AUDYT I ZARZĄDZANIE

MAGAZYN IIA

Magazyn Instytutu Audytorów Wewnętrznych IIA Polska, Kwartalnik numer 4(15)2016

ISSN 2450-9582

Instytut Audytorów Wewnętrznych IIA Polska

Wydawca:
Instytut Audytorów Wewnętrznych IIA Polska
ul. Świętokrzyska 20 pokój 520, Warszawa 00-002
Kontakt:
Instytut Audytorów Wewnętrznych IIA Polska
ul. Świętokrzyska 20 pokój 520, Warszawa 00-002
telefon: +48 (22) 110 08 13, +48 602 455 322
mail: office@iia.org.pl,
fax: +48 (22) 247 83 78
Skład i łamanie:
MARCIN BOGUŚ

ISSN 2450-9582

SPIS TREŚCI:

Szanowne Panie, Szanowni Panowie,

Przedstawiamy kolejny numer magazynu IIA Polska „Audyt i Zarządzanie" o numerze ISSN 2450-9582. Znajdziecie w nim Państwo niezwykle ciekawe i inspirujące artykuły oraz informacje, które mamy nadzieję, będą dla Państwa przyczynkiem do dyskusji, refleksji, działania, sięgania po prezentowane rozwiązania, doświadczenia, jak również polecane przez Redakcję publikacje z zakresu audytu wewnętrznego, kontroli wewnętrznej, ryzyka zarządzania itp.

W imieniu swoim i Kolegium serdecznie zapraszam do wymiany doświadczeń i współpracy poprzez tworzenie artykułów, felietonów, recenzji książek godnych polecenia, sprawozdań z konferencji.

Redakcja Magazynu czeka na artykuły, które będą źródłem ciekawych informacji, refleksji, tematem do dyskusji, a przede wszystkim inspirującą lekturą dla każdego naszego czytelnika. Więcej informacji znajduje się na stronie Instytutu Audytorów Wewnętrznych IIA Polska.

Iwona Bogucka

Dr Katarzyna Olejko*

Obowiązek monitorowania skuteczności funkcji audytu wewnętrznego w świetle nowelizacji przepisów dotyczących badań rocznych sprawozdań finansowych

Słowo kluczowe: komitet audytu, funkcja audytu wewnętrznego, monitoring skuteczności audytu, transpozycja przepisów unijnych.

Wprowadzenie

Zgodnie z zasadami *Dobrych praktyk spółek notowanych na GPW – 2016* (zasada szczegółowa III.Z.5), w przypadku, gdy w spółce działa komitet audytu, monitoruje on skuteczność systemów: kontroli wewnętrznej, zarządzania ryzykiem, compliance oraz funkcji audytu wewnętrznego. Obowiązek monitorowania funkcji audytu w jednostkach zainteresowania publicznego [dalej: JZP] usankcjonowano także ustawą z dnia 9 maja 2009 r. *o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym* (Dz. U. z 2015 r. poz. 1011 i 1844) [dalej: Ustawa o biegłych rewidentach i ich samorządzie]. Obecnie procedowana jest ustawa zmieniająca wyżej wskazaną regulację. W zakresie wprowadzanych zmian znalazły się przepisy dotyczące działalności komitetu audytu. Przyjmowane - nowe rozwiązania, z jednej strony prowadzą do wzrostu niezależności i zwiększenia rangi komitetu, z drugiej zaś, m.in. poprzez wyraźne wyartykułowanie dodatkowych obowiązków, akcentują odpowiedzialność członków komitetu za właściwą realizację powierzonych im zadań.

Celem niniejszego opracowania jest zaprezentowanie podstawowych problemów dotyczących zmian ustawowych w zakresie obowiązków komitetu audytu, w szczególności tych związanych z funkcją audytu wewnętrznego, na tle zmian regulacji wspólnotowych.

Przyczyny i kierunki zmian w obszarze podstawowych obowiązków komitetów ds. audytu

W związku z obowiązkiem transpozycji do prawa krajowego postanowień nowych przepisów prawa UE z zakresu audytu, obejmujących Dyrektywę Parlamentu Europejskiego i Rady 2014/56/UE z dnia 16 kwietnia 2014 zmieniającą dyrektywę 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. *w sprawie ustawowych*

* Dr Katarzyna Olejko – audytor wewnętrzny w spółce notowanej na GPW. Starszy wykładowca na Wydziale Biznesu, Finansów i Administracji Uniwersytetu Ekonomicznego w Katowicach. Jako nauczyciel akademicki zajmuje się problematyką związaną z rachunkowością finansową oraz zarządczą. Autorka szeregu publikacji naukowych i branżowych. Członek IIA.

badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych [dalej: Dyrektywa 2006/43/WE] oraz Rozporządzenie Parlamentu Europejskiego i Rady Nr 537/2014 z dnia 16 kwietnia 2014 r. *w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publiczneg*o, wszczęto proces przygotowania zmian zapisów obowiązującej ustawy o biegłych rewidentach i ich samorządzie.

Głównym celem nowelizacji wyżej wymienionych przepisów wspólnotowych oraz zmiany regulacji krajowych było i wciąż pozostaje:

1. Wzmocnienie niezależności i obiektywizmu rewidentów oraz firm audytorskich;
2. Poprawa jakości badań ustawowych uzyskana m.in. w wyniku:
   1) poprawy jakości raportowania z badania na rzecz różnych odbiorców;
   2) wzmocnienia dialogu pomiędzy audytorami a organami nadzorującymi;
   3) kontrolę jakości wykonanego zlecenia badania JZP przed wydaniem ostatecznego sprawozdania z badania;
   4) uszczegółowienie zasad organizacji firm audytorskich;
   5) wzmocnienie roli i zadań komitetu audytu;
3. Wzmocnienie nadzoru publicznego poprzez zapewnienie jego niezależności od środowiska biegłych rewidentów.

Istotne znaczenie przypisano tutaj doprecyzowaniu zasad tworzenia oraz działania komitetów audytu, między innymi poprzez:

1. Ustanowienie katalogu JZP, które mają obowiązek posiadania komitetu audytu wraz ze wskazaniem tych, które są zwolnione z tego obowiązki;
2. Utrzymanie możliwości pełnienia funkcji komitetu audytu przez radę nadzorczą we wskazanych jednostkach;
3. Umożliwienie warunkowego zwolnienia z posiadania KA funduszom inwestycyjnym i funduszom emerytalnym;
4. Określenie obowiązku posiadania kompetencji niezbędnych dla KA jako całości, odnosząc się do branży, w której działa JZP;
5. Wskazanie obowiązku zachowania niezależności większości członków KA od badanego podmiotu, zgodnie z odpowiednimi kryteriami niezależności;
6. Zachowanie wymogu, aby przynajmniej jeden z członków KA posiadał kwalifikacje w zakresie rachunkowości lub badania sprawozdań finansowych;
7. Wprowadzenie wymogu posiadania przez JZP polityki w zakresie wyboru firmy audytorskiej oraz obowiązku opracowania jej przez KA.

Ze względu na szeroki zakres zmian, które należy wprowadzić do obowiązującej regulacji krajowej, aby zrealizować wszystkie wyżej wskazane cele, zdecydowano się na opracowanie nowej ustawy.

Obowiązki komitet ds. audytu w regulacjach unijnych

Realizując wyżej przedstawione założenia, zgodnie z pierwotną wersją Dyrektywy 2006/43/WE, komitet ds. audytu zobowiązano miedzy innymi do[1]:

1. Monitorowania:
   1) procesu sprawozdawczości finansowej;
   2) skuteczności systemów kontroli wewnętrznej, audytu wewnętrznego „w stosownych przypadkach", a także zarządzania ryzykiem;
   3) ustawowego badania rocznych i skonsolidowanych sprawozdań finansowych;
2. Dokonywania przeglądu i monitorowania niezależność biegłego rewidenta lub firmy audytorskiej, a w szczególności świadczenia dodatkowych usług na rzecz badanej jednostki.

Po znowelizowaniu przepisów wspólnotowych w 2014 roku, w ujednoliconym tekście Dyrektywy 2006/43/WE uwzględniającym zmiany wprowadzone m.in. Dyrektywą 2014/56/EU, rozszerzono zakres działania komitetu. Komitet ds. audytu zobowiązany został miedzy innymi do[2]:

1. Informowania odpowiednich organów: administracyjnych lub nadzorczych badanej jednostki o wynikach ustawowego badania;
2. Wyjaśniania, w jaki sposób badanie to wpłynęło na rzetelność sprawozdawczości finansowej, a także, jaka była rola komitetu ds. audytu w tym procesie;
3. Monitorowania procesu sprawozdawczości finansowej;
4. Wydawania zaleceń lub propozycji, pozwalających na zapewnienie rzetelności sprawozdania finansowego;
5. Monitorowania skuteczność wykorzystywanych w przedsiębiorców systemów wewnętrznej kontroli, jakości i systemów zarządzania ryzykiem oraz, **w stosownych przypadkach, jego audytu wewnętrznego w zakresie sprawozdawczości finansowej badanej jednostki, bez naruszania jego niezależności;**
6. Monitorowania procesu badania ustawowego rocznych i skonsolidowanych sprawozdań finansowych;
7. Kontroli oraz monitorowania niezależności biegłych rewidentów czy firm audytorskich, ze szczególnym uwzględnieniem zasadności świadczenia na rzecz badanej jednostki usług nie będących badaniem sprawozdań finansowych;
8. Opracowania oraz nadzorowania realizacji procedury wyboru biegłego rewidenta lub firm audytorskich i przedstawienia zaleceń dotyczących powołania biegłego rewidenta lub firmy audytorskiej.

1 Dyrektywy 2006/43/WE Rozdział X Przepisy szczególne dotyczące badania ustawowego jednostek interesu publicznego, regulującym zakres działania Komitetów Audytu art. 41 Komitet ds. audytu ust. 2.

2 Ujednolicony tekst Dyrektywy 2006/43/WE Rozdział X Przepisy szczególne dotyczące badania ustawowego jednostek interesu publicznego, regulującym zakres działania Komitetów Audytu art. 39 Komitet ds. audytu ust. 6.

Zgodnie z Dyrektywą, wszystkie wyżej wymienione zadania komitet ds. audytu musi realizować bez uszczerbku dla odpowiedzialności członków organów administracyjnych, zarządzających lub nadzorczych, bądź innych członków powołanych przez walne zgromadzenie wspólników badanej jednostki.

Wraz z wprowadzenie powyższej regulacji, powierzony komitetowi obowiązek monitorowania funkcji audytu ograniczono do „stosownych przypadków" dotyczących obszarów sprawozdawczości finansowej. Jednocześnie podkreślono wyraźnie potrzebę uwzględnienia w działaniach nadzorczych obowiązku zachowania niezależności audytu wewnętrznego.

Obowiązki komitetu ds. audytu – regulacje krajowe

W wyniku transpozycji do prawa krajowego Dyrektywy 2006/43/WE, w Ustawie o biegłych rewidentach i ich samorządzie, do zadań KA zaliczono, w szczególności:

1. „Monitorowanie procesu sprawozdawczości finansowej;
2. Monitorowanie skuteczności systemów kontroli wewnętrznej, audytu wewnętrznego oraz zarządzania ryzykiem;
3. Monitorowanie wykonywania czynności rewizji finansowej;
4. Monitorowanie niezależności biegłego rewidenta i podmiotu uprawnionego do badania sprawozdań finansowych, w tym w przypadku świadczenia usług, o których mowa w art. 48 ust. 2"[1].

W trakcie obecnie trwającego procesu legislacyjnego, w przygotowanym projekcie ustawy z dnia 11.04.2016 r. zmieniającej Ustawę o biegłych rewidentach i ich samorządzie, rozszerzono katalog obowiązków komitetu audytu. Znalazły się w nim:

„monitorowanie:

- procesu sprawozdawczości finansowej;
- skuteczności systemów kontroli wewnętrznej, **audytu wewnętrznego** oraz zarządzania ryzykiem;
- wykonywania czynności rewizji finansowej, w szczególności monitorowania wykonania przez podmiot uprawniony do badania sprawozdania finansowego lub skonsolidowanego sprawozdania finansowego, z uwzględnieniem wszelkich
- wniosków i ustaleń Komisji Nadzoru Audytowego wynikających z kontroli
- przeprowadzonej w podmiocie uprawnionym"[2].

1 Ustawa z dnia 9 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym (Dz. U. z 2015 r. poz. 1011 i 1844)- Rozdział 8 Czynności rewizji finansowej w jednostkach zainteresowania publicznego art. 86 ust. 7.

2 www.legislacja.rcl.gov.pl/projekt/12284259, Projekt ustawy o biegłych rewidentach i ich samorządzie z dnia 11.04.2016r. - Rozdział 12 Czynności rewizji finansowej w jednostkach zainteresowania publicznego: art. 128 ust.10.

Do pozostałych obowiązków komitetu zaliczono:

1. „Kontrolowanie i monitorowanie niezależności biegłego rewidenta i podmiotu uprawnionego do badania sprawozdań finansowych, w tym w szczególności w sytuacji, gdy na rzecz JZP świadczone są przez podmiot uprawniony do badania sprawozdań finansowych inne usługi niż badanie sprawozdań finansowych;
2. Informowanie organu nadzorczego JZP o wynikach badania oraz wyjaśnienie, w jaki sposób badanie to przyczyniło się do rzetelności sprawozdawczości finansowej w JZP, a także, jaka była rola komitetu audytu w procesie badania;
3. Dokonywanie oceny niezależności biegłego rewidenta na potrzeby zatwierdzenia świadczenia przez niego dozwolonych usług niebędących badaniem w JZP;
4. Opracowanie polityki w zakresie wyboru podmiotu uprawnionego do badania sprawozdań finansowych;
5. Opracowanie polityki w zakresie świadczenia - przez podmiot uprawniony do badania sprawozdań finansowych badający sprawozdanie finansowe JZP, przez podmioty powiązane z tym podmiotem uprawnionym do badania oraz przez członka sieci tego podmiotu uprawnionego do badania sprawozdań finansowych - dodatkowych usług niebędących badaniem, w tym usług warunkowo zwolnionych z zakazu świadczenia;
6. Szczegółowe określenie procedury wyboru podmiotu uprawnionego do badania sprawozdań finansowych przez JZP oraz przedstawienie organowi nadzorczemu JZP rekomendacji zawierającej propozycję dwóch podmiotów uprawnionych do badania sprawozdań finansowych do przeprowadzenia badania;
7. Przedkładanie zaleceń mających na celu zapewnienie rzetelności procesu sprawozdawczości finansowej w JZP”[1].

Po przeprowadzeniu licznych konsultacji i po uwzględnieniu wniosków dotyczących dostosowania przepisów dotychczasowego prawa krajowego, do regulacji unijnych w przedmiotowym zakresie, w projekcie ustawy z dnia 05.10.2016 roku, skorygowany został zapis dotyczący obowiązku monitorowania działań audytu wewnętrznego. I tak, komitet audytu został zobowiązany do monitorowania:

- „procesu sprawozdawczości finansowej,
- skuteczności systemów kontroli wewnętrznej i systemów zarządzania ryzykiem **oraz audytu wewnętrznego w zakresie sprawozdawczości finansowej,**
- wykonywania czynności rewizji finansowej […]”[2].

Dodatkowo w ust. 2 wyżej przywołanego artykułu potwierdzono prawo komitet audytu do żądania, bez pośrednictwa rady nadzorczej, udzielenia informacji oraz innych wyjaśnień, a także przekazania dokumentów niezbędnych do wykonania zadań, o których mowa w ust. 1. Taki zapis zwiększa swobodę działania komitetu. Stworzenie możliwość bezpośredniego

1 Tamże: art.128 ust. 10.

2 www.legislacja.rcl.gov.pl/projekt/12284259;Projekt Ustawy o biegłych rewidentach i ich samorządzie z dnia 5.10.2016r. - Rozdział 9 Czynności rewizji finansowej, w tym w jednostkach zainteresowania publicznego: art. 124 ust.1.

domagania się szerokiego wachlarza informacji stanowi usankcjonowanie praktyki, która w zasadniczym stopniu determinuje skuteczność działania komitetu.

Podsumowanie

Pomimo, że w wyżej przedstawianych projektach ustawy widać wyraźne wzmocnienie roli i znaczenia komitetu audytu, to jednak wciąż artykułowane są pewne wątpliwości dotyczące proponowanych zmian. Wiążą się one głównie z niedosytem w zakresie szczegółowości uregulowania zasad funkcjonowania komitetów audytu w ramach rad nadzorczych. Projektowana korekta zapisu dotyczącego obowiązku monitorowania audytu nie ogranicza prawa delegowania komitetowi obowiązku pełnego monitoringu skuteczności funkcji audytu wewnętrznego. Wydaje się to szczególnie istotne, biorąc pod uwagę inne regulacje, tj. wymienione na wstępie zasady dobrych praktyk spółek notowanych na GPW. Należy podkreślić, że nałożenie na komitet obowiązku monitorowania audytu wewnętrznego nie zwalnia rady nadzorczej z obowiązku dokonania rocznej oceny jego skuteczności.

Bibliografia:

1. Dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. *w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych* (Dz.U. UE L 157/87)*;*
2. Dyrektywa 2014/56/UE Parlamentu Europejskiego i Rady z dnia 16 kwietnia 2014 zmieniającą dyrektywę 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych (Dz.U. UE L 158/196)*;*
3. Projekt Ustawy o biegłych rewidentach i ich samorządzie podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym z 11.04.2016 r. Rządowe Centrum Legislacji, www.legislacja.rcl.gov.pl/projekt/12284259 (dostęp: 08.11.2016r.);
4. Projekt Ustawy o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym z dnia 5.10.2016r.; Rządowe Centrum Legislacji, www.legislacja.rcl.gov.pl/projekt/12284259 (dostęp: 08.11.2016r.);
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 537/2014 z dnia 16 kwietnia 2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego (Dz.U. UE L 158/77);
6. Ustawa z dnia 9 maja 2009 r. *o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym* (Dz. U. z 2015 r. poz. 1011 i 1844).

Streszczenie:

W związku z obowiązkiem transpozycji do prawa krajowego postanowień nowych przepisów prawa UE, wszczęta została procedura przygotowania zmian zapisów obowiązującej ustawy o biegłych rewidentach i ich samorządzie. Celem procedowanych zmian jest między innymi zwiększenie znaczenia komitetów audytu, poprzez doprecyzowanie zasad ich tworzenia oraz rozszerzenie zakresu ich działania. Jednym z wielu zadań powierzonych komitetom jest monitoring funkcji audytu wewnętrznego. W projekcie procedowanej obecnie ustawy zaproponowano uściślenie zakresu obligatoryjnego monitoringu wyżej wskazanej funkcji. W prezentowanym artykule wskazane zostały podstawowe zmiany zapisów dotyczących zakresu działania komitetu audytu, wprowadzone i projektowane w regulacjach unijnych oraz w przepisach krajowych.

Matt Suozzo*,
Józef Puzyna**.

W oczekiwaniu na uregulowania w zakresie bezpieczeństwa informacji

Wprowadzenie

Wraz ze wzrostem zagrożeń i naruszeń bezpieczeństwa danych nasila się nadzór regulacyjny.

1. Page Content

Każdy, kto śledzi bieżące wydarzenia nie mógł nie dostrzec niemal nieprzerwanego strumienia artykułów na temat organizacji wszystkich typów i rozmiarów, które doświadczyły naruszenia bezpieczeństwa, prowadzących do ujawnienia informacji o klientach. Organy regulacyjne i agencje rządowe również to dostrzegły, jak również zwiększyły swoje wysiłki, aby egzekwować istniejące wytyczne dotyczące bezpieczeństwa, poprawić wytyczne,

* Matt Suozzo jest zastępcą dyrektora Departamentu Konsultingu IT i Praktyk Audytu Wewnętrznego w firmie Protiviti, mieszczącej się w Overland Park (USA, Kansas).
** Tłumaczenie Józef Puzyna, Kierownik Biura Audytu Wewnętrznego CARDIF BNP PARIBAS GROUP.

jednocześnie zwiększając oczekiwania i tworząc nowe wymagania i cele.

Amerykańskie organizacje w bankowości, opiece zdrowotnej, a także agencje rządowe od dawna stykały się wymogami regulacyjnymi związanymi z bezpieczeństwem za pośrednictwem ustaw: *Gramm-Leach Bliley Act*, ustawy o przenośności ubezpieczenia zdrowotnego i odpowiedzialności (*Health Insurance Portability* i *Accountability Act*) oraz ustawy o federalnym zarządzaniu bezpieczeństwem informacji (*Federal Information Security Management Act* - FISMA). Jako, że zagrożenia ewoluują i naruszenia bezpieczeństwa danych stają się bardziej powszechne, nadzór regulacyjny i jego egzekwowanie rozprzestrzenia się na inne branże. Ostatnie działania wykonawcze organów amerykańskich takich jak Komisja Papierów Wartościowych i Giełdy oraz Biura Ochrony Finansowej Konsumentów (CFPB) zdają się być oznakami przyszłych zdarzeń.

Na przykład w marcu 2016 r. CFPB wymierzyło pierwszą grzywnę związaną z bezpieczeństwem informacji w stosunku do platformy płatności online. CFPB stwierdziło, że organizacja niewłaściwie prezentowała swoje mechanizmy kontrolne i praktyki wokół bezpieczeństwa danych, wymierzyło kwotę 100.000 USD kary i zażądała, aby organizacja wprowadziła zmiany w swoich praktykach bezpieczeństwa. Według Dyrektora CFPB Richard'a Cordray'a „Z naruszeniami bezpieczeństwa danych stającymi się coraz bardziej powszechnymi i większą liczbą konsumentów korzystających z systemów płatności online, ryzyko dla konsumentów rośnie. Istotne jest, aby firmy wprowadziły systemy ochrony informacji i dokładnie informowały konsumentów o ich praktykach w zakresie bezpieczeństwa danych". To było pierwsze działanie nadzorcze CFPB w dziedzinie bezpieczeństwa danych i wiele organizacji zostało postawionych w stan gotowości.

Większość organizacji ma jakąś formę kontroli bezpieczeństwa i procesów, ale te nie zawsze mogą mierzyć się z najlepszymi praktykami w branży. Istnieją pewne procesy i kontrole, które organizacje w każdej branży powinny rozważyć w oczekiwaniu na zwiększenie kontroli regulacyjnej.

2. Ustanowienie procesu oceny ryzyka bezpieczeństwa

Ocena ryzyka jest podstawą do budowania i realizacji godnych zaufania procesów bezpieczeństwa informacji i kontroli. Tradycyjne podejście do bezpieczeństwa informacji opierało się na zgodności lub regułach. Zastosowanie podejścia opartego na ryzyku jest bardziej skuteczne w przewidywaniu, gdzie będą kierować się kontrole regulacyjne. Jeżeli organizacje niewłaściwie oceniają swoje ryzyka, jak mogą zapewnić wdrożenie mechanizmów kontroli bezpieczeństwa w celu ochrony swoich najważniejszych zasobów?

Istnieje wiele różnych podejść do przeprowadzania oceny ryzyka bezpieczeństwa. Zazwyczaj organizacje opracowują wykaz swoich zasobów, katalogują, gdzie znajdują się dane wrażliwe oraz identyfikują potencjalne zagrożenia. Każdemu zasobowi zostaje przypisana miara nieodłącznego (*inherent risk*) w zależności od krytyczności danych, która jest w nim dostępna. Następnie organizacje identyfikują potencjalne możliwości, które ma osoba lub organizacja o złych zamiarach, aby uzyskać dostęp do najbardziej ryzykownych zasobów.

Wówczas organizacja identyfikuje jakie mechanizmy kontrolne lub procesy są stosowane w celu ograniczenia stwierdzonych zagrożeń. Tam, gdzie istnieją luki w systemie kontroli, organizacja ocenia koszt i korzyść albo wdrożenia nowych mechanizmów kontrolnych lub procesów albo zmiany istniejących praktyk w celu rozwiązania problemu.

W ciągle zmieniającym się krajobrazie technologii bezpieczeństwa, wymogów regulacyjnych, zagrożeń i podatności, ocena ryzyka bezpieczeństwa powinna być wykonywana regularnie oraz w razie potrzeby w sytuacjach znaczących zmianach w organizacji. Większość organizacji przeprowadza oceny w ujęciu rocznym lub półrocznym, w zależności od branży i tolerancji ryzyka. Ocena ryzyka powinna być powtarzalna i dobrze udokumentowana, aby umożliwić konsekwentne raportowanie wyników i ich porównywanie w czasie. Wyniki oceny ryzyka powinny być udokumentowane i przekazane Zarządowi i innym interesariuszom (np. działom: prawnemu, zgodności), aby pomóc w podejmowaniu decyzji.

3. Opracowanie/udoskonalenie programu ochrony informacji

Organizacjom, które chcą antycypować przyszłe wymagania regulacyjne, przyjęcie powszechnie akceptowanych w branży standardów bezpieczeństwa jest solidnym fundamentem, na którym można się oprzeć. Standardy te obejmują m.in. ISO 27001, zasady cyberbezpieczeństwa Narodowego Instytutu Norm i Technologii (*National Institute of Standards and Technology - NIST*), FISMA, różne aspekty COBIT i *IT Infrastructure Library*. Jeden rozmiar nie pasuje każdemu. Na przykład, jeśli organizacja przyjmuje NIST 800 -53 jako standard, skądinąd wszechstronny i stosowny dla większości agencji rządowych, to nie wszystkie jego wymagania mogą być wdrożone, zważywszy na profil ryzyka danej organizacji. Organizacje powinny ocenić wybrany standard i zmapować do istniejącego środowiska. Jeżeli istnieją luki, kierownictwo powinno ocenić ekspozycję na ryzyko i określić plany działania dostosowane do tolerancji ryzyka i ogólnych celów.

Skoro niezbędne kontrole bezpieczeństwa informacji zostały zidentyfikowane i potencjalnie wdrożone, organizacja powinna albo udokumentować, albo zaktualizować swój program ochrony. Dokument ten służy jako podstawa procesów bezpieczeństwa informacji i praktyk w całej organizacji, a najprawdopodobniej będzie jednym z pierwszych dokumentów, którego będzie oczekiwał regulator. Dokument powinien opisać strukturę zarządzania, z uwzględnieniem polityk oraz różnych kontroli i procesów, które pomagają ograniczyć ryzyka związane z bezpieczeństwem.

Organizacja może wydać nieograniczone zasoby na najnowocześniejszą technologię zabezpieczeń, ale jeśli możne ona zostać ominięta przez pracownika przypadkowo uszkadzającego stację roboczą, klikając na złośliwy link w poczcie elektronicznej, cały wysiłek idzie na marne. Realizacja programu w zakresie świadomości ochrony pracowników ma kluczowe znaczenie dla powodzenia programu bezpieczeństwa. Pracownicy powinni być kształceni, testowani i stale powinno im się przypominać o bieżących zagrożeniach i najlepszych praktykach w celu zminimalizowania skuteczności socjotechniki.

4. Weryfikacja środowiska kontroli

W momencie wdrożenia programu ochrony oraz stosownych procesów i kontroli, organizacje powinny opracować proces okresowej oceny i weryfikacji środowiska kontroli. Większość organizacji obecnych w Internecie jest codziennie skanowana i oceniana przez atakujących, ręcznie lub przez zautomatyzowane ataki. Organizacje powinny starać się pozostać jeden krok do przodu, wykonując własne oceny, które często obejmują automatyczne skanowania podatności i testy penetracyjne.

Kontrole inne nietechniczne, takie jak polityki, procedury, a także oceny ryzyka, powinny być okresowo oceniane w celu ustalenia, czy są one wykonywane zgodnie z ustalonym programem bezpieczeństwa. Dla procesów jest naturalne, że zostają określone, a następnie podupadają ze względu na czynniki takie jak zmiany w kierownictwie lub konkurujące priorytety. Poprzez wykonywanie czynności sprawdzania poprawności, organizacja może wykazać, że stworzyła skuteczny program ochrony, a także regularnie dokonuje przeglądu swojego otoczenia, aby zapewnić, że pozostaje na bieżąco ze zmianami w krajobrazie bezpieczeństwa.

Organizacje mogą przygotowywać się do wymogów bezpieczeństwa, które nie zostały jeszcze określone. Poprzez wykonywanie oceny ryzyka bezpieczeństwa, przyjmując branżowo akceptowane standardy bezpieczeństwa oraz wdrożenie i sprawdzenie skuteczności kontroli bezpieczeństwa, organizacja może pozycjonować się nie tylko w kierunku zmniejszenia ryzyka dla siebie i swoich klientów, ale także zminimalizowanie wpływu nowych przepisów i wymogów regulacyjnych. Organizacje powinny monitorować stale zmieniające się zagrożenia bezpieczeństwa i krajobraz regulacyjny oraz próbować przewidywać procesy lub kontrole, które obecnie nie są częścią ich programów. Ponadto, organizacje powinny monitorować przepisy prawa w krajach, w których działają, lub zamierzają działać, aby upewnić się, że wytyczne są rozumiane i realizowane w ramach programu bezpieczeństwa. Jeśli chodzi o bezpieczeństwo informacji, zarówno z punktu widzenia przestrzegania przepisów jak i technicznych mechanizmów kontroli, bardziej skuteczne jest wyprzedzanie trendu niż podejmowanie prób nadążenia za nim.

Mariusz Jedynak[*]**,**
Łukasz Borowski[**]**.**

Audytowe „zarządzanie zmianą" – doświadczenia Zakładu Ubezpieczeń Społecznych

1. WPROWADZENIE/ WSTĘP

Budowa i kształtowanie różnorodnych systemów zarządzania w organizacji (m.in. system zarządzania przez cele, zintegrowany system zarządzania ryzykiem), a także dynamiczne procesy zachodzące w jednostkach (m.in. wartościowanie stanowisk, optymalizacja struktur organizacyjnych itp.) oraz związana z powyższymi aktywność kierownictwa jednostki we wdrażaniu zmian, implikuje na audytorach konieczność „wpasowania się" nie tylko w strukturę organizacyjną, ale także – a może przede wszystkim – w sposób zarządzania jednostką przez kierownictwo.

Optymalną staje się sytuacja, gdy audyt, poprzez wyniki swojego działania, czy to zapewniającego, czy – aktualnie przede wszystkim – doradczego, staje się realnym partnerem dla kierownictwa jednostki.

Wyznaczenie takiej pozycji w organizacji wymaga od nas, częściej niż bywało to jeszcze kilka lat temu, umiejętności „dopasowania" naszego profilu działalności do bieżących potrzeby kierownictwa.

Zapewne to zabrzmi jak banał, ale - jak jeszcze nigdy dotąd – aktualne stało się z jednej strony podejście/nastawienie kierownictwa do wykorzystywania dużego potencjału analitycznego komórki audytu, a z drugiej – umiejętność zarządzającego audytem w odpowiedzi (wynikami swojej pracy) na oczekiwania kierownictwa. Suma powyższego daje audytowi bardzo silną pozycję. Z perspektywy czasu, doświadczeń w budowie i wykorzystywaniu naszych – audytorskich – kompetencji, a także w oparciu o obserwacje dotyczące zachowywania się organizacji jako odbiorcy naszych prac, możemy śmiało powiedzieć, że mocny audyt, to także mocna organizacja.

Departament Audytu w ZUS, wykorzystując istniejące w Zakładzie Ubezpieczeń Społecznych systemy zarządzania (m.in. wspomniane wyżej zarządzanie przez cele oraz zarządzanie ryzykiem) oraz opierając się na wdrażanych projektach (optymalizacja organizacji w wielu wymiarach, wartościowanie, etatyzacja) realizuje zadania audytowe, które bazują na ww. rozwiązaniach i w sposób realny wspierają Zarząd oraz kadrę zarządzającą ZUS w podejmowaniu decyzji zarządczych, w tym wspierają efektywność organizacji zarówno w odniesieniu do już istniejących rozwiązań, jak również mają wpływ na podejmowanie decyzji i zwiększanie efektywności rozwiązań dopiero projektowanych. Rola niezależnego doradcy, właściwie permanentnie obecnego w procesie zarządzania,

* Dyrektor Departamentu Audytu w Zakładzie Ubezpieczeń Społecznych.
** Wicedyrektor Departamentu Audytu w Zakładzie Ubezpieczeń Społecznych.

pozwala na przedstawianie wyników analiz, które mają bezpośredni wpływ na doskonalenie skuteczności działania organizacji.

Obserwacja tego typu relacji, z poziomu zarządzającego audytem jest niezwykle motywująca.

2. ZMIANY ZACHODZĄCE W ORGANIZACJI I ICH WPŁYW NA REALIZACJĘ FUNKCJI AUDYTU

Pozycja Zakładu Ubezpieczeń Społecznych w sektorze publicznym podlega ciągłym zmianom – w szczególności przepisów powszechnie obowiązujących, regulujących wektor działania ZUS, jak i rosnącym wymaganiom nadzorcy (Ministerstwo). W takich warunkach, budowa wizerunku organizacji w kontekście zapewnienia jakości usług dla klientów (a tych mamy – bezpośrednio i pośrednio - około 25 milionów) wymaga także od audytu szybkości w reagowaniu na zmienne warunki zewnętrzne i oczekiwania kierownictwa. Systematyczna ocena systemu kontroli zarządczej nie tylko nabiera w takiej sytuacji nowych wymiarów, ale także staje się niejako działaniem standardowym, w dobrym tego słowa znaczeniu – rzecz jasna usystematyzowane, metodyczne podejście do realizacji zadań zapewniających stało się w tym przypadku bardzo pomocne.

W świetle oczekiwań kierownictwa Zakładu, ważniejsza wydaje się jednak być nasza rola doradcza, realizowana praktycznie w każdej możliwej formie. Począwszy do typowego doradztwa w formie czynności doradczych, poprzez udział w zespołach roboczych – na zasadzie silnego głosu doradczego, wspomaganie wdrażania zarządzania ryzykiem w jednostce, dostarczanie wyników prac analitycznych, czy wreszcie analizy ad–hoc wspierające podejmowanie decyzji zarządczych (w tym m.in. w zakresie możliwości optymalizacji struktury organizacyjnej), to bardzo ważna część naszej działalności, na którą – co więcej – stale rośnie zapotrzebowanie w naszej organizacji.

Nie bez wpływu na powyższe była zmiana kultury organizacyjnej w ZUS – przejście na zarządzanie przez cele na poziomie strategicznym – cele długoterminowe (Strategia) i poziomie operacyjnym – cele krótkoterminowe (Plan działalności Zakładu, ale także zarządzanie procesowe, usługowe i system oceny pracy oddziałów). Zmiana filozofii funkcjonowania Zakładu z typowego podejścia realizacji zadań, na rzecz zdefiniowanych celów, mierników i ich pomiaru stanowiła szansę dla audytu do przejścia z roli recenzenta do roli partnera wspierającego rozwój organizacji. Z pewnością zarząd każdej organizacji zdecydowanie bardziej woli otrzymać takie wyniki, które dają komfort podjęcia decyzji zamiast raportu z wnioskiem - „zarządzie masz problem".

Nasze dotychczasowe doświadczenia potwierdzają słuszność przyjętego kierunku. Zmiany zarządzania organizacją zainicjowały zmianę funkcji audytu oraz kierunek tych zmian – przejście od audytu zgodności do audytu efektywności. Z drugiej strony, zmiany zachodzące w ZUS stały się katalizatorem, a w konsekwencji doprowadziły do zmiany pewnych zachowań (zmiana potrzeb i oczekiwań kierownictwa jednostki, zarządzanie przez cele przy jednoczesnym dążeniu do maksymalizacji jakości oferowanych usług

i produktów, ukierunkowanie na klienta) i dały „zielone światło" do wprowadzenia dobrej praktyk w zakresie prowadzenia audytu.

Nie ukrywamy, że taka perspektywa jest dla audytu bardzo kusząca i daje pewien komfort pracy, który jest tak ważny w realizacji funkcji audytu w organizacji.

Naszym zdaniem, to – ciągle jeszcze innowacyjne – podejście do realizacji ustawowej funkcji audytu, daje się zauważyć w coraz większej ilości jednostek. To bardzo dobrze wróży na przyszłość, jeśli chodzi o rolę audytu, nie tylko w sektorze jednostek finansów publicznych.

3. REALIZACJA AUDYTU W KONTEKŚCIE CELÓW JEDNOSTKI

Poniżej przedstawiamy kilka obszarów, w których obecnie, jako audyt, najczęściej poruszamy się w Zakładzie i kluczowe czynniki sukcesu, w oparciu o które powyższe aktywności realizujemy.

Podstawowymi kryteriami, które nakreślają kontekst aktywności audytu, są cele strategiczne i operacyjne. Bez wyraźnie postawionych celów w jednostce, jako punktu odniesienia, nie jest możliwa efektywna realizacja funkcji audytu. Dlatego już od momentu sporządzenia planu audytu, w/w cele są adresowane w audycie. Plan audytu powstaje w oparciu o analizę ryzyka, która obejmuje min. analizę wspomnianych celów strategicznych oraz operacyjnych, ale także priorytety kierownictwa (członków Zarządu), którymi są oczekiwania, wprost nakierunkowane na efektywność działania organizacji. Zadania audytowe są automatycznie bezpośrednio powiązane z celami jednostki, a ścieżka audytu obejmuje odniesienie zarówno do realizacji celu, ocenę sposobu jego realizacji, jak i sygnalizowanie najważniejszych ryzyk w kontekście celu. Także raportowanie wyników przeprowadzonych audytów następuje w odniesieniu do zagrożenia osiągnięcia celów długo i krótkookresowych przez Zakład. Wreszcie rola doradcza, polegająca m.in. na opiniowaniu wewnętrznych aktów prawnych w zakresie spełnienia wymagań standardów kontroli zarządczej oraz identyfikowania i analizy ryzyk obejmuje m.in. analizę relacji pomiędzy celami strategicznymi i operacyjnymi, wyznaczonymi dla Zakładu w danym obszarze, który jest objęty regulacją, a możliwością monitorowania sposobu ich osiągania.

Dostarczanie wyników oczekiwanych przez kierownictwo Zakładu nie byłoby możliwe bez określania ścisłych kryteriów, którymi kierujemy się przy realizacji audytów efektywnościowych. Do najważniejszych kryteriów należą oczywiście te ustawowe:

- efektywność – ocena wyników realizacji zadania, czy wykorzystywane zasoby oraz zaprojektowane mechanizmy kontroli zapewniają pełny „workflow"[1] procesu,
- adekwatność – precyzująca, czy przebieg procesu oraz wykonywane czynności zostały zaprojektowane w sposób optymalny – najbardziej odpowiedni do celu i sposobu realizowanego zadania;

1 Work flow [ang] – dosł. przepływ pracy.

– skuteczność – przedstawiająca, czy realizacja procesu prowadzi do pełnej i prawidłowej realizacji zadania.

Jednak realizacja efektywnościowej funkcji audytu, w pełnym tego słowa znaczeniu, wymaga stosowania również dodatkowych kryteriów, w tym m.in. kryterium:

– wydajności – weryfikacji podlegają wydajność produktu/usługi, koszty jednostkowe, wskaźniki np. określające poziom wykorzystania zasobów, czas oczekiwania na usługę, czy też,
– gospodarności – minimalizacji wykorzystywanych zasobów (środki finansowe, zasoby kadrowe, wyposażenie, zasoby lokalowe), przy jednoczesnym zachowaniu odpowiedniej jakości realizowanych działań.

Omawiane kryteria są każdorazowo adresowane w naszych raportach, a organizacja jest przyzwyczajona do wskazywania przez nas – czasami prostych, ale bardzo wymownych – relacji opartych na tychże kryteriach.

Powyższe podejście zapewnia możliwość wskazania konkretnych korzyści (rezultatów) kierownictwu jednostki, a tym samym determinuje postrzeganie audytu jako autora optymalnych rekomendacji, w zakresie wskazania szans na wzrost efektywności procesów, realnych oszczędności, czy też możliwości niwelacji ryzyk ponadobszarowych, co w konsekwencji zapewnia odpowiednią komunikację pomiędzy audytorem wewnętrznym, a klientem audytu (kierownictwem) i ma bezpośrednie przełożenie na realny wpływ na zmianę kultury organizacji.

Rzecz jasna, powyższe aktywności związane są nieodłącznie z wyzwaniami, jakie stały przed komórką audytu w zakresie zmiany podejścia do przeprowadzania audytu opartego o system zarządzania przez cele i zarządzania ryzykiem, a które dotyczyły m.in. utrzymania/wykorzystania/rozwoju kompetencji audytorów w kluczowych obszarach działania organizacji (operacyjnych, wspomagających, zarządczych), ciągłego rozwijania kompetencji analitycznych pracowników (kluczowe narzędzia audytu wewnętrznego umożliwiające: prowadzenie badań powiązań/relacji pomiędzy zbiorami danych, ekstrapolację wniosków na inne obszary działania – wnioskowanie oraz prace na próbach reprezentatywnych, wykorzystanie nowych narzędzi oraz technik prezentowania wyników), czy wreszcie wysiłku w dostosowanie w/w zasobów do oczekiwanych rezultatów pracy.

Nie oznacza to oczywiście, że obyło się bez jakichkolwiek problemów we wdrażaniu omawianego podejścia:– wielkiej determinacji wymaga np. zbudowanie kompetencji w zakresie audytów informatycznych i bezpieczeństwa informacji oraz znalezienie optymalnych narzędzi, mogących wspomóc wykonywanie działań dosyć dużego zespołu. Wzmożonej pracy wymagało także kształtowanie postaw audytorów w tym zakresie - zmiana nastawienia i postępowania w zakresie odejścia od typowego badania zgodności na rzecz efektywności, zwiększona elastyczność, budowa kreatywności działania/myślenia/postrzegania problemów (ze względu na brak szablonowego działania w trakcie przeprowadzania audytu efektywnościowego). Zapewniamy, że się opłacało.

Ważną dodatkową kwestią, na którą należy zwrócić uwagę, jest rosnąca rola zarządzania ryzykiem w jednostce, jako systemu umożliwiającego ustawienie wektora działania audytu. Zarządzanie ryzykiem na poziomie operacyjnym i strategicznym (w perspektywie operacyjnej ma na celu ograniczenie poziomu ryzyk mogących mieć wpływ na realizację celów i zadań Zakładu, a tym samym wzmocnienie działań prowadzących do realizacji nadrzędnego celu ujętego w Strategii organizacji w perspektywie strategicznej). Informacje, dostarczane z w/w systemu, wraz z analizą kluczowych wskaźników ryzyka (KRI), stają się bazowymi elementami zarówno planowania pracy, jak i raportowania wyników audytu. Jeśli dodamy do powyższego rolę koordynacyjną i edukacyjną komórki audytu w systemie zarządzania ryzykiem, otrzymujemy pełne narzędzie do monitorowania osiągania celów jednostki i możliwość reagowania na niebezpieczeństwa. To bardzo ważny głos w organizacji.

4. STRESZCZENIE:

Optymalne zarządzanie zmianą w audycie to ciągłe szukanie – niejednokrotnie także nowej – roli audytu wewnętrznego w jednostce i (najczęściej udane) próby odnalezienia się w gąszczu coraz to nowych, wyższych, wymagań stawianych przed audytorami przez kierownictwo jednostki.

Bardziej, niż kiedykolwiek aktualne stało się obecnie pytanie: czy to nadal środowisko wewnętrzne organizacji określa i wyznacza naszą rolę, czy to już raczej my – jako pełnoprawny partner kierownika jednostki – (współ)określamy kształt tego środowiska, dostarczając kierownictwu wyniki prac w zakresie, w którym oczekiwana jest aktywność audytu? Przejście od funkcji typowo zapewniającej do funkcji doradczej zdecydowanie zmieniło wektor naszej aktywności.

Równie ważne staje się tym samym znalezienie odpowiedzi na wątpliwości, czy i gdzie przesuwa się naturalna granica możliwego działania audytu i w jaki sposób wyniki naszej pracy wpływają na kształtowanie ładu organizacyjnego w jednostce.

Cieszy fakt, że to my, audytorzy, mamy coraz większy udział w określaniu tej optymalnej roli, a wyniki naszej pracy znajdują bezpośrednie odzwierciedlenie w decyzjach podejmowanych na najwyższym poziomie w organizacji. To bardzo dobry punkt wyjścia w dyskusji, dokąd powinien zmierzać audyt.

Słowa klucze: audyt efektywnościowy, doradztwo, zarządzanie zmianą, zarządzanie ryzykiem.

Olga Petelczyc*
Elżbieta Paliga**
Krzysztof Pakoński***
Jakub Syta****
Maciej Jędrzejewski*****
Katarzyna Celińska******

Relacja z konferencji „Samorządowe Forum Kapitału i Finansów”

Samorządowe Forum Kapitału i Finansów to prestiżowa konferencja, która od czternastu lat jest platformą wymiany doświadczeń szefów samorządów z przedstawicielami administracji państwowej i biznesu. W tym roku wydarzenie miało miejsce w dniach 22-23 września 2016 roku, w **Katowicach w budynku Międzynarodowego Centrum Kongresowego.**

Tegoroczna konferencja objęła ponad 60 paneli i debat, które złożyły się na 10 konferencji tematycznych, a uczestniczyło w nim ponad 1000 osób. Jednym z tematów istotnych i interesujących, o czym świadczyła liczba uczestników był „Audyt wewnętrzny w JST”, który już po raz drugi współorganizował Instytut Audytorów Wewnętrznych IIA Polska wraz z Kołem AW JST IIA Polska.

Pierwszym panelem, który odbył się tuż po sesji inauguracyjnej, był: „Kontrole NIK i RIO w samorządzie”. Pytanie, jakie nasunęło się w czasie debaty i na które szukano odpowiedzi było: Co zrobić, żeby kontrola nie była postrzegana, jako zło konieczne?

Uczestnicy spotkania, już na samym początku panelu, zgodnie zaznaczyli, iż kontrola jest potrzebna, ważne jednak

Autor zdjęcia: : Katarzyna Celińska, IIA Polska.

* Wiceprezes IIA Polska.
** Kierownik Biura Audytu Wewnętrznego, UM Dąbrowa Górnicza, Koordynator Koła JST w IIA Polska.
*** Audytor Generalny, Urząd Miasta Krakowa.
**** Jakub Syta Ekspert ds. Cyberbezpieczeństwa, bezpiecznik.pl.
***** Specjalista ds. Bezpieczeństwa Informacji, Centralny Ośrodek Informatyki.
****** IIA Polska.

jest to, aby nie tylko rozliczać nieprawidłowości, ale również pokazywać narzędzia, dzięki którym w przyszłości będziemy mogli uniknąć błędów. Ponadto, narzędzie te, często można w późniejszym czasie wykorzystać do wskazywania ryzyk i dawania szansy, gdyż uchybienia mają często różny charakter i mogą być nieprzewidywalne.

Na stronach Regionalnych Izb Obrachunkowych dostępne są wyniki prac nadzorczych i opiniodawczych, które mogą być przydatne w codziennym funkcjonowaniu. Raporty z przeprowadzonych już audytów i kontroli dostępne na stronach RIO i NIK dla kierowników jednostek i dla audytorów to cenne źródło informacji w procesie zarządzania ryzykiem.

Podsumowując rozważania i dyskusje podjęte w panelu należy podkreślić wniosek, iż kontrola jest integralną częścią organizacji. Jej istotnym elementem jest współpraca audytu z kontrolą oraz z organami zewnętrznymi. Kontrola pozwala nam stosować profilaktykę, audyt wewnętrzny zaś powinien być wspierany kontrolą/audytem zewnętrznym.

W drugim panelu, rozważania dotyczyły Audytu funduszy europejskich. Panel

Autor zdjęcia: : Katarzyna Celińska, IIA Polska.

dopełniła dyskusja pomiędzy ekspertami. Zaczął się optymistycznym akcentem, iż prognoza na lata 2014-2020 jest bardzo korzystna dla Polski. Ważne jest między innymi, aby bazować na strategii przy pisaniu projektów oraz zwracać uwagę na planowanie i analizę potrzeb. Podstawą jest efektywne wydatkowanie środków unijnych i umiejętność unikania błędów, tak aby racjonalnie wykorzystywać audyt wewnętrzny w JST w ramach realizacji projektów współfinansowanych ze środków europejskich należy zwrócić uwagę na planowanie i analizę potrzeb.

Problem jest zadłużenie samorządów, które często nie mają niestety środków na wkład własny, który potrzebny jest przy składaniu wniosków.

Zdaniem ekspertów ważny jest również dobór zespołów projektowych i rachunkowość projektowa, czyli zainwestowanie zarówno w kadrę jak i szkolenia. Audytorzy wewnętrzni mogą wspierać kierowników jednostek na każdym etapie realizacji projektów.

Wczesne wykrywanie problemów czy błędu istotnie ogranicza ryzyko korekt finansowych, które może być odczuwalne dla samorządów.

Dodatkową korzyścią z dobrze przygotowanej dokumentacji szczególnie rozliczeniowej jest skrócenie procesu rozliczania, a to z kolei przekłada się na szybszą wypłatę środków i lepszą płynność finansową. Wszyscy uczestnicy panelu zgodnie podkreślali, że fundusze europejskie są ogromną szansa na rozwój i poprawę, jakości życia mieszkańców samorządów!

Głównym źródłem finansowania w gminach są wpływy z podatków lokalnych. Mają one kluczowe znaczenie dla samodzielności finansowej jednostek samorządu terytorialnego. Gminom zostały przekazane uprawnienia tzw. władztwa w zakresie kształtowania lokalnych obciążeń podatkowych. Niestety korzystanie przez gminy z władztwa podatkowego skutkuje także utratą części ich dochodów, a tym samym zaburzone przez spadek dochodów są dwie inne funkcje systemu fiskalnego: redystrybucyjna i stymulacyjna, które służą kreowaniu swoistego kompromisu pomiędzy celami fiskalnymi, gospodarczymi i społecznymi opodatkowania[1].

Występujące w praktyce sprzeczności pomiędzy tymi funkcjami wymagają permanentnego dokonywania wyborów przez władze gmin[2] . W krótkim okresie rezygnacja władz gmin z części dochodów pewnie w jakimś stopniu ogranicza ich możliwości funkcjonowania bądź naraża na konieczność pozyskiwania dodatkowych środków[3], w długim jednak okresie może pojawić się pozytywne oddziaływanie pozostawienia większych pieniędzy w rękach lokalnych podatników[4]. Bardzo ważnym elementem weryfikacji oraz oceny budżetu gminy, a co za tym idzie dalej stabilności finansowej gminy jest audyt wewnętrzny.

Audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze.

1 Adamiak J., *Jak władze gminy mogą wykorzystywać funkcje pozafiskalne podatków i opłat lokalnych do wspierania rozwoju regionalnego [w:] Polski system podatkowy. Założenia a praktyka*, red. A. Pomorska, Wydawnictwo UMCS, Lublin, 2004.

2 Owsiak S., *Finanse publiczne. Teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 2002.

3 Będzieszak M., *Władztwo dochodowe i dochody gmin w sytuacji spowolnienia gospodarczego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 646, 2010.

4 Przygodzka R., *Władztwo podatkowe a stabilność finansowa gmin,* Nierówności Społeczne a Wzrost Gospodarczy, nr 40 (4/2014).

Podatki lokalne to istotne źródło dochodów jednostek samorządu terytorialnego. Ich prawidłowa i skuteczna realizacja przyczynia się do zasilenia lokalnego budżetu, który umożliwia zaspokojenie potrzeb lokalnej społeczności. Jednak z procesem kształtowania wymiaru tych podatków oraz ich ściągania wiąże się szereg ryzyk. Dlatego proces ten powinien podlegać systematycznej ocenie, dokonywanej m.in. przez audyt wewnętrzny.

W tym kontekście należy postawić pytanie: Jak przebiega proces kształtowania wymiaru lokalnych podatków oraz ich ściąganie? Jakie ryzyka i jakie nieprawidłowości zidentyfikowano w tym zakresie? Jakie główne obszary związane z tym procesem powinny być przedmiotem badań audytu wewnętrznego? Kto jeszcze odgrywa istotną rolę w zapewnieniu prawidłowości tego obszaru?

Odpowiedź na powyższe pytania udzielili eksperci w ramach panelu Audytu Podatków. Rozmawiano również o dochodach JST i czynnikach kształtujących zmiany dochodów w samorządach, odpowiedzialności i roli Skarbnika JST. Podjęto również temat głównych obszarów prowadzenia audytu na przykładzie podatków lokalnych, ściągalności podatków, jako źródła dochodów gmin pobieranych przez naczelników urzędów skarbowych, a także roli audytu wewnętrznego w ograniczeniu ryzyka korupcji na przykładzie podatków lokalnych oraz jej przeciwdziałaniu.

Należy pamiętać, że audyt wewnętrzny podatków w gminie ma dostarczyć kierownikowi jednostki ocenę kontroli zarządczej. Audyt wewnętrzny różni się od kontroli tym, iż w zasadzie nie jest samą kontrolą, a raczej stanowi system oceny oraz sprawowania kontroli". Dostarcza Kierownikowi Jednostki obiektywnej i niezależnej oceny kontroli zarządczej w zakresie wymiaru, ewidencji i egzekucji podatków po to, aby dać uzyskać racjonalne zapewnienie, iż funkcjonujące mechanizmy kontrolne pozwalają na prawidłową realizację zadania w zakresie pozyskiwania dochodów z tytułu podatków.

Najważniejszym krokiem do przygotowania planów audytu wewnętrznego jest analiza ryzyka. Zakres pracy audytora opiera się na ocenie istotności i ocenie ryzyka obszarów działalności organizacji, która będą podlegać audytowi.

W panelu poświęconym *„Audytowi planów strategicznych i rozwojowych"* uczestnicy spotkania wspólnie odpowiadali na pytania dotyczące między innymi zadań audytowych, dzielili się dobrymi praktykami w zakresie zarządzania strategicznego JST i wskazywali te najbardziej interesujące, i które warto zaproponować, jako kryteria do badań jednostce audytowej.

Podczas Konferencji Forum Kapitału i Finansów miała miejsce również debata panelowa poświęcona *„Audytowi bezpieczeństwa informacji"*. Dyskusja toczyła się wokół następujących tematów:

1. Jak tak naprawdę wygląda rzeczywistość w zakresie cyberbezpieczeństwa urzędów?
2. Kto może mieć interes by zaszkodzić bezpieczeństwu informacji w urzędach?
3. Jakie są najbardziej oczywiste a także najgroźniejsze scenariusze?

4. Jakie rodzaje informacji przede wszystkim należy chronić?
5. Jakie są potencjalne skutki wycieku tych informacji?
6. Czego oczekują samorządy by lepiej zarządzać bezpieczeństwem informacji?
7. Jakie są kluczowe czynności by wdrożyć i utrzymywać skutecznie działający system zarządzania bezpieczeństwem informacji?
8. Czego oczekiwać od osób odpowiedzialnych za wdrożenie SZBI w urzędzie? Kto to powinien wykonywać?
9. Co jest największą przeszkodą dla ochrony informacji?

Eksperci zastanawiali się wspólnie jak sprawić by było „lepiej i bezpieczniej" akcentowali, że jest potrzeba szerokiej komunikacji z najwyższą kadrą zarządzającą w zakresie zapewniania bezpieczeństwa informacji. Podkreślano, że częste zmiany kadrowe powodują odpływanie wiedzy. Została również zwrócona uwaga na potrzebę przyjrzenia się przez NIK kwestii wynagrodzenia informatyków w urzędach, co ma wpływ na to, na ile doświadczone są osoby pełniące kluczowe role dla powszechnego bezpieczeństwa.

Dostrzeżono także rolę samej NIK, jako niejakiego „straszaka", który mobilizuje najwyższe kierownictwo do działania na rzecz bezpieczeństwa informacji. Rozmówcy zwrócili również uwagę na potrzebę opracowania jednolitych ram zarządczych w zakresie ochrony administracji samorządowej w całym kraju. Opracowanie jednolitych szablonów - wytycznych dotyczących tego jak przeprowadzać analizę ryzyka w powtarzalnych jednostkach typu urząd miasta, gminy. a następnie wytycznych jak wdrażać spójny system zarządzania bezpieczeństwem, byłaby zdaniem rozmówców i licznie zgromadzonej publiczności bardzo zasadne.

W czasie panelu uczestnicy Konferencji poznali plany Ministerstwa Cyfryzacji, do których zobowiązano się po opublikowaniu poprzedniego raportu Najwyższej Izby Kontroli w zakresie cyberbezpieczeństwa i zastanawiali się jak wprowadzenie w życie tych kwestii wpłynie na zarządzanie bezpieczeństwem informacji.

Licznie zgromadzeni uczestnicy podkreślali, że sporo pracy czeka jeszcze administrację publiczną, by zapewnić należyty poziom ochrony. Wszyscy jednak mają nadzieję, że stanie się to już niedługo, niemniej w pierwszej kolejności niezbędne będzie posiadanie podstawowych środków finansowych na zabezpieczanie cennych informacji.

Głównym motywem przewodnim panelu Audyt Informatyczny, było wskazanie, że audyt IT nie jest równoznaczny z audytem zgodności z ustawą o ochronie danych osobowych. Nie sprowadza się tylko do przeglądu procedur i instrukcji ochrony danych osobowych, które oczywiście mogą być elementem tego audytu. Obejmuje szerokie spektrum zagadnień takich jak:

1. Czy hasła używane są trudne do złamania, w jaki sposób i gdzie zachowane są informacje dotyczące haseł?
2. Kto i jak informacje o hasłach weryfikuje?
3. Czy (Access Control List ACL) przedstawiają realny obraz sytuacji z informacjami, kto ma dostęp, do jakich zasobów? Czy dostępne są logi serwerów?
4. Czy sposoby zabezpieczenia sieci informatycznej są odpowiednie?
5. Czy firma nie korzysta z jakichkolwiek niepotrzebnych aplikacji i usług informatycznych?
6. Czy systemy operacyjne i aplikacje maja wgrane najnowsze aktualizacje?
7. W jaki sposób i gdzie przechowywane są media z back-up'u? Kto ma do niego dostęp? Czy jest aktualny?
8. Czy jest plan odtworzenia systemu po katastrofie (disaster recovery)? Czy kierownictwo firmy zna go oraz wie jak postępować w takiej sytuacji?
9. Czy firma posiada właściwe narzędzia do szyfrowania danych? Czy narzędzia do szyfrowania danych są właściwie skonfigurowane?
10. Czy aplikacje stworzone dla organizacji zostały stworzone i wdrożone zgodnie z polityką bezpieczeństwa firmy?
11. W jaki sposób zostały przetestowane aplikacje stworzone dla firmy? Czy firma posiada i gdzie raporty z przeprowadzonych testów bezpieczeństwa?

Dyskusja w czasie panelu dała potwierdzenie, iż temat dobrych praktyk wykorzystania audytu wewnętrznego w podnoszeniu sprawności JST w obszarze IT jest ważnym aspektem do rozmów i przedstawiania przykładów.

Tegoroczna konferencja była okazją do wymiany doświadczeń i dyskusji ekspertów i sympatyków audytu. Stała się już po raz drugi miejscem do spotkań i rozmów o audycie w JST.

Anna Janiszewska [*],
Katarzyna Celińska [**]

VI Konferencja Finansowa IIA Polska

Audytorzy wewnętrzni z sektora usług finansowych **już po raz szósty spotkali się 12 października 2016 roku**, na konferencji finansowej organizowanej przez Instytut Audytorów Wewnętrznych IIA Polska. Tematem tegorocznej konferencji był **"Audyt wewnętrzny i jego relacje z interesariuszami".**

W czasie spotkania mieliśmy możliwość uczestniczyć w bardzo interesujących panelach w czasie, których poruszane były tematy związane z rolą audytu wewnętrznego w organizacji i jego wpływu na jej funkcjonowanie. Podsumowaniem panelu był wniosek: audytorzy wewnętrzni, aby mogli skutecznie wypełniać swoją rolę w organizacji powinni być włączeni w najważniejsze procesy zachodzące w firmie.

Audytor wewnętrzny, niezależnie od tego, czy ma być zaufanym doradcą, czy ograniczać się jedynie do udzielania zapewnienia, powinien cechować się odwagą w ocenie zasobów, kompetencji umieć ten stan zakomunikować kierownictwu i radzie. Podniesione zostało również, że to aktywne uczestniczenie audytora w procesach biznesowych, z zachowaniem jego obiektywizmu, rozwija audytora, poprzez wzrost świadomości istnienia ryzyka w prowadzeniu biznesu.

Autor zdjęcia: : Katarzyna Celińska, IIA Polska.

* Koordynator BKF IIA Polska.
** IIA Polska.

Dyskusja panelowa stała się istotną częścią spotkania angażującą wszystkich uczestników konferencji do dużej aktywności oraz kierowania bezpośrednich pytań do zaproszonych ekspertów.

W czasie spotkania mieliśmy również okazję wysłuchać prelekcji Adama Piołunowicza o etyce, zdaniem, którego istnieją profesje, których istotną częścią jest zaufanie klienta a wynika to z delikatności poruszanych kwestii w relacjach klient – profesjonalista, oraz pozornego konfliktu interesów, w jakim znajduje się profesjonalista. Takie profesje to: prawnik, lekarz, audytor wewnętrzny i biegły rewident. Z uwagi na informacje, do których mają dostęp wymienieni profesjonaliści, niezwykle ważne jest ich etyczne postępowanie.

Podczas spotkania mieliśmy okazje wysłuchać również prezentacji Ewy Jakubczyk-Cały, Prezesa Zarządu PKF Consult, Członka KIBR, dotyczącej zmian w przepisach o Komitetach Audytu uregulowanych projektem nowej ustawy o biegłych rewidentach oraz wynikających z niej nowych ryzykach, które powinny zostać uwzględnione w analizie ryzyka, poprzedzającej tworzenie planu rocznego.

Kolejny panel poświęcony był dyskusji o raportowaniu niefinansowym i wpływie, jaki zmiany w prawie mogą wywrzeć na organizację, jej funkcjonowanie i rolę audytu wewnętrznego, wzięli w nim udział Liliana Anam CSR Info, Olga Petelczyc Wiceprezes IIA Polska a także Ewa Sowińska Zastępca Prezesa KIBR.

Sebastian Burgemejster*

Konferencja XII POLCAAT

Dnia 22 listopada 2015 r. odbyła się już XII konferencja PolCAAT. IIA Polska kontynuuje 12 letnią tradycję wsparcia audytorów wewnętrznych w obszarach związanych z technologiami IT. Tym razem cała konferencja skupiała się na zmianach prawnych oraz zgodności, edukacji i wiedzy, wykorzystaniu narzędzi oraz zarządzaniu cyberbezpieczeństwem w łańcuchu dostaw, a motywem przewodnim był temat „Nowoczesny audyt wewnętrzny jako firewall następnej generacji".

Konferencja została objęta **honorowym patronatem Ministerstwa Cyfryzacji. Partnerem konferencji było OWASP (OWASP – z ang. Open Web Application Security Project – jest globalną, profesjonalną fundacją, działającą charytatywnie (non-profit), otwartą dla każdego, kto interesuje się zabezpieczeniami w oprogramowaniu. Główną ideą stowarzyszenia jest poprawa bezpieczeństwa aplikacji webowych.). Patronatem medialnym konferencję objęli Infor.pl, IT Professional, IT w Administracji, Dziennik Internautów oraz Sekurak.pl.**

Autor zdjęcia: : Katarzyna Celińska, IIA Polska.

* Prezes IIA Polska.

Konferencja była podzielona na cztery główne obszary przewodnie: zmiany prawne i zgodność, wykorzystanie narzędzi, łańcuch dostaw oraz edukacja i wiedza.

W obszarze zmiany prawne i zgodność Michał Grzybowski, Dyrektor wykonawczy Fundacji Bezpieczna Cyberprzestrzeń omówił nowe wyzwania, jakie czekają Polskę oraz organizacje podlegające pod Dyrektywę NIS. Wskazał na główne uprawnienia i odpowiedzialności uczestników procesu, struktury raportowania oraz słabości i niedociągnięcia dyrektywy.

Następnie Andrzej Szyszko, Koordynator Wydziału Strategii i Współpracy Międzynarodowej, Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji omówił założenia projektu wdrażającej Dyrektywę NIS ustawy o cyberbezpieczeństwie RP. Wskazał, jakie podmioty będą podlegały pod nowo projektowany system cyberbezpieczeństwa, jakie będą ich zadania oraz opisał całą strukturę raportowania. Dodatkowo wskazał na już rozpoczęte działania koordynacji kwestii cyberbezpieczeństwa w RP na przykładzie dobrych praktyk wypracowanych podczas Szczytu NATO oraz Światowych Dni Młodzieży w 2016 roku.

W kolejnym wystąpieniu Maciej Kołodziej, Wiceprezes Stowarzyszenia Administratorów Bezpieczeństwa Informacji (SABI) wprowadził uczestników w arkana zmian dotyczących ochrony danych osobowych wynikających z wprowadzeniem rozporządzenia GPDR (RODO). Wskazał na różnice w dotychczasowym podejściu do ochrony danych osobowych oraz akcent położył w swoim wystąpieniu na znaczące zagrożenia i wyzwania, jakie niesie ono dla wszystkich podmiotów przetwarzających dane osobowe. Największymi różnicami są m.in.: budowa całościowego systemu ochrony danych osobowych, wbudowanego w systemy organizacji, zmiana wymogów dotyczących zgody na przetwarzanie danych oraz wymogów informacyjnych, podwyższenie wymogów ochrony systemów IT, podniesienie rangi ABI (w RODO IBI), obowiązek informacyjny o wystąpieniu incydentu oraz wprowadzenie kar od obrotu.

Na zakończenie tego bloku programowego Pan Artur Miękina, Ekspert Polskiej Izby Informatyki i Telekomunikacji, Asseco Data System S.A. omówił jakie konsekwencje będzie miało wdrożenie rozporządzenia eIDAS dla rynku transakcji elektronicznych. Rozporządzenie ustanowiło dla całej UE ramy prawne dla takich usług jak: podpisy elektroniczne, pieczęci elektroniczne, elektroniczne znaczniki czasu, dokumenty elektroniczne, usługi potwierdzonych doręczeń elektronicznych oraz usługi certyfikacyjne do celu uwierzytelniania witryn internetowych. Rozporządzenie eIDAS wprowadziło nowy rozdział w budowaniu usług administracji publicznej.

W bloku wykorzystanie narzędzi otwierającą prezentacją było wystąpienie Pana Andrzeja Brągiela, IIA Polska, Audytora Wewnętrznego Ministerstwa Rodziny, Pracy i Polityki Społecznej. W swojej prezentacji omówił on historię hackingu oraz rozwój narzędzi do hackowania, w tym w szczególności Kali Linuksa. Przedstawiono szczegółowo możliwości poszczególnych wersji oprogramowania oraz dostępne aplikacje do wykonywania specyficznych rodzajów ataków.

W kolejnej prezentacji Michał Sajdak, CISSP, CEH, CTT+, IT Security Consultant – Securitum przedstawił pokaz Live hackig urządzeń sieciowych. Przedstawiono „bardzo proste" metody wyszukiwania urządzeń dostępnych w sieci Internet oraz zdalne uruchamianie kodu poprzez błędy w kodzie, które pozostawiono na etapie projektowania oprogramowania.

Ostatnim wykładem z tego bloku i wstępem do kolejnego było omówienie wykorzystania standardu ASVS w definiowaniu i weryfikowaniu bezpieczeństwa oprogramowania. Prezentację przedstawił Wojciech Dworakowski, Chapter Leader OWASP Poland, Prezes Securing. Na przykładach wskazał na błędy w niewłaściwym definiowaniu wymagań dla aplikacji, co skutkowało incydentami bezpieczeństwa. Prowadzący zaprezentował w jaki sposób dzięki standardowi ASVS można było uniknąć w/w błędów oraz dlaczego projektowanie, a później weryfikacja oprogramowania podnosi poziom bezpieczeństwa.

W ramach bloku zarządzania cyberbezpieczeństwem w łańcuchu dostaw odbył się panel z udziałem ekspertów: Jan Anisimowicz, Dyrektora w grupie C&F odpowiedzialnego za produkt AdaptiveGRC, Mirosława Błaszczaka, Dyrektora IT w grupie OpusCapita, Wojciecha Dworakowskiego, Chapter Leader OWASP Poland, Prezesa Securing oraz Pawła Kurzelewskiego, Global Information Security Manager w grupie QuintilesIMS. Panel moderował Jakub Syta, CISA, CISSP, CRISC, CISM, niezależny ekspert ds. cybersecurity. W trakcie panelu zaproszeni goście dyskutowali o roli zaufania w wyborze dostawcy, sposobach weryfikacji dostawcy (arkusze ryzyka, audyt na miejscu) oraz roli certyfikacji w ocenie dostawcy.

Blok edukacja i wiedza w cyberbezpieczeństwie rozpoczął się od wystąpienia Adama Haertle, CISA, CRISC, IT Security Officer. Wskazał on, iż głównym zagrożeniem dla infrastruktury krytycznej są wiewiórki oraz ptaki. Dotychczas nie odnotowano znaczącej ilości ataków, których skutki w rozległym stopniu ograniczyłyby usługi dla obywateli lub Państw. W prezentacji na konkretnych przykładach przedstawiono obecnie najczęstsze cyberzagrożenia tj. ransomware, malwersacje związane z błędami w architekturze rozwiązań bankowo – telekomunikacyjnych oraz błędami w systemie bankowym.

Na zakończenie konferencji odbył się panel dyskusyjny, w którym zaproszeni eksperci dyskutowali o zarządzaniu wiedzą w obszarze cyberbezpieczeństwa. Uczestnikami panelu byli: Adam Haertle, CISA, CRISC, IT Security Officer, Sebastian Burgemejster, CISA, CCSA, CGAP, CRMA, CSX, Prezes IIA, Andrzej Szyszko, MCSA, MCITP, CCNA, ITIL, PRINCE2, audytor wiodący SZBI, Koordynator Wydziału Strategii i Współpracy Międzynarodowej, Departament Cyberbezpieczeństwa, Ministerstwo Cyfryzacji oraz Eryk Trybulski, Certyfikowany audytor systemów informatycznych, CSO w Soflab sp. z o.o. Moderatorem panelu była Agnieszka Boboli, CISA, Pełnomocnik ds. IT IIA Polska. Eksperci poruszyli tematykę pozyskiwania wiedzy o cyberbezpieczeństwie, threat inteligence, narzędziach wspomagających zarządzanie wiedzą, propagowaniu wiedzy w organizacjach oraz o podstawowych elementach budowy systemów oraz słabościach w ich projektowaniu i utrzymywaniu.

Renata Pradela*,
Anna Królak,**
Andrzej Bojanek*.**

Audyt w praktyce, podsumowanie spotkania szkoleniowego w Karpaczu

W dniach 20-21 października 2016, z inicjatywy 5 kół regionalnych: Dolnośląskiego, Śląskiego, Poznańskiego, Łódzkiego i Lubelskiego oraz Koła Audytorów Wewnętrznych JST IIA Polska odbyło się spotkanie szkoleniowe dla członków i sympatyków Instytutu Audytorów Wewnętrznych IIA Polska. Ten prekursorski, oddolny projekt szkoleniowo-integracyjny był możliwy dzięki patronatowi i dofinansowaniu przez Zarząd IIA Polska, a także społecznemu zaangażowaniu prelegentów i koordynatorów kół, jako organizatorów.

Na miejsce spotkania koordynatorzy wybrali Dolny Śląsk, miasto Karpacz, u podnóża królowej Karkonoszy - Śnieżki, bo piękniejsze od Karkonoszy jesienią, mogą być tylko Karkonosze zimą.

Spotkanie, które było podzielone na kilka podstawowych bloków tematycznych, urozmaiconych dodatkowymi tematami z zakresu praktyki audytu wewnętrznego poprowadziła Renata Pradela.

Inauguracyjny temat pierwszego dnia szkoleniowego: *Skuteczne programy etyczne wsparciem audytu wewnętrznego*, zaprezentowały Zuzanna Dobrowolska i Anna Wojciechowska-Nowak, doświadczone trenerki z firmy LINIA ETYKI, specjalizującej się m.in. we wdrażaniu kodeksów etycznych oraz promowaniu szeroko pojętej etyki biznesu. Program etyczny jako proces i to szyty na miarę, może być dla audytora punktem odniesienia. Czy ma zawierać podstawowe zasady i ogólne wartości, a szczegóły mają doprecyzowywać polityki, zależy od dojrzałości etycznej oraz charakteru firmy. Ważne, by program obejmował także klienta zewnętrznego, np. dostawców, odbiorców, czy społeczności lokalne. O kryteriach oceny i narzędziach badawczych stosowanych w audycie etycznym mówiła również Jolanta Sałęga[1]. Audyty etyczne stanowią nowy obszar działalności audytorów wewnętrznych w jednostkach sektora finansów publicznych, który jest przede wszystkim obszarem wymagającym pionierskich rozwiązań w zakresie zdiagnozowania stanu świadomości etycznej pracowników jednostki, zidentyfikowania występowania zjawiska nieetycznych praktyk oraz skali tego zjawiska, oceny systemu kontroli zarządczej w tym obszarze oraz opracowania rekomendacji, mających udoskonalić obszar w którym stwierdzone zostały słabości systemu.

* Koordynator Dolnośląskiego Koła Regionalnego IIA Polska.
** Koordynator Łódzkiego Koła Regionalnego IIA Polska.
*** Koordynator Lubelskiego Koła Regionalnego, Przewodniczący Komisji Rewizyjnej IAW IIA Polska.
1 Urząd Marszałkowski Województwa Śląskiego.

Tematem w czasie popołudniowych sesji stały się zagadnienia z zakresu oceny rozwiązań wprowadzonych rozporządzeniem wykonawczym w sprawie audytu wewnętrznego, którego podjęła się między innymi Anna Morow[1]. Temat ten, wciąż wzbudza wiele emocji i jest szeroko dyskutowany w gronie audytorów - praktyków, dlatego kontynuując ten wątek zagadnienia rozporządzenia wykonawczego, w kontekście podręcznika audytu wewnętrznego Katarzyna Lenczyk-Woroniecka[2] omówiła wątpliwości dotyczące praktycznego stosowania zapisów oraz wskazała zaprojektowane w nadzorowanej komórce rozwiązania, dotyczące wdrożenia wymogu udokumentowania pisemnego wyboru kryteriów oceny mechanizmów kontrolnych, monitorowania wykonania zaleceń i czynności sprawdzających. Omówiła także wzory dokumentów i zmiany w podręczniku audytu wewnętrznego wynikające z aktualizacji rozporządzenia.

Następnie Elżbieta Paliga[3] podzieliła się swoim doświadczeniem w budowaniu kwestionariuszy kontroli wewnętrznej w audycie podatków od środków transportu. Zwróciła uwagę na jakże ważne sprawdzenie poprawności algorytmów wpisanych w system dedykowany do rozliczania podatków, np. czy prawidłowo określono liczbę dni roboczych, uwzględniając święta.

Drugi dzień spotkania szkoleniowego również obfitował w interesujące tematy i ożywione dyskusje, które prowadziła Anna Królak[4], przede wszystkim zostały one zdominowane przez tematy związane z bezpieczeństwem informacji, ochrony danych osobowych i zamówieniami publicznymi, w różnych ujęciach.

Autor zdjęcia: Andrzej Bojanek, Koordynator Lubelskiego Koła Regionalnego IIA Polska.

1 Audytor, wieloletni praktyk w prowadzeniu kontroli wewnętrznych i zewnętrznych.
2 Urząd Marszałkowski Województwa Dolnośląskiego.
3 Urzad Miejski w Dąbrowie Górniczej.
4 Koordynator Łódzkiego Koła Regionalnego IIA Polska.

Blok dotyczący bezpieczeństwa informacji otworzył Andrzej Bojanek[1], który przedstawił temat istotny dla audytorów urzędów marszałkowskich pełniących funkcję Instytucji Zarządzających w PROW.: Temat wystąpienia: *Ocena prawidłowości realizacji zadań instytucji zarządzającej dla funduszy prow 2007-2013 w obszarze bezpieczeństwa informacji*. Podstawą do analiz audytorskich tego obszaru była norma ISO/IEC 27002, która szeroko bada bezpieczeństwo informacji w wielu aspektach: sprzętowym, dokumentacji, okablowania, czynności konserwacyjnych, systemów wspomagających technicznie, wymóg stosowania klimatyzacji, zabezpieczeń przeciwpożarowych, przygotowanie kompetencyjne, szkolenia merytoryczne pracowników realizujących ten obszar w Programie Rozwoju Obszarów Wiejskich.

Pozostając w nurcie tematycznym Olga Reyzz-Rubini[2]**,** zaprezentowała temat audyt bezpieczeństwa informacji, w ujęciu praktycznym: jak przygotować się do audytu nie będąc informatykiem, jak przeprowadzić wstępny przegląd, sporządzić program audytu, zidentyfikować ryzyka, wykonać audyt krok po kroku i zinterpretować jego efekty.

Ważnym aspektem poruszonym w czasie rozmów było również omówienie przez Jolantę Gasiewicz[3], na co powinien zwrócić uwagę audytor w audycie ochrony danych osobowych oraz, iż audyt warto rozpocząć od zidentyfikowania wybranego w organizacji modelu ochrony danych osobowych, tj. «z powołanym ABI» czy «bez powołanego ABI», ponieważ będzie to determinowało dalsze zadania i obowiązki po stronie administratora danych, które należałoby zweryfikować w trakcie audytu. Jednocześnie, warto zacząć już teraz przygotowywać się do zweryfikowania i wdrożenia wymagań z przyjętego przez UE Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, tzw. RODO, którego stosowanie będzie obligatoryjne od maja 2018 roku i wprowadzi wysokie administracyjne kary pieniężne.

Blok obejmujący tematykę zamówień publicznych reprezentowali Paweł Gad[4], omawiający prelekcję pod tytułem: Testy zgodności i wiarygodności w audycie zamówień - omówienie wyników testów oraz Piotr Komenda[5], w temacie: Proces identyfikacji i analizy ryzyka w obszarze zamówień publicznych przy zastosowaniu diagramu Ishikawy. Ciekawe tematy, pozwoliły od praktycznej strony spojrzeć na proces udzielania zamówień publicznych i wzbudziły bardzo duże zainteresowanie, przejawiające się licznymi pytaniami, ze strony słuchaczy.

Warto również podkreślić, iż tematami uzupełniającymi w drugim dniu spotkania były:

- Audyt wewnętrzny w szpitalu, prezentowany przez Annę Koźmińską[6] oraz Monikę Jankowska[7], - Czynności sprawdzające realizację rekomendacji – przykłady dokumentacji audytowej, prezentowany przez Roberta Lipkę[8].

1 MBA, CGAP, Koordynator Lubelskiego Koła Regionalnego, Przewodniczący Komisji Rewizyjnej IAW IIA Polska.

2 II Wiceprezes, Członek Zarządu IIA Polska Certyfikowany Audytor Wewnętrzny (CIA) oraz audytor Systemu Bezpieczeństwa Informacji zgodnie z ISO 27001 i ISO 9001.

3 Trener i praktyk w zarządzaniu bezpieczeństwem informacji oraz ochronie danych osobowych.

4 Pracownik Biura Audytu Wewnętrznego Urzędu Miejskim w Dąbrowie Górniczej.

5 Wieloletni praktyk w zakresie zamówień publicznych i zarządzania ryzykiem, reprezentujący Urząd Marszałkowski Województwa Śląskiego.

6 Specjalista ds. kontroli w Starostwie Powiatowym w Krotoszynie.

7 Współwłaścicielka firmy doradczej Business Watch, z wieloletnim stażem w audycie wewnętrznym w sektorze prywatnym i publicznym oraz koordynatorka Wielkopolskiego Koła Regionalnego IIA Polska.

8 Koordynatora Śląskiego Koła Regionalnego IIA Polska. Koordynator, Audytora Wewnętrznego Urzędu Marszałkowskiego Województwa Śląskiego.

Z rozmów i wrażeń przekazywanych przez uczestników szkolenia jego organizatorom wynika, że była to inicjatywa nader potrzebna, bardzo pouczająca, a jej aspekt integracyjny pozwolił na nawiązanie i utrwalenie nowych znajomości audytorskich. Koordynatorzy wspólnie zadeklarowali, że przedsięwzięcie to będzie miało swoją kontynuację w przyszłości.

Iwona Bogucka*

Recenzja książki „Zarządzanie projektami w administracji publicznej" autorstwa A. Jaskenis, M. Marczewska, M. Darecki, Wydawca PRESSCOM sp. z o.o., Wrocław 2015, s. 284

Jak zaplanować projekt, zorganizować jego wykonanie i sterować przebiegiem tak, aby terminowo i w ramach ustalonego budżetu osiągnąć wyznaczone cele? Jak zbudować kompetentny zespół? W jaki sposób eliminować typowe problemy podczas realizacji zadania projektowego w administracji publicznej?

Książka prezentuje teorię, metodykę oraz liczne przykłady zastosowania w praktyce technik i narzędzi zarządzania projektami przez jednostki administracji publicznej.

W opracowaniu poruszone zostały zagadnienia dotyczące m.in.:

1. Planowania, organizowania i sterowania przebiegiem projektu.
2. Zamknięcia projektu i wyliczania wartości uzyskanej EVM.
3. Doboru członków zespołu i komunikacji między nimi.
4. Zasad wyceny projektów i opracowywania realnych budżetów.
5. Sposobów reakcji na pojawiające się ryzyko.
6. Zasad przygotowania SIWZ, która zagwarantuje poprawność wykonania zleconych zamówień.
7. Kontroli projektów realizowanych przez osoby i podmioty zewnętrzne.
8. Kwestie związane z otoczeniem informatycznym, w tym wprowadzanie do programu ProjectLibre.

Publikacja została dodatkowo wzbogacona w liczne schematy, tabele i rysunki. Będzie szczególnie przydatna podczas realizacji przez jednostki administracji publicznej projektów: budowlanych, informatycznych, promocyjnych, edukacyjnych, organizacyjnych oraz badawczo – rozwojowych. Projekty natomiast są coraz częściej realizowanymi działaniami pozwalającymi organizacjom na osiągnięcie ich długoterminowych celów. Dynamicznie zmieniające się otoczenie, nakazuje organizacjom podejmowanie działań ukierunkowanych na osiągnięcie unikalnych celów i niepowtarzalnych rezultatów –

* Członek Zarządu IIA Polska, Redaktor Naczelna Magazynu „Audyt i Zarządzanie".

określonych pod względem czasu i kosztów realizacji, – jakimi mogą być zarówno produkty czy usługi, jak i inne różnorodne rozwiązania.

Zdaniem autorów sprawne i skuteczne zarządzanie projektami przyczynia się do osiągnięcia przez organizację wymiernych korzyści oraz daje im możliwości sprostania potrzebom i oczekiwaniom ich kluczowych interesariuszy. Książka ta łączy zagadnienia techniczne i społeczne związane z realizacją projektów. Tym samym odnosi się ona zarówno do technicznych aspektów realizacji projektów, tj. planowania, organizowania, sterowania przebiegiem projektu i jego zamknięcia, jak i do kwestii społecznych, które dotyczą budowy zespołu projektowego, kierowania zespołem projektowym, zarządzania konfliktami i interesariuszami w ramach projektu.

Publikacja składa się z sześciu rozdziałów. Pierwszy poświęcony zagadnieniom teoretycznym i filozofii zarządzania oraz istotę zarządzania projektami. Drugi poświęcony jest zagadnieniom związanym z planowaniem projektowym: definiowanie, inicjowanie, przygotowanie projektów. Następne poświęcone są zagadnieniom budowy zespołu projektowego. W czwartym autorzy zwracają uwagę na problemy i ryzyka typowe dla zarządzania projektami. Ostatni rozdział poświęcony jest możliwościom zarządzania projektami przy zastosowaniu narzędzi komputerowych.

W książce autorzy zwracają uwagę na coraz bardziej powszechną sytuację, w której organizacje działają wyłącznie przez projekty, rezygnując z innych typów podejmowanych działań, i wskazują, w jaki sposób zarządzać wieloma projektami jednocześnie i korzystać z doświadczeń projektowych

Książka jest adresowana przede wszystkim do osób pracujących w szeroko pojętej administracji publicznej, których praca w coraz większym stopniu polega na planowaniu i realizacji projektów. Wyposaża czytelnika w niezbędną i szeroką wiedzę o zarządzaniu projektami oraz pomaga mu kształcić umiejętności stosowania wybranych technik, metod i narzędzi zarządzania projektami.

informacje dotyczące promocji i reklamy

Zapraszamy do reklamowania Państwa produktów oraz usług na łamach Magazynu Instytutu Audytorów Wewnętrznych IIA Polska.

Wszystkie potrzebne informacje na temat reklamy w Magazynie do uzyskania u osoby kontaktowej w Biurze IIA Polska:

Renata Zysiak
Email: office@iia.org.pl
Tel./fax: +48 (22) 110 08 13

Instytut Audytorów Wewnętrznych IIA Polska
ul. Świętokrzyska 20 (pokój 508, V piętro).
00-002 Warszawa

Zgodnie z postanowieniami Dyrektywy Administracyjnej Nr 4 IIA Global – 2011 wkład do publikacji powinien dotyczyć głównych zagadnień związanych z posiadanym certyfikatem lub zakresu związanego z CBOK, oraz lub ogólnego zakresu tematycznego certyfikatów specjalistycznych. Opublikowane książki lub artykuły niezwiązane bezpośrednio z audytem wewnętrznym będą akceptowane, o ile osoba certyfikowana jest w stanie udowodnić, że te działania przyczyniają się do biegłości w zawodzie audytora.

CIA	CCSA	CSFA	CGAP	CRMA
Maksymalna liczba przyznanych godzin 25			Maksymalna liczba przyznanych godzin 10	
Ogólnie jedna strona publikacji z pojedynczym odstępem jest równa 2 godzinom CPE, jednak w ramach poniższych limitów:				
Książki – 25 godzin CPE			Książki – 12 godzin CPE	
Artykuły – 15 godzin CPE			Artykuły – 6 godzin CPE	
Opisy badań – 15 godzin CPE			Opisy badań – 6 godzin CPE	

Wymogi redakcyjne do nadsyłanych tekstów do magazynu IIA:

1. Układ artykułu (tekst Times New Roman 12 odstęp między wierszami pojedynczy):
   a) Informacja o autorze (imię nazwisko, stanowisko, miejsce pracy, adres email itp.)
   b) Tytuł
   c) Cel
   d) Wstęp
   e) Kolejno ponumerowane rozdziały
   f) Krótkie streszczenie,
   g) Słowa klucze
   h) Bibliografia
2. Przypisy do tekstu na każdej stronie (odesłanie do autora i strony patrz Bibliografia (wielkość czcionki 9 Times New Roman).
3. Rysunki w formie edytowalnej z odesłaniem do źródła, np. Tabela nr (źródło kursywą 10 Times New Roman) źródło: opracowanie na podstawie Nowak J., Perspektywy rozwoju audytu, Wydawnictwo PTM, Warszawa 2016, s. 12-16.
4. Tabele w formie edytowalnej z odesłaniem do źródła jak wyżej.
5. Wykresy patrz jak wyżej.
6. Bibliografia np. Nowak J., Perspektywy rozwoju audytu, Wydawnictwo PTM, Warszawa 2016, (tekst Times New Roman 12 odstęp 1,0).
7. Terminy nadsyłania tekstów do każdego 15 drugiego miesiąca kwartału.

8. Artykuły przesłane do druku, po uzyskaniu pozytywnych recenzji, zostaną wydrukowane w magazynie w języku polskim. Objętość tekstu maksymalnie do pół arkusza wydawniczego (20 000 - 22 000 znaków – około 10 stron).
9. Autorzy tekstów zakwalifikowanych do druku otrzymają punkty CPE zgodnie Dyrektywą Administracyjną nr 4 IIA Global- 2011.

Więcej informacji na www.iia.org.pl.