URZĄD MIASTA I GMINY
74-100 Gryfino, ul. 1 Maja 16
tel.091 416 22 10, fax 091 416 27 02
Regon 000528333 NIP 858-11-27-857
e-mail: burmistrz@gryfino.pl
(nazwa i adres jednostki sektora finansów publicznych, w której jest zatrudniony audytor wewnętrzny)

BURMISTRZ
Miasta i Gminy
GRYFINO
Mieczysław Sawaryn
18.01.2016

BAW.1721.1.2016

SPRAWOZDANIE
Z WYKONANIA PLANU AUDYTU ZA ROK 2015

1. Jednostki sektora finansów publicznych objęte audytem wewnętrznym

Lp.	Nazwa jednostki
1	2
1.	Urząd Miasta i Gminy w Gryfinie – jednostka zatrudniająca Audytora Wewnętrznego
2.	Zespół Szkół w Gryfinie
3.	Szkoła Podstawowa Nr 1 im. Marii Dąbrowskiej w Gryfinie
4.	Szkoła Podstawowa Nr 2 im. kpt. ż. w. Mamerta Stankiewicza w Gryfinie
5.	Szkoła Podstawowa im. Księcia Barnima I w Żabnicy
6.	Szkoła Podstawowa im. Małych Zesłańców Sybiru w Radziszewie
7.	Zespół Szkół Ogólnokształcących w Gryfinie
8.	Zespół Szkół w Gardnie
9.	Zespół Szkół w Chwarstnicy
10.	Ośrodek Sportu i Rekreacji w Gryfinie
11.	Zakład Ekonomiczno – Administracyjny Szkół w Gryfinie
12.	Gryfiński Dom Kultury
13.	Biblioteka Publiczna w Gryfinie
14.	Ośrodek Pomocy Społecznej
15.	Młodzieżowy Ośrodek Sportowy w Gryfinie
16.	Centrum Wodne „Laguna" w Gryfinie
17.	Przedszkole Nr 1 im. Krasnala Hałabały w Gryfinie
18.	Przedszkole Nr 2 z oddziałami żłobkowymi im. Misia Uszatka w Gryfinie
19.	Przedszkole Nr 3 im. Kubusia Puchatka w Gryfinie
20.	Przedszkole Nr 4 w Gryfinie
21.	Przedszkole Nr 5 w Gryfinie

2. Podstawowe informacje o komórce audytu wewnętrznego

Lp.	Imię i nazwisko[1]	Nazwa stanowiska	Numer telefonu	Adres poczty elektronicznej	Wymiar czasu pracy (w etatach)	Kwalifikacje zawodowe[2]	Udział w szkoleniach w roku sprawozdawczym (w osobodniach)
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1.	Anna Myśko (do dnia 1 marca 2015 r.)	Audytor wewnętrzny	(091) 416 20 11	audyt@gryfino.pl	1	CGAP, egzamin MF	14[3]

Czy w roku sprawozdawczym dokonywano udokumentowanej samooceny audytu wewnętrznego?	Tak

3. Przeprowadzone zadania zapewniające i czynności doradcze w roku sprawozdawczym

Lp.	Temat zadania zapewniającego albo przedmiot czynności doradczych	Zadanie zapewniające albo czynności doradcze *podać odpowiednio*	Zadanie zapewniające ujęte w planie audytu na rok sprawozdawczy *Tak/ Nie*	W przypadku audytu wewnętrznego zleconego wskazać podmiot zlecający audyt	Obszar działalności związany z dysponowaniem środkami europejskimi, o których mowa w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych[4] /tak/nie/ *tak/nie*	Obszar ryzyka, w którym przeprowadzono zadanie audytowe *wskazać odpowiedni obszar*	Typ obszaru działalności *wpisać odpowiednio: „p" dla działalności podstawowej albo „w" dla działalności wspomagającej*	Powołanie rzeczoznawcy *tak/nie*	Liczba osobodni planowanych na przeprowadzenie zadania zapewniającego */w przypadku zadań zrealizowanych poza planem wpisać „-"/*	Liczba osobodni wykorzystanych na przeprowadzenie zadania zapewniającego albo wykonanie czynności doradczych	Liczba zaleceń zawartych w sprawozdaniu *odnosi się do zadań zapewniających*	Liczba zaleceń zaakceptowanych do realizacji *odnosi się do zadań zapewniających*	Liczba wdrożonych zaleceń *odnosi się do zadań zapewniających*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*

[1] Należy wpisać dane wszystkich osób zatrudnionych w komórce audytu wewnętrznego, według stanu na 31 grudnia roku sprawozdawczego.
[2] Kwalifikacje zawodowe, o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2013 r., poz. 885 ze zm.). W przypadku braku ww. kwalifikacji zawodowych należy wpisać „–".
[3] Szkolenia merytorycznie związane z zakresem audytu wewnętrznego oraz samoszkolenie.
[4] Zgodnie z brzmieniem art. 2 pkt 5 ustawy z dnia z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2013 r., poz. 885 ze zm.) przez pojęcie środki europejskie - rozumie się środki, o których mowa w art. 5 ust. 3 pkt 1, 2 i 4 przedmiotowej ustawy.

Lp.	Temat zadania zapewniającego albo przedmiot czynności doradczych	Zadanie zapewniające albo czynności doradcze *podać odpowiednio*	Zadanie zapewniające ujęte w planie audytu na rok sprawozdawczy *Tak/ Nie*	W przypadku audytu wewnętrznego zleconego wskazać podmiot zlecający audyt	Obszar działalności związany z dysponowaniem środkami europejskimi, o których mowa w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych[4] /tak/nie/ *tak/nie*	Obszar ryzyka, w którym przeprowadzono zadanie audytowe *wskazać odpowiedni obszar*	Typ obszaru działalności *wpisać odpowiednio: „p" dla działalności podstawowej albo „w" dla działalności wspomagającej*	Powołanie rzeczoznawcy *tak/nie*	Liczba osobodni planowanych na przeprowadzenie zadania zapewniającego */w przypadku zadań zrealizowanych poza planem wpisać „-"/*	Liczba osobodni wykorzystanych na przeprowadzenie zadania zapewniającego albo wykonanie czynności doradczych	Liczba zaleceń zawartych w sprawozdaniu *odnosi się do zadań zapewniających*	Liczba zaleceń zaakceptowanych do realizacji *odnosi się do zadań zapewniających*	Liczba wdrożonych zaleceń *odnosi się do zadań zapewniających*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
1.	Czynności doradczych dot. procedur udzielania zamówień publicznych	Czynności doradcze	-	-	tak	zamówienia publiczne	w	nie	-	6	-	-	-
2.	Czynności doradcze dotyczące analizy postępowań administracyjnych zmierzających do wykonania: „Przedsięwzięcia polegającego na budowie elektrowni wiatrowych w Parsówku"	Czynności doradcze	-	-	nie	Gospodarka odpadami/ochrona środowiska/utrzymanie porządku i czystości oraz Inwestycje	p	nie	-	19	-	-	-
3.	Analiza wybranych zagadnień z kultury fizycznej	Czynności doradcze	-	-	nie	Młodzieżowy Ośrodek Sportowy/Sport i rekreacja	p	nie	-	3	-	-	-
4.	Ocena systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Gryfinie w zakresie realizacji zadań związanych z utrzymaniem porządku i	Zadanie zapewniające	Tak	-	nie	Gospodarka odpadami/ochrona środowiska/utrzymanie porządku i czystości Ochrona informacji/danych/bezpieczeństwo teleinformatyczne	p/w	nie	40	40	55	55	Czynności sprawdzające zaplanowano na 2016 rok

Lp.	Temat zadania zapewniającego albo przedmiot czynności doradczych	Zadanie zapewniające albo czynności doradcze *podać odpowiednio*	Zadanie zapewniające ujęte w planie audytu na rok sprawozdawczy *Tak/ Nie*	W przypadku audytu wewnętrznego zleconego wskazać podmiot zlecający audyt	Obszar działalności związany z dysponowaniem środkami europejskimi, o których mowa w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych[4] /tak/nie/ *tak/nie*	Obszar ryzyka, w którym przeprowadzono zadanie audytowe *wskazać odpowiedni obszar*	Typ obszaru działalności *wpisać odpowiednio: „p" dla działalności podstawowej albo „w" dla działalności wspomagającej*	Powołanie rzeczoznawcy *tak/nie*	Liczba osobodni planowanych na przeprowadzenie zadania zapewniającego *(w przypadku zadań zrealizowanych poza planem wpisać „-"/*	Liczba osobodni wykorzystanych na przeprowadzenie zadania zapewniającego albo wykonanie czynności doradczych	Liczba zaleceń zawartych w sprawozdaniu *odnosi się do zadań zapewniających*	Liczba zaleceń zaakceptowanych do realizacji *odnosi się do zadań zapewniających*	Liczba wdrożonych zaleceń *odnosi się do zadań zapewniających*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
	czystości												
5.	Uwagi do przebudowy strony internetowej Gminy Gryfino	Czynności doradcze	-	-	nie	Polityka informacyjna/Udostępnianie informacji publicznej	w	nie	-	3	-	-	-
6.	Skuteczność systemu rozpatrywania skarg i wniosków obywateli	Zadanie zapewniające	Tak	-	nie	Skargi i wnioski	p	nie	40	46	24	24	Czynności sprawdzające zaplanowano na 2016 rok

Wskazanie przyczyn(y) zaistnienia ewentualnych znaczących odstępstw od realizacji planu audytu *(w tym przyczyny odstąpienia od przeprowadzenia zadania audytowego np. przeprowadzenie niemożliwe albo niecelowe, wystąpienie nowego ryzyka, zmiana oceny ryzyka, inne)*

Audyt wewnętrzny realizował swoje zadania od marca 2015 r. w oparciu o Plan Audytu Wewnętrznego z dnia 30 marca 2015 r. oraz uzasadnioną zmianą ww. dokumentu z dnia 17 sierpnia 2015 r.

4. Przeprowadzone czynności sprawdzające w roku sprawozdawczym

Lp.	Temat zadania zapewniającego, którego dotyczą czynności sprawdzające	Liczba osobodni planowanych na przeprowadzenie czynności sprawdzających	Liczba osobodni wykorzystanych na przeprowadzenie czynności sprawdzających	Liczba zaleceń zawartych w sprawozdaniu *odnosi się do zadań zapewniających*	Liczba zaleceń zaakceptowanych do realizacji *odnosi się do zadań zapewniających*	Liczba wdrożonych zaleceń *odnosi się do zadań zapewniających*

1	2	3	4	5	6	7
1.	System zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Gryfinie	6	6	81	81	47 zaleceń wdrożonych; 18 zaleceń – zrealizowane częściowo (podjęte działania wymagają uzupełnienia); 16 zaleceń nie zrealizowano
2.	Zasady tworzenia i modyfikacji planów zagospodarowania przestrzennego w odniesieniu do potrzeb społeczności lokalnej	6	7	41	41	33 zaleceń wdrożonych;; 5 zaleceń – zrealizowane częściowo (podjęte działania wymagają uzupełnienia); 3 zaleceń nie zrealizowano. Wszystkie zalecenia zostały uzupełnione lub zrealizowane w terminie późniejszym – monitoring wykonany w ramach weryfikacji dalszych działań w ramach czynności audytora w systemie zarządzania jakością ISO 9001.

Wskazanie przyczyn(y) zaistnienia ewentualnych znaczących odstępstw od realizacji planu audytu:

---

5. Omówienie zidentyfikowanych istotnych ryzyk i słabości kontroli zarządczej

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
1.	Czynności doradczych dot. procedur udzielania zamówień publicznych	Czynności doradcze	- niezgodności niektórych projektowanych mechanizmów kontrolnych projektu zarządzenia Burmistrza Miasta i Gminy Gryfino w sprawie *Zasad wykonywania w Urzędzie Miasta i Gminy w Gryfinie oraz innych jednostkach organizacyjnych Gminy Gryfino ustawy PZP oraz Regulaminu pracy komisji przetargowej Urzędu Miasta i Gminy w Gryfinie.* Zalecono doprowadzenie do zgodności treści projektowanego zarządzenia z brzmieniem przepisów o zamówieniach publicznych w szczególności w zakresie regulacji zawartych w ustawie Prawo zamówień publicznych w zakresie określania wartości, od których uzależnione jest stosowanie przepisów ustawy oraz wykonywania czynności technicznych i pomocniczych: a) prowadzenia rejestrów zamówień publicznych,	- niezgodność projektowanej regulacji dotyczącej systemu udzielania zamówień publicznych w Urzędzie Miasta i Gminy w Gryfinie z przepisami prawa powszechnie obowiązującego; - ryzyko nieprawidłowego wykonywania czynności w postępowaniu o udzielenie zamówienia publicznego; - ryzyko powielania nieścisłości zawartych w projektowanym zarządzeniu przez pracowników Urzędu Miasta i Gminy w Gryfinie

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			b) tworzenia *Planu zamówień publicznych,* c) sporządzania *Informacji o zamówieniu publicznym.* ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.13. Ochrona zasobów***	
2.	Czynności doradcze dotyczące analizy postępowań administracyjnych zmierzających do wykonania: „Przedsięwzięcia polegającego na budowie elektrowni wiatrowych w Parsówku"	Czynności doradcze	- niespójności w dokumentacji przedkładanej przez Inwestorów do kompetentnych organów; - istotne braki w zakresie komunikacji wewnętrznej pomiędzy w komórkami organizacyjnymi w Urzędzie Miasta i Gminy w Gryfinie, które realizują odrębne, merytoryczne czynności w toku obsługi procesu inwestycyjnego konkretnego projektu Konieczność wzmocnienia efektywnego systemu komunikacji wewnętrznej w Urzędzie Miasta i Gminy w Gryfinie (w kierunku pionowym i poziomym) w zakresie obsługi procesu inwestycyjnego jako całości realizowanego projektu. Konieczność weryfikacji treści raportu o oddziaływaniu przedsięwzięcia na środowisko, przez organy biorące udział w procedurze oddziaływania w oceny oddziaływania na środowisko planowanych przedsięwzięć. ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.13. Ochrona zasobów*** ***Nr D.16 Bieżąca komunikacja*** ***Nr D.17. Komunikacja wewnętrzna***	- ryzyko wystąpienia istotnych nieprawidłowości w zakresie obsługi procesu inwestycyjnego; - istotne braki w ustanowieniu efektywnego systemu komunikacji wewnętrznej w Urzędzie Miasta i Gminy w Gryfinie (przepływ informacji w kierunku pionowym i poziomym)
3.	Analiza wybranych zagadnień z kultury fizycznej	Czynności doradcze	- niespójności w dokumentacji; ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.13. Ochrona zasobów*** Zalecono dokonywane weryfikacji projektów planów finansowych jednostek organizacyjnych Gminy Gryfino, na etapie planowania budżetowego, ze szczególnym uwzględnieniem poprawności i transparentności przepływów finansowych pomiędzy jednostkami organizacyjnymi Gminy Gryfino. Ponadto precyzyjne określanie poszczególnych jednostek lub organizacji, na rzecz których wydatkuje się środki finansowe. W celu zapewnienia poprawności oraz wyeliminowania potencjalnych nieprawidłowości w składanych przez organizacje pozarządowe sprawozdaniach z realizacji zadań publicznych (finansowanych z dotacji) zaproponowano, by wesprzeć ww. organizacje poprzez przekazywanie wniosków wynikających z analizy przedkładanych rozliczeń środków finansowych oraz akcentowania istotnych zmian w przepisach prawa (np. podczas cyklicznych spotkań z	- ryzyko dokonywania transferu środków finansowych na zadania realizowane przez organizacje pozarządowe za pośrednictwem jednostek organizacyjnych Gminy Gryfino – potencjalny brak ich ujęcia w planie dotacji, stanowiącym załącznik do budżetu Gminy Gryfino; - ryzyko wystąpienia nieprawidłowości przy rozliczaniu środków z udzielonych dotacji

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			organizacjami pozarządowymi).	
4.	Ocena systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy w Gryfinie w zakresie realizacji zadań związanych z utrzymaniem porządku i czystości	Zadanie zapewniające	- niekompletność dokumentacji wewnętrznej systemu bezpieczeństwa informacji w szczególności w zakresie: procedur tworzenia kopii zapasowych zbiorów danych przetwarzanych w niektórych systemach; - brak rozdzielenia pełnienia funkcji Administratora Bezpieczeństwa Informacji (ABI) oraz Administratora Systemów Informatycznych (ASI); istotna słabość konstrukcji systemu bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Gryfinie z uwzględnieniem wyznaczenia konkretnych osób do pełnienia funkcji ABI i Pełnomocnika Ochrony Danych Osobowych oraz ASI w opinii audytora wewnętrznego nie jest poprawna ze względu na wzajemne powiązania oraz podległości pomiędzy osobami wyznaczonymi do pełnienia ww. funkcji oraz wykonywanymi czynnościami; ***Luki w standardach kontroli zarządczej:*** ***Nr A.3. Struktura organizacyjna*** ***Nr C.14. Szczegółowe mechanizmy kontroli – podział obowiązków*** Zalecono w szczególności: - podział obowiązków dla zachowania bezpieczeństwa i unikania konfliktu interesów oraz nadzorowania samego siebie (w szczególności w przypadku funkcji ABI) lub w sytuacji, gdy, z uzasadnionych przyczyn, pewnych funkcji nie można przydzielić różnym osobom – nie można rozdzielić konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych o charakterze kompensującym (nadzór). - brak aktualizacji właścicieli aktywów w postaci sprzętu informatycznego; - brak wdrożenia i wykorzystywania posiadanych narzędzi informatycznych służących utrzymywaniu aktualności inwentaryzacji sprzętu i oprogramowania do przetwarzania informacji obejmującej ich rodzaj i konfigurację; - brak prowadzenia rejestru zbiorów, o których mowa w art. 36a ust. 2 pkt 2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; - brak określania nazw zbiorów danych osobowych powierzanych do przetwarzania podmiotom zewnętrznym oraz rozbieżności zakresu powierzanych do przetwarzania w zbiorze danych osobowych w porównaniu ze wskazanymi we wnioskach rejestracyjnych przekazanych do GIODO. ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr C.13. Ochrona zasobów*** Zalecono w szczególności: - prowadzenie bieżącej aktualizacji właścicieli aktywów; - zapewnienie prowadzenia rejestru zbiorów, o których mowa w art. 36a ust. 2	- niska efektywność kontroli zarządczej w zakresie mechanizmów kontroli związanych z podziałem kluczowych obowiązków; - ryzyko niepoprawności w rzeczywistym funkcjonowaniu i wykonywaniu sprawowanej kontroli; - potencjalne ryzyko instalowania i użytkowania sprzętu i oprogramowania stanowiącego zagrożenie dla bezpieczeństwa informacji; - niejasności w powierzaniu przetwarzania danych osobowych podmiotom zewnętrznym;

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			pkt 2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; - nie przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy; - przyjęcie i zastosowanie środków organizacyjnych i technicznych niezgodnych z wymaganiami wskazanymi w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zalecono wdrożenie i zapewnienie przeprowadzania okresowych analiz ryzyka ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, ze szczególnym uwzględnieniem analizy ryzyka dla infrastruktury informatycznej ***Luki w standardach kontroli zarządczej:*** ***Nr B Cele i zarządzanie ryzykiem*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr C.13. Ochrona zasobów***	- brak funkcjonowania formalnego, udokumentowanego procesu zarządzania ryzykiem
			- brak prowadzenia bieżącej ewidencji osób upoważnionych do przetwarzania danych osobowych; - nadawanie uprawnień do pracy w systemach informatycznych z pominięciem formalnego procesu autoryzacji; - nieprzestrzeganie zasad użytkowania poufnych informacji uwierzytelniających; - brak kompleksowego podejścia do zarządzania infrastruktura informatyczną zapewniającą ochronę przetwarzanych danych; - brak ustanowienia formalnego nadzoru nad procesami zewnętrznymi; - luki w określaniu trybu dostępu do zasobów własnych w umowach zawieranych z podmiotami zewnętrznymi; - nieścisłości w zakresie wskazania osób odpowiedzialnych za ochronę elementów infrastruktury informatycznej; - luki w zakresie realizacji procedur związanych z fizycznym dostępem do chronionych zasobów informacyjnych; - brak zapewnienia środków bezpieczeństwa na wymaganym poziomie w jednym z systemów informatycznych wykorzystywanych do przetwarzania danych osobowych; - brak zobligowania użytkowników do informowania o zdarzeniach, incydentach nie związanych z przetwarzaniem danych osobowych oraz dotyczącego zbiorów danych przetwarzanych w sposób tradycyjny tj. papierowo;	- ryzyko prawne – niespełnienie wymagań wskazanych w przepisach prawa powszechnie obowiązujących; - istotne osłabienie systemu kontroli; - ryzyko konieczności działania „ad hoc" wobec zmaterializowania się konkretnego ryzyka; - ryzyko udostępnienia informacji osobom nieupoważnionym wobec braku możliwości sprawowania bezpośredniej kontroli w zakresie działań (wykonywania czynności na bazach danych) użytkowników zewnętrznych; - brak funkcjonowania systemu bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony z góry ustalony sposób umożliwiający niezwłoczne podjecie działań korygujących; - zmniejszona ochrona przed uszkodzeniem lub zakłóceniami w sytuacji stwierdzenia nieścisłości w zakresie wykonywania i przechowywania kopii zapasowych systemów informatycznych – ryzyko niezapełnienia ciągłości pracy systemu informatycznego;

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			- brak prowadzenia rejestru incydentów, zdarzeń itp. – ograniczenie możliwości „uczenia się" organizacji; - nieścisłości w zakresie wykonywania i przechowywania kopii zapasowych systemów informatycznych; ***Luki w standardach kontroli zarządczej:*** ***Nr A Środowisko wewnętrzne*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr C.13. Ochrona zasobów*** ***Nr C.15 Mechanizmy kontroli dotyczące systemów informatycznych*** Zalecono w szczególności: - wskazanie użytkowników uprzywilejowanych do poszczególnych systemów informatycznych; - wzmocnienie świadomość pracowników w zakresie naruszeń bezpieczeństwa informacji; - nadawanie uprawnień do pracy w systemach informatycznych dla osób z zewnątrz lub pełniących funkcję ASI winno podlegać szczególnemu nadzorowi – i odbywać się zgodnie z procedurą wskazaną dla użytkowników systemów; - uzupełnienie dokumentacji wewnętrznej wykorzystywanej przy nadawaniu uprawnień do pracy w systemach informatycznych; - opracowanie dokumentu identyfikującego potrzeby informatyczne opartego na analizie procesów zachodzących w Urzędzie Miasta i Gminy w Gryfinie – zbudowanie „strategii rozwoju infrastruktury informatycznej". Powyższe przyczyni się do zapewnienia przez Kierownictwo Urzędu Miasta i Gminy w Gryfinie warunków umożliwiających realizację i egzekwowanie zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami co w połączeniu z procesem budżetowania i zarządzania ryzykiem stworzy narzędzie wspierające zarządzanie infrastrukturą informatyczną w dłuższym okresie czasu; - ustanowienie formalnego nadzoru nad zasobami informacyjnymi i informatycznymi: wskazywanie, w umowach serwisowych, osób uprawnionych do zasobów i wykonujących czynności w systemach informatycznych (na zasobach); - zmiana rozwiązań organizacyjnych w zakresie dostępu podmiotów zewnętrznych do zasobów własnych; - uzupełnienie procedur wewnętrznych o korzystanie z dostępu do dedykowanych systemów informatycznych spoza budynku Urzędu Miasta i Gminy w Gryfinie; - bezpośrednie i precyzyjne wskazywanie osób odpowiedzialnych realizację poszczególnych zadań wykonywanych w systemie bezpieczeństwa informacji; - zapewnić realizację wykonywania kontroli przez ABI, związaną w szczególności z funkcjonowaniem zabezpieczeń systemów, w których przetwarzane są dane osobowe oraz przedkładanie informacji o jej wynikach ADO, w tym Burmistrzowi Miasta i Gminy Gryfino;	

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			- ustanowienie zarządzania i formalnego nadzoru nad kluczami do istotnych pomieszczeń infrastruktury informatycznej Urzędu Miasta i Gminy w Gryfinie; - założenie i prowadzenie rejestru zdarzeń, incydentów, itp. związanych z przetwarzaniem danych osobowych przetwarzanych w sposób tradycyjny i w systemach informatycznych oraz w systemach informatycznych nie zawierających danych osobowych. Należy wskazać osoby odpowiedzialne za jego bieżące prowadzenie; - zapewnienie nadzoru nad działaniami sprawdzającymi, korygującymi i zapobiegawczymi wykonywanymi w ramach postępowania ze zgłoszeniami incydentów, zdarzeń, naruszeń, niedostatecznie zabezpieczonych punktów systemu; - zgłoszenie do Pełnomocnika ds. Zarządzania Jakością w Urzędzie Miasta i Gminy w Gryfinie i wykorzystanie wskaźników systemu bezpieczeństwa informacji np. w zakresie skuteczności zarządzania incydentami – jako narzędzia monitorowania systemu bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Gryfinie w ramach funkcjonującego systemu ISO 9001;	
			- brak dokonania analizy spełniania przez systemy informatyczne wymogu wskazanego w § 21 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w zakresie rozliczalności w systemach teleinformatycznych – wiarygodne dokumentowanie w postaci elektronicznych zapisów w dziennikach systemów (logach); - ustalony stan faktyczny uniemożliwiający jednoznaczną rozliczalność działań wykonywanych w systemach informatycznych, w odniesieniu m.in. do użytkowników uprzywilejowanych; ***Luki w standardach kontroli zarządczej:*** ***Nr A Środowisko wewnętrzne*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr C.13. Ochrona zasobów*** ***Nr C.15 Mechanizmy kontroli dotyczące systemów informatycznych*** Zalecono w szczególności: - należy zapewnić jednoznaczną identyfikację informacji o założeniu lub zablokowaniu konta użytkownika w systemie *e-SOD* pozwalającą na bezpośrednią identyfikację użytkownika (którego dotyczy czynność założenia/blokowania uprawnień); - dokonanie analizy spełniania warunku rozliczalności w zakresie wymogów wskazanych w § 21 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych dla	- ryzyko wystąpienia zjawiska nadmiarowości uprawnień koniecznych do wykonania czynności;

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			systemu informatycznego ODPADY. Powyższe należy wykonać w we współpracy z podmiotem serwisującym system informatyczny; - należy zapewnić spełnianie przez systemy informatyczne wymagań wskazanych w § 21 ust. 4 i 5 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; - należy wprowadzić obowiązek przeglądu logów systemów przez ASI w celu bieżącej weryfikacji poprawności i stabilności funkcjonowania ww. systemów informatycznych w celu nadzoru i wzmocnienia zabezpieczenia przed brakiem dostępności bądź wystąpieniem błędów w systemach; - należy wskazać w dokumentacji wewnętrznej okres przechowywania logów systemowych (dostępności logów) – określić czas retencji (przechowywania).	
5.	Uwagi do przebudowy strony internetowej Gminy Gryfino	Czynności doradcze	- niedostosowanie strony internetowej www.gryfino.pl do potrzeb osób z dysfunkcjami słuchu, mowy – brak spełniania standardów dostępności dla osób niepełnosprawnych wskazanych w § 19 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 (Dz. U. poz. 526 ze zm.); - brak umieszczenia na stronie internetowej informacji wymaganych przepisami ustawy o języku migowym; ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr D.18. Komunikacja zewnętrzna*** W ramach usprawnienia wskazano m.in.: - ze względu na dynamiczny rozwój informatyzacji administracji wskazano na konieczność dostosowania strony internetowej www.gryfino.pl. W opinii audytu odpowiednia prezentacja informacji umożliwi kształtowanie korzystnych zmian w zakresie samodzielnego funkcjonowania osób z różnym rodzajem i stopniem niepełnosprawności – mieszkańców wspólnoty samorządowej Gminy Gryfino – w przestrzeni publicznej; - umieszczenie na stronie internetowej informacji wymaganych przepisami ustawy o języku migowym, w tym dla osób mających trwałe lub okresowe trudności w komunikowaniu się i wymagające w związku z tym wsparcia w kontaktach z organami administracji publicznej oraz niepełnosprawnych ruchowo (w zakresie ułatwień dostępu do obiektów użyteczności publicznej jak i usuwania barier). - wobec dynamicznie rozwijającego się projektu Ministerstwa Administracji i Cyfryzacji pn. Regionalny System Ostrzegania (RSO) oraz faktu, że komunikaty (ostrzeżenia) generowane są przez Wojewódzkie Centrum Zarządzania Kryzysowego na stronie internetowej urzędu wojewódzkiego zaproponowano umieszczenie na stronie linku do odpowiedniej strony internetowej	- niespełnienie wymagań stawianych w aktach prawa powszechnie obowiązującego; - niepełne wykorzystanie możliwości technicznych w zakresie usprawnienia komunikacji zewnętrznej z mieszkańcami; - niepełne wykorzystanie możliwości technicznych w zakresie usprawnienia realizacji zadań

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			Zachodniopomorskiego Urzędu Wojewódzkiego. Powyższe może zapewnić mieszkańcom Gminy Gryfino oraz potencjalnym odwiedzającym szerokie źródło informacji w zakresie m.in. informacji drogowych (w tym drogi wojewódzkie), meteorologicznych, hydrologicznych, promieniowania, przerw w zasilaniu (dostawy różnych operatorów) i in. - wykorzystanie dostępnych narzędzi w ramach zintegrowanych systemów informatycznych w Urzędzie Miasta i Gminy w Gryfinie i umieszczenie na na stronie internetowej narzędzia powiązanego z modułem płatności Krajowej Izby Rozliczeniowej. Powyższe może stanowić ułatwienie i usprawnienie dla pracy Urzędu w zakresie realizacji zadań, a dla mieszkańców Gminy w zakresie wywiązywania się z obowiązków, związanych w szczególności z odpowiednio poborem i wnoszeniem podatków i opłat.	
6.	Skuteczność systemu rozpatrywania skarg i wniosków obywateli	Zadanie zapewniające	- luki oraz niespójności w regulacjach wewnętrznych dotyczących skarg i wniosków; - niezgodne z przepisami prawa powszechnie obowiązującego funkcjonowanie systemu przyjmowania skarg i wniosków przez Radę Miejską w Gryfinie; - brak wyraźnego wskazywania informacji dotyczących przyjmowania skarg i wniosków obywateli przez poszczególne organy Gminy Gryfino: Burmistrza Miasta i Gminy Gryfino oraz Radę Miejską w Gryfinie (w szczególności: na stronie internetowej, stronie podmiotowej BIP, tablicach ogłoszeń w siedzibie jednostki samorządu terytorialnego, w jednostkach organizacyjnych Gminy Gryfino); ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr D.17. Komunikacja wewnętrzna*** ***Nr D.18. Komunikacja zewnętrzna*** Zalecono w szczególności: - przyjąć rozwiązania organizacyjne pozwalające na skuteczne wypełnienie obowiązku nałożonego na organ stanowiący Gminy Gryfino – Radę Miejską w Gryfinie, a wskazany w art. 253 § 2 – 3 Kpa – w zakresie przyjmowania obywateli w sprawach skarg i wniosków. W przyjętych regulacjach należy uwzględnić rozwiązanie organizacyjne pozwalające na zapewnienie realizacji przyjęć obywateli w sytuacji, gdy wyznaczony dzień jest dniem wolnym od pracy; - zapewnić, by informacje związane z przyjmowaniem obywateli w sprawach skarg i wniosków przez organy Gminy Gryfino, umieszczane i publikowane na różnych nośnikach (np. główna strona podmiotowa BIP, tablice ogłoszeniowe – tak w siedzibie Urzędu Miasta i Gminy w Gryfinie jak i poza nią) miały spójne i jednolite treści oraz wyraźnie wskazywały na poszczególne organy Gminy Gryfino - brak zapewnienia formalnej obsługi organizacyjno – technicznej przyjęć obywateli	- ryzyko braku dokumentowania ewentualnych skarg i wniosków składanych ustnie, co może rodzić problemy w zakresie weryfikacji ich rozpatrywania i załatwiania. Powyższe może rzutować na rzetelność statystycznych informacji przekazywanych do Urzędu Wojewódzkiego w ramach raportowania o działalności organów Gminy Gryfino - niekompletność rozwiązań organizacyjnych w zakresie przyjmowania

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Omówienie zidentyfikowanych istotnych ryzyk i słabości systemu kontroli zarządczej	Ryzyka, do których odnoszą się wydane zalecenia lub opinie i wnioski
1	2	3	4	5
			w sprawie skarg i wniosków – co skutkuje brakiem pełnych informacji w zakresie ewentualnych skarg i wniosków składanych w trakcie przyjmowania obywateli; - umieszczenie na stronie podmiotowej BIP informacji wymaganych przepisami ustawy o języku migowym, w tym dla osób mających trwałe lub okresowe trudności w komunikowaniu się i wymagające w związku z tym wsparcia w kontaktach z organami administracji publicznej oraz niepełnosprawnych ruchowo (w tym zakresie ułatwień dostępu do obiektów użyteczności publicznej jak i usuwania barier) - umieszczenie informacji ułatwiających złożenie skargi/wniosku ***Luki w standardach kontroli zarządczej:*** ***Nr A.3 Struktura organizacyjna;*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr C.11. Nadzór*** ***Nr D.18. Komunikacja zewnętrzna*** Zalecono w szczególności: - wskazanie wyodrębnionej komórki organizacyjne lub imiennie wyznaczonych pracowników, którym powierzono przyjmowanie i koordynowanie rozpatrywania skarg i wniosków składanych do poszczególnych organów Gminy Gryfino: Rady Miejskiej w Gryfinie oraz Burmistrza Miasta i Gminy Gryfino. Ponadto zgodnie z brzmieniem § 3 ust. 2 rozporządzenia w sprawie organizacji przyjmowania skarg i wniosków ww. informację należy umieścić w siedzibie danej jednostki organizacyjnej, w widocznym miejscu.	skarg i wniosków przez organy Gminy Gryfino; - niespełnienie wymagań stawianych w aktach prawa powszechnie obowiązującego; - niepełne wykorzystanie możliwości technicznych w zakresie usprawnienia komunikacji zewnętrznej z mieszkańcami;
			- brak możliwości wnoszenia petycji za pomocą e-PUAP; - niezgodność treści regulacji wewnętrznych z przepisami prawa powszechnie obowiązującego w zakresie możliwych sposobów wnoszenia petycji ***Luki w standardach kontroli zarządczej:*** ***Nr C.10. Dokumentowanie systemu kontroli zarządczej*** ***Nr D.18. Komunikacja zewnętrzna*** Zalecono w szczególności: - zapewnienie możliwości wnoszenia petycji w formie wskazanej w ustawie w szczególności za pomocą e-PUAP oraz dokonać uaktualnienia informacji wskazanych w na stronie e-PUAP w zakładce właściwej do wniesienia skarg/wniosków.	- ograniczenie możliwych, w skazanych przez przepisy prawa powszechnie obowiązującego sposobów wnoszenia petycji do organów państwowych

6. Niezrealizowane zaplanowane zadania

Lp.	Temat zadania zapewniającego lub przedmiot czynności doradczej	Zadanie zapewniające albo czynność doradcza /wskazać odpowiednio/	Przyczyna niezrealizowania zadania zapewniającego lub czynności doradczej
1.	2	3	4
1.	-	-	-

7. Inne istotne informacje związane z prowadzeniem audytu wewnętrznego w roku sprawozdawczym / w tym inne istotne informacje ustalone z w porozumieniu z kierownikiem jednostki/

1) Audyt wewnętrzny realizował swoje zadania od 2 marca 2015 r. w oparciu o Plan Audytu Wewnętrznego z dnia 30 marca 2015 r. oraz uzasadnioną zmianą ww. dokumentu z dnia 17 sierpnia 2015 r.

2) Audytor wewnętrzny dokonał analizy ogólnej oceny zgodności funkcji audytu wewnętrznego z „*Międzynarodowymi standardami praktyki zawodowej audytu wewnętrznego*" wg skali ocen zaproponowanej w publikacji Quality Assessment Manual – for the Internal Audit Activity 2013 wydana przez The IIA Research Foundation. Potwierdzono generalną zgodność audytu wewnętrznego z wymaganiami ww. dokumentu.

3) Działania audytu wewnętrznego podlegają integracji z funkcjonującymi systemami zarządzania w Urzędzie Miasta i Gminy w Gryfinie. W ramach monitorowania realizacji zaleceń w przypadku ich nie wdrożenia, po przeprowadzeniu czynności sprawdzających, dalsze działania podlegają weryfikacji w ramach funkcjonującego w Urzędzie Miasta i Gminy w Gryfinie systemu zarządzania jakością ISO 9001.

18.01.2016 r.
(data)

AUDYTOR WEWNĘTRZNY
mgr Anna Myśko
.....
(podpis i pieczęć audytora wewnętrznego/kierownika komórki audytu wewnętrznego)