INTOSAI GOV 9100

Najwyższa Izba Kontroli

Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym

INTOSAI GOV 9100

ISBN 978 -83-92-9290-5-5

Najwyższa Izba Kontroli

Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym

INTOSAI GOV 9100

INTOSAI

Tytuł oryginału:
Guidelines for Internal Control Standards for the Public Sector

Publikacja Międzynarodowej Organizacji Najwyższych Organów Kontroli.

Szanowni Państwo !

W roku 2011 Najwyższa Izba Kontroli przejęła przewodniczenie Podkomisji ds. Standardów Kontroli Wewnętrznej INTOSAI, której kluczowym zadaniem jest rozwój i promocja dobrych praktyk w dziedzinie kontroli wewnętrznej oraz położenie większego nacisku na odpowiedzialność/rozliczalność kadry kierowniczej w jednostkach sektora publicznego. Jednym z działań przyjętych w planie pracy podkomisji jest promocja standardów oraz wytycznych kontroli wewnętrznej w sektorze publicznym oznaczonych symbolem INTOSAI GOV. Dokument pn. Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym INTOSAI GOV 9100*, opracowany na podstawie zintegrowanej struktury ramowej kontroli wewnętrznej wypracowanej przez Komitet Organizacji Sponsorujących Komisję Treadway (COSO), zatwierdzony został przez XVIII Kongres INTOSAI w Budapeszcie w 2004 roku.*

W wytycznych INTOSAI GOV 9100 *określono ramy zalecane dla systemu kontroli wewnętrznej w sektorze publicznym oraz zasady oceny tego systemu. Kolejne rozdziały zawierają definicję kontroli wewnętrznej i ograniczenia dotyczące skuteczności kontroli, komponenty systemu kontroli wewnętrznej oraz rolę i odpowiedzialność pracowników. Ponadto do wytycznych załączono przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej oraz słownik zawierający najważniejsze terminy techniczne.*

Wytyczne INTOSAI GOV 9100 były konsultowane z Ministerstwem Finansów oraz Stowarzyszeniem Audytorów Wewnętrznych IIA Polska i zostały pozytywnie przyjęte przez obydwu partnerów NIK współpracujących w ramach zawartych porozumień. Spostrzeżenia MF dotyczące ujednolicenia definicji kontroli wewnętrznej przyjętej przez INTOSAI z definicjami COSO i IIA odnosiły się jedynie do niekonsekwencji w definiowaniu i używaniu niektórych pojęć w treści oryginału, co nie jest możliwe do zmodyfikowania poprzez odpowiednie tłumaczenie. Dlatego zamieściliśmy w przypisach dodatkowe objaśnienia odwołujące się do pojęć i definicji używanych w jednostkach sektora publicznego w Polsce. Ewentualne modyfikacje i korekty w samym dokumencie możliwe będą do wprowadzenia podczas pierwszego przeglądu zaplanowanego przez INTOSAI na rok 2016.

Mam nadzieję, że przedstawione przez Najwyższą Izbę Kontroli tłumaczenie Wytycznych w sprawie standardów kontroli wewnętrznej w sektorze publicznym INTOSAI GOV 9100 *posłuży promocji tych standardów oraz ułatwi dyskusję nad ich przyszłą aktualizacją.*

Jacek Jezierski

Prezes Najwyższej Izby Kontroli

Przedmowa

Wytyczne INTOSAI[1] w sprawie standardów kontroli wewnętrznej z 1992 r. pomyślane były jako otwarty dokument, odzwierciedlający wizję promowania standardów projektowania, wdrażania i ewaluacji kontroli wewnętrznej. Wizja ta uwzględnia także postulat podejmowania ciągłych działań na rzecz uaktualniania tych wytycznych.

17. INCOSAI[2], który miał miejsce w 2001 roku w Seulu, uznał, że istnieje wyraźna potrzeba aktualizacji wytycznych z 1992 r. i uzgodnił, że za jej podstawę należy przyjąć zintegrowaną strukturę ramową systemu kontroli wewnętrznej wypracowaną przez Komitet Organizacji Sponsorujących Komisję Treadway[3] (COSO). Wynikiem dalszych poszukiwań były dodatkowe zalecenia ujęcia wartości etycznych i przekazania większej ilości informacji na temat ogólnych zasad prowadzenia działań związanych z przetwarzaniem informacji w ramach systemu kontroli. Zrewidowane wytyczne uwzględniają te zalecenia i powinny ułatwić zrozumienie nowych pojęć w odniesieniu do kontroli wewnętrznej.

Zrewidowane wytyczne należy traktować jak dokument otwarty, który z czasem będzie wymagał dalszych rozwinięć i dopracowań, przy uwzględnieniu nowego opracowania COSO dotyczącego zarządzania ryzykiem korporacyjnym[4].

Niniejsza aktualizacja stanowi wynik współpracy członków Komisji Standardów Kontroli Wewnętrznej[5] INTOSAI. Aktualizacje te koordynuje zespół zadaniowy wyłoniony spośród członków Komitetu – przedstawicieli NOK Boliwii, Francji, Holandii, Litwy, Rumunii, Stanów Zjednoczonych, Węgier, Wielkiej Brytanii i Belgii (przewodnictwo).

Plan działań na rzecz aktualizacji wytycznych został przedłożony i zatwierdzony na 50. spotkaniu Zarządu (w październiku 2002 r. w Wiedniu). O postępach prac poinformowano Zarząd na 51. spotkaniu w październiku 2003 r. w Budapeszcie. Projekt był omówiony i w ogólnym zarysie przyjęty na spotkaniu komisji w lutym 2004 r. w Brukseli. Po spotkaniu komisji przekazano go wszystkim członkom INTOSAI w celu uzyskania uwag końcowych.

Otrzymane uwagi przeanalizowano i wprowadzono dalsze zmiany, które uznano za właściwe.

1 INTOSAI – International Organisation of Supreme Audit Institutions – Międzynarodowa Organizacja Najwyższych Organów Kontroli (przyp. red.).

2 INCOSAI – International Congress of Supreme Audit Institutions – Międzynarodowy Kongres Najwyższych Organów Kontroli (przyp. red.).

3 COSO, the Committee on Sponsoring Organizations of the Treadway Commission (przyp. red.).

4 COSO, Enterprise Risk Management – Integrated Framework (Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa), www.coso.org, 2004.

5 Internal Control Standards Committee (przyp. red.).

Chciałbym podziękować wszystkim członkom Komisji Standardów Kontroli Wewnętrznej INTOSAI za ich oddanie i współpracę podczas realizacji niniejszego projektu. Szczególne podziękowania składamy członkom zespołu zadaniowego.

Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym zostały przedstawione do zatwierdzenia przez XVIII INCOSAI w 2004 r. w Budapeszcie[6].

Franki VANSTAPEL

Prezes Beligijskiego Trybunału Obrachunkowego

Przewodniczący Komisji Standardów Kontroli Wewnętrznej INTOSAI

6 Wytyczne zostały zatwierdzone (przyp. red.).

Wprowadzenie[7]

W 2001 r. INCOSAI podjął decyzję o aktualizacji wytycznych INTOSAI z 1992 r. w sprawie standardów kontroli wewnętrznej, uwzględniając przy tym znaczący postęp dokonany w ostatnim okresie w dziedzinie kontroli wewnętrznej oraz włączając do dokumentu INTOSAI koncepcję zaczerpniętą z raportu COSO zatytułowanego *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa.*

Wdrażając poprzez wytyczne model COSO, Komisja stawia sobie za cel nie tylko aktualizację koncepcji kontroli wewnętrznej, ale również wniesienie wkładu do wspólnego pojmowania kontroli wewnętrznej wśród najwyższych organów kontroli (NOK). Oczywiście niniejszy dokument uwzględnia charakterystyczne cechy sektora publicznego. Właśnie to zainspirowało Komisję do uwzględnienia pewnych dodatkowych tematów i zmian.

W porównaniu z definicją COSO i wytycznymi z 1992 r., w niniejszych wytycznych dodano etyczny aspekt działań. Włączenie go do celów ogólnych kontroli wewnętrznej jest uzasadnione, gdyż od lat dziewięćdziesiątych[8] coraz silniejszy nacisk kładzie się na znaczenie zachowań etycznych, a także zapobieganie oraz wykrywanie nadużyć i korupcji w sektorze publicznym. Powszechnym stało się oczekiwanie, by urzędnicy w służbie publicznej uczciwie służyli interesowi publicznemu oraz właściwie zarządzali zasobami publicznymi. Obywatele powinni spotykać się z bezstronnym traktowaniem na zasadach legalności i sprawiedliwości. Dlatego też etyka w działalności publicznej stanowi warunek wstępny, a zarazem fundament zaufania publicznego i zwornik dobrego zarządzania.

Podkreślenia wymaga znaczenie ochrony zasobów w sektorze publicznym, dlatego że zazwyczaj mają one postać pieniądza publicznego, którego wykorzystanie w interesie publicznym wymaga szczególnej dbałości.

Co więcej, rachunkowość budżetowa na zasadzie kasowej, chociaż nie dostarcza wystarczającego zapewnienia odnoszącego się do pozyskiwania, wykorzystywania i zbywania zasobów, to jednak pozostaje nadal praktyką szeroko stosowaną w sektorze publicznym. W rezultacie jednostki sektora publicznego nie zawsze mają aktualny zapis wszystkich swoich aktywów, co powoduje, że są one bardziej narażone na utratę. Z tego względu ochronę zasobów uznano za ważny cel kontroli wewnętrznej.

Podobnie jak w 1992 r. kontrola wewnętrzna nie ograniczała się do tradycyjnego obrazu kontroli finansowej i powiązanej z nią kontroli administracyjnej, obejmując szerszą kon-

[7] Publikując *Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym,* Najwyższa Izba Kontroli dążyła do wprowadzenia precyzyjnej i jednoznacznej terminologii, która przyczyni się do lepszego rozumienia istoty dokumentu przez użytkowników z jednostek sektora publicznego w Polsce. Źródłem tej terminologii były m.in. ujęte w Glosariuszu polskojęzyczne wersje publikacji i dokumentów (przyp. red.).

[8] XVI INCOSAI, Montevideo, Urugwaj, 1998.

cepcję kontroli zarządczej. W niniejszym dokumencie podkreśla się także znaczenie informacji niedotyczącej finansów.

Z uwagi na szerokie stosowanie systemów informacyjnych we wszystkich jednostkach sektora publicznego wzrosło znaczenie informatycznych mechanizmów kontroli, co uzasadniło wprowadzenie odrębnego akapitu w niniejszych wytycznych. Informatyczne mechanizmy kontroli wiążą się z każdym z elementów procesu kontroli wewnętrznej podmiotu, łącznie ze środowiskiem wewnętrznym, oceną ryzyka, działaniami w ramach systemu kontroli, informacją i komunikacją, a także monitorowaniem. Jednak dla potrzeb prezentacji omówiono je w punkcie „Działania w ramach systemu kontroli”[9].

Celem Komisji jest opracowanie wytycznych do ustanowienia i utrzymania skutecznej kontroli wewnętrznej w sektorze publicznym. Dlatego ważnym adresatem tych wytycznych jest kadra kierownicza sektora publicznego. Kadra kierownicza rządu może wykorzystać te wytyczne jako podstawę do wdrażania i wykonywania kontroli wewnętrznej w podległych jednostkach.

Ponieważ ewaluacja kontroli wewnętrznej jest powszechnie przyjętym standardem warsztatowym w kontrolowaniu sektora publicznego[10], kontrolerzy mogą wykorzystać niniejsze wytyczne jako narzędzie audytu. Z tego względu wytyczne w sprawie standardów kontroli wewnętrznej zawierające model COSO mogą być wykorzystywane zarówno przez kierownictwo sektora rządowego[11] jako przykład solidnych ram kontroli wewnętrznej dla ich własnej jednostki, jak i przez audytorów, jako narzędzie oceny kontroli wewnętrznej. Wytyczne te nie są jednak pomyślane jako substytut standardów kontroli INTOSAI ani innych odnośnych standardów audytu.

Niniejszy dokument określa zalecane ramy kontroli wewnętrznej w sektorze publicznym oraz stanowi podstawę ewaluacji tej kontroli. Prezentowane w nim podejście stosuje się do wszelkich aspektów działalności jednostki, jednak jego celem nie jest ograniczenie należycie udzielonych uprawnień do opracowywania aktów prawnych, ustanawiania zasad lub innego kształtowania polityki jednostki na zasadach uznaniowości, w które to uprawnienia nie ingeruje.

---

9 *System kontroli wewnętrznej* jest synonimem *kontroli wewnętrznej*, dlatego w celu właściwego rozumienia pojęcia *control activities,* na potrzeby niniejszego dokumentu wersja polska tego pojęcia brzmi *działania w ramach systemu kontroli* (przyp. red.).

10 Standardy kontroli INTOSAI.

11 Personel operacyjny nie jest wyraźnie wymieniony jako grupa adresatów. Jednak kontrola wewnętrzna wywiera wpływ na członków tej grupy, którzy podejmują działania odgrywające ważną rolę w realizacji kontroli, w odróżnieniu od kierownictwa nie ponosząc ostatecznej odpowiedzialności za wszystkie działania jednostki związane z systemem kontroli wewnętrznej. Poszczególne role i obowiązki przedstawiono w rozdziale 3. niniejszych wytycznych.

Kontrolę wewnętrzną w jednostkach sektora publicznego należy rozumieć w kontekście ich specyficznych cech, tj.: ich koncentracji na realizacji ogólnych celów społecznych lub politycznych, wykorzystywania przez nie funduszy publicznych, znaczenia cyklu budżetowego, złożoności ich zadań (co wymaga zachowania równowagi pomiędzy tradycyjnymi wartościami, takimi jak legalność, uczciwość i przejrzystość, a nowoczesnymi wartościami zarządczymi, jak wydajność i skuteczność) oraz odpowiednio szerokiego zakresu ich rozliczalności publicznej.

W podsumowaniu należy wyraźnie stwierdzić, że niniejszy dokument zawiera wytyczne w sprawie standardów. Wytyczne te nie podają szczegółowych polityk, procedur i praktyk wdrażania kontroli wewnętrznej, ale raczej tworzą szerokie ramy, wewnątrz których podmioty mogą opracowywać szczegółowe mechanizmy kontrolne. Oczywiście Komisja nie ma uprawnień, by egzekwować stosowanie standardów.

Jaka jest struktura tego dokumentu?

W rozdziale pierwszym zdefiniowano pojęcie kontroli wewnętrznej i określono jej zakres. Zwrócono również uwagę na ograniczenia kontroli wewnętrznej. W rozdziale drugim przedstawiono i omówiono komponenty systemu kontroli wewnętrznej. Dokument zamyka rozdział trzeci o rolach i obowiązkach.

W każdej części, w zacienionej na szaro ramce, najpierw w skrócie przedstawiono główne zasady, pod którymi umieszczono dalsze informacje. Znalazły się tam również odniesienia do konkretnych przykładów, które można odnaleźć w załącznikach. Do dokumentu załączono także glosariusz zawierający najważniejsze terminy techniczne.

1. Kontrola wewnętrzna

1.1 Definicja

Kontrola wewnętrzna jest integralnym procesem, na który wpływ ma zarówno kierownictwo jednostki, jak i pracownicy; zwraca uwagę na ryzyka i dostarcza racjonalnego zapewnienia, że w działalności podmiotu realizującego swoją misję osiągnięte zostaną następujące cele ogólne:

- wykonywanie zadań w sposób uporządkowany, etyczny, oszczędny, wydajny i skuteczny;
- wypełnianie zobowiązań w zakresie rozliczalności;
- przestrzeganie obowiązującego prawa i regulacji;
- zabezpieczenia zasobów przed utratą, niewłaściwym wykorzystaniem i zniszczeniem.

Kontrola wewnętrzna jest dynamicznym, integralnym procesem, nieprzerwanie dostosowującym się do zmian, przed jakimi staje jednostka. Zarówno kierownictwo, jak i pracownicy wszystkich szczebli muszą być zaangażowani w ten proces, by zwracać uwagę na ryzyka i dostarczyć racjonalnego zapewnienia realizacji misji i celów ogólnych podmiotu.

Proces zintegrowany

Kontrola wewnętrzna nie jest pojedynczym zdarzeniem lub sytuacją, ale serią czynności, które przenikają działalność podmiotu. Czynności te przebiegają w sposób ciągły, w trakcie działań realizowanych przez podmiot. Są one wszechobecne i nieodłączne od sposobu, w jaki kierownictwo zarządza jednostką. Dlatego kontrola wewnętrzna różni się od poglądu prezentowanego przez niektórych obserwatorów, którzy uznają ją za coś dodanego do działań podmiotu albo za nieuniknione obciążenie. System kontroli wewnętrznej wplata się w działalność podmiotu i jest najbardziej skuteczny, kiedy zostaje wbudowany w infrastrukturę podmiotu jako integralny składnik istotnych działań wewnątrz jednostki.

Kontrola wewnętrzna powinna być wbudowana w bieżącą działalność, nie zaś stanowić jej dodatkowy element, tzn. nadbudowany. Poprzez wbudowanie kontrola wewnętrzna staje się częścią zintegrowaną z podstawowymi procesami zarządzania, tzn. planowania, wykonania i monitorowania.

Wbudowana kontrola wewnętrzna ma także znaczący wpływ na ograniczanie kosztów. Natomiast dodawanie nowych procedur kontrolnych, które są odrębne od już istniejących, mnoży koszty. Jednostka ma często możliwość uniknięcia niepotrzebnych procedur i kosztów poprzez skupienie się na istniejących rozwiązaniach i ich wykorzystanie w skutecznej kontroli wewnętrznej oraz poprzez zintegrowanie mechanizmów kontroli z podstawowymi działaniami operacyjnymi.

Realizowana przez kierownictwo i innych pracowników

To ludzie powodują, że kontrola wewnętrzna działa. Jej funkcjonowanie wewnątrz jednostki zależy od poszczególnych osób, od tego, co robią i mówią. Co za tym idzie, kontrola wewnętrzna jest skutecznie realizowana przez ludzi, którzy muszą znać swoje role i obowiązki oraz granice uprawnień. Ze względu na wagę tej koncepcji poświęcono jej odrębny rozdział (3).

Przez pojęcie „ludzie jednostki" należy rozumieć kierownictwo i pozostałych jej pracowników. Kierownictwo przede wszystkim sprawuje nadzór, ale także wyznacza cele podmiotu i ponosi całościową odpowiedzialność za system kontroli wewnętrznej. Ponieważ kontrola wewnętrzna zawiera mechanizmy stanowiące niezbędną pomoc do zrozumienia ryzyka w kontekście celów podmiotu, to kierownictwo będzie ustanawiało działania w ramach tej kontroli, monitorowało je i dokonywało ich ewaluacji. Wdrożenie kontroli wewnętrznej wymaga znaczącej inicjatywy zarządczej i intensywnej komunikacji kierownictwa z pozostałymi pracownikami. Dlatego też kontrola wewnętrzna jest narzędziem stosowanym przez kierownictwo i bezpośrednio powiązanym z celami podmiotu. Niemniej jednak wszyscy pracownicy jednostki odgrywają istotną rolę w jej urzeczywistnieniu.

Podobnie na kontrolę wewnętrzną ma wpływ natura ludzka. W wytycznych kontroli wewnętrznej uznano, że ludzie nie zawsze w sposób jednolity rozumieją, przekazują informację lub wykonują zadania. Każdy człowiek wnosi do miejsca pracy niepowtarzalne przygotowanie i potencjał merytoryczny oraz ma różne potrzeby i priorytety. Te realia wywierają wpływ na kontrolę wewnętrzną, a zarazem podlegają jej wpływowi.

W dążeniu do wypełniania misji podmiotu

Każda jednostka troszczy się przede wszystkim o wypełnianie własnej misji. Podmioty istnieją w jakimś celu – sektor publiczny, ogólnie rzecz biorąc, zajmuje się świadczeniem jakiejś usługi oraz uzyskaniem, w interesie publicznym, korzystnego wyniku tego działania.

Ustosunkowanie się do ryzyka

Wypełnianiu misji, bez względu na jej charakter, będą towarzyszyć różne ryzyka. Zadaniem kierownictwa jest zidentyfikować je i zareagować na nie w sposób maksymalizujący prawdopodobieństwo wypełnienia przez jednostkę własnej misji. Kontrola wewnętrzna może pomóc w ustosunkowaniu się do tych ryzyk, jednakże jest jedynie w stanie dostarczyć racjonalnego zapewnienia co do wypełnienia misji i celów ogólnych.

Dostarcza racjonalnego zapewnienia

Nawet najlepiej zaprojektowana i wdrażana kontrola wewnętrzna nie jest w stanie dostarczyć kierownictwu absolutnego zapewnienia dotyczącego osiągnięcia celów ogólnych. W zamian wytyczne uznają, że możliwy do osiągnięcia jest tylko „racjonalny" poziom zapewnienia.

Racjonalne zapewnienie oznacza zadawalający poziom zaufania przy uwzględnieniu danych kosztów, korzyści i ryzyk. Osądu wymaga określenie, jaki poziom zapewnienia jest racjonalny. Dokonując takiego osądu, kierownicy powinni zidentyfikować ryzyka nieodłączne dla własnych działań i poziomy ryzyka możliwe do przyjęcia w różnych okolicznościach oraz ocenić ryzyko zarówno w kategoriach ilościowych, jak i jakościowych.

Racjonalne zapewnienie odzwierciedla pogląd, że niepewność i ryzyko wiążą się z przyszłością, której nikt z całą pewnością nie jest w stanie przewidzieć. Możliwość osiągnięcia założonych celów zależy również od czynników pozostających poza kontrolą lub zakresem wpływu jednostki. Ograniczenia wynikają także z następujących realiów: ludzki osąd przy podejmowaniu decyzji może być ułomny, mogą zdarzyć się awarie z powodu prostych błędów lub pomyłek, w wyniku zmowy dwóch lub więcej osób może dojść do obejścia mechanizmów kontroli, kierownictwo może przekroczyć i naruszyć system kontroli wewnętrznej. Ponadto kompromisy w systemie kontroli wewnętrznej odzwierciedlają fakt, że mechanizmy kontroli wiążą się z ponoszeniem kosztu. Ograniczenia te z góry wykluczają uzyskanie przez kierownictwo absolutnej pewności, że cele zostaną osiągnięte.

Racjonalne zapewnienie zakłada, że koszt kontroli wewnętrznej nie powinien przekraczać uzyskanych dzięki niej korzyści. Decyzje o reakcjach na ryzyko i ustanawianiu mechanizmów kontroli powinny uwzględniać stosunek kosztów do korzyści. Koszt to finansowa miara zasobów zużytych w dążeniu do osiągnięcia konkretnego celu i ekonomiczna miara utraconych korzyści, na przykład na skutek opóźnienia działań, spadku poziomu lub wydajności świadczenia usług, obniżenia morale pracowników. Korzyść mierzona jest stopniem, w jakim zmniejszono ryzyko niepowodzenia realizacji ustalonego celu. Przykłady obejmują zwiększenie prawdopodobieństwa wykrycia oszustwa, marnotrawstwa, nadużycia lub błędu, zapobieżenie niewłaściwemu działaniu, wzmocnienie zgodności z regulacjami.

Zaprojektowanie mechanizmów kontroli wewnętrznej, które są korzystne kosztowo, a jednocześnie obniżają ryzyko do poziomu możliwego do przyjęcia, wymaga od kierownictwa dokładnego rozumienia celów całościowych, które mają zostać osiągnięte. W przeciwnym razie kierownicy sektora rządowego mogą projektować systemy obarczone nadmiarem mechanizmów kontroli w jednym obszarze działalności, co niekorzystnie wpłynie na inne działania, np.: pracownicy mogą podejmować próby obchodzenia uciążliwych procedur, niesprawne działania mogą powodować opóźnienia; rozbudowane ponad miarę procedury mogą hamować kreatywność i zdolność do rozwiązywania problemów wśród pracowników lub mieć niekorzystny wpływ na terminowość, koszt lub jakość usług świadczonych na rzecz beneficjentów. W ten sposób korzyści czerpane z rozbudowanych ponad miarę mechanizmów kontroli, ustanowionych w jednym obszarze, mogą zostać zniwelowane lub przewyższone przez zwiększone koszty innych działań.

Zagadnienie należy jednak rozpatrywać również z punktu widzenia jakości – ważne może być ustanowienie właściwych mechanizmów kontroli dla transakcji charakteryzujących się wysokim stopniem ryzyka przy niskim koszcie jednostkowym, np. pensje, rozliczenia kosztów delegacji czy reprezentacji, itp. Koszt właściwych mechanizmów kontroli mógłby wydać się nadmierny wobec kwot niewielkich w stosunku do całości wydatków sektora rządowego, lecz może okazać się, że taka kontrola ma zasadnicze znaczenie dla podtrzymania zaufania publicznego do rządów i związanej z nimi jednostki.

Osiąganie celów

Kontrola wewnętrzna ukierunkowana jest na osiągnięcie odrębnych, ale wzajemnie powiązanych celów ogólnych. Te cele ogólne realizowane są za pomocą wielu konkretnych celów cząstkowych, funkcji, procesów i działań.

Cele ogólne to:

- *wykonywanie uporządkowanych, etycznych, oszczędnych, wydajnych i skutecznych działań*

Działania jednostki powinny być uporządkowane, etyczne, oszczędne, wydajne i skuteczne. Muszą być one spójne z jej misją.

Działanie uporządkowane oznacza działanie dobrze zorganizowane, metodyczne.

Działania etyczne wiążą się z zasadami moralnymi. Od lat 90. XX w. rośnie nacisk na znaczenie zachowań etycznych, a także – zapobieganie oszustwom i korupcji oraz wykrywanie ich w sektorze publicznym. Ogólnie rzecz biorąc, od urzędników publicznych oczekuje się służby w interesie publicznym z zachowaniem zasad sprawiedliwości i prawidłowego gospodarowania zasobami publicznymi. Obywatele powinni doświadczać bezstronnego traktowania na zasadach legalności i sprawiedliwości. Dlatego etyka w działalności

publicznej stanowi warunek wstępny do budowania zaufania publicznego oraz zwornik ładu organizacyjnego.

Działanie oszczędne wolne jest od rozrzutności i ekstrawagancji. Oznacza to uzyskanie właściwej ilości zasobów o właściwej jakości, dostarczonych we właściwym czasie i we właściwe miejsce, przy najniższych kosztach.

Działanie wydajne odnosi się do związku pomiędzy zużytymi zasobami i wynikami uzyskanymi podczas realizacji celów. Oznacza to wykorzystanie minimalnych nakładów w celu osiągnięcia wyniku charakteryzującego się określoną ilością i jakością, albo osiągnięcie maksymalnych wyników z użyciem nakładów o określonej ilości i jakości.

Działanie skuteczne dotyczy osiągnięcia celów lub zakresu, w jakim wyniki z działalności odpowiadają celowi lub też oczekiwanym efektom tego działania.

- *wypełnianie zobowiązania podmiotu w zakresie rozliczalności*

Rozliczalność to proces, za sprawą którego jednostki w ramach służby publicznej i działające wewnątrz nich osoby rozlicza się z odpowiedzialności za podejmowane decyzje i działania, w tym za obsługę przez nie funduszy publicznych oraz wszelkie aspekty wykonania zadań.

Będzie to realizowane przez opracowywanie, aktualizację i udostępnianie wiarygodnych i istotnych informacji finansowych i niefinansowych oraz rzetelne ujawnianie tych informacji w sporządzanych terminowo sprawozdaniach przeznaczonych dla odbiorców wewnętrznych lub zewnętrznych.

Informacje niefinansowe mogą być związane z oszczędnością, wydajnością i skutecznością polityk i działań (informacje o wykonaniu zadań) oraz kontrolą wewnętrzną i jej skutecznością.

- *dochowanie zgodności z ustawami i przepisami*

Od jednostki wymaga się przestrzegania ustaw i przepisów. W jednostkach sektora publicznego ustawy i regulacje legitymizują pobieranie i wydatkowanie pieniądza publicznego oraz sposób prowadzenia działań. Przykładami są ustawa budżetowa, umowy międzynarodowe, ustawy dotyczące prawidłowego administrowania, ustawy/standardy rachunkowości, prawo regulujące ochronę środowiska i prawa obywatelskie, przepisy o podatku dochodowym oraz ustawy antykorupcyjne i dotyczące zwalczania nadużyć.

- *ochrona zasobów przed utratą, marnotrawstwem i szkodą w wyniku zniszczenia, nadużyć, niegospodarności, błędu, oszustwa lub nieprawidłowości*

Choć czwarty cel ogólny można uznać za podkategorię pierwszego (działania uporządkowane, etyczne, oszczędne, wydajne i skuteczne), w sektorze publicznym należy podkreślić znaczenie ochrony zasobów. Wynika to z faktu, że zasoby w sektorze publicznym

zasadniczo mają postać pieniądza publicznego, a ich wykorzystanie w interesie publicznym wymaga zazwyczaj szczególnej dbałości. Ponadto rozliczenia budżetowe na zasadzie kasowej, które nadal są powszechną praktyką w sektorze publicznym, nie dają racjonalnego zapewnienia w odniesieniu do nabywania, wykorzystywania i zbywania zasobów. W rezultacie jednostki sektora publicznego nie zawsze dysponują aktualnym spisem wszystkich środków będących w ich posiadaniu, co czyni je tym bardziej podatnymi na straty. Dlatego mechanizmy kontroli powinny zostać wbudowane w każde z działań związanych z zarządzaniem zasobami podmiotu, od chwili ich nabycia do zbytu.

Chronione powinny być również inne zasoby, takie jak informacje, dokumenty źródłowe i zapisy księgowe mające kluczowe znaczenie dla osiągnięcia przejrzystości i rozliczalności działań administracji rządowej. One również są bowiem zagrożone kradzieżą, niewłaściwym spożytkowaniem lub zniszczeniem.

Ochrona pewnych zasobów i zapisów staje się jeszcze ważniejsza od czasu pojawienia się systemów komputerowych. Informacje wrażliwe przechowywane na nośnikach komputerowych mogą zostać zniszczone lub skopiowane, rozpowszechnione i wykorzystane w sposób szkodliwy, jeśli nie zadba się o ich ochronę.

1.2 Ograniczenia skuteczności kontroli wewnętrznej[12]

System kontroli wewnętrznej nie może sam z siebie zapewnić osiągnięcia określonych wcześniej celów ogólnych.

Skuteczny system kontroli wewnętrznej, bez względu na to, jak dobrze jest pomyślany i wykorzystywany, może dostarczyć kierownictwu jedynie racjonalnego – a nie absolutnego – zapewnienia co do osiągnięcia celów podmiotu lub jego przetrwania. System ten może dać kierownictwu informacje o postępach podmiotu (lub ich braku) na drodze do realizacji celów. Jednak kontrola wewnętrzna nie może zamienić kierownika nieudolnego w dobrego. Ponadto zmiany polityki rządowej lub programów, uwarunkowania demograficzne lub gospodarcze, zazwyczaj pozostają poza kontrolą kierownictwa i mogą wymagać od zarządzających przeprojektowania mechanizmów kontroli lub ich dostosowania do dopuszczalnego poziomu ryzyka.

Skuteczny system kontroli wewnętrznej zmniejsza prawdopodobieństwo nieosiągnięcia celów. Zawsze jednak będzie istniało ryzyko, że kontrola wewnętrzna zostanie nieudolnie zaprojektowana lub nie zadziała w zamierzony sposób.

[12] Konieczne jest podkreślenie ograniczeń skuteczności kontroli wewnętrznej, aby uniknąć nadmiernych oczekiwań w wyniku nieporozumień co do zakresu jej faktycznej skuteczności.

Ponieważ kontrola wewnętrzna zależy od *czynnika ludzkiego*, może ucierpieć na skutek niedoskonałości projektu, błędów osądu lub interpretacji, nieporozumień, niedbalstwa, zmęczenia, roztargnienia, zmowy, nadużycia czy przekroczenia.

Innym czynnikiem ograniczającym jest projekt systemu kontroli wewnętrznej, który napotyka na *ograniczenia zasobów*. Korzyści, jakie przynoszą mechanizmy kontroli, muszą być konsekwentnie rozpatrywane w relacji do ich kosztów. Utrzymywanie systemu kontroli wewnętrznej, który wyklucza ryzyko strat, jest nierealne i prawdopodobnie jego koszty przewyższałyby gwarantowane dzięki niemu korzyści. Rozstrzygając, czy należy wprowadzić określony mechanizm kontroli, bierze się pod uwagę prawdopodobieństwo wystąpienia danego ryzyka i jego potencjalnego skutku dla podmiotu na równi z kosztami, jakie wiążą się z wprowadzeniem nowego mechanizmu kontroli.

Zmiany organizacyjne i postawa kierownictwa mogą mieć głęboki wpływ na skuteczność systemu kontroli wewnętrznej i osób obsługujących ten system. Zatem jest konieczne, by kierownictwo stale dokonywało przeglądów i aktualizacji mechanizmów kontroli, informowało pracowników o zmianach oraz dawało przykład stosowania się do tych mechanizmów kontroli.

2. Komponenty systemu kontroli wewnętrznej

Kontrola wewnętrzna składa się z pięciu wzajemnie powiązanych komponentów. Są to:

- środowisko wewnętrzne,
- ocena ryzyka,
- działania w ramach systemu kontroli,
- informacja i komunikacja,
- monitorowanie.

Kontrola wewnętrzna ma dostarczać racjonalnego zapewnienia o osiągnięciu celów ogólnych jednostki. Dlatego jasno określone cele są warunkiem wstępnym skuteczności procesu kontroli wewnętrznej.

Środowisko wewnętrzne[13] jest fundamentem całego systemu kontroli wewnętrznej. Zapewnia ono dyscyplinę i strukturę, a także klimat, który wywiera wpływ na ogólną jakość kontroli wewnętrznej. Przesądza o tym, jak ustanawia się strategię i cele oraz strukturę działań w ramach systemu kontroli.

Po określeniu jasnych celów i ustanowieniu skutecznego środowiska wewnętrznego ocena ryzyk stojących przez podmiotem, który podejmuje starania na rzecz realizacji własnej misji i celów, stanowi podstawę do opracowania właściwej reakcji na ryzyko.

Główna strategia ograniczania ryzyka prowadzi poprzez wewnętrzne *działania w ramach systemu kontroli*. Działania w ramach systemu kontroli mogą mieć charakter zapobiegawczy i/lub wykrywający. Działania naprawcze stanowią uzupełnienie działań kontroli wewnętrznej dla osiągnięcia wyznaczonych celów. Działania w ramach systemu kontroli i działania naprawcze powinny wnosić wartość w zamian za wydatkowane pieniądze. Ich koszt nie powinien przekraczać uzyskiwanych dzięki nim korzyści (opłacalność).

Skuteczna *informacja i komunikacja* mają żywotne znaczenie dla prowadzenia oraz kontrolowania własnych działań jednostki. Kierownictwo jednostki potrzebuje dostępu do istotnych, kompletnych, wiarygodnych, prawidłowych i terminowych informacji związanych ze zdarzeniami zarówno wewnętrznymi, jak i zewnętrznymi. Informacje te są niezbędne w całej jednostce do osiągnięcia jej celów.

[13] Na potrzeby niniejszego dokumentu wersja polska pojęcia *control environment* brzmi *środowisko wewnętrzne* (przyp. red.).

W końcu, skoro kontrola wewnętrzna jest procesem dynamicznym, który musi być w sposób ciągły dostosowywany do ryzyk i zmian, przed jakimi staje jednostka, konieczne jest *monitorowanie* systemu kontroli wewnętrznej, aby wspomóc działania na rzecz zapewnienia harmonii kontroli wewnętrznej ze zmieniającymi się celami, środowiskiem, zasobami i ryzykami.

Powyższe komponenty określają podejście zalecane dla systemu kontroli wewnętrznej w sektorze publicznym i tworzą podstawę, która jest odniesieniem do przeprowadzania ewaluacji tej kontroli. Komponenty te stosuje się do wszystkich aspektów działań jednostki.

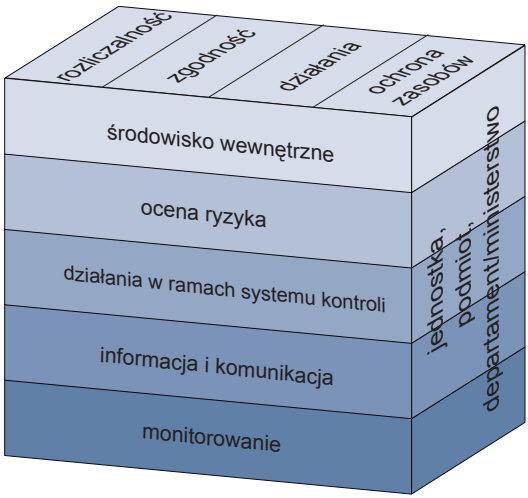
Niniejsze wytyczne zarysowują ramy ogólne. Wdrażając je, kierownictwo jest odpowiedzialne za opracowanie szczegółowych polityk, procedur i praktyk dopasowanych do działań prowadzonych przez jednostkę, oraz za zapewnienie, że są one wbudowane jako integralna część tych działań.

Związek celów ogólnych i komponentów

Istnieje bezpośredni związek pomiędzy celami ogólnymi, które przedstawiają to, co podmiot stara się osiągnąć, a komponentami kontroli wewnętrznej, które przedstawiają to, co jest konieczne do realizacji rzeczonych celów ogólnych. Związek ten ukazuje trójwymiarowa macierz w formie sześcianu.

Wspomniane wyżej cztery cele ogólne – rozliczalność (i sprawozdawczość), zgodność (z ustawami i przepisami), (uporządkowane, etyczne, oszczędne, wydajne i skuteczne) działania oraz ochrona zasobów – przedstawiono jako kolumny pionowe; pięć komponentów przedstawiono jako rzędy poziome, a jednostkę lub podmiot oraz departamenty istniejące wewnątrz przedstawiono jako trzeci wymiar macierzy.

Każdy rząd poziomy przedstawiający komponent „przecina" szereg każdego z celów ogólnych i do każdego z nich ma zastosowanie. Na przykład, dane finansowe i niefinansowe, pochodzące ze źródeł wewnętrznych i zewnętrznych, które należą do komponentu informacji i komunikacji, są potrzebne, aby zarządzać działaniami, sprawozdawać i wypełniać cele z zakresu rozliczalności oraz zachować zgodność z obowiązującym prawem.



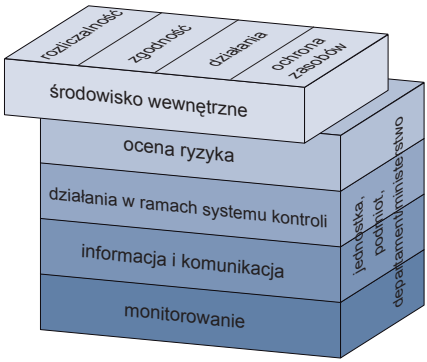
Podobnie, w przypadku celów ogólnych, wszystkie pięć komponentów odnosi się do każdego celu. Uwzględnienie jednego celu, takiego jak skuteczność i wydajność działań, jasno pokazuje, że wszystkie pięć komponentów stosuje się i jest ważne dla jego osiągnięcia.

Kontrola wewnętrzna odnosi się nie tylko do całej jednostki, ale także do pojedynczego departamentu. Związek ten ukazuje trzeci wymiar, który przedstawia jednostki, podmioty i departamenty. W ten sposób można skoncentrować się na dowolnej z komórek macierzy.

O ile ramy kontroli wewnętrznej są istotne i dają się zastosować do wszystkich jednostek, o tyle sposób, w jaki zostaną one zastosowane przez kierownictwo, pozostanie szeroko zróżnicowany, odpowiednio do charakteru podmiotu, i zależny od pewnej liczby specyficznych dla niego czynników. Czynniki te obejmują, między innymi: strukturę organizacyjną, profil ryzyka, środowisko działania, wielkość, złożoność działania i stopień regulacji. W konkretnej sytuacji podmiotu, aby zastosować ramowe komponenty systemu kontroli wewnętrznej, kierownictwo dokona szeregu wyborów, które mają związek ze złożonością wdrażanych procesów i metodologii.

W tekście poniżej zwięźle przedstawiono każdy z powyższych komponentów wraz z dodatkowymi uwagami.

2.1 Środowisko wewnętrzne



Środowisko wewnętrzne nadaje ton jednostce, wywierając wpływ na świadomość kontrolną jej kadry. Stanowi ono fundament wszystkich innych komponentów kontroli wewnętrznej, ustanawiając dyscyplinę i strukturę.

Elementy środowiska wewnętrznego to:

1) uczciwość osobista i zawodowa oraz wartości etyczne wśród kierownictwa i kadry, łącznie z postawą wspierania kontroli wewnętrznej w każdym czasie i w każdym miejscu jednostki;
2) zobowiązanie do kompetencji;
3) ton nadawany przez kierownictwo (tzn. filozofia i styl działania kierownictwa);
4) struktura organizacyjna;
5) polityki i praktyki związane z zasobami ludzkimi.

Uczciwość osobista i zawodowa oraz wartości etyczne kierownictwa i kadry

Uczciwość osobista i zawodowa oraz wartości etyczne członków kierownictwa i kadry determinują ich preferencje i osądy wartościujące, które przekładają się na normy zachowania. Powinni oni prezentować postawę wspierania kontroli wewnętrznej w każdym czasie i w każdym miejscu jednostki.

Każda osoba – spośród kierownictwa i pracowników – zaangażowana w sprawy jednostki musi utrzymywać i wykazywać uczciwość osobistą i zawodową oraz wartości etyczne, a także w każdym czasie przestrzegać stosownego kodeksu postępowania. Na przykład,

może to obejmować ujawnianie osobistych interesów finansowych, stanowisk poza jednostką i podarunków (np. przez urzędników wybieralnych i wysokiej rangi urzędników sektora publicznego) oraz zgłaszanie konfliktu interesów.

Również jednostki sektora publicznego muszą zachować i wykazać uczciwość oraz wartości etyczne; powinny też uwidocznić je w kontaktach ze społeczeństwem, we własnych deklaracjach dotyczących misji i kluczowych wartości. Ponadto ich działania muszą być etyczne, uporządkowane, oszczędne, wydajne i skuteczne, a także spójne z ich misją.

Zobowiązanie do kompetencji

Zobowiązanie do kompetencji obejmuje poziom wiedzy i umiejętności potrzebnych do wspomagania działania na rzecz zapewnienia uporządkowanego, etycznego, oszczędnego i skutecznego wykonania zadań, a także dobrego zrozumienia indywidualnych obowiązków wobec kontroli wewnętrznej.

Kierownicy i pracownicy muszą utrzymywać taki poziom kompetencji, który pozwala im zrozumieć ważność opracowania, wdrożenia i prowadzenia dobrej kontroli wewnętrznej oraz wykonywania przez nich obowiązków tak, aby osiągnąć ogólne cele tej kontroli i zrealizować misję jednostki. W jednostce każdy zaangażowany jest w kontrolę wewnętrzną za sprawą własnych specyficznych obowiązków.

Kierownicy i ich kadry muszą zatem utrzymywać i wykazywać się poziomem umiejętności koniecznym do oceny ryzyka i wspomagania działań na rzecz skutecznego i wydajnego wykonania zadań oraz zrozumieniem kontroli wewnętrznej wystarczającym do skutecznego wypełniania własnych obowiązków.

Na przykład zapewnienie szkoleń może podnieść świadomość urzędników sektora publicznego dotyczącą celów kontroli wewnętrznej, a zwłaszcza celu działań etycznych, a także pomóc im zrozumieć cele kontroli wewnętrznej oraz rozwinąć umiejętność właściwego traktowania dylematów etycznych.

Ton nadawany przez kierownictwo

„Ton na górze" nadawany przez kierownictwo (tzn. filozofia i styl działania kierownictwa) odzwierciedla:

- postawę wspierającą, w każdej chwili, wobec kontroli wewnętrznej, niezależność, kompetencję i przywództwo;
- kodeks postępowania określony przez kierownictwo, doradztwo oraz oceny wykonania zadań, które wspierają cele kontroli wewnętrznej, szczególnie dotyczące działań etycznych.

Postawa przyjęta przez najwyższe kierownictwo znajduje odzwierciedlenie we wszystkich aspektach jego działań. Oddanie, zaangażowanie i wsparcie najwyższych urzędników sektora rządowego i ustawodawców nadających „ton na górze" sprzyja pozytywnej postawie i ma zasadnicze znaczenie dla pozytywnej i wspierającej postawy wobec kontroli wewnętrznej w jednostce.

Jeśli najwyższe kierownictwo wierzy, że kontrola wewnętrzna jest ważna, inne osoby w jednostce wyczują to i zareagują, sumiennie stosując ustanowione mechanizmy kontroli. Na przykład utworzenie komórki audytu wewnętrznego jako części systemu kontroli wewnętrznej, to silny sygnał płynący od kierownictwa, że kontrola wewnętrzna jest ważna.

Z drugiej strony, jeśli pracownicy jednostki czują, że kontrola wewnętrzna nie jest przedmiotem poważnej troski najwyższego kierownictwa i raczej mówi się o niej, niż znacząco wspiera, jest niemal pewne, że cele kontrolne jednostki nie zostaną skutecznie osiągnięte.

W rezultacie nacisk na etyczne postępowanie i prezentowanie go wśród kierownictwa ma żywotne znaczenie dla celów kontroli wewnętrznej, a zwłaszcza dla celu „etyczności działań". Realizując swą rolę, kierownictwo powinno dawać dobry przykład poprzez własne działania, a jego postępowanie powinno odzwierciedlać to, co jest właściwe, nie zaś – akceptowalne lub korzystne. W szczególności polityki, procedury i praktyki kierownictwa powinny promować zachowania uporządkowane, etyczne, oszczędne, wydajne i skuteczne.

Na uczciwość kierowników i ich kadr wpływa jednak wiele elementów. Dlatego okresowo należy przypominać kadrze o obowiązkach wynikających z zapisów obowiązującego kodeksu postępowania wydanego przez najwyższe kierownictwo. Równie ważne są doradztwo i ocena wykonania zadań. Całościowa ocena wyników działania powinna opierać się na ocenie wielu kluczowych czynników, w tym roli pracowników w dokonaniach kontroli wewnętrznej.

Struktura organizacyjna

Struktura organizacyjna podmiotu określa:

- formalne przekazanie pełnomocnictwa i odpowiedzialności;
- upoważnienie i rozliczalność;
- właściwe sposoby sprawozdawania.

Struktura organizacyjna określa kluczowe zakresy pełnomocnictwa i odpowiedzialności podmiotu. Upoważnienie i rozliczalność odnoszą się do sposobu, w jaki dokonuje się delegacji tego pełnomocnictwa i odpowiedzialności wewnątrz jednostki. Niemożliwe jest delegowanie upoważnienia czy rozliczalności bez jakiejś formy sprawozdawania. Dlatego

trzeba określić właściwe tryby sprawozdawania. W wyjątkowych okolicznościach, tak jak w przypadkach, gdy kierownictwo uczestniczy w nieprawidłowościach, należy umożliwić zaistnienie innych niż zwykłe trybów sprawozdawania.

Struktura organizacyjna może obejmować komórkę audytu wewnętrznego, która powinna być niezależna od osób zarządzających i podlegać bezpośrednio władzy najwyższego szczebla w jednostce.

O strukturze organizacyjnej traktuje również rozdział trzeci dotyczący ról i odpowiedzialności.

Polityki i praktyki związane z zasobami ludzkimi

Polityki i praktyki związane z zasobami ludzkimi obejmują zatrudnianie i obsadzanie stanowisk, wprowadzenie do wypełniania obowiązków, szkolenie (formalne i na stanowisku pracy) oraz kształcenie, prowadzenie ewaluacji i doradztwa, awansowanie i wynagradzanie oraz działania naprawcze.

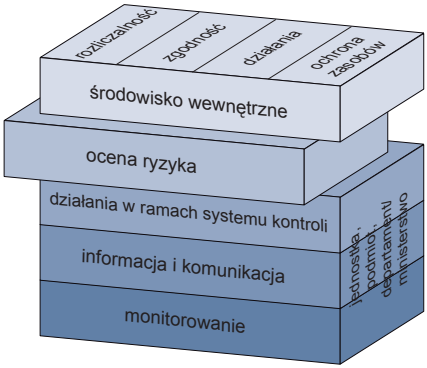
W kontroli wewnętrznej ważny jest aspekt kadrowy. Aby przeprowadzać skuteczną kontrolę, konieczna jest kompetentna i godna zaufania kadra. Dlatego metody stosowane przy zatrudnianiu, szkoleniu, ewaluacji, wynagradzaniu i awansach stanowią ważny element środowiska wewnętrznego. Z tego względu decyzje o zatrudnieniu i obsadzie stanowisk powinny obejmować zapewnienie, że dane osoby odznaczają się uczciwością, odpowiednim wykształceniem i doświadczeniem do wykonywania zadań wymaganych na ich stanowiskach pracy oraz że realizowane są konieczne szkolenia formalne dotyczące stanowiska pracy i z zakresu etyki. Kierownicy i pracownicy, którzy dobrze rozumieją kontrolę wewnętrzną i wykazują chęć wzięcia na siebie takiej odpowiedzialności, mają żywotny wkład w skuteczność tej kontroli.

Zarządzanie zasobami ludzkimi ma także zasadniczą rolę w promowaniu etycznego środowiska, rozwijaniu profesjonalizmu i egzekwowaniu przejrzystości w codziennej praktyce. Staje się to widoczne w procesach naboru, oceny i awansu, które powinny opierać się na zasługach. Zapewnienie otwartości procesu selekcji przez publikowanie zarówno zasad naboru, jak i wakujących stanowisk, również sprzyja realizacji etycznego zarządzania zasobami ludzkimi.

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

2.2. Ocena ryzyka



Ocena ryzyka to proces identyfikowania i analizowania ryzyk istotnych z punktu widzenia celów podmiotu i określenia właściwej reakcji na ryzyko.

Oznacza to:

1. identyfikację ryzyka:
   - związanego z celami podmiotu;
   - całościową;
   - obejmującą ryzyka wywoływane przez czynniki zewnętrzne i wewnętrzne, zarówno na poziomie podmiotu, jak i działania;
2. ewaluację ryzyka:
   - z oszacowaniem istotności ryzyka;
   - z uwzględnieniem prawdopodobieństwa wystąpienia ryzyka;
3. ocenę apetytu na ryzyko jednostki (skłonności jednostki do ryzyka);
4. reakcję na ryzyko:
   - należy uwzględnić cztery typy reakcji na ryzyko: przeniesienie, tolerowanie, przeciwdziałanie lub likwidację; dla niniejszych wytycznych najistotniejsze z nich jest przeciwdziałanie, ponieważ skuteczna kontrola wewnętrzna jest głównym mechanizmem przeciwdziałania ryzyku;
   - zastosowane właściwe mechanizmy kontroli mogą być albo wykrywające, albo zapobiegawcze.

Ponieważ uwarunkowania związane z rządzeniem, gospodarką, określoną branżą, przepisami i rodzajem działań podlegają ciągłym zmianom, ocena ryzyka powinna

być ciągłym, systematycznie powtarzanym procesem. Oznacza to identyfikowanie i analizowanie zmienionych warunków, szans i ryzyk (cykl oceny ryzyka) oraz modyfikowanie kontroli wewnętrznej w celu ustosunkowania się do zmian ryzyka.

Jak podkreślono w definicji, kontrola wewnętrzna może dostarczyć jedynie racjonalnego zapewnienia o realizacji celów jednostki. Ocena ryzyka, jako komponent kontroli wewnętrznej, odgrywa kluczową rolę w wyborze i podjęciu odpowiednich działań kontrolnych. Jest to proces identyfikowania i analizowania istotnych zagrożeń dla osiągnięcia celów podmiotu i określania stosownej reakcji.

Wynika z tego, że określenie celów stanowi warunek wstępny oceny ryzyka. Cele muszą zostać ustalone, zanim kierownictwo będzie mogło określić ryzyko ich osiągnięcia i podjąć konieczne działania, aby tymi ryzykami zarządzać. Oznacza to potrzebę stworzenia ciągłego procesu ewaluacji i odniesienia się do wpływu ryzyk w sposób opłacalny oraz dysponowania kadrą o odpowiednich umiejętnościach, by identyfikować i oceniać potencjalne zagrożenia. Działania kontroli wewnętrznej są reakcją na ryzyko, a planuje się je tak, aby pohamować zidentyfikowaną niepewność co do osiągnięcia wyniku.

Jednostki sektora publicznego muszą zarządzać ryzykami, które prawdopodobnie będą miały wpływ na świadczenie usług i osiąganie pożądanych wyników.

Identyfikacja ryzyka

Strategiczne podejście do oceny ryzyka zależy od określenia zagrożeń dla kluczowych celów organizacyjnych. Następnie rozważa się i ewaluuje ryzyka istotne ze względu na te cele, w efekcie uzyskując niewielki zbiór kluczowych zagrożeń.

Identyfikowanie kluczowych ryzyk jest ważne nie tylko jako droga do wskazania najważniejszych obszarów, na które skierować należy zasoby przeznaczone do oceny ryzyka, ale także jako podstawa rozdzielenia obowiązków zarządzania tymi ryzykami.

Wykonanie zadań przez podmiot może być zagrożone przez czynniki wewnętrzne lub zewnętrzne, zarówno na poziomie jednostki, jak i działania. Ocena ryzyka powinna uwzględnić wszystkie zagrożenia, jakie mogą wystąpić (łącznie z ryzykiem oszustwa i korupcji). Dlatego jest ważne, aby identyfikacja ryzyka była wszechstronna. Identyfikacja ryzyka powinna być procesem ciągłym i iteracyjnym, tzn. okresowo powtarzanym, a często także zintegrowanym z procesem planowania. Często pożyteczne bywa rozważenie ryzyka z pozycji „czystej kartki papieru", zamiast ograniczonych odniesień do poprzedniego przeglądu. Takie podejście ułatwia identyfikację zmian profilu ryzyka[14]

[14] Przegląd lub macierz podstawowych ryzyk stojących przed podmiotem lub jego komórką organizacyjną obejmuje także poziom wpływu (np. wysoki, średni, niski) prawdopodobieństwa lub prawdopodobieństwo wystąpienia zdarzenia.

jednostki jako wyniku zmian w środowiskach gospodarczym i regulacyjnym, wewnętrznych i zewnętrznych warunkach działania oraz wprowadzenia nowych lub zmodyfikowanych celów.

Konieczne jest przyjęcie właściwych narzędzi identyfikacji ryzyka. Dwa spośród najczęściej stosowanych narzędzi to zlecenie przeprowadzenia przeglądu ryzyk i samoocena ryzyka[15].

Ewaluacja ryzyka

Podejmowanie decyzji dotyczącej potraktowania ryzyka zasadniczo związane jest nie tylko ze wskazaniem istnienia pewnego typu zagrożenia, ale także z dokonaniem ewaluacji jego istotności oraz prawdopodobieństwa wystąpienia. Metodologia analizowania ryzyk może być zróżnicowana, ponieważ wiele zagrożeń trudno ująć w kategoriach ilościowych (np. zagrożenia dla reputacji), podczas gdy inne mogą być przedstawione ilościowo (zwłaszcza ryzyko finansowe). W pierwszym przypadku możliwa jest jedynie subiektywna opinia. Ewaluację ryzyka można w tej sytuacji traktować raczej jako sztukę niż naukę. Jednak stosowanie kryteriów systematycznej klasyfikacji zagrożeń ograniczy subiektywizm tego procesu, wyznaczając ramy dla logicznie formułowanych osądów.

Jednym z kluczowych celów ewaluacji ryzyka jest informowanie kierownictwa o obszarach ryzyka, w których należy podjąć działanie oraz wskazanie priorytetów. Dlatego zazwyczaj konieczne jest opracowanie pewnego systemu kategoryzacji wszystkich ryzyk, na przykład na wysokie, średnie lub niskie. Ogólnie rzecz biorąc, lepiej jest zminimalizować liczbę kategorii, gdyż nadmierna szczegółowość może doprowadzić do sztucznego rozdzielenia poziomów, których w rzeczywistości nie da się wyraźnie rozgraniczyć.

Drogą takiej ewaluacji można utworzyć ranking ryzyk, aby wyznaczyć priorytety zarządcze i przedstawić informację do decyzji kierowniczych w sprawie zagrożeń wymagających

15 *Zlecenie przeglądów ryzyka*:
Postępowanie to ma charakter odgórny. Powoływany jest zespół, którego zadaniem jest rozpatrzenie wszystkich działań i czynności jednostki w kontekście jej celów oraz identyfikacja związanych z nimi ryzyk. Zespół przeprowadza szereg rozmów z kluczowymi członkami kadry na wszystkich szczeblach organizacyjnych w celu sporządzenia profilu ryzyka dla różnorodnych czynności. Identyfikuje w ten sposób dziedziny, czynności i funkcje szczególnie podatne na ryzyko (w tym ryzyko oszustwa i korupcji).
Samoocena ryzyka:
Postępowanie to ma charakter oddolny. Poszczególne szczeble lub części jednostki proszone są o przegląd swojej działalności i przekazanie informacji o rozpoznanych ryzykach wyższemu szczeblowi. Można to osiągnąć środkami dokumentacyjnymi (wówczas ryzyka wskazywane są w kwestionariuszu) lub poprzez organizację warsztatów z prezentacją wprowadzającą.
Podejścia te nie są wzajemnie sprzeczne, a wręcz pożądane jest połączenie wkładu odgórnego i oddolnego do procesu oceny ryzyka, ułatwia to bowiem identyfikację ryzyk dotyczących zarówno całej jednostki, jak i pojedynczych czynności.

ustosunkowania się (na przykład tych obarczonych poważnym potencjalnym skutkiem i wysokim prawdopodobieństwem wystąpienia ryzyka).

Ocena „apetytu na ryzyko" jednostki

Ważną kwestią przy rozważaniu reakcji na ryzyko jest określenie apetytu na ryzyko w jednostce. Apetyt na ryzyko to poziom zagrożenia, na jaki podmiot jest przygotowany, zanim osądzi, że konieczne jest podjęcie działania. Decyzje o reakcjach na ryzyko muszą być podejmowane w powiązaniu z identyfikacją poziomu zagrożenia, jakie może być tolerowane.

Aby określić apetyt na ryzyko, należy uwzględnić zarówno ryzyka nieodłączne, jak i pozostałe (rezydualne). Ryzyko nieodłączne to zagrożenie dla podmiotu przy braku wszelkich działań, jakie kierownictwo mogłoby podjąć, aby zmienić prawdopodobieństwo wystąpienia tego ryzyka lub jego skutek. Ryzyko pozostałe to ryzyko pozostające po reakcji kierownictwa na dane zagrożenie.

Apetyt na ryzyko jest zróżnicowany zależnie od postrzegania znaczenia danych zagrożeń. Na przykład możliwa do tolerowania strata finansowa może być zróżnicowana odpowiednio do całego wachlarza cech, w tym wysokości danego budżetu, źródła straty lub innych powiązanych ryzyk, takich jak negatywny rozgłos. Identyfikacja apetytu na ryzyko to kwestia subiektywna, stanowi jednak ważny etap w formułowaniu całościowej strategii dotyczącej ryzyka.

Reakcja na ryzyko

W wyniku powyżej zarysowanych działań jednostka sporządza profil ryzyka, a następnie może rozważyć stosowną reakcję. Reakcje na ryzyko można podzielić na cztery kategorie. W niektórych przypadkach ryzyko można *przenieść, tolerować lub zlikwidować*[16]. Jednak w większości przypadków ryzyku należy odpowiednio *przeciwdziałać*, a podmiot

[16] W przypadku niektórych ryzyk najlepszym rozwiązaniem może być ich *przeniesienie*. Można to osiągnąć poprzez konwencjonalne ubezpieczenie, płacąc podmiotowi zewnętrznemu za przejęcie ryzyka lub poprzez klauzule umowne.
W przypadku niektórych ryzyk możliwości oddziaływania na nie mogą być ograniczone lub koszt podjęcia działań może być niewspółmierny do potencjalnych korzyści. W takiej sytuacji właściwym rozwiązaniem może być *tolerowanie ryzyka*.
Na niektóre ryzyka da się oddziaływać lub ograniczać je do akceptowalnego poziomu tylko przez *wycofanie się* z działalności, która je wywołuje. W sektorze publicznym możliwości wycofania się z działalności mogą być poważnie ograniczone w porównaniu z sektorem prywatnym. Wiele czynności wykonywanych jest w sektorze publicznym, ponieważ związane z nimi ryzyko jest tak znaczne, że nie istnieje inny sposób na osiągnięcie wyniku lub skutku potrzebnego dla dobra publicznego.

musi wdrożyć i utrzymywać skuteczny system kontroli wewnętrznej, aby zachować ryzyko na możliwym do przyjęcia poziomie.

Celem przeciwdziałania ryzyku nie musi być koniecznie jego eliminacja, ale – co bardziej prawdopodobne – ograniczenie go. Procedury, które ustanawia jednostka w celu przeciwdziałania ryzyku, zwane są działaniami kontroli wewnętrznej. Ocena ryzyka powinna odegrać kluczową rolę w wyborze właściwych działań kontrolnych. I znów trzeba tu powtórzyć, że nie jest możliwe wyeliminowanie wszelkiego ryzyka, a kontrola wewnętrzna może jedynie udzielić racjonalnego zapewnienia osiągnięcia celów jednostki. Jednakże jednostki, które aktywnie identyfikują ryzyka i zarządzają nimi, będą prawdopodobnie lepiej przygotowane do szybkiej reakcji w przypadku złego obrotu spraw i w ogóle do reakcji na zmiany.

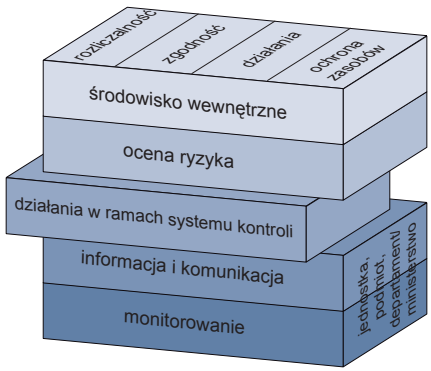
Przy opracowywaniu systemu kontroli wewnętrznej ważne jest, aby ustanowione działanie kontrolne było proporcjonalne do ryzyka. Poza skrajnie niepożądanym wynikiem, zazwyczaj wystarczy opracować mechanizm kontroli stanowiący źródło racjonalnego zapewnienia utrzymania straty w granicach apetytu na ryzyko danej jednostki (akceptowalnego poziomu ryzyka). Z każdą kontrolą wiąże się jakiś koszt, a działanie kontrolne musi wnosić wartość w zamian za poniesiony koszt, proporcjonalnie do ryzyka, którego dotyczy.

Z uwagi na ciągłe zmiany uwarunkowań związanych z sektorem rządowym, gospodarką, przemysłem, przepisami i działaniami, środowisko ryzyka każdej jednostki także stale się zmienia, a zatem priorytety celów i, co za tym idzie, hierarchia ważności ryzyk, będą się przemieszczać i zmieniać. Podstawą oceny ryzyka jest ciągły i iteratywny proces, w którym identyfikowane są zmiany warunków (cykl oceny ryzyka) i w miarę potrzeby podejmowane działania. Profile ryzyka i związane z nimi mechanizmy kontroli muszą być regularnie na nowo przeglądane i rozpatrywane dla zapewnienia stałej aktualizacji tego profilu, właściwego i współmiernego ukierunkowania reakcji na ryzyko oraz utrzymania skuteczności mechanizmów kontroli ograniczających ryzyko, pomimo zmian ryzyka w czasie.

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

2.3. Działania w ramach systemu kontroli



Działania w ramach systemu kontroli to polityki i procedury ustanowione dla ustosunkowania się do ryzyka i osiągnięcia celów podmiotu.

Aby działania w ramach systemu kontroli były skuteczne, muszą być właściwe, funkcjonować w sposób spójny, zgodnie z planem przez cały okres i być opłacalne, całościowe, racjonalne oraz bezpośrednio powiązane z celami kontroli.

Działania w ramach systemu kontroli prowadzone są w całej jednostce na wszystkich szczeblach i w odniesieniu do wszystkich funkcji. Obejmują one zakres zróżnicowanych kontrolnych działań wykrywających i zapobiegawczych, jak na przykład:

(1) procedury upoważniania i zatwierdzania;

(2) rozdział obowiązków (upoważnianie, przetwarzanie, zapis lub rejestracja, dokonywanie przeglądów);

(3) mechanizmy kontroli dostępu do zasobów i zapisów dokumentacji;

(4) weryfikacje;

(5) uzgodnienia;

(6) przeglądy wykonania zadań na poziomie operacyjnym;

(7) przeglądy działań, procesów i czynności;

(8) nadzór (przydzielanie obowiązków, przegląd i przyjmowanie wykonanych zadań, wytyczne i szkolenia).

Podmioty powinny osiągnąć równowagę pomiędzy wykrywającymi i zapobiegawczymi działaniami w ramach systemu kontroli.

Aby osiągnąć cele jednostki, należy podjąć działania naprawcze, które są koniecznym uzupełnieniem działań w ramach systemu kontroli.

Działania w ramach systemu kontroli to polityki i procedury ustanowione oraz wykonywane, żeby ustosunkować się do ryzyk i osiągnąć cele podmiotu.

Skuteczne działania w ramach systemu kontroli powinny:

- być właściwe (właściwa kontrola we właściwym miejscu i współmierna do ryzyka, którego dotyczy);
- funkcjonować konsekwentnie i zgodnie z planem przez cały okres (oznacza to ich ścisłe przestrzeganie przez wszystkich pracowników, których dotyczą i niepomijanie ich, gdy kluczowa kadra jest nieobecna albo obciążenie pracą jest duże);
- być opłacalne (to znaczy, że koszt wykonania kontroli nie powinien przekraczać uzyskiwanych dzięki niej korzyści);
- być całościowe, racjonalne i bezpośrednio wiązać się z celami kontrolnymi.

Działania w ramach systemu kontroli obejmują zróżnicowane polityki i procedury, takie jak:

1. Procedury upoważniania i zatwierdzenia

Upoważnianie i przeprowadzanie transakcji oraz zdarzenia realizowane są tylko przez kadrę działającą w zakresie swojej władzy. Upoważnienie to zasadniczy środek zapewnienia, że inicjowane są jedynie ważne transakcje i wydarzenia odpowiadające zamierzeniom kierownictwa. Procedury upoważnienia, które powinny być przejrzyście udokumentowane i przekazane kadrze kierowniczej i pracownikom, powinny zawierać konkretne warunki i okoliczności przydzielania upoważnień. Wypełnienie warunków upoważnienia oznacza, że pracownicy działają zgodnie z dyrektywami i w ramach ograniczeń ustanowionych przez kierownictwo lub zawartych w ustawodawstwie.

2. Rozdział obowiązków (upoważnianie, przetwarzanie, zapis lub rejestracja, dokonywanie przeglądów)

Aby zmniejszyć ryzyko błędu, marnotrawstwa lub szkodliwych działań oraz ryzyko niewykrycia takich problemów, kontrola wszystkich kluczowych etapów transakcji lub wydarzeń nie powinna być prowadzona przez jedną osobę ani jeden zespół. Obowiązki i zakresy odpowiedzialności powinny raczej być systematycznie przydzielane pewnej liczbie osób, co zapewnia istnienie zróżnicowanej i skutecznej kontroli. Kluczowe obowiązki obejmują udzielanie zgody na wykonanie i rejestrację transakcji, przetwarzanie i dokonywanie przeglądów lub kontrolowanie transakcji. Jednakże zmowa może zmniejszyć lub zniszczyć skuteczność działania kontroli wewnętrznej. Mała jednostka może mieć zbyt mało pracowników, aby w pełni zrealizować taką kontrolę. W takich przypadkach kierownictwo musi być świadome zagrożeń i rekompensować je innymi mechanizmami kon-

troli. Rotacja pracowników może pomóc w zapewnieniu, że jedna osoba nie zajmuje się przez nadmiernie długi okres wszystkimi kluczowymi aspektami transakcji lub zdarzeń. Również zachęcanie lub wymaganie wykorzystania corocznych urlopów może pomóc w zmniejszeniu ryzyka poprzez doprowadzenie do czasowej wymiany obowiązków.

3. Mechanizmy kontroli dostępu do zasobów i zapisów dokumentacji

Dostęp do zasobów i dokumentacji jest ograniczony do upoważnionych osób, które są odpowiedzialne za ochronę i /lub wykorzystanie zasobów. Rozliczalność z tytułu tej ochrony jest udokumentowana za pomocą pokwitowań, spisów inwentaryzacyjnych lub innych zapisów przekazania pod ochronę oraz rejestrujących jej przeniesienie. Ograniczenie dostępu do zasobów zmniejsza ryzyko ich nieupoważnionego wykorzystania lub utraty środków publicznych oraz pomaga zrealizować wytyczne kierownictwa. Stopień ograniczenia zależy od wrażliwości zasobu i ryzyka jego utraty lub niewłaściwego wykorzystania go. Powinien on być okresowo oceniany. Przy określaniu wrażliwości zasobu należy brać pod uwagę jego koszt, możliwość przemieszczania i zbycia.

4. Weryfikacje

Transakcje i znaczące zdarzenia są weryfikowane przed i po realizacji, na przykład przy dostawie liczba towarów jest weryfikowana z zamówieniem. Następnie liczba towarów wyszczególnionych na fakturze jest weryfikowana z liczbą towarów otrzymanych. Również stan magazynu weryfikowany jest na podstawie inwentaryzacji.

5. Uzgodnienia

Zapisy są regularnie uzgadniane z odpowiednimi dokumentami; na przykład zapisy księgowe dotyczące rachunków bankowych są uzgadniane z odpowiednimi wyciągami bankowymi.

6. Przeglądy wykonania zadań

Wykonanie zadań podlega regularnemu przeglądowi w kontekście zestawu standardów, w celu dokonania oceny skuteczności i wydajności. Jeśli przeglądy wykonania zadań wykażą, że faktyczne osiągnięcia nie odpowiadają przyjętym celom lub standardom, to procesy i czynności ustanowione dla osiągnięcia celów powinny podlegać przeglądowi, aby określić, czy wymagają usprawnienia.

7. Przeglądy działań, procesów i czynności

Działania, procesy i czynności powinny być okresowo poddawane przeglądowi dla zapewnienia, że pozostają one w spójności z aktualnymi przepisami, politykami, procedurami lub innymi wymogami. Ten typ przeglądu rzeczywistych działań danej jednostki powinien zostać wyraźnie odróżniony od monitorowania kontroli wewnętrznej, którą omówiono oddzielnie w części 2.5.

8. Nadzór (przydzielanie, przeglądanie i zatwierdzanie, wytyczne i szkolenia)

Kompetentny nadzór pomaga zapewnić osiąganie celów kontroli wewnętrznej. Przydzielanie, przeglądanie i zatwierdzanie wykonania prac przez pracowników obejmuje:

- przejrzyste komunikowanie o obowiązkach, odpowiedzialności i rozliczalności przypisanych każdemu pracownikowi;
- systematyczne przeglądy pracy każdego pracownika w koniecznym zakresie;
- zatwierdzanie wykonywania prac w ich kluczowych punktach dla zapewnienia, że ich tok odpowiada zamierzeniom.

Przydzielanie zadań przez zwierzchnika nie powinno zmniejszać jego rozliczalności dotyczącej tych obowiązków i zadań. Zwierzchnicy także dają pracownikom niezbędne wskazówki i zapewniają szkolenia, aby zagwarantować ograniczenie do minimum błędów, marnotrawstwa i szkodliwych działań oraz zrozumienie i realizację poleceń kierownictwa.

Wspomniana wyżej lista nie wyczerpuje, lecz wymienia najpowszechniejsze działania zapobiegawcze i wykrywające w ramach systemu kontroli. Działania 1-3 są zapobiegawcze, 4-6 bardziej wykrywające, podczas gdy 7-8 są zarówno zapobiegawcze, jak i wykrywające. Podmioty powinny osiągnąć równowagę pomiędzy działaniami wykrywającymi a zapobiegawczymi w ramach systemu kontroli. W związku z tym, w celu zrekompensowania konkretnych braków poszczególnych kontroli, często stosuje się mieszankę mechanizmów kontroli.

Z chwilą wdrożenia działania w ramach systemu kontroli zasadnicze znaczenie ma uzyskanie zapewnienia o jego skuteczności. W konsekwencji działania naprawcze stanowią niezbędne uzupełnienie działań w ramach systemu kontroli. Co więcej, musi być jasne, że działania w ramach systemu kontroli stanowią jedynie jeden komponent systemu kontroli wewnętrznej i powinny być zintegrowane z pozostałymi czterema komponentami.

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

2.3.1 Działania informatyczne w ramach systemu kontroli

Systemy informacyjne wymagają specyficznego typu działań w ramach systemu kontroli. Z tego względu informatyczne mechanizmy kontroli obejmują dwie szerokie grupy:

(1) Mechanizmy kontroli powszechnego zastosowania

Mechanizmy kontroli powszechnego zastosowania to struktury, polityki i procedury, które stosuje się do całości lub znacznej części systemów przekazu informacji danego podmiotu i które pomagają w zapewnieniu ich właściwego działania. Składają się one na środowisko, w którym działają systemy aplikacyjne i mechanizmy kontroli.

Najważniejszymi kategoriami mechanizmów kontroli powszechnego zastosowania są: (1) obejmujące całość podmiotu planowanie i zarządzanie programem bezpieczeństwa, (2) mechanizmy kontroli dostępu, (3) mechanizmy kontroli opracowania, utrzymania i zmian oprogramowania aplikacyjnego, (4) mechanizmy kontroli oprogramowania systemowego, (5) rozdział obowiązków, (6) ciągłość działania usług.

(2) Mechanizmy kontroli aplikacji

Mechanizmami kontroli aplikacji są struktury, polityki i procedury dostosowane do odrębnych, jednostkowych systemów aplikacyjnych, bezpośrednio związane z poszczególnymi aplikacjami komputerowymi. Mechanizmy te są zazwyczaj zaprojektowane w celu zapobiegania, wykrywania i korygowania błędów oraz nieprawidłowości w czasie przepływu informacji przez systemy informacyjne.

Mechanizmy kontroli powszechnego zastosowania i aplikacji są wzajemnie powiązane i na równi potrzebne do zapewnienia kompletności i dokładności przetwarzania informacji. Ponieważ informatyka zmienia się szybko, także związane z nią mechanizmy kontroli muszą stale zmieniać swoją postać, aby zachować skuteczność.

W miarę postępów informatyki jednostki stają się coraz bardziej zależne od skomputeryzowanych systemów informacyjnych w realizacji operacji oraz przetwarzaniu, przechowywaniu i sprawozdawaniu istotnych informacji. W związku z tym niezawodność i bezpieczeństwo skomputeryzowanych danych i systemów, które przetwarzają, przechowują i sprawozdają te dane, są istotnym problemem, zarówno dla kierownictwa, jak i audytorów jednostki. Pomimo że systemy informacyjne zakładają konkretne typy działań w ramach systemu kontroli, technologia informacyjna nie jest „samodzielnym" zagadnieniem kontroli, ale integralną częścią większości tych działań.

Wykorzystanie systemów skomputeryzowanych do przetwarzania informacji powoduje kilka ryzyk, które muszą zostać uwzględnione przez jednostki. Ryzyka te wynikają między innymi z jednolitego przetwarzania transakcji; automatycznego rozpoczynania transakcji przez systemy informacyjne; zwiększonego potencjału niewykrytych błędów; istnienia, kompletności i ilości ścieżek audytu; rodzaju używanego sprzętu komputerowego i oprogramowania oraz zapisywania transakcji niezwykłych lub nierutynowych. Na przykład ryzyko nieodłączne wynikające z ujednoliconego przetwarzania transakcji polega na tym, że każdy błąd wynikający z problemów z oprogramowaniem komputera będzie konsekwentnie występował w podobnych transakcjach. Skuteczne informatyczne mechanizmy kontroli mogą być dla kierownictwa źródłem racjonalnego zapewnienia, że informacja przetworzona przez systemy odpowiada pożądanym celom kontroli, takim jak zapewnienie kompletności, terminowości i aktualności danych oraz zachowanie ich rzetelności.

Informatyczne mechanizmy kontroli obejmują dwie szerokie grupy, a mianowicie mechanizmy kontroli ogólnego zastosowania i mechanizmy kontroli aplikacji.

Mechanizmy kontroli ogólnego zastosowania

Mechanizmami kontroli ogólnego zastosowania są struktura, polityki i procedury, które stosuje się do wszystkich lub znacznej części systemów informacyjnych podmiotu – takich jak duży system komputerowy, minikomputer, sieć i środowiska użytkowników końcowych – aby pomóc w zapewnieniu ich właściwego działania. Tworzą one środowisko, w którym działają systemy aplikacji i mechanizmy kontroli. Głównymi kategoriami mechanizmów kontroli ogólnego zastosowania są:

(1) *Planowanie i zarządzanie programem bezpieczeństwa obejmujące całość podmiotu*, które zapewnia strukturę ramową i ciągłość cyklu działań na rzecz zarządzania ryzykiem, opracowania polityk bezpieczeństwa, przydzielania obowiązków oraz monitorowania adekwatności związanych z systemem komputerowym mechanizmów kontroli podmiotu.

(2) *Mechanizmy kontroli dostępu* ograniczające lub wykrywające dostęp do zasobów komputerowych (dane, programy, sprzęt i funkcje) i chroniące je w ten sposób przed nieupoważnioną modyfikacją, utratą i ujawnieniem. Mechanizmy kontroli dostępu obejmują zarówno kontrole fizycznego dostępu, jak i statusu dostępu.

(3) *Mechanizmy kontroli opracowania, przechowywania i zmian oprogramowania aplikacyjnego* zapobiegające wprowadzaniu nieautoryzowanych programów lub zmian do istniejących programów.

(4) *Mechanizmy sterowania oprogramowania systemowego* ograniczające i monitorujące dostęp do programów i plików, które sterują sprzętem komputerowym i zabezpieczają aplikacje obsługiwane przez system.

(5) *Rozdział obowiązków* zakładający ustanowienie polityk, procedur i struktury organizacyjnej, w celu uniemożliwienia jednej osobie kontrolowania wszystkich kluczowych aspektów operacji związanych z wykorzystaniem komputera, a tym samym przeprowadzania nieupoważnionych działań lub uzyskania nieupoważnionego dostępu do środków lub zapisów.

(6) *Mechanizmy kontroli ciągłości usługi* pomagające, w razie nieoczekiwanego zdarzenia, nieprzerwanie zapewnić kontynuację lub szybkie wznowienie kluczowych operacji, a także ochronę kluczowych i wrażliwych danych.

Mechanizmy kontroli aplikacji

Mechanizmami kontroli aplikacji są struktura, polityki i procedury, które stosuje się do odrębnych pojedynczych systemów aplikacyjnych, takich jak: zobowiązania płatnicze, inwentaryzacja, lista płac, granty lub kredyty. Zaprojektowane są one tak, aby objąć przetwarzanie danych w ramach konkretnego oprogramowania aplikacyjnego.

Te mechanizmy kontroli są zazwyczaj przeznaczone do zapobiegania, wychwytywania i korygowania błędów oraz nieprawidłowości w trakcie przepływu informacji przez systemy informacyjne.

Mechanizmy kontroli aplikacji i sposób, w jaki informacja przepływa przez system informacyjny, mogą zostać podzielone na kategorie w trzech fazach cyklu przetwarzania:

- na wejściu: dane są autoryzowane, przetwarzane w formę skomputeryzowaną oraz wprowadzane do aplikacji w sposób dokładny i kompletny oraz w odpowiednim czasie;
- przetwarzanie: dane są właściwie przetworzone przez komputer, a pliki prawidłowo aktualizowane;
- na wyjściu: pliki i raporty generowane przez aplikacje odzwierciedlają transakcje lub zdarzenia, które faktycznie wystąpiły i dokładnie odzwierciedlają wyniki przetwarzania, a raporty są kontrolowane i rozprowadzane do upoważnionych użytkowników.

Mechanizmy kontroli aplikacji mogą również być podzielone na kategorie według rodzajów celów kontroli, z jakimi się wiążą, łącznie z tym, czy transakcje i informacje są autoryzowane, kompletne, dokładne i aktualne. Mechanizmy kontroli upoważnień dotyczą ważności transakcji i pomagają zapewnić, że transakcje odzwierciedlają zdarzenia, które faktycznie wystąpiły w danym okresie. Kompletność mechanizmów kontroli wiąże się z zapisywaniem wszystkich ważnych transakcji oraz ich właściwym sklasyfikowaniem. Dokładność mechanizmów kontroli obejmuje prawidłowość zapisów transakcji oraz dokładność wszystkich elementów danych. Brak mechanizmów kontroli rzetelności plików przetwarzania i plików danych mógłby unicestwić każdy ze wspomnianych powyżej mechanizmów kontroli i umożliwić wystąpienie nieautoryzowanych transakcji, a także przyczy-

nić się do powstania niekompletnych i niedokładnych danych. Mechanizmy kontroli aplikacji obejmują zaprogramowane działania w ramach systemu kontroli, takie jak automatyczne edycje oraz ręczne działania następcze prowadzone na wynikach wygenerowanych przez komputer na wyjściu, jak przeglądy raportów wskazujące na odrzucone lub nietypowe elementy.

Mechanizmy kontroli aplikacji i ogólnego zastosowania w systemach komputerowych są ze sobą wzajemnie powiązane

Skuteczność mechanizmów kontroli ogólnego zastosowania jest istotnym czynnikiem przy określaniu skuteczności mechanizmów kontroli aplikacji. Jeśli mechanizmy kontroli ogólnego zastosowania są słabe, to poważnie zmniejszają czy też obniżają niezawodność mechanizmów kontroli związanych z poszczególnymi aplikacjami. Bez skutecznych mechanizmów kontroli ogólnego zastosowania mechanizm kontroli aplikacji może okazać się nieskuteczny z powodu ignorowania, pomijania lub modyfikacji. Przykładowo kontrole edycji, mające zapobiegać wprowadzaniu przez użytkowników nierealnych liczb przepracowanych godzin (na przykład więcej niż 24 na dobę) do systemu listy płac, mogą stanowić skuteczny mechanizm kontroli aplikacji. Jednakże na tej kontroli nie można polegać, jeśli mechanizmy kontroli ogólnego zastosowania pozwalają na nieautoryzowane modyfikacje programów, dopuszczające wyłączenie niektórych transakcji spod kontroli edycji.

O ile podstawowe cele ogólne kontroli nie zmieniają się, to gwałtowne zmiany w technologii informatycznej wymagają ewolucji mechanizmów kontroli, aby pozostały one skuteczne. Zmiany takie jak zwiększone zaufanie do funkcjonowania w sieci, mocne komputery, które przesuwają odpowiedzialność za przetwarzanie danych na użytkowników końcowych, handel elektroniczny i internet, będą wywierały wpływ na charakter i wdrożenie konkretnych działań w ramach systemu kontroli.

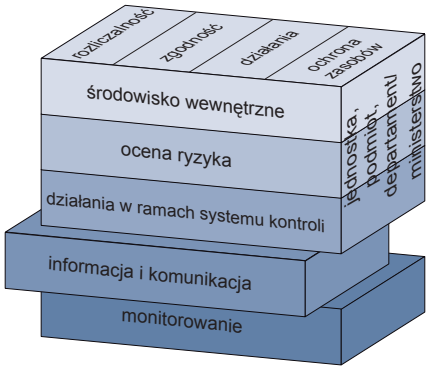
Więcej informacji na temat działań informatycznych w ramach systemu kontroli można uzyskać z materiałów Stowarzyszenia do spraw Audytu i Kontroli Systemów Informatycznych[17] (ISACA), a zwłaszcza standardów ISACA Control Objectives for Information and related Technology (COBIT) oraz postępowania komitetu audytu informatycznego INTOSAI (INTOSAI IT-audit comittee).

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

[17] Information Systems Audit and Control Association (ISACA).

2.4. Informacja i komunikacja



Informacja i komunikacja są podstawą do osiągnięcia wszystkich celów kontroli.

Informacja

Warunkiem wstępnym wiarygodnej i istotnej informacji jest szybkie zapisywanie i właściwa klasyfikacja transakcji i zdarzeń. Istotna informacja powinna zostać zidentyfikowana, wychwycona i przekazana w formie i ramach czasowych, które umożliwiają pracownikom realizację ich działań z zakresu kontroli wewnętrznej oraz innych obowiązków (przekaż właściwym ludziom we właściwym czasie). Z tego względu system kontroli wewnętrznej jako taki i wszystkie transakcje oraz znaczące wydarzenia powinny być w pełni dokumentowane.

Systemy informacyjne generują raporty, które zawierają informacje operacyjne, finansowe i niefinansowe, oraz dotyczące zgodności, a także umożliwiają prowadzenie i kontrolę działań. Dotyczą one nie tylko danych generowanych wewnętrznie, ale także informacji o zdarzeniach wewnętrznych, działaniach i warunkach koniecznych, by możliwe były podejmowanie decyzji i sprawozdawczość.

Zdolność kierownictwa do podejmowania właściwych decyzji jest kształtowana przez jakość informacji, co oznacza, że informacja powinna być właściwa, terminowa, aktualna, dokładna i dostępna.

Informacja i komunikacja są podstawą do realizacji wszystkich celów kontroli wewnętrznej. Na przykład jednym z jej celów jest wypełnienie zobowiązań wynikających z rozliczalności sektora publicznego. Można to osiągnąć przez opracowanie i przechowywanie wiarygodnych oraz istotnych informacji finansowych i niefinansowych, a także przekazywanie tych informacji za pomocą ich rzetelnego ujęcia w opracowywanych na czas sprawoz-

daniach. Informacja i komunikacja dotyczące wykonania zadań przez jednostkę stworzą możliwość ewaluacji działań w zakresie ładu, etyki, oszczędności, wydajności i skuteczności. W wielu przypadkach, aby zachować zgodność z ustawami i przepisami, trzeba dostarczać pewnych informacji lub musi istnieć komunikacja.

Informacja konieczna jest na wszystkich szczeblach jednostki do uzyskania skutecznej kontroli wewnętrznej i osiągnięcia celów podmiotu. Z tego względu wachlarz istotnych, wiarygodnych i odpowiednich informacji powinien zostać wskazany, wychwycony i przedstawiony w formie i ramach czasowych umożliwiających pracownikom wykonanie ich zobowiązań z zakresu kontroli wewnętrznej oraz innych. Warunkiem wstępnym wiarygodnej i odpowiedniej informacji jest szybkie zapisywanie i właściwa klasyfikacja transakcji i zdarzeń.

Jeśli informacja ma pozostać istotna i wartościowa dla kierownictwa w działaniach kontrolnych oraz podejmowaniu decyzji, to transakcje i zdarzenia muszą być zapisywane natychmiast, kiedy nastąpią. Stosuje się to do całego procesu lub cyklu życia transakcji lub zdarzenia, łącznie z ich rozpoczęciem i autoryzacją oraz wszystkimi etapami w trakcie procesu, a także ostateczną klasyfikacją tej transakcji w zapisach podsumowujących. Stosuje się to również do szybkiego uaktualnienia wszelkiej dokumentacji w celu podtrzymania jej istotności.

Aby zapewnić wiarygodność oraz dostępność informacji dla kierownictwa, wymagana jest również właściwa klasyfikacja transakcji i zdarzeń. Oznacza to organizowanie, klasyfikowanie i sformatowanie informacji, które są źródłem do przygotowania sprawozdania, planów i deklaracji finansowych.

Systemy informacyjne generują raporty, które zawierają informacje operacyjne, finansowe i niefinansowe oraz dotyczące zgodności, a także umożliwiają prowadzenie i kontrolowanie operacji. Systemy te nie tylko zajmują się formami jakościowymi i ilościowymi danych generowanych wewnętrznie, ale także informacjami o zdarzeniach wewnętrznych, działaniach i warunkach koniecznych do świadomego podejmowania decyzji i sprawozdawczości. Zdolność kierownictwa do podejmowania właściwych decyzji jest warunkowana przez jakość informacji, co oznacza, że informacja jest:

- właściwa (czy zawiera potrzebne informacje?);
- terminowa (czy jest wtedy, kiedy jest wymagana?);
- aktualna (czy dostępna jest najnowsza informacja?);
- dokładna (czy jest poprawna?);
- dostępna (czy da się uzyskać łatwo przez strony, których dotyczy?).

Aby pomóc w zapewnieniu jakości informacji i sprawozdawczości w działaniach kontroli wewnętrznej i wypełnianiu jej obowiązków oraz zwiększeniu skuteczności i spraw-

ności monitorowania, system kontroli wewnętrznej jako taki i wszystkie transakcje oraz znaczące zdarzenia powinny zostać w pełni i przejrzyście udokumentowane (na przykład diagramami przepływów i opisami wydarzeń). Dokumentacja ta powinna być łatwo dostępna do wglądu.

Dokumentacja systemu kontroli wewnętrznej powinna zawierać określoną strukturę, polityki i kategorie działań jednostki oraz wzajemnie powiązane cele i procedury kontrolne. Jednostka musi posiadać pisemny materiał dowodowy dotyczący komponentów procesu kontroli wewnętrznej, łącznie z jego celami i działaniami w ramach systemu kontroli.

Zakres dokumentacji dotyczącej kontroli wewnętrznej danego podmiotu zmienia się wraz z wielkością podmiotu, jego złożonością i podobnymi czynnikami.

Komunikacja

Skuteczna komunikacja powinna przebiegać pionowo – z góry w dół i z dołu do góry jednostki, oraz poziomo, poprzez wszystkie jej komponenty i całą strukturę.

Wszyscy pracownicy powinni otrzymywać od najwyższego szczebla kierowniczego przejrzysty przekaz dotyczący poważnego traktowania obowiązków kontrolnych. Powinni oni rozumieć swoją rolę w systemie kontroli wewnętrznej, a także to, w jaki sposób ich indywidualne działania wiążą się z pracą innych.

W kontaktach ze stronami zewnętrznymi także potrzebna jest skuteczna komunikacja.

Podstawą komunikacji jest informacja, która musi spełniać oczekiwania grup i osób, umożliwiając im skuteczną realizację własnych obowiązków. Skuteczna komunikacja powinna przebiegać we wszystkich kierunkach, płynąc w dół, w poprzek i w górę jednostki, poprzez wszystkie jej komponenty i całą strukturę. Jeden z kluczowych kanałów komunikacji przebiega pomiędzy kierownictwem a pracownikami. Kierownictwo musi być na bieżąco informowane o wykonaniu zadań, postępach, zagrożeniach i funkcjonowaniu kontroli wewnętrznej oraz innych istotnych zdarzeniach i problemach. Tą samą drogą kierownictwo powinno komunikować własnym pracownikom, jakiej informacji potrzebuje, a także przesyłać informację zwrotną i wskazówki. Kierownictwo powinno również przekazywać konkretne i ukierunkowane informacje dotyczące jego oczekiwań w zakresie zachowania. Obejmuje to przejrzystą deklarację filozofii i podejścia kontroli wewnętrznej danego podmiotu oraz nadawanie uprawnień.

Komunikacja powinna podnosić świadomość o wadze i istotności skutecznej kontroli wewnętrznej, mówić o apetycie na ryzyko i tolerancji ryzyka podmiotu oraz uświadamiać pracownikom ich role i obowiązki w skutecznym wdrażaniu i wspieraniu komponentów systemu kontroli wewnętrznej.

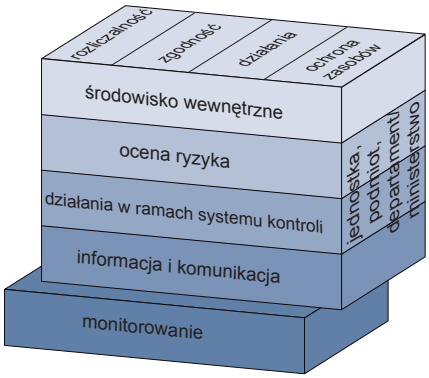
Ponieważ komunikacja zewnętrzna może stać się źródłem informacji wpływającej na zakres realizacji celów własnych jednostki, kierownictwo, obok komunikacji wewnętrznej, powinno zapewnić odpowiednie środki komunikowania i uzyskiwania informacji od stron zewnętrznych.

W oparciu o dane pochodzące z przekazów wewnętrznych i zewnętrznych, kierownictwo musi podjąć konieczne działania i realizować na czas działania następcze.

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

2.5. Monitorowanie



Systemy kontroli wewnętrznej powinny być monitorowane w celu oceny jakości funkcjonowania sytemu w miarę upływu czasu. Monitorowanie dokonywane jest poprzez rutynowe działania, odrębne ewaluacje lub kombinacje ich obu.

(1) Ciągłe monitorowanie

Ciągłe monitorowanie kontroli wewnętrznej wbudowane jest w normalne, cyklicznie powtarzane działania operacyjne danego podmiotu. Obejmuje regularne działania zarządcze i nadzorcze oraz inne działania, jakie podejmują pracownicy przy realizacji własnych zadań.

Ciągłe monitorowanie obejmuje każdy z komponentów kontroli wewnętrznej i pociąga za sobą przeciwdziałanie nieprawidłowemu, nieetycznemu, niegospodarnemu, niewydajnemu i nieskutecznemu systemowi kontroli wewnętrznej.

(2) Odrębne ewaluacje

Zakres i częstotliwość odrębnych ewaluacji uzależnione są przede wszystkim od oceny ryzyka oraz skuteczności procesu ciągłego monitorowania.

Konkretne odrębne ewaluacje obejmują ewaluację skuteczności systemu kontroli wewnętrznej i zapewniają osiągnięcie pożądanych wyników w oparciu o wcześniej zdefiniowane metody i procedury. Niedociągnięcia kontroli wewnętrznej powinny być sprawozdawane kierownictwu właściwego szczebla.

Monitorowanie powinno zapewnić właściwe i szybkie wprowadzanie w życie ustaleń i zaleceń kontroli.

Monitorowanie kontroli wewnętrznej ma na celu zapewnienie działania mechanizmów kontroli zgodnie z ich przeznaczeniem oraz modyfikowania ich adekwatnie do zmiany warunków. Monitorowanie powinno także ocenić, czy w dążeniu do realizacji misji podmiotu osiągane są cele ogólne określone w definicji kontroli wewnętrznej. Uzyskuje się to drogą ciągłego monitorowania, odrębnych ewaluacji lub kombinacji ich obu. Celem tych działań jest pomoc w uzyskaniu zapewnienia stosowania kontroli wewnętrznej na wszystkich szczeblach całego podmiotu oraz osiągania przez kontrolę wewnętrzną pożądanych wyników. Monitorowanie działań kontroli wewnętrznej jako takich powinno być wyraźnie odróżniane od przeglądów działań realizowanych przez jednostkę, te bowiem stanowią element działania w ramach systemu kontroli wewnętrznej, jak opisano powyżej w części 2.3.

Ciągłe monitorowanie kontroli wewnętrznej występuje w trakcie normalnych, powtarzalnych działań jednostki. Realizowane jest ono w sposób ciągły w czasie rzeczywistym i wplatane w działania podmiotu jako dynamiczna reakcja na zmieniające się warunki. W rezultacie jest ono bardziej skuteczne niż odrębne ewaluacje, a działania naprawcze są potencjalnie mniej kosztowne. Ponieważ odrębne ewaluacje mają miejsce po fakcie, często problemy będą identyfikowane szybciej w trakcie ciągłego monitorowania.

Zakres i częstotliwość odrębnych ewaluacji powinny zależeć przede wszystkim od oceny ryzyka i skuteczności procedur ciągłego monitorowania. Określając to, jednostka powinna uwzględnić rodzaj i zakres zmian wynikających zarówno ze zdarzeń wewnętrznych, jak i zewnętrznych, oraz związanych z nimi ryzyk; kompetencje i doświadczenie kadry wdrażającej reakcję na ryzyka i związane z tym mechanizmy kontroli oraz wyniki ciągłego monitorowania. Odrębne ewaluacje kontroli mogą także być przydatne, ponieważ koncentrują się bezpośrednio na skuteczności mechanizmów kontroli w konkretnym czasie. Ewaluacje te mogą też przyjąć formę samooceny oraz przeglądu przyjętej koncepcji kontroli i bezpośredniego testowania kontroli wewnętrznej. Mogą być również realizowane przez NOK-i oraz audytorów wewnętrznych lub zewnętrznych.

Zazwyczaj pewna kombinacja ciągłego monitorowania i odrębnych ewaluacji okazuje się pomocna w zapewnieniu utrzymania skuteczności kontroli wewnętrznej, w miarę upływu czasu.

Komunikat o wszystkich niedociągnięciach wykrytych w trakcie ciągłego monitorowania lub poprzez odrębne ewaluacje powinien być przekazany osobom, które z racji zajmowanego stanowiska podejmą konieczne działania. Termin „niedociągnięcia" odnosi się do sytuacji wpływającej na zdolność podmiotu do realizacji jego własnych celów. W związku z tym niedociągnięcia mogą być zauważalnym, potencjalnym lub rzeczywistym niedostatkiem lub też szansą na wzmocnienie kontroli wewnętrznej, a poprzez to na zwiększenie prawdopodobieństwa osiągnięcia celów ogólnych podmiotu.

Kluczowe znaczenie ma dostarczanie właściwej stronie koniecznych informacji dotyczących niedociągnięć kontroli wewnętrznej. Należy ustanowić protokoły umożliwiające identyfikację, które informacje są konieczne na konkretnym szczeblu do skutecznego podejmowania decyzji. Protokoły te odzwierciedlają ogólną zasadę, że kierownik powinien uzyskać informację wpływającą na działania lub zachowanie podległych mu pracowników, a także informację konieczną do osiągnięcia konkretnych celów.

Informacja generowana w toku działań jest zazwyczaj sprawozdawana normalnymi kanałami, to znaczy osobie odpowiedzialnej za daną funkcję, a także przynajmniej jednemu szczeblowi kierowniczemu powyżej tej osoby. Jednak powinny również istnieć alternatywne kanały komunikacji do sprawozdawania informacji wrażliwej, takiej jak działania sprzeczne z prawem lub niewłaściwe.

Monitorowanie kontroli wewnętrznej powinno obejmować polityki i procedury mające na celu zapewnienie odpowiednich i niezwłocznie podjętych rozstrzygnięć dotyczących ustaleń z audytu oraz innych przeglądów. Kierownicy mają (1) niezwłocznie dokonywać ewaluacji ustaleń z audytu oraz innych przeglądów, łącznie z tymi ukazującymi braki oraz zaleceniami sprawozdanymi przez audytorów i inne osoby dokonujące ewaluacji działań agencji; (2) określać właściwe działania w odpowiedzi na ustalenia oraz zalecenia pochodzące z kontroli i przeglądów oraz (3) realizować w określonych ramach czasowych wszystkie działania, które naprawiają lub w inny sposób rozwiązują kwestie przedstawione w celu zwrócenia ich uwagi.

Proces rozwiązywania zaczyna się od przekazania kierownictwu wyników kontroli lub innego przeglądu, a kończy się dopiero po podjęciu działań (1) poprawiających zidentyfikowane niedociągnięcia; (2) doprowadzających do poprawy lub (3) wykazujących, że ustalenia i zalecenia nie wymagają podjęcia działań przez kierownictwo.

Przykłady

Odsyłamy czytelnika do załączników, w których zamieszczono spójne przykłady dotyczące poszczególnych celów i komponentów systemu kontroli wewnętrznej.

3. Role i odpowiedzialności

Każdy w jednostce ma pewną odpowiedzialność wobec kontroli wewnętrznej:

Kierownicy	są bezpośrednio odpowiedzialni za wszystkie działania w jednostce, łącznie z projektowaniem, wdrażaniem, nadzorowaniem prawidłowego funkcjonowania, utrzymywania i dokumentowania systemu kontroli wewnętrznej. Ich obowiązki zróżnicowane są odpowiednio do funkcji pełnionych przez nich w jednostce oraz charakteru jednostki.
Audytorzy wewnętrzni	badają i przyczyniają się poprzez własne ewaluacje i zalecenia do ciągłej skuteczności systemu kontroli wewnętrznej, odgrywając przez to znaczącą rolę w skuteczności kontroli wewnętrznej. Nie ponoszą jednak głównej odpowiedzialności za projektowanie, wdrażanie i utrzymywanie oraz dokumentowanie kontroli wewnętrznej, która przypisana jest kierownictwu.
Pracownicy	również wnoszą wkład w kontrolę wewnętrzną, która jest częścią obowiązków każdego z nich, wyrażonych bezpośrednio lub pośrednio. Wszyscy pracownicy odgrywają pewną rolę w skutecznej kontroli i powinni być odpowiedzialni za sprawozdawanie dotyczące problemów w działaniach, niezgodności z kodeksem postępowania lub naruszania polityki.

Strony zewnętrzne także odgrywają ważną rolę w procesie kontroli wewnętrznej. Mogą one przyczynić się do osiągania celów jednostki lub dostarczać informacji przydatnych do wykonywania kontroli wewnętrznej. Jednakże nie są one odpowiedzialne za projektowanie, wdrażanie, właściwe funkcjonowanie, utrzymywanie lub dokumentowanie systemu kontroli wewnętrznej danej jednostki.

Najwyższe organy kontroli (NOK-i)	zachęcają i wspierają działania na rzecz ustanowienia skutecznej kontroli wewnętrznej w sektorze rządowym. Ocena kontroli wewnętrznej jest sprawą zasadniczą dla audytów zgodności, finansowych i wykonania zadań przeprowadzanych przez NOK-i. Przekazują one swoje ustalenia i zalecenia właściwym interesariuszom.
Audytorzy zewnętrzni	audytują pewne jednostki sektora rządowego w niektórych krajach. Oni oraz ich stowarzyszenia zawodowe powinni udzielać porad i zaleceń dotyczących kontroli wewnętrznej.
Organy ustawodawcze i regulacyjne	ustanawiają zasady i dyrektywy dotyczące kontroli wewnętrznej. Powinny one wnosić wkład w jednolite rozumienie kontroli wewnętrznej.
Inne strony	współdziałają z jednostką (beneficjenci, dostawcy, itp.) i dostarczają informacji dotyczących realizacji jej celów.

Kontrola wewnętrzna jest przede wszystkim wykonywana przez wewnętrznych interesariuszy podmiotu łącznie z kierownictwem, audytorami wewnętrznymi i innymi pracownikami. Jednak działania zewnętrznych interesariuszy także mają wpływ na system kontroli wewnętrznej.

Kierownicy

Wszyscy pracownicy jednostki odgrywają ważne role w funkcjonowaniu kontroli wewnętrznej. Jednakże to kierownictwo ponosi całościową odpowiedzialność za projektowanie, wdrażanie, właściwe funkcjonowanie nadzoru, utrzymywanie i dokumentowanie systemu kontroli wewnętrznej. Struktura kierownictwa może obejmować zarządy i komitety audytu, które pełnią różne role i mają różny skład oraz podlegają odrębnym przepisom prawnym w poszczególnych krajach.

Audytorzy wewnętrzni

Kierownictwo często ustanawia komórkę audytu wewnętrznego jako część systemu kontroli wewnętrznej i wykorzystuje ją do wspomagania monitorowania skuteczności tej kontroli. Audytorzy wewnętrzni regularnie dostarczają informacji o funkcjonowaniu kontroli wewnętrznej, koncentrując w znacznym stopniu uwagę na ewaluacji projektu i działaniach kontroli wewnętrznej. Przekazują informacje o mocnych i słabych stronach oraz zalecenia poprawy kontroli wewnętrznej. Jednak ich niezależność i obiektywizm powinny być zagwarantowane.

Z tego względu wykonywanie audytu wewnętrznego powinno być działaniem niezależnym, obiektywnie zapewniającym i doradczym, przysparzającym wartości i poprawiającym działanie jednostki. Pomaga to jednostce osiągnąć własne cele, wnosząc systematyczne, zdyscyplinowane podejście do ewaluacji i poprawy skuteczności procesów zarządzania, kontroli i zarządzania ryzykiem.

Pomimo że audytorzy wewnętrzni mogą być wartościową edukacyjną i doradczą siłą w systemie kontroli wewnętrznej, nie powinni oni zastępować silnego systemu kontroli wewnętrznej.

Dla skutecznego funkcjonowania audytu wewnętrznego istotne jest, aby kadra audytu wewnętrznego była niezależna od kierownictwa, pracowała w pozbawiony uprzedzeń, prawidłowy i rzetelny sposób oraz podlegała bezpośrednio najwyższemu szczeblowi władzy wewnątrz jednostki. Umożliwi to audytorom wewnętrznym przedstawianie bezstronnych opinii i własnych ocen kontroli wewnętrznej oraz obiektywne prezentowanie propozycji mających na celu poprawę ujawnionych niedociągnięć. Jako profesjonalne wytyczne audytorzy wewnętrzni powinni wykorzystywać „Ramowe zasady praktyki zawodowej”[18] Instytutu Audytorów Wewnętrznych (IIA), zawierające definicje, kodeks etyki, standardy i rady praktyczne. Dodatkowo audytorzy wewnętrzni powinni stosować Kodeks etyki INTOSAI.

Obok własnej roli w monitorowaniu kontroli wewnętrznej podmiotu, odpowiednia kadra audytu wewnętrznego może przyczynić się do skutecznych działań audytu zewnętrznego poprzez bezpośrednią pomoc audytorowi zewnętrznemu. Charakter, zakres lub rozłożenie w czasie procedur stosowanych przez audytora zewnętrznego może zostać zmodyfikowane, jeśli audytor zewnętrzny może polegać na pracy audytora wewnętrznego.

Członkowie kadry

Członkowie kadry i inni pracownicy także wdrażają kontrolę wewnętrzną. Często właśnie te osoby z pierwszej linii kontaktu, które stosują mechanizmy kontroli w realizacji swoich codziennych obowiązków, dokonują przeglądu tych mechanizmów, korygują ich niewłaściwe zastosowanie oraz identyfikują problemy, które mogą być najlepiej rozwiązane dzięki mechanizmom kontroli.

Strony zewnętrzne

Druga ważna grupa interesariuszy kontroli wewnętrznej to strony zewnętrzne, takie jak audytorzy zewnętrzni (łącznie z NOK), ustawodawcy i organy regulacyjne oraz inne strony. Mogą oni przyczyniać się do osiągania celów jednostki lub być źródłem informa-

[18] *Professional Practices Framework (PPF) of the Institute of Internal Auditors (IIA).*

cji użytecznej do wykonywania kontroli wewnętrznej. Jednak nie są oni odpowiedzialni za projektowanie, wdrożenie, właściwe funkcjonowanie, utrzymywanie lub dokumentowanie systemu kontroli wewnętrznej jednostki.

NOK i audytorzy zewnętrzni

Zadania stron zewnętrznych, zwłaszcza audytorów zewnętrznych i NOK, obejmują ocenę funkcjonowania systemu kontroli wewnętrznej i informowanie kierownictwa o ustaleniach dotyczących tego systemu. Jednak uwagi strony zewnętrznej dotyczące systemu kontroli wewnętrznej zdeterminowane są przez zakres jej upoważnienia.

Ocena kontroli wewnętrznej dokonana przez audytorów zakłada:

- ustalanie dotyczące znaczenia i wrażliwości na ryzyko ocenianego mechanizmu kontroli;
- ocenianie podatności na niewłaściwe wykorzystanie zasobów, niepowodzenie w realizacji celów w zakresie etyki, oszczędności, wydajności i skuteczności lub niewypełnienie zobowiązań w zakresie rozliczalności oraz niezgodność z ustawami i przepisami;
- zidentyfikowanie i zrozumienie istotnych mechanizmów kontroli;
- ustalanie, co już wiadomo na temat skuteczności kontroli;
- ocenianie adekwatności koncepcji kontroli;
- ustalanie za pomocą badań skuteczności mechanizmów kontroli;
- sprawozdawanie dotyczące ocen kontroli wewnętrznej oraz omawianie koniecznych działań naprawczych.

Najwyższy organ kontroli jest także istotnie zainteresowany, aby w przypadku zaistnienia takiej potrzeby zapewnić utworzenie silnych komórek audytu wewnętrznego. Komórki audytu stanowią istotny element kontroli wewnętrznej i są funkcjonującym w sposób ciągły narzędziem poprawy działań jednostki. Jednak w niektórych krajach komórkom audytu wewnętrznego może brakować niezależności, mogą też być słabe lub faktycznie nie istnieć. W takich przypadkach NOK powinien – tam, gdzie to możliwe – oferować pomoc oraz doradztwo na rzecz ustanowienia i rozwoju takiego potencjału, a także zapewniać niezależność działaniom audytora wewnętrznego. Pomoc taka mogłaby obejmować oddelegowanie lub użyczenie kadry, przeprowadzenie wykładów, udostępnienie materiałów szkoleniowych oraz opracowanie metodologii i programów roboczych. Powinno to być przeprowadzone bez zagrożenia dla niezależności NOK lub audytora zewnętrznego.

NOK potrzebuje również zbudowania dobrej relacji roboczej z komórkami audytu wewnętrznego, w sposób umożliwiający dzielenie się doświadczeniem i wiedzą oraz

wzajemne dopełnianie i uzupełnianie się pracy. Włączanie, gdy potrzeba, uwag audytu wewnętrznego i uznawanie ich wkładu w sprawozdania z audytu zewnętrznego, może także wzmocnić te relacje. NOK powinien wypracować procedury dotyczące oceny pracy komórki audytu wewnętrznego, aby określić, w jakim zakresie można na niej polegać. Silna komórka audytu wewnętrznego może zmniejszyć działania w ramach systemu kontroli wykonywane przez NOK i przyczynić się do uniknięcia niepotrzebnego jej dublowania. NOK powinien dopilnować, żeby miał dostęp do sprawozdań z audytu wewnętrznego, powiązanych z nimi opracowań roboczych i informacji o uchwałach audytu.

NOK-i powinny również odgrywać wiodącą rolę w odniesieniu do reszty sektora publicznego poprzez ustanowienie ramowego programu kontroli wewnętrznej w swojej jednostce, w sposób spójny z zasadami określonymi w niniejszej wytycznej.

Nie tylko NOK-i, ale również audytorzy zewnętrzni odgrywają ważną rolę, wnosząc wkład w osiągnięcie celów kontroli wewnętrznej, a zwłaszcza „realizację zobowiązań w zakresie rozliczalności" oraz „ochronę zasobów". Dzieje się tak, ponieważ audyty zewnętrzne sprawozdań finansowych i informacji stanowią integralną część rozliczalności i właściwego zarządzania. Audyty zewnętrzne są nadal pierwszorzędnym mechanizmem wykorzystywanym przez interesariuszy zewnętrznych do przeprowadzania przeglądów wykonania zadań oraz w odniesieniu do informacji niefinansowej.

Organy ustawodawcze i regulacyjne

Ustawodawstwo może być źródłem wspólnego rozumienia definicji kontroli wewnętrznej oraz celów, jakie mają zostać osiągnięte. Może także określać polityki, jakie interesariusze wewnętrzni i zewnętrzni mają stosować przy realizacji ich zadań i obowiązków w odniesieniu do kontroli wewnętrznej.

Załącznik 1

Przykłady

Wypełnianie zobowiązań w zakresie rozliczalności, przykład (1): Ministerstwo, które jest odpowiedzialne za zarządzanie bezpieczeństwem transportu drogami wodnymi śródlądowymi i morskimi, ma w swojej strukturze organizacyjnej różne departamenty usługowe odpowiedzialne za pilotowanie, oznakowanie bojami, kontrolę jakości wód, promocję wykorzystania szlaków wodnych, inwestycje w zakresie infrastruktury i jej utrzymanie (mosty, rowy, kanały i śluzy).

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Dla każdego z departamentów usługowych mianuje się kierownika do spraw operacyjnych, który musi podlegać kierownikowi departamentu. Kierownicy do spraw operacyjnych mają odpowiednie umiejętności i władzę, aby podejmować pewne decyzje. Wszyscy oni również podpisują kodeks właściwego postępowania.	Ewentualne ryzyka to kolizje statków, wyciek toksycznych odpadów lub paliwa i przelanie rowów. Gdyby te nieszczęśliwe wydarzenia zostały powiązane z zaniedbaniami ze strony ministerstwa, to mogłoby ono zostać obarczone ogromnymi roszczeniami.	Działania w ramach systemu kontroli, które mogą zostać podjęte, obejmują pilotaż statków przez kompetentnych pilotów, umieszczenie boi, znaków świetlnych i innego oznakowania; inspekcję wizualną z powietrza i pobieranie próbek wody.	Informacja i komunikacja powiązane z tą sytuacją mogą obejmować sprawozdawanie z kolizji, aby ostrzec inne statki; informowanie statków o warunkach pogodowych i publikowanie nazw podmiotów zanieczyszczających środowisko oraz sankcji, na jakie się narażają, a także podejmowanie akcji naprawczych.	Śledzenie liczby kolizji, naruszeń przepisów prawa środowiskowego, wyników badań pobranych próbek i porównania z innymi krajami oraz danymi z przeszłości mogą pomóc w monitorowaniu skuteczności i sprawności pilotowania statków, rozmieszczenia znaków świetlnych i innego oznakowania, inspekcji i próbek wody.

Wypełnianie zobowiązań w zakresie rozliczalności, przykład (2): Kierownik departamentu sportu w ubiegłym roku przyjął cel, w którym określił, że uprawianie sportu miałoby wzrosnąć o 15% w nadchodzących latach.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Z uwagi na dobrą reputację kierownika, komitet wykonawczy zaufał mu i nie przeprowadził zwyczajowych statutowych spotkań, aby sprawdzić ego postępy. *(opisana powyżej sytuacja nie stanowi przykładu dobrej praktyki!)*	Niewyszczególnianie celów rodzi ryzyko nieosiągania ich. Istnieje również niebezpieczeństwo, że sprawozdawanie nie będzie realizowane na czas, a kierownik będzie chciał poczekać ze swoim raportem do chwili, gdy będzie mógł powiedzieć, że zrealizował cel 15% wzrostu. Co więcej, nie określono, jak zmierzyć 15% wzrostu, a zatem kierownik może powiedzieć, że wzrosła liczba ludzi uprawiających sport lub liczba godzin, kiedy ludzie uprawiają sport, a nawet wzrosła o 15% liczba ośrodków sportowych lub klubów sportowych. W ten sposób jakość sprawozdawanej informacji w zasadniczy sposób się obniża.	To ryzyko można zmniejszyć poprzez ustanowienie właściwych sposobów sprawozdawania i modelu sprawozdawczości, określających informację, która powinna zostać przedstawiona.	Ten raport powinien zostać przedstawiony na czas i zgodnie ze ściśle określonym modelem sprawozdawczym. Powinien on określać cele wzrostu, sposoby mierzenia ich oraz uzasadnienie takiego sposobu mierzenia. Powinna zostać udostępniona wszelka informacja ogólna.	Weryfikacja tego, czy raport jest zadowalający, czy nie, oraz jaka informacja zostaje podana i jakiej informacji nadal brakuje, może być formą monitorowania.

Zgodność z odnośnymi przepisami ustawowymi i wykonawczymi, przykład: Ministerstwo obrony chce zakupić nowe myśliwce w drodze zamówienia publicznego i publikuje wszystkie postanowienia i procedury dotyczące tego przetargu rządowego. Wszystkie otrzymane oferty przetargowe pozostają zamknięte do końca okresu trwania postępowania. W tym momencie wszystkie oferty zostają otwarte w obecności odpowiedzialnych kierowników i pewnej liczby wyższych urzędników. Jedynie te otwarte oferty zostaną zbadane i porównane, aby podjąć decyzję, która z nich jest najlepsza.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Zespół, który przeprowadzi te transakcje, jest złożony z kompetentnych osób, które podpisały dokument świadczący, że nie mają żadnych powiązań finansowych ani zobowiązań/układów z żadnym ze startujących w przetargu. Dokument ten podpisali także odpowiedzialni kierownicy i wyżsi urzędnicy.	Jednym z ryzyk związanych z przetargami rządowymi i zamówieniami publicznymi jest zakulisowe zaangażowanie się kogoś z zespołu. Jeden z oferentów może dysponować uprzednio uzyskaną wiedzą o ofertach pozostałych oferentów i mógłby sporządzić zwycięską ofertę na podstawie tej informacji, prowadząc do tego, co mogłoby okazać się nie najlepszym wyborem spośród wszystkich ofert. Inne ryzyko polega na wyborze niewłaściwej oferty, co może doprowadzić do ogłoszenia nowego zamówienia publicznego, ponieważ inne nie sprostały oczekiwaniom. Także inni oferenci, którzy mają poczucie, że zostali potraktowani nieuczciwie, mogą przedstawić swoje roszczenia.	Aby ograniczyć ryzyka, powinno się opracować i zastosować procedury pozostające w zgodzie ze wszystkimi odnośnymi przepisami ustawowymi i wykonawczymi dotyczącymi zamówień publicznych.	Procedury związane z publikacją wszystkich postanowień dotyczących tego przetargu rządowego, ocena uzyskanych ofert i ogłoszenie wybranego oferenta powinny zostać udokumentowane na piśmie i wyszczególniać wszystkie działania, jakie zostaną podjęte. Przy ocenie ofert wszystkie powody, dla których dana oferta została lub nie została wybrana, powinny zostać udokumentowane.	Audyt wewnętrzny może dokonać przeglądu dokumentacji poszczególnych ofert i śledzić przedstawione roszczenia.

Uporządkowane, etyczne, gospodarne, sprawne i skuteczne operacje, przykład (1): Departament kultury chce zwiększyć liczbę wizyt w muzeach. Aby to osiągnąć, proponuje wybudowanie nowych muzeów, ofiarowanie każdemu obywatelowi czeku na uczestnictwo w kulturze i obniżkę cen biletów. Aby osiągnąć cele gospodarności, skuteczności i wydajności, kierownictwo musi rozważyć i oszacować, czy cele tak sformułowane mogą lub nie mogą zostać osiągnięte drogą realizacji tych propozycji oraz jak dużo te propozycje będą kosztować.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Departament kultury musi upewnić się, że jego struktura organizacyjna jest odpowiednia do wspierania nadzoru nad projektowaniem i konstrukcją proponowanych dodatków, a także planowaniem i działaniem nowych muzeów.	Jednym z możliwych ryzyk jest brak wzrostu liczby wizyt w muzeach. Istnieje również ryzyko, że niektóre propozycje przyniosą odwrotny skutek oraz że dojdzie do przekroczenia zaplanowanego na nie budżetu. Na przykład, jeśli obniżka cen biletów nie zwiększy liczby wizyt, to doprowadzi do obniżenia dochodów rządu. Co więcej, wybudowanie nowych muzeów bez właściwego planowania i rozważenia wymogów w zakresie oświetlenia, temperatury i zabezpieczeń może doprowadzić do kosztownych przeróbek w trakcie lub po zakończeniu budowy.	Działaniami w ramach systemu kontroli związanymi ze wspomnianymi wyżej ryzykami mogą być kontrola budżetu, która porównuje stan faktyczny z budżetem, obserwację postępów w budowie i wymaganie uzasadnienia dla przekroczeń budżetu.	Informacja i komunikacja powiązane z tym przykładem mogą obejmować dokumentację spotkań z architektami, przedstawicielami straży pożarnej (w zakresie przepisów bezpieczeństwa), artystami i innymi. Mogą również objąć różne raporty dotyczące dalszych działań w sferze budżetu i postępów w pracach budowlanych.	Część monitorowania stanowi analiza uzasadnienia przekroczenia budżetu i związanych z tym kosztów odsetek wynikających z opóźnienia prac lub płatności.

Uporządkowane, etyczne, gospodarne, skuteczne i wydajne działania, przykład (2): Rząd chce rozwinąć rolnictwo i poprawić jakość życia na obszarach wiejskich. Udostępnia fundusze na subsydiowanie budowy sieci melioracyjnej i wiercenia studni.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Rząd musi upewnić się, że ma właściwy departament zdolny do wdrożenia i przeprowadzenia subsydiowanych działań oraz nadać właściwy ton dla sprawnego ukończenia na czas całego projektu.	Ryzykiem z tym związanym jest zakwalifikowanie się do uzyskania grantów przez pozbawione skrupułów stowarzyszenia, które nie wykorzystają pieniędzy zgodnie z ich przeznaczeniem.	Działania w ramach systemu kontroli mogą obejmować: - Sprawdzenie kwalifikacji stowarzyszeń starających się o granty. - Sprawdzenie na miejscu postępów i dokonywanie przeglądów sprawozdań z postępów albo raportów z postępów w pracach budowlanych. - Sprawdzenie wydatków stowarzyszeń przez dokonanie przeglądu ich faktur oraz opóźnianie wypłat całości lub części subsydiów, dopóki przegląd nie zostanie zakończony.	- Sprawozdania z postępów wyszczególniające koszty i liczby studni, które zostały wywiercone, oraz liczby akrów, do których dotarła sieć nawadniająca. - (Kopie) faktur są wymagane jako uzasadnienie dla wydatków pokrywanych z subsydiów.	Monitorowanie może obejmować śledzenie prac związanych z wierceniem studni i budowaniem sieci melioracyjnej oraz porównanie z innymi podobnymi projektami. Można również rozważyć śledzenie działań na ziemi objętej melioracją.

Ochrona zasobów, przykład (1): Ministerstwo obrony ma kilka magazynów, składów wojskowych oraz składów paliwa. Zgodnie z przyjętą przez dowództwo wojska polityką zapasy te są przeznaczone wyłącznie do wykorzystania w wojsku, a nie do użytku osobistego.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Dobra polityka w zakresie kapitału ludzkiego powinna być skuteczna w zakresie rekrutacji i utrzymania odpowiedniego personelu, aby obsadzić nim stanowiska i prowadzić tego rodzaju magazyny.	Istnieje ryzyko, że ludzie będą starali się wykraść broń, aby posłużyć się nią w sposób niewłaściwy lub ją sprzedać. Również inne zapasy, takie jak paliwo, mogą być narażone na kradzież.	Działania w ramach systemu kontroli ukierunkowane na zapobieganie tym ryzykom mogą polegać na postawieniu płotów i muru wokół składów i magazynów lub umieszczeniu przy wejściach uzbrojonej straży z psami. W ochronie zasobów pomocne będzie także regularne sprawdzanie zapisów z inwentaryzacji i procedura potwierdzająca wydanie zapasów jedynie przy akceptacji wyższego oficera albo wyższego urzędnika.	Sprawozdania o zniszczonych płotach i różnicach dostrzeżonych w trakcie remanentów. Źródłem informacji i komunikacji związanej z tym celem są również potwierdzenia stanu zapasów i procedury.	Monitorowanie może obejmować inspekcję płotu, niezapowiedziane remanenty, śledzenie przemieszczania zapasów, a nawet tajne testy bezpieczeństwa.

Zabezpieczanie zasobów, przykład (2): Duże ilości wrażliwych informacji są gromadzone w komputerowych środkach przekazu agencji ministerstwa sprawiedliwości. Jednakże niedoceniane jest znaczenie informatycznych mechanizmów kontroli, w wyniku czego kontrola informatyczna ma niedociągnięcia.

Środowisko wewnętrzne	Ocena ryzyka	Działania w ramach systemu kontroli	Informacja i komunikacja	Monitorowanie
Kierownictwo musi podjąć swoje zobowiązanie do kompetencji i właściwego postępowania dotyczącego informatyki oraz zapewnić odpowiednie szkolenie w tym zakresie. Kluczową rolę w ustanowieniu pozytywnego środowiska wewnętrznego w zakresie zagadnień informatycznych odgrywają również polityki dotyczące kapitału ludzkiego.	Na szczeblu mechanizmów kontroli ogólnego zastosowania agencja nie: - ograniczyła dostępu dla użytkowników wyłącznie do zakresu koniecznego do wypełniania ich obowiązków; - rozwinęła wystarczających mechanizmów kontroli oprogramowania systemowego w celu ochrony programów i danych wrażliwych; - udokumentowała zmiany oprogramowania; - oddzieliła niezgodnych zakresów obowiązków; - ustosunkowała się do ciągłości obsługi; - ochroniła swoich sieci przed nieupoważnioną wymianą. Na szczeblu mechanizmów kontroli aplikacji agencja nie utrzymała autoryzacji dostępu *(To nie jest przykład dobrej praktyki!).*	Agencja może: - wdrożyć logiczne (to znaczy bazujące na hasłach) i fizyczne mechanizmy kontroli dostępu (na przykład zamki, plakietki identyfikacyjne, alarmy); - odmówić możliwości zalogowania się do systemu operacyjnego użytkownikom aplikacji; - ograniczyć dostęp do środowiska produkcji dla pracowników tworzących aplikacje; - wykorzystać dzienniki operacyjne audytu rejestrujące każdy dostęp (próbę dostępu) i polecenia, do wykrycia naruszenia bezpieczeństwa; - mieć plany awaryjne i powrotu do prawidłowego działania po załamaniu, aby zapewnić dostępność zasobów o kluczowym znaczeniu i ułatwić ciągłość działania; - mieć zabezpieczenia informatyczne i monitorować działalność serwera sieciowego, aby zabezpieczyć wymianę informacji w sieci.	Procedury z zakresu kontroli informatycznej powinny być dostępne, a zmiany oprogramowania powinny zostać udokumentowane, zanim oprogramowanie zostanie skierowane do praktycznego wykorzystania. Należy opracować polityki i opisy stanowisk pracy wspierające zasady rozdzielenia obowiązków. Dzienniki operacyjne audytu dotyczącego dostępu (lub usiłowań dostępu) i (nieupoważnionych) poleceń powinny być okresowo sprawozdawane i przeglądane.	Częścią monitorowania środowiska informatycznego może być prowadzenie audytu informatycznego, przeprowadzenie ćwiczenia symulowanego załamania działania i monitorowanie działania serwera sieciowego.

Załącznik nr 2

Glosariusz

Poniższy glosariusz opracowano z myślą o zapewnieniu jednolitego rozumienia głównych terminów zastosowanych w niniejszych wytycznych z odniesieniem do definicji i praktyk kontroli wewnętrznej. Obok niektórych definicji, jakie wprowadziliśmy w tym dokumencie, wykorzystaliśmy także definicje zaczerpnięte z rozmaitych źródeł, które podajemy poniżej:

- *Code of ethics and auditing standards*, INTOSAI, 2001 (INTOSAI auditing standards)
- *Internal Control – Integrated Framework,* COSO, 1992 (COSO 1992)
- *Glossarium*, Office for official publications of the European communities, P. Everard i D.Wolter, 1989 (glossarium)
- *Auditing and assurance services, an integrated approach*, A. A. Arens, R. J. Elder and M.S.Beasley, Prentice Hall international edition, ninth edition, 2003 (Arens, Elder & Beasley)
- The COSO exposure draft „Enterprise Risk Management Framework", COSO, 2003 (COSO ERM)
- *Handbook of international auditing, assurance, and ethics pronouncements*, IFAC, 2003 (IFAC)
- *Transparency International Source Book 2000* (Transparency International)
- XVI INCOSAI, Montevideo, Urugway, 1998, Principal Paper Theme 1A (*Preventing and Detecting Fraud and Corruption*), February 1997 (XVI INCOSAI, Uruguay, 1998)
- *Professional Practices Framework*, The Institute of Internal Auditors (IIA)

Tłumaczenie niektórych terminów i definicji użytych w polskiej wersji wytycznych zaczerpnięte zostało z wydanych w języku polskim następujących publikacji i dokumentów:

- *Kontrola wewnętrzna – zintegrowana struktura ramowa* (COSO I), PIKW, 2008.
- *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa* (COSO ERM), PIKW, 2007.

- „Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego", tłumaczenie na język polski, załącznik do komunikatu nr 4 Ministra Finansów z dnia 20.05.2011.
- Komunikat Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych.

A

Apetyt na ryzyko, skłonność do ryzyka *(Risk appetite)*

- Poziom ryzyka, na podjęcie jakiego dany podmiot jest przygotowany, bez uznania konieczności podjęcia działań.
- Poziom ogólnie rozumianego ryzyka, jakie firma lub inny podmiot są zdecydowane podjąć w toku realizacji własnej misji lub wizji. (COSO ERM)

Aplikacja *(Application)*

Program komputerowy zaprojektowany jako pomoc przydatna osobom wykonującym prace określonego typu, w tym konkretnie specjalne funkcje, takie jak sporządzanie list płac, inwentaryzacja, księgowanie lub wspieranie misji jednostki. Aplikacja w zależności od typu pracy, do jakiej jest zaprojektowana, może przetwarzać tekst, liczby i grafikę jako oddzielne elementy lub w określonej kombinacji.

Audyt *(Audit)*

Badanie działań i czynności podmiotu w celu uzyskania zapewnienia, że były one wykonywane lub funkcjonowały zgodnie z przyjętymi celami, budżetem, przepisami i standardami. Celem tego badania jest sprawdzanie w regularnych odstępach czasu występowania odstępstw, które mogłyby wymagać działań naprawczych. (glossarium)

Audyt wewnętrzny *(Internal audit)*

- Narzędzia funkcjonalne, za pomocą których kierownictwo jednostki ze źródeł wewnętrznych uzyskuje zapewnienie, że procesy, za które jest odpowiedzialne, działają w sposób ograniczający do minimum prawdopodobieństwo wystąpienia oszustwa, błędu oraz niewydajnego / niesprawnego lub nieoszczędnego działania. Posiada wiele cech audytu zewnętrznego, ale może wykonywać prawidłowo instrukcje szczebla kierowniczego, któremu podlega. (Standardy kontroli INTOSAI)

- Audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego i przyczynia się do poprawy ich działania. Pomaga organizacji osiągnąć cele, dostarczając zapewnienie o skuteczności tych procesów, jak również poprzez doradztwo. (IIA)
- Audyt wewnętrzny jest działaniem oceniającym, ustanowionym wewnątrz podmiotu na zasadzie usługi. Jego funkcje obejmują m.in. badanie, ocenianie i monitorowanie adekwatności i skuteczności systemów rachunkowości i systemów kontroli wewnętrznej. (IFAC)

Audytor wewnętrzny / audytorzy wewnętrzni *(Internal auditor(s))*

Bada i przyczynia się do bieżącej skuteczności poprawy systemu kontroli wewnętrznej poprzez jego ewaluację i opracowywanie zaleceń, ale nie ponosi głównej odpowiedzialności za jego koncepcję, wdrożenie, utrzymanie i dokumentowanie.

Audyt zewnętrzny *(External audit)*

Audyt wykonywany przez podmiot zewnętrzny i niezależny od podmiotu audytowanego, mający na celu wydanie opinii i przedstawienie sprawozdania dotyczącego rachunków i sprawozdań finansowych, prawidłowości i legalności działań i/lub zarządzania finansowego. (glossarium)

B

Budżet *(Budget)*

Program środków zaplanowanych na dany okres ujęty w [kategoriach] ilościowych i finansowych. Budżet sporządza się w celu zaplanowania przyszłych operacji i sprawdzenia ex post uzyskanych wyników. (glossarium)

Blokowy schemat działania *(Flowchart)*

Przedstawienie w formie wykresu dokumentów i zapisów klienta z uwzględnieniem kolejności, w jakiej są przetwarzane. (Arens, Elder i Beasley)

C

COSO *(COSO)*

Komitet Organizacji Sponsorujących Komisję Treadway (Committee of sponsoring Organisations of the Treadway Commission), grupa kilku jednostek zajmujących się rachunkowością. W 1992 r. opublikowała znaczące studium dotyczące kontroli wewnętrznej zatytułowane: *Internal Control – Integrated Framework (Kontrola wewnętrzna – zintegrowana struktura ramowa)*. Opracowanie to często określa się jako Raport COSO.

Cykl oceny ryzyka *(Risk assessment cycle)*

Ciągły, powtarzany okresowo proces identyfikacji i analizy zmian warunków, szans i ryzyk oraz podejmowania w miarę potrzeby stosownych działań, zwłaszcza – modyfikacji kontroli wewnętrznej w reakcji na zmieniające się ryzyko. Profile ryzyka i związane z nimi mechanizmy kontroli muszą być regularnie rewidowane i rozważane na nowo dla uzyskania zapewnienia, że profil ryzyka pozostaje aktualny, reakcje na ryzyko są właściwie ukierunkowane i współmierne, a zmniejszające ryzyko mechanizmy kontroli pozostają skuteczne pomimo następujących wraz upływem czasu zmian ryzyka.

D

Dane *(Data)*

Fakty i informacje, które mogą być zakomunikowane i przetworzone.

Działanie w ramach systemu kontroli *(Control activity)*

Działania w ramach systemu kontroli to polityki i procedury ustanowione dla ustosunkowania się do ryzyka i osiągnięcia celów podmiotu. Procedury, które ustanawia jednostka, by przeciwdziałać ryzyku, zwane są działaniami kontroli wewnętrznej. Działania w ramach systemu kontroli wewnętrznej są reakcją na ryzyko, a planuje się je tak, aby pohamować zidentyfikowaną niepewność co do osiągnięcia wyniku.

Dokumentacja *(Documentation)*

Dokumentacja struktury kontroli wewnętrznej to fizyczny i pisemny materiał dowodowy dotyczący składników procesu tej kontroli, obejmujący identyfikację struktury i polityki jednostki oraz jej kategorie działania, powiązane z tym cele i działania w ramach systemu kontroli. Powinny one występować w takich dokumentach jak wytyczne dla kierownictwa, polityki administracyjne, podręczniki procedur oraz podręczniki księgowania.

Dostęp fizyczny *(Physical Access)*

W kontroli dostępu, uzyskanie dostępu do fizycznych obszarów i jednostek (np. plików, przekazów); (zobacz dostęp logiczny).

Duży system komputerowy *(Mainframe)*

Komputer wysokiego poziomu zaawansowania technicznego przeznaczony do najbardziej intensywnych zadań obliczeniowych. Z komputerowego dużego systemu często korzysta wspólnie wielu użytkowników połączonych z nim za pośrednictwem terminali.

Działania *(Operations)*

Stosowane z takimi pojęciami, jak cele lub mechanizmy kontroli, odnoszą się do skuteczności i wydajności działań podmiotu, włączając w to cele związane z wydajnością i rentownością oraz ochroną zasobów. (COSO 1992)

Funkcje, procesy i działania, przez które realizowane są cele jednostki.

E

Efekt za pieniądze *(Value for Money)*

Zobacz: oszczędność, skuteczność i wydajność.

Etyczny *(Ethical)*

Wiąże się z zasadami moralnymi.

Ewaluacja ryzyka *(Risk evaluation)*

Oznacza oszacowanie znaczenia ryzyka i ocenę prawdopodobieństwa jego wystąpienia.

I

Instytut Audytorów Wewnętrznych *(Institute of Internal Auditors (IIA))*

IIA to organizacja, która określa standardy etyczne i praktyki, kształci i wzmacnia profesjonalizm własnych członków.

Interesariusze, udziałowcy *(Stakeholders)*

Strony podlegające skutkom działania danego podmiotu, takie jak udziałowcy, społeczności, wśród których podmiot działa, pracownicy, klienci i dostawcy. (COSO ERM)

Interwencja zarządu (Management intervention)

Działania kierownictwa zmierzające do uchylenia obowiązujących polityk lub procedur dla uprawnionych celów. Interwencja zarządu jest zwykle niezbędna wobec transakcji lub zdarzeń niepowtarzalnych lub niestandardowych, które przy jej braku byłyby potraktowane przez system niewłaściwie (przeciwieństwo: przekroczenie zarządu). (COSO 1992)

J

Jednostka audytu wewnętrznego *(Internal audit unit)*

Departament (lub działanie) wewnątrz podmiotu, któremu kierownictwo powierzyło sprawdzanie i ocenę systemów i procedur dla zminimalizowania prawdopodobieństwa nadużyć, błędów i mało wydajnych praktyk. Audyt wewnętrzny musi mieć niezależność wewnątrz jednostki i sprawozdawać bezpośrednio kierownictwu. (glossarium)

Departament, wydział, zespół konsultantów lub innych ekspertów świadczący usługi zapewniające i doradcze, działający niezależnie i obiektywnie w celu przysporzenia wartości i usprawnienia działalności operacyjnej organizacji. Audyt wewnętrzny systematycznie, w uporządkowany sposób ocenia procesy zarządzania ryzykiem, kontroli i ładu organizacyjnego, i przyczynia się do poprawy ich działania, tym samym pomagając organizacji osiągnąć cele. (IIA)

K

Kierownictwo *(Management)*

Obejmuje wyższych rangą przedstawicieli jednostki wykonujących najważniejsze funkcje zarządcze. Członkami kierownictwa są dyrektorzy (członkowie zarządu) i członkowie komitetu audytu tylko wtedy, kiedy wykonują najważniejsze funkcje zarządcze. (IFAC)

Komitet audytu *(Audit committee)*

Komitet dyrektorów, którego rola skupia się zazwyczaj na aspektach sprawozdawczości finansowej, procesach podmiotu ukierunkowanych na zarządzanie działalnością i ryzykiem finansowym oraz zgodności z obowiązującymi istotnymi wymogami prawnymi,

etycznymi i regulacyjnymi. Komitet audytu zazwyczaj wspiera zarząd w nadzorowaniu (a) rzetelności sprawozdań finansowych podmiotu, (b) zgodności działań podmiotu z wymogami prawnymi i regulacyjnymi, (c) niezależności i kwalifikacji audytorów, (d) wykonywania funkcji audytu wewnętrznego podmiotu i niezależnych audytorów, (e) wynagradzania kadry kierowniczej (w przypadku braku odrębnego komitetu ds. wynagrodzeń).

Komponent systemu kontroli wewnętrznej *(Component of internal control)*

Jeden z pięciu składników systemu kontroli wewnętrznej. Komponenty systemu kontroli wewnętrznej to środowisko wewnętrzne, ocena ryzyka, działania w ramach systemu kontroli, informacja i komunikowanie oraz monitorowanie. (COSO 1992)

Komputerowe mechanizmy kontroli *(Computer controls)*

1. Mechanizmy kontroli działające w komputerze, np. mechanizmy kontroli zaprogramowane w komputerze (przeciwieństwo manualnych mechanizmów kontroli).

2. Mechanizmy kontroli komputerowego przetwarzania informacji, obejmujące mechanizmy kontroli ogólnego zastosowania i mechanizmy kontroli aplikacji (obydwa zaprogramowane i manualne). (COSO 1992)

Komputerowy system informacyjny *(Computer information system)*

Środowisko komputerowego systemu informacyjnego (KSI) istnieje wtedy, gdy komputer dowolnego rodzaju i wielkości zaangażowany jest w przetwarzanie przez jednostkę informacji (finansowych) mających znaczenie dla audytu, niezależnie od tego, czy komputer ten jest obsługiwany przez dany podmiot, czy przez stronę trzecią. (IFAC)

Kontrola *(Control)*

- 1. W znaczeniu podmiotowym, np. istnienie kontroli – polityka lub procedura będąca częścią kontroli wewnętrznej. Kontrola może istnieć w obrębie każdego z pięciu elementów. 2. Rzeczownik użyty jako dopełnienie, np. wpływać na kontrolę – wynik polityk i procedur stworzonych do kontroli; wynik ten może, ale nie musi być skuteczną kontrolą wewnętrzną; 3. Czasownik, np. kontrolować – regulować: regulować; ustanowić lub stosować politykę oddziałującą na kontrolę. (COSO 1992)
- Każde działanie podejmowane przez kierownictwo, radę lub inne jednostki w celu zarządzania ryzykiem i zwiększenia prawdopodobieństwa zrealizowania ustalonych celów i zadań. Kierownictwo planuje, organizuje i kieruje wykonaniem właściwych

działań, dając racjonalne zapewnienie, że cele i zadania zostaną zrealizowane. (IIA)

Kontrola budżetowa *(Budgetary control)*

Kontrola, przez którą władza przyznająca budżet danemu podmiotowi upewnia się, że budżet ten został wykonany zgodnie z szacunkami, uprawnieniami i przepisami. (glossarium)

Kontrola dostępu *(Access control)*

W informatyce – mechanizmy kontroli zainstalowane w celu ochrony zasobów przed nieuprawnioną modyfikacją, utratą lub ujawnieniem.

Kontrola wewnętrzna *(Internal control)*

Kontrola wewnętrzna jest integralnym procesem, na który wpływ ma zarówno kierownictwo jednostki, jak i pracownicy; zwraca uwagę na ryzyka i dostarcza racjonalnego zapewnienia, że w działalności podmiotu realizującego swoją misję osiągnięte zostaną następujące cele ogólne: wykonywanie zadań w sposób uporządkowany, etyczny, oszczędny, wydajny i skuteczny; wypełnianie zobowiązań w zakresie rozliczalności;, przestrzeganie obowiązującego prawa i regulacji; zabezpieczenia zasobów przed utratą, niewłaściwym wykorzystaniem i zniszczeniem.

Kontrola zapobiegawcza/prewencyjna *(Preventive control)*

Kontrola stworzona w celu uniknięcia niepożądanych zdarzeń lub skutków (przeciwieństwo: kontrola wykrywająca). (COSO 1992)

Kontrola wykrywajaca *(Detective control)*

Kontrola stworzona w celu wykrycia niezamierzonych zdarzeń lub skutków (przeciwieństwo kontroli prewencyjnej). (COSO 1992)

Kontrole edycji *(Edit checks)*

Zaprogramowane mechanizmy kontroli wbudowane we wczesnych etapach, na wejściu procesu dla identyfikacji pól błędnych danych. Na przykład, znaki alfanumeryczne wprowadzone do pól numerycznych mogą zostać odrzucone przez tę kontrolę. Zaprogramo-

wane mechanizmy kontroli edycji mogą zostać zastosowane również wtedy, gdy na przykład dane dotyczące transakcji przesłane z innej aplikacji pojawiają się na wejściu cyklu przetwarzania.

Korupcja *(Corruption)*

- Wszelka forma nieetycznego wykorzystywania władzy publicznej dla korzyści osobistej lub prywatnej. (XVI INCOSAI, Urugwaj, 1998)
- Nadużycie powierzonej władzy dla prywatnego zysku. (Transparency International)

M

Manualne mechanizmy kontroli *(Manual controls)*

Mechanizmy kontroli stosowane ręcznie, bez korzystania z komputera (przeciwieństwo: komputerowe mechanizmy kontroli). (COSO 1992)

Mechanizmy kontroli aplikacji *(Application controls)*

- Struktura, polityki i procedury, które są dostosowane do odrębnych, jednostkowych systemów aplikacyjnych i zaprojektowane tak, aby objąć przetwarzanie danych w ramach określonego oprogramowania aplikacyjnego.
- Procedury wbudowane w oprogramowania komputerowe i związane z nimi procedury manualne stworzone, by zapewnić kompletność i dokładność przetwarzania informacji. Przykładami są sprawdzanie edycji wprowadzonych danych, badanie sekwencji liczbowych i procedury manualne sprawdzające pozycje zawarte w raportach odchyleń. (COSO 1992)

Mechanizmy kontroli ciągłości działania usług *(Service continuity control)*

Ten typ mechanizmów kontroli służy, w razie wystąpienia nieoczekiwanego zdarzenia, do nieprzerwanego zapewnienia kontynuacji lub szybkiego wznowieniu kluczowych operacji, a także ochrony kluczowych i wrażliwych danych.

Mechanizmy kontroli ogólnego zastosowania *(General controls)*

- Mechanizmy kontroli ogólnego zastosowania to struktura, polityki i procedury, które stosuje się do wszystkich lub znacznej części systemów informacyjnych podmiotu

w celu pomocy w zapewnieniu ich właściwego działania. Tworzą one środowisko, w którym działają systemy aplikacji i mechanizmy kontroli.

- Polityki i procedury, które pomagają zapewnić ciągłe i prawidłowe działanie komputerowych systemów informacyjnych. Obejmują one mechanizmy kontroli w zakresie zarządzania systemami informatycznymi, infrastrukturą informatyczną, bezpieczeństwem, oraz pozyskiwania, opracowywania i utrzymania oprogramowania. Mechanizmy kontroli ogólnego zastosowania wspierają funkcjonowanie zaprogramowanych mechanizmów kontroli aplikacji. Innymi określeniami używanymi czasem, by opisać mechanizmy kontroli ogólnego zastosowania są powszechne komputerowe mechanizmy kontroli i informatyczne mechanizmy kontroli. (COSO ERM)

Mechanizmy kontroli oprogramowania systemowego *(System software controls)*

Mechanizmy kontroli zbioru programów komputerowych i powiązanych z nimi procedur zaprojektowane w celu obsługi i sterowania urządzeniami wewnętrznymi komputera.

Międzynarodowa Organizacja Najwyższych Organów Kontroli

(International Organisation of Supreme Audit Institutions INTOSAI)

INTOSAI to profesjonalna organizacja najwyższych organów kontroli (NOK) krajów należących do Organizacji Narodów Zjednoczonych lub jej wyspecjalizowanych agencji. NOK odgrywają główną rolę w kontrolowaniu finansowych rozliczeń i operacji sektora rządowego oraz promowaniu rzetelnej gospodarki finansowej i rozliczalności własnych rządów. INTOSAI został założony w roku 1953 i z 34 krajów założycieli rozrósł się do ponad 170 członków NOK.

Monitorowanie *(Monitoring)*

Monitorowanie jest komponentem kontroli wewnętrznej i procesem, który ocenia jakość działania systemu kontroli wewnętrznej w czasie.

N

Najwyższy Organ Kontroli (NOK) *(Supreme Audit Institution SAI)*

Podmiot publiczny w strukturach państwa, który – bez względu na sposób powołania, ukonstytuowania lub zorganizowania – na mocy prawa wypełnia najwyższą funkcję kontroli sektora publicznego tego państwa. (Standardy kontroli INTOSAI i IFAC)

Niedostatek *(Deficiency)*

Odczuwalne potencjalne lub rzeczywiste braki kontroli wewnętrznej, bądź okazja do wzmocnienia systemu kontroli wewnętrznej zapewniająca większe prawdopodobieństwo, że jednostka osiąga swe cele. (COSO 1992)

Niepewność *(Uncertainty)*

Niemożność poznania z wyprzedzeniem prawdopodobieństwa wystąpienia lub skutku przyszłych zdarzeń. (COSO ERM)

Niezależność *(Independence)*

- Swoboda udzielona podmiotowi audytującemu i jego audytorom w celu działania bez jakichkolwiek zewnętrznych przeszkód zgodnie z udzielonymi uprawnieniami audytorskimi. (glossarium)
- Swoboda NOK w kwestiach dotyczących audytowania w celu działania zgodnie z własnym mandatem audytorskim bez ukierunkowania lub jakichkolwiek zakłóceń z zewnątrz. (Standardy kontroli INTOSAI)
- Wolność od warunków zagrażających obiektywizmowi lub domniemanemu obiektywizmowi. Zarządzanie zagrożeniami obiektywizmu musi odbywać się na poziomie każdego audytora i zadania, jak również na poziomie funkcjonalnym i organizacyjnym. (IIA)
- Zdolność audytora do utrzymania bezstronności w wykonywaniu usług zawodowych (niezależność faktyczna). (Arens, Elder & Beasley)
- Zdolność audytora do utrzymania bezstronności w oczach innych osób (wrażenie niezależności). (Arens, Elder i Beasley)

O

Obiektywizm *(Objectivity)*

Bezstronne nastawienie umożliwiające NOK, audytorom wewnętrznym i zewnętrznym wykonywanie zleceń w sposób pozwalający im mieć szczere zaufanie do wyników własnej pracy, bez wątpliwości, że doszło do istotnego naruszenia jakości tej pracy. Obiektywizm wymaga, aby audytorzy nie podporządkowywali swojego osądu spraw audytowanych osądowi innych osób.

Ocena ryzyka *(Risk assessment)*

Ocena ryzyka to proces identyfikacji i analizy istotnych rodzajów ryzyka na drodze do osiągnięcia celów przez podmiot wraz z wyborem stosownych sposobów reakcji.

Odwzorowanie przepływów, sporządzanie wykresów przepływów/chronologicznych *(Flow-charting)*

Ilustruje ciąg procedur, informacji lub dokumentów. Technika ta umożliwia przedstawienie w opisowej formie podsumowania złożonych dróg obiegu lub procedur. (glossarium)

Ograniczenia nieodłączne *(Inherent limitations)*

Ograniczenia wszystkich systemów kontroli wewnętrznej odnoszące się do granic ludzkiego osądu, ograniczeń zasobów i konieczności rozważenia kosztu kontroli w stosunku do oczekiwanych korzyści, realności wystąpienia awarii oraz możliwości przekroczeń zarządu i zmowy. (COSO 1992).

Oprogramowanie systemowe *(System software)*

Oprogramowanie przeznaczone głównie do koordynowania i kontrolowania zasobów sprzętowych i komunikacyjnych, dostępu do plików i zapisów, kontroli i porządku stosowania aplikacji.

Organ audytu *(Audit institution)*

Podmiot publiczny, który, bez względu na sposób jego powołania, składu i organizacji, wypełnia zgodnie z prawem obowiązki z zakresu audytu zewnętrznego. (glossarium)

Oszczędność *(Economy)*

- Ograniczenie do minimum kosztów zasobów wykorzystanych w celu realizacji działań z uwzględnieniem właściwej jakości. (Standardy kontroli INTOSAI)
- Pozyskanie we właściwym czasie i najniższym kosztem zasobów finansowych, ludzkich i rzeczowych, które są odpowiednie zarówno pod względem jakości, jak i ilości. (glossarium)

Oszczędny *(Economical)*

Wolny od marnotrawstwa lub przesady. Oznacza uzyskanie właściwej ilości zasobów o prawidłowej jakości dostarczonych we właściwym czasie, na właściwe miejsce i najniższym kosztem.

Oszustwo *(Fraud)*

Sprzeczna z prawem interakcja dwóch podmiotów, gdzie jedna ze stron świadomie zwodzi drugą metodami fałszywego przedstawiania faktów, aby zdobyć nielegalną, nieuprawnioną korzyść. Obejmuje akty zwodzenia, podstępu, skrywania lub nadużycia zaufania, które stosuje się w celu uzyskania nierzetelnej lub nieuczciwie zdobytej korzyści. (XVI INCOSAI, Urugwaj, 1998)

P

Podmiot *(Entity)*

Jednostka dowolnych rozmiarów, stworzona do określonego celu. Podmiotem może być na przykład przedsiębiorstwo, firma przemysłowa, organizacja niekomercyjna, organ rządowy lub placówka naukowa. Inne określenia stosowane jako synonimy obejmują jednostkę i departament. (COSO 1992)

Profil ryzyka *(Risk profile)*

Przegląd lub matryca (macierz) obejmująca podstawowe rodzaje ryzyk, jakim podmiot lub jego jednostka mają sprostać, z uwzględnieniem poziomu skutków (np. wysoki, średni, niski) oraz prawdopodobieństwa lub możliwości wystąpienia określonego zdarzenia.

Polityka *(Policy)*

Nakaz zarządu dotyczący tego, co musi być zrobione, by wpłynąć na kontrolę. Polityka służy jako podstawa dla procedur, które ją implementują. (COSO 1992)

Procedura *(Procedure)*

Działanie wdrażające politykę. (COSO 1992)

Proces zarządzania *(Management process)*

Szereg działań podejmowanych przez zarząd przy prowadzeniu przedsiębiorstwa. System kontroli wewnętrznej jest częścią procesu zarządzania i jest z nim zintegrowany. (COSO 1992)

Program bezpieczeństwa *(Security program)*

Obejmujący całą jednostkę program planowania zabezpieczeń i zarządzania nimi, stanowiący fundament struktury kontroli bezpieczeństwa danej jednostki i odzwierciedlenie stopnia zaangażowania wyższego kierownictwa w zapobieganie zagrożeniom bezpieczeństwa. Program powinien ustanowić ramy i ciągły cykl działań w celu oceny ryzyka, opracowywania i wdrażania skutecznych procedur bezpieczeństwa oraz monitorowania skuteczności tych procedur.

Przekroczenie zarządu *(Management override)*

Uchylenie przez kierownictwo obowiązujących polityk lub procedur dla nieuprawnionych celów z zamiarem osiągnięcia korzyści osobistych wyolbrzymienia sytuacji finansowej albo jej statusu zgodności z przepisami jako lepsze od rzeczywistych (przeciwieństwo: interwencja zarządu). (COSO 1992)

Przetwarzanie *(Processing)*

W informatyce wykonywanie instrukcji programu przez jednostkę centralną komputera.

Przetwarzanie danych przez użytkownika końcowego *(End user computing)*

Odnosi się do wykorzystania niescentralizowanego (tzn. prowadzonego poza departamentem informatyki) przetwarzania danych z wykorzystaniem skomputeryzowanych narzędzi opracowanych przez końcowych użytkowników, zazwyczaj za pomocą pakietów oprogramowania (np. arkuszy kalkulacyjnych i baz danych). Procesy wykonywane przez użytkowników końcowych mogą być złożone i stać się niezmiernie ważnym źródłem informacji zarządczej. Wątpliwość może budzić to, czy zostały odpowiednio przetestowane i udokumentowane.

R

Racjonalne zapewnienie *(Reasonable assurance)*

- Równa się zadowalającemu poziomowi pewności przy uwzględnieniu istniejących kosztów, korzyści i ryzyk.
- Koncepcja stanowiąca, że kontrola wewnętrzna, bez względu na to, jak dobrze jest zaprojektowana, nie może zagwarantować, że cele podmiotu będą zrealizowane. Dzieje się tak ze względu na nieodłączne ograniczenia wszystkich systemów kontroli wewnętrznej. (COSO 1992)

Rozdzielenie (lub wydzielenie) obowiązków *(Segragation (or separation) of duties)*

Aby ograniczyć ryzyko błędu, marnotrawstwa lub działań niedozwolonych oraz ryzyko niewykrycia podobnych problemów, żadna pojedyncza osoba ani pojedynczy zespół nie powinny kontrolować wszystkich kluczowych etapów (uprawnianie, przetwarzanie, zapisywanie, rewizja) transakcji lub zdarzenia.

Rozliczalność *(Accountability)*

- Proces, w wyniku realizacji którego jednostki służb publicznych i osoby działające w ich ramach zostają uznane za odpowiedzialne za podjęte decyzje i działania z uwzględnieniem obsługi funduszy publicznych oraz wszystkich aspektów wykonania przez nie zadań.
- Spoczywający na kontrolowanych osobie lub podmiocie obowiązek wykazania, że powierzone jej lub jemu fundusze były zarządzane lub kontrolowane zgodnie z warunkami, na jakich zostały udostępnione. (glossarium)

Rozliczalność publiczna *(Public accountability)*

Zobowiązania osób lub podmiotów, w tym przedsiębiorstw i korporacji publicznych, którym powierzono zasoby publiczne do odpowiedzialności z tytułu obowiązków o charakterze fiskalnym, zarządczym i programowym, jakie zostały na nie nałożone. (Standardy kontroli INTOSAI)

Ryzyko, zagrożenie *(Risk)*

Możliwość, że jakieś zdarzenie nastąpi i spowoduje skutki niekorzystne dla realizacji celów. (COSO ERM)

Ryzyko nieodłączne *(Inherent risk)*

Ryzyko, które ponosi podmiot w przypadku braku wszelkich działań, jakie kierownictwo mogłoby podjąć, aby zmienić prawdopodobieństwo wystąpienia ryzyka lub jego skutków. (COSO ERM)

Ryzyko pozostałe *(Residual risk)*

Ryzyko, które pozostaje po reakcji kierownictwa na jego wystąpienie.

S

Sektor publiczny *(Public sektor)*

Termin „sektor publiczny" odnosi się do rządów krajowych, rządów regionalnych (np. stanowych, prowincji, terytoriów), rządów lokalnych (na przykład miasta, wsi) i powiązanych z nimi podmiotów rządowych (np. agencje, rady, komisje i przedsiębiorstwa). (IFAC)

Sieć *(Network)*

W informatyce jest to grupa komputerów wraz z urządzeniami powiązanymi połączona ze sobą poprzez urządzenia komunikacyjne. Sieć może obejmować połączenia stałe, takie jak przewody, lub połączenia tymczasowe, np. poprzez łącza telefoniczne lub inne łącza komunikacyjne. Sieć może mieć charakter lokalny, jeżeli obejmuje niewielką liczbę komputerów, drukarek i innych urządzeń albo składać się ze znacznej liczby różnej wielkości komputerów rozmieszczonych na dużym obszarze geograficznym.

Skuteczność *(Effectiveness)*

- Zakres, w jakim osiąga się cele i związek pomiędzy zamierzonym a faktycznym skutkiem danego działania. (Standardy kontroli INTOSAI)
- Stopień, w jakim przyjęte cele zrealizowano w sposób opłacalny. (glossarium)

Skuteczny *(Effective)*

Odnosi się do osiągania celów lub zakresu, w jakim wyniki danego działania są zgodne z przyjętym celem lub jego zamierzonymi skutkami.

Status dostępu (Logical Access)

Przydzielenie (status) dostępu do danych komputerowych. Dostęp może być ograniczony „wyłącznie do odczytu"; lecz w szerszym rozumieniu prawa dostępu obejmują możliwość modyfikacji danych, albo też pełną możliwość zmiany – tworzenia i kasowania danych (zobacz również: dostęp fizyczny).

System kontroli wewnętrznej (lub proces, lub architektura) ***Internal Control System (or Process, or Architecture)***

Synonim kontroli wewnętrznej wdrożonej w konkretnym podmiocie. (COSO 1992)

Ś

Środowisko wewnętrzne ***(Control environment)***

Środowisko wewnętrzne nadaje ton jednostce, wywierając wpływ na świadomość kontrolną jej kadry. Stanowi ono fundament pozostałych komponentów kontroli wewnętrznej, ustanawiając dyscyplinę i strukturę.

T

Tolerancja ryzyka ***(Risk tolerance)***

Możliwe do przyjęcia odchylenie wyników od założonych celów. (COSO ERM)

U

Uczciwość ***(Integrity)***

Jakość lub stan stosowania się do zdrowych zasad moralnych; prawość, szczerość, potrzeba dobrego postępowania, wyrażanie i postępowanie zgodnie z zespołem wartości i oczekiwań. (COSO 1992)

Uporządkowany ***(Ordery)***

Oznacza działanie w sposób dobrze zorganizowany lub metodycznie.

Ustawodawca / władza ustawodawcza ***(Legislature)***

Władza stanowiąca prawo w danym kraju, np. parlament. (Standardy kontroli INTOSAI)

W

Wartości etyczne *(Ethical values)*

Wartości moralne, które umożliwiają osobie podejmującej decyzję ustalenie właściwego sposobu zachowania. Wartości te powinny bazować na tym, co jest „prawidłowe", co może wykraczać poza, iść ponad to, co jest „legalne". (COSO 1992)

Wkład / dane wejściowe *(Input)*

Wszelkie dane wprowadzone do komputera lub proces ich wprowadzania do komputera.

Wydajność *(Efficiency)*

- Związek między wynikami w kategoriach dóbr, usług lub innych osiągniętych wyników a zasobami wykorzystanymi do ich uzyskania. (Standardy kontroli INTOSAI)
- Wykorzystanie zasobów finansowych, ludzkich i materialnych w taki sposób, aby zmaksymalizować wynik dla danej ilości zasobów, albo zminimalizować wkład dla uzyskania danej ilości lub jakości wyników. (glossarium)

Wydajny *(Efficient)*

Dotyczy związku pomiędzy zasobami wykorzystanymi a wynikami osiągniętymi na drodze do realizacji celów długofalowych. Oznacza wykorzystanie minimalnych zasobów jako wkładu w osiągnięcie wyników w danej ilości i o danej jakości, lub maksymalnego wyniku z wykorzystaniem wkładu w danej ilości i o danej jakości.

Wynik, produkt na wyjściu, wydajność *(Output)*

W informatyce, dane lub informacje uzyskane w wyniku przetwarzania komputerowego, np. obraz na monitorze lub wydruk.

Z

Zamiar / Plan *(Design)*

1. Zamiar: zgodnie z definicją kontroli wewnętrznej ustanawia się z zamiarem uzyskania racjonalnego zapewnienia dotyczącego osiągnięcia założonych celów; gdy zamiar zostaje zrealizowany, system można uznać za skuteczny. 2. Plan: sposób, w jaki system ma działać, w odróżnieniu od tego, jak aktualnie działa. (COSO 1992)

Zgodność *(Compliance)*

- Przestrzeganie ustaw i rozporządzeń dotyczących danej jednostki. (COSO 1992)
- Wierność przyjętym zasadom i spójność z polityką, planami, procedurami, przepisami prawa, regulacjami, umowami lub innymi wymaganiami. (IIA)

Zmowa *(Collusion)*

Współdziałanie podjęte przez pracowników w celu dokonania oszustwa dotyczącego gotówki, towaru lub innych zasobów. (Arens, Elder i Beasley)

Spis treści

Przekład i opracowanie:
Najwyższa Izba Kontroli

NAJWYŻSZA IZBA KONTROLI
www.nik.gov.pl
ISBN 978 -83-92-9290-5-5