EKSPERT RADZI

Patrycja Szulin

Zarządzanie ryzykiem jako element kontroli zarządczej w JST

Wolters Kluwer

Spis treści

Patrycja Szulin

Zarządzanie ryzykiem jako element kontroli zarządczej w JST

Kontrolę zarządczą, zgodnie z aktualnym brzmieniem art. 68 ustawy z 27.08.2009 r. o finansach publicznych – dalej u.f.p., stanowi „ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy". Zatem ogół działań, nie dokumentów, sporo jednostek wpadło jednak w pułapkę rozbudowanych systemów kontroli zarządczej, jakby zapominając, że kontrola zarządcza ma wspomóc efektywność, a nie przysporzyć dokumentów. W komunikacie nr 23 Ministra Finansów z 16.12.2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych – dalej komunikat nr 23 – znajdują się informacje o **potrzebie udokumentowania jedynie procesu zarządzania ryzykiem oraz standardu samooceny kontroli zarządczej.** Jednocześnie wytyczne te nie wskazują sposobu realizacji właściwego dla spełnienia poszczególnych standardów – w tym względzie jednostki sektora finansów publicznych mają pewną swobodę. Pewną, ponieważ sektor finansów publicznych działa w warunkach ściśle nadzorowanych. Kompetencje są ograniczone do zasady legalizmu – na podstawie i granicach prawa.

Wprowadzenie

Standardy kontroli zarządczej mogą być matrycą, która pozwala obejrzeć funkcjonowanie jednostki zarówno wewnątrz niej samej, jak i w stosunkach zewnętrznych. Dlatego kontrola zarządcza jest tak interesującym obiektem dla audytu wewnętrznego. Stanowi niejako system naczyń połączonych – **brak odpowiedniego funkcjonowania któregokolwiek ze standardów wpłynie na całą organizację.**

Układ standardów kontroli zarządczej wskazuje, od czego zacząć, przyglądając się funkcjonowaniu kontroli zarządczej w danej organizacji: od środowiska wewnętrznego przez cele i zarządzanie ryzykiem, mechanizmy kontroli, informację i komunikację aż po monitorowanie i ocenę.

Na podkreślenie zasługuje okoliczność, że dla zarządzania ryzykiem szczególnie istotne jest **poprawne działanie wszystkich standardów kontroli zarządczej.** W podobnym tonie brzmi komunikat nr 6 Ministra Finansów z 6.12.2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem: „Każdy z (...) elementów jest równie istotny i powiązany z pozostałymi. Ich prawidłowe funkcjonowanie determinuje także skuteczność zarządzania ryzykiem".

Ryzyko jest zasadniczo zjawiskiem niepożądanym. Jest definiowane jako „niebezpieczeństwo, że coś zdarzy się w inny od oczekiwanego sposób; «dobrze skalkulowana niepewność»" (https://sjp.pl/ryzyko, dostęp: 15.11.2019 r.). Jednak podobnie jak strach bywa sprzymierzeńcem człowieka, tak i ryzyko może oddziaływać pozytywnie na działalność jednostki. Odpowiednie rozumienie standardów kontroli zarządczej i wykorzystanie tych standardów w codziennym funkcjonowaniu jednostki są doskonałą odpowiedzią na już istniejące i ciągle pojawiające się ryzyka.

Zarządzanie ryzykiem jest **jednym z bloków tematycznych kontroli zarządczej** – „Cele i zarządzanie ryzykiem". Zatem punktem wyjściowym do rozpoczęcia procesu zarządzania ryzykiem jest właściwe ułożenie celów i zadań jednostki, czyli wskazywanie kierunków działania stosownie do przyjętych strategii.

Tu jednak należy wykazać czujność. Ustalenie celów zbyt ambitnych może zadziałać demobilizująco na pracowników. Brak realnej możliwości osiągnięcia zaplanowanych celów zdecydowanie obniży motywację do działania i może być źródłem frustracji. Natomiast ustalenie celów zbyt oczywistych i niewymagających żadnego wysiłku (np. działanie zgodne z prawem) w żadnej mierze nie wpisze się w strategię, a dodatkowo może sprawić, że działania będą prowadzone rutynowo, bez większego zaangażowania. A rutyna, jak wiadomo, doskonale usypia czujność i otwiera drogę do zaistnienia wielu ryzyk, których wcześniej nikt nie przewidział („tak było zawsze i nigdy nic się nie wydarzyło, więc dlaczego miałoby się teraz wydarzyć").

W pewnej mierze kontrola zarządcza niezwykle przypomina **system zarządzania jakością –** opiera się na procesach, planowaniu, monitorowaniu, ciągłym działaniu. Doskonale to odzwierciedla system PDCA, tzw. cykl Deminga:

Planuj → Wykonaj → Sprawdzaj → Działaj

To istota kontroli zarządczej, która jest pewnym modelem zarządzania, wyposażonym w narzędzia w postaci 22 standardów.

1. Zasada odpowiedniego planowania celów

Rozwiązaniem tego problemu i kluczową kwestią dla zapewnienia efektywnego działania jednostki jest planowanie celów zgodnie z **zasadą SMART.** Cel ma być **S**pecyficzny – czyli wyrażony w jednoznaczny sposób, **M**ierzalny – czyli umożliwiający zmierzenie poziomu jego osiągnięcia, **A**dekwatny – odpowiednio ambitny i dostosowany do misji i możliwości jednostki, **R**ealny – możliwy do osiągnięcia, **T**erminowy – ograniczony w czasie.

Właściwie ułożone cele, spójne ze strategią i misją jednostki, wyznaczają kierunek działania i pozwalają w prosty sposób monitorować postępy w działaniu.

W przypadku jednostek samorządu terytorialnego zarządzanie ryzykiem nie następuje nigdy tylko w odniesieniu do jednego konkretnego obszaru.

Dla przykładu, misją gminy jest treść art. 7 ustawy z 8.03.1990 r. o samorządzie gminnym – zaspokajanie zbiorowych potrzeb wspólnoty. Zakres zadań własnych określanych w wymienionym przepisie nie wyczerpuje działalności gmin – katalog zadań własnych gminy ma charakter otwarty, a ponadto należy jeszcze uwzględniać współpracę z instytucjami, realizację zadań zleconych.

2. Tytułem przykładu

W przypadku jednostek samorządu terytorialnego już istniejące dokumenty strategiczne i operacyjne powinny w zupełności wystarczyć dla pracowania nad zabezpieczeniem legalnej, efektywnej, oszczędnej i terminowej realizacji celów i zadań. To – dla niektórych być może nazbyt śmiałe – twierdzenie ma swoje uzasadnienie w praktyce.

Gotowe cele i zadania wyznaczane są w już istniejących dokumentach, w oparciu o które np. samorząd gminny pracuje. **Najbardziej czytelnymi przykładami mogą być:**

- budżet,
- plan postępowań o udzielenie zamówień.

Identyfikacja i analiza ryzyka względem celów inwestycyjnych z pewnością będą się opierały na tych dwóch dokumentach. **Po pierwsze,** oba dokumenty są wymagane przepisami rangi ustawowej, a **po wtóre** – bez planu finansowego nie może być mowy o planowaniu inwestycji, zaś wybór wykonawcy dla zamawiającego należącego do sektora finansów publicznych jest dokonywany w ramach postępowań w sprawie udzielenia zamówienia publicznego.

Dla powołanego powyżej przykładu związanego z inwestycjami trudno sobie wyobrazić prawidłowy przebieg procesu bez właściwie funkcjonujących standardów komunikacji wewnętrznej, wartości etycznych, kompetencji zawodowych, delegowania kompetencji, nadzoru czy szczegółowych mechanizmów kontroli dotyczących operacji finansowych i gospodarczych.

Każda organizacja jest jednym układem funkcjonalnym – im większa złożoność, tym większa rola i znaczenie właściwie funkcjonującej kontroli zarządczej. Doskonale to stwierdzenie obrazuje **cykl Deminga,** czyli wspomniany już wcześniej PDCA.

3. Identyfikacja i analiza ryzyka jako standardy współistniejące z innymi standardami kontroli zarządczej

Często zdarza się, że poszczególne standardy kontroli zarządczej wzajemnie się przenikają i występują w kilku rolach naraz. Tytułem przykładu można tu wskazać audyt wewnętrzny, który występuje jako samodzielny standard w postaci narzędzia oceny kontroli zarządczej, a może także stanowić jedną z podstaw innego standardu – uzyskania zapewnienia o stanie kontroli zarządczej czy monitorowania systemu kontroli zarządczej. Audyt wewnętrzny wykorzystuje także szereg innych standardów kontroli zarządczej – **w pierwszym rzędzie identyfikację ryzyka, analizę ryzyka czy monitorowanie systemu kontroli zarządczej.**

Zarządzanie ryzykiem jest szczególnym obszarem kontroli zarządczej. Odpowiednie funkcjonowanie tego bloku standardów kontroli zarządczej powinno stanowić **gwarancję realizowania zaplanowanych celów.**

Identyfikacja ryzyka oraz analiza ryzyka składają się na proces immanentnie związany z obszarami działania jednostki samorządu terytorialnego w zakresie audytu wewnętrznego oraz bezpieczeństwa informacji.

Audyt wewnętrzny, jednocześnie jeden ze standardów kontroli zarządczej, korzysta z zarządzania ryzykiem w ramach swojego działania. Przy konstruowaniu planu audytu na dany rok, o czym stanowi art. 283 ust. 3 u.f.p., kierownik komórki audytu wewnętrznego w porozumieniu z kierownikiem jednostki przygotowuje **na podstawie analizy ryzyka** plan audytu na następny rok. Podobnie według zapisów § 14 i 15 rozporządzenia Ministra Finansów z 4.09.2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu audytor wewnętrzny **w programie zadania audytowego wskazuje obszary ryzyka** w konkretnych zadaniach audytowych. Zatem identyfikacja i analiza ryzyka są w tym przypadku standardami współistniejącymi ze standardem audytu wewnętrznego. **Bez analizy ryzyka audyt wewnętrzny nie zadziała.** Identyfikacja i analiza ryzyka konfrontują ogólne wyobrażenia z potencjalnymi zagrożeniami. Faktem jest, że audytor dokonuje szacowania ryzyka na etapie wstępnym, zarówno planowania audytu na dany rok, jak i przeglądu wstępnego. Jednak wartość takiej analizy jest znaczna – w zależności od metodologii za pomocą obiektywnych kryteriów można otrzymać wstępne obszary potencjalnego zagrożenia dla jednostki, możliwych luk w systemie. Audyt wewnętrzny jako tzw. trzecia linia obrony może i powinien te zagrożenia identyfikować i wspomagać jednostkę w adekwatnych reakcjach na te zagrożenia.

Nadto należy mieć na względzie istotę audytu wewnętrznego, tj. **ocenę funkcjonowania kontroli zarządczej.** Zatem, z oczywistych względów, audytor wewnętrzny nie może wskazywać akceptowalnego poziomu ryzyka ani też przyjmować odpowiedzialności z tego tytułu czy też podejmować działań operacyjnych.

W zakresie bezpieczeństwa informacji kontrola zarządcza wyróżnia przede wszystkim standardy ochrony zasobów oraz standardy mechanizmów kontroli dotyczących systemów informatycznych. Istotnym regulatorem w tym zakresie jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – dalej RODO. W art. 32 RODO jest mowa o obowiązku administratora danych i podmiotu przetwarzającego dotyczącym wdrożenia – **adekwatnych do ryzyka** – środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa. Zatem, aby wdrożyć odpowiednie mechanizmy kontrolne – środki techniczne i organizacyjne – należy **zidentyfikować i poddać analizie istniejące ryzyka** towarzyszące przetwarzaniu danych. Brak zaprojektowania adekwatnych środków ochrony, czyli odpowiedniej struktury organizacji, oraz brak zaprojektowania i wdrożenia optymalnych zabezpieczeń technicznych z pewnością zmaterializują ryzyko w obszarze bezpieczeństwa informacji. O możliwych skutkach incydentów oraz niewłaściwie realizowanej polityki bezpieczeństwa nie trzeba nikogo przekonywać – od czasu wejścia w życie RODO Prezes Urzędu Ochrony Danych Osobowych zakończył już kilka postępowań, których finałem była decyzja nakładająca karę na administratorów danych osobowych, z czego jedna z decyzji dotyczy jednostki samorządu terytorialnego (zob. decyzja PUODO z 18.10.2019 r., ZSPU.421.3.2019, LEX nr 516286).

Dla bezpieczeństwa informacji znaczenie ma również **ocena skutków dla ochrony danych.** Zgodnie z art. 35 RODO administrator ochrony danych dokonuje takiej oceny, jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. I w tym przypadku bez wstępnego oszacowania ryzyka nie sposób właściwie realizować standardy kontroli zarządczej związanej z bezpieczeństwem informacji: standard ochrony danych oraz standard mechanizmów kontroli dotyczących systemów informatycznych.

Zatem zarządzanie ryzykiem nie jest procesem samym dla siebie. Łączy się z każdym rodzajem działalności jednostki i polega na minimalizowaniu zagrożeń z wykorzystaniem właściwych reakcji na ryzyko, w tym wykorzystaniu optymalnych mechanizmów kontroli.

4. Możliwe sposoby reakcji na ryzyko

Stosownie do standardów kontroli zarządczej ogłoszonych w komunikacie nr 23 są możliwe cztery sposoby reakcji na ryzyko: **tolerowanie, przeniesienie, wycofanie się, działanie**. Reakcja jest uzależniona od poziomu akceptacji ryzyka, jaki został w jednostce przyjęty. Ma to ścisły związek z następującymi elementami:

1. **poziomem istotności ryzyka** – czyli iloczynem skutku (wpływu) zmaterializowanego ryzyka oraz prawdopodobieństwa, że to ryzyko się zmaterializuje;

2. przyjętym w jednostce **poziomem akceptacji ryzyka** (tzw. apetyt na ryzyko) – jaki poziom ryzyka jednostka jest w stanie zaakceptować bez reagowania na nie w jakikolwiek sposób.

5. Jak to zrobić w praktyce

Pomocnym narzędziem oceny poziomu istotności ryzyka jest **matryca wskazująca współczynniki skutku** (co się może wydarzyć) **oraz prawdopodobieństwa** (na ile jest możliwe, że coś się wydarzy).

W pierwszej kolejności należy określić taką samą skalę punktową (np. od 1 do 6) dla skutku i dla prawdopodobieństwa. Następnie kierownik jednostki powinien określić wartości punktowe dla ryzyka na poziomie niskim, średnim i wysokim.

Tabela. Przykładowa matryca współczynników skutku i prawdopodobieństwa

	Skala prawdopodobieństwa					
Skala skutku	1	2	3	4	5	6
	2	4	6	8	10	12
	3	6	18	12	15	18
	4	8	12	16	20	24
	5	10	15	20	25	30
	6	12	18	24	30	36

Źródło: opracowanie własne

Na przykład można założyć, że ryzyko na poziomie niskim zamyka się w wartości liczbowej 6 i nie wymaga podjęcia żadnych działań, tym samym jest ryzykiem akceptowalnym oznaczającym tzw. apetyt na ryzyko. Na matrycy zaznaczymy to ryzyko **kolorem żółtym.** Oznacza to, że nawet jeśli prawdopodobieństwo jest na poziomie maksymalnym, ale skutek będzie na poziomie minimalnym, to poziom istotności ryzyka pozostanie niski: 6 × 1 = 6.

Kolejno, dla oznaczenia poziomu średniego można przyjąć maksymalną wartość 20 punktów. Na matrycy zaznaczmy ten poziom **kolorem pomarańczowym.**

Wreszcie, dla poziomu istotności ryzyka powyżej 20 punktów przyjmijmy poziom ryzyka wysokiego.

Kolejną decyzją zarządczą powinno być zaprojektowanie właściwych reakcji dla określonych poziomów ryzyka. Dla ryzyka niskiego najwłaściwszą reakcją będzie włączenie tolerowania. Natomiast dla ryzyka na poziomie średnim i wysokim pozostają do zastosowania pozostałe **trzy możliwe sposoby reakcji:**

1. **działanie** – włączanie możliwych mechanizmów kontroli dla zminimalizowania poziomu ryzyka. Dla przywołanego wyżej przykładu związanego z planem zamówień publicznych oraz planem finansowym może to być mechanizm kontrolny w postaci przeniesienia środków budżetowych dla zadania inwestycyjnego, wobec którego najkorzystniejsza ze złożonych ofert wykonawców przewyższa środki, które zamawiający zabezpieczył na realizację zadania;
2. **przeniesienie** – przeniesienie ryzyka z jednostki na podmiot zewnętrzny. Najprościej rzecz ujmując, można tu wskazać usługi zewnętrzne, ubezpieczenie itp.;
3. **wycofanie** – reakcja najmniej oczekiwana, ale czasem konieczna. W jednostce wycofanie z realizacji zadania czy osiągnięcia celu jest podejmowane w przypadku, gdy spodziewane korzyści nie są współmierne do poniesionych w tym celu nakładów. W przypadku jednostek sektora finansów publicznych kapitalne znaczenie ma treść art. 44 u.f.p. – wydatkowanie musi następować w sposób oszczędny i celowy oraz wedle ściśle określonych zasad: efektywności, racjonalności i terminowości.

6. Podsumowanie

Aby stale monitorować ryzyko określone na wysokim poziomie, warto stworzyć centralny rejestr ryzyka, gdzie można wprowadzić cel/zadanie zagrożone ryzykiem, ustalić osoby odpowiedzialne za wdrożenie określonych mechanizmów i termin dokonania tych czynności. Dla większej czytelności takiego rejestru warto skupić się na ryzyku, na poziomie którego należy podjąć reakcję związaną z działaniem, czyli powyżej poziomu niskiego. Powinien to być proces ciągły – ryzyko jest podatne na wpływy, a sposoby reakcji powinny być adekwatne dla rodzaju ryzyka i możliwości jednostki.

Autor:
Patrycja Szulin - absolwentka prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, wieloletni praktyk w zakresie kontroli zarządczej i systemu zarządzania jakością. Od 2001 r. zawodowo związana z administracją samorządową, a od 2014 r. audytor wewnętrzny CGAP.

Źródło: **Materiał pochodzi z LEX Administracja (komentarz praktyczny)**

Stan prawny: **2019 r.**

Nowa jakość w zarządzaniu samorządem

LEX Kontrola Zarządcza

Sprawdź, co zyska Twój urząd

LEX Kontrola Zarządcza to **oprogramowanie**, które kompleksowo wspiera jednostki samorządu terytorialnego w:

bieżącym **monitorowaniu zgodności** działania z prawem i procedurami wewnętrznymi

zarządzaniu **ryzykiem**

realizacji **obowiązku ustawowego** w zakresie kontroli zarządczej (art. 68 ust. o finansach publicznych)

Wolters Kluwer

www.produkty.LEX.pl/kontrola-zarzadcza

Wolters Kluwer Polska Sp. z o.o.
ul. Przyokopowa 33
01-208 Warszawa
PL-poczta@wolterskluwer.com
www.wolterskluwer.pl

Infolinia 801 04 45 45
22 535 88 00