AUDYT I ZARZĄDZANIE

MAGAZYN IIA

Magazyn Instytutu Audytorów Wewnętrznych IIA Polska, Kwartalnik numer 3 (17)2017

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

Bogumiła Bujska[1]

Burzymy silosy… budujemy procesy

Wyższość podejścia procesowego nad „silosowym" w zarządzaniu ryzykiem w organizacji

Współczesne organizacje najczęściej podzielone są na piony, działy, zespoły, czy inne komórki organizacyjne. Zdarza się, że część jednostek skoncentrowana jest na własnych zadaniach i celach, nie współpracuje z innymi zespołami. Pracownicy wykonują swoje zadania automatycznie i dla siebie samych – w taki sposób, jakby ich praca służyła tylko im samym i nie wpływała na działania innych poza ich zespołem. Taką praktykę możemy nazwać „myśleniem silosowym".

Organizacyjne „silosy" zacierają rozumienie wspólnego celu firmy, pracownicy nie wiedzą, jakie znaczenie ma efekt ich działania, ani, jakie ma to przełożenie na pracę innych komórek organizacyjnych. Ponieważ nie mają wglądu do informacji dostępnych w innych zespołach, tracą czas na tworzenie własnych danych. W konsekwencji, taka praktyka prowadzi do dublowania oraz rozproszenia informacji w organizacji, co znacznie utrudnia skuteczne zarządzanie ryzykiem.

Charakterystyczne dla „organizacji silosowej" jest również to, że wyodrębnianie ryzyk w poszczególnych komórkach organizacyjnych odbywa się bez rozumienia celu instytucji, co dodatkowo komplikuje fakt, że komórki organizacyjne mają różne, często sprzeczne ze sobą, cele. Zarządzanie wszystkimi ryzykami oddzielnie w poszczególnych jednostkach organizacyjnych bez uwzględnienia współzależności pomiędzy różnymi rodzajami ryzyka, zwiększa również koszty wprowadzanych zabezpieczeń. Największy problem pojawia się na stykach komórek organizacyjnych, w punktach, gdzie efekt pracy jednego zespołu przekazywany jest do drugiego zespołu. W tym miejscu dobre zarządzanie ograniczone jest przez brak jednoznacznie wskazanej odpowiedzialności za ryzyko, które się tu pojawiło. Jednocześnie brak komunikacji i współpracy między komórkami organizacyjnymi, powoduje, że zarządzanie ryzykiem nie służy osiągnięciu celów organizacji.

Rozwiązaniem problemu jest zburzenie „silosów" i zamiana ich na procesy. Kiedy czynności wykonywane przez poszczególne jednostki organizacyjne ułożymy w jeden logiczny łańcuch, łatwiej będzie dostrzec, że wszyscy mają jeden wspólny cel. Proces złożony z uszeregowanych czynności łączy pracowników z niezależnych komórek organizacyjnych w grupy pracujące nad wspólnym celem, komunikujących się ze sobą i przede wszystkim świadomych tego, jak ich praca wpływa na pracę innych.

Zarządzanie ryzykiem w podejściu procesowym pozwala podejść całościowo do postrzegania ryzyka i umożliwia jego zrozumienie w całej organizacji. Określenie na samym

[1] Audytor Wewnętrzny PKO Finat – technologicznej Spółki z Grupy PKO Banku Polskiego, która specjalizuje się miedzy innymi w outsourcingu specjalistów IT.

początku celów, które będą jasne dla wszystkich uczestników procesu, pozwoli zidentyfikować zdarzenia, które mogłyby przeszkodzić w ich osiągnięciu. Zbudowanie świadomości pracowników, jak realizacja ich zadań wpływa na działania innych, pozwala na skuteczną samokontrolę własnej pracy. To z kolei przekłada się na minimalizację liczby błędów w procesie, zmniejszenie czasu jego trwania oraz redukcję kosztów osiągnięcia celu. Podejście procesowe ułatwia skuteczną komunikację, co jest niezbędne dla dobrego zarządzania ryzykiem w organizacji. Całościowe podejście do ryzyka pozwala też na uwzględnienie zależności pomiędzy różnymi rodzajami ryzyka, co w konsekwencji wiąże się z obniżeniem kosztów wprowadzenia zbędnych i drogich zabezpieczeń w skali całej organizacji. Określenie właściciela procesu ułatwia „znalezienie" właściciela ryzyka, odpowiedzialnego za zarządzanie danym ryzykiem.

Podejście procesowe nie tylko pomaga dobrze zarządzać ryzykiem w organizacji, ale pozwala także zaoszczędzić czas i zmniejszyć koszty, jakie firmy ponoszą zarządzając ryzykiem w organizacji silosowej. Warto grać do jednej wspólnej bramki.

Katarzyna Lenczyk-Woroniecka[2], Małgorzata Krystek[3]

Audyt etyczny- studium przypadku

Cel

Celem artykułu jest przybliżenie tematyki audytu w obszarze etyki na przykładzie praktycznym jednostki samorządu terytorialnego. Obszar etyczny stanowi istotną część systemu zarządzania jednostką i wiele instytucji coraz większą wagę przykłada do zagadnień obejmujących przyjęte normy zachowania, czy wartości. Wyznaczenie przez kierownictwo norm postępowania nie jest już tylko prawnym wymogiem kontroli zarządczej, ale staje się powoli samoistną potrzebą uporządkowania w każdej organizacji przyjętych wzorów akceptowalnych zachowań w obszarze tak subtelnej materii jaką jest kultura osobista.

Wstęp

Słowo **etyka** pochodzi od greckich słów *ethikos* – **zwyczajny,** oraz *etos* – **obyczaj, zwyczaj.** Etyka jest więc zespołem norm charakterystycznych dla danej organizacji, przy czym kluczową rolę lidera zachowań etycznych pełni jej kierownictwo. Popularne powiedzenia „ryba psuje się od głowy" i „przykład idzie z góry" najlepiej obrazują wpływ zachowań szefów na zachowania pracowników w organizacji. Dopuszczalność pewnych nieakceptowanych społecznie zachowań rzutuje na działalność organizacji powodując okazje korupcyjne, zachowania mobbingowe wobec pracowników, fałszowanie dokumentów, a także w skrajnych przypadkach może prowadzić do upadku firmy. Przez lata wiele przedsiębiorstw informowało tylko ustnie o swoich oczekiwaniach etycznych[4]. Okazało się, że tego typu rozwiązania są nie tylko nieskuteczne, ale przede wszystkim ignorowane. Po szeregu różnych afer finansowych zarówno w USA jak i w Europie zauważono, że zasady etyczne, zgodność i ład korporacyjny w przedsiębiorstwie pozwalają skutecznie chronić organizację przed łapownictwem i korupcją. Przy czym istotą dobrego funkcjonowania programu etycznego jest zachowanie pisemności oraz jego promocja.

Przyjęcie zarządzania biznesowego w realizację procesów i zadań budżetowych w Polsce stopniowo ewaluowało wprowadzając kolejno definicje kontroli wewnętrznej (nie instytucjonalnej), kontroli finansowej a na końcu kontroli zarządczej w środowisko prawne jednostek sektora finansów publicznych. Zmiana ustawy o finansach publicznych w 2009 roku[5] wprowadziła jako jeden z celów, który ma zapewniać prawidłowe funkcjonowanie jednostek, przestrzeganie i promowanie zasad etycznego postępowania. Praktycznie od tego momentu zarządzający jednostkami sektora publicznego musieli uwzględniać w swoich uregulowaniach aspekty etyczne jako istotny element kierowania.

[2] CGAP, Członek Zarządu IIA Polka, Dyrektor Wydziału Audytu Wewnętrznego UMWD.
[3] CGAP Audytor Wewnętrzny w Wydziale Audytu Wewnętrznego UMWD.
[4] Robert Moeller, Nowoczesny Audyt Wewnętrzny, Wyd. Wolters Kluwert Polska Sp. Z o.o., 2011, str. 663.
[5] ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (w brzmieniu Dz.U. 2009 Nr 157, poz. 1240).

Dlaczego audyt etyczny w organizacji

Istotą audytu jest wspieranie kierownictwa w procesie podejmowania decyzji oraz zapewnienie zgodności w wymogami. Audyty etyczne są więc szczególnym narzędziem wspomagającym wewnętrzne zarządzanie w obszarze zarządzania personelem. Z jednej strony prezentują pracownikom wartości wyznawane przez organizację oraz zobowiązania i konsekwencje z nich wynikające. Z drugiej dla kadry zarządzającej stanowią lustro własnych zachowań. Ponadto celem audytu aspektów etycznych jest informowanie kierownictwa o potencjalnych zagrożeniach związanych z etyką. Ujawnia on miejsca, w których struktura i procesy organizacyjne uniemożliwiają (pracownikom) właściwe postępowanie. Może również służyć do stwierdzania efektywności organizacji w dziedzinie etyki: w tym przypadku mierzone są skutki społeczne oraz wpływ na interesariuszy zewnętrznych.[6]

Dużo wskazówek w zakresie audytu etyki można znaleźć w Praktycznym przewodniku – Ocena programów i działań związanych z etyką[7], który zawiera wiele wskazówek, w tym pytań ankietowych, i który był również inspiracją w trakcie przeprowadzonego zadania. Cele audytu uzgodnione z kierownictwem miały odpowiedzieć na dwa zagadnienia:

1. Jaka jest **świadomość** obowiązywania w organizacji Kodeksu etyki?
2. zbadanie: Czy istnieje **potrzeba wprowadzenia w nim zmian.**

Kryteria oceny dla realizacji zadania związane ww. zagadnieniami uzgodniono z audytowanym:

1. Ocena świadomości obowiązywania kodeksu etyki wśród pracowników
   1) ustalenie i ocena podjętych działań w celu promocji kodeksu etyki,
   2) ankieta pracownicza zamieszczona w intranecie.
2. Ocena przyjętych i obowiązujących uregulowań w zakresie etyki - analiza uregulowań wewnętrznych.

Analiza uregulowań wewnętrznych

Zasady etyki w urzędzie przed wprowadzeniem Kodeksu wynikały głównie w ustawy o pracownikach samorządowych[8]. Podstawowe obowiązki pracownika: dbałość o wykonywanie zadań publicznych oraz o środki publiczne, z uwzględnieniem interesu publicznego oraz indywidualnych interesów obywateli określa w art. 24 ustawy o pracownikach samorządowych. Ustawa wymienia również enumeratywnie pozostałe obowiązki w tym wskazujące sposób postępowania, takie jak: zachowanie uprzejmości i życzliwości w kontaktach z obywatelami, zwierzchnikami, podwładnymi oraz współpracownikami oraz zachowanie się z godnością w miejscu pracy i poza nim.

[6] Sheena Carmichael, Ethical auditing: uncovering the shadow side of the organisation. Opublikowano w RSA Journal, lipiec 1997.
[7] Międzynarodowe Ramowe Zasady Praktyki Zawodowej (IPPF) Praktyczny przewodnik – Ocena programów i działań związanych z etyką, IIA Global, czerwiec 2012r.
[8] ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz. U. z 2016 poz.902 z późń. zm.).

Aktualny Kodeks Etyki Pracowników Urzędu został ustalony poprzez Zarządzenie Marszałka w grudniu 2012[9] roku i opublikowany na Intranecie jednostki. Określa i opisuje 7 zasad, którymi powinien kierować się pracownik Urzędu w realizacji powierzonych mu zadań i obowiązków:

1. ZASADA PRAWORZĄDNOŚCI

Pracownik wykonując powierzone mu zadania zachowuje należytą staranność z zastosowaniem uregulowań i procedur określonych w obowiązujących przepisach prawnych.

2. ZASADA UCZCIWOŚCI I RZETELNOŚCI

Pracownik wykonuje powierzone mu zadania bezstronnie, uczciwie i rozsądnie z zachowaniem odpowiedzialności za podejmowane decyzje; pracownik działa niezależnie, nie ulega żadnym naciskom, nie przyjmuje żadnych korzyści materialnych ani osobistych.

3. ZASADA UPRZEJMOŚCI

Pracownik w swoich kontaktach z obywatelami, przełożonymi, podwładnymi oraz współpracownikami zachowuje się właściwie, uprzejmie i życzliwie; w przypadku popełnienia błędu naruszającego prawa lub interesy Klientów pracownik przeprasza za to i stara się skorygować skutki popełnionego przez siebie błędu w jak najwłaściwszy sposób.

4. ZASADA JAWNOŚCI

Pracownik realizuje swoje zadania w sposób jawny z poszanowaniem prawa obywateli do informacji w oparciu o obowiązujące przepisy prawne i regulacje wewnętrzne Urzędu; jednocześnie pracownik jest zobowiązany do udzielania informacji w sposób jasny, zrozumiały i przejrzysty dla obywatela z uwzględnieniem sfery prywatności i nietykalności osobistej chroniąc dane osobowe w zakresie przewidzianym przepisami prawa, z zachowaniem tajemnicy państwowej, służbowej i bezpieczeństwa informacji; pracownik nie podejmuje żadnej pracy oraz zajęć, które kolidowałyby z obowiązkami służbowymi oraz wywołały uzasadnione podejrzenie o stronniczość lub interesowność.

5. ZASADA PROFESJONALIZMU

Pracownik wykonując powierzone mu zadania posiada wiedzę dotyczącą funkcjonowania Urzędu, podnosi kwalifikacje oraz rozwija wiedzę zawodową; Pracownik zna akty prawne dotyczące funkcjonowania Urzędu oraz zapoznaje się ze wszystkimi istotnymi okolicznościami faktycznymi i prawnymi prowadzonych przez siebie spraw; w wykonaniu zadań pracownik opiera się na rzeczowej argumentacji a w przypadku popełnienia błędów jest gotowy do przyjęcia krytyki, uznania ich i naprawienia konsekwencji z nich wynikających.

6. ZASADA GODNEGO ZACHOWANIA W MIEJSCU PRACY I POZA NIM

Pracownik wykonuje zadania z poszanowaniem zasad współżycia społecznego i godności innych osób, w tym zarówno przełożonych i podwładnych, jak i współpracowników, zachowując przy tym wysoki poziom kultury osobistej; relacje z obywatelami

[9] Zarządzenia Nr 125/2012 Marszałka Województwa Dolnośląskiego z 31 grudnia 2012 roku.

i współpracownikami opiera na życzliwości i przyjaznej atmosferze w pracy; wygląd i strój pracownika powinien być dostosowany do charakteru wykonywanej pracy oraz powagi Urzędu, w szczególności powinien być estetyczny, czysty i schludny; Pracownik powinien dbać również o czystość swojego stanowiska pracy; sprawując swoją funkcję pracownik Urzędu winien również właściwie zachowywać się poza pracą i unikać zachowań, które mogłyby mieć negatywny wpływ na wizerunek Urzędu.

7. ZASADA NIEDYSKRYMINOWANIA

Pracownik przy wykonywaniu zadań zobowiązany jest do równego traktowania wszystkich klientów; W przypadku różnic w traktowaniu pracownik powinien zapewnić, aby wynikało to z uzasadnionych i obiektywnych przyczyn wynikających z zakresu danej sprawy. W szczególności pracownik powinien unikać nieusprawiedliwionego nierównego traktowania obywateli ze względu na ich narodowość, rasę, płeć, kolor skóry, pochodzenie społeczne lub etniczne, cechy genetyczne, język, religię lub wyznanie, przekonania polityczne, przynależność do mniejszości narodowej, urodzenie, posiadaną własność, wiek, inwalidztwo lub preferencje seksualne.

Pracownicy na mocy Zarządzenia Marszałka wprowadzającego Kodeks zobowiązani są do przestrzegania przepisów Kodeksu i kierowania się jego zasadami. Zarządzenie określa, że nieprzestrzeganie zasad etyki skutkować będzie odpowiedzialnością służbową, jak za nieprzestrzeganie należytej organizacji i porządku w procesie pracy, lub karą dyscyplinarną określoną w ustawie o pracownikach samorządowych i Kodeksie Pracy. Aktualnie Kodeks Etyki nie wskazuje wprost ścieżki, procesu, mechanizmu postępowania w przypadku ewidentnego złamania ustalonych zasad. Pozostaje źródłem pożądanych wzorców zachowań. W ostatnich latach nie stwierdzono przypadków ukarania pracownika za nieprzestrzeganie zasad etyki określonych w Kodeksie.

Ocena promocji Kodeksu etyki

W celu dokonania oceny promocji Kodeksu Etyki przeanalizowano wewnętrzną stronę internetową organizacji oraz poproszono osobę odpowiedzialną za jej utrzymanie o udostępnienie statystyk. Kodeks publikowany jest na aplikacji intranetowej Urzędu – Intranet (w zakładce Baza Wiedzy – Dobre Praktyki i Procedury Przeciwdziałania Nadużyciom). Koncepcja wyodrębnienia zakładki o tym tytule wynikała z potrzeby zebrania w jednym miejscu artykułów, dokumentów zorientowanych na przeciwdziałanie nadużyciom finansowym i zapobieganie korupcji. Strona zawiera zbiór linków wyodrębnionych wg grup odsyłających do następujących dokumentów i procedur:

1. KODEKS ETYKI
2. NADUŻYCIA FINANSOWE I PRANIE BRUDNYCH PIENIĘDZY
3. WSPÓŁPRACA ZE SŁUŻBAMI
4. KORUPCJA I TRANSPARENTNOŚĆ
5. DYSCYPLINA FINANSÓW PUBLICZNYCH
6. TAJEMNICA SKARBOWA

Ustalono, że na przestrzeni 4 lat komunikowano obowiązywanie Kodeksu Etyki poprzez przesyłaną systematycznie co miesiąc informację w Newsletter. 6-krotnie ogłaszano konkursy w Intranecie Urzędu zawierające pytania za znajomości treści Kodeksu. Ponadto przeprowadzone było szkolenie i konkurs podczas akcji sadzenia drzew w 2016 roku.

Ocena świadomości obowiązywania Kodeksu Etyki

Ocena została sporządzona w oparciu o anonimową ankietę udostępnioną w Intranecie. Taki sposób dotarcia do pracowników miał na celu objęcie nią jak największą ilość zatrudnionych, badanie różnych grup pracowniczych (pracownicy administracyjni, urzędnicy, kadra kierownicza różnych szczebli) oraz zapewnić wygodę i zminimalizować zaangażowanie czasu potrzebnego na jej wypełnienie. Automatyzacja zbierania danych pozwoliła na szybkie i wygodne podsumowanie statystyczne oraz zestawienie odpowiedzi z pytań otwartych. Do tej pory ankiety zbierane w jednostce przy innych zadaniach audytowych były przekazywane mailowo a wydruki zbierane były przez audytorów indywidulanie. Zebranie ankiet elektronicznych stanowiło więc pierwszą próbę tego typu, pozwoliło zebrać doświadczenia w zakresie konstrukcji pytań oraz poznać zaufanie pracowników do tego typu narzędzia.

Zestawienie pytań do ankiety:

1. Podaj nazwę komórki w której pracujesz
2. Określ rodzaj swojego stanowiska.
3. Czy wiesz, że w Urzędzie funkcjonuje Kodeks Etyki Pracowników Urzędu?
4. Czy zetknąłeś się z zachowaniami nieetycznymi w miejscu pracy?
5. Jeżeli zetknąłeś się z zachowaniami nieetycznymi w miejscu pracy, której zasady to dotyczyło?
6. Czy widząc nieprzestrzeganie Kodeksu Etyki podjąłbyś jakieś działania?
7. Czy dostrzegasz potrzebę wprowadzenia zmian w zapisach Kodeksu Etyki?
8. Napisz propozycje zmian lub inne uwagi do Kodeksu Etyki Pracowników Urzędu.

Szczególnie cenne dla potrzeb audytu były wypowiedzi otwarte, które dotyczyły uwag co do treści postanowień Zarządzenia ws. Kodeksu Etyki oraz jego oddziaływania na organizację pracy Urzędu np. postanowień.

- dotyczące potwierdzenia przez pracownika zapoznania się z Zarządzeniem Marszałka przez podpisanie oświadczenia,
- wprowadzenia procedury zgłaszania i weryfikacji zachowań nieetycznych,
- potrzeby szkoleń pracowników i kadry kierowniczej w zakresie etyki,
- potrzeby upowszechniania Kodeksu Etyki,
- potrzebę uwypuklenia zapisów dotyczących dress-code,
- potrzeby wyraźnego ujęcia w jednej z zasad, zagrożenia korupcją.

Podsumowanie

Przeprowadzenie audytu etycznego dla organizacji pozwala dotknąć indywidulanie aspektu pracownika jako człowieka oraz członka zbiorowości. Wyznaczenie odpowiednich standardów etycznych jest bowiem wypadkową z jednej strony potrzeb samej organizacji, jej specyfiki i branży w której działa, z drugiej jednak przyjęte zasady tylko wtedy zadziałają gdy będą akceptowalne i zgodne z zasadami zespołu pracowników. W przedstawionym przypadku z punktu widzenia kierownictwa najważniejsze ustalenia audytowe dotyczyły potwierdzenia świadomości obowiązywania Kodeksu Etyki, czyli że:

- Kodeks Etyki jest wszechstronny i obejmuje wiele aspektów etycznych;
- Nie wymaga aktualizacji;
- Nie jest narzędziem do oceny etycznego postępowania, ale zbiorem oczekiwanych zachowań;
- Pracownicy znają i akceptują zasady Kodeksu Etyki;

Natomiast w zakresie proponowanych zmian rekomendowano wzmocnienie formy przyjęcia Kodeksu Etyki przez pracowników oraz wyodrębnienie go w oddzielnej zakładce w Intranecie. Patrząc na zdobyte doświadczenia zarówno w zakresie metodologii realizacji tego typu zadań jak i samych ustaleń, prowadzenie audytu etyki jest na pewno swego rodzaju wyznaniem intelektualnym, wymagającym taktu i dużego dystansu a jego przeprowadzenie pozwala na poznanie pracowników jednostki z innej, nieformalnej strony.

Słowa klucze: audyt, kodeks etyki, zasady etyki

Bibliografia:

Robert Moeller, Nowoczesny Audyt Wewnętrzny, Wyd. Wolters Kluwert Polska Sp. Z o.o., 2011

Title: Ethical audit case study

In Summary

The aim of the article is to present the topic of ethical audit in the practical example of the local government unit by presenting the provisions of the Code of Ethics. The area of ethics is an important part of the management unit and many institutions attaches increasing importance to issues involving accepted norms of behavior, or values. The essence of the good functioning of the ethical program is preservation of writing and its promotion. The article presents an example of the task of ethical audit, discussing the need for it, the legal aspects, including the sample Code of Ethics of the office, the methodology and the results of the study. Audit objectives agreed with the management were to answer two issues: 1) what is the awareness of being in the organization of the Code of Ethics, 2) examine whether there is a need for changes. The evaluation of the Code of Ethics promotion and its awareness of the validity of the Code of Conduct described in the article gave an answer to management inquiries. Looking at the gained experience both in terms of methodology of implementation of tasks and arrangements, conduct of ethics audit is certainly a kind of intellectual confession that requires tact and distance and its implementation allows to recognize the employees of the unit from the informal side.

Keywords: internal audit, Code of Ethics, ethics

Timur Khasanov-Batirov

What Internal Auditor Should Know About Implementation of the Anticorruption Compliance Program at Emerging Markets?

Creating and implementing a corporate anticorruption compliance program is a challenge, especially when dealing with emerging markets. I have learned through my own experiences and wrote this article to give businesses practical insights on implementing Compliance programs in former Soviet Union regions. In a nutshell, these are the Do's and Don'ts which will help you to avoid pitfalls, save time, and overcome barriers caused by instituting corporate ethics in a totally different business environment. The most practical way to share the tips contained in this article is to compare them to the respective points within the *Hallmarks of the Effective Compliance Program* listed in *Resource Guide to the U.S. Foreign Corrupt Practices Act*[10] ("FCPA Guide"). Tips are marked with a **T** sign.

CHAPTER I: TONE FROM THE TOP AND POLICY MAKING

Hallmark #1: Commitment from Senior Management and a Clearly Articulated Policy against Corruption

T **Why does this really matter in this region?** Without a "Tone at the Top" atmosphere, local personnel (as probably anywhere in the world) will view the company as having no ethics. Locals do not believe in mottos or declarations, they simply look at the actual practice of the business.
Look closely: Talk to your country head or to whoever is in charge of business in the region. If you are told: *"No worries, everything is already written in our policy, but I can't remember exactly where"* **or** *"There is a compliance/legal person down there who deals with all this…you'll figure it out yourself, "* **you will probably want to find out what is actually going on.**

Hallmark #2: Code of Conduct and Compliance Policies and Procedures

T Please make sure that your Code of Business Conduct is translated into local language (s). If you have it posted at your corporate website with it translated into various languages, ask a native speaker to check the translation so it can be understood by your target audience. There is a strong chance that the initial version will require corrections

[10] https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

to avoid "lost in translation" passages. It is critical that the right language and phraseology be used in different languages for your Code and also in key company policies. When answering a recent survey question: "Are your anti-bribery and corruption procedures translated into multiple languages? " only 59% of corporate risk professionals answered "Yes."[11] We expect that among those 59% there are probably very few companies that have translations in Azeri, Kazakh, or into the Ukrainian languages, despite those languages being fairly prominent in the respective regions.

CHAPTER 2: RISK ASSESMENT AND IMPLEMENTATION

Hallmark #3: Oversight, Autonomy, and Resources

T In some cases, compliance functions are assigned to a department not specifically designed for compliance, such as HR or Internal Audit. This happens to either technically meet the requirements on designating a compliance person, or due to budgetary constraints. Sometimes compliance personnel are appointed with additional responsibilities. The latter trend is noted in a survey from 2016: **"*Many companies have been cutting costs, both in their headcounts and training programmes, or stretching their existing compliance teams' responsibilities to include additional duties*."**[12] I would not recommend the above approaches. There may be a conflict of interest between Internal Audit, Corporate Governance, or HR by designating them compliance functions. Based on my own observations, in 20% of high-risk situations, that is to say conflicts of interest between non-compliance and compliance function, the "owner of two hats" might make poor judgments and risky decisions.

Hallmark #4: Risk Assessment

T **Where are the risks? Is there a trustworthy source that can list your priorities?** I suggest referring to OECD's statistics on bribery motives in international business, which, from our perspective, reflects the main risks in the region: *"In the majority of cases, bribes were paid to obtain public procurement contracts (57%), followed by clearance of customs procedure (12%), favorable tax treatment (6%) and other preferential treatment. Bribes were paid to obtain a license or other form of authorization in 6% of cases, whereas in 4% of cases bribes were in return of access to confidential information…"*[13]

Hallmark #5: Training and Continuing Education

[11] https://home.kpmg.com/content/dam/kpmg/pdf/2016/06/tr-anti-bribery-corruption-survey-2015.pdf
[12] http://www.pwc.ru/en/recs2016.pdf
[13] http://www.ethicalsystems.org/sites/default/files/files/OECD%20Foreign%20Bribery%20Report.pdf

T Introduce training on compliance risks as part of your company's regular business meetings for personnel (for instance, cycle meets in the pharmaceutical industry) and implement training for new staff. However, a routine and boring session might actually do more harm than good. That is why it is critical to carry out engaging, tailored, and interesting training based on real life scenarios. I find it very helpful to engage business heads in co-leading sessions, which will also effectively demonstrate support of your company's integrity efforts.

Hallmark #6: Incentives and Disciplinary Measures

T **Be careful if you plan to impose disciplinary action on an employee in any state of the former Soviet Union.** You must be sure to follow local laws to record the breach, determine whether the ethics violation matches the list of sanctioned actions under your internal written rules/employee's job description/applicable legislation, as well as providing evidence that the employee was duly informed about such compliance rules.

Hallmark #7: Third-Party Due Diligence and Payments

T If you contract with a local distributor to participate in state bids with your products, we strongly recommend that you examine the distributor's entire supply chain, including sub-distributors, before entering into the contract. This is to ensure you have the right level of comfort regarding the local distributor's financial transparency and shipment evidence before entering into a legal relationship. **Consider this from Philip Urofsky, a former federal prosecutor responsible for FCPA investigations: "*Compliance teams can sometimes get bogged down in the routine (but FCPA-related) paperwork and filings that go with such things as gifts and entertainment, but miss many of the other ways bribes can be paid, such as through a chain of intermediaries about which you know nothing.*"**[14]

CHAPTER 3: INVESTIGATIONS AND EFFICIENCY

Hallmark #8: Confidential Reporting and Internal Investigations

T **Who should lead our internal investigations?** You may often find yourself facing two very different situations:

1. Too many departments who each conduct various types of internal investigations, and
2. Inadequate inspections and investigations in middle-sized businesses.

As a result, large companies might suffer because there are "too many cooks in the kitchen," while smaller companies might not be prepared to promptly and properly investigate integrity breaches. I recommend big companies to review the functions of

[14] http://www.fcpablog.com/blog/2017/2/8/the-future-of-fcpa-enforcement-a-discussion-with-philip-urof.html#sthash.yGQGB09v.dpuf

corporate control departments (such as compliance, legal, security, internal control, etc.) to avoid conflicts and the same roles being held by the different departments. This could be achieved based on the "Three Lines of Defense" concept.

Hallmark #9: Continuous Improvement: Periodic Testing and Review

As noted in the FCPA Guide "*compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements*." Both the DOJ and SEC expect companies to test their internal controls and "*think critically*" about risk areas. What can be done to enforce these requirements?

T Compliance functions play a significant role in raising awareness about ethics and integrity standards across an organization. In practice, we have seen compliance teams counseling internal audit departments on anti-corruption requirements for further audits (i.e. audit of compliance function). I am not sure if this right or wrong, but I know that without such educational session those internal audit departments would have never included anti-bribery checks in its scope.

What expertise of internal audit departments in FCPA are important for organizations? Let's have a look at the DOJ's criteria regarding Internal Audit's role in bribery prevention: "*What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings?... How often has internal audit generally conducted assessments in high-risk areas?* "[15]

Hallmark #10: Mergers and Acquisitions: Pre-Acquisition Due Diligence and Post-Acquisition Integration

T According to regulators, a company should attempt to perform its due diligence in determining compliance before it purchases a target business. The trick is simple: try to get an M&A project team to evaluate a target's compliance risks as early in the process as you can.

In Summary

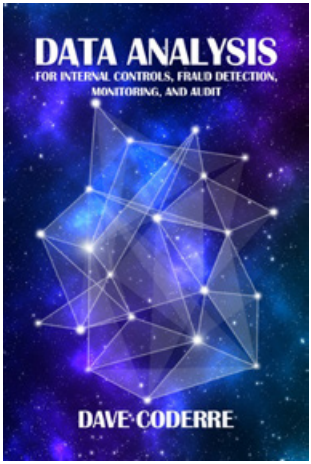
We have covered the steps necessary to help you enforce corporate compliance programs at emerging markets. To save time, money, and to comply with all applicable anti-corruption laws, I recommend checking all applicable regulations and common business practices in a particular region before establishing any type of anti-corruption and/or compliance program.

Key words: FCPA, Compliance Program, Emerging Markets

[15] https://www.justice.gov/criminal-fraud/page/file/937501/download

Autor tłumaczenia: Dariusz Kaźmierczyk[16]

Przez lata z analizą danych …



Zanim zaczniemy kolejny odcinek opowieści o doświadczeniach David Coderre w pracy audytora i jego zamiłowaniu do analizy danych, chciałbym przedstawić najnowszą pozycję książkową wydaną przez Davida a mianowicie: *„Data Analysis for Internal Controls, Fraud Detection, Monitoring, and Audit”*. W większości jest to zebrany i opracowany przez niego materiał opublikowany na blogu, którego tłumaczeniem są nasze publikowane odcinki.

Książka ta jest oczywiście wydana w języku angielskim i można ją zamówić bezpośrednio na stronie autora:

https://caats.ca/product/data-analysis-for-internal-controls-fraud-detection-monitoring-and-audit/

Osobiście nie mogłem odmówić sobie przyjemności posiadania tej pozycji w swojej biblioteczce, dlatego jak tylko się ukazała nie omieszkałem ją zamówić. Osoby, które wykorzystują oprogramowanie ACL, na pewno słyszały o wartości publikacji D. Coderre, dlatego jest to pozycja godna polecenia.

Na stronie o adresie wskazanym powyżej można zamówić również inne pozycje, z czego zwłaszcza dla osób chcących zagłębić się w świat możliwości ACL należałoby wskazać *„Fraud Analysis Techniques Using ACL”*. To książka z dodatkiem elektronicznym, gdzie są opisane i pokazane kody skryptów, jakie można używać przy pracach analitycznych podczas zadań audytowych, zwłaszcza wykorzystując oprogramowanie ACL. Również takich zadań, które David opisuje w swojej opowieści.

To tyle tytułem wstępu, a teraz czas na kolejne fascynujące przygody ze świata audytu i analizy danych.

David Coderre

Rok 4 – 1991 – Działalność

W 1991 r. wykorzystanie analizy danych dla wspierania audytu wewnętrznego miało się dobrze w organizacji. Co miesiąc opracowywałem raporty, w których wskazywałem w jaki sposób analityka była wykorzystywana przez różne zespoły audytowe w celu:

[16] Główny Inspektor Kontroli, Regionalna Izba Obrachunkowa w Krakowie, członek IIA, CGAP, ACDA, email: kazmieda@poczta.fm

– poprawy efektywności ich pracy,
– poszerzenia zakresu badań,
– osiągania lepszych wyników oraz
– badania całej populacji zamiast próbkowania.

Zespół ds. Analityki (wciąż tylko dwuosobowy) opracował poradniki CAATTs (komputerowo wspomaganych narzędzi audytowych), aby pokazać możliwości wykorzystania zasobów informacji finansowych i inwentarzowych, do których mieliśmy dostęp. Pracowaliśmy również nad podręcznikiem dla systemu HR (zasoby ludzkie). Te poradniki zawierały szereg standardowych testów, które mogły być realizowane przez audytorów, jak również opis zasobów danych, które były dostępne od ręki i na których można było wykonać testy od razu. Jako zespół mieliśmy dostęp do około 25–30 systemów, z czego 7–8 było wykorzystywanych regularnie, a inne okazjonalnie lub jednorazowo. W przypadku korzystania w sposób regularny z systemów, mieliśmy przygotowane standardowe procedury poboru danych, które były realizowane co miesiąc. W tym czasie również zaczęliśmy proces tworzenia wieloletnich przekrojowych raportów (np. podsumowania wg kont księgi głównej dla danego roku w przekroju ostatnich 3 lat). Pozwalało to nam obserwować trendy w danych, m.in. takich jak korzystanie z nadgodzin przez pracowników lub zamawianie usług zewnętrznych w stosunku do wypłacanych wynagrodzeń. W przyszłości mogliśmy wykorzystać te informacje przy sporządzaniu rocznego planu audytu opartego na analizie ryzyka (w tym momencie wybiegam tu jeszcze daleko do przodu). Na ówczesną chwilę pomagało to w planowaniu audytu, co i tak było zwiększeniem udziału analityki danych w procesie audytu poza dotychczas wpierany etap wyłącznie jego realizacji.

Zespół analityków starał się być w kontakcie z kierownikami zespołów audytowych już na wczesnym etapie planowania zadań, aby określić wymagania dotyczące danych oraz by ich zachęcać do korzystania z analityki podczas planowania, prowadzenia, a nawet raportowania audytów. Nadal było to raczej podejście, gdzie my dawaliśmy propozycje a nie odpowiadaliśmy na zapotrzebowanie audytorów. Byliśmy zmuszeni zatem, by zrozumieć ich potrzeby i na ich podstawie przedstawiać rozwiązania z użyciem analityki danych. Dzięki temu jednak, że sporządzaliśmy miesięczne sprawozdania z naszych działań z wykorzystaniem narzędzi analizy danych, było to coraz łatwiejsze zadanie.

Zespół ds. analizy nadal miał inne obowiązki. Nadal byłem odpowiedzialny za prowadzenie audytów w dziedzinach związanych z informatyką, natomiast druga osoba odpowiadała za naszą sieć LAN i aplikacje wspierające funkcje audytu wewnętrznego (np. opracowano system raportowania czasu pracy). Mimo tego i tak zdobyliśmy wiele cennej wiedzy i doświadczenia, a każdy z nas pomagał w 3–4 audytach jednocześnie.

Zostałem poproszony o wsparcie jednego z moich pierwszych audytów operacyjnych. Korzystaliśmy z floty ciężarówek, która przewoziła towary i dostarczała zamówienia. Były to samochody ciężarowe począwszy od samochodów dostawczych aż do dużych 18-to kołowców. Audyt miał ocenić ich właściwy dobór do wykonania poszczególnych zadań

(np. czy potrzebna była ciężarówka 18-to kołowa czy też wystarczył samochód dostawczy na danej trasie). Większość realizowanych przewozów miała wiele przystanków, z czego załadunek i rozładunek odbywał się na każdym z nich. Dane o realizowanych trasach obejmowały zarówno typ ciężarówki (pojemność pod względem objętości i ciężaru), jak i ilość załadowanego i rozładowanego towaru (objętość i ciężar) na każdym przystanku. Używając ACL byłem w stanie obliczyć objętość i ciężar towaru dla każdego samochodu na każdym przystanku i określić maksymalny wymagany typ samochodu dla trasy. Obliczając maksymalne wymagania dla każdej trasy w ciągu roku, byłem w stanie określić wymagany rozmiar samochodu ciężarowego dla jej obsługi. Udało mi się nawet zdefiniować takie wymagania dla każdego miesiąca lub nawet dnia tygodnia, jednakże przypisywanie różnym rozmiarom ciężarówek różnych tras dziennych lub miesięcznych wykraczało poza bieżące możliwości operacyjne. Rozliczaliśmy się zatem co kwartał wg maksymalnej wielkości samochodu ciężarowego. Ponieważ nie posiadaliśmy na własność żadnej z ciężarówek, mogliśmy zamawiać je naprawdę dowolnie, zatem zmniejszenie rozmiaru zamawianych ciężarówek powodowało natychmiastowe oszczędności, zarówno kosztów wynajmu, jak i paliwa.

Analiza wykazała, że dla 30% tras można było zmniejszyć rozmiar ciężarówek o 1 poziom a dla 10% tras o dwa. Oszczędność wynosiłaby około 2 mln USD rocznie. Na początku zarząd przedsiębiorstwa nie był przekonany do naszych wniosków, ale dokonaliśmy odpowiednich testów na 10 trasach przez jeden miesiąc. Analiza okazywała się poprawna i jej rezultaty zostały wdrożone w pełnym zakresie. Oszczędności za cały rok obliczono na 2,4 mln USD (7,2 mln USD w ciągu trzech lat).

Powinienem wspomnieć w tym miejscu, że dział zarządzania operacyjnego opracowywał program w języku COBOL, aby wykonać podobne obliczenia. Program miał ponad 5000 linii kodu i nie działał poprawnie. Program w ACL, który napisałem, miał mniej niż 70 linii i testy dowiodły jego prawidłowość.

Kolejny audyt, który wspierałem, analizował ceny jednostkowe płacone za różne standardowe produkty. Prosta analiza zidentyfikowała cenę minimalną, maksymalną i cenę średnią płaconą za każdy przedmiot. W większości przypadków była duża zgodność (tzn. stosunek ceny maksymalnej do ceny minimalnej był bliski 1,0), a tam, gdzie nie było, występowały uzasadnione powody (np. zwiększona jakość, pilność zakupu). Jednakże analiza wykryła także, pierwszy w mojej karierze, przypadek oszustwa. Osoba zamawiająca płaciła więcej za standardowe przedmioty w zamian za łapówki. Było bardzo ekscytującym zadaniem analizować takie dane, dopóki nie zdałem sobie sprawy, że to nie była anomalia w danych liczbowych, ale sytuacja, gdzie ktoś może być zwolniony z pracy, a nawet iść do więzienia. Zawiadomiliśmy policję, która poprosiła mnie o współpracę. Oficer śledczy zauważył, że czuję się odpowiedzialny za całą sytuację (w końcu to ja wykryłem oszustwo) i zapytał mnie, czy zatem on też powinien się czuć się źle za każdym razem, gdy aresztuje kogoś za przestępstwo. Pomogło mi to zrozumieć, że to nie moja wina, że dana osoba jest aresztowana. Wiedziałem jednak, że jeśli kontrola byłaby lepsza, nie byłoby okazji, aby ktoś mógł dopuścić się oszustwa.

Uwaga: Nadużycia finansowe są częstsze, gdy są szanse na ich dokonanie, występuje presja ich dokonania i możliwość racjonalizacji skutków[17]. W tym przypadku słabość mechanizmów kontroli doprowadziła do wystąpienia okazji popełnienia oszustwa.

Nie byłem specjalistą w wykrywaniu nadużyć czy przestępstw, ale nie był to ostatni raz, kiedy przyszło mi wykrywać oszustwo przy pomocy analizy danych.

Analiza: wykorzystane polecenia ACL: SUMMARIZE, EXPRESSION, GROUP, CLASSIFY, (Statystyka dla Min i Max)

Wnioski: Ważne jest, aby używać odpowiedniego narzędzia do danej pracy. COBOL był dobry w swoim czasie i nadal był odpowiedni dla wielu rzeczy, ale nie mógł konkurować z narzędziem analizy, takim jak ACL, który posiada wbudowane procedury ułatwiające zadania. Ludzie z pionu zarządzania operacyjnego byli lepszymi programistami niż ja, ale brakowało im odpowiednich narzędzi do wykonania tej pracy. Byli żądni wiedzy, zatem kolejny wniosek: audyt może wspomóc organizację bardziej niż tylko poprzez sam raport z rekomendacjami. Opisaliśmy całą logikę naszej analizy, dzięki czemu w oparciu o nią można było zbudować własny program monitorowania w danym obszarze. By to początek czegoś, co nazywaliśmy „transferem technologii audytu". Wybiegając w czasie 15 lat do przodu, byłoby to podobieństwo do testów audytu ciągłego, dostarczanych kierownictwu jako element sytemu ciągłego monitoringu.

Zdałem sobie również sprawę, że słabości kontroli wewnętrznej mogą doprowadzić dobrych ludzi do podejmowania złych decyzji. Audyt, zapewniając prawidłową kontrolę, jest odpowiedzialny za ochronę ludzi przed możliwością dokonywania złych wyborów.

I wreszcie, analiza danych musi nie tylko stale przynosić rezultaty, ale również musi być promowana i musi wychodzić do audytorów ze swoimi możliwościami. W późniejszych latach uznałbym to za bardzo frustrujące – ciągle reklamowanie użycia analityki danych mimo już znanych pozytywnych wyników z jej stosowania. Nawet gorsza sprawa, gdy kierownictwo się zmienia, musimy ponownie uzasadniać potrzebę funkcjonowania oraz ponoszenie i tak skromnych w stosunku do efektów, nakładów na analitykę danych. Dlatego słowo do wszystkich rozważnych osób: sprawdzaj korzyści z poczynionych inwestycji i nigdy nie spoczywaj na laurach. Jesteś tylko tak dobry, jak twoja następna analiza.

Rok 5 – 1992 – Budowa trwałego zespołu

Zespół analityków składał się wtedy z trzech osób – dlatego mogliśmy się wzajemnie uzupełniać wiedzą na temat systemów, z których regularnie korzystaliśmy. Na przykład oznaczało to, że nie jestem już jedyną osobą, która rozumie system finansowy. Teraz mieliśmy co najmniej dwie osoby dla każdego z 10–12 systemów, z których danych regularnie korzystaliśmy. Z wszystkich systemów, oprócz magazynowego (baza danych

[17] Donald R. Cressey, Other People's Money; Montclair: Paterson Smith; 1973 str. 30.

IMS, z którą łączyliśmy się interfejsem ACL dla MVS IMS) otrzymywaliśmy comiesięczne zestawy danych. Odbywało się to albo poprzez uruchomienie poleceń importu danych, albo pozyskanie standardowych raportów.

Pierwsze pytanie, na które musiałem odpowiedzieć przy budowaniu zespołu, dotyczyło poziomu wiedzy i doświadczenia osób, które powinny być częścią funkcji analitycznej. Kolejne pytanie brzmiało: czy audytor powinien być uczony programowania (ekstrakcja i analiza danych), czy raczej to programista powinien być uczony wykonywania audytów? Błędy w implementacji analityki mają jedną wspólną cechę: oznacza to, że nie przydzielono odpowiedniej osoby czy też osób do danego zadania. Zbyt często młody programista z małym doświadczeniem w audycie lub zupełnie go pozbawiony, zajmujący się tylko aspektami IT w pracy, jest przeznaczony do rozwijania funkcji analitycznej. Biorąc pod uwagę charakter zadań – dotyczą one bowiem właścicieli procesów biznesowych, programistów systemów i rewidentów – to funkcja analityczna musi być obsadzona ludźmi na odpowiednim poziomie i z niezbędnym doświadczeniem. Największą przeszkodą jest brak posiadania wiedzy na temat procesów biznesowych, która jest niezbędna przy typowaniu analiz do wykonania. Z uwagi na posiadane wsparcie kierownictwa, mogłem zatrudnić ludzi na poziomie starszego audytora czy też kierownika zespołu. Jednym z nich był programista z doświadczeniem z zakresu audytu IT, drugi to programista chętny do nauki o audycie.

Problem wielkości funkcji analitycznej to kolejna sprawa, którą należy rozwiązać. Zależy ona od ogólnego rozmiaru funkcji audytu, a także od rodzaju wykonywanych analiz oraz zasobów wiedzy i doświadczenia technicznego dostępnego w organizacji. Jeśli odpowiedzialność za prowadzenie analizy danych jest przypisywana jednej osobie, on lub ona muszą być co najmniej równoważni poziomowi kierownika zespołu i muszą mieć doświadczenie w imporcie danych, analizie, dokonywaniu ocen lub w audycie. Oznacza to zatrudnienie kogoś o wymaganych umiejętnościach z zewnątrz, jeśli nie ma takich osób w firmie. Wraz ze wzrostem wykorzystania analizy danych, funkcja analityczna może poszerzać się o niższe poziomy pracowników, wytyczając im ścieżkę kariery oraz stawać się bardziej elestyczną.

Wreszcie, funkcja analityczna musi być widoczna i zrozumiała oraz reagować na potrzeby zespołów realizujących przeglądy. Jednocześnie musi być również proaktywna w rozpoznawaniu możliwości wykorzystania analizy danych oraz w marketingu istniejących i nowych technologii. Ja starałem się upewnić, że zespół robi wszystkie z tych rzeczy.

Audyty:

Badałem projekt o wartości 4 mld USD, który miał na celu zaprojektowanie, budowę i utrzymanie specjalistycznego sprzętu. Biuro projektu miało funkcjonować około 7–8 lat. Dyrektor finansowy projektu zakupił system komputerowy do ewidencji i rozliczania przestojów w pracy, zamówień i prowadzenia sprawozdawczości finansowej oraz określił koszty i niezbędne elementy do bieżącego utrzymania. Kierowałem audytem biura zarządzania tym projektem, a jednym z celów zadania było zapewnienie, że informacje

pochodzące z systemu zarządzania projektem były dokładne i kompletne, kontrola były odpowiednia i skuteczna oraz, że wymiana danych między systemem zarządzania projektem a systemem finansowym korporacji działała poprawnie.

Dla realizacji części audytu pobrałem informacje z systemu zarządzania projektem i porównałem je z danymi pochodzącymi z systemu finansowego. Pozwoliło to ocenić dokładność i kompletność wymiany danych między systemami oraz prawidłowość raportowania systemu zarządzania projektami do zespołu kierującego.

Pierwszą rzeczą, jaką zauważyłem było to, że choć system projektu ewidencjonował szczegóły przestojów, w systemie finansowym korporacji nie odnotowano wystarczających informacji finansowych, które były potrzebne dla szacowania bieżących kosztów utrzymania. Prosta klasyfikacja wg kont księgi głównej z podsumowaniem kwot wykazała, że system projektu przesyłał dane tylko czterech kont księgi głównej, dotyczących: wynagrodzenia, nadgodzin, kosztów podróży i łącznych kosztów projektu. Informacje te nie były wystarczające, ponieważ użycie tylko czterech kont sprawiało, że szacowanie bieżącego wykorzystania sprzętu stanie się niemożliwe po zamknięciu biura projektu. Zazwyczaj bowiem bieżące utrzymanie szacuje się jako procent kosztów użycia sprzętu, bez usług i kosztów pozostałych.

Drugą rzeczą, jaką zauważyłem było to, że przesył danych do systemu finansowego był realizowany w sposób ręczny i wysyłano tylko dane ogólne (kwoty według kont księgi głównej za dany okres). Porównując dane szczegółowe zauważyłem również, że ilość nadgodzin była znacznie wyższa niż zaewidencjonowana w systemie finansowym. Podobnie zresztą jak kwota dotycząca zamówionych usług oraz środki na rozwój i utrzymanie IT. Kwoty dotyczące nadgodzin i zamówień były przeksięgowywane w każdym miesiącu jako normalne wynagrodzenia za pomocą poleceń księgowania. Skorygowane kwoty były przekazywane do systemu finansowego. Raporty projektu przekazane zespołowi kierującemu, przypuszczalnie pochodzące z systemu projektu, zostały zmienione tak, aby zgadzały się z sumami w systemie finansowym.

Poprosiłem zastępcę kierownika o wyjaśnienie, dlaczego zamówienia usług specjalistycznych oraz wydatki na rozwój i utrzymanie IT były rejestrowane jako normalne wynagrodzenia. Powiedział, że w budżecie są dodatkowe środki na wynagrodzenia, natomiast budżet na zakup usług był niewystarczający. Znałem ten problem już wcześniej, ale wiedziałem też, że łatwo było prawidłowo dokonać zmian w budżecie projektu pomiędzy poszczególnymi zakresami, zwłaszcza w przypadku tak dużego projektu. Kiedy poinformowałem go o tym, to wciągnął mnie do pustej sali konferencyjnej i cicho wyjaśnił, że dyrektor finansowy projektu celowo ukrywał nakłady na kontrakty i IT, ponieważ wykorzystywał fundusze na projekty specjalne, aby wspierać rozwój korporacyjnego systemu zarządzania projektami bez zgody wyższego kierownictwa.

Na zorganizowanym spotkaniu dyrektor finansowy projektu wyjaśnił mi, że firma, która dostarczyła oprogramowanie do zarządzania projektem, zerwała umowę i teraz jesteśmy właścicielem oprogramowania i legalnie zgodziliśmy się na jego modyfikowanie.

Stwierdził również, że ponieważ firma miała wiele dużych projektów, skorzystamy na posiadaniu niestandardowego pakietu oprogramowania do zarządzania projektami. Jednak gdy rozmawiałem o tym z główną dyrektor projektu, wyraźnie mi powiedziała, że nie miała uprawnień do wydawania środków projektu na opracowywanie innych aplikacji do zarządzania projektami i nie była świadoma działań dyrektora finansowego.

Przeglądałem umowy związane z usługami informatycznymi i okazało się, że z funduszy projektu wydano ponad 12 mln USD na modyfikację oprogramowania do zarządzania projektami bez sporządzenia planu rozwoju systemu, bez procesu modyfikacji oraz bez innych dokumentów przy tego rodzaju pracach.

Kontynuowałem przegląd szczegółów kontraktu analizując warunki zawarcia umowy: tryby udzielenia zamówień, konkurencyjność/brak konkurencyjności. Okazało się, że wszystkie umowy były zamówieniami z wolnej ręki zleconymi jednej firmie, a kwoty umów były podprogowe (poniżej progu, od którego zamówienia musiały być udzielane w trybie konkurencyjnym). Kiedy zapytałem o to dyrektora ds. zamówień, to w odpowiedzi usłyszałem, że dyrektor finansowy polecił mu tak podzielić zamówienia, aby mogły być udzielone w trybie z wolnej ręki. Zapytałem go, dlaczego te 14 umów, które miałem w ręku nie były przez niego podpisane, lecz przez dyrektora finansowego, skoro wszystkie inne on sygnował swoją ręką. Dziwiłem się osobiście, że dyrektor finansowy podpisywał umowy, bo wydawało się to być oczywistym konfliktem interesów. Dyrektor ds. zamówień powiedział, że umowy te dotyczyły zamówień realizowanych przez córkę dyrektora finansowego (miała ona nazwisko po mężu), i dlatego odmówił ich podpisania. Twierdził, że córka dyrektora finansowego zarabiała jak starszy programista, choć w rzeczywistości nie miała z tym nic wspólnego i wykonywała tylko obowiązki biurowe. Cóż, znowu zostałem wciągnięty w sprawę ewentualnego oszustwa.

Przeprowadziłem dodatkowe testy: porównałem adresy kontrahentów względem adresów pracowników; obliczyłem maksymalne ceny zamówień; weryfikowałem nadgodziny i stawki wynagrodzeń w stosunku do danych wykazywanych w systemach płacowych; weryfikowałem koszty podróży służbowych. W końcu wobec dyrektora finansowego wszczęto śledztwo pod kątem ewentualnych oszustw, niewłaściwego wykorzystania funduszy projektu i złego zarządzania. To, co miało być tylko audytem IT mającym na celu zbadanie kompletności, dokładności oraz zasad wymiany danych pomiędzy systemami, stało się faktycznie trzema zadaniami: audytem IT, audytem zamówień na usługi informatyczne; wykrywaniem nadużyć.

Dzięki analizie danych udało mi się wykazać, że:

- wymiana danych pomiędzy systemem zarządzania projektem, a systemem finansowym była niewłaściwa;
- informacje przekazywane do systemu finansowego nie miały wystarczającej szczegółowości (przekazywano dane zbiorcze i wg zbyt mało rozbudowanej analityki) oraz nie były zgodne z danymi zawartymi w systemie zarządzania projektami.

Analizowałem również dane wg zakresów kwot zamówień (stratyfikacja) w celu znalezienia przypadków podziału zamówień tj. o wartości ustalonych tuż poniżej progu kwotowego, od którego obowiązuje stosowanie trybów konkurencyjnych. Porównałem także dane pochodzące z systemu zarządzania projektem i systemu finansowego, dzięki czemu wykryłem niewłaściwe wykorzystania funduszy projektu (12,2 mln USD) oraz kilka innych nieprawidłowości przy zawieraniu umów. Dochodzenie w sprawie nadużyć finansowych skutkowało zwolnieniem dyrektora finansowego, a zastępca kierownika projektu został zdegradowany za kumoterstwo i nepotyzm. Dyrektor zarządzający projektem również został usunięty.

Kolejne zadanie audytowe tamtego roku dotyczyło standardowego zagadnienia tj. gospodarki towarowej w dużym magazynie. Cel był jasny: weryfikacja czy zabezpieczenie materiałów i towarów było odpowiednie. Ze względu na wielkość magazynu i charakter składowanych w nim towarów – nowoczesnych, przenośnych i atrakcyjnych przedmiotów – był on sprawdzany co kilka lat. Zwykle w czasie takich audytów porównywano to, co znajdowało się na półkach z tym, co zostało zaewidencjonowane w systemie. Mimo, iż stwierdzano niewielkie różnice, audyty co do zasady nie wykazywały istotnych problemów.

Program audytu przewidywał pobranie próbki danych z systemu magazynowego zawierających informacje o numerze danej pozycji magazynowej i jej ilości. Następnie audytorzy przeszli do magazynu i policzyli liczbę przedmiotów na półkach. Kierownik zespołu znał się na technikach oszustw zatem polecił audytorom otworzyć opakowania, aby upewnić się, że rzeczywiście zawierają wymagane przedmioty. Znane były bowiem przypadki piasku lub kamieni umieszczanych w pudełkach, gdy dokonywano kradzieży.

Po raz pierwszy w tym audycie wykorzystaliśmy oprogramowanie do analizy danych w celu wygenerowania próbki. Poprzednio w audytach w tym magazynie po prostu braliśmy co setny elementów lub generowaliśmy listę liczb losowych i dopasowaliśmy ją do listy zawierającej listy artykułów w magazynie. Teraz mogliśmy przyjrzeć się ilościom i dokonać próbkowania warstwowego. W tym celu wykorzystałem statystykę i dokonałem podziału danych na poszczególne zakresy wg liczby pozycji i ilości. Pozwoliło to nam wybrać niektóre elementy, których było więcej lub większej wartości wartości (górne warstwy) lub które zostały uznane za atrakcyjne (np. komputery i inne nowoczesne sprzęty). Pozwoliło to na bardziej skuteczną metodę pobierania próbek oraz ich lepszą reprezentatywność.

Chciałem by ten audyt był pełniejszy i nie dotyczył tylko porównania danych z systemu z liczbą przedmiotów na półkach ustalonych w trakcie ręcznego liczenia, ale byśmy na podstawie danych o przychodach i rozchodach z magazynu sami ustalili ilości poszczególnych elementów, które winny znajdować się w magazynie. Otrzymaliśmy plik z operacjami zawierający wszystkie „przychody" i „rozchody". Wpływy do magazynu zostały zarejestrowane na rampie odbiorczej i określały otrzymaną ilość przedmiotów, w podziale na poszczególne pozycje, umowy, przesyłki. Wydania z magazynu były bardziej złożone i mogły dotyczy: zamówień, zwrotów, odpadów itd. Aby wypełnić postawione cele audytu dokonano obliczeń dla poszczególnych pozycji magazynowych (ogółem =

przychody – rozchody), a następnie porównano je z zapisami w systemie. Podobnie jak w poprzednich latach, wystąpiły bardzo małe rozbieżności.

Wykonywałem również statystyki dotyczące ilości odbieranych i wydawanych towarów – po to, aby uzyskać pełną informację o strukturze danych. Wyniki pokazały liczbę pozycji pozytywnych, negatywnych, 5 najwyższych, 5 najniższych itd. Podczas przeglądu tych rezultatów zauważyłem, że były ujemne przychody magazynu. Przedstawiłem wyniki kierownikowi zespołu audytowego i wspólnie zastanawialiśmy się, co mogą oznaczać te ujemne przychody. Nie mogły to być zwroty, zamówienia w trybie szybkiej sprzedaży, czy kwestie dotyczące rozchodów w ramach projektów, ponieważ system zezwalał pracownikowi odbierającemu towary na realizację operacji tylko i wyłącznie przychodowych. Dokonałem kategoryzacji danych z ujemnymi przychodami wg pracowników i okazało się, że takie ujemne dane zostały wpisane do systemu tylko przez dwóch z 15 pracowników, z czego jeden z nich już nie pracował. Kierownik zespołu audytowego postanowił zapytać pracownika o te wpisy. Kiedy ten przyszedł, kierownik powiedział: *„Chcemy porozmawiać o tych ujemnych pozycjach przychodowych”*.

Pracownik od razu złamał się i powiedział: *„Wiedziałem, że mnie w końcu złapiesz”*. Pomimo zmieszania takim nagłym przyznaniem się, kierownik zespołu szybko doszedł do siebie i powiedział: *„Tak, ale chcieliśmy dać Ci szansę wyjaśnienia, jak i dlaczego to zrobiłeś”*. Pracownik poinformował nas, że mechanizmy kontrolne uniemożliwiają mu wejście w jakiekolwiek inne operacje poza przychodami. Zawarte w programie mechanizmy nie zabraniały jednak dokonywania ujemnych wpisów jako przychodów. Zatem mógł on wprowadzić przychód 10 laptopów na podstawie odpowiedniego numeru faktury. Następnie był ewidencjonowany przychód -2 laptopów (bez numerów faktury) i w ten sposób następowała kradzież dwóch laptopów. System magazynowy wykazywałby 8 laptopów, które zgadzały się ze stanem faktycznym. Ilość towarów z faktury byłaby równa ilości otrzymanej tj. 10 szt., zatem dostawca otrzymałby zapłatę. Mimo, iż operacje z ujemnym przychodem nie miały numeru faktury, to nie pojawiały się w raportach o niezgodnościach, ponieważ zaprzychodowana ilość była mniejsza od 0, a algorytm programu wybierał tylko pozycje, gdzie przychody towarów były większe niż 0. Pracownik nauczył się wykorzystywać tę lukę w mechanizmach kontrolnych od swojego innego, niepracującego już kolegi.

Łączna kwota ujemnych przychodów wynosiła w ciągu ostatnich 5 lat 375 tys. USD. W tym czasie przeprowadzono trzy audyty i nie znaleziono poważnego problemu w zakresie kontroli nad ochroną aktywów.

Analiza: wykorzystane polecenia ACL: FILTER; EXPRESSION, STATISTICS, STRATIFY, CLASSIFY, JOIN i SAMPLE.

Wnioski: Zawsze warto pytać „*Dlaczego*”. *„Dlaczego występowały ujemne ilości? Dlaczego nie podpisałeś tych umów? Dlaczego wszystkie kwoty są niższe od kwoty progowej przy udzielaniu zamówień? ”* Mogłem zignorować te sprawy lub po prostu wykazać niezgodność, ale zadając takie pytania, udało nam się znaleźć przyczynę główną i źródło problemu.

Coraz więcej procesów biznesowych jest obsługiwanych przez zintegrowane aplikacje i zautomatyzowane mechanizmy kontrolne (np. trójstopniowe porównywanie ilości i ceny jednostkowej). Ale jeśli dane mogą być zmieniane, to takie mechanizmy są nieskuteczne. Kontrola nad bezpieczeństwem aktywów obejmuje dokładne wprowadzanie informacji oraz monitorowanie nieuprawnionych wpisów lub manipulacji danymi. To nie tylko porównanie danych z systemu z liczbą sztuk przedmiotów ujawnioną podczas fizycznego liczenia tego co znajduje się na półkach. Standard SAS #99 (Statements on Auditing Standards, American Institute of Certified Public Accountants – http://http://www.aicpa.org/research/standards/auditattest/pages/sas.aspx#SAS84 – przyp. red.) stwierdza, że testy merytoryczne nie są wystarczające, a audytorzy muszą testować mechanizmy kontrolne w zakresie IT. Wymaga to także od audytorów wykorzystywania technologii (analiza danych) w procedurach audytowych ukierunkowanych na badanie nadużyć finansowych oraz IT.

Zawsze należy być sceptycznym co do skuteczności mechanizmów kontrolnych i procesów monitorowania. Nawet duże projekty z biurami zarządzania, komitetami nadzoru i ścisłymi wymagania dotyczącymi sprawozdawczości bazują na przekonaniu, iż prawidłowo funkcjonuje kontrola i nadzór. Główny dyrektor projektu zrzekł się wszystkich obowiązków związanych z finansami i zamówieniami na rzecz dyrektora finansowego. Dopuszczenie do sprawowania obowiązków przez jedną osobę tj. dyrektora finansowego w zakresie finansów oraz udzielania zamówień było poważnym błędem przy podziale zakresu zadań, ale wynikało to głównie z faktu, że nie było właściwego nadzoru. Osoba ta była nawet w stanie wprowadzić w błąd komitet nadzoru nad projektem, składając fałszywe sprawozdania i zmieniając dane przed przesłaniem ich do systemu finansowego korporacji.

Wyjaśnienie:
Polecenia wskazane przez D. Coderre, a nie omówione już poprzednio: GROUP, CLASSIFY, STRATIFY, SAMPLE wykonują w środowisku ACL następujące zadania:

- GROUP – formalnie GROUP nie jest poleceniem możliwym do wywołania z poziomu menu programu ACL. Jest to element pewnej struktury, możliwej do realizacji wyłącznie poprzez skrypty ACL. Umożliwia ona rozdzielenie jak i grupowanie poszczególnych poleceń do przetworzenia w trakcie wykonywania programu zapisanego w skryptach w zależności od występujących warunków. Umożliwia także sterowanie wykonywaniem poszczególnych sekwencji skryptu. Bardzo trudno jest w kilku słowach przedstawić ideę wykorzystania struktury GROUP … ELSE … END bez szczegółowych przykładów. Być może wrócimy do tej sprawy w odrębnych publikacjach, gdy będzie takowe zainteresowanie;
- CLASSIFY – grupuje rekordy według identycznej wartości jednego pola znakowego lub numerycznego. Dodatkowo zlicza rekordy w każdej grupie i podsumowuje wybrane pole numeryczne dla każdej grupy. Wyniki są zapisywane do nowej tabeli lub wyświetlane na ekranie. Jak widać polecenie to jest bardzo

zbliżone do opisywanego już wcześniej SUMMARIZE, jednakże bazuje tylko na wartościach jednego pola. Cała operacja wykonywana jest w pamięci komputera i nie jest wymagana operacja wstępnego sortowania;

– STRATIFY – polecenie, dzięki któremu możliwe jest wyznaczenie przedziałów wartościowych wg danej wartości numerycznej oraz zliczenie ilości rekordów należących do danego przedziału oraz ustalenie wartości danego przedziału;
– SAMPLE – pozwala na wybór próbki z populacji danych.

Jan Anisimowicz[1] **dr Łukasz Cichy**[2]

Matryca funkcji kontroli w teorii i praktyce systemów IT

Wstęp

Rozporządzenie Ministra Rozwoju i Finansów *w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego* z dnia 6 marca 2017 r. (dalej: rozporządzenie) mocą § 36 ust. 3 pkt 2 wprowadziło w stosunku do zastąpionej uchwały nr 258/2011 KNF istotne novum w postaci tzw. matrycy funkcji kontroli (dalej: MFK). Zmiana jest na tyle znacząca, że okres wejścia w życie obowiązku sporządzenia matrycy wydłużono do 1 lipca 2017 r., albowiem, jak można przeczytać w uzasadnieniu do rozporządzenia: *Sporządzenie (...) opisu w formie matrycy funkcji kontroli (...) może być – w przypadku niektórych banków – procesem złożonym, wymagającym od banków istotnych nakładów czasowych, przeglądu dotychczasowych procesów oraz odpowiedniego delegowania zadań w ramach struktury organizacyjnej*. Tym bardziej więc należy się skupić na jak najbardziej efektywnym procesie wdrażania matrycy, zwłaszcza w przypadku, gdy zarządzenie matrycą ma zostać odzwierciedlone w postaci systemu IT.

Jednocześnie należy podkreślić, **że** w stosowanych modelach systemu kontroli wewnętrznej i zarządzania ryzykiem sama matryca funkcji kontroli (risk control matrix, internal control template) nie jest czymś nowym, niemniej jednak przejście na taki sposób rozumienia systemu kontroli wewnętrznej wymaga od banku nie tylko odpowiedniego dostosowania **własnych regulacji i procedur wewnętrznych**, ale zmiany całościowego rozumienia kontroli wewnętrznej w banku.

1. Matryca funkcji kontroli – konsekwencje wymogów regulacyjnych

Zgodnie z § 36 ust. 3 pkt 2 rozporządzenia *Bank zapewnia dokumentację funkcji kontroli w szczególności przez opis, w formie matrycy funkcji kontroli, powiązania celów, o których mowa w art. 9c ust. 1 ustawy – Prawo bankowe, z procesami w działalności banku, które przez bank zostały uznane za istotne oraz kluczowymi mechanizmami kontrolnymi i niezależnym monitorowaniem przestrzegania tych mechanizmów kontrolnych*. Dalsza konkretyzacja znajduje się w rekomendacjach 4.3, 24.5e, 25.3f, 26.1d oraz przede wszystkim 9.1-9.4 nowej Rekomendacji H KNF. Jak wskazuje rozporządzenie, matryca funkcji kontroli jest opisem dokumentującym ową funkcję, który to opis składa się na powiązanie określonych elementów. Wymóg ten poniekąd determinuje charakter matrycy, która w wersji minimalnej ma jedynie odzwierciedlać pewne relacje między określonymi elementami, a nie generować określone wyniki (np. rejestrować nieprawidłowości). Oczywiście rozbudowywanie matrycy

[1] Ekspert GRC (Governance, Risk and Compliance) w firmie C&F.
[2] Governace Risk Compliance Director w zespole Ryzyka regulacyjnego i Compliance kancelarii prawnej Wierzbowski Eversheds Sutherland.

o wyniki np. testowania pionowego jest jak najbardziej dopuszczalne, nie mniej jednak nie wydaje się, by od 1 lipca 2017 wymagało tego rozporządzenie. Samo powiązanie wystarczy. Do obowiązkowych elementów matrycy należą cele systemu kontroli wewnętrznej, procesy istotne, kluczowe mechanizmy kontrolne oraz niezależne monitorowanie skuteczności mechanizmów. Nie znaczy to, że matryca pozbawiona jest elementów obowiązkowych „warunkowo", czy też elementów fakultatywnych. W przypadku tych pierwszych, zgodnie z Rekomendacją 9.4 Rekomendacji H *Bank powinien uzupełniać matrycę funkcji kontroli o dodatkowe elementy wynikające z systemu kontroli wewnętrznej jego podmiotów zależnych, jeżeli mają one wpływ na zapewnianie osiągania celów systemu kontroli wewnętrznej w procesach istotnych*. Dodatkowo w przypadku banków nienależących do tzw. systemu ochrony, w ramach celów systemu kontroli wewnętrznej należy określić cele szczegółowe. Z kolei do elementów fakultatywnych może należeć wszystko to, co w opinii banku jest istotne z punktu widzenia wprowadzonej funkcji kontroli np. ryzyko nieosiągnięcia celów systemu kontroli wewnętrznej, rodzaj mechanizmu kontrolnego, proces nieistotny, czy nawet ujęcie danego procesu w cyklu audytowym.

Każdy z powyższych obowiązkowych elementów matrycy jest szczegółowo opisany w Rekomendacji, wobec czego sama czynność powiązania tych elementów w matrycy stanowi niejako element finalny całościowego procesu wdrażania funkcji kontroli. W konsekwencji najpierw należy wdrożyć poszczególne elementy matrycy funkcji kontroli (np. określić procesy istotne), a dopiero potem opracować koncepcję ich powiązania, by wreszcie móc to wszystko finalnie odzwierciedlić w samej matrycy. Jednocześnie należy pamiętać, że matryca funkcji kontroli, jako obowiązkowy element dokumentujący ową funkcję, sama powinna spełniać wymóg skuteczności i adekwatności. A to możliwe jest tylko wtedy, gdy nie tylko zawiera wszystkie elementy konieczne, ale także gdy jest właściwie zarządzana, w tym zwłaszcza aktualizowana. Każda zmiana w procesie istotnym, mechanizmie kluczowym, czy też jednym z czterech rodzajów niezależnego monitorowania, powinna być niezwłocznie zaktualizowana w matrycy.

2. Matryca funkcji kontroli – rozwiązania praktyczne w systemie IT

Matryca funkcji kontroli znacząco rozszerza podejście do zapewnienia mechanizmów kontrolnych w ramach instytucji finansowej. Łączy w sobie cele ogólne z celami szczegółowymi, procesami istotnymi oraz wspierającymi je mechanizmami kontrolnymi odnoszącymi się do weryfikacji oraz testowania (zarówno pionowego jak i poziomego). Z uwagi na zdefiniowaną znaczną liczbę podanych wymiarów oraz jeszcze większą liczbę możliwych przecięć i interakcji między wymiarami, zarządzanie taką strukturą może być kłopotliwe i czasochłonne. Dodatkowo oprócz jej przygotowania trzeba zadbać także o to, aby stworzone narzędzie było łatwe w utrzymaniu i zarządzaniu zmianami, które będą zachodzić w czasie. Oczywiście pierwszym i prawie oczywistym wyborem jest stworzenie matrycy bezpośrednio w narzędziu MS Excel. Jest to narzędzie dostępne w każdej organizacji, elastyczne, choć niepozbawione wad – głównie w ramach pracy grupowej, ograniczenia dostępu poszczególnym użytkownikom, czy też pewności co do tzw. jednej

wersji prawdy opisanej w MFK. W dalszej części artykułu pokażemy Państwu, jak można wykonać to zadanie w narzędziu informatycznym, które daje nam dodatkowe korzyści oraz możliwości (np. w zakresie integracji, zarządzania strukturą wymiarów matrycy, wsparciem weryfikacji zgodności), jednocześnie usuwając istniejące ograniczenia związane z pracą w MS Excel.

Do całości zagadnienia można podejść w sposób metodyczny i procesowy. Analizę poszczególnych wymagań i oczekiwań KNF dotyczących MFK można oddać w ramach przedstawionego poniżej diagramu, przedstawiającego cykl działania zorganizowanego.

Diagram nr 1. Cykl działania zorganizowanego- matryca funkcji kontroli

Źródło: opracowanie własne na przykładzie Adaptive MFK

Całość działań można podzielić na trzy etapy, które powinny być realizowane cyklicznie (nie jest to działanie jednorazowe).

W pierwszym kroku (ANALIZA) trzeba wiedzieć, jak wygląda nasza organizacja w kontekście oczekiwań wymaganych przez regulatora. Najbardziej efektywnym sposobem jest wykonanie analizy luki, która pomoże zidentyfikować obszary wymagające przeprowadzenia działań naprawczych. W kontekście rekomendacji H wykonanie tego kroku będzie możliwe po przygotowaniu zbioru pytań. Przykładowa lista takich pytań (z pełnej listy ponad 600) znajduje się w tabeli poniżej.

Tabela nr 1 Przykładowa lista pytań

Paragraf	Treść pytania
9.2.	Czy za aktualizację informacji w matrycy odpowiada komórka organizacyjna funkcjonująca w ramach drugiej linii obrony?
12.5.	Czy wysokość wynagrodzenia (w tym premii) kierującego komórką do spraw zgodności jest zatwierdzana przez radę nadzorczą lub komitet audytu?
15.1.	Czy komórka do spraw zgodności jest odpowiedzialna za projektowanie, wprowadzanie i stosowanie procedur i metodyk identyfikacji ryzyka braku zgodności?
23.2.	Czy strategia działalności komórki audytu wewnętrznego jest opiniowana przez zarząd banku i komitet audytu oraz zatwierdzana przez radę nadzorczą?
25.5.	Czy w ramach strategicznego (długoterminowego) planu badań audytowych kierujący komórką audytu wewnętrznego wskazuje minimalną częstotliwość obejmowania badaniem audytowym wszystkich obiektów audytowych z uniwersum audytu?

Źródło: opracowanie własne na podstawie wytycznych z Rekomendacji H

Stwierdzone braki powinniśmy zarejestrować na liście zidentyfikowanych niezgodności. Pomoże nam to później przełożyć te elementy na konkretne działania naprawcze, realizowane w etapie tworzenia matrycy funkcji kontroli.

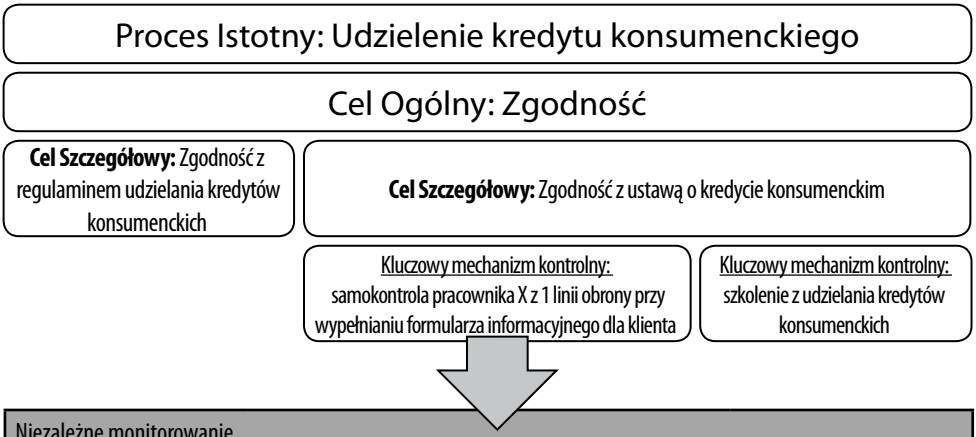
W tym miejscu należy zaznaczyć, iż dobrą praktyką w organizacji powinno być posiadanie każdej regulacji przedstawionej w formie wytycznych/pytań/checklisty. Taka wspólna biblioteka regulacyjna umożliwi nam nie tylko cykliczną analizę luki, ale także monitorowanie (zwłaszcza testowanie). Pozwoli to oddać charakter zmian zgodności zachodzący w czasie. Niewątpliwą zaletą takiego podejścia jest możliwość powiązania ze sobą wytycznych/pytań pochodzących z różnych regulacji. Da nam to opcję analizy luki (bądź jej monitorowania) dla wielu regulacji jednocześnie, przy znacznej oszczędności czasu i większej dokładności analizy. Dodatkowo każda nowa regulacja będzie mogła być przeanalizowana pod kątem jej podobieństwa do już istniejących w systemie regulacji. W przypadku znacznego podobieństwa, znacznie uprości i przyspieszy to tryb jej wprowadzenia w organizacji.

Po wykonaniu tego pierwszego etapu, można przystąpić do tworzenia matrycy funkcji kontroli. Powinna ona uwzględniać wszystkie wymagane w Rekomendacji H rekomendacje szczegółowe. Trzeba także w trakcie jej tworzenia zadbać o zidentyfikowane na etapie analizy niezgodności.

Sama matryca funkcji kontroli ma oczywiście strukturę hierarchiczną, która łączy cele, procesy i mechanizmy kontrolne oraz ich niezależne monitorowanie w jedną spójną

całość. Trzeba mieć jednak na uwadze fakt, że znaczna liczba wymiarów oraz możliwość istnienia cykli w relacjach pomiędzy obiektami może bardzo skomplikować tworzoną hierarchię. W tym wypadku zdecydowanie lepszym rozwiązaniem jest zastosowanie grafu skierowanego. Posiada on zalety struktury hierarchicznej, ale dodatkowo oddaje możliwość tworzenia bardziej elastycznych relacji pomiędzy obiektami. Ta właściwość nabierze dodatkowego znaczenia w trakcie operacyjnego użytkowania (zarządzanie cyklem zmian i aktualizacjami)

Rys. nr 1 Przykładowa implementacja matrycy może wyglądać następująco



Niezależne monitorowanie			
WB pozioma	Testowanie poziome	WB pionowa	Testowanie pionowe
weryfikacja przez pracownika Y z 1 linii obrony danych wprowadzonych przez pracownika X przed wypełnieniem formularza	testowanie przez pracownika Y z 1 linii obrony wybranej grupy wypełnionych formularzy	akceptacja sposobu wypełniania formularzy przez komórkę 2 linii obrony	testowanie przez komórkę 2 linii obrony sposobu wypełniania przez pracowników 1 linii obrony wybranej grupy formularzy

Źródło: opracowanie własne

Dla każdego mechanizmu kontrolnego, także na poziomie poszczególnych obszarów niezależnego monitorowania, powinniśmy mieć zdefiniowane atrybuty i powiązania dotyczące:

- Osoby/Jednostki odpowiedzialnej,
- Częstotliwości wykonywania niezależnego monitorowania (dzienna, tygodniowa, miesięczna, kwartalna, roczna),
- Historii zmian w matrycy funkcji kontroli (np. osób odpowiedzialnych).

Po inicjalnym zdefiniowaniu MFK kluczowym zadaniem jest zapewnienie efektywnego działania matrycy w codziennej pracy organizacji. Trzeba mieć na uwadze, że w trakcie realizacji niezależnego monitorowania będą identyfikowane nieprawidłowości. W konsekwencji będą one wymagać zastosowania określonych środków naprawczych i dyscyplinujących (wykonania akcji i działań w celu ich usunięcia lub ograniczenia negatywnego wpływu). Dodatkowo może pojawić się ryzyko, o którym mowa w definicji kluczowego mechanizmu kontrolnego, tj. nieakceptowalne przez bank ryzyko, że dany cel nie zostanie osiągnięty. Także ono będzie wymagać określonych działań. Wszystkie omawiane do tej pory obiekty powinny być ze sobą powiązane tak, aby możliwa była ocena ich wzajemnego na siebie wpływu. Pomoże to ustalić efektywną ścieżkę zarządzania oraz rozwiązywania pojawiających się niezgodności.

Ostatnim, ale jednocześnie bardzo ważnym elementem całego ekosystemu MFK jest posiadanie efektywnego mechanizmu wymiany informacji. Proces niezależnego monitorowania, jak i samo zarządzanie matrycą funkcji kontroli powinny być osadzone w mechanizmie wspierającym przepływ pracy (workflow), zapewniając:

- Weryfikację i akceptację wprowadzanych zmian,
- Mechanizm notyfikacji o akcjach do wykonania przez poszczególne linie.

Podsumowanie

W niniejszym artykule przybliżyliśmy podstawowe założenia związane z matrycą funkcji kontroli. Opisane zagadnienie nie jest łatwe w przygotowaniu i zapewne dla części organizacji będzie stanowić wyzwanie. Jak jednak pokazaliśmy w naszym artykule, zastosowanie podejścia zorganizowanego ułatwia wykonanie postawionego przez regulatora zadania. Dodatkowe wsparcie tego procesu odpowiednio przygotowanym systemem informatycznym może być kluczowym wskaźnikiem sukcesu.

Wartość takiego rozwiązania będzie rosła z czasem. Trzeba pamiętać, iż to po stworzeniu matrycy konieczne jest zapewnienie jej utrzymanie w związku z zachodzącymi zmianami (wykonywane testy, przeprowadzane weryfikacje, zmiany odpowiedzialności w matrycy, zidentyfikowane nieprawidłowości). Dodatkowym wyzwaniem jest przystosowanie matrycy funkcji kontroli do rozwiązań stosowanych przez podmioty dominujące banków. Głęboko jednak wierzymy, że niezależnie od wybranego podejścia, matryca funkcji kontroli pomoże lepiej nadzorować istotne procesy w organizacji.

Streszczenie

Ze wszystkich wytycznych najnowszej Rekomendacji H KNF jedno pojęcie budzi największe wątpliwości, sprzeczne opinie i gorączkowe pytania odnośnie procesu implementacyjnego. Jest nim tzw. matryca funkcji kontroli. W artykule tym przedstawimy podejście do implementacji i zarządzania matrycą funkcji kontroli, co pozwoli choćby w przybliżeniu zarysować skalę problemu i przykłady jego skutecznego rozwiązania.

Słowa kluczowe: GRC, matryca funkcji kontroli, funkcja kontroli, mechanizm kontrolny, niezależny monitoring

Title: The Control Function Matrix in Theory and Practice of IT systems

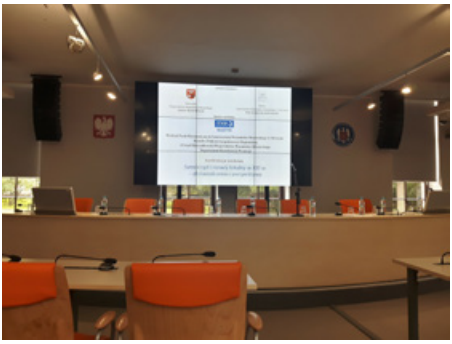
In summary

Of all the guidelines of the recent H Recommendation of the Financial Supervision Authority (KNF), one concept raises the biggest doubts, conflicting opinions and feverish questions about the implementation process. It is, the so called, control function matrix. In this article we will present an approach to the implementation and management of the control function matrix, which will allow us to approximate the scale of the problem and examples of its effective solution.

Key words: GRC, internal control matrix, control function, control mechanism, independent monitoring

Marcin Dublaszewski[18]

Relacja z konferencji naukowej



fot. Marcin Dublaszewski

W dniach 21-22 września 2017 miała miejsce w Olsztynie konferencja naukowa „Samorząd i rozwój lokalny w XXI w. – doświadczenia i perspektywy". W wydarzeniu tym, organizowanym przez Wydział Nauk Ekonomicznych Uniwersytetu Warmińsko – Mazurskiego wziął udział koordynator Warmińsko – Mazurskiego Koła Regionalnego IIA w Olsztynie Marcin Dublaszewski. Konferencja była niejako podsumowaniem dużego projektu badawczego «Sprawność instytucjonalna vs. lokalny rozwój gospodarczy – czynniki kształtujące i interakcje»

Tematyka Konferencji bez wątpienia wchodzi w zakres zainteresowania audytu wewnętrznego realizowanego w samorządzie. Naukowy charakter wydarzenia przekładał się na sposób prezentowania poszczególnych punktów programu, który polegał na badawczym podejściu do zidentyfikowanych problemów. Audytora wewnętrznego w sposób szczególny powinna zainteresować próba zdefiniowania sprawności instytucjonalnej samorządu gminnego. W badaniu punktem wyjścia były oczekiwania społeczności lokalnej, w szczególności przedsiębiorców. Prezentowane w części plenarnej wydarzenia badania przeprowadzone były w formie ankiet i objęły zakresem około 1200 gmin (tyle wypełniło ankietę badawczą i wzięło udział w badaniu). Naukowcy zdefiniowali czynniki wpływające na rozwój gospodarczy oraz przeanalizowali sprzężenie zwrotne pomiędzy sprawnością instytucjonalną a rozwojem gospodarczym.

Wyniki badań są dostępne publicznie, a użyte ankiety oraz stworzone na potrzeby badania definicje mogą zostać wykorzystane w realizacji audytu wewnętrznego. Materiały te dostępne są na stronie:

http://www.uwm.edu.pl/konferencjakpgir/pliki/raport_z_projektu.pdf

[18] Koordynator Warmińsko - Mazurskiego Koła Regionalnego IIA Polska CIA CGAP CRMA.

Urszula Kamińska[19]

Relacja z 16 Międzynarodowego Kongresu Kontroli Wewnętrznej, Audytu Wewnętrznego, Antykorupcji i Zwalczania Oszustw

Jak co roku, pod koniec września w Krakowie spotkali się specjaliści audytu i kontroli wewnętrznej, eksperci zwalczania oszustw i korupcji z kraju i zagranicy.

Prezydent Krakowa, Jacek Majchrowski w przesłanym do uczestników liście napisał m.in.: Z radością i satysfakcją przyjąłem wiadomość o ponownym wyborze naszego miasta na miejsce 16 Międzynarodowego Kongresu Kontroli Wewnętrznej, Audytu Wewnętrznego, Antykorupcji i Zwalczania Oszustw. (…) Właśnie mija 15 lat od chwili, gdy pod patronatem ówczesnego Prezesa Narodowego Banku Polskiego prof. Leszka Balcerowicza odbyło się w Krakowie pierwsze międzynarodowe spotkanie zorganizowane przez Polski Instytut Kontroli Wewnętrznej. Od tamtej pory rokrocznie, każdej jesieni, mamy zaszczyt gościć w naszym mieście uczestników tego jakże ważnego wydarzenia. Kongres trwale wpisał się w życie Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, zajął stałe i ważne miejsce wśród prestiżowych konferencji odbywających się w naszym mieście.

Prof. Klemens Budzowski - Kanclerz Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego

Wręczenie nagrody SUPER KONTROLER 2017: Magdalena Gorbaczuk - laureatka, Piotr Grzybowski i Ireneusz Jabłoński - członkowie Zarządu PIKW, organizatora konkursu

fot. Joanna Palka/PIKW

Krakowska Akademia od wielu jest naszym stałym partnerem – powiedział Piotr Grzybowski, członek zarządu PIKW. – Współorganizujemy podyplomowe studia dla audytorów wewnętrznych i innych specjalistów kontroli wewnętrznej, i to na kilku kierunkach, naukowe konferencje, a z Kongresem gościmy w Akademii już po raz 10.

[19] Redaktor Naczelna Kontroler INFO

To także już tradycja, że inauguracyjne przemówienie wygłosił Kanclerz Uczelni. Prof. Klemens Budzowski, witając uczestników, podkreślił, jak ważne jest łączenie nauki i praktyki codziennej i wyraził przekonanie, że ta właśnie formuła, zaproponowana 16 lat temu przez PIKW, jak zwykle przyniesie wiele korzyści wszystkim, którzy zdecydowali się na udział w tegorocznej imprezie.

Mieczysław Łuczak - Wiceprezes NIK

A Instytut zrobił kolejny krok na tej drodze. Zorganizował konkurs Super Kontroler 2017 na najlepsze naukowe opracowanie w dziedzinie systemów kontroli i bezpieczeństwa i zaprosił do Krakowa jego zwycięzczynię. Pani Magdalena Gorbaczuk odebrała dyplom, a z uczestnikami Kongresu podzieliła się swoimi dokonaniami i doświadczeniami.

Małgorzata Lazar, Łukasz Cichy, Piotr Chmiel - specjaliści Compliance

Na Kongresie bywam niemal od początku istnienia tej imprezy – powiedziała jedna z uczestniczek – i przyjeżdżam tu nie tylko po wiedzę, ale i nowe, profesjonalne kontakty. Wielokrotnie posiłkowałam się rozwiązaniami swoich polskich i zagranicznych kolegów. W tym roku nastawiłam się przede wszystkim na tematykę związaną z informacją, bezpieczeństwem i ochroną danych oraz kontrolą biznesową – dodała. Kiedy zauważyła, że patrzę na zaznaczone przez nią na agendzie Kongresu wystąpienia, z uśmiechem dodała: na następnej stronie zakreśliłam kolejne trzy prelekcje.

Marek Zieliński - ekspert kontroli biznesowej KIKB

fot. Joanna Pałka/PIKW

Udało się nam porozmawiać nie tylko ze stałymi bywalcami, ale i z osobami, które po raz pierwszy brały udział w Kongresie. Dla nich każde wystąpienie, każdy temat był ważny, nic więc dziwnego, że wszystkie wystąpienia robiły na słuchaczach wrażenie, a uczestnicy mieli tak wiele pytań. Aula była mocno rozdyskutowana, przez co obrady pierwszego dnia przedłużyły się ponad godzinę. Z największym oddźwiękiem spotkała się prelekcja Marka Zielińskiego, eksperta

Krajowego Instytutu Kontroli Biznesowej. Okazało się, że choć zagadnienie nie jest nowe, to temat kontroli biznesowej nie jest jeszcze właściwie rozpoznany. Przewidziany czas na pytania do prelegenta został trzykrotnie przekroczony i prowadzący zaproponował, by dyskusję dokończyć w kuluarach. Długo trzeba było czekać „w kolejce" ze swoim pytaniem czy problemem, ale udało się i w dziale „Bezpieczna Organizacja" można się o efektach naszych zabiegów o rozmowę przekonać.

A że podatki i kontrole podatkowe zawsze budzą emocje, nic więc dziwnego, że Janusz Jasiński Dyrektor Departamentu Zarządzania Strategicznego i Wdrożeń Ministerstwa Finansów także został zasypany gradem pytań.

Równie gorącymi tematami były zagadnienia związane z ochroną i bezpieczeństwem danych oraz nowymi obowiązkami przedsiębiorców, wynikającymi z wprowadzanego w życie rozporządzenia unijnego. Temat przedstawiano i omawiano w różnych kontekstach, zaprezentowano też dwa e-learnigowe kursy, które w tym mogą pomóc. Widać, że potrzeba jest duża, bo po wystąpieniu Krystyny Szawłowskiej z firmy TECHNE na taki kurs zapisało się kilkudziesięciu uczestników Kongresu.

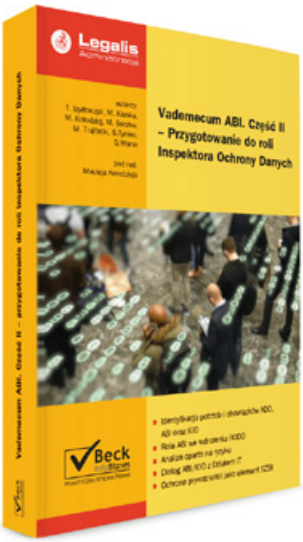
Mówiąc o biznesie pod kontrolą, działaniu zgodnym z prawem, zwalczaniu przestępstw gospodarczych i korupcji zawsze odwołać się trzeba do zagadnień związanych z etyką. I na tegorocznym kongresie sporo czasu im poświęcono.

Kilka wystąpień, w tym panel dyskusyjny zajęło się problematyką compliance. Temat okazał się interesujący i nie obyło się bez pytań z sali. Rozważania Piotra Chmiela: Compliance prawne czy Compliance etyczne: różne oczekiwania i różne zadania w ujęciu tej samej funkcji otrzymało od słuchaczy najlepszą recenzję – oklaski.

Na zakończenie przedstawiciele organizatora zaprosili uczestników 16 Kongresu na kolejne spotkanie już za rok.

Sebastian Burgemejster[20]

Recenzja Książki: „Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych”



Przyjęcie w dniu 27.04.2016 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (zwane dalej RODO), które zacznie obowiązywać od dnia 25.05.2018 r., spowodowało wzrost wymagań dla podmiotów przetwarzających dane osobowe. Jednocześnie wprowadzenie sankcji finansowych sięgających 4% światowego obrotu lub kwoty 20 000 000 Euro znacząco podniosło poziomy dla ryzyk zgodności.

Książka „Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych” pod redakcją Macieja Kołodzieja, Wydawnictwa C.H. Beck, Warszawa 2017 r. jest przewodnikiem w obszarze ochrony danych osobowych, jak również porusza podstawowe kwestie z obszaru cyberbezpieczeństwa bezpieczeństwa. Rozdział I opisuje uwarunkowania związane z przyjęciem RODO, jak również przedstawia zmiany jakie zostają wprowadzone w systemie ochrony danych osobowych. Rozdział II i III koncentruje się na roli Inspektora Ochrony Danych (jeszcze obecnego Administratora Bezpieczeństwa Informacji), w tym jego uprawnieniach i odpowiedzialnościach, w tym związanych zarówno z pełnieniem funkcji przez osobę zatrudnioną na umowę o pracę, jak i relacje B2B. Rozdział IV jest przewodnikiem po aspektach cyberbezpieczeństwa w pracy Inspektora Ochrony Danych, ale może również posłużyć innym osobom realizującym role zapewniające do poznania podstaw z tego obszaru. Rozdział V przedstawia „nową” w rozumieniu RODO koncepcję ochrony danych opartą o analizę ryzyka. Dla wielu osób zajmujących się zawodowo audytem, ryzykiem, compliance, bezpieczeństwem informacji takie rozwiązanie nie jest novum i wpisuje się w dotychczasowe bieżące działania. Należy jednak zwrócić szczególną uwagę na kwestie naruszenia poszczególnych atrybutów ochrony danych osobowych. Rozdział VI opisuje relacje pomiędzy wymaganiami bezpieczeństwa informacji, Krajowych Ram Interoperacyjności (dalej KRI), ochroną

[20] Prezes IIA Polska.

danych osobowych, a system zarządzania bezpieczeństwa informacji i ochrony danych osobowych. Jednocześnie autor dokonuje analizy wymagań normy ISO 27002 i KRI w kontekście ochrony danych osobowych. Rozdział VII koncentruje się na temacie powierzenia danych osobowych, wymaganiach oraz ryzykach z tym związanych. Ostatni VIII Rozdział przedstawia przykładowe wzory dokumentów wymaganych przez RODO.

Podsumowując należy podkreślić, iż przedstawiona publikacja powinna znaleźć się w bibliotece każdego ABI/IOD, jak również osób pełniących funkcje zapewniające w organizacjach, w których zakresie obowiązków będzie weryfikacja poziomu zabezpieczeń mitygujących ryzyka w obszarze wymagań RODO. Czego w książce mi zabrakło i mam nadzieję, że w kolejnym wydaniu ten obszar zostanie rozszerzony. Z uwagi, iż ryzyka związane z cyberbezpieczeństwem są w pierwszej trójce najbardziej poważnych ryzyk, jakie mogą dotknąć organizacje obszar technologii informatycznych oraz sposobu materializacji zagrożeń, w szczególności wynikających ze świadomego działania powinien zostać rozszerzony. Ponadto należałoby wskazać inne niż KRI i normy serii ISO 27000 wymagania i dobre praktyki w obszarze bezpieczeństwa informacji/cyberbezpieczeństwa.

Iwona Bogucka[21]

Recenzja książki Kazimiery Winiarskiej „Audyt Wewnętrzny. Teoria i zastosowanie”

Wydawnictwo Difin, Warszawa 2017, s. 351

Książka zawiera 11 rozdziałów oraz 6 załączników. Celem publikacji jest prezentacja roli audytu wewnętrznego. Na podstawie literatury zagranicznej autorka przedstawia zakres zastosowania audytu wewnętrznego i obowiązujące międzynarodowe standardy oraz główne obszary zainteresowania i kwalifikacje audytorów na świecie. Uwzględniając regulacje krajowe prezentuje metodykę prac audytowych i oceny ryzyka. W publikacji podkreślono wpływ wytycznych Unii Europejskiej na wprowadzenie audytu wewnętrznego w Polsce i jego powiązanie z kontrolą wewnętrzną i audytem zewnętrznym. W jedenastu rozdziałach przedstawiono kompleksowo problematykę audytu wewnętrznego, rozpoczynając od genezy, a kończąc wskazaniem przyszłości tej dyscypliny. Audytor wewnętrzny jest doradcą kierownika jednostki. Od audytora wewnętrznego oczekuje się niezależności i obiektywizmu oraz wykonywania pracy zgodnie z profesjonalnymi standardami czytamy we wstępie.

W pierwszym rozdziale zatytułowanym Pojęcie i klasyfikacja audytu wewnętrznego autorka przedstawia klasyfikację ról audytu wewnętrznego od tych podstawowych poprzez dopuszczalne funkcje, aż do prezentacji ról, których audyt wewnętrzny nie powinien pełnić. Rozdział drugi poświęcony rozwojowi audytu na świecie w zakresie aktualnych i perspektywicznych celów audytu wewnętrznego prezentuje wyniki badań w zakresie m.in. umiejętności behawioralnych, technicznych, kompetencji i wykształcenia audytorów wewnętrznych.

Rozdział trzeci poświęcony filozofii audytu wewnętrznego odnosi się do 10 przykazań, które powinni przestrzegać audytorzy wewnętrzni. Pierwsze: Pozostaw każde miejsce trochę lepszym, niż je zastałeś, inne: Każda niedoskonałość jest zakorzeniona w naruszeniu jakiejś zasady dobrego zarządzania i tak, aż do dziesięciu(…).

[21] Wiceprezes IIA Polska.

Rozdział czwarty Wpływ wytycznych Unii Europejskiej na wprowadzenie audytu wewnętrznego w Polsce odnosi się do początku instytucji audytu wewnętrznego, kiedy to realizując strategiczny cel pełnego członkostwa w Unii Europejskiej Polska zobowiązała się do racjonalizacji wydatków publicznych, dbałości o prawidłowe wykorzystanie środków pochodzących z UE oraz przeciwdziałania nadużyciom finansowym.

W sposób niezwykle interesujący autorka w rozdziale piątym Powiązania między audytem wewnętrznym a kontrolą wewnętrzną i audytem zewnętrznym przedstawia podstawowe zasady, które należy przestrzegać prowadząc audyt wewnętrzny.

Następne rozdziały odnoszą się do audytora wewnętrznego jako doradcy kierownika jednostki, standardów audytu wewnętrznego, zastosowania analizy ryzyka w audycie wewnętrznym. Natomiast rozdział jedenasty poświęcony jest przyszłości audytu wewnętrznego. Autorka odnosi się do 7 czynników, które w najbliższych latach wpłyną na funkcje audytu wewnętrznego. W przyszłości audyt wewnętrzny będzie musiał zmierzyć się ze złożonymi procesami gospodarczymi i skomplikowaną technologią.

Publikacja może być traktowana jako podręcznik dla osób przygotowujących się do egzaminu na audytora wewnętrznego oraz jako pomoc dla studentów piszących pracę z tematyki audytu wewnętrznego, a także dla praktyków z uwagi na niezwykle ciekawe i inspirujące wyniki prezentowanych badań.

XIII KONFERENCJA POLCAAT

IT GRC przyszłością zarządzania IT

30 listopada 2017 r. Hotel Marriott w Warszawie

Partner

Finat

Partroni

NIK · BCMG · PIBR · ISACA Katowice Chapter · ISACA Warsaw Chapter · POLRISK Stowarzyszenie

Patroni medialni

Audyt i Zarządzanie · KontrolerINFO · INFOR.PL · 4PM.p · Business&Prestige portal kobiet biznesu · KwF Kariera w Finansach.pl · IT w administracji · IT professional · brandsIT

www.iia.org.pl

15 LAT IIA Polska

Instytut Audytorów Wewnętrznych IIA Polska

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, (Podsumowanie)
   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.

informacje dla autorów

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.

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