AUDYT I ZARZĄDZANIE

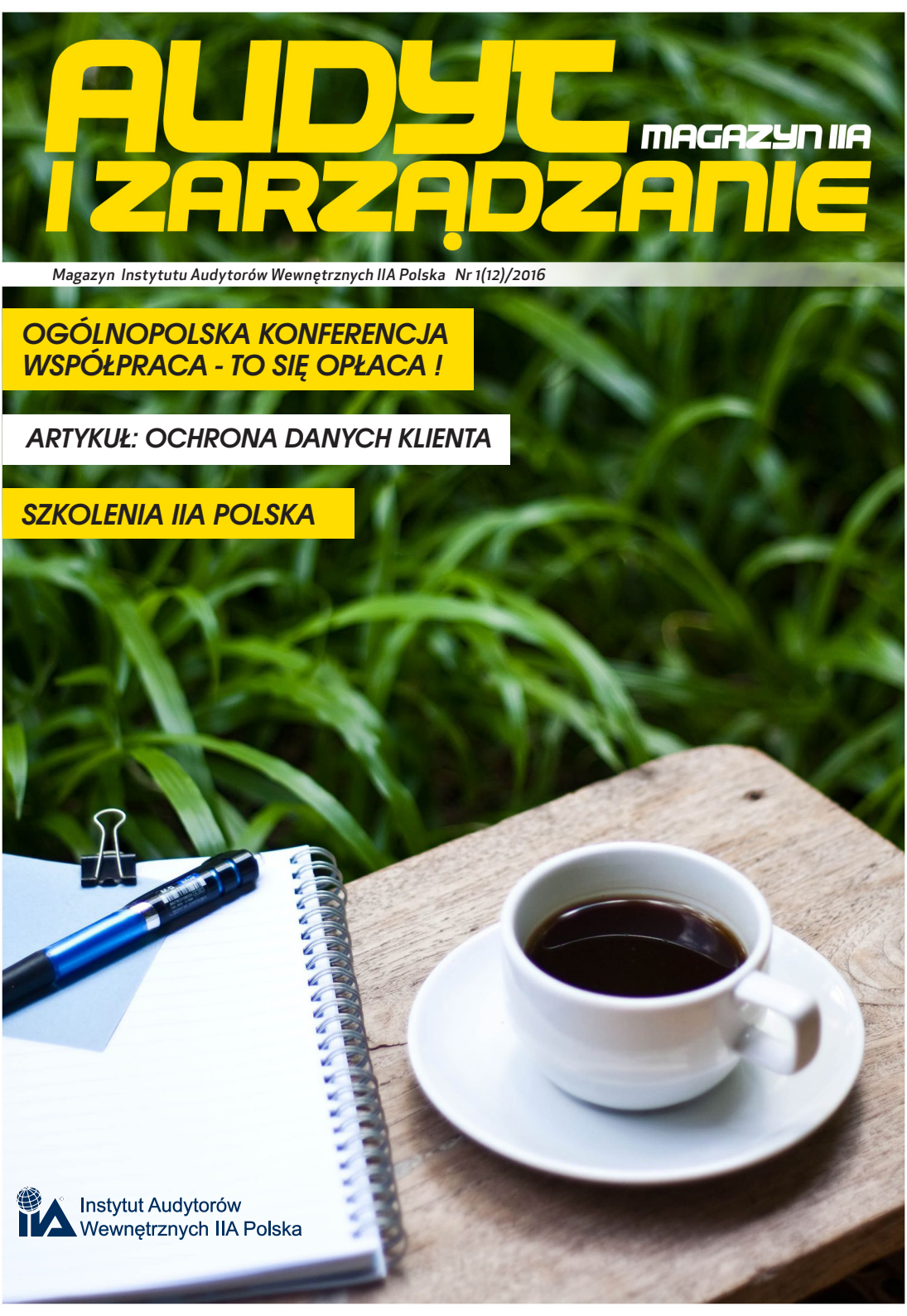
MAGAZYN IIA

Magazyn Instytutu Audytorów Wewnętrznych IIA Polska Nr 1(12)/2016

OGÓLNOPOLSKA KONFERENCJA WSPÓŁPRACA - TO SIĘ OPŁACA !

ARTYKUŁ: OCHRONA DANYCH KLIENTA

SZKOLENIA IIA POLSKA



Instytut Audytorów Wewnętrznych IIA Polska

SPIS TREŚCI:

Szanowni Państwo,

przestawiamy kolejny numer magazynu „Audyt i Zarządzanie". Mamy nadzieję, że wiosenny numer naszego czasopisma będzie dla Państwa również interesujący. Przygotowaliśmy ciekawy artykuł Ochrona danych Klienta jak również wiele informacji bieżących i ciekawą ofertę szkoleń.

Życzymy miłej lektury,
Zarząd IIA Polska

OGÓLNOPOLSKA KONFERENCJA WSPÓŁPRACA - TO SIĘ OPŁACA !

11-13 kwietnia 2016 r., Iława.

Aktualizacja i poszerzenie wiedzy ze szczególnym uwzględnieniem zmian w regulacjach, wymiana dobrych praktyk pomiędzy audytorami wewnętrznymi i osobami wykonującymi zawody pokrewne, promowanie dobrych praktyk zarządzania ze szczególnym uwzględnieniem CSR, duża dawka inspiracji i motywacji do działania, na co dzień to główne cele i zakres konferencji „Współpraca - to się opłaca!", organizowanej przez Instytut Audytorów Wewnętrznych IIA Polska.

Więcej informacji oraz agenda na stronie IIA Polska: LINK

W czasie konferencji, sesje będą odbywać się w czterech ciekawych blokach tematycznych przeplatanych panelami dyskusyjnymi nt.: współpracy audytu wewnętrznego z audytem zewnętrznym, Komitetem Audytu czy kontrolą. W ramach rozmów panelowych i sesji tematycznych skupimy się na wyzwaniach, jakie niosą zmiany w regulacjach i szansach, jakie stoją przed audytem wewnętrznym, jako głównym dostarczycielu usług zapewniających w organizacji.

Bloki tematyczne:

- Przywództwo i zarządzanie wiedza;
- Cyberbezpieczeństwo i IT;
- Metodyka pracy;
- Procesy operacyjne

Będzie nam również bardzo miło, zaprezentować Państwu w czasie konferencji przyjętą przez Zarząd strategię IIA Polska na lata 2015 – 2020.

Konferencja skierowana jest przede wszystkim dla: audytorów wewnętrznych, biegłych rewidentów, członków ACCA, audytorów zewnętrznych, kontrolerów i wszystkich innych, którzy na co dzień w pracy wykorzystują wiedze z zakresu audytu, zarządzania ryzykiem, ładu organizacyjnego jak i szeroko rozumianej praktyki zarządzania.

Partner strategiczny:

EY Building a better working world

Partnerzy Konferencji:

Think Ahead ACCA KibR 25 LAT GPW NIK

Patronat medialny:

INFOR

KONFERENCJA DOROCZNA 2016

Tegoroczna konferencja odbędzie się 16 czerwca 2016 r., w Warszawie.

Wstępny tytuł konferencji to „Trzy linie obrony. Przeżytek czy skuteczny system ochrony w turbulentnym środowisku?"

W konferencji udział weźmie przedstawiciel IIA Global jak również przedstawiciele polskich instytucji kontrolnych i regulatorów stanowiących 4 linię obrony oraz reprezentantów środowisk odpowiedzialnych za wypełnianie zadań z 2 linii obrony.

Już niedługo na stronie IIA Polska znajdą się szczegółowe informacje!

Już dzisiaj zarezerwuj sobie czas w kalendarzu! Zapraszamy.

OCHRONA DANYCH KLIENTA

Dla zagrożonych danych osobowych, audytorzy wewnętrzni muszą dostarczyć zapewnienia dla wielu aspektów, które składają się na bezpieczeństwo danych.

Michael Levy

Według Privacy Rights Clearinghouse, organizacji z San Diego zajmującej się badaniami oraz programami wsparcia, w ostatnich 10 latach w USA włamano się do ponad 750 milionów rekordów możliwych do personalnej identyfikacji, a ponad 80 milionów rekordów zostało narażonych na włamanie w samym roku 2015. Te incydenty obejmują różnego rodzaju typy naruszeń, włączając złośliwe hakerstwo, oszustwa związane z kartami płatniczymi, oraz fizyczną utratę aktywów. Definicja danych klienta obejmuje wszelkie dane, które zawierają informacje umożliwiające identyfikację personalną klienta jak np. dane medyczne, numery ubezpieczeń społecznych, informacje bankowe i dotyczące kart płatniczych, oraz informacje dotyczące prawa jazdy.

Organizacje mają naturalny obowiązek ochrony danych osobowych. Zostały także opracowane przepisy i wytyczne, które (organizacje) powinny przestrzegać w celu łagodzenia ryzyka braku zgodności. Jednak liczba naruszeń wskazuje, na to że organizacje muszą zintensyfikować swoje wysiłki (patrz „Kluczowe przepisy i wytyczne" na końcu artykułu). Mimo, Jest to okazja dla audytorów wewnętrznych, by pomóc swojej organizacji rozumieć, identyfikować oraz łagodzić potencjalne ryzyko wypływające zarówno ze źródeł wewnętrznych, jak i zewnętrznych.

Obrona Organizacyjna

Organizacje i ich pracownicy przechowują coraz więcej danych używając do tego celu różnych mediów, w tym urządzeń mobilnych oraz aplikacji opartych na technologii chmury (cloud). Wielorakość systemów, które mogą być użyte zwiększa ryzyko naruszenia bezpieczeństwa danych personalnych. W celu ochrony danych należy wprowadzać kontrole i inne środki zaradcze, które zajmują się zagrożeniami zarówno wewnętrznymi jak i zewnętrznymi.

Szkolenia i Edukacja

Ochrona danych klienta jest odpowiedzialnością nie tylko działu IT. Leaderzy Biznesu powinni rozumieć specyficzne ryzyka biznesowe i zapewnić, aby każdy w organizacji był przeszkolony, i był w stanie podjąć odpowiednie działania w celu ochrony danych swoich klientów.

Szyfrowanie danych

Stosowanie protokołów szyfrowania danych jest rzeczą fundamentalną, jeśli chodzi o ochronę danych klientów. Organizacje powinny zdefiniować dane wrażliwe i je szyfrować, aby zapewnić ich bezpieczeństwo. Szyfrowania na poziomie indywidulanego użytkownika zapewnia ochronę danych klienta. Okresowo, organizacje powinny ponownie oceniać swoje polityki dotyczące szyfrowania, aby w odpowiednim czasie identyfikować konieczne zmiany. Co więcej, powinny oceniać rodzaj obecnie używanego szyfrowania w celu weryfikacji, czy nadal ochrania ono przed najnowszymi zagrożeniami. Dla przykładu Standard Szyfrowania Danych DES (the Data Encryption Standard), który był rozwinięty w latach 70- tych nie jest

obecnie uważany za zapewniający bezpieczeństwo i został zastąpiony przez „Triple DES" i „the Advanced Encryption Standard" (Zaawansowany Standard Szyfrowania).

Ochrona przed utratą danych (Data Loss Prevention (DLP)

Organizacje, które przechowują duże ilości danych klientów powinny rozważyć korzystanie z narzędzi DLP (Ochrony Utraty Danych). Narzędzia te umożliwiają funkcji IT automatyzację i ochronę danych przed ich utratą, której źródło może być zarówno wewnętrzne jak i zewnętrzne. Co więcej, narzędzia mogą oceniać dane w ruchu i uniemożliwiać przypadkowe ujawniania opierając się na wcześniej ustalonych politykach.

Ryzyko związane z "chmurą" (cloud)

W ostatnich latach technologie „chmury" stały się głównymi strategiami operacyjnymi organizacji. Skalowalność oraz łatwość używania rozwiązań związanych z „chmurą" spowodowały, że są one atrakcyjnym rozwiązaniem. W trakcie przejścia do rozwiązania opartego na „chmurze", bezpieczeństwo danych musi być centralnym punktem w procesie decyzyjnym. Organizacje muszą rozumieć powstałe ryzyka posiadania danych klientów w „chmurze" i wymagać, by dostawca „chmury" stosował się do przynajmniej takich samych standardów i poziomu bezpieczeństwa, jakie są stosowane dla systemów własnych organizacji. Poprzez włączenie od samego początku w proces decyzyjny, audytor wewnętrzny może pomóc w zapewnieniu, że odpowiednie kontrole są wdrożone.

Urządzenia Mobilne

Przy coraz szerszym wykorzystaniu przez firmy oraz klientów smartfonów, tabletów, i innych

urządzeń mobilnych do wykonywania pracy i utrzymania kontaktu, ochrona danych staje się nadrzędna. Organizacje, które udostępniają te urządzenia dla swoich pracowników są w stanie zachować kontrolę nad danymi w celu zapewnienia ich bezpieczeństwa. Organizacje, która posiadają polityki „przynieś swoje własne urządzenie" (bring your own device – BYOD) mogą obniżyć swoje koszty związane z udostępnieniem urządzeń i dają pracownikom więcej elastyczności, ale zapewnienie bezpieczeństwa danych pozostaje wyzwaniem. Bez wykorzystania wyspecjalizowanych narzędzi, zgubione lub skradzione urządzenie mobilne mogą narazić dane klientów na szwank. W celu złagodzenia tego ryzyka wiele organizacji posiadających polityki „BYOD" używają oprogramowań, które chronią dane przed możliwością przechowywania na urządzeniach mobilnych.

Logi danych.

Organizacje muszą ustanowić polityki dotyczące logów danych wokół głównych serwerów oraz zapór ogniowych (firewalls), aby mieć możliwość badania incydentów związanych z bezpieczeństwem.. Jeśli nastąpi naruszenie, muszą znać źródło oraz skalę procederu. Logi są drogą do identyfikacji problemu w sposób szybki oraz kosztowo efektywny.

Rola Audytu Wewnętrznego

Dodatkowo do zapewnienia, że organizacje stosują te działania kontrolne, audyt wewnętrzny powinien przeprowadzić przegląd pozostałych aspektów ochrony danych.

Ocena ryzyka

Przeprowadzenie oceny ryzyka może pomóc audytorom zrozumieć specyficzne ryzyka otaczające dane klientów oraz technologię wykorzystaną do dostępu oraz ich przechowywania. Kadra zarządzająca oraz działy IT zazwyczaj są w stanie szybko zidentyfikować „bolące/chore miejsca" w procesie. Może umożliwić audytowi wewnętrznemu koncentrację na obszarach priorytetowych.

Strategia governance / ładu organizacyjnego

Jednym z pierwszych pytań, jakie audytor wewnętrzny powinien zadać zanim przystąpi do jakiegokolwiek projektu jest pytanie czy organizacja posiada strategię governance (ładu organizacyjnego), która wspiera ochronę danych klientów. Ten strategiczny dokument powinien w skrócie przedstawiać główne miejsca, gdzie są przechowywane dane klientów, rodzaj tych danych, i osoby odpowiedzialne za ich przechowywanie.

Ocena Benchmarkingu

Bezpieczeństwa IT Ostatnie szeroko znane naruszenia danych doprowadziły wiele organizacji do wprowadzenia zabezpieczeń w celu złagodzenia ryzyka poniesienia takiej samej szkody. Audyt wewnętrzny może dodać wartości poprzez benchmarking obecnych praktyk dotyczących bezpieczeństwa danych wobec standardów w branży i uznanych modeli takich jak the „National Institute of Standards" i „Technology Cybersecurity Framework". Taki benchmarking umożliwia audytorom identyfikację obszarów (braków), gdzie organizacja nie dorównuje standardom oraz wspieranie organizacji w rozwijaniu planu działania dla pojawiających się zagrożeń i poprawy procesu ochrony danych.

Polityka dotycząca klasyfikacji danych

Klasyfikacja danych to proces identyfikacji i kategoryzacji, tego co stanowi informacje wrażliwe wewnątrz organizacji oraz zdefinio-

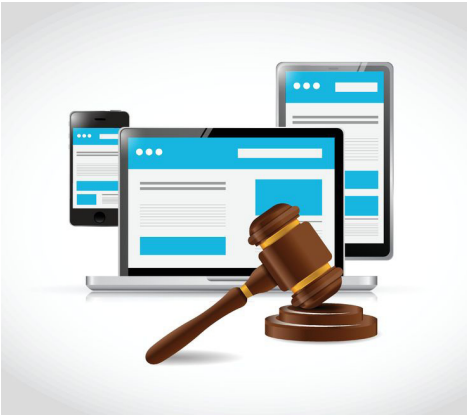
wania wymagań, co do dostępu oraz zajmowania się danymi w oparciu o ustaloną kategoryzację. Zrozumienie, w jaki sposób dane klientów są sklasyfikowane i ograniczanie dostępu pomaga w ochronie danych. Audytorzy wewnętrzni powinni ocenić i przetestować tę politykę, aby sprawdzić, czy jest ona wprowadzona w całej organizacji. Audytorzy powinni również upewnić się, czy polityka identyfikuje wszystkie dane klientów i jest spójna z tolerancją na ryzyko menadżerów.

Szkolenie i edukacja

Jeśli organizacja nie posiada solidnego programu szkoleniowego edukującego pracowników czym są dane klientów oraz jakie kroki powinny być podjęte w celu ich ochrony, audyt wewnętrzny może rekomendować sposoby wprowadzenia takiego szkolenia. Szkolenia mogą przybrać różne formy, włączając tradycyjne sesje szkoleniowe prowadzone w sali szkoleniowej, miesięczne konkursy na temat świadomości w obszarze bezpieczeństwa, oraz internetowe moduły szkoleniowe. Tematy, które powinny być pokryte zależą od środowiska biznesowego organizacji. Specjalistyczne tematy, które należy rozważyć obejmują obszary: bezpieczeństwa fizycznego, bezpieczeństwa nośników, haseł zabezpieczających, phishingu (wyłudzania danych), hoaxes (plotki, „łańcuszki"), oraz złośliwego oprogramowania.

Kluczowi Właściciele

Jeśli nie przedstawiono tego w organizacyjnej strategii ładu korporacyjnego, audyt wewnętrzny powinien potwierdzić, że organizacja wskazała rozlicznych właścicieli danych oraz określiła ich odpowiedzialność.. Audytorzy powinni przeprowadzić ocenę listy właścicieli oraz potwierdzić, że wszyscy posiadają wymagane kompetencje oraz uprawnienia. Dodatkowo, powinni oni współpracować z kadrą zarządzającą, by zrozumieć rolę każdego właściciela oraz potwierdzić, czy właściciele okresowo wykonują prowadzą działania w celu zabezpieczenia swoich danych.



Zgodność z przepisami

Dopóki nie jest to przypisane do innej funkcji w organizacji, roczny plan audytu wewnętrznego powinien weryfikować, czy organizacja działa w zgodzie z przepisami, które mogą się różnić w zależności od branży i kraju. Organy regulacyjne interesują się coraz bardziej bezpieczeństwem danych, co może skutkować dla organizacji zwiększeniem intensywności działań związanych z utrzymaniem zgodności.

Praca wewnątrz całego biznesu

Audyt wewnętrzny może mieć ogromny wpływ na ochronę danych klientów w swojej organizacji. Poprzez pracę wewnątrz całej firmy audyt wewnętrzny może uspójniać rozbieżności pomiędzy proponowanymi oraz aktualnymi strategiami, wymogami regulacyjnymi oraz tym, co każdy dział musi wykonać w celu uzyskania zgodności. W tej roli audyt wewnętrzny może stać się zaufanym doradcą dla biznesu i pomóc chronić organizację.

Kluczowe regulacje i wytyczne

W użyciu stosowanych jest szereg regulacji oraz modeli zarządzania ochroną i prywatnością danych., włączając w to najlepsze praktyki branżowe, które powinny być rozważone przez organizacje przy opracowywaniu swojej własnej strategii ochrony danych.

Regulacje prawne i branżowe

European Union (EU) Labor and Privacy Regulations Pracownicze Przepisy Unijne oraz regulacje dotyczące prywatności Pomimo znacznych różnić w zakresie, europejskie przepisy dot. pracy i ochrony danych osobowych skupiają się na możliwościach organizacji do monitorowania informacji obywateli, oraz ochrony ich „prawa do bycia zapomnianym". Organizacje muszą zapewnić, że posiadają polityki dot. przechowywana danych po to, by informacje na temat każdej osoby mogły być usunięte na jej życzenie.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA definiuje prywatność pacjenta i bezpieczeństwa w branży medycznej. HIPAA nakłada na dostawców usług zdrowotnych odpowiedzialność za ochronę szczegółowych typów danych pacjentów, które gromadzą. Przepisy dot. bezpieczeństwa HIPAA także ustanawiają odpowiednie szczegółowe kroki, które muszą być podjęte w celu zapewnienia bezpieczeństwa fizycznego, ochrony technicznej, dostępu i poufności danych pacjentów.

The Health Information Technology for Economic and Clinical Health Act (HITECH)

HITECH został ustanowiony w 2009 w celu poprawy jakości opieki zdrowotnej, bezpieczeństwa oraz efektywności.Regulacjom podlegają dane elektroniczne dot. zdrowia, by zapewnić, że wymiana danych jest bezpieczna i chroni informacje pacjentów.

Payment Card Industry Data Security Standard (PCI DSS)

Intencją PCI DSS jest zapewnienie, że wszystkie organizacje, które przetwarzają i przechowują dane kart kredytowych wykonują to w bezpiecznym środowisku. Ten standard do zapewnianie zgodności wymaga testowania i walidowania danych..

U.K. Information Commissioner's Office Data Protection Principles

Wielka Brytania ustanowiła ten organ, aby stał na straży prawa do prywatności informacji. Zasady Ochrony Danych zapewniają, że dane są przetwarzane oraz przechowywane w rzetelny sposób, w odpowiednim celu, oraz przez odpowiedni czas. Określone atrybuty dają pojedynczym osobom prawo dostępu do ich informacji, sprzeciwu co do danych, oraz domagania się zadośćuczynienia za szkody.

Modele

National Institute of Standards and Technology Cybersecurity Framework

Model ten przedstawia kluczowe standardy dot. bezpieczeństwa w sieci w celu przeciwdziałania i ochrony przed atakami cybernetycznymi. Model ten był ważnym krokiem w standaryzacji głównych zasad cyber-bezpieczeństwa w Stanach Zjednoczonych i dostarcza najlepszych praktyk na całym świecie.

COBIT

ISACA ustanowiło model COBIT w roku 1996 by sformalizować zarządzanie IT i ładem korporacyjnym. Najnowsza wersja COBIT 5 określa cele kontroli IT do wykorzystania przez osoby zajmujące się bezpieczeństwem danych, w celu tworzenia i optymalizacjić procesów oraz wsparcia ochrony danych klientów.

Oprócz powyższych modeli publikacja IIA pt. „Global Technology Audit Guide 15: Information Security Governance", dostarcza wytycznych w obszarze audytowania bezpieczeństwa danych. Dodatkowo, do ochrony danych może być zastosowana aktualizacja publikacji pt. "Internal Control–Integrated Framework" z roku 2013 wydana przez The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) .

O Autorze:

Michael Levy

Michael Levy, CRMA, CISA, CISSP, jest Managerem Audytu Wewnętrznego w firmie Burlington Stores Inc. in Burlington, N.J. Został uznany jako jeden z Wschodzących Leaderów roku 2013 przez magazyn "Internal Auditor" i obecnie pełni rolę przewodniczącego działu IIA " Emerging Leaders Task Force" (Grupa robocza IIA „Wschodzących Leaderów").

INICJATYWA DOLNOŚLĄSKIEGO KOŁA REGIONALNEGO „SPOŁECZNY PROGRAM PRZYGOTOWUJĄCY DO EGZAMINU CGAP"

Kolejny raz podjęliśmy w Kole Dolnośląskim IIA próbę wsparcia merytorycznego w przygotowaniach w części do egzaminu CGAP.

Grupa jaka powstała na początku liczyła ponad 30 osób, w efekcie końcowym 28 osób. W ocenie frekwencji uważam, że trudy i skomplikowane tematy szkolenia przeszło 19 osób (najwyższa frekwencja na szkoleniu) z czego, do 31 grudnia 2015 – wydano uczestnikom 13 rekomendacji. Dalsze rekomendacje – można powiedzieć, w drodze, bo ciągle ktoś z grupy deklaruje chęć przystąpienia do certyfikacji.

Tematyka szkolenia praktycznie objęła wszystkie wymagane tematy w poszczególnych domenach (I-IV). Uczestnicy szkolenia, członkowie i sympatycy IIA korzystali z materiałów zamieszczonych na stronie Instytutu, materiałów własnych oraz opracowanych przez wykładowców, kol.: Katarzynę Lenczyk-Woroniecką, Urszulę Prus, Małgorzatę Krystek i Ryszarda Juszczyka.

Praca szkoleniowa była przeprowadzona w formie prezentacji, wykładów oraz stałego, indywidualnego kontaktu z uczestnikami szkolenia drogą mailową.

Dlaczego inicjatywę wsparcia do egzaminu uważam za udaną?

Po pierwsze, zintegrowano na Dolnym Śląsku skutecznie – szkoleniowo, w sposób nie budzący wątpliwości, kolejnych członków i sympatyków IIA.

Po drugie, ludzie zaczęli pracować do egzaminu w grupach, wymieniają się doświadczeniem, spotykają się, celem kontynuacji nabytej wiedzy, są świadomi podnoszenia kwalifikacji.

Hasłami przewodnimi koordynatora szkolenia było – Nie macie innego wyjścia, musicie zdać egzamin…Ten egzamin jest do zadania :)

I co najważniejsze, gdyby nie zaangażowanie kol. Renaty Pradeli – koordynatora Koła Dolnośląskiego, kol. Mariana Lampczaka oraz życzliwości audytorskiej szefostwa Dolnośląskiego Ośrodka Doradztwa Rolniczego – szkolenie nie miałoby szans.

Teraz czekamy na „połamanie myszek" przy kompie na teście do CGAP. Oby jak najwięcej.

Ryszard Juszczyk

Dolnośląskie Koło Regionalne IIA Polska

★ ★ ★

Z ŻYCIA ZARZĄDU …

KOLEJNE POSIEDZENIA ZARZĄDU IIA POLSKA, W CZASIE KTÓRYCH:

1. Zarząd dokonał podsumowania swojej działalności za ostatnie pół roku. Uzgodniono wstępny katalog szkoleń, który został opublikowany na stronie internetowej IIA Polska. Tematami szkoleń będą między innymi:

- „Akademia Audytora – od identyfikacji procesów do programu audytu.
- „Ocena jakości audytu wewnętrznego QA"
- „Audyt w grupie kapitałowej"
- „ Audyt bezpieczeństwa informacji"
- „Prawo zamówień publicznych w świetle najnowszych zmian"
- Zintegrowane zarządzanie audytem projektów w organizacji"
- „Audyt poziomu dojrzałości etyki w organizacji"
- „Sztuka perswazji"
- Zarządzanie ryzykiem nadużyć w funduszach europejskich"
- „Radzenie sobie w trudnych rozmowach"

Zarząd II Polska zdecydował również o rozpoczęciu w połowie roku planowania szkoleń na rok 2017.

2. Została podjęta ostateczna decyzja oraz wstępne założenia konferencji:

Iława 11-13 kwietnia 2016. Osobą odpowiedzialną za konferencję jest Olga Petelczyc Wiceprezes IIA Polska.

Główne cele i zakres konferencji:

- aktualizacja i poszerzenie wiedzy ze szczególnym uwzględnieniem zmian w regulacjach;
- dobre praktyki – wymiana doświadczeń pomiędzy audytorami wewnętrznymi i osobami wykonującymi zawody pokrewne;
- promowanie dobrych praktyk zarządzania ze szczególnym uwzględnieniem CSR;
- duża dawka inspiracji i motywacji do działania, na co dzień.

Bloki tematyczne:

- Przywództwo i zarządzanie wiedzą;
- Cyberbezpieczeństwo i IT;
- Metodyka pracy;
- Procesy operacyjne.

Konferencja kierowana jest m.in. do: audytorów wewnętrznych, biegłych rewidentów, członków ACCA, audytorów zewnętrznych, kontrolerów i wszystkich innych, którzy, na co dzień w pracy wykorzystują wiedze z zakresu audytu, zarządzania ryzykiem, ładu organizacyjnego jak i szeroko rozumianej praktyki zarządzania.

Rozpoczęto promocję konferencji zarówno przez IIA Polska jak i Partnera strategicznego: EY, Partnerów merytorycznych: ACCA Polska, KIBR,GPW i NIK oraz Patrona medialnego: Infor.pl

Wszystkie informację dostępne są na stronie IIA Polska LINK

3. Konferencja Doroczna 2016 – data 16/06. Osoba koordynująca – Sebastian Burgemejster Prezes IIA Polska

Wstępny tytuł konferencji brzmi „Trzy linie obrony. Przeżytek czy skuteczny system ochrony w turbulentnym środowisku?" Na konferencji będzie przedstawiciel IIA Global. Planowane jest zaproszenie również innych zagranicznych gości oraz przedstawicieli polskich instytucji kontrolnych i regulatorów stanowiących 4 linię obrony oraz reprezentantów środowisk odpowiedzialnych za wypełnianie zadań z 2 linii obrony. Zostały również wysłane zaproszenia do wykładowców.

4. Informacje z Koła Finansowego. Wybrano zastępcę koordynatora koła Panią Magdę Maciejewską. Liderem projektu mentoringu została Pani Dominika Drzewiecka.

5. IIA Polska objął patronatem Konferencję „Sprawność i skuteczność zarządzania w świetle audytów prowadzonych w jednostkach sektora finansów publicznych"

Konferencja organizowana jest przez Koło Audytorów Wewnętrznych Jednostek Samorządów Terytorialnych IIA Polska oraz Łódzkie Koło Regionalne IIA Polska we współpracy z Katedrą Zarządzania Miastem i Regionem Wydziału Zarządzania Uniwersytetu .

Więcej informacji LINK

6. Trwają prace nad ponownym udziałem IIA Polska w Forum Samorządowym w Katowicach w dniach 22-23 września 2016 r.

7. Wypracowane standardy promocji dla:
- eventów;
- szkoleń;
- publikacji

Harmonogram działań został wysłany do wszystkich Koordynatorów Kół Regionalnych i Branżowych.

8. IIA Polska będzie jednym z partnerów merytorycznych konferencji w dniach 10-13 maja 2016r., w Kopenhadze, Annual CISO Europe Summit & Roundtable. Dla członków IIA Polska zniżka na udział w konferencji. Więcej informacji LINK

9. W tym 2016 roku w USA odbędą się uroczyste obchody 75-lecia IIA. IIA Polska reprezentować będą SB – Prezes, OP – Wiceprezes

10. Zarząd IIA wraz z Kołem Finansowym opracowuje zasady opiniowania aktów prawnych, standardów oraz wytycznych. W dokumencie mają znaleźć się zapisy zabezpieczające przed potencjalnym konfliktem interesów.

11. IIA Polska zawarł porozumienie o współpracy z IIA Ukraina. Trwają prace związane z nawiązaniem bliższej współpracy z NIK oraz KNF.

12. Zarząd IIA Polska przyjął Strategię na lata 2015-2020, która zostanie zaprezentowana w czasie Ogólnopolskiej Konferencji w Iławie.

Trwają dalsze prace nad strategią dotyczące mierników, wskaźników etc. Na tę chwilę obecną realizowana jest większość działań strategicznych.

13. Został omówiony plan finansowy IIA Polska na rok 2016. Sytuacja instytutu jest stabilna. Założenia budżetu będą osiągnięte.

14. Aktywności kół regionalnych.

Łącznie wszystkie Koła Regionalne zorganizowały 40 spotkań. Ukazały się artykuły w prasie lokalnej o wydarzeniach organizowanych przez IIA i KR.

15. Planowanie konferencji na II połowę roku.

Zostały zaplanowane Konferencje: finansowa i PolCAAT;

Branżowe Koło Finansowe i zespół organizacyjny od kwietnia rozpoczną opracowywać zarys konferencji. Wstępny termin konferencji to druga połowa października.

16. IIA Polska wystąpił do Biblioteki Narodowej o przyznanie numeru ISSN dla Magazynu „Audyt i Zarządzanie". Trwają prace nad powołaniem komitetu redakcyjnego.

★ ★ ★

RAPORTOWANIE NIEFINANSOWE: BUDOWANIE ZAUFANIA Z AUDYTEM WEWNĘTRZNYM

Przedstawiamy kolejną ciekawą i merytoryczną publikację Raportowanie niefinansowe: budowanie zaufania z audytem wewnętrznym, która opisuje różnorodne role jakie audytorzy wewnętrzni mogą odgrywać oraz rekomenduje zintegrowane podejście poprzez koordynowanie różnych dostawców usług zapewniających wewnętrznych jak i zewnętrznych.

Audyt wewnętrzny może odgrywać różne role w procesie wdrażania nowej dyrektywy: doradczą, zapewniającą oraz doradczo-zapewniającą. Audyt może również wspierać organizacje we wdrożeniu zintegrowanego zapewnienia. Ważne jest, aby role i obowiązki zostały jasno określone przez Radę, która jest ostatecznie odpowiedzialna za ład organizacyjny

Publikacja dostępną jest na stronie IIA Polska
LINK

★ ★ ★

SZKOLENIA IIA POLSKA

Szkolenia i rozwój zawodowy są integralną częścią pracy każdego profesjonalisty pragnącego utrzymać wysoki poziom wiedzy oraz ugruntować swoją pozycję jako zawodowca w swojej organizacji.

Dlatego też, kontynuując zapoczątkowany w 2014 roku cykl szkoleń, przedstawiamy listę szkoleń, które planowane są na pierwsze półrocze 2016 r.

Proponowane szkolenia są zarówno dla osób rozpoczynających swoją przygodę z audytem i kontrolą, jak i dla doświadczonych audytorów. Oferujemy zarówno szkolenia zawodowe jak i tzw. szkolenia miękkie.

Mamy nadzieję, że zaproponowane szkolenia spotkają się z Państwa zainteresowaniem. Jeżeli na naszej liście nie ma szkolenia / tematu, który byłby dla Państwa interesujący, prosimy o kontakt. Postaramy się spełnić Państwa oczekiwania.

W przypadku jakichkolwiek pytań prosimy o kontakt z biurem IIA Polska.

22/04 – „Audyt poziomu dojrzałości etyki w organizacji" (LINK)

25/04 - „Sztuka perswazji" (LINK)

26-27/04 - Szkolenie „Wprowadzenie do audytowania systemów zarządzania bezpieczeństwem informacji" (LINK)

10-11/05 - Szkolenie "Audytowanie kluczowych obszarów w zakresie zarządzania bezpieczeństwem informacji" (LINK)

12-13/05 - „Zarządzanie ryzykiem nadużyć w funduszach europejskich" (LINK)

19-20/05 - „Ocena jakości audytu wewnętrznego - QA" (LINK)

6/06 - Szkolenie "Nowe przepisy w zamówieniach publicznych w 2016 r. czyli implementacja (dyrektywy klasycznej 2014/24/UE oraz sektorowej 2014/25/UE) ale także zmiany nie wynikające z dyrektyw "(LINK)

10/06 - „Radzenie sobie w trudnych rozmowach" (LINK)

1-31/10 - Szkolenie „Akademia Audytora - od identyfikacji procesów do programu audytu" (LINK)

25-26/10 - Szkolenie „Wprowadzenie do audytowania systemów zarządzania bezpieczeństwem informacji"(LINK)

8-9/11 - Szkolenie "Audytowanie kluczowych obszarów w zakresie zarządzania bezpieczeństwem informacji" (LINK)

5-6/12 - Szkolenie "Ocena jakości audytu wewnętrznego - QA" (LINK)

SERDECZNIE ZAPRASZAMY!

CENTRUM EDUKACJI KIBR ZAPRASZA NA SZKOLENIA Z UMIEJĘTNOŚCI MIĘKKICH

Umiejętności miękkie są dziś niezbędne do prowadzenia biznesu na konkurencyjnym rynku. Przedstawiciele zawodów finansowych także powinni je nabywać. Dlatego Centrum Edukacji Krajowej Izby Biegłych Rewidentów poszerzyło o tę tematykę ofertę swoich kursów.

Warto doskonalić umiejętności miękkie

Na Uniwersytecie Harvarda od ponad 20 lat prowadzone są badania na temat inteligencji emocjonalnej, opisuje je w swoich książkach psycholog, autor bestsellerów - Daniel Goleman. Wynika z nich, że czynnikiem warunkującym sukces w życiu nie jest sam intelekt i stopnie uzyskiwane podczas edukacji, a właśnie inteligencja emocjonalna i społeczna - wyjaśnia Anna Dąbrowska, trener, coach, wykładowca Akademii Leona Koźmińskiego. Zdaniem Golemana sukces w życiu zależy w znacznej mierze od umiejętności kierowania emocjami i radzenia sobie w sytuacjach społecznych. Ta zasada dotyczy także sfery zawodowej. Bo umiejętności miękkie są dziś tak samo potrzebne do prowadzenie biznesu jak tradycyjne kompetencje twarde: wiedza techniczna czy ekspercka. Umiejętność komunikacji, budowania relacji, współpracy i pracy zespołowej, planowania czasu, rozwiązywania problemów, czy asertywność i autoprezentacja to dziś kompetencje, które mogą okazać się decydujące w wyścigu po klienta na konkurencyjnym rynku. A przedstawiciele zawodów finansowych, np. biegli rewidenci to także przedsiębiorcy, którzy muszą umieć odnaleźć się w biznesie. - Dobra informacja jest taka, że każdy może rozwijać obie formy inteligencji, zarówno inteligencję społeczną jak i emocjonalną - mówi Anna Dąbrowska. - Dlatego warto, żeby biegli także doskonalili te kompetencje - dodaje Ewa Sowińska zastępca prezesa KRBR i przewodnicząca Komisji ds. szkoleń.

KIBR uczy kompetencji miękkich

Jakich konkretnie kompetencji potrzebują zatem biegli rewidenci? Zdaniem Anny Dąbrowskiej będą to na pewno kompetencje komunikacyjne. - Biegli rewidenci powinni umieć rozmawiać ze swoimi klientami, wiedzieć, jak uzyskać od nich pożądane informacje, ale też powinni umieć potem w zrozumiały sposób przedstawić wyniki badania, odpowiedzieć na pytania klienta, przygotować prezentację dla innych pracowników firmy - wyjaśnia ekspert. Ważne też, żeby biegli rewidenci umieli być asertywni w komunikacji z klientem. To znaczy wiedzieć, jak radzić sobie w trudnych sytuacjach, np. gdy klient nie chcę podać jakichś informacji, albo wręcz odwrotnie, nadużywa kontaktów z audytorem, dzwoni w dzień i w nocy - wylicza Anna Dąbrowska i dodaje, że ważne i pożądane na rynku kompetencje to też umiejętność zarządzania projektami - bo przecież badanie to także pewien proces (swoisty projekt), który można usprawnić i sprawić by był bardziej efektywny. Ale kompetencje miękkie, których nie należy lekceważyć to także umiejętność zarządzania czasem, a więc dbanie o zachowanie równowagi między pracą a życiem osobistym. - Jedną nogą człowieka jest praca, ale jest też druga - życie osobiste - ciężko stać tylko na jednej nodze, potrzebujemy w życiu tego balansu.

Naprzeciw tym potrzebom kompetencyjnym

wyszła Krajowa Izba Biegłych Rewidentów. Teraz biegli rewidenci, ale nie tylko, bo kursy są dedykowane wszystkim zainteresowanym, będą mogli nabyć te wszystkie kompetencje w Centrum Edukacji KIBR. CEK poszerzył ofertę kursów właśnie o szkolenia z umiejętności miękkich. – Uczestnicy będą mieli szansę dowiedzieć się, jak prowadzić negocjacje w biznesie, jak skutecznie komunikować się z klientem, czy jak zarządzać projektami - wyjaśnia Ewa Sowińska. W trakcie kursów nauczą się jak efektywnie optymalizować czas, dowiedzą się też jak radzić sobie ze stresem. Wszystkie kursy będą prowadzone w formule warsztatowej. - W trakcie kursu uczestnicy będą angażowani w różnorodne działania, będą przepracowywane konkretne schematy odpowiadające realnym sytuacjom biznesowym - zapowiada Anna Dąbrowska, która będzie odpowiedzialna za prowadzenie kursów, i dodaje, że uczestnicy mogą spodziewać się pracy w grupach i na forum, ale też pracy indywidualnej, przykładów z życia, a nawet odgrywania scenek i gier.

Szkolenia z umiejętności miękkich jako samokształcenie

Od 16 lutego 2016 roku biegli rewidenci mogą szkolenia z umiejętności miękkich włączyć w zakres samokształcenia i zaliczyć tym samym część obligatoryjnego doskonalenia zawodowego. Krajowa Rada Biegłych Rewidentów przyjęła uchwałę, w której ustaliła tematykę samokształcenia biegłych rewidentów. Powinna ona obejmować głównie zagadnienia związane z wykonywaniem zawodu biegłego rewidenta i od 16 lutego po raz pierwszy dotyczyć może także umiejętności miękkich, których posiadanie niezbędne jest do wykonywania profesji. - Mogą to być szkolenia w obszarze bieżącej pracy z klientami (np. negocjacje biznesowe, zarządzanie projektami, sztuka prezentacji), budowania relacji z klientem (np. komunikacja, asertywność i współpraca) czy umiejętności osobistych wspierających efektywność działań (np. zarządzanie czasem) - wylicza Ewa Sowińska.

POZNAJ OFERTĘ KURSÓW CENTRUM EDUKACJI KIBR Z UMIEJĘTNOŚCI MIĘKKICH:

TERMIN	OFERTA	TEMAT	PROWADZĄCY
08.04.2016	POZNAJ PEŁNĄ OFERTĘ	Zarządzanie projektami w praktyce biegłego rewidenta	Anna Dąbrowska
28-29.04.2016	POZNAJ PEŁNĄ OFERTĘ	Skuteczne negocjacje w praktyce zawodowej	Anna Dąbrowska
12.05.2016	POZNAJ PEŁNĄ OFERTĘ	Style komunikacji czyli jak budować dobre relacje z klientami	Anna Dąbrowska
13.05.2016	POZNAJ PEŁNĄ OFERTĘ	Efektywne zarządzanie czasem czyli jak lepiej radzić sobie w sytuacji natłoku zadań	Anna Dąbrowska
03.06.2016	POZNAJ PEŁNĄ OFERTĘ	Jak prowadzić skuteczne prezentacje dla klientów cz. I	Anna Dąbrowska
10.06.2016	POZNAJ PEŁNĄ OFERTĘ	Komunikacja z klientami	Anna Dąbrowska
27.06.2016	POZNAJ PEŁNĄ OFERTĘ	Jak prowadzić skuteczne prezentacje dla klientów cz. II	Anna Dąbrowska
30.08.2016	POZNAJ PEŁNĄ OFERTĘ	Trening antystresowy	Anna Dąbrowska
31.08.2016	KURS WKRÓTCE DOSTĘPNY DO REJESTRACJI	Asertywność w praktyce biegłego rewidenta	Anna Dąbrowska

CENTRUM EDUKACJI KIBR

Wszelkie pytania prosimy kierować do Centrum Edukacji KIBR, pod adresem: ce@kibr.org.pl lub telefonicznie: 22 637 31 04. Więcej informacji - ce.kibr.org.pl

ogłoszenie

Chętni do współpracy poszukiwani – w nagrodę CPE!

IIA Polska poszukuje osób chętnych do podjęcia się tłumaczenia publikacji. Chętne osoby proszone są o zadeklarowanie jednej najbardziej preferowanej i trzech mniej preferowanych i przesłanie informacji zwrotnej na adres k.celinska@iia.org.pl. Godziny CPE za tłumaczenie będą przyznane zgodnie z Dyrektywą Administracyjną nr 4

1.Internal Audit and the Second Line of Defense LINK
2. Auditing Anti-bribery and Anti-corruption Programs LINK
3.Developing the Internal Audit Strategic Plan LINK
4.Evaluating Corporate Social Responsibility/Sustainable Development LINK
5. GTAG 12: Auditing IT Projects LINK

PRAKTYCZNE NARZĘDZIA ZARZADZANIA RYZYKIEM W JEDNOSTKACH SEKTORA PUBLICZNEGO

Wydawnictwo C.H. Beck
Warszawa 2015
Agata Kumpiałowska

Autorka zwraca uwagę, że system zarządzania ryzykiem jako element kontroli zarządczej to nowoczesne narzędzie zarządzania jednostką w celu osiągnięcia zaplanowanych celów i zadań w warunkach niepewności. Obserwując rozwiązania funkcjonujące w podmiotach publicznych, można stwierdzić, że często był on budowany w oderwaniu od życia jednostki. Wdrażane systemy są w wielu przypadkach zbyt skomplikowane i drogie w utrzymaniu, często niezrozumiałe dla użytkowników lub też odwrotnie, na tyle ogólnikowe, że nie mają odpowiedniego waloru informacyjnego dla zarządzających. Twierdzi także, że nowoczesne organizacje wiedzą, że nie można osiągnąć zamierzonych rezultatów bez właściwego zaangażowania pracowników zwracając uwagę na aspekt skutecznego zarządzania zespołem

W rozdziale skuteczne zarządzanie jednostką sektora finansów publicznych autorka podkreśla, że rozwój zarządzania w administracji publicznej stanowi dziś jedno z kluczowych wyzwań dla decydentów polskich instytucji, którzy to coraz częściej dostrzegają konieczność zmiany dotychczasowej formuły zarządzania, koncentrując swoja uwagę na zwiększeniu efektywności, skuteczności i racjonalność wydatkowania środków publicznych oraz podnoszenia jakości usług publicznych.

Drugi rozdział poświęcony jest doskonaleniu przyjętych rozwiązań kontroli zarządczej. Kilka lat funkcjonowania kontroli zarządczej, w tym systemu zarządzania ryzykiem w jednostkach sektora publicznego, pokazało, że organizacje te projektowały i wdrażały nie zawsze rozwiązania na podstawie diagnozy, która uwzględniałaby zarówno możliwości jednostki oraz potrzeby, jak i oczekiwania jej decydentów. Dlatego też zdaniem autorki modele dojrzałości są wartościowym narzędziem, cenionym i wykorzystywanym przez wiele instytucji, przede wszystkim z sektora prywatnego. Modele są bezpośrednim sposobem na to, jak opisać, rozpowszechnić, a także wdrożyć proces ulepszeń.

polecamy

W rozdziale trzecim znajdziemy wiele niezwykle cennych treści w zakresie wyznaczania celów jednostki i identyfikacji ryzyka. Ten rozdział odnosi się do różnej praktyki w zakresie wyznaczania celów i zadań administracji publicznej, a także przyjmowania określonych ram systemu zarządzania ryzykiem. Autorka podkreśla, że nie można dobrze zrozumieć istoty w zakresie wyznaczania celów, bez znajomości zasad dobrego zarządzania i oczekiwań, jakie są skierowane do decydentów w tym zakresie.

Rozdział czwarty odpowiada na pytania i dylematy związane z oceną skutków i prawdopodobieństwa ryzyka. Znajdziemy tu odpowiedź na pytanie jak dobrze przygotować się do szacowania ryzyka, jakie wykorzystać techniki oceny ryzyka, jakie przyjąć skale do oceny prawdopodobieństwa i skutku i ostatecznie jaka podjąć reakcję w stosunku do zidentyfikowanego ryzyka.

Rozdział piąty poświęcony jest monitoringowi. Zarządzanie ryzykiem zmienia się w jednostce wraz z upływem czasu, co jest zjawiskiem naturalnym. Sposoby reagowania na ryzyko- kiedyś odpowiednie, mogą w pewnym momencie, okazać się nieskuteczne.

W rozdziale szóstym znajdziemy wzory np. arkuszy identyfikacji ryzyka, okresowe sprawozdania itp. Do książki dołączona jest także płyta CD ze wzorami.

Polecam tym, którzy dopiero przystępują do projektowania modelu zarządzania ryzykiem, jak również praktykom do zweryfikowania zastosowanych w swoich jednostkach rozwiązań w zakresie kontroli zarządczej oraz przyjętych modeli zarządzania ryzykiem.

Iwona Bogucka

Członek zarządu IIA

★ ★ ★

stopka redakcyjna

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

REDAKCJA

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

telefon: +48 (22) 110 08 13

fax: +48 (22) 247 83 78

Redaktor Naczelna i skład:
Katarzyna Celińska

tel. 604 171 529

mail: k.celinska@iia.org.pl