BIBLIOTECZKA IZBY RZECZOZNAWCÓW PTI

Przemysław Jatkiewicz

Raport z badań:
Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego

35 lat PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

POLSKIE TOWARZYSTWO INFORMATYCZNE

Przemysław Jatkiewicz

Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego

Raport z badań

WARSZAWA 2016

ISBN 978–83–60810–82-8 (druk)
ISBN 978–83–60810–83-5 (e-book)

Badanie wykonał Zespół w składzie:

Przemysław Jatkiewicz (kierownik), Adam Mizerski, Krystyna Pełka-Kamińska, Anna Szczukiewicz, Janusz Żmudziński

Recenzenci:

Prof. dr hab. Zdzisław Szyjewski – Uniwersytet Szczeciński

Dr inż. Adrian Kapczyński – Politechnika Śląska w Gliwicach

Korekta: zespół

Skład: Marek W. Gawron

Wydawca:

POLSKIE TOWARZYSTWO INFORMATYCZNE
00-394 Warszawa, ul. Solec 38 lok. 103
tel. +48 22 838 47 05
e-mail: pti@pti.org.pl
www.pti.org.pl

Druk i oprawa:

ELPIL
08-110 Siedlce, ul. Artyleryjska 11
tel. +48 25 643 65 51
e-mail: info@elpil.com.pl

Wszystkie tabele, rysunki i wykresy, o ile nie zaznaczono inaczej, zostały wykonane przez Autora

Spis treści

Szanowni Państwo,

mamy przyjemność przekazać w Państwa ręce trzecią książkę z cyklu wydawniczego Polskiego Towarzystwa Informatycznego ***Biblioteczka Izby Rzeczoznawców PTI***.

Celem cyklu jest przedstawienie treści mogących zainteresować zarówno osoby zajmujące się zawodowo informatyką, jak i tych z Państwa, którzy w swojej pracy stykają się z zagadnieniami i problemami związanymi z informatyką.

Autorem trzeciego tomu z cyklu ***Biblioteczka Izby Rzeczoznawców PTI*** jest rzeczoznawca Izby Rzeczoznawców PTI, dr inż. Przemysław Jatkiewicz. Monografia prezentuje wyniki badań przeprowadzonych w roku 2015, a dotyczących przepisów Rozporządzenia Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, związanych z zarządzaniem systemami informatycznymi. W trybie dostępu do informacji publicznej pozyskano dane od 339 jednostek samorządowych, które pozwoliły na weryfikację postawionych na wstępie hipotez.

Zapraszamy do lektury niniejszego oraz poprzednich i kolejnych tomów z serii ***Biblioteczka Izby Rzeczoznawców PTI***.

Marian Noga

Prezes
Polskiego Towarzystwa Informatycznego

Tomasz Szatkowski

Dyrektor Izby Rzeczoznawców
Polskiego Towarzystwa Informatycznego

Warszawa 1 marca 2016 roku

Wstęp

30 maja 2012 roku weszło w życie rozporządzenie Rady Ministrów z 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[1], zwane w dalszej części jako KRI. Rozporządzenie zostało wydane na podstawie art. 18 ustawy z 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne[2]. Artykuł 18 zobowiązuje Radę Ministrów do określenia w drodze rozporządzenia, wymagań mających na uwadze zapewnienie między innymi:

- spójności działania systemów teleinformatycznych,
- sprawnej i bezpiecznej wymiany informacji w postaci elektronicznej,
- dostępu do zasobów informacji osobom niepełnosprawnym.

Zapisy KRI zaczynają obowiązywać w różnych terminach. Podmioty realizujące zadania publiczne zostały zobowiązane do dostosowania systemów teleinformatycznych do standardu WCAG 2.0 na poziomie AA[3] w ciągu 3 lat, a więc do dnia 1 czerwca 2015 roku.

Sposób zarządzania usługami realizowanymi za pomocą systemów teleinformatycznych, wymiana danych pomiędzy systemami, jak i system zarządzania bezpieczeństwem informacji, powinny spełniać przepisy KRI przy wdrożeniu lub w dniu ich pierwszej istotnej modernizacji. Wobec dużego znaczenia wspomnianych przepisów dla procesu informatyzacji instytucji publicznych oraz dochodzących alarmujących sygna-

[1] Dz.U. 2012 poz. 526.
[2] Dz.U. 2005 nr 64 poz. 565.
[3] Web Content Accessibility Guidelines (WCAG) 2.0 W3C Recommendation 11 December 2008.

łów o ich realizacji w organizacjach samorządowych, Polskie Towarzystwo Informatyczne, na mocy uchwały Zarządu Głównego nr 027 / XII / 2015 z 24 stycznia 2015 roku, podjęło prace badawcze związane z oceną stanu wdrożenia KRI w jednostkach samorządowych.

Metodyka

Celem badania było stwierdzenie, czy jednostki samorządowe spełniają przepisy KRI lub podjęły prace nad wdrożeniem odpowiednich mechanizmów. Przeprowadzono je w pierwszych 3 kwartałach 2015 roku. Badana populacja liczyła 2 917 podmiotów, na które składały się urzędy marszałkowskie, powiatowe, miejskie i gminne.

Sformułowano następujące hipotezy badawcze:

Hipoteza 1: Większość badanych podmiotów nie zarządza usługami realizowanymi za pomocą systemów teleinformatycznych zgodnie z przepisami KRI.

Hipoteza 2: Stopień wdrożenia przepisów KRI dotyczących zarządzania usługami realizowanymi za pomocą systemów teleinformatycznych jest zależny od wielkości podmiotu, liczby i wykształcenia osób związanych z IT.

Hipoteza 3: Większość badanych podmiotów nie wdrożyła prawidłowo systemu zarządzania bezpieczeństwem informacji.

Hipoteza 4: Stopień wdrożenia systemu zarządzania bezpieczeństwem informacji zależy od wielkości podmiotu, liczby i wykształcenia osób związanych z IT.

Hipoteza 5: Większość systemów teleinformatycznych służących do prezentacji zasobów informacji badanych podmiotów nie jest zgodnych ze standardem WCAG 2.0.

Hipoteza 6: Jednostki wyższego szczebla bardziej dbają o zgodność swoich systemów teleinformatycznych służących do prezentacji zasobów informacji ze standardem WCAG 2.0.

Hipoteza 7: Główną przeszkodą we wdrożeniu KRI jest brak adekwatnych kwalifikacji kadry badanych jednostek.

W celu weryfikacji wymienionych hipotez, jak również uzyskania dodatkowych cennych informacji, opracowano ankietę stanowiącą załącznik nr 1.

Hipotezę nr 1 weryfikowano na podstawie odpowiedzi na pytania szczegółowe. Można ją uznać za prawdziwą, jeśli większość z badanych podmiotów spełnia przynajmniej 1 z 3 następujących warunków:

1) Posiadanie certyfikatu zgodności z PN-ISO/IEC 20000[4] zgodnie z § 15. 3 KRI.
2) Przeszkolenie przynajmniej 1 pracownika lub zakup normy PN-ISO/IEC 20000 wraz z przeprowadzeniem audytu na zgodność z PN-ISO/IEC 20000.
3) Posiadanie przynajmniej po 1 udokumentowanej procedurze zgodnie z § 15. 2 KRI, dotyczącej wdrażania, eksploatacji, wycofywania i testowania aktywów teleinformatycznych.

Hipotezę nr 2 weryfikowano na podstawie ustalenia zależności pomiędzy wielkością jednostki, określoną na podstawie jej szczebla zgodnie z tabelą 1, a liczbą punktów przyznawanych wedle klucza prezentowanego w tabeli 2.

Tabela 1. Klasy wielkości w odniesieniu do szczebla instytucji

Rodzaj urzędu	Wielkość jednostki
Urząd Marszałkowski	Duża
Urząd Miejski w mieście na prawach powiatu	Duża
Urząd Dzielnicy (Warszawa)	Duża
Urząd Powiatowy	Średnia
Urząd Miejski	Średnia
Urząd Miasta i Gminy	Mała
Urząd Gminy	Mała

[4] PN-ISO/IEC 20000-1: 2007 – Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja, PN-ISO/IEC 20000-2: 2007 – Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania.

Tabela 2. Punktacja cech dla hipotezy nr 2

Punktowana cecha	Liczba punktów
Szkolenie przynajmniej 1 osoby z zakresu wymagań PN-ISO/IEC 20000 lub zakup normy PN-ISO/IEC 20000	**4**
Audyt na zgodność z PN-ISO/IEC 20000	4
Procedura wdrażania nowych aktywów teleinformatycznych	1
Procedura bieżącej eksploatacji aktywów teleinformatycznych	1
Procedura wycofania aktywów teleinformatycznych	1
Procedura testowania systemów teleinformatycznych	1

Hipotezę nr 3 można uznać za prawdziwą, jeśli większość z badanych podmiotów spełnia przynajmniej 1 z 3 następujących warunków:

1) Posiadanie certyfikatu zgodności z PN-ISO/IEC 27001[5], zgodnie z § 20. 3 KRI.
2) Przeszkolenie przynajmniej jednego pracownika oraz przeprowadzenie audytu na zgodność z PN-ISO/IEC 27001.
3) Posiadanie i aktualizowanie:
    a. inwentaryzacji aktywów teleinformatycznych,
    b. analizy ryzyka,
    c. rejestru incydentów,
    d. polityki bezpieczeństwa i informacji opartych o PN-ISO/IEC 27001.

Hipotezę nr 4 weryfikowano na podstawie ustalenia zależności pomiędzy wielkością jednostki, określoną na podstawie jej wielkości zgodnie z tabelą 1 oraz liczbą i wykształceniem kadry odpowiedzialnej za zarządzanie przetwarzaniem informacji, w powiazaniu z liczbą punktów przyznawanych zgodnie z kluczem prezentowanym w tabeli 3.

[5] PN-ISO/IEC 27001:2014, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Tabela 3. Punktacja cech dla hipotezy nr 4

Punktowana cecha		Liczba punktów
Szkolenie przynajmniej 1 osoby z zakresu wymagań PN-ISO/IEC 27001 lub zakup normy PN-ISO/IEC 27001		15
Audyt na zgodność z PN-ISO/IEC 27001		15
Szkolenie przynajmniej 1 osoby z zakresu wymagań PN-ISO/27005 lub zakup normy PN-ISO/IEC 27005[6]		1
Szkolenie przynajmniej 1 osoby z zakresu wymagań PN-ISO/24762 lub zakup normy PN-ISO/IEC 24762[7]		1
Wykonanie inwentaryzacji aktywów teleinformatycznych		7
Wykonanie analizy ryzyka		6
Prowadzenie rejestru incydentów		6
Ustanowienie polityki bezpieczeństwa informacji	według UODO	1
	według PN-ISO/27001	2
	okres przeglądu poniżej roku	1
	okres przeglądu powyżej roku	-1
	audytowanie	1
	aktualizacja	1

Warunkiem przyznania punktów za wykonanie inwentaryzacji aktywów teleinformatycznych było podanie w ankiecie daty jej wykonania, liczby aktywów, aktywnych węzłów sieci oraz baz danych. Uznano, iż liczba aktywów teleinformatycznych oraz aktywnych węzłów sieci znacząco mniejsza niż liczba zatrudnionych pracowników (10%) jest błędem i oznacza niepoprawne wykonanie inwentaryzacji. W takiej sytuacji punkty nie były przyznawane.

[6] PN-ISO/IEC 27005:2014, PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
[7] PN-ISO/IEC 24762:2010, Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

Punkty za wykonanie analizy ryzyka były przyznawane, jeśli podana została metodyka oraz data aktualizacji, a czas jaki upłynął od jej wykonania nie był dłuższy niż 1 rok.

Uznano, iż badany podmiot prowadzi rejestr incydentów, jeśli zadeklarowano w ankiecie jego prowadzenie i określono datę rejestracji ostatniego incydentu.

Weryfikacja hipotezy nr 5 polegała na kontroli zgodności w badanych podmiotach systemów teleinformatycznych służących do prezentacji zasobów informacji ze standardem WCAG 2.0.

Pełny audyt wszystkich systemów jest zadaniem daleko wykraczającym poza możliwości zespołu realizującego badania. Badania przeprowadzono jedynie wobec startowych stron BIP w zakresie zgodności z wytycznymi zamieszczonymi w tabeli 4.

Tabela 4. Kontrolowane wytyczne WCAG 2.0

Zasada	Wytyczna	Kontrolowana cecha
Zasada nr 1: Postrzegalność	Wytyczna 1.1 Alternatywa w postaci tekstu	1.1.1 Treść nietekstowa: wszelkie treści nietekstowe przedstawione użytkownikowi posiadają swoją tekstową alternatywę, która pełni tę samą funkcję
	Wytyczna 1.4 Możliwość rozróżnienia	1.4.3 Kontrast (minimalny): wizualne przedstawienie tekstu lub obrazu tekstu posiada kontrast wynoszący przynajmniej 4,5:1
Zasada nr 4: Solidność	Wytyczna 4.1 Kompatybilność	4.1.1 Parsowanie: w treści wprowadzonej przy użyciu języka znaczników, elementy posiadają pełne znaczniki początkowe i końcowe, elementy są zagnieżdżane według swoich specyfikacji, elementy nie posiadają zduplikowanych atrybutów oraz wszystkie ID są unikalne, za wyjątkiem przypadków, kiedy specyfikacja zezwala na wyżej wymienione cechy

Do kontroli zgodności wyszczególnionych cech z poszczególnymi wytycznymi, użyto W3C Markup Validation Service oraz przeglądarkę Mo-

zilla Firefox z zainstalowanymi dodatkami WAVE Toolbar i WCAG Contrast checker.

Hipotezę nr 6 weryfikowano na podstawie liczby systemów spełniających kontrolowane cechy eksploatowanych przez poszczególne klasy i wielkości instytucji przedstawione w tabeli 1.

Prawdziwość hipotezy nr 7 sprawdzono na podstawie odpowiedzi na pytanie nr 7 ankiety, w którym respondenci przyznają punkty 0÷5 dla czynników, które stanowiły problem przy ustanowieniu i wdrożeniu Polityki bezpieczeństwa.

Pomimo, że badana populacja nie jest zbyt duża, zdecydowano się na reprezentacyjną metodę badań. Przyjęto, iż cechy mają rozkład hipergeometryczny, który przybliżono rozkładem normalnym i zastosowano następujący wzór na minimalną wielkość próby[8]:

$$n = \frac{p(1-p)u^2}{\delta^2 + \frac{p(1-p)u^2}{N}} \quad (1)$$

gdzie:

n – liczebność próby
N – liczebność populacji
δ^2 – błąd
p – wielkość frakcji
u – 1.96, kwantyl rozkładu normalnego dla testu dwustronnego przy poziomie ufności 95%.

Przy liczebności próby wynoszącej 2 917, błędzie 5% oraz przyjętej wielkości frakcji 0,5 minimalna liczebność próby to 339.

W celu wyboru obiektów wykonano losowanie bez zwracania, warstwowe, przy pomocy generatora liczb pseudolosowych. Oddzielnie losowano podmioty należące do każdego rodzaju wyszczególnionego w tabeli 1, z uwzględnieniem częstości jego występowania w populacji. Liczby wylosowanych podmiotów przedstawiono w tabeli 5.

[8] J. Steczkowski, *Metoda reprezentacyjna w badaniach zjawisk ekonomiczno-społecznych*, Wydawnictwo Naukowe PWN, Warszawa 1995, s. 190.

Tabela 5. Liczba wylosowanych podmiotów

Rodzaj urzędu	Liczba wylosowanych podmiotów
Urząd Marszałkowski	2
Urząd Miejski w mieście na prawach powiatu	8
Urząd Dzielnicy (Warszawa)	2
Urząd Powiatowy	36
Urząd Miejski	38
Urząd Miasta i Gminy	70
Urząd Gminy	183
Razem	**339**

Przebieg badań

Do wszystkich wylosowanych podmiotów wysłano pocztą ankiety w formie wniosku o udostępnienie informacji publicznej. Przyjęta forma miała zagwarantować szybki i 100% zwrot ankiet, gdyż w myśl art. 4 ust. 1 p. 4 ustawy z 6 września 2001 roku o dostępie do informacji publicznej[9], organy administracji samorządowej zobowiązane są do jej udostępnienia a termin udzielenia odpowiedzi wynosi 14 dni.

Generalnie termin 14 dni nie był dotrzymywany. Ankiety systematycznie spływały przez okres 1,5 miesiąca, w trakcie którego odbierano liczne telefony z prośbą o dodatkowe informacje lub przedłużenie terminu odpowiedzi. Urzędnicy zwracali się z pytaniami o znaczenie terminów: aktywa informacyjne i aktywne węzły sieci. Nie rozumieli też, co oznacza metodyka wykonania analizy ryzyka.

Nieliczni respondenci upierali się, iż nie mogą udzielić odpowiedzi ze względu na politykę ochrony informacji. Problem dotyczył zwłaszcza pytania nr 2 w zakresie liczby aktywów, węzłów i baz danych oraz pytania nr 3 w zakresie rejestracji incydentów.

Zdaniem autora zastrzeżenia te są bezpodstawne, gdyż zgodnie z ustawą o dostępie do informacji publicznej: „*Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych*". Ankieta nie zawierała pytań o dane osobowe, a traktowanie odpowiedzi jako tajemnicy przedsiębiorstwa wydaje się nadinterpretacją. Większość informacji, które pozyskiwane były podczas badań, zostało niemalże

[9] Dz.U. 2001 nr 112 poz. 1198.

wprost wymienionych w art. 6 ustawy o dostępie do informacji publicznej, co zostało zaprezentowane w tabeli 6.

Tabela 6. Odniesienie pytań ankiety do rodzajów informacji publicznej wyszczególnionych w ustawie o dostępie do informacji publicznej

Nr pytania	Treść	Odniesienie	Rodzaj informacji publicznej
1.	Zakupione normy	Art. 6.1 2f	Majątek podmiotów realizujących zadania publiczne
1.	Przeszkolone osoby	Art. 6.1 2d	Kompetencje osób pełniących funkcje w podmiotach realizujących zadania publiczne
1.	Audyty i certyfikacje	Art. 6.1 4a	Dokumentacja przebiegów i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających
2.	Inwentaryzacja	Art. 6.1 4a	Dokumentacja przebiegów i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających
2.	Analiza ryzyka	Art. 6.1 4a	Dokumentacja przebiegów i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających
3.	Rejestr incydentów	Brak odniesienia	
4.	Polityka bezpieczeństwa	Art. 6.1 4a	Treść i postać dokumentów urzędowych Dokumentacja przebiegów i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających
5.	Liczba i kompetencje pracowników	Art. 6.1 2a i 2d	Organizacja podmiotów realizujących zadania publiczne Kompetencje osób pełniących funkcje w podmiotach realizujących zadania publiczne
6.	Procedury	Art. 6.1 3	Zasady działania podmiotów realizujących zadania publiczne

Respondenci trzykrotnie zauważyli, iż pytanie nr 3 odnosi się do opinii, nie zaś informacji publicznej. Zarzut ten jest – niestety – słuszny.

Dwukrotnie wpłynęło wezwanie do uzupełnienia braków formalnych i złożenia wniosku zgodnego ze wzorem określonym w rozporządzeniu

Ministra Administracji i Cyfryzacji z 17 stycznia 2012 roku w sprawie wzoru wniosku o ponowne wykorzystanie informacji publicznej[10].

Według urzędników, z treści złożonego wniosku (ankieta), wynika że jest on zgodnie z treścią art. 23a ust. 1 ustawy o dostępie do informacji publicznej, wnioskiem o udostępnienie informacji publicznej w celu jej ponownego wykorzystania. Treść przytoczonego przepisu jest następująca: „*Wykorzystywanie przez osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej informacji publicznej lub każdej jej części, będącej w posiadaniu podmiotów, o których mowa w ust. 2 i 3, niezależnie od sposobu jej utrwalenia (w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej), w celach komercyjnych lub niekomercyjnych, innych niż jej pierwotny publiczny cel wykorzystywania, dla którego informacja została wytworzona, stanowi ponowne wykorzystywanie informacji publicznej i odbywa się na zasadach określonych w niniejszym rozdziale*". Ponieważ interpretacja wydaje się jak najbardziej prawidłowa, ponowiono wniosek przy użyciu odpowiedniego formularza zgodnego ze wzorem.

Definitywnie nie można się jednak zgodzić z żądaniem uzasadnienia wniosku. Przedstawiciel Urzędu Gminy Jedlnia Letnisko uzależnił udzielenie odpowiedzi od wykazania powodów, dotyczących każdego z 7 punktów wniosku, dla których spełnienie jego żądania będzie szczególnie istotne dla interesu publicznego. Za podstawę swojego stanowiska przyjął przepisy art. 3.1 ust. 1 ustawy o dostępie do informacji publicznej o brzmieniu „*Prawo do informacji publicznej obejmuje uprawnienia do uzyskania informacji publicznej, w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego*".

Poparł je fragmentem uzasadnienia wyroku Wojewódzkiego Sądu Administracyjnego w Poznaniu z 23 stycznia 2014 roku: „*Informacją przetworzoną będzie zatem taka informacja, co do której podmiot zobowiązany do jej udzielenia nie dysponuje taką »gotową« informacją na dzień złożenia wniosku, ale jej udostępnienie wymaga podjęcia dodatkowych czynności. Reasumując informacja będzie miała charakter informacji przetworzonej w sytuacji gdy jej udostępnienie co do zasady wymaga dokonania stosownych analiz, obliczeń,*

[10] Dz.U. 2012 poz. 94.

zestawień statystycznych itp. połączonych z zaangażowaniem w ich pozyskanie określonych środków osobowych i finansowych"[11].

Pominął jednak znaczący fragment mówiący o tym iż: „*Nie stanowi zaś przesłanki dla uznania informacji publicznej za informację przetworzoną okoliczność, iż wymaga ona poszukiwania w zasobach archiwalnych podmiotu zobowiązanego. W dalszym ciągu chodzi bowiem o informację, której udostępnienie nie wymaga jakichkolwiek analiz, obliczeń, zestawień statystycznych itp., a jedynie prostego odnalezienia jej w zbiorze dokumentów*". Podkreślić należy, że odpowiedzi na pytania zawarte w ankiecie nie wymagały dokonywania żadnych analiz, zestawień czy obliczeń.

W tym samym piśmie powołano się również na wyrok Naczelnego Sądu Administracyjnego z 5 kwietnia 2013 roku[12], który stwierdza: „*… informacją przetworzoną jest informacja publiczna opracowana przez podmiot zobowiązany przy użyciu dodatkowych sił i środków, na podstawie posiadanych przez niego danych, w związku z żądaniem wnioskodawcy i na podstawie kryteriów przez niego wskazanych, czyli innymi słowy informacja, która zostanie przygotowana »specjalnie« dla wnioskodawcy wedle wskazanych przez niego kryteriów. Informacja przetworzona to taka informacja, której wytworzenie wymaga intelektualnego zaangażowania podmiotu zobowiązanego*".

Sprawdzenie danych w prowadzonych przez urząd rejestrach lub oficjalnych dokumentach czy procedurach wymaga wysiłku intelektualnego znacznie mniej intensywnego niż włożony w przygotowanie takiej odpowiedzi.

W konkluzji przytoczono także wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 7 marca 2013 roku[13]: „*W sytuacji, w której nieudzielenie informacji publicznej przetworzonej następuje z powodu niewykazania, że jest to szczególnie istotne dla interesu publicznego, należy wydać decyzję o odmowie udzielenia informacji. »Odmowa« pozytywnego załatwienia wniosku nie może następować poprzez decyzję umarzającą postępowanie. (…) w przypadku ustalenia, że nie zachodzą przesłanki określone w art. 3 ust. 1 pkt*

[11] II SAB/Po 123/13.
[12] I OSK 89/13.
[13] II SA/Po 1060/12.

1 u.d.i.p., organ powinien wydać decyzję o odmowie udzielania informacji publicznej".

Dane, o które wnioskowano w toku badań, zdecydowanie nie można uznać za informację przetworzoną, gdyż wynikają wprost z odpowiednich dokumentów, które nie mają nawet charakteru archiwalnego. W tej sytuacji należy stosować przepis art. 2.2 ustawy o dostępie do informacji publicznej – „*Od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego*".

Operacji przeniesienia informacji na papier i przesłania do wnioskującego nie można traktować jako przetworzenia lecz jako przekształcenie[14].

Brak możliwości odpowiedzi na pytania ankietowe urzędnicy tłumaczyli również rozpoczynającym się właśnie procesem wdrożenia Polityki bezpieczeństwa i trwającą inwentaryzacją na potrzeby opracowywanej analizy ryzyka (Starostwo Powiatowe w Augustowie). W badaniach chodziło jednak o ustalenie stanu faktycznego na dzień złożenia wniosku, nie zaś o efekty, jakie w przyszłości być może zostaną osiągnięte.

Jeden z urzędników uznał, że nie musi udzielić odpowiedzi, powołując się na przepisy § 23: „*Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o których mowa w rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia*".

Urząd, który reprezentował, od dnia wejścia w życie KRI do dnia złożenia wniosku nie dokonał żadnej istotnej modernizacji. Pomylony został w tym przypadku wymóg dostosowania systemów informatycznych do przepisów KRI z obowiązkiem udzielenia informacji publicznej. Badania, a tym samym pytania zawarte w ankiecie, miały na celu między innymi odpowiedź na pytanie o stopień przygotowania urzędu.

[14] *Ustawa o dostępie do informacji publicznej: komentarz*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002, s. 32.

W rezultacie wszystkich zastrzeżeń i odmów, z 339 respondentów odpowiedzi udzieliło jedynie 254. Zdecydowano się więc na wniesienie zażalenia na niezałatwienie sprawy w terminie – na podstawie art. 37 Kodeksu postępowania administracyjnego[15] – do Samorządowych Kolegiów Odwoławczych, odpowiednich dla poszczególnych urzędów. Treść zażalenia stanowi załącznik nr 2. Zażalenia, podpisane przez Dyrektor Generalną Zarządu Głównego Polskiego Towarzystwa Informatycznego, składane były za pośrednictwem urzędów, których dotyczyły.

Spora liczba respondentów zareagowała niemal natychmiast, dzwoniąc i prosząc o wycofanie pisma, obiecując jednocześnie niezwłoczne załatwienie sprawy. Rozwiązanie takie było efektem oczekiwanym przez prowadzących badania i pozwoliło na uzyskanie kolejnych 44 odpowiedzi. Pozostali respondenci rozpatrywali sprawy we własnym zakresie lub prawidłowo przekazywali je do Samorządowych Kolegiów Odwoławczych. Kolegia te wzywały Polskie Towarzystwo Informatyczne do przedstawienia upoważnienia Dyrektor do reprezentowania Towarzystwa oraz okazania dowodu nadania pisma, z uwagi na oświadczenia urzędów o braku przedmiotowej korespondencji. Wskazywały też na Wojewódzkie Sądy Administracyjne jako jednostki właściwe do rozpatrywania dalszych zażaleń, w tym na bezczynność urzędów.

Ponieważ celem było ukończenie badań, nie zaś wikłanie się w spory prawne mogące je w sposób znaczący opóźnić, podjęto decyzję o dopuszczeniu do umorzenia spraw i wykonaniu dodatkowego losowania uzupełniającego pulę respondentów.

Na rysunku 1 pokazano procentowy rozkład udzielenia odpowiedzi w efekcie podjętych działań.

[15] Dz.U. 1960 nr 30 poz. 168.

Rys. 1. Procentowy rozkład udzielenia odpowiedzi

4 Wyniki badań

4.1. Stosowanie norm PN-ISO/IEC

Badane urzędy zakupiły łącznie 31 norm wyszczególnionych w KRI, przy czym najmniejszym zainteresowaniem cieszyła się norma PN-ISO/IEC 20000, dotycząca zarządzania usługami realizowanymi przez systemy teleinformatyczne. Zdecydowana większość instytucji tj. 309, co stanowi ponad 91% badanych, nie zakupiła ani jednej normy. W zakresie stosowania odpowiednich norm PN-ISO/IEC dokonano 2 973 szkolenia przypadające na pojedynczego urzędnika, co stanowi ok. 11% zatrudnionych (niektórzy urzędnicy byli jednak szkoleni z kilku norm).

Szczegółowe dane odnośnie szkoleń zostały zaprezentowane w tabeli 7.

Tabela 7. Szkolenia w zakresie stosowania norm PN-ISO/IEC

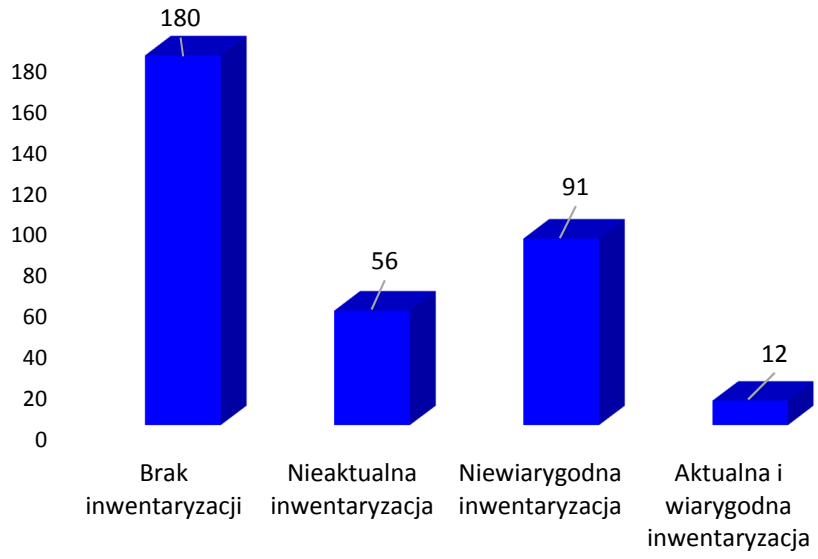
Norma	Liczba przeszkolonych	Liczba urzędów realizujących szkolenia
PN-ISO/IEC 20000	106	6
PN-ISO/IEC 27001	2 564	23
PN-ISO/IEC 27005	160	11
PN-ISO/IEC 24762	143	6

Jedynie 7 urzędów przeprowadziło audyt na zgodność z normą PN-ISO/IEC 20000. Audyt dotyczący normy PN-ISO/IEC 27001 wykonało trochę więcej organizacji, tj. 24. Znacznie mniej uzyskało certyfikat – odpowiednio 3 i 10 urzędów – przy czym oba posiadał jedynie Urząd Miasta Bydgoszczy oraz Urząd Gminy Świdwin.

4.2. Inwentaryzacja aktywów teleinformatycznych

Wykonanie inwentaryzacji aktywów teleinformatycznych zadeklarowało 159 urzędów (46,9%) przy czym aktualną, nie starszą niż dwa lata, posiadały 103 jednostki (30,38%). Pomimo deklaracji, 46 urzędów nie potrafiło podać liczby aktywów, zaś kolejnych 40 podało liczbę mniejszą od sumy aktywnych węzłów sieci i baz danych. Dodatkowo 5 następnych określiło liczbę aktywnych węzłów sieci znacząco mniejszą niż liczba pracowników. Szczegóły zostały przedstawione na rysunku 2.

Ponieważ niemal każdy z pracowników urzędu wykonuje pracę biurową i dysponuje zapewne komputerem, wydaje się mało prawdopodobne, by liczba aktywnych węzłów sieci (komputery, laptopy, przełączniki, routery, serwery, drukarki sieciowe) stanowiła 90% lub mniej liczby pracowników urzędu. Reasumując, wiarygodną i aktualną inwentaryzację posiadało jedynie 3,54% badanych organizacji.

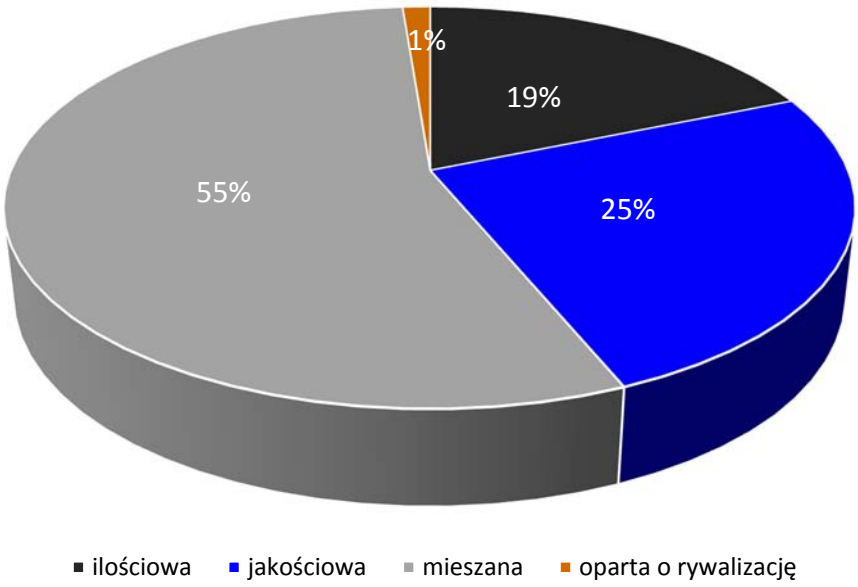


Rys. 2. Inwentaryzacje aktywów teleinformatycznych w badanych instytucjach

4.3. Analiza ryzyka

Niewiele instytucji opracowało analizę ryzyka. Z deklaracji wynika, że zrobiły to 81 jednostki (23,89%). Jedna natomiast (Urząd Gminy Mińsk Mazowiecki) odmówiła odpowiedzi, powołując się na Politykę bezpieczeństwa informacji. Jedynie 61 analiz można uznać za aktualne.

Rodzaje zastosowanych metodyk zostały zaprezentowane na rysunku 3.



Rys. 3. Rodzaje zastosowanych metodyk

Znamiennym jest, że respondenci nie umieli ustalić bądź nie znali nazw użytych metodyk. Wymieniali następujące nazwy, których większość, oznaczonych kolorem czerwonym, nie jest nazwami metodyk analizy ryzyka:

- burza mózgów (Starostwo Powiatowe w Wadowicach),
- FMEA,
- Prince 2 (Starostwo Powiatowe w Siedlcach),
- arytmetyczna (Starostwo Powiatowe w Kościerzynie),
- CMMI for Services v. 1.3,

- PMI (Urząd Gminy Niemce),
- CRAMM,
- delficka (Urząd Miasta Bydgoszcz),
- indukcyjna (Urząd Miasta i Gminy Twardogóra, Urząd Gminy w Liskowie),
- MEHARI,
- ręczna (Urząd Miejski w Łomży).

Większość z nich ma bardzo luźny związek z metodykami wykonania analiz ryzyka i dotyczy raczej zarządzania projektami lub metod badawczych. Pomimo ewidentnego braku wiedzy, tylko 11 badanych jednostek skorzystało z pomocy firm zewnętrznych. Zauważono także, iż co najmniej 7 analiz ryzyka nie było poprzedzonych inwentaryzacją aktywów teleinformatycznych.

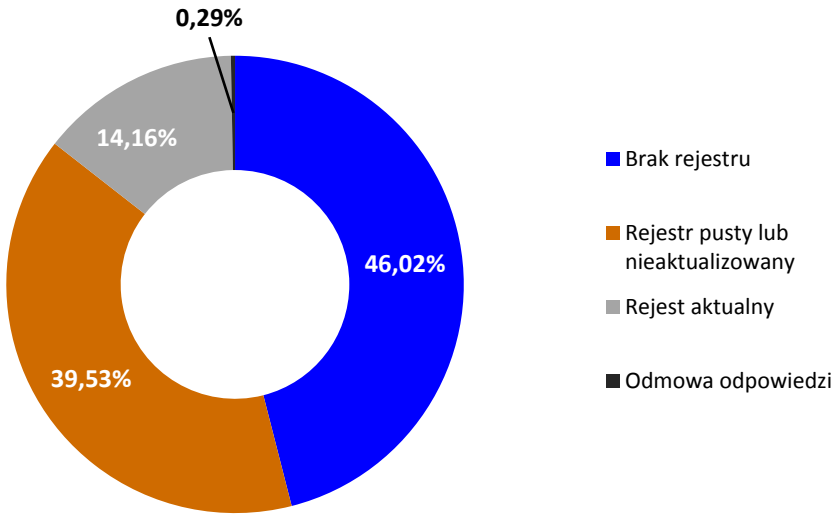
4.4. Rejestr incydentów

Ponad połowa (53,69%) respondentów zadeklarowała prowadzenie rejestru incydentów, jednakże 134 pozostają puste, gdyż nie zarejestrowano w nim żadnego incydentu. Urząd Gminy Nowy Targ uznał natomiast, iż udzielenie informacji dotyczących prowadzenia rejestru incydentów stanowi zagrożenie informacji.

Szczegółowe informacje zostały zaprezentowane na rysunku 4 na następnej stronie.

W roku 2014 zarejestrowano łącznie 11 375 incydentów. Mediana incydentów (zarejestrowanych w prowadzonych, niepustych rejestrach) wynosi zaś 4. Taka niska wartość mediany w stosunku do dużej liczby incydentów wynika ze sposobu rejestracji prowadzonej przez Urząd Marszałkowski Województwa Podkarpackiego, który rejestruje zdarzenia z systemów antywirusowych czy IDS/IPS (*Intrusion Detection System / Intrusion Prevention System*). Instytucja ta w roku 2014 zarejestrowała 11 000 incydentów. Cześć z incydentów było na tyle poważnych, iż 13 urzędów zgłosiło je do Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT, Agencji Bezpieczeństwa Wewnetrznego lub prokuratury.

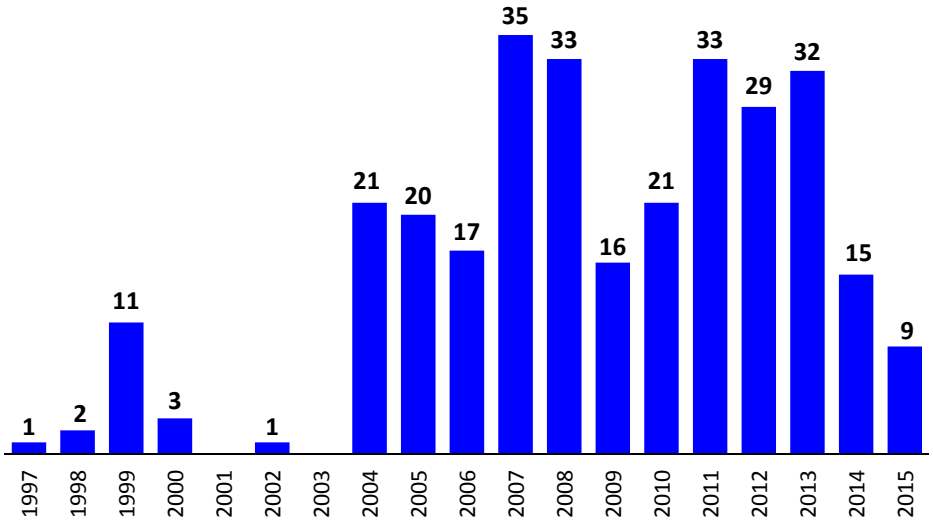
Warto zauważyć, że 3 urzędy (miasta Jaworzno, miasta Marki i gminy Łuków) dokonały takich zgłoszeń, lecz nie prowadzą rejestru incydentów.



Rys. 4. Rejestry prowadzone przez badane instytucje

4.5. Polityka bezpieczeństwa

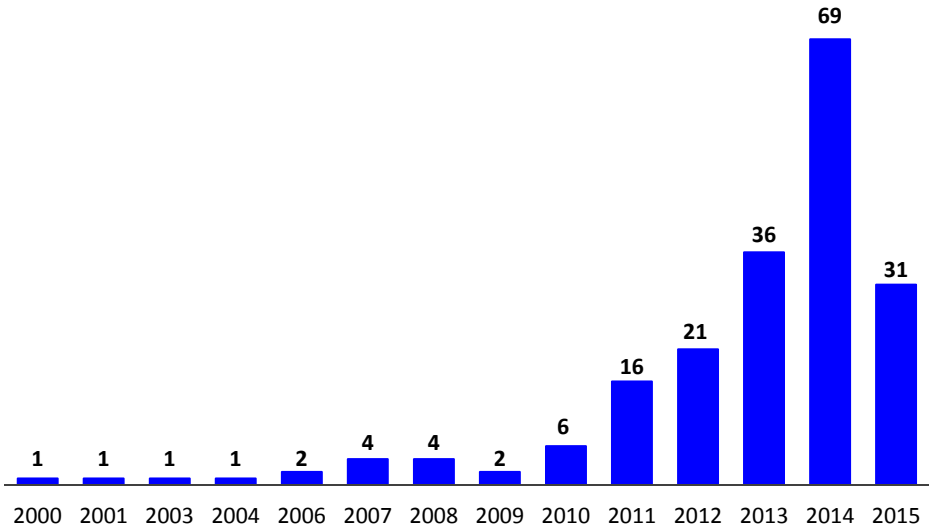
Około 12% urzędów (40 jednostek) nie posiada Polityki bezpieczeństwa informacji. Urząd Gminy Narewka – w przesłanym piśmie – uważa, że nie ma potrzeby jej opracowania. Pozostałe ustanowiły ją w bardzo różnym czasie, co zostało pokazane na rysunku 5. Spośród wspomnianych 40 instytucji, 33 posiada zarejestrowane zbiory danych osobowych w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO).



Rys. 5. Liczba ustanowień Polityk bezpieczeństwa w latach 1997-2015

Ostatnie zmiany w ustawie z 29 sierpnia 1997 roku o ochronie danych osobowych[16], wniesione ustawą z 7 listopada 2014 roku o ułatwieniu wykonywania działalności gospodarczej, obowiązują od 1 stycznia 2015 roku. Dlatego też należy uznać, iż wszystkie polityki wydane przed rokiem 2014 i nieaktualizowane w latach 2014-2015 są już nieaktualne.
Biorąc powyższe pod uwagę można stwierdzić, że liczba aktualnych polityk wynosi 114 sztuk. Na rysunku 6 przedstawiono liczbę ostatnich aktualizacji Polityk bezpieczeństwa badanych jednostek w latach 1997-2015. Zauważono także, iż część respondentów (28) podało tą samą datę ustanowienia i aktualizacji. Przy formułowaniu wniosków traktowano takie przypadki jako nieaktualizowane. Pomimo że 205 ankietowanych deklarowało roczny lub krótszy okres aktualizacji, to ponad 39% z nich aktualizowało swoje Polityki po co najmniej dwuletnim okresie czasu.

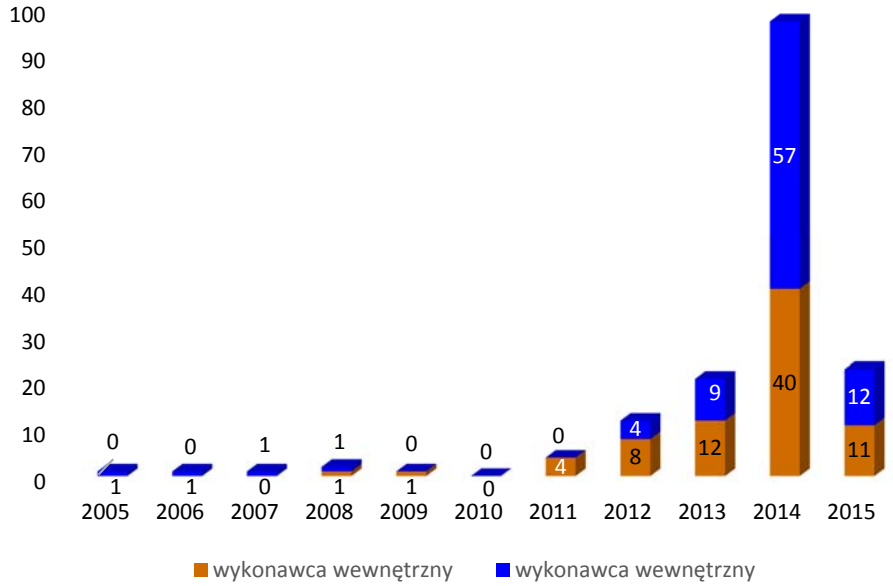
[16] Dz. U. 2014 r. poz. 1182.



Rys. 6. Liczba aktualizacji Polityk bezpieczeństwa w latach 1997-2015

Z przeprowadzonych badań wynika, że prawie połowa urzędów (48,08%) przeprowadziła audyt swojej Polityki bezpieczeństwa. Większość z nich (86), wykonała go własnymi siłami, zaś 77 posiłkowało się firmami zewnętrznymi.

Jak widać na rysunku 7, nowelizacja ustawy o ochronie danych osobowych z roku 2014 stymulowała przeprowadzenie audytów. Znamiennym jest, iż 5 organizacji przeprowadziło audyt, lecz nie posiada Polityki bezpieczeństwa. Wszystkie zamieściły informację o trwających pracach nad jej ustanowieniem, choć w przypadku Urzędu Miasta i Gminy w Zdunach, biorąc pod uwagę datę audytu, prace te trwają już około 6 lat.



Rys. 7. Przeprowadzone w latach 2005-2015 audyty Polityki bezpieczeństwa informacji

4.6. Zasoby ludzkie

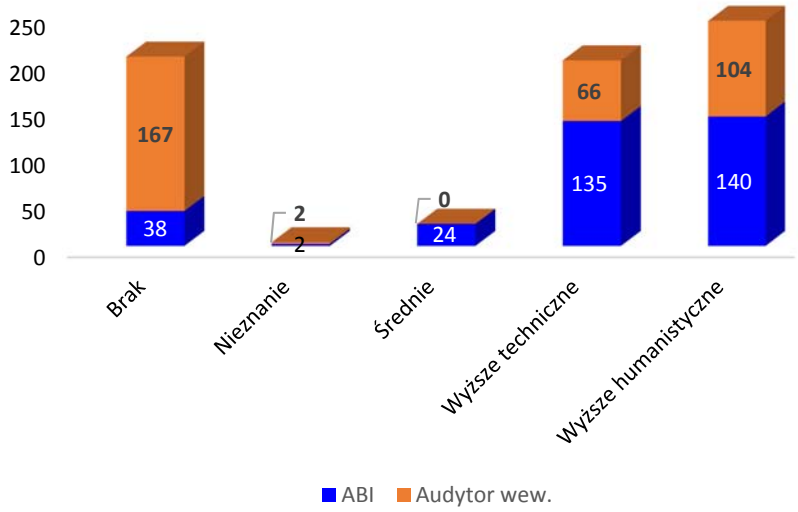
Większość urzędów (93,81%) zatrudnia informatyków, jednakże nie wszyscy z nich posiadają wykształcenie techniczne.

Dane odnośnie wykształcenia technicznego służb IT przedstawiono w tabeli 8.

Tabela 8. Kadra IT badanych jednostek

Wykształcenie	Liczba informatyków	Liczba urzędów
Brak służb IT	0	21
Wyższe techniczne	406	241
Inne	190	77
Razem (wykształcenie techniczne i inne)	596	318

Nieznacznie mniej (88,79%) jednostek posiada administratora bezpieczeństwa informacji. Znacznie mniejsza liczba urzędów (50,74%) zatrudnia audytorów wewnętrznych. Strukturę wykształcenia osób pełniących omawiane funkcje przedstawia rysunek 8. Brak oznacza nieobsadzone stanowisko. Nieznajomość wykształcenia administratora bezpieczeństwa czy audytora wewnętrznego świadczy zapewne o tym, że czynności przypisane tym funkcjom wykonują wynajęte osoby.



Rys. 8. Wykształcenie osób pełniących funkcje administratora bezpieczeństwa informacji i audytora wewnętrznego

Brak audytora wewnętrznego z wykształceniem średnim związany jest z wymaganiami ustawy z 27 sierpnia 2009 roku o finansach publicznych:

„Art. 286. 1. Audytorem wewnętrznym może być osoba, która:

1) ma obywatelstwo państwa członkowskiego Unii Europejskiej lub innego państwa, którego obywatelom, na podstawie umów międzyna-

rodowych lub przepisów prawa wspólnotowego, przysługuje prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej;

2) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

3) nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe;

4) posiada wyższe wykształcenie;

5) posiada następujące kwalifikacje do przeprowadzania audytu wewnętrznego:

a) jeden z certyfikatów: Certified Internal Auditor (CIA), Certified Government Auditing Professional (CGAP), Certified Information Systems Auditor (CISA), Association of Chartered Certified Accountants (ACCA), Certified Fraud Examiner (CFE), Certification in Control Self Assessment (CCSA), Certified Financial Services Auditor (CFSA) lub Chartered Financial Analyst (CFA), lub

b) złożyła, w latach 2003–2006, z wynikiem pozytywnym egzamin na audytora wewnętrznego przed Komisją Egzaminacyjną powołaną przez Ministra Finansów, lub

c) uprawnienia biegłego rewidenta, lub

d) dwuletnią praktykę w zakresie audytu wewnętrznego i legitymuje się dyplomem ukończenia studiów podyplomowych w zakresie audytu wewnętrznego, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi ustawami, do nadawania stopnia naukowego doktora nauk ekonomicznych lub prawnych"[17].

4.7. Procedury

Najwięcej procedur opracowanych i wdrożonych w urzędach dotyczy eksploatacji. Znacznie mniejsza liczba związana jest z wdrożeniem nowych aktywów, wycofaniem aktywów z eksploatacji oraz testowaniem.

[17] Dz.U. 2009 nr 157 poz. 1240.

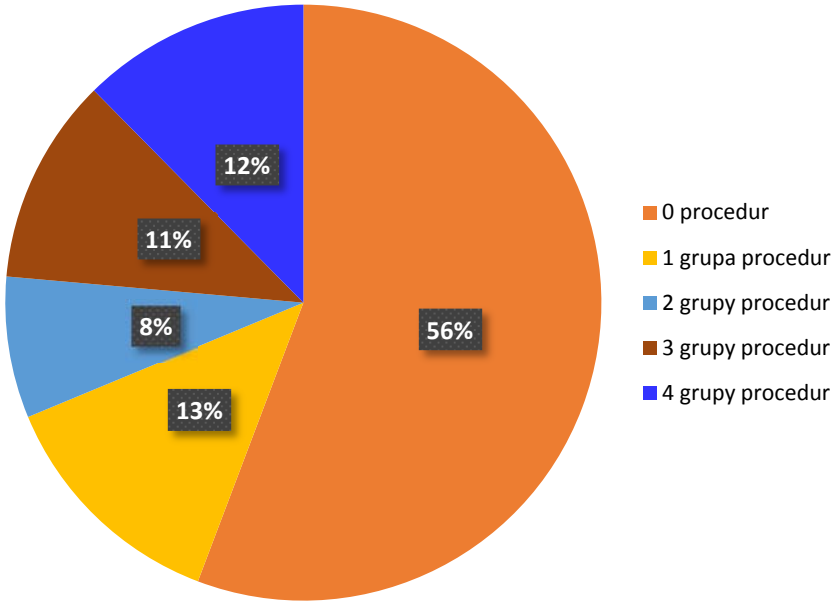
Szczegółowe informacje zostały zaprezentowane w tabeli 9. Wynika z niej, że w badanej grupie istnieją instytucje, które nie mają ani jednej z co najmniej kilku wyszczególnionych grup procedur. Odpowiednie dane zostały przedstawione na rysunku 9. Ukazuje on procent urzędów, które mają przynajmniej po jednej procedurze w każdej z grup.

Tabela 9. Procedury wdrożone w badanych urzędach

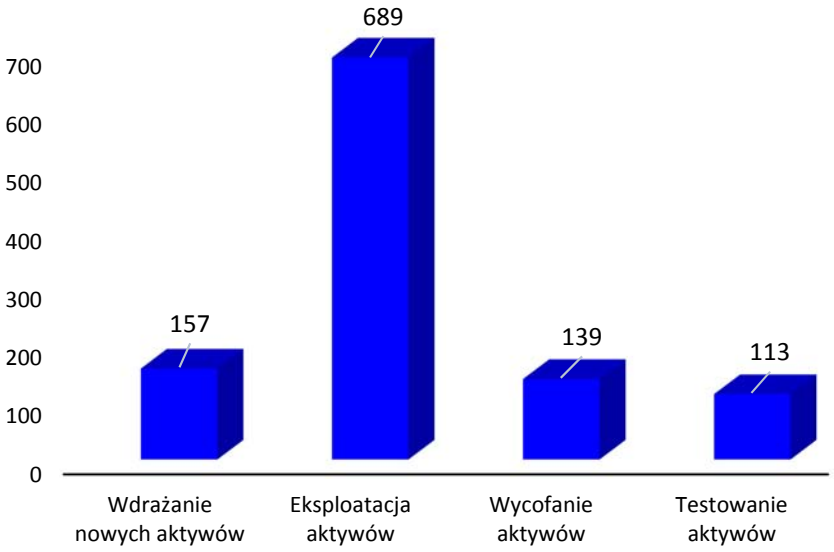
	Procedury			
	Wdrażanie aktywów	Eksploatacja aktywów	Testowanie aktywów	Wycofanie aktywów
Liczba	**157**	**68**	**113**	**139**
Średnia liczba przypadająca na pojedynczy urząd	0,46	2,03	0,33	0,41
Maksymalna liczba	**20**	**83**	**16**	**19**
Liczba organizacji bez wdrożonej procedury	249	205	278	246

Jak widać na rysunku 9, ponad połowa (56%) instytucji nie posiada żadnej procedury, natomiast przynajmniej jedną w każdej grupie posiada tylko 12%.

Największa liczba procedur opracowanych przez urzędy, dotyczyła eksploatacji aktywów. Najmniejsza liczba związana była z testowaniem aktywów. Szczegółowe liczby zostały zaprezentowane na rysunku 10.



Rys. 9. Grupy procedur w badanych instytucjach



Rys. 10. Liczba procedur opracowanych przez badane instytucje

4.8. Problemy ustanowienia i wdrożenia Polityki bezpieczeństwa

Sumaryczna ocena, dokonana przez respondentów i umieszczona w tabeli 10, jest zbliżona co do wartości dla każdego z przedstawionych w pytaniu nr 7 ankiety problemów.

Tabela 10. Sumaryczna ocena problemów związanych z ustanowieniem i wdrożeniem Polityki bezpieczeństwa

Problem	Punktacja
Wiedza, doświadczenie	827
Finanse	920
Opór czynnika ludzkiego	855

Respondenci najczęściej przyznawali maksymalną liczbę punktów problemom finansowym, co zostało pokazane w tabeli 11. Ograniczone środki finansowe wpływają na niedostateczną liczbę szkoleń oraz działań, mających na celu nie tylko pozyskanie wiedzy i kompetencji, lecz także podniesienie świadomości znaczenia ochrony informacji i występujących zagrożeń.

Tabela 11. Liczba instytucji przyznających maksymalną punktację dla poszczególnych problemów

Problem	Liczba instytucji
Wiedza, doświadczenie	36
Finanse	82
Opór czynnika ludzkiego	52

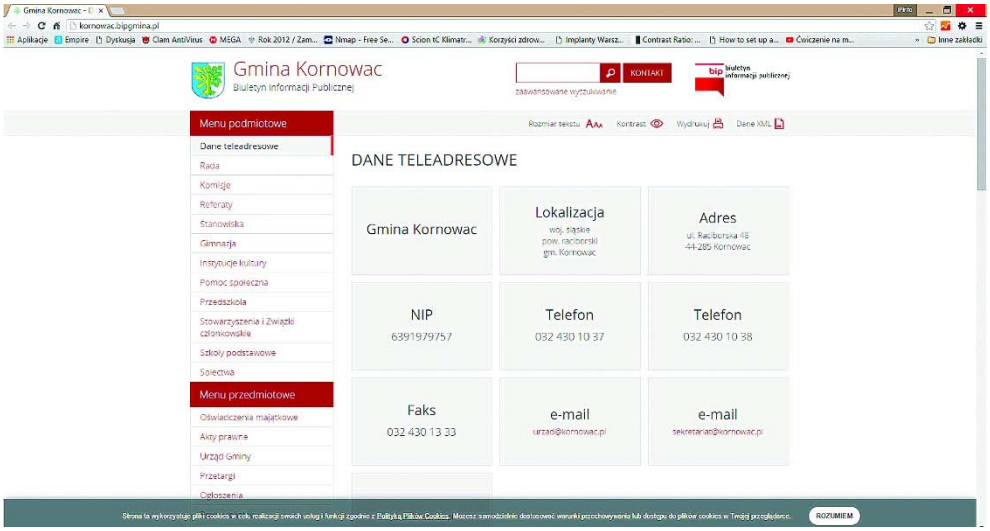
Urzędnicy dodatkowo wymienili następujące, nieskategoryzowane problemy:

- sporządzanie audytów bezpieczeństwa,
- brak czasu,

- problemy sprzętowe,
- pracochłonność,
- braki kadrowe,
- sposób przepływu danych pomiędzy systemami,
- nieprecyzyjne, niejasne, niespójne przepisy oraz ich interpretacja,
- nadmiar obowiązków,
- duża liczba zadań,
- brak zainteresowania pracowników.

4.9. Zgodność z WCAG 2.0

Można uznać, iż nie więcej niż 48 portali BIP badanych jednostek (14,16%) spełniało wymagania zgodności z WCAG 2.0. Prawie wszystkie posiadały wręcz ascetyczną formę. Do wyjątków należy portal Gminy Kornowac, którego stronę główną pokazuje rysunek 11.



Rys. 11. Biuletyn Informacji Publicznej Gminy Kornowac

5 Weryfikacja hipotez

5.1. Hipoteza 1: Większość badanych podmiotów nie zarządza usługami realizowanymi za pomocą systemów teleinformatycznych zgodnie z przepisami KRI

Hipoteza nr 1 znalazła swoje potwierdzenie w wynikach badań. Nawet pojedyncze kryteria weryfikacji nie zostały spełnione przez większość organizacji, co zostało uwidocznione w tabeli 12.

Tabela 12. Zestawienie ilościowe i procentowe jednostek spełniających pojedyncze kryteria weryfikacji hipotezy nr 1

L.p.	Kryterium	Liczba jednostek	% badanej próby
1.	Certyfikat zgodności z PN-ISO/IEC 20000	3	0,88
2.	Przeszkolenie przynajmniej 1 pracownika w zakresie wymagań PN-ISO/IEC 20000	6	1,77
3.	Zakup przynajmniej 1 normy PN-ISO/IEC 20000	8	2,36
4.	Audyt na zgodność z PN-ISO/IEC 20000	7	2,06
5.	Przynajmniej 1 udokumentowana procedura dotycząca wdrażania aktywów	90	26,55
6.	Przynajmniej 1 udokumentowana procedura dotycząca eksploatacji aktywów	134	39,53
7.	Przynajmniej 1 udokumentowana procedura dotycząca wycofania aktywów	93	27,43
8.	Przynajmniej 1 udokumentowana procedura dotycząca testowania aktywów	61	17,99

Najwięcej jednostek (39,53%) posiada przynajmniej 1 udokumentowaną procedurę dotyczącą eksploatacji aktywów teleinformatycznych. Jednakże komplet procedur funkcjonuje zaledwie w 42 urzędach.

Tabela 13 przedstawia zestawienie ilościowe i procentowe jednostek spełniających łączne kryteria weryfikacji hipotezy nr 1.

Tabela 13. Zestawienie ilościowe i procentowe jednostek spełniających łączne kryteria weryfikacji hipotezy nr 1

L.p.	Kryterium	Liczba jednostek	% badanej próby
1.	Certyfikat zgodności z PN-ISO/IEC 20000	3	0,88
2.	Przeszkolenie przynajmniej 1 pracownika w zakresie stosowania normy PN-ISO/IEC 20000 lub zakup normy PN-ISO/IEC 20000 oraz przeprowadzenie audytu na zgodność z PN-ISO/IEC 20000	5	1,47
3.	Posiadanie przynajmniej po 1 udokumentowanej procedurze dotyczącej wdrażania, eksploatacji, wycofywania i testowania aktywów teleinformatycznych	42	12,39

5.2. Hipoteza 2: Stopień wdrożenia przepisów KRI dotyczących zarządzania usługami realizowanymi za pomocą systemów teleinformatycznych jest zależna od wielkości podmiotu, liczby i wykształcenia osób związanych z IT

Hipoteza nr 2 również znalazła swoje potwierdzenie. Im większa organizacja, tym większy stopień wdrożenia przepisów KRI związanych z zarządzaniem usługami realizowanymi za pomocą systemów teleinformatycznych, co zostało pokazane w tabeli 14.

Należy jednak zauważyć, że nawet w przypadku dużych instytucji, jakimi są Urzędy Marszałkowskie, Urzędy Miejskie w miastach na prawach powiatu oraz Urzędy Dzielnicy (Warszawa), średnia liczba punktów stanowi jedynie 36,83% wszystkich możliwych do przyznania.

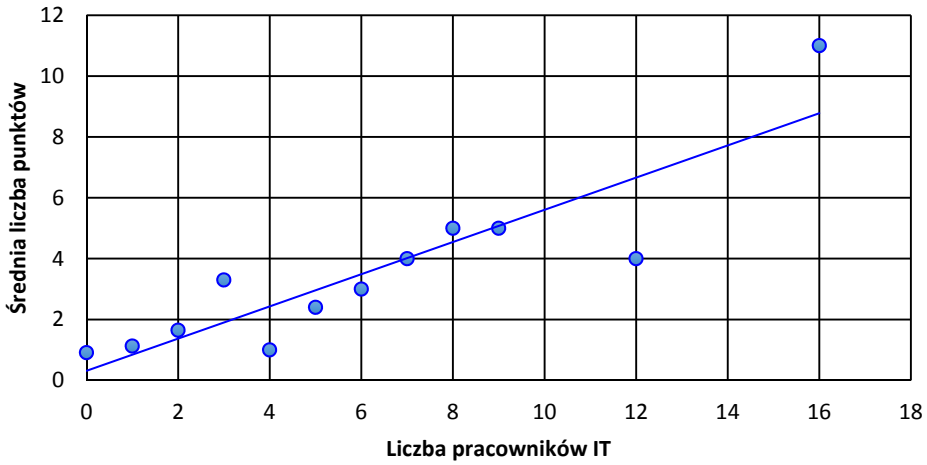
Tabela 14. Średni stopień wdrożenia przepisów KRI związanych z zarządzaniem usługami realizowanymi za pomocą systemów teleinformatycznych

Wielkość instytucji	Liczba instytucji	Liczba punktów	Średnia liczba punktów
Małe	253	246	0,97
Średnie	74	151	2,04
Duże	12	53	4,42

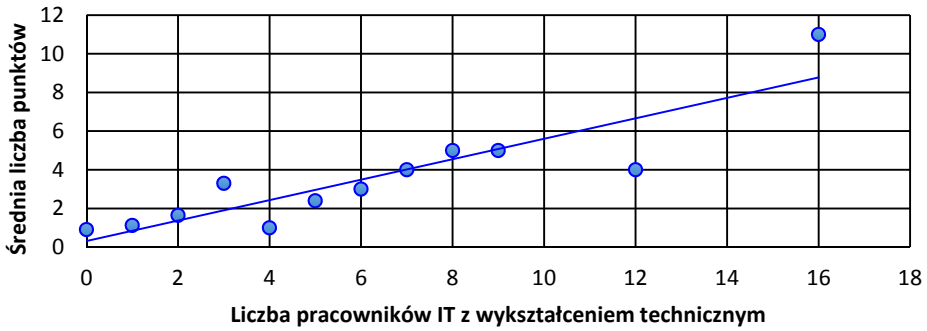
Liczba pracowników działu IT ma bezpośrednie przełożenie na stopień wdrożenia przepisów KRI związanych z zarządzaniem usługami realizowanymi za pomocą systemów teleinformatycznych.

Na rysunku 12 zaznaczono kropkami liczbę punktów przyznanych według zasad przedstawionych w tabeli 2 oraz niebieską linię trendu.

Te same oznaczenia użyto na rysunku 13, odnoszącym się do liczby pracowników związanych z IT z wykształceniem wyższym, technicznym.



Rys. 12. Zależność stopnia wdrożenia przepisów KRI dotyczących zarządzania usługami realizowanymi za pomocą systemów teleinformatycznych od liczby pracowników IT



Rys. 13. Zależność stopnia wdrożenia przepisów KRI dotyczących zarządzania usługami realizowanymi za pomocą systemów teleinformatycznych od liczby pracowników IT z wykształceniem wyższym technicznym

5.3. Hipoteza 3: Większość badanych podmiotów nie wdrożyła prawidłowo systemu zarządzania bezpieczeństwem informacji

Hipoteza nr 3, jak wynika z danych zamieszczonych w tabeli 15, jest prawdziwa. Większość badanych podmiotów nie wdrożyła prawidłowo systemu zarządzania bezpieczeństwem informacji.

Tabela 15. Zestawienie jednostek spełniających kryteria weryfikacji hipotezy nr 3

L.p.	Kryterium	Liczba jednostek	% badanej próby
1	Certyfikat zgodności z ISO 27001	11	3,24
2	Przeszkolenie przynajmniej 1 pracownika lub zakup normy ISO 27001 oraz przeprowadzenie audytu na zgodność z ISO 27001	19	5,60
3.1	Aktualna inwentaryzację aktywów teleinformatycznych	12	3,54
3.2	Aktualna analiza ryzyka	61	17,99
3.3	Aktualny rejestr incydentów	48	14,16
3.4	Aktualna Polityka bezpieczeństwa informacji oparta o ISO 27001	5	1,47

5.4. Hipoteza 4: Stopień wdrożenia systemu zarządzania bezpieczeństwem informacji zależy od wielkości podmiotu, liczby i wykształcenia osób związanych z IT

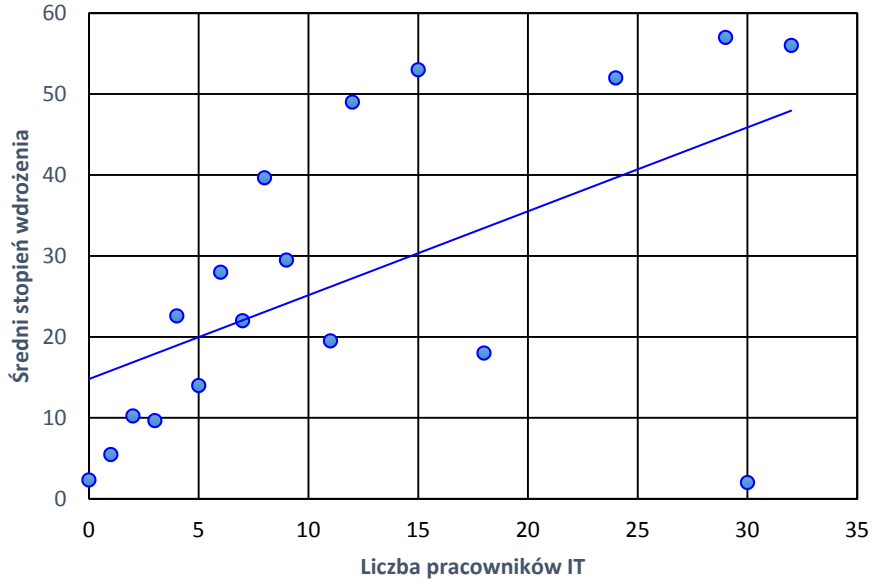
Hipotezę nr 4 także należy uznać za potwierdzoną. Jak wynika z danych zaprezentowanych w tabeli 16, większe jednostki w podwyższonym stopniu wdrożyły system zarządzania bezpieczeństwem informacji. Nawet średni stopień wdrożenia dla jednostek dużych nie był bliski maksymalnej możliwej do przyznania liczbie punktów, wynoszącej 57. Ponad 14% przebadanych jednostek posiadało stopień wdrożenia o wartości 0, a nawet niższej.

Tabela 16. Średni stopień wdrożenia systemu zarządzania bezpieczeństwem informacji

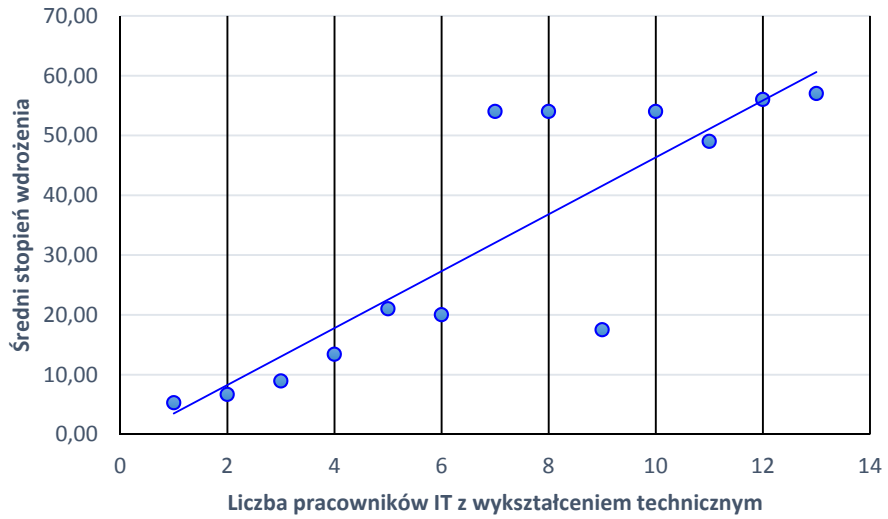
Wielkość instytucji	Liczba instytucji	Liczba punktów	Średnia Liczba punktów
Małe	253	1300	5,14
Średnie	74	1136	15,35
Duże	12	394	32,83

Zarówno liczba, jak i wykształcenie pracowników związanych z IT, ma bezpośrednie przełożenie na stopień wdrożenia systemu zarządzania bezpieczeństwem informacji, co zostało pokazane na rysunkach 14 i 15.

Za pomocą kropek oznaczono średni stopień wdrożenia dla określonych liczebności pracowników, zaś niebieska, ciągła linia jest linią trendu. Warto zauważyć, iż zerowa liczba pracowników IT związana zapewne z outsourcingiem nie zapewnia bezpieczeństwa systemu.



Rys. 14. Zależność stopnia wdrożenia systemu zarządzania bezpieczeństwem informacji od liczby pracowników IT



Rys. 15. Zależność stopnia wdrożenia systemu zarządzania bezpieczeństwem informacji od liczby pracowników IT z wykształceniem technicznym

5.5. Hipoteza 5: Większość systemów teleinformatycznych służących do prezentacji zasobów informacji badanych podmiotów nie jest zgodnych ze standardem WCAG 2.0

Hipoteza nr 5 została potwierdzona. Większość (przynajmniej 291, co stanowi 85,84% poddanych analizie) systemów teleinformatycznych badanych podmiotów służących do prezentacji zasobów informacji nie jest zgodnych ze standardem WCAG 2.0.

5.6. Hipoteza 6: Jednostki wyższego szczebla bardziej dbają o zgodność swoich systemów teleinformatycznych służących do prezentacji zasobów informacji ze standardem WCAG 2.0

Hipoteza nr 6 nie została potwierdzona. Najmniejszą dbałość o zgodność portali BIP z wytycznymi WCAG 2.0 przejawiają instytucje średniej wielkości, czyli urzędy miejskie i powiatowe. Szczegółowe dane przedstawione zostały w tabeli 17.

Tabela 17. Instytucje, których portale BIP spełniają wytyczne WCAG 2.0

Wielkość instytucji	Liczba instytucji	Liczba BIP zgodnych z WCAG 2.0	% BIP zgodnych z WCAG 2.0
Mała	253	38	15,02
Średnia	74	7	9,46
Duża	12	3	25,00

5.7. Hipoteza 7: Główną przeszkodą we wdrożeniu KRI jest brak adekwatnych kwalifikacji kadry badanych jednostek

Biorąc pod uwagę założony sposób weryfikacji w oparciu o odpowiedzi na pytanie nr 7 ankiety, w którym respondenci przyznają punkty od 0 do 5 dla czynników, które stanowiły problem przy ustanowieniu i wdroże-

niu Polityki bezpieczeństwa oraz dane z tabeli 11, należy uznać hipotezę nr 7 za nieprawdziwą.

Jednakże pozostałe dane odnoszące się do wykształcenia informatyków, administratorów bezpieczeństwa czy audytorów wewnętrznych, jak również braku szkoleń czy zakupu norm pozwalających na samodzielne dokształcanie, w powiązaniu z oczywistymi błędami w określeniu metodyk czy nieznajomością terminologii branżowej, zdaje się podważać jej prawdziwość.

Zaledwie 59% zatrudnionych przez urzędy informatyków posiada wykształcenie wyższe techniczne. Chociaż ponad 82% administratorów bezpieczeństwa informacji posiada wykształcenie wyższe techniczne, to jednakże aż 40 jednostek nie powołała go, co zgodnie z ustawą o ochronie danych osobowych, sprawia, iż funkcję tą piastuje kierownik organizacji, a więc wójt, burmistrz czy prezydent miasta.

6 Wnioski i spostrzeżenia

Jednostki samorządowe w większości nie podjęły adekwatnych starań odnośnie wdrożenia systemu zarządzania bezpieczeństwem informacji. Nie projektują, nie wdrażają oraz nie eksploatują systemów teleinformatycznych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Nie można jednak z góry założyć, że łamią w ten sposób prawo.

Wspomniane obowiązki zostały narzucone instytucjom publicznym poprzez przepisy rozdziału IV KRI. Nieokreślony jednak został termin ich wdrożenia, gdyż w § 23 KRI czytamy: „*Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia na podstawie dotychczas obowiązujących przepisów należy dostosować do wymagań, o których mowa w rozdziale IV rozporządzenia, nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia*".

Rozporządzenie nie definiuje pojęcia „istotna modernizacja", co w połączeniu z niskim tempem wymiany systemów informatycznych w instytucjach, może spowodować iż faktyczne wejście w życie wspomnianych przepisów będzie odwlekane jeszcze przez długie lata. Pomimo, że rozporządzenie wydano w roku 2012, nadal tylko nieliczne jednostki samorządowe podjęły starania związane z wdrożeniem przepisów KRI.

Wyjątkiem jest przepis § 19 KRI – spełnienie wymagań Web Content Accessibility Guidelines (WCAG 2.0) na poziomie AA przez systemy teleinformatyczne, eksploatowane przez podmioty realizujące zadania publiczne i służące prezentacji zasobów informacji.

Termin jego wdrożenia został ustalony w § 22 o treści: „*Systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu*

wejścia w życie rozporządzenia należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od dnia wejścia w życie niniejszego rozporządzenia".

Przytoczony przepis mylnie przywołuje rekomendacje jako wymagania. W literaturze spotyka się też traktowanie WCAG jako standardu. Faktycznie stały się one standardem 15 października 2012 roku jako norma ISO/IEC 40500:2012, a więc już po publikacji KRI.

Pomimo tej nieścisłości, już pobieżna inspekcja portali BIP badanych instytucji wykazała, że podjęły one działania dostosowujące je do wytycznych WCAG 2.0. Zazwyczaj posiadają funkcje zwiększające kontrast i wielkość czcionki, jednak są to jedynie 2 z 35 wytycznych. Zaobserwowano również bardzo niekorzystny trend, polegający na tworzeniu osobnych portali dla osób niepełnosprawnych, które zapewniają zgodność z WCAG 2.0. Zdaniem autora jest to objaw dyskryminacji niepełnosprawnych.

Widać jednak, że jednoznaczne określenie terminu wdrożenia stymulująco wpływa na podjęcie działań. Z tego też względu zapis § 22 należy uznać za szkodliwy. Nie skorzystano z możliwości jego skorygowania przy okazji wydania Rozporządzenia Rady Ministrów z 27 listopada 2014 roku zmieniające rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[18].

Z niewiadomych względów przedkłada się skądinąd niezwykle ważne zagadnienie dostępu do informacji osób niepełnosprawnych nad bezpieczeństwo informacji i odpowiednie nią zarządzanie. Systemowi zarządzania informacją poświęcono w KRI znaczną część rozdziału IV. Celem zawartych w nim przepisów było określenie minimalnych wymagań związanych z bezpieczeństwem informacji przetwarzanych przez podmioty publiczne. Jednocześnie utworzono niejako furtkę pozwalającą na odsuwanie w czasie ich stosowania.

[18] Dz.U. z 2014 r. poz. 1671

Jednostki samorządowe zdają sobie sprawę z niejasnej sytuacji, stąd właśnie niechęć do udzielania informacji opisana w części poświęconej przebiegowi badań. Dodatkowo brak nadzoru i kontroli, wytknięty już przez Najwyższą Izbę Kontroli[19], w połączeniu z sygnalizowanymi w badaniach barierami finansowymi, powodują iż wdrożenie przepisów KRI będzie się przeciągało.

Warto zauważyć, że działania Generalnego Inspektora Ochrony Danych Osobowych polegające na popularyzacji przepisów oraz kontroli ich przestrzegania przynoszą rezultaty. Niemalże wszystkie urzędy posiadają Politykę bezpieczeństwa dotyczącą ochrony danych osobowych. Opublikowane 26 kwietnia 2013 roku oraz zaktualizowane 9 maja 2013 roku wspólne stanowisko resortu finansów oraz Ministerstwa Cyfryzacji i Administracji, zawierające m.in. wytyczne dotyczące prowadzenia audytu wewnętrznego bezpieczeństwa informacji przetwarzanych w systemie teleinformatycznym przez komórkę audytu wewnętrznego, nie przyniosło oczekiwanych rezultatów[20]. Treść stanowiska przedstawiono w załączniku nr 3. Audytorzy wewnętrzni zazwyczaj nie posiadają odpowiednich kompetencji. Tylko 38,82% z nich posiada wykształcenie wyższe techniczne, zaś 65,29% dokonało analizy ryzyka, choć obowiązek corocznego jej wykonywania wynika z ustawy z 27 sierpnia 2009 roku o finansach publicznych[21] i wydanych na jej podstawie rozporządzeń Ministra Finansów w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu.

Nie można nie doceniać wagi wspomnianej popularyzacji. Z przeprowadzonych badań wynika, że kompetencje urzędników odpowiedzialnych za funkcjonowanie systemów informatycznych stoją na niskim poziomie. Świadczą o tym przytoczone przykłady nieznajomości terminologii i metodyk. Zaobserwowano też mylną interpretację wy-

[19] Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz krajowych ram interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu, NIK KAP-4101-002-00/2014, luty 2015.

[20] Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji.

[21] Dz.U. z 2013 r. poz. 885.

tycznych WCAG 2.0 związaną z powierzchownym zapoznaniem się jedynie z głównym dokumentem, bez materiałów dodatkowych, do których się on odnosi.

Zauważyć należy, że sam Web Content Accessibility Guidelines jest krótkim, 44 stronnicowym (po wydrukowaniu) dokumentem, który zawiera jednak odnośniki do następnych materiałów:

- How to Meet WCAG 2.0 — aktualna lista referencji WCAG 2.0;
- Understanding WCAG 2.0 — poradnik ułatwiający zrozumienie i wdrożenie WCAG 2.0,
- Techniques for WCAG 2.0 — opis technik oraz często popełnianych błędów;
- The WCAG 2.0 Documents — opis dokumentów technicznych WCAG 2.0 i zależności pomiędzy nimi.

Całość liczy ponad 1000 stron wydrukowanego tekstu, przy czym dysponujemy oficjalnym tłumaczeniem jedynie WCAG 2.0, wykonanym przez Fundację Instytut Rozwoju Regionalnego[22]. Pozostałe ponad 95% informacji pozostaje w angielskiej wersji językowej. Z tego też względu, pomimo podjętych starań, tylko nieliczne portale BIP badanych instytucji spełnia zalecenia WCAG 2.0.

Biorąc powyższe pod uwagę, Polskie Towarzystwo Informatyczne zaleca:

1. **podjęcie prac nad zmianą przepisów Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI),**
2. **ustalenie zasad i planów kontroli przestrzegania przepisów KRI,**
3. **opracowanie i wdrożenie systemu szkoleń i działań promujących przepisy KRI.**

[22] http://www.fdc.org.pl/wcag2/index.html.

Bibliografia

I OSK 89/13, Wyrok NSA, Skarga kasacyjna Zarządu Okręgowego Polskiego Związku Łowieckiego w O. od wyroku Wojewódzkiego Sądu Administracyjnego w Olsztynie z dnia 6 listopada 2012 r. sygn. akt II SA/Ol 1067/12 w sprawie ze skargi P. G. – redaktora naczelnego dziennika "[...]" na odmowę udzielenia przez Zarząd Okręgowy Polskiego Związku Łowieckiego w O. informacji prasowej

II SA/Po 1060/12, Wyrok WSA w Poznaniu, Sprawa skargi J… K. na decyzję Burmistrza W. z dnia [...] października 2012 r. nr [...] w przedmiocie umorzenia postępowania; I. uchyla zaskarżoną decyzję oraz poprzedzającą ją decyzję Dyrektora Gimnazjum nr [...] im. [...] w W. z dnia [...] września 2012 r. nr [...] (znak:[...])

II SAB/Po 123/13, Wyrok WSA w Poznaniu, Sprawa ze skargi na bezczynność "A" Sp. z o.o. w P. w przedmiocie udostępnienia informacji publicznej

How to Meet WCAG 2.0, https://www.w3.org/WAI/WCAG20/quickref/

Jabłoński M., Wygoda K., *Ustawa o dostępie do informacji publicznej: komentarz*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 21 czerwca 2013 r. w sprawie ogłoszenia jednolitego tekstu ustawy o finansach publicznych, Dz.U. z 2013 r. poz. 885

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 czerwca 2014 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych, Dz.U. 2014 r. poz. 1182

PN-ISO/IEC 20000-1: 2007 – Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja, PN-ISO/IEC 20000-2: 2007 – Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania

PN-ISO/IEC 24762:2010, Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie

PN-ISO/IEC 27001:2014, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania

PN-ISO/IEC 27005:2014, PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 17 stycznia 2012 r. w sprawie wzoru wniosku o ponowne wykorzystywanie informacji publicznej, Dz.U. 2012 poz. 94

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2012 poz. 526

Rozporządzenie Rady Ministrów z dnia 27 listopada 2014 r. zmieniające rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2014 r. poz. 1671

Steczkowski J., *Metoda reprezentacyjna w badaniach zjawisk ekonomiczno-społecznych*, Wydawnictwo Naukowe PWN, Warszawa 1995

Techniques for WCAG 2.0, https://www.w3.org/WAI/GL/WCAG20-TECHS/

Understanding WCAG 2.0 https://www.w3.org/WAI/WCAG20/versions/understanding/wcag20-understanding-20081211-a4.pdf

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Dz.U. 1960 nr 30 poz. 168

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne, Dz.U. Nr 64, poz. 565 z późn. zm.

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. 2009 nr 157 poz. 1240

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2001 nr 112 poz. 1198

Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz krajowych ram interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu, NIK KAP-4101-002-00/2014, luty 2015

Web Content Accessibility Guidelines (WCAG) 2.0 W3C Recommendation 11 December 2008

Web Content Accessibility Guidelines WCAG 2.0, http://www.fdc.org.pl/wcag2/index.html

Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji

Załącznik 1 Ankieta

Zarząd Główny, al. Solidarności 82A m. 5, 01-003 Warszawa, tel.: + 48 22 838 47 05, fax: + 48 22 636 89 87,
e-mail: pti@pti.org.pl, www.pti.org.pl Adres korespondencyjny: ul. Puławska 39 lok. 4, 02-508 Warszawa

Warszawa, dnia xx-xx-xxxx

Urząd xxxxxxxx

ul. xxxxxxxxx xx

xx-xx xxxxxxxxxxx

Polskie Towarzystwo Informatyczne wnioskuje o udostępnienie informacji publicznej na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz. U. Nr 112, poz. 1198), w następującym zakresie:

1. Czy Państwa instytucja posiada wyszczególnione poniżej normy, przeszkoliła pracowników w zakresie ich stosowania, audytowała organizację na zgodność z nimi? Proszę o wypełnienie tabeli.

Norma	Liczba zakupionych	Liczba przeszkolonych pracowników	Data audytu	Data certyfikacji
PN-ISO/IEC 20000				
PN-ISO/IEC 27001				
PN-ISO/IEC 27005			xxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxx
PN-ISO/IEC 24762			xxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxx

2. Czy Państwa instytucja przeprowadziła inwentaryzację zasobów teleinformatycznych i sporządziła w odniesieniu do nich analizę ryzyka oraz czy prowadzony jest rejestr incydentów bezpieczeństwa. Proszę o wypełnienie tabeli.

Data inwentaryzacji		
Liczba aktywów informacyjnych		
Liczba aktywnych węzłów sieci		
Liczba baz danych		
Data ostatniej aktualizacji analizy ryzyka		
Metodyka analizy ryzyka	Ilościowa/jakościowa/mieszana/oparta na rywalizacji*	
Nazwa metodyki		
Wykonawca analizy ryzyka	Wewnętrzny/zewnętrzny*	

3. Czy i jakie incydenty bezpieczeństwa zostały wykryte/zgłoszone w Państwa instytucji? Proszę o wypełnienie tabeli.

Czy instytucja prowadzi rejestr incydentów	Tak/Nie*
Ile incydentów zarejestrowano w instytucji w 2014 roku	
Data ostatnio zarejestrowanego incydentu	
Czy instytucja zarejestrowała incydent którego waga wymagała zgłoszenia do zespołu CERT ABW lub prokuratury	Tak/Nie*

4. Czy i kiedy Państwa instytucja ustanowiła Politykę bezpieczeństwa informacji oraz czy oparła ją o ustawę o ochronie danych osobowych czy normę ISO 27001 oraz czy jest ona aktualizowana? Proszę o wypełnienie tabeli.

Data ustanowienia	
Data ostatniej aktualizacji	
Oparta o ISO 27001 czy UODO	ISO 27001/UODO*
Częstotliwość przeglądu	1 rok/poniżej 1 roku/powyżej 1 roku*
Data ostatniego audytu	
Wykonawca audytu	Wewnętrzny/zewnętrzny*

5. Liczby i kompetencje pracowników. Proszę o wypełnienie tabeli.

Liczba pracowników	
Liczba pracowników odpowiedzialnych za IT	
Liczba pracowników odpowiedzialnych za IT z wykształceniem wyższym technicznym	
Wykształcenie Administratora Bezpieczeństwa Informacji (ABI)	Średnie/ wyższe humanistyczne/wyższe techniczne*
Wykształcenie audytora wewnętrznego	wyższe humanistyczne/wyższe techniczne*

6. Proszę o podanie liczby pisemnych, zatwierdzonych przez kierownictwo instytucji procedur. Proszę o wypełnienie tabeli.

Wdrażanie nowych aktywów teleinformatycznych	
Bieżąca eksploatacja aktywów teleinformatycznych	
Wycofanie aktywów teleinformatycznych	
Testowanie systemów teleinformatycznych pod kątem bezpieczeństwa informacji i zgodności prawnej	
Liczba zbiorów danych osobowych	
Liczba zbiorów danych osobowych zarejestrowanych w GIODO	

7. Który z czynników stanowił największy problem przy ustanowieniu i wdrożeniu Polityki bezpieczeństwa? Proszę o wypełnienie tabeli punktami w skali 0-5 dla każdego z czynników.

Wiedza, doświadczenie	
Finanse	
Opór czynnika ludzkiego	
Inne. Jakie?	

[*] *Niepotrzebne skreślić*

Odpowiedź prosimy przesłać w formie papierowej na adres:

Polskie Towarzystwo Informatyczne
ul. Puławska 39/4
02-508 Warszawa

Załącznik 2 Zażalenie

POLSKIE TOWARZYSTWO INFORMATYCZNE

Zarząd Główny, al. Solidarności 82A m. 5, 01-003 Warszawa, tel.: + 48 22 838 47 05, fax: + 48 22 636 89 87,
e-mail: pti@pti.org.pl, www.pti.org.pl Adres korespondencyjny: ul. Puławska 39 lok. 4, 02-508 Warszawa

Warszawa, dnia xx-xx-xxxx

Samorządowe Kolegium Odwoławcze
Wnioskodawca: Polskie Towarzystwo Informatyczne
Strona przeciwna: XXXXXXXXXXXX

Zażalenie
na niezałatwienie sprawy w terminie

Niniejszym na podstawie art. 37 Kodeksu postępowania administracyjnego składamy zażalenie na niezałatwienie przez XXXXXXXXXXXXXXXX sprawy – pomimo obowiązku wynikającego z przepisu art. 13 ust 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej – poprzez nie udzielenie informacji publicznej na wniosek z dnia XX-XX-XXXX

Wskazując na powyższe, wnoszę o:
1) zobowiązanie XXXXXXXXXXXXXXXX do udostępnienia wnioskowanej informacji publicznej.

Uzasadnienie

Wnioskiem z dnia XX-XX-XXXX zwróciliśmy się do XXXXXXXXXXX o udostępnienie informacji publicznej. Do dnia XX-XX-XXXX nie otrzymaliśmy żadnej odpowiedzi.

Załącznik:
Kopia wniosku

Załącznik 3. Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji

I. Zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji

Przepis § 20 *rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, zwanego dalej *rozporządzeniem*, określa ciążące na kierownictwie podmiotu publicznego obowiązki związane z systemem zarządzania bezpieczeństwem informacji. Jednym z nich jest wskazany w § 20 ust. 2 pkt 14 *rozporządzenia* obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Intencją projektodawcy było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzania. Uwzględniając przepis § 20 ust. 3 *rozporządzenia* należy stwierdzić, iż powyższe zobowiązanie powinno być wykonywane na jeden z dwóch sposobów.

1.

W podmiotach, w których system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, wymagania określone w § 20 ust. 1 i 2 *rozporządzenia* uznaje się za spełnione. W takich podmiotach ustanawianie za-

bezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm, związanych z tą normą. W konsekwencji przywołanej regulacji nie ma konieczności dokonywania dodatkowych/odrębnych audytów wewnętrznych, bowiem audytowanie jest jednym z już funkcjonujących elementów systemu zarządzania bezpieczeństwem informacji opisanym w normach.

2.

Jednostki, które nie wdrożyły systemu zarządzania bezpieczeństwem informacji, zgodnie z normami wskazanymi w § 20 ust. 3 *rozporządzenia*, są zobowiązane, zgodnie z § 20 ust. 2 pkt 14 *rozporządzenia*, do zapewnienia okresowego audytu wewnętrznego w zakresie informacji bezpieczeństwa informacji nie rzadziej niż raz na rok. **Użycie w *rozporządzeniu* sformułowania „audyt wewnętrzny" nie miało na celu obligatoryjnego przypisania tego obowiązku komórkom audytu wewnętrznego**, funkcjonującym w jednostkach sektora finansów publicznych na mocy przepisów Działu VI *ustawy o finansach publicznych*, zwanymi dalej komórkami audytu wewnętrznego. Jak wyżej wskazano, ustawodawca nie określił sposobu, trybu, rodzaju audytu, ani też osób czy komórek organizacyjnych, którym należałoby powierzyć prowadzenie ww. audytu. Zatem **decyzja co do tego, komu zostanie powierzone prowadzenie omawianego audytu, spoczywa na kierownictwie podmiotu**.

Kryteriami, jakimi należy się kierować przy wyborze osób/komórek organizacyjnych prowadzących audyt w zakresie bezpieczeństwa informacji są: odpowiednie kwalifikacje, doświadczenie, znajomość metodyki audytu w zakresie bezpieczeństwa informacji, a także niezależność od obszaru audytowanego. W razie wątpliwości, przy wyborze osób / komórek organizacyjnych prowadzących ww. audyt można brać pod uwagę wymogi wskazane w normach wymienionych w § 20 ust. 3 *rozporządzenia*. Upraszczając interpretację przedmiotowej regulacji audyt sytemu bezpieczeństwa informacji może być przeprowadzony w oparciu o dwa zestawy kryteriów. Po pierwsze jest to 14 kryteriów zawartych w § 20 ust. 2 *rozporządzeniem* lub jako drugi wariant audyt zgodności z normą PN-ISO/IEC 27001.

W opinii Ministerstwa Finansów oraz Ministerstwa Administracji i Cyfryzacji **nie należy automatycznie przypisywać zadania audytu w zakresie bezpieczeństwa informacji komórce audytu wewnętrznego**. Punktem odniesienia dla ustanowienia niniejszych przepisów był dla projektodawcy System Zarządzania Bezpieczeństwem Informacji w oparciu o normę PN-ISO/IEC 27001 nie zaś Dział VI *ustawy o finansach publicznych*.

II. Interpretacje przepisów

Mając na uwadze powyższe stanowisko informujemy, że podmiotem właściwym w zakresie udzielania odpowiedzi na pytania związane z interpretacją przepisów *ustawy o informatyzacji podmiotów realizujących zadania publiczne* oraz omawianego *rozporządzenia*, w tym na pytania związane z obszarem bezpieczeństwa informacji, zakresem audytu wewnętrznego oraz kryteriami, jakie należy stosować przy ocenie tego obszaru, jest Departament Informatyzacji Ministerstwa Administracji i Cyfryzacji. Natomiast w zakresie udzielania odpowiedzi na pytania dotyczące interpretacji przepisów *ustawy o finansach publicznych* oraz aktów wykonawczych do tej *ustawy* w zakresie audytu wewnętrznego właściwym jest Departament Audytu Sektora Finansów Publicznych Ministerstwa Finansów.

Załącznik 4. Wyciąg z dokumentu WCAG 2.0 dotyczącego badanych wytycznych

Wytyczne WCAG 2.0

Ta sekcja pełni funkcję normatywną.

Zasada nr 1: Postrzegalność — informacje oraz komponenty interfejsu użytkownika muszą być przedstawione użytkownikom w sposób dostępny dla ich zmysłów.

Wytyczna 1.1 Alternatywa w postaci tekstu: Dla każdej treści nietekstowej należy dostarczyć alternatywną treść w formie tekstu, która może być zamieniona przez użytkownika w inne formy (np. powiększony druk, brajl, mowa syntetyczna, symbole lub język uproszczony).

1.1.1 Treść nietekstowa: Wszelkie treści nietekstowe przedstawione użytkownikowi posiadają swoją tekstową alternatywę, która pełni tę samą funkcję, za wyjątkiem sytuacji opisanych poniżej (Poziom A):

- **Kontrolki użytkownika i wprowadzanie danych przez użytkownika:** Jeśli treść nietekstowa jest kontrolką użytkownika lub polem wprowadzania danych, wtedy posiada nazwę opisującą jej przeznaczenie. (Wytyczna 4.1 podaje dodatkowe wymagania dotyczące kontrolek oraz wprowadzania danych przez użytkownika.)

- **Media zmienne w czasie:** Jeśli treść nietekstowa to media zmienne w czasie, wtedy alternatywa w formie tekstu zawiera opis pozwalający zrozumieć przeznaczenie treści nietekstowej. (Wytyczna 1.2 podaje dodatkowe wymagania, jeśli chodzi o media.)

- **Test:** Jeśli treść nietekstowa jest testem lub ćwiczeniem, które utraciłoby swój sens ze względu na przedstawienie tej samej treści w postaci tekstu, wtedy alternatywa w postaci tekstu podawać powinna przynajmniej opis pozwalający zrozumieć przeznaczenie treści nietekstowej.

Odczucie zmysłowe: Jeśli treść nietekstowa ma za zadanie przede wszystkim tworzyć konkretne odczucie zmysłowe, wtedy alternatywa w postaci tekstu jest opisem pozwalającym zrozumieć przeznaczenie treści nietekstowej.

CAPTCHA: Jeśli celem treści nietekstowej jest potwierdzenie, że do treści ma dostęp człowiek, a nie komputer, wtedy dostarcza się alternatywę w postaci tekstu, która identyfikuje oraz opisuje cel treści nietekstowej. Dostarcza się również alternatywnych zabezpieczeń typu CAPTCHA, dostosowanych do różnych możliwości percepcji użytkowników, uwzględniając różne rodzaje niepełnosprawności.

Cele dekoracyjne, formatowanie, treść niewidoczna: Jeśli treść nietekstowa pełni jedynie funkcję dekoracyjną, używana jest do formatowania wizualnego lub też nie jest przedstawiana użytkownikowi, powinna być wdrożona w sposób umożliwiający technologiom wspomagającym jej zignorowanie.

Wytyczna 1.4 Możliwość rozróżnienia: Użytkownik powinien móc dobrze widzieć bądź słyszeć treści — mieć możliwość oddzielenia informacji od tła.

1.4.3 Kontrast (minimalny): Wizualne przedstawienie tekstu, lub obrazu tekstu posiada kontrast wynoszący przynajmniej 4,5:1, poza następującymi wyjątkami: (Poziom AA)

- **Duży tekst:** Duży tekst oraz grafiki takiego tekstu posiadają kontrast przynajmniej 3:1.

- **Przypadkowość:** Nie stosuje się wymogów minimalnego kontrastu dla tekstów lub obrazu tekstu, będących elementem nieużywanych części interfejsu użytkownika, mających cel czysto dekoracyjny, nie są widoczne lub też są częścią obrazu zawierającego inne istotne treści wizualne.

- **Logo:** Nie wymaga się minimalnego kontrastu dla tekstu, który jest częścią logo lub nazwy własnej produktu (marki).

Zasada nr 4: Solidność — Treść musi być solidnie opublikowana, tak, by mogła być skutecznie interpretowana przez różnego rodzaju oprogramowania użytkownika, w tym technologie wspomagające.

Wytyczna 4.1 Kompatybilność: Zmaksymalizowanie kompatybilności z obecnymi oraz przyszłymi programami użytkowników, w tym z technologiami wspomagającymi.

4.1.1 Parsowanie: W treści wprowadzonej przy użyciu języka znaczników, elementy posiadają pełne znaczniki początkowe i końcowe, elementy są zagnieżdżane według swoich specyfikacji, elementy nie posiadają zduplikowanych atrybutów oraz wszystkie ID są unikalne, za wyjątkiem przypadków, kiedy specyfikacja zezwala na wyżej wymienione cechy. (Poziom A)

Uwaga: Początkowe i końcowe znaczniki, w których brak kluczowych znaków, takich, jak zamykający nawias ostry lub pytajnik błędnie dopasowany do atrybutu wartości, nie są uznawane za znaczniki pełne.

Załącznik 5. Wykaz badanych podmiotów

L.p.	Nazwa Jednostki	Adres BIP
1.	Starostwo Powiatowe w Wałbrzychu	http://www.bip.sp-walbrzych.dolnyslask.pl/
2.	Starostwo Powiatowe w Złotoryi	http://www.bip.powiat-zlotoryja.pl/
3.	Starostwo Powiatowe w Krasnymstawie	http://powiatkrasnystaw.bip.lublin.pl/
4.	Starostwo Powiatowe w Lubartowie	http://splubartow.bip.lubelskie.pl/
5.	Starostwo Powiatowe w Oświęcimiu	http://bip.powiat.oswiecim.pl/
6.	Starostwo Powiatowe w Wadowicach	http://bip.malopolska.pl/spwadowice/
7.	Starostwo Powiatowe w Goleniowie	http://spow.goleniow.ibip.pl/
8.	Starostwo Powiatu Grodziskiego	http://www.bip.powiat-grodziski.pl/
9.	Starostwo Powiatowe w Mińsku Mazowieckim	http://bip.powiatminski.pl/
10.	Starostwo Powiatowe w Ożarowie Mazowieckim	http://bip.pwz.pl/
11.	Starostwo Powiatowe w Siedlcach	http://www.bip.powiatsiedlecki.pl/
12.	Starostwo Powiatowe w Krośnie	http://spkrosno.bip.gov.pl/
13.	Starostwo Powiatowe w Lesku	http://www.bip.powiat-leski.pl/
14.	Starostwo Powiatowe w Lubaczowie	http://www.lubaczow.powiat.pl/bip/
15.	Starostwo Powiatowe w Nisku	http://www.bip.powiat-nisko.pl/
16.	Starostwo Powiatowe w Przemyślu	http://bip.spprzemysl.pl/

L.p.	Nazwa Jednostki	Adres BIP
17.	Starostwo Powiatowe w Chodzieży	http://bip.wokiss.pl/chodziezp/
18.	Starostwo Powiatowe w Zambrowie	http://www.spzambrow.bip.podlaskie.pl/
19.	Starostwo Powiatowe w Będzinie	http://www.bip.powiat.bedzin.pl/
20.	Starostwo Powiatowe w Rybniku	http://www.bip.starostwo.rybnik.pl/
21.	Starostwo Powiatowe w Gołdapi	http://bip.warmia.mazury.pl/powiat_goldapski/
22.	Starostwo Powiatowe w Mrągowie	http://www.bip.powiat.mragowo.pl/
23.	Starostwo Powiatowe w Węgorzewie	http://bip.powiatwegorzewski.pl/
24.	Starostwo Powiatowe w Gnieźnie	http://bip.powiat-gniezno.pl/
25.	Starostwo Powiatowe w Lesznie	http://www.bip.powiat-leszczynski.pl/
26.	Starostwo Powiatowe w Nowym Tomyślu	http://bip.powiatnowotomyski.pl/
27.	Starostwo Powiatowe w Sławnie	http://bip.powiatslawno.pl/
28.	Starostwo Powiatowe w Międzyrzeczu	http://bip.powiat-miedzyrzecki.pl/
29.	Starostwo Powiatowe w Nowej Soli	http://www.bip.powiat-nowosolski.pl/
30.	Starostwo Powiatowe w Żarach	http://bip.wrota.lubuskie.pl/spzary/
31.	Starostwo Powiatowe w Kłodzku	http://www.bip.powiat.klodzko.pl/
32.	Starostwo Powiatowe w Kościerzynie	http://bip-koscierzyna.eurzad.eu/
33.	Starostwo Powiatowe w Kwidzynie	http://bip.powiatkwidzynski.pl/
34.	Starostwo Powiatowe w Olsztynie	http://bip.warmia.mazury.pl/powiat_olsztynski/

L.p.	Nazwa Jednostki	Adres BIP
35.	Starostwo Powiatowe w Pleszewie	http://bip.starostwo.powiatpleszewski.pl/
36.	Starostwo Powiatowe w Ostrołęce	http://www.bip.powiatostrolecki.pl/
37.	Urząd Miejski w Wolbórzu	http://www.wolborz.4bip.pl/
38.	Urząd Dzielnicy Śródmieście	http://bip.warszawa.pl/
39.	Urząd Dzielnicy Targówek	http://bip.warszawa.pl/Menu_podmiotowe/Dzielnice/Targowek/
40.	Urząd Gminy Chojnów	http://www.gmina-chojnow.bip.net.pl/
41.	Urząd Gminy Ciepłowody	http://bip.cieplowody.pl/
42.	Urząd Gminy w Jerzmanowej	http://bip.jerzmanowa.com.pl/
43.	Urząd Gminy Kotla	http://www.bip.kotla.pl/
44.	Urząd Gminy w Lubinie	http://www.bip.ug-lubin.dolnyslask.pl/
45.	Urząd Gminy Niechlów	http://www.biuletyn.net/nt-bin/start.asp?podmiot=niechlow/
46.	Urząd Gminy Nowa Ruda	http://www.bip.gmina.nowaruda.pl/
47.	Urząd Gminy Rudna	http://www.bip.rudna.pl/
48.	Urząd Gminy Zawonia	http://zawonia.biuletyn.net/
49.	Urząd Gminy Złotoryja	http://bip.zlotoryja.com.pl/
50.	Urząd Gminy w Jeziorach Wielkich	http://jeziorawielkie.bipgmina.pl/
51.	Urząd Gminy w Kęsowie	http://bip.kesowo.samorzady.pl/
52.	Urząd Gminy Kikół	http://bip.kikol.pl/
53.	Urząd Gminy Lubanie	http://bip.lubanie.kpsi.pl/
54.	Urząd Gminy Osielsko	http://www.bip.osielsko.pl/
55.	Urząd Gminy Radziejów	http://bip.ugradziejow.pl/
56.	Urząd Gminy Rogowo	http://rogowo.bip.net.pl/
57.	Urząd Gminy w Sicienku	http://www.bip.sicienko.pl/
58.	Urząd Gminy Sośno	http://www.bip.sosno.lo.pl/
59.	Urząd Gminy Stolno	http://www.bip.stolno.com.pl/

L.p.	Nazwa Jednostki	Adres BIP
60.	Urząd Gminy w Czarnym Dunajcu	http://bip.malopolska.pl/ugczarnydunajec/
61.	Urząd Gminy w Białej Podlaskiej	http://ugbialapodlaska.bip.lublin.pl/
62.	Urząd Gminy Chełm	https://ugchelm.bip.lubelskie.pl/
63.	Urząd Gminy Fajsławice	http://www.ugfajslawice.bip.e-zeto.eu/
64.	Urząd Gminy Granowo	http://granowo.bip.net.pl/
65.	Urząd Gminy Jabłoń	http://ugjablon.bip.lubelskie.pl/
66.	Urząd Gminy Janów Podlaski	http://janowpodlaski.bip.lublin.pl/
67.	Urząd Gminy Krzywda	http://ugkrzywda.bip.lubelskie.pl/
68.	Urząd Gminy Kurów	http://bip.kurow.eu/
69.	Urząd Gminy Lubycza Królewska	http://uglubyczakrolewska.bip.lubelskie.pl/
70.	Urząd Gminy Łuków	https://uglukow.bip.lubelskie.pl/
71.	Urząd Gminy Milejów	http://ugmilejow.bip.lubelskie.pl/
72.	Urząd Gminy Niemce	http://ugniemce.bip.lubelskie.pl/
73.	Urząd Gminy Potok Wielki	http://ugpotokwielki.bip.lubelskie.pl/
74.	Urząd Gminy Rejowiec	http://ugrejowiec.bip.e-zeto.eu/
75.	Urząd Gminy Rejowiec Fabryczny	http://ugrejowiecfabryczny.bip.lubelskie.pl/
76.	Urząd Gminy Rudnik	http://bip.gmina-rudnik.pl/
77.	Urząd Gminy w Stężycy	http://bip.gminastezyca.pl/
78.	Urząd Gminy Trzeszczany	http://www.bip.trzeszczany.roztocze.pl/
79.	Urząd Gminy w Andrespolu	http://andrespol.bip.cc/
80.	Urząd Gminy Brzeziny	http://www.brzeziny.bipst.pl/
81.	Urząd Gminy Srokowo	http://bip.warmia.mazury.pl/srokowo_gmina_wiejska/
82.	Urząd Gminy Daszyna	http://www.daszyna.bip.cc/
83.	Urząd Gminy Gidle	http://www.bip.gidle.pl/
84.	Urząd Gminy Głowno	http://www.bip.gmina-glowno.eu/
85.	Urząd Gminy Inowłódz	http://bip.inowlodz.pl/

L.p.	Nazwa Jednostki	Adres BIP
86.	Urząd Gminy Maków	http://makow.bipst.pl/
87.	Urząd Gminy w Mniszkowie	http://www.bip.mniszkow.pl/
88.	Urząd Gminy w Mokrsku	http://www.bip.mokrsko.akcessnet.net/
89.	Urząd Gminy Nieborów	http://www.bip.nieborow.pl/
90.	Urząd Gminy Osjaków	http://osjakow.bip.net.pl/
91.	Urząd Gminy Ostrówek	http://ugostrowek.bip.lubelskie.pl/
92.	Urząd Gminy w Parzęczewie	http://bip.parzeczew.nv.pl/
93.	Urząd Gminy Pątnów	http://www.biuletyn.net/nt-bin/start.asp?podmiot=patnow/
94.	Urząd Gminy Olszanka	http://e-bip.pl/Start/38
95.	Urząd Gminy w Charsznicy	http://bip.charsznica.pl/
96.	Urząd Gminy Dobra	http://bip.malopolska.pl/ugdobra/
97.	Urząd Gminy Gdów	http://bip.malopolska.pl/
98.	Urząd Gminy Jerzmanowice – Przeginia	http://bip.malopolska.pl/ugjerzmanowiceprzeginia/
99.	Urząd Gminy w Stoczku	http://bip.stoczek.net.pl/
100.	Urząd Gminy Kościelisko	http://bip.malopolska.pl/ugkoscielisko/
101.	Urząd Gminy Nowe Piekuty	http://www.ugpiekuty.bip.podlaskie.pl/
102.	Urząd Gminy Nowy Targ	http://bip.malopolska.pl/ugnowytarg/
103.	Urząd Gminy Pałecznica	http://bip.malopolska.pl/ugpalecznica/
104.	Urząd Gminy Sękowa	http://bip.malopolska.pl/ugsekowa/
105.	Urząd Gminy Konopnica	http://www.konopnica.finn.pl/bipkod/001
106.	Urząd Gminy w Krypnie	http://bip.ug.krypno.wrotapodlasia.pl/
107.	Urząd Gminy Zabierzów	http://bip.malopolska.pl/ugzabierzow/
108.	Urząd Gminy Zawoja	http://bip.malopolska.pl/ugzawoja/
109.	Urząd Gminy Zalesie	http://www.zalesie.bip.lublin.pl/
110.	Urząd Gminy Czerwonka	http://www.biuletyn.net/nt-bin/start.asp?podmiot=czerwonka/

L.p.	Nazwa Jednostki	Adres BIP
111.	Urząd Gminy Czosnów	http://czosnow.bip.org.pl/
112.	Urząd Gminy Goszczyn	http://bip.goszczyn.pl/
113.	Urząd Gminy w Starej Błotnicy	http://www.starablotnica.bip.org.pl/
114.	Urząd Gminy Jabłonna	http://ug.jablonna.ibip.pl/public/
115.	Urząd Gminy Jabłonna Lacka	http://www.jablonnalacka.bip.net.pl/
116.	Urząd Gminy Jedlnia-Letnisko	http://www.biuletyn.net/nt-bin/start.asp?podmiot=jedlnia/
117.	Urząd Gminy Karniewo	http://www.biuletyn.net/nt-bin/start.asp?podmiot=karniewo/
118.	Urząd Gminy w Kowali	http://www.biuletyn.net/nt-bin/start.asp?podmiot=kowala/
119.	Urząd Gminy Mińsk Mazowiecki	http://bip.minskmazowiecki.pl/
120.	Urząd Gminy Opinogóra Górna	http://ugopinogora.bip.org.pl/
121.	Urząd Gminy Prażmów	http://www.bip.prazmow.pl/
122.	Urząd Gminy w Przesmykach	http://e-bip.pl/Start/6
123.	Urząd Gminy w Rzewniu	http://rzewnie.bipgminy.pl/
124.	Urząd Gminy Słupno	http://ugslupno.bip.org.pl/
125.	Urząd Gminy Sobienie Jeziory	http://www.e-bip.pl/start/45
126.	Urząd Gminy w Sońsku	http://www.biuletyn.net/nt-bin/start.asp?podmiot=sonsk/
127.	Urząd Gminy Stara Kornica	http://www.biuletyn.net/nt-bin/start.asp?podmiot=kornica/
128.	Urząd Gminy Słupsk	http://stupsk.bipgmina.pl/
129.	Urząd Gminy w Obszy	http://ugobsza.bip.lubelskie.pl/
130.	Urząd Gminy w Wieniawie	http://bip.gminawieniawa.pl/
131.	Urząd Gminy Zakrzew	http://zakrzew.bip.gmina.pl/
132.	Urząd Gminy Zaręby Kościelne	http://zareby.ornet.pl/
133.	Urząd Gminy Zatory	http://www.biuletyn.net/nt-bin/start.asp?podmiot=zatory/

L.p.	Nazwa Jednostki	Adres BIP
134.	Urząd Gminy Zawidz	http://www.zawidz.bip.org.pl/
135.	Urząd Gminy Bierawa	http://bip.bierawa.pl/
136.	Urząd Gminy Pokój	http://bip.gminapokoj.pl/
137.	Urząd Gminy Popielów	http://bip.popielow.pl/
138.	Urząd Gminy w Zębowicach	http://bip.zebowice.pl/
139.	Urząd Gminy w Besku	http://www.besko.biuletyn.net/
140.	Urząd Gminy Chmielnik	http://www.bip.chmielnik.pl/
141.	Urząd Gminy Cmolas	http://www.cmolas.biuletyn.net/
142.	Urząd Gminy w Sierpcu	http://ugsierpc.bipgmina.pl/
143.	Urząd Gminy Jaśliska	http://www.biuletyn.net/nt-bin/start.asp?podmiot=jasliska/
144.	Urząd Gminy Niedrzwica Duża	http://ugniedrzwicaduza.bip.lubelskie.pl/
145.	Urząd Gminy Krzeszów	http://bip.krzeszow.pl/
146.	Urząd Gminy Kuryłówka	http://www.biuletyn.net/nt-bin/start.asp?podmiot=kurylowka/
147.	Urząd Gminy Lewin Kłodzki	http://lewin-klodzki.bip-gov.info.pl/
148.	Urząd Gminy Lutowiska	http://bip.lutowiska.pl/
149.	Urząd Gminy Pysznica	http://www.pysznica.bip.gmina.pl/
150.	Urząd Gminy w Solinie z/s w Polańczyku	http://esolina.pl/urzad/
151.	Urząd Gminy Tryńcza	http://www.bip.tryncza.eu/
152.	Urząd Gminy Pcim	http://bip.malopolska.pl/ugpcim/
153.	Urząd Gminy w Czyżach	http://bip.ug.czyze.wrotapodlasia.pl/
154.	Urząd Gminy Grodzisk	http://ug-grodzisk.pbip.pl/
155.	Urząd Gminy Gródek	http://ug-grodek.pbip.pl/
156.	Urząd Gminy Kolno	http://bip.ug.kolno.wrotapodlasia.pl/
157.	Urząd Gminy Łomża	http://www.gminalomza.pl/bip/
158.	Urząd Gminy Piątnica	http://www.ugpiatnica.doc.pl/
159.	Urząd Gminy w Suwałkach	http://bip.ug.suwalki.wrotapodlasia.pl/urzad_gminy/

L.p.	Nazwa Jednostki	Adres BIP
160.	Urząd Gminy Szumowo	http://ug-szumowo.pbip.pl/
161.	Urząd Gminy Choczewo	http://www.bip.choczewo.com.pl/
162.	Urząd Gminy Kaliska	http://bip.kaliska.pl/
163.	Urząd Gminy Kolbudy	http://www.ugkolbudy.bip.org.pl/
164.	Urząd Gminy Lubichowo	http://bip.lubichowo.pl/
165.	Urząd Gminy w Ostaszewie	http://ugostaszewo.ssdip.bip.gov.pl/
166.	Urząd Gminy Przechlewo	http://przechlewo.biuletyn.net/
167.	Urząd Gminy w Morzeszczynie	http://morzeszczyn.biuletyn.net/
168.	Urząd Gminy Sierakowice	http://sierakowice.biuletyn.net/
169.	Urząd Gminy Pomiechówek	http://www.bip.pomiechowek.pl/
170.	Urząd Gminy w Starym Dzierzgoniu	http://ug.starydzierzgon.samorzady.pl/
171.	Urząd Gminy Narewka	http://bip.ug.narewka.wrotapodlasia.pl/
172.	Urząd Gminy w Chybiu	http://www.chybie.samorzady.pl/
173.	Urząd Gminy Janów	http://www.bip.janow.akcessnet.net/
174.	Urząd Gminy Kornowac	http://kornowac.bipgmina.pl/
175.	Urząd Gminy Lipowa	http://bip.lipowa.pl/
176.	Urząd Gminy Miedźna	http://bip.miedzna.pl/
177.	Urząd Gminy Mierzęcice	http://www.mierzecice.bip.info.pl/
178.	Urząd Gminy Pawłowice	http://bip.gwpawlowice.finn.pl/
179.	Urząd Gminy Pawonków	http://bip.pawonkow.pl/
180.	Urząd Gminy w Przyrowie	http://www.bip.przyrow.akcessnet.net/
181.	Urząd Gminy w Rudzińcu	http://www.biuletyn.net/nt-bin/start.asp?podmiot=rudziniec/
182.	Urząd Gminy Suszec	http://bip.suszec.iap.pl/
183.	Urząd Gminy Zbrosławice	http://bip.zbroslawice.pl/
184.	Urząd Gminy w Baćkowicach	http://bip.backowice-gmina.pl/
185.	Urząd Gminy w Gowarczowie	http://www.gowarczow.asi.pl/

L.p.	Nazwa Jednostki	Adres BIP
186.	Urząd Gminy Klimontów	http://www.bip.klimontow.akcessnet.net/
187.	Urząd Gminy Gniezno	http://www.urzadgminy.gniezno.pl/bip.html
188.	Urząd Gminy Solec-Zdrój	http://solec-zdroj.pl/bip/
189.	Urząd Miasta i Gminy Stopnica	http://stopnica.pl/bip/
190.	Urząd Gminy w Wojciechowicach	http://www.bip.wojciechowice.com.pl/
191.	Urząd Gminy w Baniach Mazurskich	http://bip.warmia.mazury.pl/banie_mazurskie_gmina_wiejska/
192.	Urząd Gminy Elbląg	http://bipgminaelblag.eline2n.nazwa.pl/
193.	Urząd Gminy Ełk	http://elk-ug.bip.eur.pl/public/
194.	Urząd Gminy Lubawa	http://www.bip.gminalubawa.pl/
195.	Urząd Gminy Łukta	http://bip.warmia.mazury.pl/lukta_gmina_wiejska/
196.	Urząd Gminy Mrągowo	http://bip.warmia.mazury.pl/mragowo_gmina_wiejska/
197.	Urząd Gminy Piecki	http://bip.piecki.com.pl/
198.	Urząd Gminy Babiak	http://bip.wokiss.pl/babiak/
199.	Urząd Gminy Chocz	http://www.chocz.bip.net.pl/
200.	Urząd Gminy Chodzież	http://bip.wokiss.pl/chodziezg/
201.	Urząd Gminy w Kamieńcu	http://bip.wokiss.pl/kamieniec/
202.	Urząd Gminy Kołaczkowo	http://bip.kolaczkowo.pl/
203.	Urząd Gminy w Kraszewicach	http://www.biuletyn.net/nt-bin/start.asp?podmiot=kraszewice/
204.	Urząd Gminy Kuślin	http://www.bip.kuslin.pl/
205.	Urząd Gminy w Liskowie	http://bip.liskow.pl/
206.	Urząd Gminy w Opatówku	http://www.bip.opatowek.pl/
207.	Urząd Gminy w Sobkowie	http://www.sobkow.biuletyn.net/
208.	Urząd Gminy Połajewo	http://www.biuletyn.net/nt-bin/start.asp?podmiot=polajewo/
209.	Urząd Gminy w Powidzu	http://www.biuletyn.net/nt-bin/start.asp?podmiot=powidz/
210.	Urząd Gminy Przemęt	http://bip.wokiss.pl/przemet/
211.	Urząd Gminy Szczytniki	http://www.bip.szczytniki.ug.gov.pl/

L.p.	Nazwa Jednostki	Adres BIP
212.	Urząd Gminy Wągrowiec	http://www.bip.wagrowiec.wlkp.pl/
213.	Urząd Gminy Wijewo	http://www.bip.wijewo.pl/
214.	Urząd Gminy Żelazków	http://bip.zelazkow.pl/
215.	Urząd Gminy Mielno	http://www.mielno.bip.net.pl/
216.	Urząd Gminy w Ostrowicach	http://ug.ostrowice.ibip.pl/
217.	Urząd Gminy Świdwin	http://ug.swidwin.ibip.pl/
218.	Urząd Gminy w Reszlu	http://bip.warmia.mazury.pl/reszel_gmina_miejsko_-_wiejska/
219.	Urząd Gminy i Miasta Nowe Skalmierzyce	http://www.noweskalmierzyce.pl/bip.php
220.	Urząd Gminy i Miasta Rzgów	http://bip.rzgow.pl/
221.	Urząd Gminy i Miasta w Lubańcu	http://www.bip.lubraniec.pl/
222.	Urząd Miejski w Babimoście	http://bip.wrota.lubuskie.pl/ugbabimost/
223.	Urząd Gminy i Miasta w Zdunach	http://www.zduny.bip.cc/
224.	Urząd Gminy i Miasta w Żurominie	http://www.zuromin.ibip.net.pl/
225.	Urząd Gminy Przytoczna	http://www.przytoczna.bip.net.pl/
226.	Urząd Gminy Skąpe	http://www.bip.skape.pl/
227.	Urząd Gminy Stare Kurowo	http://www.bip.wrota.lubuskie.pl/ugstarekurowo/
228.	Urząd Gminy Świdnica	http://bip.gmina.swidnica.pl/
229.	Urząd Gminy Trzebiel	http://bip.wrota.lubuskie.pl/ugtrzebiel/
230.	Urząd Gminy Zakroczym	http://bip.zakroczym.pl/
231.	Urząd Marszałkowski Województwa Kujawsko-Pomorskiego	http://bip.kujawsko-pomorskie.pl/
232.	Urząd Marszałkowski Województwa Podkarpackiego	http://www.bip.podkarpackie.pl/

L.p.	Nazwa Jednostki	Adres BIP
233.	Urząd Miasta Aleksandrów Kujawski	http://www.bip.aleksandrowkujawski.pl/
234.	Urząd Miasta Bochnia	http://bip.malopolska.pl/umbochnia/
235.	Urząd Miasta Bolesławiec	http://www.um.boleslawiec.bip-gov.pl/
236.	Urząd Miasta Braniewo	http://www.bip.braniewo.pl/
237.	Urząd Miasta Brodnica	http://bip.brodnica.pl/
238.	Urząd Miasta Bydgoszcz	http://bip.um.bydgoszcz.pl/
239.	Urząd Miasta Bytom	http://bip.um.bytom.pl/
240.	Urząd Miasta Dzierżoniów	http://bip.um.dzierzoniow.pl/
241.	Urząd Miasta Ełk	http://bip.elk.warmia.mazury.pl/
242.	Urząd Miasta Gdyni	http://www.gdynia.pl/bip/
243.	Urząd Miasta Golub-Dobrzyń	http://golub-dobrzyn.miasto.nowoczesnagmina.pl/
244.	Urząd Miasta i Gminy Końskie	http://umkonskie.bipgmina.pl/
245.	Urząd Miasta i Gminy Gołańcz	http://bip.golancz.pl/
246.	Urząd Gminy i Miasta Nekla	http://nekla.nowoczesnagmina.pl/
247.	Urząd Miasta i Gminy Rydzyna	http://www.bip2-rydzyna.065.pl/
248.	Urząd Miasta i Gminy w Szamocinie	http://bip.wokiss.pl/szamocinm/
249.	Urząd Miasta i Gminy Czarne	http://bip.czarne.pl/
250.	Urząd Miasta i Gminy w Bogatynii	http://bip.bogatynia.pl/
251.	Urząd Miasta i Gminy Pelplin	http://www.bip.pelplin.pl/
252.	Urząd Miasta i Gminy Twardogóra	http://bip.umig-twardogora.dolnyslask.pl/
253.	Urząd Miasta i Gminy w Buku	http://bip.buk.gmina.pl/
254.	Urząd Miasta i Gminy w Mrozach	http://www.mrozy.bip.net.pl/

L.p.	Nazwa Jednostki	Adres BIP
255.	Urząd Miasta i Gminy w Szczawnicy	http://bip.malopolska.pl/umigszczawnica/
256.	Urząd Miasta i Gminy w Szlichtyngowej	http://bip.szlichtyngowa.pl/
257.	Urząd Miasta i Gminy w Wolbromiu	http://bip.malopolska.pl/umigwolbrom/
258.	Urząd Miasta i Gminy Wysoka	http://bip.gminawysoka.pl/
259.	Urząd Miasta Jastrzębie Zdrój	http://bip.jastrzebie.pl/
260.	Urząd Miasta Jaworzno	http://www.bip.jaworzno.pl/
261.	Urząd Miasta Jelenia Góra	http://bip.jeleniagora.pl/
262.	Urząd Miasta Jordanów	http://bip.malopolska.pl/umjordanow/
263.	Urząd Miasta Hajnówka	http://www.bip.hajnowka.pl/
264.	Urząd Miasta Katowice	https://bip.um.katowice.pl/
265.	Urząd Miasta Kielce	http://www.bip.kielce.eu/
266.	Urząd Miasta Kołobrzeg	http://umkolobrzeg.esp.parseta.pl/
267.	Urząd Miasta Legnica	http://um.bip.legnica.eu/
268.	Urząd Miasta Lipno	http://www.bip.umlipno.pl/
269.	Urząd Miasta Marki	http://bip.marki.pl/
270.	Urząd Miasta Namysłów	http://bip.namyslow.eu/
271.	Urząd Miasta Nowy Dwór Mazowiecki	http://bip.nowydwormaz.pl/
272.	Urząd Miasta Ostrołęki	http://bip.um.ostroleka.pl/
273.	Urząd Miasta Ostróda	http://bip.warmia.mazury.pl/ostroda_gmina_miejska/
274.	Urząd Miasta Piotrkowa Trybunalskiego	http://www.bip.piotrkow.pl/
275.	Urząd Miasta Płońsk	http://www.umplonsk.bip.org.pl/
276.	Urząd Miasta Rajgród	http://bip.um.rajgrod.wrotapodlasia.pl/
277.	Urząd Miasta Ruda Śląska	http://www.rudaslaska.bip.info.pl/
278.	Urząd Miasta Słupca	http://www.bip.umslupca.finn.pl/
279.	Urząd Miasta Starachowice	http://bip.um.starachowice.pl/

L.p.	Nazwa Jednostki	Adres BIP
280.	Urząd Miasta Szczecin	http://bip.um.szczecin.pl/
281.	Urząd Miasta Tuszyn	http://www.tuszyn.info.pl/
282.	Urząd Miasta w Bolkowie	http://umbolkow.bip.net.pl/
283.	Urząd Miasta w Kazimierzu Dolnym	http://umkazimierzdolny.bip.lubelskie.pl/
284.	Urząd Miasta Wadowice	http://bip.malopolska.pl/umwadowice/
285.	Urząd Miasta Wałbrzych	http://bip.um.walbrzych.pl/
286.	Urząd Miasta Zduńska Wola	http://www.zdunskawola.pl/portal_new/portal
287.	Urząd Miejski w Annopolu	https://umannopol.bip.lubelskie.pl/
288.	Urząd Miejski w Bychawie	https://umbychawa.bip.lubelskie.pl/
289.	Urząd Miejski w Krasnobrodzie	https://umkrasnobrod.bip.lubelskie.pl/
290.	Urząd Miasta Kalwarii Zebrzydowskiej	http://bip.malopolska.pl/umkalwariazebrzydowska/
291.	Urząd Miejski w Stawiskach	http://www.bip.stawiski.pl/
292.	Urząd Miejski w Knyszynie	http://bip.um.knyszyn.wrotapodlasia.pl/
293.	Urząd Gminy w Rymanowie	http://rymanow.bip.org.pl/
294.	Urząd Miasta i Gminy w Sieniawie	http://bip.sieniawa.pl/
295.	Urząd Miasta i Gminy Siewierz	http://bip.gmsiewierz.finn.pl/
296.	Urząd Miejski w Orzyszu	http://www.bip.orzysz.pl/
297.	Urząd Miejski w Miejskiej Górce	http://bip.miejska-gorka.pl/
298.	Urząd Miejski w Gościnie	http://bip.goscino.com.pl/
299.	Urząd Miejski w Kluczborku	http://www.bip.kluczbork.eu/
300.	Urząd Miasta w Otmuchowie	http://otmuchow.probip.pl/

L.p.	Nazwa Jednostki	Adres BIP
301.	Urząd Miejski w Leśnicy	http://www.bip.lesnica.pl/
302.	Urząd Miejski w Boguchwale	http://www.bip.boguchwala.pl/
303.	Urząd Miejski w Brzegu Dolnym	http://www.bip.um-brzegdolny.dolnyslask.pl/
304.	Urząd Miejski w Brześciu Kujawskim	http://www.bip.brzesckujawski.pl/
305.	Urząd Miejski w Nowym Mieście nad Pilicą	http://nowemiasto.eobip.pl/
306.	Urząd Miejski w Czarnej Białostockiej	http://www.bip.czarnabialostocka.pl/
307.	Urząd Miejski w Czyżewie	http://www.biuletyn.net/nt-bin/start.asp?podmiot=czyzewosada/
308.	Urząd Miejski w Drohiczynie	http://bip.um.drohiczyn.wrotapodlasia.pl/
309.	Urząd Miejski w Dzierzgoniu	http://bip.dzierzgon.pl/
310.	Urząd Miejski w Chodzieży	http://bip.wokiss.pl/chodziezm/
311.	Urząd Miejski Kargowa	http://bip.kargowa.pl/
312.	Urząd Miejski w Kartuzach	http://bip.kartuzy.pl/
313.	Urząd Miejski w Krzeszowicach	http://bip.malopolska.pl/umkrzeszowice/
314.	Urząd Miejski w Lipianach	http://bip.lipiany.pl/
315.	Urząd Miejski w Łobzie	http://www.bip.lobez.pl/
316.	Urząd Miejski w Moryniu	http://www.bip.moryn.pl/
317.	Urząd Miasta i Gminy w Szczekocinach	http://szczekociny.finn.pl/
318.	Urząd Miejski w Oławie	http://bip.um.olawa.pl/
319.	Urząd Miejski w Pogorzeli	http://bip.pogorzela.pl/
320.	Urząd Gminy i Miasta Sędziszów Małopolski	http://www.bip.sedziszow-mlp.pl/
321.	Urząd Miejski w Słubicach	http://bip.slubice.pl/

L.p.	Nazwa Jednostki	Adres BIP
322.	Urząd Miasta i Gminy w Działoszynie	http://www.e-bip.pl/start/12380
323.	Urząd Miejski w Strzegomiu	http://bip.strzegom.pl/
324.	Urząd Miejski w Szprotawie	http://www.szprotawa.pl/pl/183/bip-urzedu-miejskiego.html
325.	Urząd Miejski w Szubinie	http://www.bip.szubin.pl/
326.	Urząd Miasta Świebodzin	http://www.bip.swiebodzin.eu/
327.	Urząd Miejski w Tłuszczu	http://www.tluszcz.bip.net.pl/
328.	Urząd Miejski w Tykocinie	http://bip.um.tykocin.wrotapodlasia.pl/
329.	Urząd Miejski w Wolsztynie	http://www.bip.wolsztyn.pl/
330.	Urząd Miejski w Złocieńcu	http://bip.zlocieniec.pl/
331.	Urząd Miasta i Gminy Murowana Goślina	http://bip.murowana-goslina.pl/
332.	Urząd Miejski w Żninie	http://bip.umznin.pl/
333.	Urząd Miejski w Stargardzie Szczecińskim	http://bip.um.stargard.pl/
334.	Urząd Miejski w Kaletach	http://www.bip.kalety.pl/
335.	Urząd Miejski w Pruszczu Gdańskim	http://www.e-bip.pl/start/51
336.	Urząd Miasta Przeworska	http://www.przeworsk.bip.info.pl/
337.	Urzędu Miejskiego w Dusznikach-Zdroju	http://www.bip.duszniki.pl/
338.	Urząd Miejski w Jaworze	http://www.jawor.bip.net.pl/
339.	Urząd Miejski w Łomży	http://www.lomza.pl/bip/

Załącznik 6. Wykaz podmiotów, którym przekazano wyniki badań

Prezydent Rzeczypospolitej Polskiej
Prezes Rady Ministrów
Marszałek Sejmu Rzeczypospolitej Polskiej
Marszałek Senatu Rzeczypospolitej Polskiej
Ministerstwo Cyfryzacji
Ministerstwo Spraw Wewnętrznych i Administracji
Generalny Inspektor Ochrony Danych Osobowych
Naczelna Izba Kontroli
Sejmowa Komisja Administracji i Spraw Wewnętrznych
Sejmowa Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej
Lider Cyfryzacji Włodzimierz Marciński

Polskie Towarzystwo Informatyczne (PTI) zostało założone w roku 1981. Stowarzyszenie zrzesza zarówno osoby posiadające wysokie kompetencje i doświadczenie zawodowe w zakresie informatyki, studentów ostatnich lat kierunków informatycznych, jak i specjalistów innych dziedzin, intensywnie wykorzystujących technologie informatyczne.

PTI skupia informatyków działających w administracji publicznej, środowiskach akademickich i biznesowych.

Polskie Towarzystwo Informatyczne należy do Europejskiej Rady Stowarzyszeń Informatycznych CEPIS (Council of European Professional Informatics Societies).

Podstawowe cele **Polskiego Towarzystwa Informatycznego:**

- wspieranie działalności naukowej i naukowo-technicznej we wszystkich dziedzinach informatyki i doskonalenia metod jej efektywnego wykorzystania w gospodarce narodowej,
- popularyzacja zagadnień i zastosowań informatyki w społeczeństwie,
- ułatwianie wymiany informacji w środowisku zawodowym,
- podnoszenie poziomu kwalifikacji i etyki zawodowej informatyków,
- reprezentowanie członków Towarzystwa, ich opinii, potrzeb, interesów i uprawnień wobec społeczeństwa, władz i instytucji w kraju i za granicą.

Izba Rzeczoznawców Polskiego Towarzystwa Informatycznego

Działająca przy Polskim Towarzystwie Informatycznym **Izba Rzeczoznawców PTI** wspiera profesjonalną wiedzą oraz doświadczeniem zrzeszonych w Polskim Towarzystwie Informatycznym przedstawicieli zawodowego i naukowego polskiego środowiska teleinformatycznego.

Izba Rzeczoznawców PTI świadczy usługi na rzecz podmiotów państwowych, samorządowych, organizacji publicznych, firm komercyjnych oraz osób fizycznych w sytuacjach, gdy odwołanie się do opinii niezależnego i obiektywnego autorytetu:

- podnosi szanse powodzenia zaplanowanego przedsięwzięcia informatycznego,
- jest niezbędne do zapewnienia przejrzystości wyboru,
- służy bezstronnemu rozstrzygnięciu dylematów wynikających z realizacji przedsięwzięcia.

Ekspertyzy **Izby Rzeczoznawców PTI** realizowane są przez zespoły specjalistów z wieloletnim doświadczeniem w branży IT. Ich kwalifikacje potwierdzone są akredytacjami i certyfikacjami zarówno niezależnych organizacji takich jak The Open Group (TOGAF), ISC2 (certyfikaty CISSP), ISACA (certyfikaty CISA, CRISC, CISM), CCTE (certyfikaty PRINCE2), PMI, jak i czołowych krajowych i międzynarodowych producentów sprzętu i oprogramowania.

W obszarze zarządzania bezpieczeństwem informacji wśród ekspertów PTI znajdują się osoby posiadające kwalifikacje w zakresie prowadzenia testów penetracyjnych, certyfikaty Certified Ethical Hacker (CEH) wydane przez EEC-Council, certyfikaty audytorów wiodących systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 2700.

Rzeczoznawcy PTI posiadają Poświadczenia Bezpieczeństwa ABW umożliwiające dostęp do informacji niejawnych do poziomu objętego klauzulą „tajne" lub „poufne".

Kluczowe obszary prac realizowanych przez **Izbę Rzeczoznawców PTI** to:

- opracowywanie strategii i koncepcji informatyzacji,
- wykonywanie ekspertyz i opinii,
- przeprowadzanie audytów, w tym audytów bezpieczeństwa systemów informatycznych,
- wsparcie merytoryczne przy przygotowywaniu SIWZ oraz przy prowadzeniu procesu przetargowego,
- wsparcie i udział w pracach komitetów sterujących projektów informatycznych,
- badanie, analiza i ocena projektów informatycznych oraz systemów i rozwiązań informatycznych,
- pełnienie obowiązków biegłego instytucjonalnego.

Gwarancją ochrony interesów klientów **Izby Rzeczoznawców PTI** są:

- niezależność i obiektywizm rzeczoznawcy,
- rzetelność treści odniesiona do aktualnej wiedzy i najlepszych praktyk zawodowych,
- zachowanie poufności wszelkich otrzymanych informacji,
- recenzja wewnętrzna wykonanych przez rzeczoznawców opracowań.

Siłą **Izby Rzeczoznawców PTI** są profesjonalni, bezstronni, obiektywni i niezależni eksperci oraz wysoka jakość świadczonych przez nich usług.

dr inż. Przemysław Jatkiewicz – jest rzeczoznawcą Polskiego Towarzystwa Informatycznego, biegłym sądowym w zakresie informatyki obejmującej zagadnienia bezpieczeństwa informacji, wdrażania technologii informatycznych, zarządzania systemami informatycznymi oraz informatyki śledczej przy Sądzie Okręgowym w Gdańsku, a także biegłym skarbowym przy Izbie Skarbowej w Gdańsku. W swojej karierze zawodowej był technikiem, wdrożeniowcem i programistą. Związany jest z Gdańskim Zarządem Nieruchomości Komunalnych Samorządowy Zakład Budżetowy, gdzie początkowo zatrudniony był na stanowisku kierownika działu informatycznego. Obecnie pełni funkcję pełnomocnika dyrektora do spraw bezpieczeństwa informacji. Bierze również udział w projektach realizowanych przez Gminę Gdańsk jako członek komitetu sterującego oraz członek zespołu zadaniowego.
Prowadził badania, za które uzyskał stypendium InnDoktorant, II edycja 2011. Jego zainteresowania badawcze skupiają się na bezpieczeństwie informacji jednostek samorządu terytorialnego. Prowadzi wykłady na Uniwersytecie Gdańskim.

ISBN 978–83–60810–83–5

35 lat PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Polskie Towarzystwo Informatyczne
Izba Rzeczoznawców
www.pti.org.pl