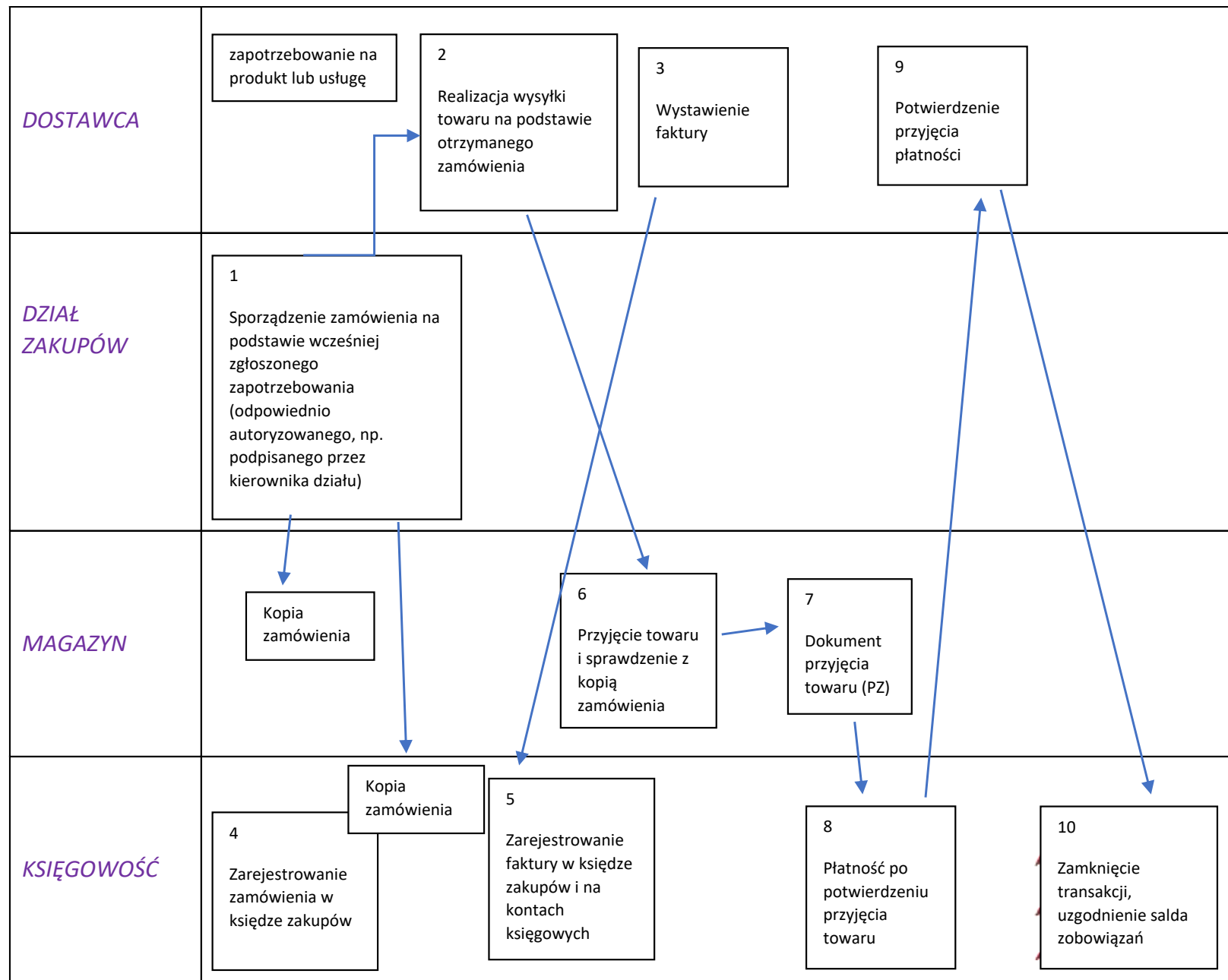
Schemat przedstawia przykładowy cykl działań, które wykonywane są w przedsiębiorstwie od momentu złożenia zamówienia przez klienta, poprzez sprzedaż, aż do uzyskania płatności.



Proces zakupów - przykład

Przykładowe ryzyka w przedstawionym obok procesie zakupów:

- zaciągnięcie niez zaakceptowanych zobowiązań,
- zapłata za towary niedostarczone lub dostarczone niezgodnie z zapotrzebowaniem,
- utrata dostawców z powodu niepłaconych zobowiązań (nieewidencjonowane, niepłacone, niemonitorowane),
- defraudacja – zakupione materiały dostarczone nie do magazynu, a do innego (prywatnego) odbiorcy,
- fałszywe zamówienia do sprawdzonego dostawcy, u którego wynegocjowano kredyt kupiecki (płatność odroczone) i „zaginięcia” towarów przy dostawie.



Procesy - sprawozdawczość

W podejmowaniu decyzji biznesowych niezwykle ważną rolę spełnia również **sprawozdawczość finansowa**. Szybki dostęp do aktualnych i rzetelnych danych finansowych to klucz do sukcesu w dzisiejszych czasach.

W prawidłowo funkcjonującym procesie na pewno zadbano o:

- terminowe i poprawne ujmowanie transakcji w księgach,
- obowiązkowe księgowania i czynności związane z zamknięciem roku wykonane terminowo tak, żeby zachowany był wystarczający czas do sporządzenia rzetelnych sprawozdań finansowych (tworzenie koniecznych rezerw, wykonywanie potwierdzeń sald, przeprowadzenie inwentaryzacji majątku itp.),
- terminowe sporządzanie informacji „wsadowych” do raportów i sprawozdań (w tym informacji zarządczych, różnych raportów, na podstawie których na bieżąco podejmowane są decyzje),
- obieg informacji, przekazywanie ich między właściwymi komórkami (np. przekazywanie przez osoby odpowiedzialne zestawień do sporządzenia zapadalności zobowiązań (czyli uszeregowania poszczególnych zobowiązań według terminów płatności od najświeższych do najstarszych),
- terminowe przygotowywanie wymaganych sprawozdań zarówno zarządczych jak i obowiązkowych (wymaganych przez ustawę o rachunkowości, czy też inne regulacje).



Przykład

Przedsiębiorca chciałby, żeby proces sprawozdawczości finansowej był w jego firmie dobrze skoordynowany. W tym celu spotkał się z dyrektorem finansowym, żeby ten wyjaśnił mu, w jaki sposób podszedł do tej kwestii. Pan Krzysztof Banknot podaje przykładowe elementy związane z zamknięciem roku obrotowego:

- pracownicy poszczególnych działów najpóźniej do 4 stycznia każdego roku muszą przekazać informacje w sprawie dokonanych zakupów, które jeszcze nie zostały zafakturowane;
- dział prawny przekazuje najpóźniej do 4 stycznia informacje na temat możliwych wyników toczących się spraw sądowych;
- pani Krystyna Eremkowska wysyła potwierdzenia sald i do 10 stycznia każdego roku sporządza protokół z tej czynności;
- do 15 grudnia każdego roku powoływana jest komisja inwentaryzacyjna, która po wykonaniu inwentaryzacji przekazuje protokół do księgowości najpóźniej do dnia 4 stycznia;
- do 10 stycznia przeprowadzane są wszystkie wyceny końcoworoczne wymagane przez przepisy;
- do 31 stycznia sporządzana jest pierwsza wersja robocza sprawozdania finansowego, a do 15 marca wersja ostateczna zgodne z obowiązującymi wzorami;
- do 31 marca przeprowadzane jest badanie sprawozdania finansowego i wydawana jest opinia z badania;
- do 30 czerwca sprawozdanie podlega zatwierdzeniu;
- nowe, nietypowe transakcje, omawiane są podczas bieżących spotkań organizowanych ad hoc.



Mapa ryzyk - przygotowanie



Mapa ryzyk - przygotowanie

Pierwszym działaniem w ramach procesu oceny ryzyka jest opracowanie **jednolitych kryteriów jego oceny**. Zazwyczaj ocena ta jest dokonywana na podstawie prawdopodobieństwa i istotności wpływu. Czasem bierze się też pod uwagę szybkość wystąpienia, czy podatność na zagrożenia.

Sama ocena ryzyka oznacza **przypisanie do niego konkretnych wartości**, ale należy pamiętać, że żadne ryzyka nie występują w izolacji i czasem może się tak zdarzyć, że ryzyko jako pojedyncze zdarzenie nie jest istotne, ale ono w połączeniu z innym już przynosi bardzo poważne konsekwencje.

Przykład:

Przedsiębiorca może indywidualnie uznać, że ryzyko straty finansowej powyżej X mln zł jest uznawane za istotne i nadać mu wagę 5 w skali pięciostopniowej, a ryzyko strat poniżej 20 tys. jako nie istotne i nadać mu wagę 1. Podobnie można podejść do oceny prawdopodobieństwa i uznać, że na przykład wystąpienie zdarzenia 2-3 razy w roku oznaczać będzie niskie prawdopodobieństwo i nadać mu wagę 1, a wystąpienie 1 – w tygodniu, to wysoka waga, czyli 5. W taki sposób, dokonując oceny na koniec można podsumować tę ocenę w formie tak zwanej matrycy (mapy) ryzyk.



Mapa ryzyk – przykładowe powiązania

	Zmiana preferencji konsumentów	Wzrost cen surowca	Fluktuacje kursów walutowych	Recesja w gospodarce
Zmiana preferencji konsumentów			x	x
Wzrost cen surowca			x	x
Fluktuacje kursów walutowych	x			x
Recesja w gospodarce	x	x	x	



Mapa ryzyk

Mapa ryzyk to zestawienie pokazujące na jednym schemacie prawdopodobieństwo i skutki (np. finansowe) w odniesieniu do konkretnego ryzyka.

Przykład dla małego przedsiębiorcy działającego w branży modowej (skala ocen 3 – wysoko, 1 – nisko):

Źródło ryzyka	Wpływ na spółkę	Prawdopodobieństwo (A)	Wpływ (B)	Ocena (A*B)
Niedostateczna kontrola cen	Utrata rentowności	3	3	9
Brak systemów motywacyjnych	Utrata personelu	1	3	3
Nierozwijane autorskie oprogramowanie	Utrata wiarygodności niektórych danych	2	2	4



Mapa ryzyk – naniesienie kontroli

Mapa ryzyk – uzupełnienie matrycy o kontrole i osoby odpowiedzialne.

Przykład dla małego przedsiębiorcy działającego w branży modowej:

Ryzyko	Kontrola	Opis	Rodzaj kontroli	Kto przygotowuje dane	Osoba odpowiedzialna	Kiedy?
Nie wszystkie transakcje są zaksięgowane w terminie	Przegląd niezaksięgowanych transakcji	Raport na temat niezaksięgowanych transakcji jest przeglądany raz w miesiącu przez głównego księgowego w celu zidentyfikowania transakcji zainicjowanych, a nie dokończonych	Wykrywająca	Dział IT z systemu finansowo-księgowego	Główny księgowy	Raz na miesiąc



Mapa ryzyk – naniesienie kontroli

Zastosowane mechanizmy kontrolne powinny być:

Efektywne – adresujące ryzyka w sposób najbardziej opłacalny (co oznacza w praktyce, że sposób, w jaki kontrola jest zbudowana w optymalny sposób adresuje ryzyko oraz osoba wykonująca kontrolę ma wystarczające uprawnienia i kwalifikacje).

Skuteczne – adresujące właściwie zidentyfikowane ryzyka (co oznacza, że kontrola niweluje przypisane ryzyko, jest prawidłowo udokumentowana, istnieją dowody potwierdzające wykonane czynności kontrolne, kontrola jest wykonywana przez kompetentne osoby i zapewnia zachowanie właściwego podziału obowiązków).

Przykład:

Pewien przedsiębiorca tak bardzo chciał zabezpieczyć się przed tym, żeby jego pracownicy nie wynosili do domu papieru toaletowego i kawy przeznaczonych do użytku firmowego, że zatrudnił dodatkową osobę, która zajmowała się tylko monitorowaniem zużycia i kontrolą monitoringu firmowego w celu wychwycenia nieprawidłowości. Kontrola była skuteczna. Incydenty przestały się powtarzać. Jednak po analizie okazało się, że całe zużycie papieru toaletowego i kawy kosztowało firmę około 5 tys złotych miesięcznie, potencjalne kradzieże wynosiły wcześniej około 10% (500 zł), podczas gdy koszty zatrudnienia dodatkowej osoby wyniosły około 6 tysięcy złotych. W tym wypadku kontrola okazała się skuteczna, ale całkowicie nieefektywna. Ponadto później okazało się, że skoncentrowano się na nieistotnych kwestiach, a obok wydarzyła się znacząca defraudacja.



[Powrót do spisu treści](#)

Rozdział 3

Reakcje na ryzyko



Proces zarządzania ryzykiem – szyty na miarę

Celem zarządzania ryzykiem jest identyfikacja potencjalnych zdarzeń (ryzyk), które mogą wywrzeć wpływ na firmę i na realizację jej celów, a następnie utrzymanie ryzyka w ustalonych granicach tak, aby założone cele zostały osiągnięte.

W procesie zarządzania ryzykiem uczestniczą zarówno właściciele i kierownictwo, jak i szeregowi pracownicy



Proces zarządzania ryzykiem – szyty na miarę

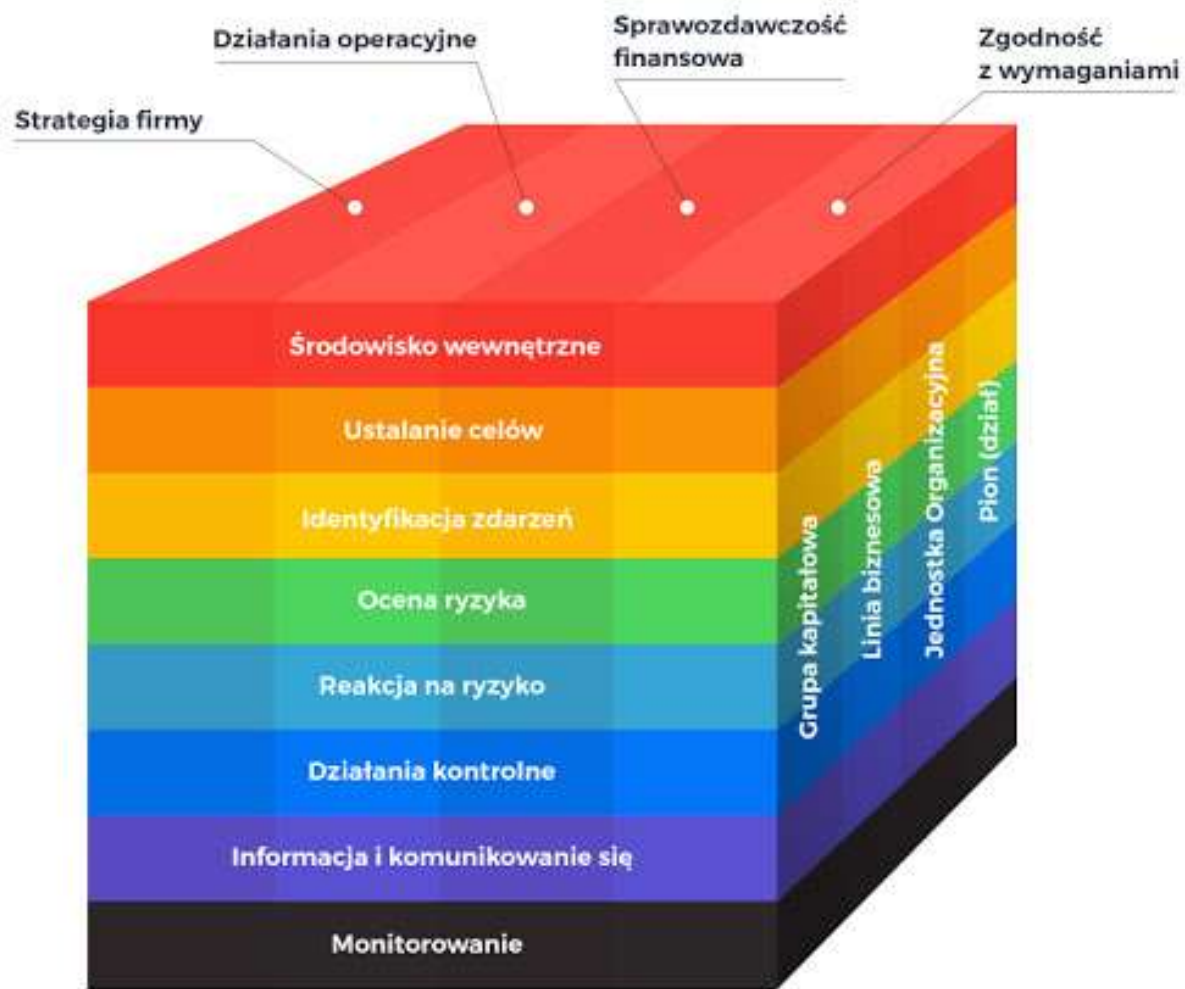
Sam proces zarządzania ryzykiem, przebiegający według określonych wcześniej planów, obejmuje:

- identyfikację, analizę i ocenę ryzyka,
- podejmowanie decyzji odnośnie sposobu postępowania z ryzykiem,
- monitoring i przegląd służący sprawdzeniu, czy wszystko „idzie zgodnie z planem” i czy nie są potrzebne jakieś zmiany.

Proces ten **dotyczy każdego ryzyka** i wymaga wykonywania powyższych czynności przez kompetentne osoby, które będą umiały stworzyć listę zagrożeń i koniecznych do podjęcia działań oraz przedsięwziąć dalsze kroki.



Model COSO – przypomnienie



Proces zarządzania ryzykiem – rola kierownictwa

Kluczowe kierownictwo/zarząd będzie odpowiedzialne za:

- definiowanie i zatwierdzanie polityki zarządzania ryzykiem,
- zapewnienie spójności kultury organizacyjnej i polityki zarządzania ryzykiem,
- określanie wskaźników, które będą wskazywały jakie rezultaty przynosi zarządzanie ryzykiem i czy wyniki są spójne ze wskaźnikami rozwoju firmy,
- dostosowania celów zarządzania ryzykiem do celów i strategii organizacji,
- zapewnienia zgodności zarządzania ryzykiem z przepisami prawa i innymi regulacjami,
- zagwarantowanie zasobów niezbędnych do zarządzania ryzykiem (np. odpowiedniego personelu),
- ciągłej weryfikacji, czy struktura ramowa zarządzania ryzykiem nie wymaga zmian.



Proces zarządzania ryzykiem – inne przykładowe role

Zidentyfikowane ryzyko	Osoba odpowiedzialna (właściciel ryzyka)
Ryzyko utraty kluczowych klientów	Kierownik do spraw relacji z klientami
Ryzyko utraty najlepszych projektantów	Dyrektor kreatywny
Ryzyko defraudacji	Różne osoby w całej firmie (ryzyko defraudacji jest obecne w wielu obszarach)
Ryzyko utraty danych dotyczących projektów – wyciek poufnych danych	Pan Michał Łindous, odpowiedzialny za IT



Proces zarządzania ryzykiem – działania kontrolne

Czynności kontrolne to różnego rodzaju zasady i procesy, które wspomagają realizację zaleceń kierownictwa.

Zapewniają, że podjęte zostały niezbędne działania w celu minimalizacji ryzyk.

Występują na każdym szczeblu w strukturze organizacyjnej (zarówno na poziomie zarządu, jak i szeregowych pracowników).

Obejmują również działania na poziomie informatycznym.



Przykładowe mechanizmy obejmują:

- opracowanie procedur i polityk wewnętrznych,
- wprowadzenie zasad opracowywania planów działalności i budżetowania,
- ogólne kontrole w środowisku IT, takie jak opracowana strategia IT, polityka haseł, back-upów, używanie tylko sprawdzonego (licencjonowanego) oprogramowania itp.,
- przeglądy wyników działalności, takie jak analizy trendów, analizy wskaźnikowe, porównania danych do budżetu i wyjaśnianie różnic oraz podejmowanie akcji naprawczych itp.),
- kontrole w procesie raportowania finansowego, takie jak: przyjęcie określonego harmonogramu zamknięcia roku i przygotowywania sprawozdań, przeglądy wersji wstępnych, analiza korekt audytorskich i listów audytora do zarządu,
- zabezpieczenie aktywów i podział obowiązków, np. fizyczna ochrona, ograniczenie dostępu do niektórych pomieszczeń „klucze mają tylko konkretne osoby” (np. serwerowni) do wskazanych osób, zobowiązania umowne pracowników do zachowania poufności itp.,
- wprowadzenie wymogów dotyczących autoryzacji, zezwoleń,
- wprowadzenie konieczności weryfikacji dokumentów przez osoby na różnych szczeblach w firmie.



Proces zarządzania ryzykiem – działania kontrolne

Zwykle jeden cel kontroli adresuje jedno ryzyko, ale nie musi to być zasada.

Celem kontroli wewnętrznej jest zasadniczo ograniczenie ryzyka. Przykładowymi celami kontroli są na przykład:

- zmiany danych stałych (np. numerów rachunków bankowych, danych adresowych itp.) są odpowiednio autoryzowane i poprawnie wprowadzone do systemu,
- tylko uzasadnione zaaprobowane faktury są ujmowane w księgach w prawidłowej wysokości, kompletnie,
- listy płatności są kompletne i zawierają poprawne dane liczbowe,
- korekty do sprawozdania finansowego są wprowadzone na właściwych kontach i we właściwych okresach sprawozdawczych,
- ceny i warunki sprzedaży są autoryzowane przez pracowników posiadających odpowiednie uprawnienia.



Proces zarządzania ryzykiem – działania kontrolne

Częstotliwość:

- regularne (np. raz w roku, raz w miesiącu, codziennie itp.),
- nieregularne (w miarę potrzeb).

Sposób zabezpieczenia:

- prewencyjny (zapobiegający powstaniu błędu),
- detekcyjny (wykrywający powstały błąd).

Sposób działania:

- manualna (wykonana bez użycia systemu informatycznego),
- automatyczna (wykonana przez komputer bez ingerencji człowieka),
- mieszana (zawierające oba elementy).



Proces zarządzania ryzykiem – działania kontrolne

Kontrole wewnętrzne powinny wspierać, a nie blokować biznes.

Warto o tym pomyśleć w kontekście ilości aplikowanych czynności, ich kosztów i korzyści z nich płynących.



Zidentyfikowane przykładowe ryzyko	Zaproponowane przykładowe działania kontrolne (ochronne)
Ryzyko utraty kluczowych klientów	Spotkania cykliczne z klientami, badanie poziomu satysfakcji, urozmaicanie oferty, programy lojalnościowe.
Ryzyko utraty najlepszych projektantów	Programy lojalnościowe, pakiety pracownicze, jasna ścieżka kariery, możliwość personalizowania określonych projektów.
Ryzyko defraudacji w obszarze sprzedaży	Tygodniowe raportowanie sprzedaży według klientów i marży przez handlowców do dyrektora sprzedaży, tygodniowe analizy sprzedaży przedstawiane i omawiane na spotkaniach z właścicielem, umowy z klientami obowiązkowo autoryzowane przez właściciela, ograniczenie dostępu do ubrań i projektów do wybranych osób, podział obowiązków w zespole sprzedaży.
Ryzyko utraty danych dotyczących projektów – wyciek poufnych danych	Zabezpieczenia fizyczne (np. sejfy, kopie zapasowe chronione), zabezpieczenia elektronicznych wersji (np. trudne do rozszyfrowania hasła, zabezpieczenia prawne (prawa autorskie)).
Ryzyko kursowe	Dopasowanie terminów i walut transakcji, transakcje zabezpieczające z bankiem (np. opcje, forward), kontrakty w walucie krajowej, zarabianie i wydawanie w tej samej walucie.
Ryzyko kredytowe	Zatwierdzanie przyznanych limitów kredytowych przez kierowników i/lub zarząd (w zależności od kwot). Analiza tygodniowych raportów sprzedaży vs należności. Regularna analiza wskaźników rotacji należności. Obowiązkowe telefony windykacyjne, w przypadku zalegania z płatnością powyżej np. 10 dni.



Koncepcja trzech linii obrony

Model trzech linii obrony zakłada, że do skutecznego zarządzania ryzykiem i efektywnej kontroli konieczne są trzy grupy osób/funkcji (tak zwane trzy linie obrony) działające pod nadzorem kierownictwa wyższego szczebla i organu nadzorczego/właściciela.

- **Pierwsza linia** obrony to tak zwani właściciele procesów (odpowiedzialni za wydajność konkretnych procesów)
- **Druga linia** obrony to osoby z kierownictwa wyższego szczebla.
- **Trzecia linia** obrony to audyt wewnętrzny

W każdej z linii powinny być zidentyfikowane osoby, które są ta zwanymi właścicielami ryzyk.



Pierwsza linia obrony

Pierwsza linia obrony to tak zwani właściciele procesów (odpowiedzialni za wydajność konkretnych procesów, np. procesu sprzedaży, zakupów, produkcji, kadrowego). Są nimi głównie pracownicy i kierownicy niższego i średniego szczebla, którzy zarządzają kontrolą i ryzykiem w codziennych działaniach.

Wiedzą najwięcej na temat obszarów, w których działają. Na przykład właścicielem procesu sprzedaży detalicznej może być kierownik handlowy. Ich głównym zadaniem jest zarządzanie ryzykiem i kontrola wewnętrzna, jak również zaprojektowanie i realizacja kontroli w odpowiedzi na te ryzyka.

Managerowie operacyjni tworzą i wdrażają kontrolę w procesach i zarządzaniu ryzykiem w firmie. Wskazują konkretne luki i ryzyka i zadania kontrolne do wykonania, jak również nieodpowiednie procesy, które wymagają zmiany/uszczelnienia.



Druga linia obrony

Druga linia obrony to osoby z kierownictwa wyższego szczebla. Ich zadaniem jest wspieranie pierwszej linii doświadczeniem oraz doskonaleniem procesów i monitorowania działań pierwszej linii. Jej celem jest zapewnienie, że ryzyko i kontrola są skutecznie zarządzane. Druga linia obrony obejmuje również działania zapewniające, że kontrole i procesy zarządzania ryzykiem wdrożone przez pierwszą linię obrony są odpowiednio zaprojektowane i działają zgodnie z przeznaczeniem.

Obowiązki osób w ramach drugiej linii obrony obejmują między innymi:

- wspieranie zarządzania w zakresie projektowania i rozwoju procesów i kontroli,
- monitorowanie adekwatności i skuteczności kontroli wewnętrznej,
- wskazywanie istotnych problemów i nowych zagrożeń,
- dostarczenie wiedzy na temat sposobów zarządzania ryzykiem,
- identyfikację zmian w poziomie apetytu na ryzyko i tolerancji ryzyka,
- szkolenia na temat procesów zarządzania ryzykiem i kontroli.



Trzecia linia obrony

Trzecia linia obrony to audyt wewnętrzny, którego zadaniem jest potwierdzenie kierownictwu, że działania dwóch pierwszych linii nie budzi zastrzeżeń.

Zazwyczaj osoby z trzeciej linii składają raporty bezpośrednio organom nadzorczym (właścicielom). Ich celem jest dostarczenie niezależnej oceny dotyczącej skuteczności zarządzania ryzykiem i kontroli.

Trzecia linia dostarcza kierownictwu wyższego szczebla i właścicielom zapewnienia, że działania pierwszej i drugiej linii są zgodne z ich oczekiwaniami.

Trzecia linia obrony nie jest zazwyczaj upoważniona do wykonywania funkcji zarządczych, co ma chronić jej obiektywność i niezależność organizacyjną.



Rola audytu wewnętrznego

Systematyczna i uporządkowana ocena procesów:

- zarządzania ryzykiem,
- kontroli i ładu organizacyjnego,
- przyczynia się do poprawy ich działania.

Komórka audytu wewnętrznego powinna być **niezależna**, żeby mogła spełniać swoją funkcję.



Ryzyko cyfrowe

Postęp technologiczny w dzisiejszych czasach niesie za sobą nie tylko perspektywę dynamicznego rozwoju, ale także szereg towarzyszących temu zagrożeń.



Ryzyko cyfrowe

- Ryzyko utraty lub kradzieży danych dotyczących klientów.
- Ryzyko utraty lub kradzieży danych dotyczących receptur produktów.
- Ryzyko utraty części przychodów w wyniku awarii (bądź celowego zablokowania) oprogramowania do celów sprzedaży internetowej.
- Ryzyko utraty danych dotyczących sprzedaży oraz ryzyko, że sprzedaż nie będzie kompletna (nie wszystkie transakcje zostaną zarejestrowane przez biuro rachunkowe).
- Ryzyko utraty lub kradzieży danych dotyczących firmy z biura rachunkowego.
- Ryzyko mechanicznego uszkodzenia sprzętu (komputerów, serwera).
- Ryzyko nieautoryzowanego dostępu (np. księgowych do tajnych receptur produktów).
- Ryzyko różnych błędów popełnianych przez autorskie oprogramowanie projektowe.



Cyberryzyko

Kim są cyberprzestępcy? Są nimi na przykład:

- Zorganizowani przestępcy, którzy używają zaawansowanych metod i oprogramowania do kradzieży pieniędzy lub danych.
- Terroryci, którzy wykorzystują internet do przeprowadzania cyberataków na przykład na jakieś przedsiębiorstwa, czy instytucje finansowe.
- Tak zwani hakywiści, którzy chcą zmanifestować jakąś społeczną akcję poprzez kradzież lub publikację danych (na przykład może nie podobać im się, że jakaś firma zatrudnia zbyt mało kobiet, więc wykradają z firmy poufne dane i publikują je w sieci).
- Insidersi, którymi są zaufane osoby wewnątrz firmy wykorzystujące swoją pozycję do kradzieży danych.
- Złośliwi aktorzy, którzy chcą uzyskać szybką korzyść finansową.



Cyberryzyko – przykładowe kontrole

- Ograniczenie fizycznego dostępu do sprzętu (np. zamknięcie serwerów w odrębnym pomieszczeniu, do którego dostęp mają tylko określone osoby).
- Określenie bezpiecznych haseł dostępu i korzystanie z kontroli haseł przez osoby z dostępem online w celu uniemożliwienia wykonywania funkcji, które nie powinny być ze sobą łączone.
- Podział obowiązków i funkcji w ramach firmy (np. programiści nie mogą mieć dostępu do wdrażania rozwiązań).
- Zastosowanie firewall'a.
- Szyfrowanie.
- Automatyczne wylogowania.
- Prowadzenie dziennika logowań.



Cyberryzyko – przykładowe kontrole

- Korzystanie tylko z autoryzowanego, sprawdzonego oprogramowania.
- Obowiązkowo wykonywane kopie danych (bezpiecznie przechowywane).
- Zatrudnienie ochrony.
- Ograniczenie możliwości logowania się do aplikacji tylko dla upoważnionych osób.
- Wprowadzenie automatycznego raportowania w przypadku podjęcia próby zalogowania się przez osobę nieuprawnioną.
- Blokada logowania w przypadku podania nieprawidłowego hasła trzykrotnie.
- Wprowadzenie tokenów dla potrzeb logowania się do wewnętrznej sieci (intranetu) z zewnątrz firmy (np. z domu).



Powrót do spisu treści

Kontakt:

Aneta Wilk-Łyś

tel.: +48 883 931 312

e-mail: aneta.wilk.lys@gazeta.pl, aneta.wilk.lys@gmail.com

