Doświadczenia Urzędu Miasta Stołecznego Warszawy w realizacji audytów bezpieczeństwa informacji oraz ochrony danych osobowych w świetle zmieniającego się otoczenia prawnego

Biuro Audytu Wewnętrznego Urzędu m.st. Warszawy

Wymagania KRI - § 20 ust. 2

- wielkim wyzwaniem organizacyjnym dla Urzędu m.st. Warszawy

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, **nie rzadziej niż raz na rok.**

Miasto Stołeczne Warszawa

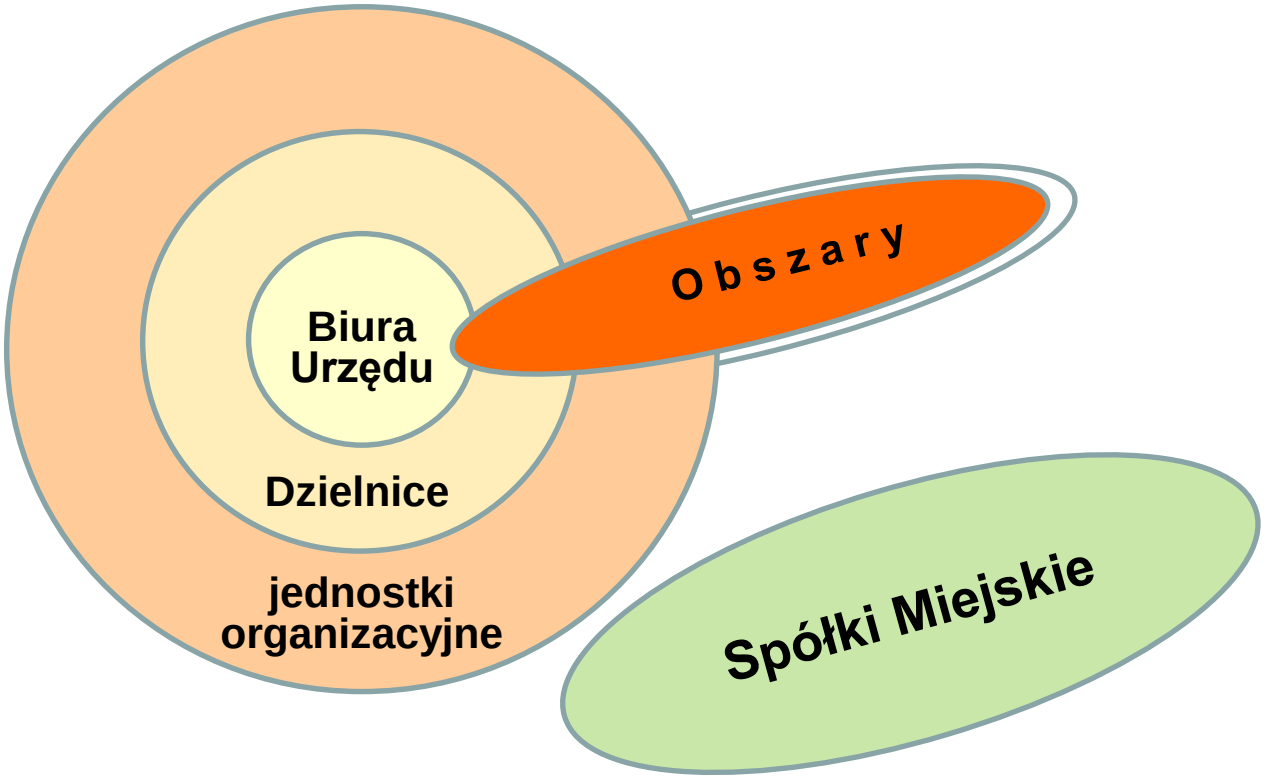
Podstawowym wyzwaniem duża liczba audytowanych jednostek

Należy pamiętać, że:
Miasto Stołeczne Warszawa to:

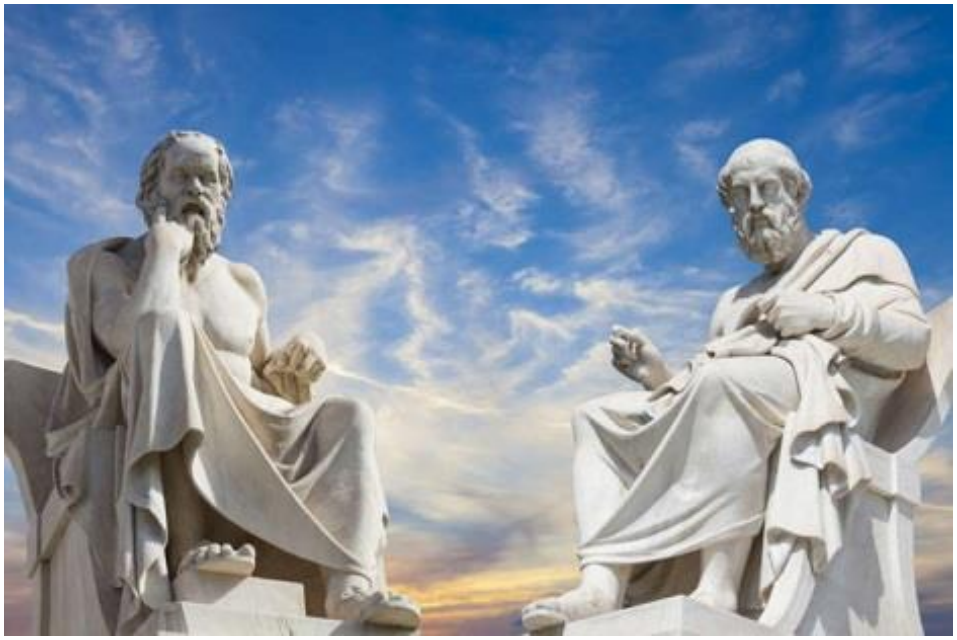
- **40** Biur Urzędu
- **18** Urzędów Dzielnic
- **ponad 1000** jednostek organizacyjnych i osób prawnych, które podlegają lub są nadzorowane przez Prezydenta m.st. Warszawy

Miasto Stołeczne Warszawa

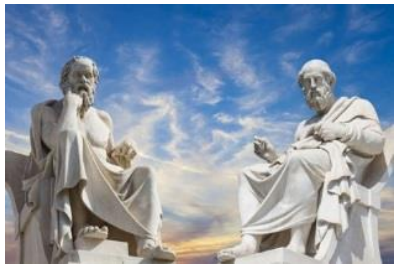
Podstawowym wyzwaniem duża liczba audytowanych jednostek



Filozofia różnych dróg zapewnienia audytu w m.st. Warszawa



Fot. shutterstock.com



Poszukiwanie optymalnej drogi postępowania

Filozofie różnych dróg prowadzących do celu …

W realizowanym rozwiązaniu organizacyjnym uwzględniono propozycje zgłoszone w grupie dyskusyjnej wskazując następujące kierunki:

- ✓ drogi tradycyjnej poprzez **audyty zapewniające**.
- ✓ ścieżki pomocniczej poprzez **audyty analityczne**

Wybór właściwej drogi zależy od wyników przeprowadzonej analizy ryzyka i rachunku kosztów.

Wyboru dokonał Prezydent m.st. Warszawy w uzgodnieniu osobą kierującą audytem.

Pierwsze działania organizacyjne
- Trochę historii

- **2008**: Pierwszy audyt bezpieczeństwa informacji w Urzędzie (w tym w Urzędach Dzielnic – wsparcie eksperta zewnętrznego),
- **2011-12**: audyty bezpieczeństwa informacji i ochrony danych osobowych zrealizowany własnymi zasobami osobowymi. Komórki audytu wspierane przez pracowników komórki IT oraz ochrony danych osobowych,
- **2013**: audyt bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie zrealizowany przez usługodawcę zewnętrznego,
- **2013**: audyt zapewniający bezpieczeństwo informacji i ochrony danych osobowych w wybranych jednostkach organizacyjnych m.st. Warszawy zrealizowany przez pracowników nowo utworzonej komórki w ramach audytu.
- **2013**: 1-szy audyt analityczny bezpieczeństwa informacji i ochrony danych osobowych w wybranych jednostkach organizacyjnych Miasta Stołecznego Warszawy (58 jednostek),
- Od **2015** roku audyt zapewniający bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie i w wybranych jednostkach organizacyjnych Miasta Stołecznego Warszawy realizowany przez pracowników komórki audytu,
- Od **2017** audyt analityczny wszystkich jednostkach organizacyjnych Miasta Stołecznego Warszawy w zrealizowany przy wykorzystaniu systemu informatycznego.

Program zadania audytowego zapewniającego - wyciąg

1. **Bezpieczeństwo informacji i ochrony danych osobowych na poziomie całej jednostki:**
   a) Organizacja procesu zarządzania bezpieczeństwem informacji i ochrony danych osobowych,
   b) Działania prewencyjne w kierunku zapewnienia bezpieczeństwa informacji,
   c) System zarządzania uprawnieniami do przetwarzania danych osobowych,
   d) Zarządzanie zasobami informatycznymi,
   e) Identyfikacja i analiza ryzyka w kierunku utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do przeprowadzonej analizy; ocena skutków dla ochrony danych.

Program zadania audytowego zapewniającego - wyciąg

f) Zarządzanie incydentami bezpieczeństwa informacji, naruszenia ochrony danych osobowych,

g) Ochrona przed złośliwym oprogramowaniem,

h) Bezpieczeństwo sieci informatycznej,

i) Testowanie, nadzorowanie i monitorowanie bezpieczeństwa.

2. Bezpieczeństwo IT na poziomie wybranego systemu

a) Dokumentacja techniczna systemu informatycznego,

b) Zarządzanie kontami i uprawnieniami użytkowników systemu informatycznego,

c) Zapewnienie ochrony przetwarzanych informacji przed nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,

d) Rozliczalność działań podejmowanych w systemie informatycznym.

Program zadania audytowego zapewniającego - wyciąg

3. Ocena serwisów internetowych pod względem bezpieczeństwa oraz spełniania wymagań WCAG wskazanych w Rozporządzeniu KRI:

a) Monitorowanie, testowanie i eliminowanie podatności serwisów internetowych,

b) Delegowanie odpowiedzialności w procesie zarządzania informacjami zamieszczanymi,

c) Dostosowanie serwisów internetowych do wymagań WCAG wskazanych w Rozporządzeniu KRI.

COBIT 5
AN ISACA® FRAMEWORK

W realizacji audytów
wykorzystujemy ocenę dojrzałości organizacji
wg metodyki COBIT 4.1,
aby ustalić dostosowanie / spełnienie wymogów
Rozporządzenia KRI oraz RODO

Metodyka COBIT 4.1
6 stopni modelu dojrzałości organizacji

Poziom dojrzałości organizacji	Opis poszczególnych poziomów dojrzałości organizacji
0 - Nieistniejący	Całkowity brak rozpoznawalnych procesów. Organizacja nie dostrzegła nawet istnienia problemu, który wymaga rozwiązania.
1 - Wstępny/doraźny	Istnieją dowody na to, że organizacja dostrzegła problemy wraz z koniecznością ich rozwiązania. Nie są to jednak ustandaryzowane procesy. Zamiast nich, do rozwiązywania poszczególnych problemów stosuje się doraźne podejście. Ogólne podejście do zarządzania nie jest podejściem zorganizowanym.
2 - Powtarzalny lecz intuicyjny	Procesy zostały rozwinięte do poziomu, na którym różne osoby wykonujące to samo zadanie postępują zgodnie z podobnymi procedurami. Nie ma formalnych szkoleń, standardowe procedury nie zostały zakomunikowane, a podjęcie odpowiedzialności pozostawiono jednostkom. Występuje wysoki poziom zależności od wiedzy poszczególnych osób, dlatego prawdopodobne jest występowanie błędów.

Metodyka COBIT 4.1
6 stopni modelu dojrzałości organizacji

Poziom dojrzałości organizacji	Opis poszczególnych poziomów dojrzałości organizacji
3 - Zdefiniowane procesy	Istnieją ustandaryzowane i udokumentowane procedury, które zostały zakomunikowane poprzez szkolenie. Pracownicy są upoważnieni do ich stosowania. Jest jednak mało prawdopodobne, że odstępstwa od stosowania procedur zostaną wykryte. Procedury nie są zaawansowane, a są raczej formalizacją istniejących praktyk.
4 - Kontrolowany i mierzalny	Kierownictwo monitoruje i ocenia zgodność z procedurami, a także podejmuje odpowiednie czynności, gdy procesy nie działają efektywnie. Procesy są stale doskonalone i stanowią źródło dobrych praktyk. W ograniczony lub fragmentaryczny sposób wykorzystywane są rozwiązania zautomatyzowane oraz narzędzia.
5 - Zoptymalizowany	Procesy zostały dopracowane do poziomu dobrej praktyki w oparciu o efekty ciągłego doskonalenia i modelowanie dojrzałości w innych organizacjach. Technologia informatyczna jest wykorzystywana w zintegrowany sposób do automatyzacji toku pracy, zapewniając narzędzia służące poprawie jakości i wydajności oraz sprawiając, że jednostka szybko adaptuje się do zmieniających się warunków.

Co oceniamy?

Oceniane obszary i podobszary – Poziom dojrzałości jednostki w skali 0-5		Jednostka 1	Jednostka 2	Jednostka 3	Jednostka 4	Jednostka 5	Jednostka 6
Bezpieczeństwo informacji i ochrony danych osobowych na poziomie całej jednostki	a) Organizacja procesu zarządzania bezpieczeństwem informacji i ochrony danych osobowych	2	2	1	1	2	1
	b) Działania prewencyjne w kierunku zapewnienia bezpieczeństwa informacji	1	2	0	0	1	0
	c) System nadawania upoważnień do przetwarzania danych osobowych	2	3	1	1	3	2
	d) Zarządzanie zasobami informatycznymi	1	1	0	1	2	1
	e) Identyfikacja i analiza ryzyka w kierunku utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko stosownie do przeprowadzonej analizy	2	1	1	1	2	0
	f) Zarządzanie incydentami bezpieczeństwa informacji	3	1	0	1	1	1
	g) Ochrona przed złośliwym oprogramowaniem	4	1	0	1	1	1
	h) Bezpieczeństwo sieci informatycznej	4	1	1	0	2	2
	i) Testowanie, nadzorowanie i monitorowanie bezpieczeństwa	2	1	2	0	2	1
Bezpieczeństwo IT na poziomie wybranego systemu	a) Dokumentacja techniczna systemu informatycznego	4	1	0	1	2	1
	b) Zarządzanie kontami i uprawnieniami użytkowników systemu informatycznego	4	3	0	1	1	1
	c) Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami	3		0	1	1	0
Ocena bezpieczeństwa serwisów internetowych oraz spełniania wymagań WCAG 2.0	a) Monitorowanie, testowanie i eliminowanie podatności serwisów internetowych w tym BIP	1	0	0	0	0	0
	b) Delegowanie odpowiedzialności w procesie zarządzania informacjami zamieszczanymi w BIP	3	1	1	1	2	1
	c) Dostosowanie serwisów internetowych do wymagań WCAG 2.0 wskazanych w Rozporządzeniu KRI	1	0	0	0	1	0

Audyt zapewniający

Ocena dojrzałości
oraz rzeczywiste badanie systemów informatycznych

Dlaczego badając obszar bezpieczeństwa informacji zagłębiamy się w badania systemów informatycznych?

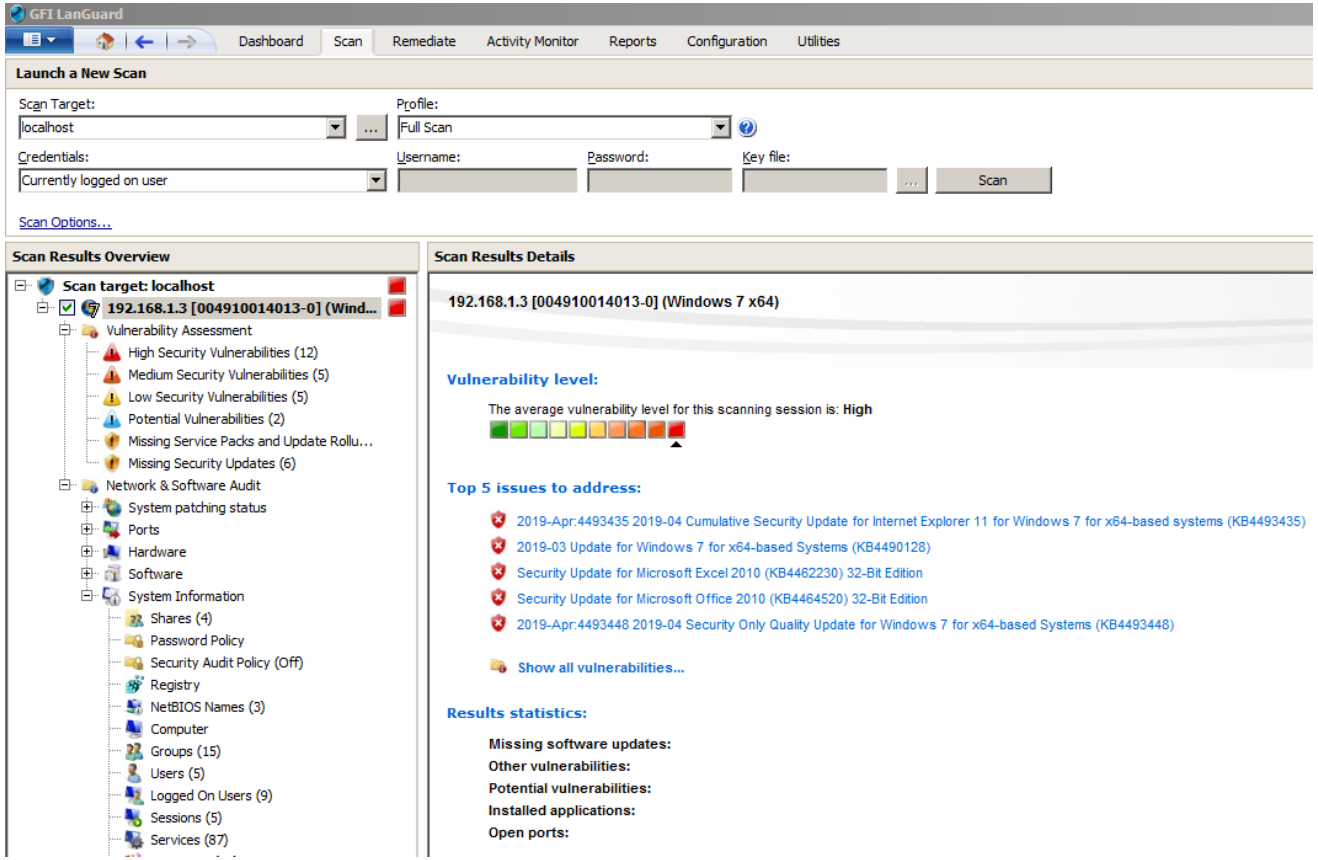
W dokumentach jak w pentagonie,

realizacja jak w przedszkolu.

Audyt zapewniający

Co badamy poza dokumentacją?

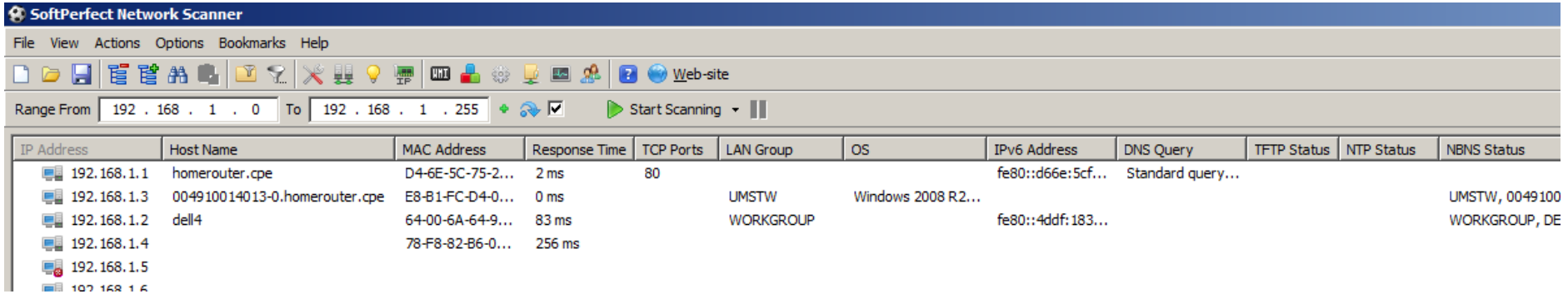
- Stan aktualizacji stacji roboczych i serwerów pod kątem oprogramowania systemowego i niesystemowego – realizowane za pomocą skanera podatności



Audyt zapewniający

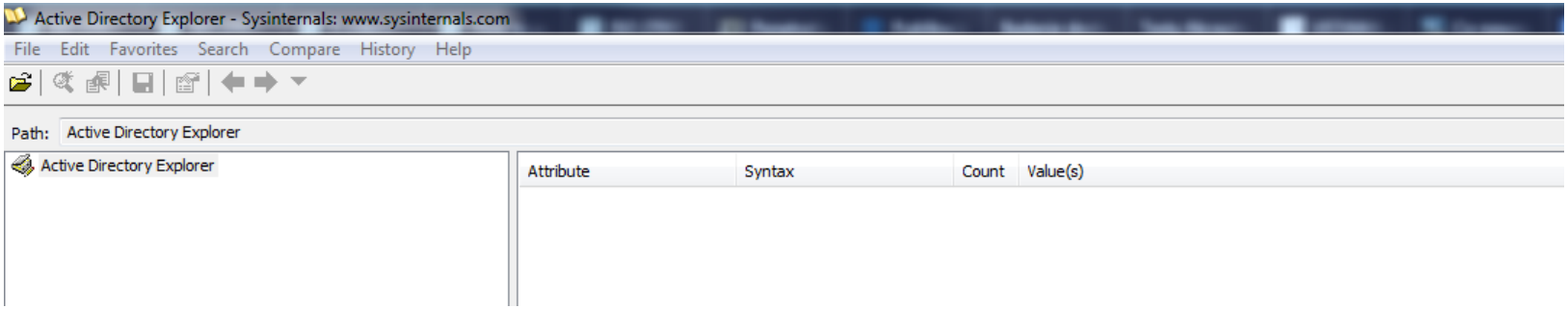
Co badamy poza dokumentacją?

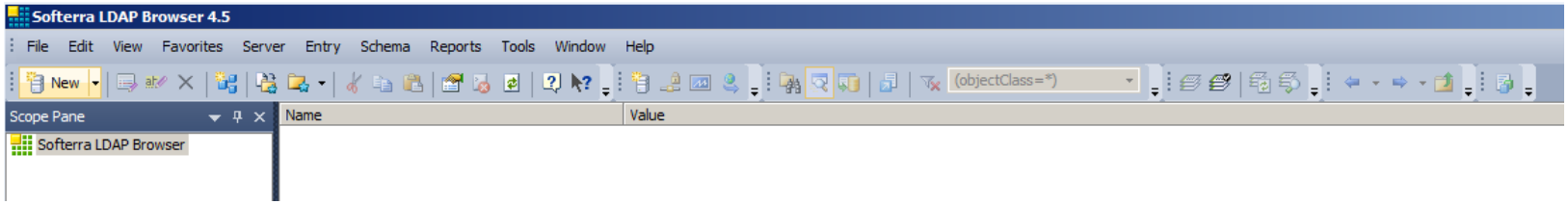
- Usługi uruchomione w wewnętrznych sieciach komputerowych, udostępnione udziały sieciowe, urządzenia sieciowe – realizowane za pomocą automatycznych skanerów



Audyt zapewniający
Co badamy poza dokumentacją?

- Ustawienia polityk usługi katalogowej Active Directory

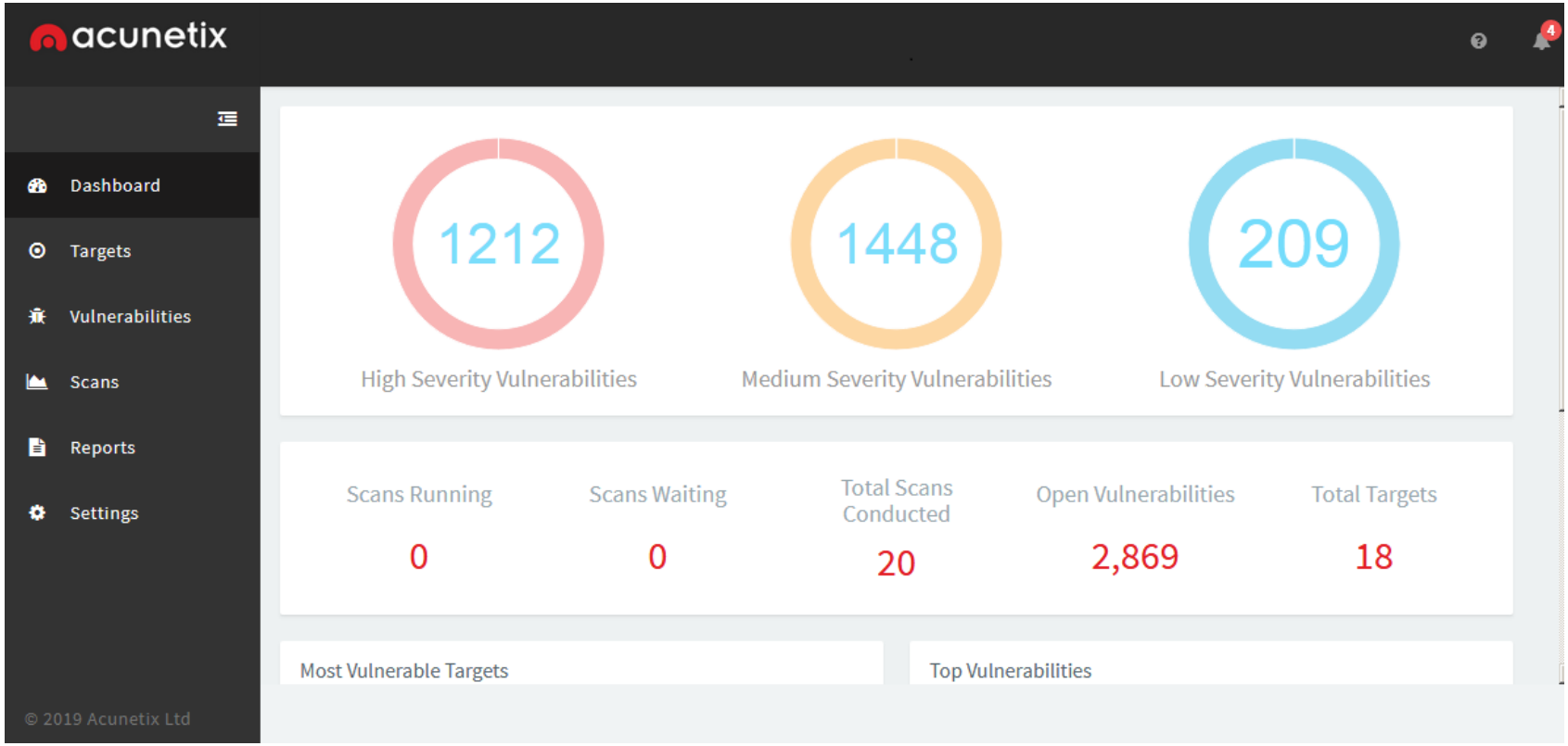




Audyt zapewniający

Co badamy poza dokumentacją?

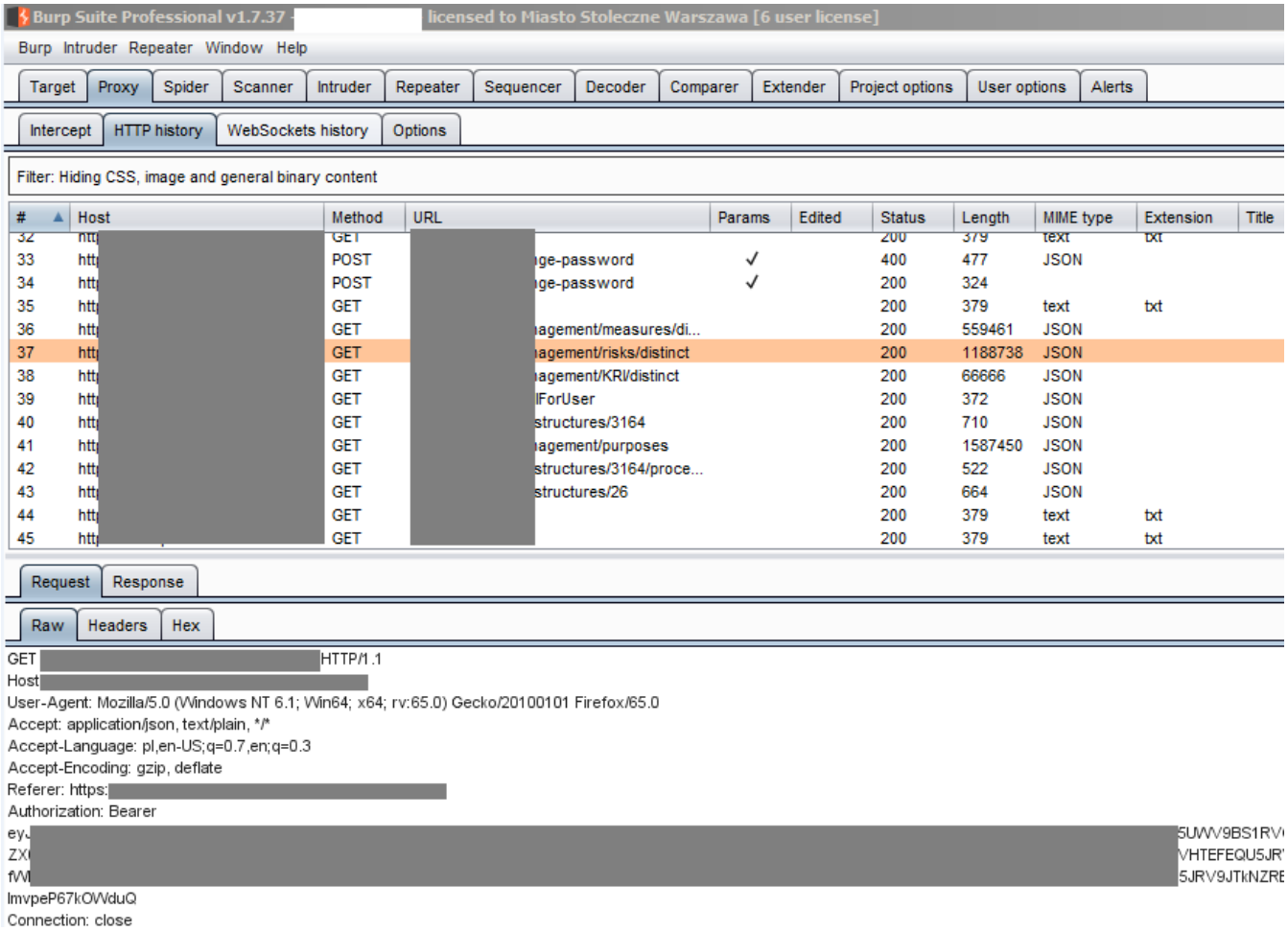
- Testy bezpieczeństwa serwisów internetowych – automatyczny skaner podatności



Audyt zapewniający

Co badamy poza dokumentacją?

- Testy bezpieczeństwa serwisów internetowych - testy manualne



Audyt zapewniający

Co badamy poza dokumentacją?

- Pliki potencjalnie objęte prawami autorskimi
- Pliki potencjalnie szkodliwe, crack-i,
- Licencje na zainstalowane oprogramowanie
- Zintegrowane zapory sieciowe – czy skonfigurowane, czy zarządzane
- Systemy bezpieczeństwa – czy aktualne definicje
- Logi z systemów
- WCAG

Audyt zapewniający

Dlaczego wychodzimy poza badanie dokumentacji

- kierownictwo komórek audytowanych dostaje informacje o faktycznym stanie bezpieczeństwa, a nie tylko tym wynikającym z istnienia dokumentacji
- zwykle wiele czynności nie jest udokumentowanych (brak czasu, wygoda, bycie niezastąpionym)
- brak Systemu Zarządzania Bezpieczeństwem Informacji – działania informatyków są często podejmowane zwyczajowo
- działania komórek IT są trudne do kontrolowania bez wiedzy informatycznej
- nadzór i rozliczanie wewnętrznych służb IT lub podmiotów zewnętrznych świadczących opiekę informatyczną jest nierzadko dla kierowników audytowanych komórek zadaniem trudnym
- organizacja uczy się realizując zadania

Audyty analityczne i zapewniające

Wspólne elementy …

Księga procedur:

URZĄD MIASTA STOŁECZNEGO WARSZAWY
Biuro Audytu Wewnętrznego

KSIĘGA PROCEDUR BIURA AUDYTU WEWNĘTRZNEGO URZĘDU M.ST. WARSZAWY	
Data wydania – 30 czerwca 2018 r.	Wersja 8

KSIĘGA PROCEDUR

BIURA AUDYTU WEWNĘTRZNEGO URZĘDU M.ST. WARSZAWY

STANDARD 2040
ZASADY I PROCEDURY

MIĘDZYNARODOWE STANDARDY PRAKTYKI ZAWODOWEJ AUDYTU WEWNĘTRZNEGO

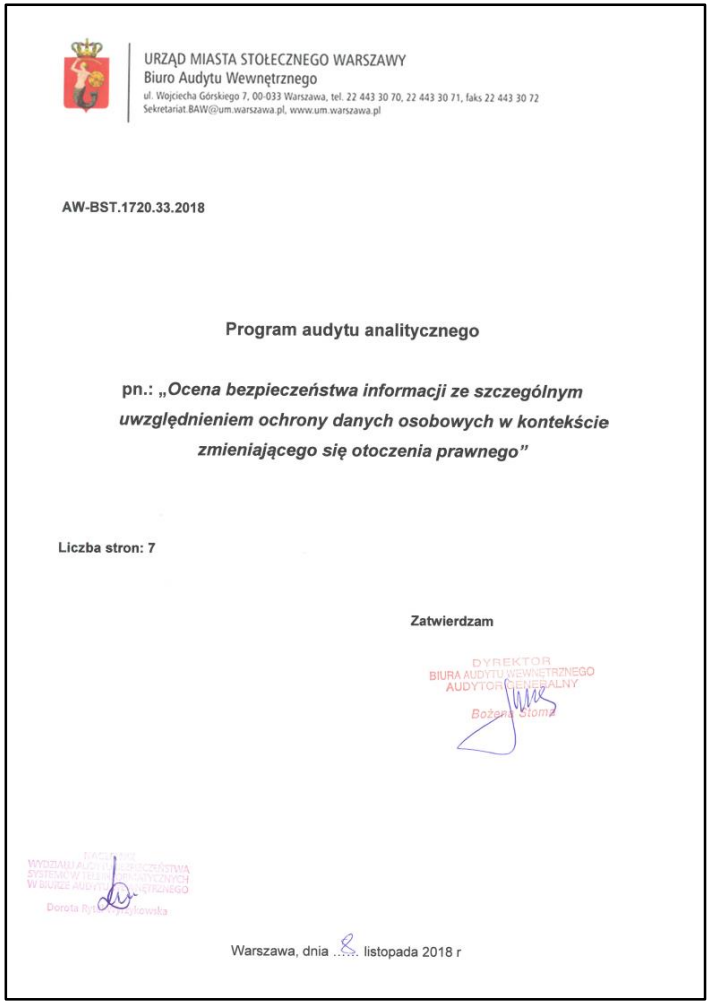
AKCEPTOWAŁ	ZATWIERDZIŁ
DYREKTOR BIURA AUDYTU WEWNĘTRZNEGO AUDYTOR GENERALNY Bożena Stoma	PREZYDENT MIASTA STOŁECZNEGO WARSZAWY Hanna Gronkiewicz-Waltz
29.06.2018 Data podpis	Data podpis

Przygotowano w Wydziale Wsparcia Merytorycznego

Audyty analityczne i zapewniające

Wspólne elementy …

Program zadania:



URZĄD MIASTA STOŁECZNEGO WARSZAWY
Biuro Audytu Wewnętrznego
ul. Wojciecha Górskiego 7, 00-033 Warszawa, tel. 22 443 30 70, 22 443 30 71, faks 22 443 30 72
Sekretariat.BAW@um.warszawa.pl, www.um.warszawa.pl

AW-BST.1720.33.2018

Program audytu analitycznego

pn.: *„Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego”*

Liczba stron: 7

Zatwierdzam

DYREKTOR
BIURA AUDYTU WEWNĘTRZNEGO
AUDYTOR GENERALNY
Bożena Słoma

Warszawa, dnia 8 listopada 2018 r

Audyt analityczny

Mocne strony

Przykładowe mocne strony:

1. Audyt analityczny jest ukierunkowany na jednoczesne badanie licznych grup jednostek samorządu terytorialnego (JST). Podstawą badania są odpowiedzi w tym samym czasie, na takie same pytania zawarte w kwestionariuszu.
2. Relatywnie „krótki” czas zadania audytowego w formie audytu analitycznego, niemożliwy do uzyskania w formie audytu zapewniającego, przy tak dużej zróżnicowanej populacji.
3. Przejrzysta prezentacja wyników audytu.

Audyt analityczny
Problemy i ryzyka

- niezrozumienie pytań, spowodowane m.in. niedostatecznymi kompetencjami merytorycznymi lub niezrozumieniem językowym,
- brak obecności badającego w procesie przeprowadzania badania, który mógłby wyjaśnić wątpliwości na bieżąco,
- zafałszowanie udzielanych odpowiedzi, które mogą być spowodowane chęcią osiągnięcia lepszych wyników ankiety, według subiektywnego zrozumienia jej przez wypełniającego lub niską motywacją badanego do udzielenia rzetelnych odpowiedzi na zadane pytania,
- niepełne dostosowanie pytań do szczegółowej specyfiki jednostek przy użyciu wystandaryzowanego narzędzia informatycznego,
- problemy techniczne z funkcjonowaniem narzędzia informatycznego, zarówno w warstwie sprzętowej jak i programowej,
- brak kontroli nad czynnikami zewnętrznymi, które mogą rozpraszać osobę wypełniającą podczas badania,
- brak możliwości weryfikacji autentyczności osób wypełniających ankietę.

Audyt analityczny

Kwestionariusz audytowy

Kwestionariusz audytu w zakresie oceny bezpieczeństwa informacji	
	Temat zadania audytowego:
	Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego
	Nr zadania: **AW-BST.1720.33.2018**

1. Cześć A - Dane o jednostce

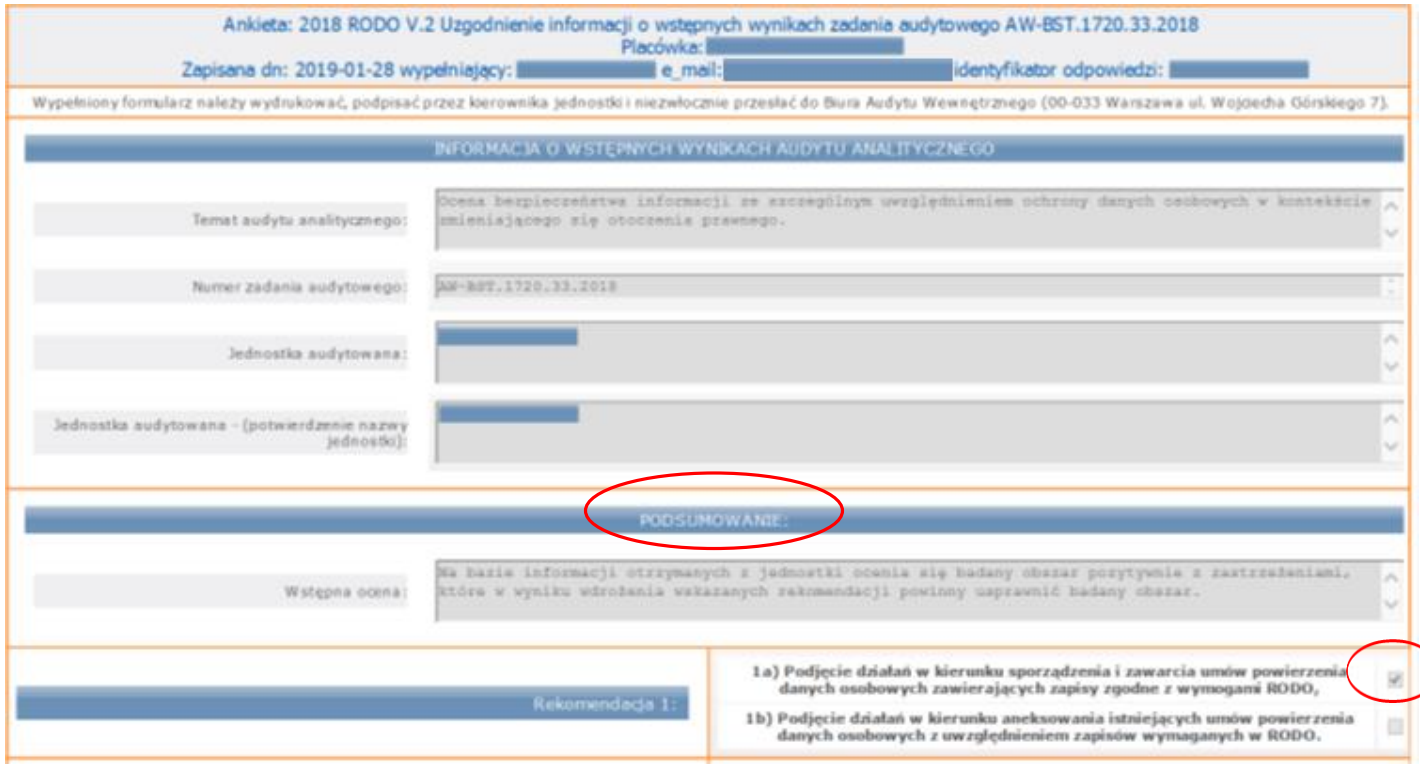
1.1 Pełna nazwa jednostki:	
1.2 Skrócona nazwa jednostki:	
1.3 Adres do korespondencji:	
1.4 Adres poczty elektronicznej sekretariatu badanej jednostki:	
1.5 Imię i nazwisko osoby wypełniającej "Kwestionariusz", email i telefon kontaktowy:	
1.6 Stanowisko (funkcja)	Kierownik jednostki / Inspektor Ochrony Danych / Kierownik komórki organizacyjnej / Pracownik wykonujący zadania IT/ Inna osoba

2. Część B – Badanie audytowe

Lp.	Pytanie	Odpowiedź (Słownik)
2.1	Czy jednostka przetwarza zwykłe[v] kategorie danych osobowych? *(Dawniej nazywane zwykłymi danymi osobowymi - podział przed obowiązkiem stosowania RODO obejmował dane zwykłe i wrażliwe)*	Tak / Nie
2.2	Czy jednostka przetwarza szczególne[2] kategorie danych? *(Obejmują większość dawnych danych wrażliwych, sensytywnych, prawie cały art. 27 poprzedniej ustawy o ochronie danych osobowych z 1997 roku oraz dodatkowe dane biometryczne i ...)*	Tak / Nie
2.3	Czy jednostka przetwarza dane dotyczące wyroków skazujących i czynów zabronionych?	Tak / Nie
2.4	Czy jednostka przetwarza dane dzieci (do 18 roku życia)?	Tak / Nie
2.5	Czy jednostka przetwarza powierzone dane osobowe?	Tak / Nie
2.6	Ile podmiotów powierza dane osobowe jednostce?	[Liczba]
2.7	Ile umów powierzenia danych osobowych z tych jednostek jest obecnie aktywnych?	[Liczba]
2.8	Czy jednostka powierza przetwarzanie danych osobowych poza jednostkę?	Tak / Nie
2.9	Ilu podmiotom jednostka powierza dane osobowe?	[Liczba]
2.10	Ile umów powierzenia danych osobowych jednostki, innym podmiotom jest obecnie aktywnych?	[Liczba]

Audyt analityczny

Uzgodnienie



Ankieta: 2018 RODO V.2 Uzgodnienie informacji o wstępnych wynikach zadania audytowego AW-BST.1720.33.2018
Placówka: [redacted]
Zapisana dn: 2019-01-28 wypełniający: [redacted] e_mail: [redacted] identyfikator odpowiedzi: [redacted]

Wypełniony formularz należy wydrukować, podpisać przez kierownika jednostki i niezwłocznie przesłać do Biura Audytu Wewnętrznego (00-033 Warszawa ul. Wojciecha Górskiego 7).

INFORMACJA O WSTĘPNYCH WYNIKACH AUDYTU ANALITYCZNEGO

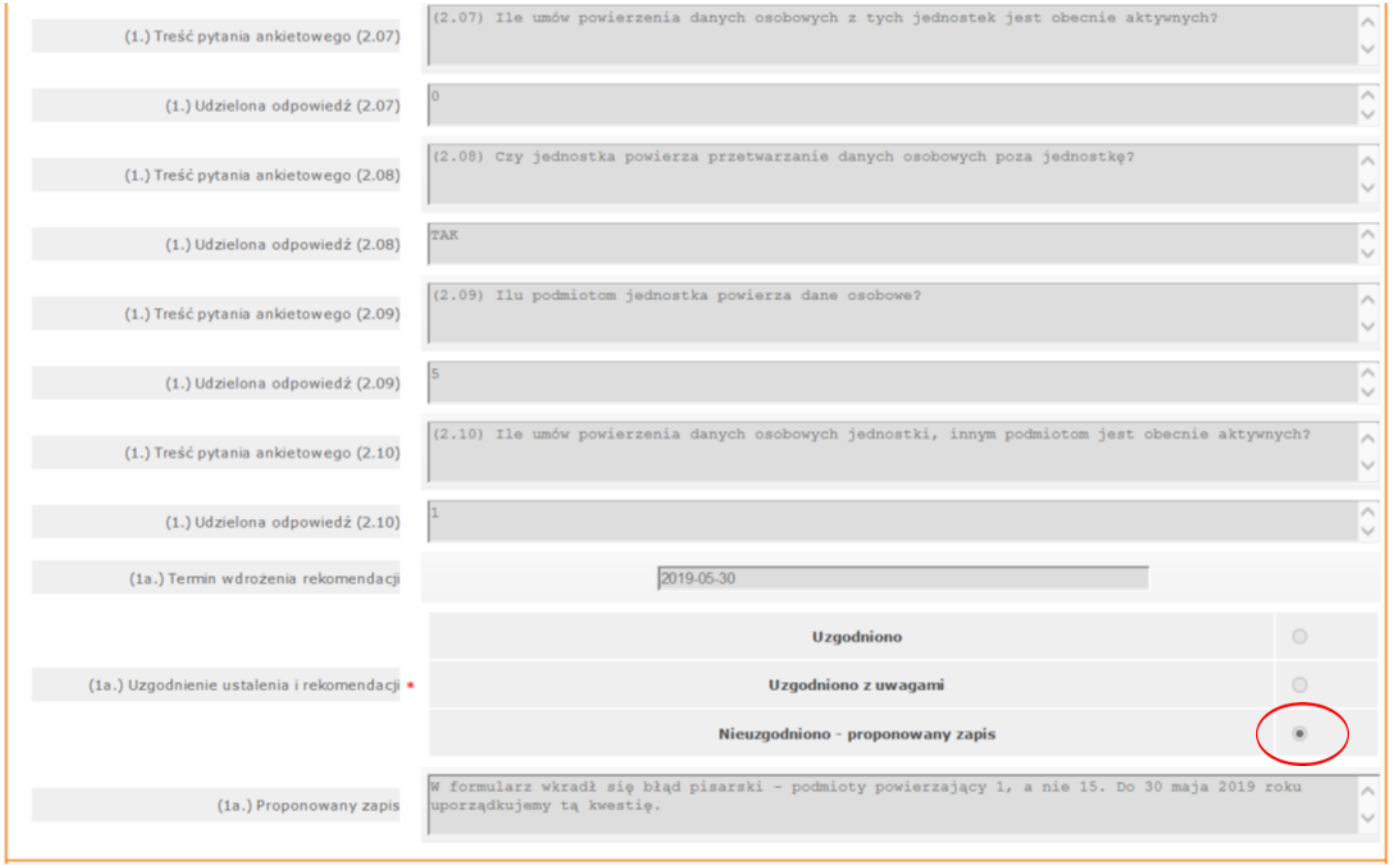
Temat audytu analitycznego:	Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego.
Numer zadania audytowego:	AW-BST.1720.33.2018
Jednostka audytowana:	[redacted]
Jednostka audytowana - (potwierdzenie nazwy jednostki):	[redacted]

PODSUMOWANIE:

Wstępna ocena:	Na bazie informacji otrzymanych z jednostki ocenia się badany obszar pozytywnie z zastrzeżeniami, która w wyniku wdrożenia wskazanych rekomendacji powinny usprawnić badany obszar.

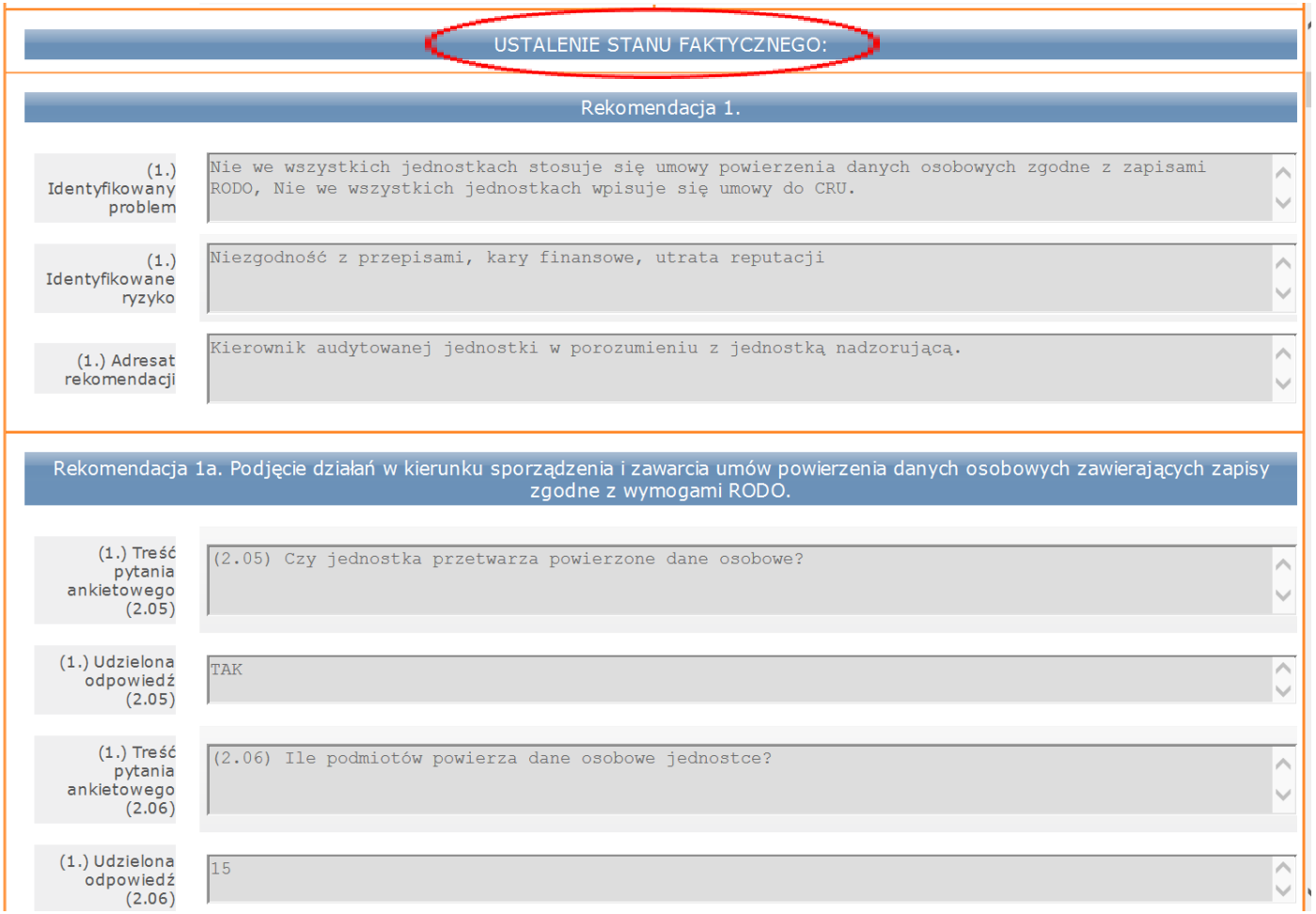
Rekomendacja 1:	1a) Podjęcie działań w kierunku sporządzenia i zawarcia umów powierzenia danych osobowych zawierających zapisy zgodne z wymogami RODO, ☑
	1b) Podjęcie działań w kierunku aneksowania istniejących umów powierzenia danych osobowych z uwzględnieniem zapisów wymaganych w RODO. ☐

Audyt analityczny
Uzgodnienie



Audyt analityczny

Sprawozdanie



USTALENIE STANU FAKTYCZNEGO:

Rekomendacja 1.

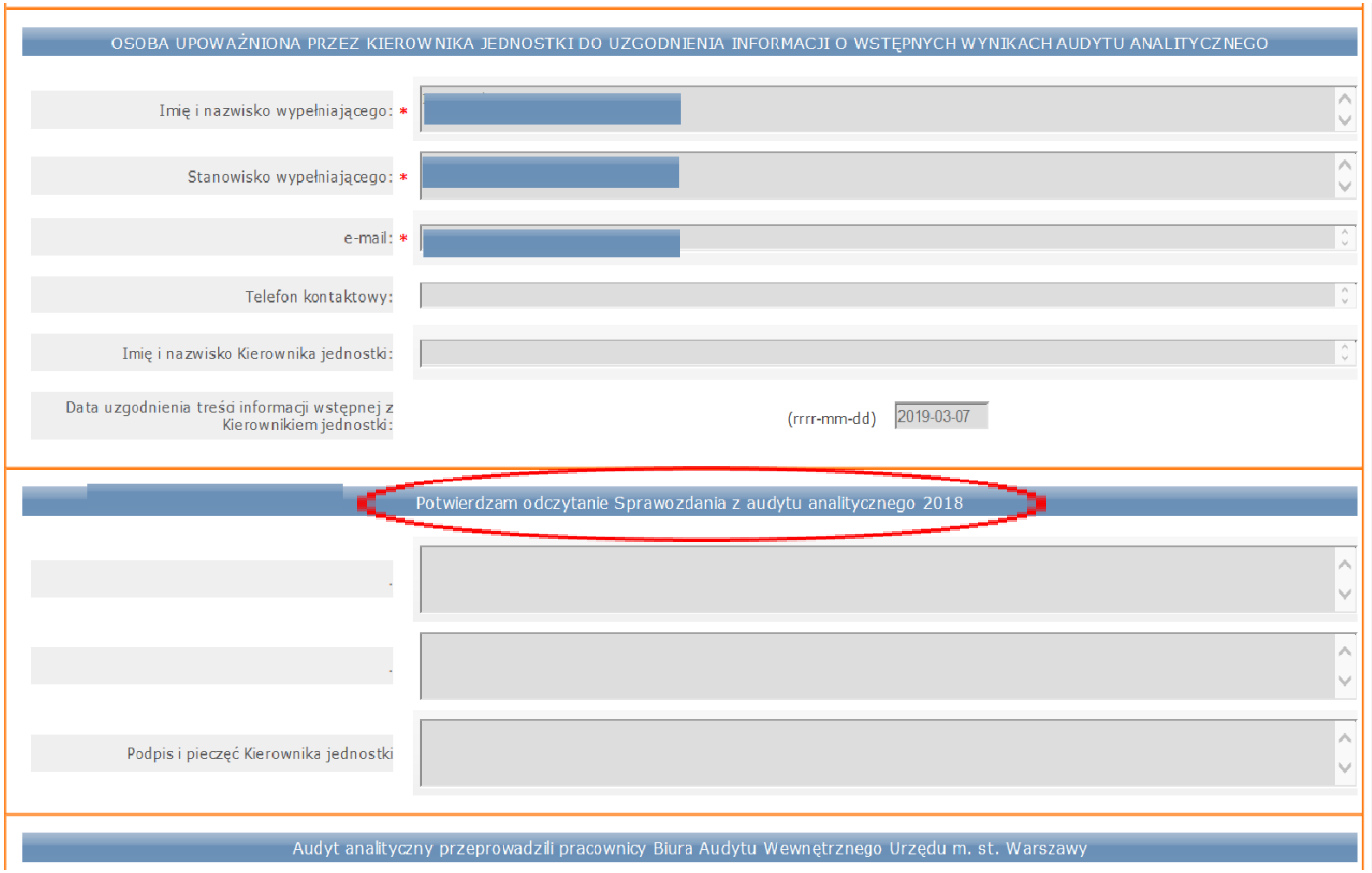
(1.) Identyfikowany problem	Nie we wszystkich jednostkach stosuje się umowy powierzenia danych osobowych zgodne z zapisami RODO, Nie we wszystkich jednostkach wpisuje się umowy do CRU.
(1.) Identyfikowane ryzyko	Niezgodność z przepisami, kary finansowe, utrata reputacji
(1.) Adresat rekomendacji	Kierownik audytowanej jednostki w porozumieniu z jednostką nadzorującą.

Rekomendacja 1a. Podjęcie działań w kierunku sporządzenia i zawarcia umów powierzenia danych osobowych zawierających zapisy zgodne z wymogami RODO.

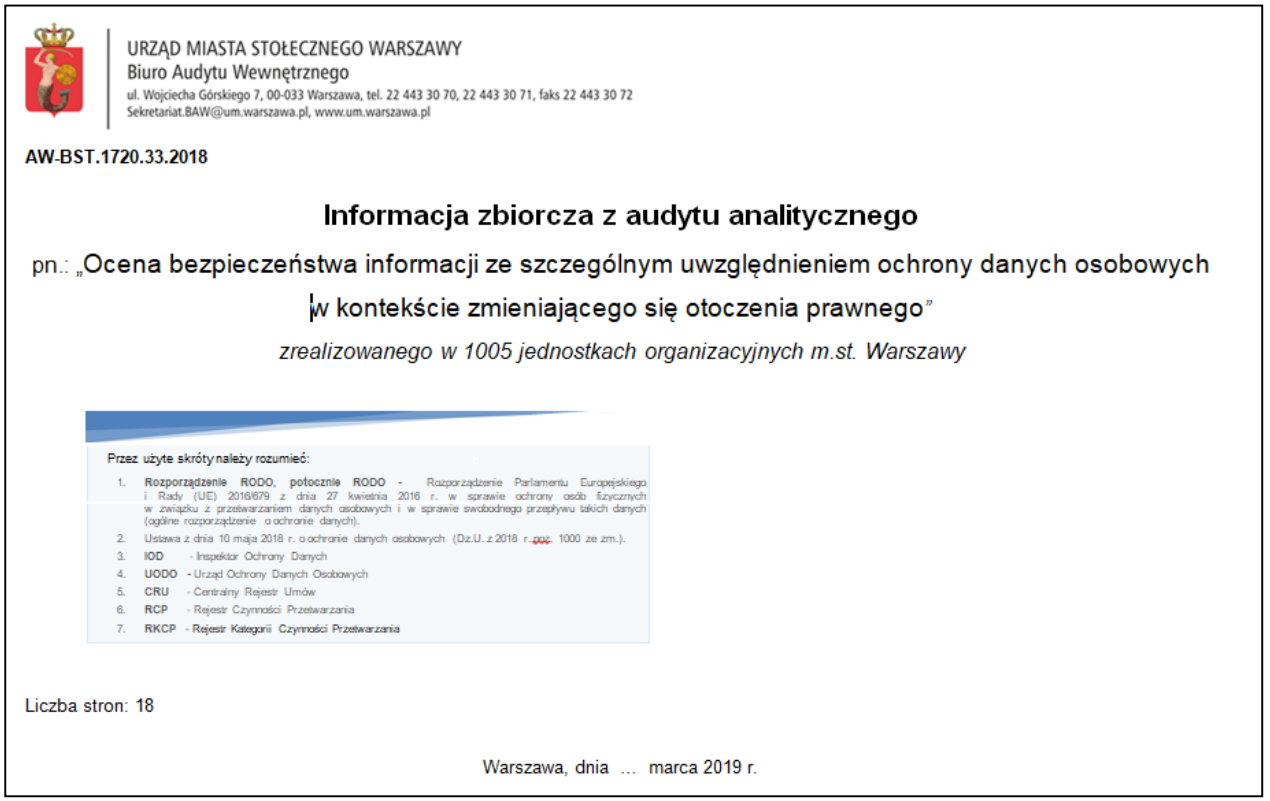
(1.) Treść pytania ankietowego (2.05)	(2.05) Czy jednostka przetwarza powierzone dane osobowe?
(1.) Udzielona odpowiedź (2.05)	TAK
(1.) Treść pytania ankietowego (2.06)	(2.06) Ile podmiotów powierza dane osobowe jednostce?
(1.) Udzielona odpowiedź (2.06)	15

Audyt analityczny

Sprawozdanie



Audyt analityczny
Informacja zbiorcza



URZĄD MIASTA STOŁECZNEGO WARSZAWY
Biuro Audytu Wewnętrznego
ul. Wojciecha Górskiego 7, 00-033 Warszawa, tel. 22 443 30 70, 22 443 30 71, faks 22 443 30 72
Sekretariat.BAW@um.warszawa.pl, www.um.warszawa.pl

AW-BST.1720.33.2018

Informacja zbiorcza z audytu analitycznego

pn.: „Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego"

zrealizowanego w 1005 jednostkach organizacyjnych m.st. Warszawy

Przez użyte skróty należy rozumieć:

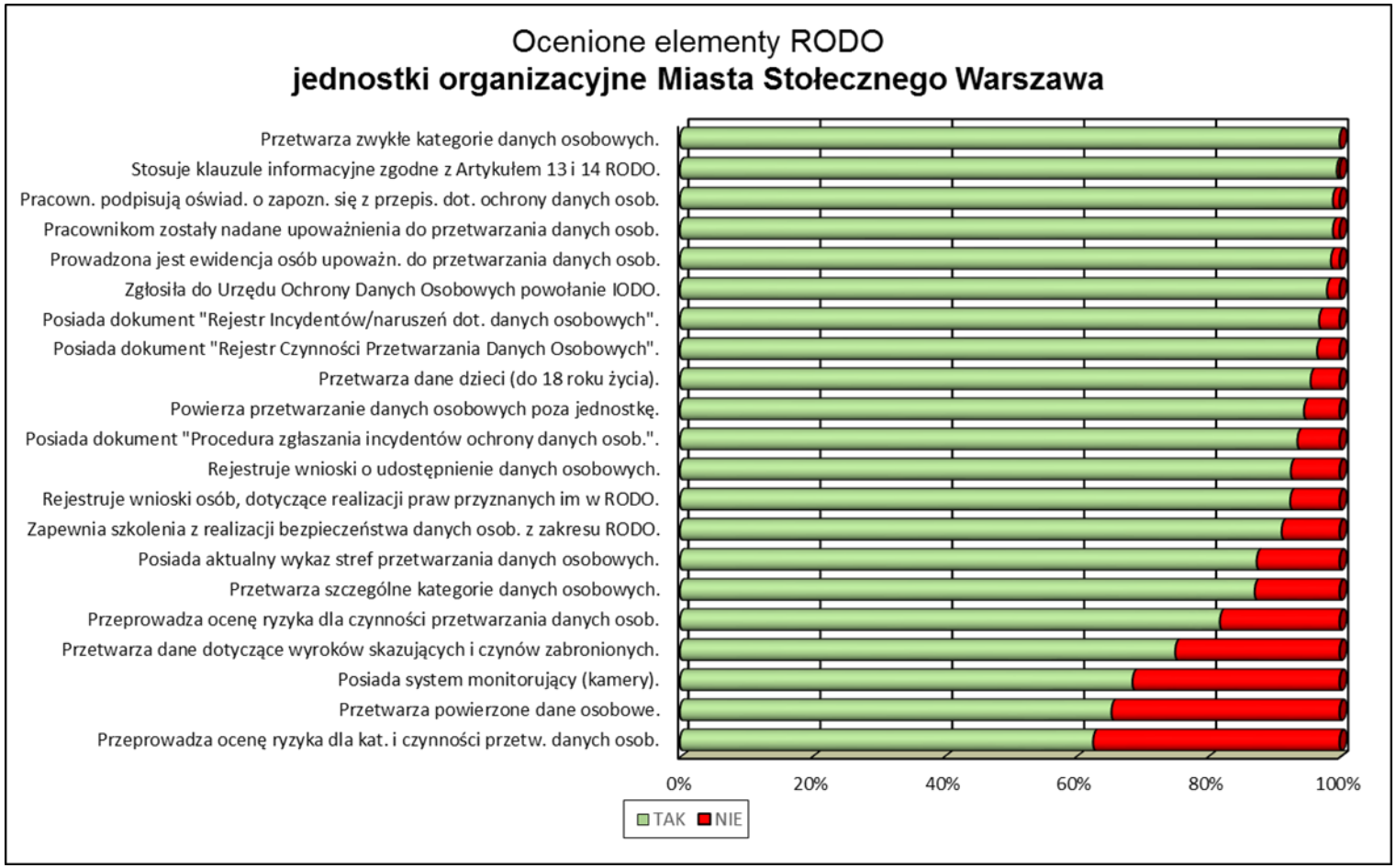
1. **Rozporządzenie RODO, potocznie RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.).
3. **IOD** - Inspektor Ochrony Danych
4. **UODO** - Urząd Ochrony Danych Osobowych
5. **CRU** - Centralny Rejestr Umów
6. **RCP** - Rejestr Czynności Przetwarzania
7. **RKCP** - Rejestr Kategorii Czynności Przetwarzania

Liczba stron: 18

Warszawa, dnia ... marca 2019 r.

Audyt analityczny

Informacja zbiorcza



Audyt analityczny

Informacja zbiorcza

Nazwa Obszaru	Liczba audytowanych jednostek	Liczba rekomendacji nr:												
		1 a)	1 b)	2 a)	2 b)	2 c)	2 d)	2 e)	3 a)	3 b)	4 a)	4 b)	5	6
Edukacja	804	101	43	11	24	43	22	36	4	7	133	151	70	11
Kultura	70	8	3	1	4	7	3	7	3	7	18	15	8	1
Pomoc Społeczna	66	13	3	0	1	5	3	5	1	2	11	15	8	2
Sport i Rekreacja	18	1	1	0	2	3	0	2	1	1	3	2	3	1
Ochrona Zdrowia	17	2	0	0	0	2	0	1	1	0	0	1	1	0
Gospodarowanie Nieruchomościami Miasta	14	1	0	0	1	1	0	1	0	0	1	1	2	1
Aktywność Obywatelska	1	0	0	0	0	0	0	0	0	0	1	1	0	0
Architektura i Urbanistyka	1	0	0	0	0	0	0	0	0	0	1	0	0	0
Bezpieczeństwo i Porządek Publiczny	1	1	1	0	0	0	0	0	0	0	0	0	0	0
Finanse Publiczne	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Funkcjonowanie Organów Władzy	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Gospodarowanie Środowiskiem	4	0	0	0	0	0	0	0	0	0	0	0	0	0
Transport, Komunikacja i Drogownictwo	3	0	0	0	0	0	0	0	0	0	1	1	0	0
Usługi Komunalne	3	1	0	0	0	0	0	0	0	0	0	1	0	0
Razem:	1005	128	51	12	32	61	28	52	10	17	169	188	92	16

Audyt zapewniający i analityczny

Korzyści z połączenia audytu zapewniającego i analitycznego

- Audyt analityczny to możliwość wykorzystania analizy do przeglądu wstępnego do audytu zapewniającego
- Ocena obszaru na podstawie licznej populacji jednostek audytowanych
- Analiza trendu zamian w poszczególnych obszarach
- Upowszechnienie wiedzy o wymaganiach względem KRI i RODO
- Zwiększenie wiarygodności informacji przekazywanych przez audytowanych w kwestionariuszach z audytu analitycznego
- Obniżenie kosztów audytu
- Podejście systemowe do procesów bezpieczeństwa informacji u audytowanych

Dziękujemy

Prelegenci z Biura Audytu Wewnętrznego Urzędu m.st. Warszawy:

Dorota Rytel-Wyrzykowska (drytel@um.warszawa.pl)

Mariusz Urban (mariusz.urban@um.warszawa.pl)