Powiązania norm ISO z Krajowymi Ramami Interoperacyjności i kontrolą zarządczą

Punkt widzenia audytora i kierownika jednostki

Agnieszka Boboli
Ministerstwo Finansów 22.05.2013 r.

Agenda

- **Rola kierownika jednostki.**
- **Cele kontroli zarządczej.**
- **Sposób funkcjonowania kontroli zarządczej.**
- **Rola audytora wewnętrznego.**
- **Wybrane aspekty bezpieczeństwa informacji.**
- **Audyt bezpieczeństwa informacji.**

Rola kierownika jednostki

- Kierownik jednostki sektora finansów publicznych, jest odpowiedzialny za całość gospodarki finansowej tej jednostki, co określa artykuł 53 ustawy o finansach publicznych.

- Pod pojęciem gospodarki finansowej rozumie się także całokształt działań podejmowanych w jednostce sektora finansów publicznych (pobieranie należności, dokonywanie wydatków, zaciąganie zobowiązań, wykonywanie obowiązków w zakresie rachunkowości i sprawozdawczości budżetowej, udzielanie zamówień publicznych, organizowanie i kierowanie pracą jednostki.

Cele kontroli zarządczej

- Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.
- Kontrola zarządcza obejmuje formułowanie celów i zdań jednostki, a następnie sprawdzanie ich realizacji.

Cele kontroli zarządczej

Zadaniem kontroli zarządczej wskazanym w ustawie o finansach publicznych (art. 68 ust.2) jest zapewnianie:

- **zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi,**
- **skuteczności i efektywności,**
- **wiarygodności sprawozdań,**
- **ochrony zasobów,**
- **przestrzegania i promowania zasad etycznego postępowania,**
- **efektywności i skuteczności przepływu informacji,**
- **zarządzania ryzykiem.**

Sposób funkcjonowania kontroli zarządczej

Każda jednostka sektora finansów publicznych powinna posiadać sprawny, prosty i zarazem efektywny system kontroli zarządczej. Obowiązek ten wynika z powszechnie przyjętych standardów kontroli w systemie finansów publicznych. System kontroli zarządczej w każdej z jednostek sektora finansów publicznych będzie unikatowy, bowiem każda z grup jednostek sektora finansów publicznych realizuje odmienne rodzaje zadań, wyznaczane najczęściej przez normy prawne.

W związku z tym, że działalność każdej z jednostek sektora finansów publicznych będzie miała charakterystyczny (indywidualny) układ procesów związanych z realizacją jej celów, każda z tych jednostek będzie charakteryzowała się swoistym system kontroli zarządczej.

Sposób funkcjonowania kontroli zarządczej

Ustawa nakłada na kierowników jednostek sektora finansów publicznych - ogólnie określony – obowiązek zapewnienia funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej (art. 69), przy czym ustawodawca nie wskazuje odgórnie form i sposobów jej zorganizowania.

Przepisy dają daleko idącą autonomię w korzystaniu z różnych środków zapewniania właściwej kontroli zarządczej.

Sposób funkcjonowania kontroli zarządczej

Narzędziem pomocniczym dla kierownika jednostki sektora finansów publicznych są – wydane przez Ministra Finansów – standardy kontroli zarządczej dla jednostek sektora finansów publicznych.

Odpowiedzialność za funkcjonowanie kontroli zarządczej

Ustawa (art. 69 ust. 1) wskazuje podmioty odpowiedzialne za zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej, są to:

- **minister w kierowanych przez niego działach administracji rządowej;**
- **wójt, burmistrz, prezydent miasta, przewodniczący zarządu jednostki samorządu terytorialnego;**
- **kierownik jednostki.**

Sposób funkcjonowania kontroli zarządczej

- **Efektywne funkcjonowanie kontroli zarządczej wymaga aktywnego działania ze strony kierownika jednostki i wszystkich osób na stanowiskach kierowniczych, które mają udział w zarządzaniu jednostką.**
- **Kontrola zarządcza nie może zostać przypisana lub ograniczona do jednej jednostki, jako grupa jej wyłącznych obowiązków.**
- **Istotną rolę w systemie kontroli zarządczej odgrywa audyt wewnętrzny. Ocena systemu kontroli zarządczej, a także czynności doradcze wykonywane przez audyt wewnętrzny mają wspierać kierownika jednostki w realizacji celów i zadań jednostki.**

Rola audytora wewnętrznego

- Audytor wewnętrzny powinien stanowić dla kierownika jednostki źródło obiektywnej i profesjonalnej oceny systemu kontroli zarządczej.
- Poprzez przeprowadzanie zadań audytowych i czynności doradczych audytor wskazuje słabości w funkcjonowaniu jednostki (jeżeli takie występują) oraz proponuje usprawnienia
- Słabości nie zawsze należy rozumieć jako nieprawidłowości czy stan niezgodności z prawem – mogą to być również obszary, w których działalność może być prowadzona efektywniej czy skuteczniej.

Rola audytora wewnętrznego

- Audytor nie może przejmować odpowiedzialności za zarządzanie w jednostce , bowiem to rola i zadanie kierownika jednostki.
- Decyzje co do tego, czy należy wdrażać wydane przez audytora rekomendacje zawsze winien podjąć kierownik komórki organizacyjnej lub jednostki).
- Audytor nie ponosi odpowiedzialności za wdrożenie wydanych rekomendacji.

Współpraca kierownika jednostki z audytorem wewnętrznym

- Kierownik jednostki odpowiada za stworzenie takich warunków, w których audytor wewnętrzny wie i rozumie, jakie są priorytety jednostki oraz ma dostęp do wszystkich istotnych z punktu widzenia prowadzonej działalności informacji.
- Niezmiernie ważny jest bezpośredni kontakt audytora z kierownikiem jednostki, regularna i szczera komunikacja, a także wzajemne zaufanie.

ISO 22301:2012

- **Przywództwo – odpowiednie osoby z kierownictwa wyższego szczebla powinny wykazać swoje zaangażowanie w SZCD.**
- **Zaangażowanie kierownictwa – ustanowienie polityk i celów zgodnych ze strategicznymi kierunkami organizacji, integracja z procesami biznesowymi, dostępność zasobów, komunikowanie istotności, zapewnianie osiągania celów systemu, nadzorowanie i wspieranie, promowanie doskonalenia, wspieranie działania pozostałych osób).**

ISO 22301:2012 Przywództwo

- Zadania, odpowiedzialność i uprawnienia w organizacji.
- Polityka – odpowiednia do celów organizacji, wprowadza ramowe zasady dla osiągania celów ciągłości działania, obejmuje zaangażowanie w stosowanie wymogów i ciągłe doskonalenie, udokumentowana, dostępna, zakomunikowana, przeglądana).

Administrator danych osobowych

- **Organ, jednostkę organizacyjną, podmiot lub osobę decydujące (samodzielnie) o celach i środkach przetwarzania danych osobowych(art. 7 pkt 4 uodo). Jest to podmiot praw i obowiązków, który sprawuje władztwo nad przetwarzaniem danych osobowych przez zaciąganie zobowiązań i rozporządzanie prawami.**

Obowiązki administratora danych osobowych

- **Zabezpieczenie przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym oraz zabraniem przez osobę nieuprawnioną.**
- **Przetwarzanie danych zgodnie z wymogami ustawy.**
- **Chronienia danych przed zmianą, utratą, uszkodzeniem lub zniszczeniem.**

Zadania administratora danych osobowych

- **Opracowanie dokumentacji.**
- **Monitorowanie czynności wykonywanych na zbiorze danych.**
- **Zapewnienie technicznych środków bezpieczeństwa.**
- **Obowiązek opracowania Polityki Bezpieczeństwa Danych Osobowych.**
- **Obowiązek opracowania Instrukcji Zarządzania Systemem Informatycznym.**

Administrator bezpieczeństwa informacji

- **Wyznaczenie Administratora Bezpieczeństwa Informacji (ABI) jest jednym z obowiązków administratora danych, wynikającym z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, służącym właściwemu zabezpieczeniu danych. Administrator danych powinien dołożyć szczególnej staranności, aby wybrana osoba dawała rękojmię prawidłowego wykonywania obowiązków w zakresie nadzoru nad przestrzeganiem zasad zabezpieczenia danych osobowych.**

Audyt bezpieczeństwa informacji oparty na wytycznych normy ISO 27001

- Polityka bezpieczeństwa.
- Organizacja bezpieczeństwa informacji.
- Zarządzanie aktywami.
- Bezpieczeństwo zasobów ludzkich.
- Bezpieczeństwo fizyczne i środowiskowe.
- Zarządzanie systemami i sieciami.
- Kontrola dostępu.
- Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
- Zarządzanie ciągłością działania.

Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

- § 20 ust. 2 pkt 14 obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
- Ustawodawca nie określił sposobu, trybu, rodzaju audytu, ani też osób czy komórek organizacyjnych, którym należałoby powierzyć prowadzenie ww. audytu.
- **Decyzja dotycząca powierzenia prowadzenia audytu bezpieczeństwa informacji spoczywa na kierownictwie podmiotu**.

Realizacja obowiązku zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji

- System zarządzania bezpieczeństwem informacji opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001- wymagania określone w § 20 ust. 1 i 2 *rozporządzenia* uznaje się za spełnione.
- Pozostałe przypadki – decyzja kierownika jednostki.

Kryteria wyboru komórki organizacyjnej odpowiedzialnej za audyt bezpieczeństwa informacji

- **Kwalifikacje.**
- **Doświadczenie.**
- **Znajomość metodyk audytu w zakresie bezpieczeństwa informacji.**
- **Niezależność.**

Prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu wewnętrznego

- Formalne przypisanie zadania (uzupełnienie karty audytu oraz innych dokumentów wewnętrznych określających cel, zakres i uprawnienia audytu wewnętrznego w jednostce, o zapisy jednoznacznie wskazujące komórkę audytu jako odpowiedzialną za realizację tego zadania).
- Zadanie zapewniające – umieszczenie zadania w planie audytu, przygotowanie programu zadania audytowego, sprawozdanie.

Dziękuję za uwagę

Agnieszka Boboli

agnieszka.boboli@mac.gov.pl
Tel. 602767604