Załącznik Nr 1
do Zarządzenia Nr 648/17
Burmistrza Brus z dnia 19 grudnia 2017 r.

Urząd Miejski w Brusach
ul. Na Zaborach
89-632 Brusy

SPRAWOZDANIE Z WYKONANIA PLANU AUDYTU WEWNĘTRZNEGO ZA ROK 2017

1. Jednostki sektora finansów publicznych objęte audytem wewnętrznym

Lp.	*Nazwa jednostki*
1	Urząd Miejski w Brusach
2	Przedszkole Nr 1 z Brusach
3	Szkoła Podstawowa Nr 2 w Brusach
4	Szkoła Podstawowa im. Jana Pawła II w Brusach
5	Szkoła Podstawowa w Czapiewicach
6	Szkoła Podstawowa im. Bł. Ks. Józefa Jankowskiego w Czyczkowach
7	Szkoła Podstawowa im. Kardynała Stefana Wyszyńskiego w Leśnie
8	Szkoła Podstawowa w Męcikale
9	Szkoła Podstawowa im. Księdza Kanonika Bolesława Śledzia w Kosobudach
10	Szkoła Podstawowa im. Stanisława Sikorskiego w Wielkich Chełmach
11	Szkoła Podstawowa w Zalesiu
12	Szkoła podstawowa im. Tajnej Organizacji „Gryf Pomorski" w Lubni
13	Centrum Kultury i Biblioteki im. Jana Karnowskiego w Brusach
14	Zakład Gospodarki Komunalnej
15	Gminny Zarząd Oświaty
16	Miejsko-Gminny Ośrodek Pomocy Społecznej

BURMISTRZ
dr inż. Witold Ossowski

2. Podstawowe informacje o komórce audytu wewnętrznego

Lp.	*Imię i nazwisko osób zatrudnionych w komórce audytu*	*Nazwa stanowiska*	*Numer telefonu*	*Adres poczty elektronicznej*	*Wymiar czasu pracy*	*Kwalifikacje zawodowe*
1	Beata Sarnowska – Gierszewska	Umowa zlecenie	---	---	Umowa zlecenie	(Zaświadczenie nr 2086/2006 Wydane przez Ministerstwo Finansów)

3. Przeprowadzone zadania audytowe w roku sprawozdawczym

Lp.	Temat zadania audytowego	Zadanie zapewniające (Z), czynność doradcza (D) czynności sprawdzające (S)	Audyt wewnętrzny zlecony)	Typ obszaru działalności *	Obszar działalności związany z dysponowaniem środkami, o których mowa w ustawie o finansach publicznych	Opis obszaru działalności wspomagającej**	Liczba audytorów wewnętrznych przeprowadzających audyt wewnętrzny		Czas przeprowadzenia zadania audytowego (w dniach)		Powołanie rzeczoznawcy
							Plan	Wykonanie	Plan	Wykonanie	
1	2	3	4	5	6	7	8	9	10	11	12
1	Realizacja zadań Pełnomocnika ds. Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii	(Z)	-	Działalność podstawowa	NIE	---	1	1	70	35	Nie
2	Realizacja zadań z zakresu udzielania zamówień publicznych przez jednostki organizacyjne podległe Gminie Brusy - Zakład Gospodarki Komunalnej w Brusach	(Z)	-	Działalność wspomagająca	NIE	Gospodarka finansowa/Zakupy/Zarządzanie	1	1	70	31	Nie
3	Bezpieczeństwo informacji	(Z)	-	Działalność wspomagająca	NIE	Bezpieczeństwo / Systemy informatyczne / Zarządzanie	1	1	35	31	Nie
4	Funkcjonowanie kontroli zarządczej w jednostkach organizacyjnych podległych Gminie Brusy	(D)	-	-	NIE	Zarządzanie	1	1	40	47	Nie

* działalność podstawowa obejmuje działalność merytoryczną, statutową, charakterystyczna dla danej jednostki. Działalność wspomagająca obejmuje ogólnie rozumiany proces zarządzania jednostką, zapewnia sprawność i skuteczność działań w obszarze działalności podstawowej, np. zamówienia publiczne, zarządzanie kadrami.

**należy wypełnić tylko w przypadku wskazanie w kolumnie 3 „działalność wspomagająca". Wówczas należy wybrać odpowiednio: „Gospodarka finansowa", albo „Zakupy", albo Zarządzanie mieniem", albo Bezpieczeństwo", albo „Systemy informatyczne", albo „Zarządzanie".

4. Informacje o zadaniach audytowych

Lp.	*Temat zadania zapewniającego lub przedmiot czynności doradczej* *(również te które nie były ujęte w planie)*	*Zadanie zapewniające (Z), czynność doradcza (D)*	*Efekt przeprowadzenia zadania audytowego****	*Podstawowe zalecenia lub opinie i wnioski*	*Zidentyfikowane ryzyka i słabości kontroli*
1	Realizacja zadań Pełnomocnika ds. Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii	(Z)	Wzrost efektywności i skuteczności działania	Zakres działalności, jaki poddany został audytowi wewnętrznemu to zagadnienia związane z realizacją zadań ukierunkowanych na profilaktykę wynikającą z przepisów ustaw: o przeciwdziałaniu alkoholizmowi i przeciwdziałaniu narkomanii. Jako główne obiekty audytu wyróżniono: 1) analizę struktury zatrudnienia i zadań realizowanych w zakresie tematyki zadania, 2) ocenę konstrukcji systemu pod względem struktury, skuteczności koordynacji oraz zgodności z przepisami prawa, 3) analizę funkcjonowania w audytowanej komórce organizacyjnej systemu kontroli zarządczej. Zasady i mechanizmy funkcjonowania poszczególnych procesów zostały przedstawione w postaci tabelarycznej. Na tej podstawie zidentyfikowano istniejące mechanizmy kontroli, które następnie poddane zostały analizie poprzez przeprowadzenie testów zgodności i testów rzeczywistych - aby sprawdzić czy mechanizmy te funkcjonują prawidłowo. Potwierdzenie zawartych ustaleń dokonano poprzez użycie niżej wymienionych technik: uzyskanie wyjaśnień i informacji, tabelaryczną analizę procesów, przeglądy, analizy, próbkowanie, potwierdzanie, przeglądy analityczne, sprawdzenie rzetelności informacji przez porównanie ich z informacją pochodzącą z innego źródła. Czynnikami ryzyka, które w szczególności trzeba mieć na uwadze, są: 1) nieskuteczny podział zadań i kompetencji, 2) niezgodne (nieaktualne) z obowiązującymi przepisami określenie obowiązków w wewnętrznych uregulowaniach, 3) brak i/lub nieskuteczne realizowanie wewnętrznych procedur, 4) brak lub nieskuteczna kontrola wewnętrzna, 5) niezgodne z obowiązującymi przepisami wykonywanie obowiązków, 6) brak procedur bezpieczeństwa bądź ich lekceważenie, 7) nadinterpretacja lub błędna interpretacja przepisów,	

				8) słabe planowanie, 9) niefachowo sporządzane dokumenty, 10) zapisy nieodpowiednio chroniące interesy Gminy, 11) brak określenia kluczowych funkcji wykonywanych przez komórkę organizacyjną Urzędu. W Urzędzie Miejskim w Brusach powołano stanowisko Pełnomocnika ds. Rozwiązywania Problemów oraz Przeciwdziałania Narkomanii. W dniu 1 października 2013 r. wydane zostało Zarządzenie Nr 474/13 Burmistrza Brus w sprawie Regulaminu Organizacyjnego Urzędu Miejskiego w Brusach. Regulamin określa organizację i zasady funkcjonowania Urzędu. Zarządzenie było 4-krotnie zmieniane, jednakże zmiany nie wpłynęły na zapisy dotyczące analizowanego stanowiska. W § 35 Regulaminu Organizacyjnego zawarte zostały zadania Pełnomocnika ds. Rozwiązywania Problemów oraz Przeciwdziałania Narkomanii. Zadania Pełnomocnika zostały podzielne na 3 grupy: 1) zadania wynikające z ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, 2) zadania wynikające z ustawy o przeciwdziałaniu narkomanii, 3) zadania wynikające z ustawy o przeciwdziałaniu przemocy w rodzinie. Do zadań wynikających z ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi należy: 1) opracowywanie Gminnego Programu Profilaktyki i Rozwiazywania Problemów Alkoholowych, 2) koordynowanie zadań realizowanych przez jednostki organizacyjne Gminy w ramach Gminnego Programu Profilaktyki i Rozwiazywania Problemów Alkoholowych, 3) diagnoza problemów związanych z alkoholizmem i ryzykownym spożywaniem napojów alkoholowych 4) organizowane pomocy psychospołecznej i prawnej rodzinom, w których występuje problem alkoholowy, 5) współpraca z przedszkolami, szkołami podstawowymi, gimnazjami i szkołami ponadgimnazjalnymi w zakresie organizacji działalności profilaktycznej w zakresie przeciwdziałania alkoholizmowi, 6) organizowanie profilaktycznej działalności informacyjnej i edukacyjnej dla mieszkańców Gminy, 7) wspomaganie działalności instytucji, stowarzyszeń i osób fizycznych służącej rozwiązywaniu problemów alkoholowych,

				8) organizowanie szkoleń oraz zwiększanie dostępności do informacji o zagrożeniach wynikających z używania alkoholu, 9) współpraca z Gminną Komisją Rozwiązywania Problemów Alkoholowych, 10) współpraca z instytucjami realizującymi zadania wynikające z ustaw dotykających problemu używania alkoholu: Państwową Agencją Rozwiązywania Problemów Alkoholowych, Urzędem Marszałkowskim Województwa Pomorskiego, MOPS, Posterunkiem Policji itp., 11) realizacja i wprowadzenie nowych zadań zgodnych z rekomendacjami Państwowej Agencji Rozwiązywania Problemów Alkoholowych. Do zadań wynikających z ustawy o przeciwdziałaniu narkomanii należy: 1) opracowanie Gminnego Programu Przeciwdziałania Narkomanii, 2) koordynowanie zadań realizowanych przez jednostki organizacje Gminy w ramach Gminnego Programu Przeciwdziałania Narkomanii, 3) diagnoza problemów związanych z narkomanią, 4) organizowanie pomocy psychospołecznej i prawnej rodzinom, w których występują problemy związane z substancjami psychoaktywnymi, 5) współpraca z przedszkolami, szkołami podstawowymi, gimnazjami i szkołami ponadgimnazjalnymi w zakresie organizacji działalności profilaktycznej w zakresie narkomanii, 6) organizowanie profilaktycznej działalności informacyjnej i edukacyjnej dla mieszkańców Gminy, 7) wspomaganie działalności instytucji, stowarzyszeń i osób fizycznych służącej rozwiązywaniu problemów wynikających z nadużywania narkotyków, 8) organizowanie szkoleń oraz zwiększanie dostępności do informacji o zagrożeniach wynikających z używania narkotyków, 9) współpraca z instytucjami realizującymi zadania wynikające z w/w ustawy, np.: Krajowym Biurem ds. Przeciwdziałania Narkomanii, Urzędem Marszałkowskim Województwa Pomorskiego, MOPS, Posterunkiem Policji itp., 10) organizowanie i koordynowanie działań wychowawczych, edukacyjnych, informacyjnych i zapobiegawczych dla mieszkańców Gminy określonych w Krajowym Programie Przeciwdziałania Narkomanii. Do zadań wynikających z ustawy o przeciwdziałaniu przemocy w rodzinie należy: 1) tworzenie systemu przeciwdziałania przemocy w rodzinie oraz planowanie i realizacja zadań w ramach Gminnego Programu Profilaktyki

				i Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii, 2) organizowanie poradnictwa w zakresie przeciwdziałania przemocy w rodzinie, 3) organizowanie szkoleń dla realizatorów zadań wynikających z ustawy np. pracowników służby zdrowia, nauczycieli, 4) organizowanie profilaktycznej działalności informacyjnej i edukacyjnej dla mieszkańców Gminy, 5) współpraca z instytucjami realizującymi zdania wynikające z w/w ustawy np. Państwową Agencją Rozwiązywania Problemów Alkoholowych, Ogólnopolskim Porozumieniem Niebieska Linia, Ośrodkiem Terapii Uzależnień, MOPS, Posterunkiem Policji, PCPR, itp., 6) wykonywanie innych zadań zleconych przez Burmistrza. Szczególną uwagę zwrócić należy na funkcjonujący w Gminie Punkt Konsultacyjny, zapewniający dostępność pomocy terapeutycznej dla osób uzależnionych od alkoholu. Udzielana jest także pomoc – psychologiczna i prawna - rodzinom, w których występują problemy alkoholowe. Na terenie Gminy organizowany jest szereg imprez, w szczególności dla dzieci i młodzieży, dotyczących profilaktycznej działalności informacyjnej i edukacyjnej w zakresie rozwiązywania problemów alkoholowych i przeciwdziałania narkomanii, w tym prowadzenie pozalekcyjnych zajęć sportowych, a także działań na rzecz dożywiania dzieci uczestniczących w pozalekcyjnych programach opiekuńczo-wychowawczych i socjoterapeutycznych. Ze środków Gminy wspomagane są także inne instytucje, stowarzyszenia i osoby fizyczne, których działalność służy rozwiązywaniu problemów alkoholowych. W analizowanym okresie nie wystąpiły przypadki, konieczności podejmowania interwencji w związku z naruszeniem przepisów określonych w art. 13^1 i 15 ustawy oraz występowanie przed sądem w charakterze oskarżyciela publicznego. Na terenie Gminy nie powołano centrum integracji społecznej. Wszelkie zadania w opisywanym zakresie realizowane są przez Punkt Konsultacyjny. Analizując zagadnienia audytu wskazać należy zapisy Strategii Rozwoju Miasta i Gminy Brusy do roku 2020. Na uwagę zasługują także zapisy Strategii rozwiązywania problemów społecznych Gminy Brusy na lata 2015 – 2020.

				Rada Miejska w Brusach, Uchwałą Nr 111-26/03 z dnia 26 marca 2003 roku ustaliła zasady usytuowania oraz liczbę punktów sprzedaży napojów alkoholowych zawierających powyżej 4,5% alkoholu. Dodatkowo Uchwałą Nr XVIII/180/05 Rady Miejskiej w Brusach z dnia 27 maja 2005 roku wprowadziła zakaz spożywania napojów alkoholowych w wyznaczonych miejscach na terenie miasta i gminy Brusy. W dniu 30 marca 2011 r. wydane zostało Zarządzenie Nr 51/11 Burmistrza Brus w sprawie powołania Gminnej Komisji Rozwiązywania Problemów Alkoholowych. Kompetencje oraz zasady pracy komisji określa Regulamin Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Brusach, przyjęty Zarządzeniem Burmistrza Brus Nr 309/2009 z dnia 6 kwietnia 2009 r. Istotne znaczenie w ramach omawiania niniejszego Obiektu zadania audytowego ma Uchwała Nr VIII/69/15 Rady Miejskiej w Brusach z dnia 4 grudnia 2015 r. w sprawie przyjęcia Gminnego Programu Profilaktyki i Rozwiązywania Problemów Alkoholowych oraz Przeciwdziałania Narkomanii na 2016 rok. Uchwała w sprawie uchwalenia Gminnego Programu Profilaktyki i Rozwiązywania Problemów Alkoholowych oraz Przeciwdziałania Narkomanii na 2016 rok przedstawia katalog zadań do realizacji w zakresie przeciwdziałania alkoholizmowi oraz narkomanii na terenie miasta i gminy Brusy, oraz podziału środków planowanych na finansowanie tych zadań. W sprawozdaniu z realizacji audytu szczegółowo zaprezentowano analizę poszczególnych zadań w/w Programu. Jako zadania wyróżniono: 1) Zwiększenie dostępności pomocy terapeutycznej i rehabilitacyjnej dla osób uzależnionych i współuzależnionych od alkoholu; udzielanie rodzinom, w których występują problemy alkoholowe, pomocy psychospołecznej i prawnej - a w szczególności ochrony przed przemocą w rodzinie. 2) Prowadzenie profilaktycznej działalności informacyjnej i edukacyjnej w zakresie rozwiązywania problemów alkoholowych dzieci i młodzieży. 3) Kontynuowanie prac Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Brusach. 4) Zwiększanie dostępności pomocy terapeutycznej i rehabilitacyjnej dla osób uzależnionych i zagrożonych uzależnieniem, w tym udzielanie pomocy psychospołecznej i prawnej rodzinom, w których występują

				problemy narkomanii. 5) Prowadzenie profilaktycznej działalności informacyjnej, edukacyjnej i szkoleniowej w zakresie rozwiązywania problemów narkomanii, ze szczególnym uwzględnieniem dzieci i młodzieży. 6) Wspomaganie działalności instytucji, organizacji pozarządowych i osób fizycznych, służącej rozwiązywaniu problemów narkomanii. W trakcie realizacji audytu dokonano weryfikacji działań w celu potwierdzenia efektywności wdrożonych systemów zarządzania i kontroli. Przeprowadzony audyt systemów zarządzania i kontroli skierowany był głównie na określenie, czy systemy działają efektywnie w celu zapobiegania nieprawidłowościom oraz czy tam gdzie mogą pojawić się ewentualne błędy i nieprawidłowości, systemy efektywnie wykryją je i skorygują. W trakcie realizacji zadania dokonano korekty Sprawozdania z realizacji Gminnego Programu Rozwiązywania problemów Alkoholowych. Ocena konstrukcji mechanizmów kontroli i systemu kontroli polegała na identyfikacji celów, analizie konkretnych ryzyk, identyfikacji kluczowych kontroli, ocenie atutów i słabości kontroli oraz dokonaniu oceny systemu kontroli. Przedstawiona w niniejszym sprawozdaniu opinia audytora jest rezultatem zebranych dowodów oraz własnego osądu. Opiera się o procedury audytowe oraz ustalone fakty i ma na celu poszukiwanie możliwości ewentualnych usprawnień. Wśród zaleceń wskazano: 1) Podjąć działania mające na celu egzekwowanie, od podmiotów, którym udzielono dotacji, składania sprawozdań z wykorzystania przyznanych środków - w ustalonym terminie. 2) Poprawić współpracę Pełnomocnika ds. Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii z komórką finansów, w zakresie ewidencjonowania środków Gminnego Programu Rozwiązywania Problemów Alkoholowych i Przeciwdziałania Narkomanii. Podczas realizacji zadania audytor zapoznał się ze środowiskiem, w tym z regulacjami prawnymi, uczestnikami procesu, oraz procedurami. Podsumowując, nie sposób nie wspomnieć jak istotne zadania postawiono przed Pełnomocnikiem ds. Rozwiązywania Problemów Alkoholowych

				i Przeciwdziałania Narkomanii. W obecnych czasach, kiedy dostęp do napojów alkoholowych czy środków odurzających (narkotyków), pomimo wprowadzanych przez państwo zakazów/ograniczeń jest niestety dostępny niemalże na każdym kroku, realizacja zadań Pełnomocnika jest szczególnie ważna. Poza pełnomocnikiem działania w opisywanym zakresie oczywiście wykonuje szereg innych podmiotów. Jednakże z punku widzenia Gminy, to właśnie od jego prawidłowo wykonywanych zadań zależy sprawna pomoc mieszkańcom. Pełnomocnik bowiem koordynuje działania innych podmiotów oraz prowadzi dokumentację, bierze udział w posiedzeniach, organizuje szkolenia dla członków innych podmiotów, udziela porad i pomocy, a także pozyskuje środki dla realizacji zadań przez inne podmioty. Pełnomocnik czynnie też uczestniczy w organizacji różnego rodzaju imprez dla dzieci, jak i całych rodzin zagrożonych wykluczeniem społecznym. Analizę systemu dokonano w oparciu o należytą staranność (standardy audytu wewnętrznego) i wiedzę audytora wewnętrznego w badanym zakresie. W sprawozdaniu przedstawiono charakterystykę 3 obiektów audytu. Podsumowując audytor wewnętrzny udziela zapewnienia o adekwatności, efektywności i skuteczności przyjętych mechanizmów dla kontroli, zarządzania ryzykiem i nadzoru, jednakże zwraca uwagę kierownictwa na zasadność wprowadzenia ujętych w sprawozdaniu zaleceń.

2.	Realizacja zadań z zakresu udzielania zamówień publicznych przez jednostki organizacyjne podległe Gminie Brusy - Zakład Gospodarki Komunalnej w Brusach	(Z)	Wzrost efektywności i skuteczności działania	Zakres działalności, jaki poddany został audytowi wewnętrznemu to zagadnienia związane z udzielaniem zamówień publicznych przez Zakład Gospodarki Komunalnej w Brusach. Jako główny obiekt audytu wyróżniono: 1) ocenę konstrukcji systemu pod względem struktury, skuteczności koordynacji systemu oraz zgodności z przepisami prawa, w tym: a) analizę wewnętrznych procedur w zakresie zamówień publicznych, b) weryfikację wybranego do badania postępowania o udzielenie zamówienia publicznego. Zasady i mechanizmy funkcjonowania poszczególnych procesów zostały przedstawione w postaci tabelarycznej. Na tej podstawie zidentyfikowano istniejące mechanizmy kontroli, które następnie poddane zostały analizie poprzez przeprowadzenie testów zgodności i testów rzeczywistych - aby sprawdzić czy mechanizmy te funkcjonują prawidłowo. Potwierdzenia zawartych ustaleń dokonano poprzez użycie niżej wymienionych technik: uzyskanie wyjaśnień i informacji, tabelaryczną analizę procesów, sprawdzenie rzetelności informacji przez porównanie ich z informacją pochodzącą z innego źródła. Czynnikami ryzyka, które w szczególności trzeba mieć na uwadze, są: 1) nieskuteczny podział zadań i kompetencji, 2) niezgodne (nieaktualne) z obowiązującymi przepisami określenie obowiązków w wewnętrznych uregulowaniach, 3) brak i/lub nieskuteczne przeprowadzanie postępowań skutkujących udzieleniem zamówienia publicznego, 4) brak i/lub nieskuteczne realizowanie wewnętrznych procedur regulujących wykonywanie obowiązków dotyczących postępowania w procesach udzielenia zamówienia publicznego, 5) niezgodne z obowiązującymi przepisami wykonywanie obowiązków, 6) brak lub nieskuteczna kontrola wewnętrzna, 7) brak procedur bezpieczeństwa bądź ich lekceważenie, 8) ucieczka z systemu zamówień publicznych/obchodzenie prawa/, 9) ograniczanie konkurencji, 10) nadinterpretacja lub błędna interpretacja przepisów, 11) słabe planowanie zamówień, 12) niefachowo sporządzane dokumenty, 13) nadużywanie trybów nieprzetargowych, 14) niewystarczające uzasadnienie i informowanie o motywach podjętych decyzji,

				15) częste unieważniane postępowań o udzielanie zamówień, 16) duża liczba zamówień udzielanych w trybach innych niż przetargowe. W trakcie realizacji audytu dokonano weryfikacji działań w celu potwierdzenia efektywności wdrożonych systemów zarządzania i kontroli. Przeprowadzony audyt systemów zarządzania i kontroli skierowany był głównie na określenie, czy systemy działają efektywnie w celu zapobiegania nieprawidłowościom oraz czy tam gdzie mogą pojawić się ewentualne błędy i nieprawidłowości, systemy efektywnie wykryją je i skorygują. Ocena konstrukcji mechanizmów kontroli i systemu kontroli polegała na identyfikacji celów, analizie konkretnych ryzyk, identyfikacji kluczowych kontroli, ocenie atutów i słabości kontroli oraz dokonaniu oceny systemu kontroli. Zakład Gospodarki Komunalnej w Brusach jest gminną jednostką organizacyjną działającą w formie samorządowego zakładu budżetowego utworzonego na podstawie Uchwały Rady Miejskiej w Brusach Nr III-19/94 z dnia 8 września 1994 r. w sprawie utworzenia Zakładu Gospodarki Komunalnej w Brusach powołanego do realizacji zadań określonych w statucie. W trakcie realizacji niniejszego zadania audytowego, przedstawiono „Plan postępowań o udzielenie zamówień publicznych w roku 2016". W Rejestrze zamówień publicznych wskazano w/w dwa przedmioty zamówienia 1) Zakup i dostawa samochodu ciężarowego z urządzeniem hakowym 2) Dostawa paliw płynnych dla pojazdów ZGK w 2017 r. Po zakończeniu roku w Jednostce sporządzone zostało „Roczne sprawozdanie o udzielonych zamówieniach publicznych w roku 2016". 1) Zamówienia o wartości przekraczającej wyrażonej w złotych równowartość kwoty, o której mowa w art. 4 pkt 8 ustawy, i mniejszej od kwot określonych w przepisach wydanych na podstawie art. 11 ust 8 ustawy: a) Dwa postępowania w trybie przetargu nieograniczonego, o wartości zawartych umów na kwotę 413.322,00 zł. 2) Zamówienia udzielone z wyłączeniem procedur określonych przepisami ustawy: a) Zamówienia, których wartość nie przekracza wyrażonej

				w równowartości kwoty, o której mowa w art. 4 pkt 8 ustawy, łączna wartość udzielonych zamówień bez podatku i usług: 1.749.632,00 zł. Wybrane do badania postępowanie przeprowadzane było w trybie przetargu nieograniczonego: Zakup i dostawa samochodu ciężarowego z urządzeniem hakowym. Regulamin dotyczy zamówień na dostawy usługi i roboty budowlane, których wartość przekracza wyrażoną w złotych równowartość kwoty określonej w art. 4 pkt 8 ustawy tj. 30 tys. euro. Na podstawie wybranych kryteriów audytor przeprowadził testy rzeczywiste mające na celu zapewnienie o legalności przeprowadzanych postępowań o udzielenie zamówienia publicznego. Badaniu podlegały postępowania wybrane do analizy po przeprowadzonej wcześniej analizie ryzyka. Na podstawie uzyskanych wyników badań, stwierdzono, że postępowania o zamówienia publiczne przebiegały z zachowaniem obowiązujących przepisów w zakresie zamówień publicznych. Badanemu obszarowi audytor wydał pozytywną opinię. Przedstawiona w niniejszym sprawozdaniu opinia audytora jest rezultatem zebranych dowodów oraz własnego osądu. Opiera się o procedury audytowe oraz ustalone fakty i ma na celu poszukiwanie możliwości ewentualnych usprawnień. Audytor przeprowadził testy przeglądowe mające na celu diagnozę zasad organizacyjnych udzielania zamówień publicznych w ZGK w Brusach, w zakresie przygotowywania, przeprowadzania i rozstrzygania postępowań skutkujących udzieleniem zamówienia publicznego. W celu legalnej realizacji przepisów ustawy Prawo zamówień publicznych oraz aktów wykonawczych do ustawy w Jednostce opracowano i wdrożono szereg wewnętrznych regulacji, normujących tryb postępowania przy udzielaniu zamówień publicznych. Postępowanie o udzielenie zamówienia publicznego jest jawne. Do dotrzymania tej zasady należy założyć, że każde, pozornie nawet mało znaczące działanie zamawiającego w postępowaniu w sprawie zamówienia publicznego powinno być udokumentowane. Takie postępowanie jest doskonałym elementem kontroli wewnętrznej, wpływa również na przejrzystość. Na podstawie badanej dokumentacji dot. udzielanych zamówień publicznych audytor potwierdza zgodność wykonywania zadań z procedurami.

				Poprawnie określano przedmiot zamówienia. Dokonywany przez zamawiającego w SIWZ opis przedmiotu zamówienia wpływa na przebieg postępowania o udzielenie zamówienia publicznego oraz stanowi o istotnych postanowieniach późniejszej umowy. Stąd też na zamawiającym spoczywa obowiązek jasnego i precyzyjnego określenia przedmiotu zamówienia. Innymi równie ważnymi dokumentami są SIWZ oraz protokół. Specyfikacja przygotowana w sposób umożliwiający manipulowanie wynikami przetargu może być poważnym źródłem patologii. Wadliwe sporządzanie SIWZ skutkuje również poza przetargowym udzieleniem zamówień dodatkowych (nagminnym w przypadku zamówień na roboty budowlane), albo dążeniem do zmiany zawartej umowy z powołaniem się na konieczność takich zmian, spowodowaną okolicznościami, których nie można było rzekomo przewidzieć. Przygotowując postępowanie o udzielenie zamówienia publicznego, zamawiający musi podjąć strategiczną decyzję, jakie warunki postawi wykonawcom, którzy będą ubiegać się o to zamówienie. Na tym etapie postępowania trzeba pamiętać, że powzięte ustalenia będą miały kluczowe znaczenie w trakcie późniejszego dokonywania oceny spełnienia tych warunków przez wykonawców i mogą spowodować, że postępowanie nie zakończy się udzieleniem zamówienia. Istotne znaczenie ma załączanie wzoru przyszłej umowy do SIWZ. Jest to doskonałe narzędzie zapewniające zgodność zawartej umowy z wymaganiami zamawiającego. Prawidłowo czy zgodnie z przepisami formalnymi oraz zgodnie z zasadami udzielania zamówień publicznych, sporządzona specyfikacja, utrudnia lub wręcz uniemożliwia działania patologiczne w procesie udzielania zamówienia publicznych. Należy zwracać uwagę także na to, aby w umowie zawarte zostały odpowiednie zapisy chroniące interesy zamawiającego np. określające odpowiedzialność wykonawcy za niewykonanie, opóźnienie lub nierzetelne wykonanie zamówienia. W umowie winny także zostać zawarte procedury oceny i odbioru wykonanych robot budowlanych, usług lub dostaw. Przeprowadzone przez audytora badania wskazały, że w Jednostce badany obszar funkcjonuje prawidłowo. W celu efektywnego i legalnego przeprowadzania postępowań skutkujących udzieleniem zamówienia publicznego opracowano i wdrożono wewnętrzne procedury. Analiza ich treści wskazała na ich zgodność z obowiązującymi w tym zakresie przepisami prawa. Przeprowadzone testy potwierdziły, że przeprowadzane postępowania o udzielenie zamówienia publicznego przebiegały w zgodności z obowiązującymi w tym zakresie przepisami i wewnętrznymi uregulowaniami.

				W związku z powyższym wydane rekomendacje, mają za zadanie jedynie charakter informacyjny, mający przyczynić się do doskonalenia procesu przeprowadzania postępowań skutkujących udzieleniem zamówienia publicznego. Można przypomnieć ogromną odpowiedzialność za udzielanie zamówień publicznych. Za zamówienia publiczne i gospodarkę finansową odpowiadają kierownicy jednostek. To na kierowniku jednostki ciąży obowiązek zapewnienia w kierowanej przez siebie placówce takiej organizacji pracy, która pozwala na prawidłowe wykonywanie obowiązków jednostki. Kierownicy jednostek, nie wypełniając obowiązków w zakresie wykonywania zobowiązań jednostki sektora finansów publicznych, zaciągania zobowiązań oraz dotyczących zamówień publicznych, narażają się na odpowiedzialność za naruszenie dyscypliny finansów publicznych. Jednymi z podstawowych aktów prawnych, które kierownik jednostki sektora finansów publicznych obowiązany jest znać i stosować, są właśnie przepisy dotyczące zamówień publicznych. Odpowiedzialność zaś z tego tytułu ponoszą kierownicy jednostek sektora finansów publicznych oraz inni pracownicy, którym powierzono czynności przewidziane w przepisach o zamówieniach publicznych (w zakresie wynikającym z powierzonych obowiązków lub upoważnień). Z analizy najnowszego orzecznictwa komisji orzekających, Głównej Komisji Orzekającej oraz sądów administracyjnych w sprawach o naruszenie dyscypliny finansów publicznych wynika, że jednym z najczęstszych naruszeń było nieprzestrzeganie lub niewłaściwe zastosowanie przepisów prawa zamówień publicznych. Potwierdzają to również eksperci. Istotne znaczenie dla badanego systemu ma efektywność funkcjonujących mechanizmów kontrolnych. Obszary ryzyka związane z badaną działalnością w przypadku nieprawidłowego funkcjonowania, mogłyby implikować poważne straty w działalności Jednostki. Analizę systemu dokonano w oparciu o należytą staranność (standardy audytu wewnętrznego) i wiedzę audytora wewnętrznego w badanym zakresie. W sprawozdaniu przedstawiono charakterystykę 1 obiektu audytu. Audytor wewnętrzny nie wnosi zastrzeżeń odnośnie prawidłowości stosowanych mechanizmów kontroli w badanym zakresie. Podsumowując audytor wewnętrzny udziela zapewnienia o adekwatności, efektywności i skuteczności przyjętych mechanizmów dla kontroli, zarządzania ryzykiem i nadzoru. Jednakże zwraca uwagę kierownictwa na zasadność wprowadzenia ujętych w sprawozdaniu zaleceń.

3.	Bezpieczeństwo informacji	(Z)	Wzrost efektywności i skuteczności działania	Zakres działalności, jaki poddany został audytowi wewnętrznemu to zagadnienia związane z ochroną informacji w systemach informatycznych. Jako obiekt audytu wyróżniono realizację zagadnień określonych w § 20 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, w tym w szczególności: 1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, 2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, 3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, 4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, 5) zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4, 6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich, 7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

				8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, 9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie, 10) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, 11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, 12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania, b) minimalizowaniu ryzyka utraty informacji w wyniku awarii, c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e) zapewnieniu bezpieczeństwa plików systemowych, f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa, 13) bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących. Ogólne ryzyka jakie mogą wiązać się z ochroną danych w systemach informatycznych to między innymi: 1) brak planów awaryjnych dla systemów, 2) brak wykazu osób odpowiedzialnych za sprawność systemu, 3) brak przypisania zasobów informatycznych do poszczególnych osób – brak świadomości pracowników, 4) brak procedur tworzenia i przechowywania kopii zapasowych, 5) brak kontroli fizycznego dostępu do zasobów informatycznych, 6) brak zasileń awaryjnych UPS, 7) niezabezpieczone pomieszczenia, 8) brak ochrony antywirusowej,

				9) brak określonych procedur ochrony danych, 10) nieodpowiednie przechowywania nośników danych, 11) brak procedur rejestracyjnych sprzętu lub oprogramowania, 12) utrata, utrata częściowa lub modyfikacja danych, 13) nieautoryzowany dostęp, 14) zakłócenie kluczowych procesów, 15) niska sprawność techniczna urządzeń, wysoka awaryjność, 16) brak procedur bezpieczeństwa bądź ich lekceważenie, 17) brak założeń bezpieczeństwa dla systemów, 18) brak zasad stałego monitorowania systemów i usuwania błędów, 19) brak zasad bezpieczeństwa korzystania z internetu, 20) brak zdefiniowania sytuacji kryzysowych, 21) występujące, niepotrzebne opóźnienia w przywracaniu działania kluczowych systemów i procesów informatycznych po wystąpieniu awarii, 22) utrata lub brak dostępu do danych w momencie wystąpienia poważnych awarii systemu i/lub przerw w jego działaniu, 23) plan usuwania skutków awarii jest nieskuteczny i/lub niemożliwy do przeprowadzenia, 24) przerwa w ciągłości działania po utracie lub awarii systemów informatycznych, 25) strata finansowa będąca konsekwencją awarii, 26) utrata lub uszkodzenie danych po awarii systemu, 27) nieodpowiednie nośniki, na których wykonano kopie zapasowe uniemożliwiają odzyskanie danych po awarii lub innej sytuacji kryzysowej, 28) utrata, zniszczenie lub brak dostępności nośnika z kopią zapasową, 29) użytkownicy nieumyślnie wprowadzają wirusa, który powoduje brak dostępu do systemu, utratę i/lub uszkodzenie danych, 30) zainfekowanie przez wirusy prowadzi do braku dostępu do systemu, utraty i/lub uszkodzenia danych, 31) istnieje możliwość dostępu do niestosownych witryn internetowych lub niewłaściwego korzystania z poczty elektronicznej, 32) obniżona wydajność personelu: użytkownicy w czasie pracy wykorzystują narzędzia internetowe do celów prywatnych, 33) narzędzia internetowe nie są wykorzystywane w sposób wydajny i efektywny, 34) niestosowne materiały przesyła się drogą e-mailową,

				35) nieautoryzowany dostęp do sieci wewnętrznej jednostki, jej systemów i/lub danych, 36) infekcja wirusem lub innym złośliwym oprogramowaniem, 37) nieuprawniony dostęp fizyczny do sprzętu komputerowego, 38) przypadkowe lub zamierzone uszkodzenie sprzętu komputerowego, 39) utrata danych na skutek braku zasilania, 40) straty finansowe lub spowolnienie procesu przywracania stanu sprzed awarii spowodowane brakiem funduszy, 41) brak koordynacji sieci, co w konsekwencji nie spełnia ona oczekiwań jednostki ani użytkowników, 42) nieautoryzowany dostęp do połączonych siecią systemów i zawartych w nich danych, 43) nieautoryzowany dostęp do danych poufnych lub o kluczowym znaczeniu dla jednostki przekazywanych przez sieć, 44) brak podziału obowiązków prowadzący do oszustw oraz nadużyć. Zakres działalności, jaki poddany został audytowi wewnętrznemu to działania, procesy i procedury związane z bezpieczeństwem informacji. Zasady i mechanizmy funkcjonowania poszczególnych procesów zostały przedstawione w postaci tabelarycznej. Na tej podstawie zidentyfikowano istniejące mechanizmy kontroli, które następnie poddane zostały analizie poprzez przeprowadzenie testów zgodności i testów rzeczywistych - aby sprawdzić czy mechanizmy te funkcjonują prawidłowo. Potwierdzenia zawartych ustaleń dokonano poprzez użycie niżej wymienionych technik: uzyskanie wyjaśnień i informacji, tabelaryczną analizę procesów, kwestionariusz kontroli wewnętrznej, sprawdzenie rzetelności informacji przez porównanie ich z informacją pochodzącą z innego źródła. W trakcie realizacji audytu dokonano weryfikacji działań w celu potwierdzenia efektywności wdrożonych systemów zarządzania i kontroli. Przeprowadzony audyt systemów zarządzania i kontroli skierowany był głównie na określenie, czy systemy działają efektywnie w celu zapobiegania nieprawidłowościom oraz czy tam gdzie mogą pojawić się ewentualne błędy i nieprawidłowości, systemy efektywnie wykryją je i skorygują. Ocena konstrukcji mechanizmów kontroli i systemu kontroli polegała na identyfikacji celów, analizie konkretnych ryzyk, identyfikacji kluczowych kontroli, ocenie atutów i słabości kontroli oraz dokonaniu oceny systemu kontroli. Przedstawiona w niniejszym sprawozdaniu opinia audytora jest rezultatem zebranych dowodów oraz własnego osądu. Opiera się o procedury

				audytowe oraz ustalone fakty i ma na celu poszukiwanie możliwości ewentualnych usprawnień. Wycieki poufnych informacji stanowią ogromne zagrożenie dla bezpieczeństwa ochrony informacji. Coraz więcej jest dróg wydostawania się informacji poza urząd. Pracownicy przygotowują i przechowują sporządzane dokumenty zawierające informacji na komputerach mających dostęp do sieci internetowej lub wewnętrznej sieci urzędu. Różnego rodzaju dane są przesyłane za pomocą poczty elektronicznej, przez komunikatory internetowe. Teoretycznie mogą zdarzyć się również kradzieże samego sprzętu, na którym znajdują się poza innymi dokumentami również zawierające poufne informacje. W całej masie potencjalnych ścieżek, którymi mogą wypływać dane, liczą się również motywy, a te mogą być najróżniejsze. Ochrona informacji może dla wielu pracowników wydawać się niewygodna. Potrzeba więc zmiany sposobu myślenia. Niestety duża cześć naszych przyzwyczajeń, uproszczeń i dróg na skróty powoduje narażenie na utratę lub ujawnienia informacji. Sprawy mogą mieć się zupełnie inaczej jeśli pracownikom wytłumaczy się, dlaczego konieczna jest ochrona informacji. To bardzo ważny krok, od którego może zależeć powodzenie całego przedsięwzięcia. Jeśli uda się sprzedać idee ochrony informacji, przekonać że jest to konieczne i ważne oraz że zagrożenia naprawdę istnieją, to sukces mamy gwarantowany. Dbałość o bezpieczeństwo musi stać się codziennym elementem pracy. W związku z coraz bardziej masowym wykorzystywaniem systemów i sieci teleinformatycznych we wszystkich rodzajach działalności, problem występujących zagrożeń i sposobów przeciwdziałania im staje się jednym z kluczowych problemów związanych z elektronicznym przetwarzaniem danych. Powszechność przetwarzania danych w systemach i sieciach teleinformatycznych powoduje zarówno zwiększenie skali zagrożeń jak i zmniejsza możliwość bezpośredniej kontroli poszczególnych etapów procesu przetwarzania. Rodzaje zagrożeń: 1) naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikowanie, dodanie, zniszczenie), 2) nieuprawnione skopiowanie danych i wyprowadzenie ich z urzędu przez pracownika, 3) włamanie dokonywane do systemu teleinformatycznego, 4) nieuprawniony dostęp do zasobów systemu dzięki ujawnieniu haseł innych użytkowników,

				5) niepowołany dostęp do miejsca przetwarzania danych, 6) zniszczenie elementów lub całości infrastruktury technicznej systemu teleinformatycznego, 7) nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura). W ostatnich latach w Urzędzie Miejskim w Brusach wprowadzono szereg mechanizmów mających na celu zwiększenie bezpieczeństwa danych w systemach informatycznych. Jako główne obiekty audytu wyróżniono realizację zagadnień określonych w § 20 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. Uwagi w zakresie zagadnień określonych w § 20 Rozporządzenia, o którym mowa powyżej: 1) *ZAPEWNIENIE AKTUALIZACJI REGULACJI WEWNĘTRZNYCH W ZAKRESIE DOTYCZĄCYM ZMIENIAJĄCEGO SIĘ OTOCZENIA* W w/w zakresie przypomniano, że od 25 maja 2018 r. w ochronie danych osobowych nic nie będzie już takie samo. Firmy i urzędy/jednostki muszą spełnić szereg restrykcyjnych wymogów. Rozporządzenie o Ochronie Danych Osobowych (RODO), to nowe unijne prawo, które w zupełnie inny, niż dotychczas, sposób definiuje zasady przetwarzania, wykorzystywania i przechowywania danych osobowych. Trzeba je wdrożyć do 25 maja przyszłego roku. Przepisy obejmują wszystkie podmioty, które gromadzą i wykorzystują dane dotyczące osób fizycznych. Nadchodzące zmiany będą dotyczyły zarówno firm, jak i administracji. Co ważne – RODO będą musiały wdrożyć wszystkie organy administracji publicznej. Zarówno te duże firmy, czy urzędy jak i te małe kilku - czy kilkunastoosobowe firmy, sklepy internetowe, szkoły, ośrodki pomocy społecznej czy domy kultury itp. muszą przetwarzać dane osobowe zgodnie z prawem.

				2) ZAPEWNIENIE OCHRONY PRZETWARZANYCH INFORMACJI PRZED ICH KRADZIEŻĄ, NIEUPRAWNIONYM DOSTĘPEM, USZKODZENIAMI LUB ZAKŁÓCENIAMI, PRZEZ: a) MONITOROWANIE DOSTĘPU DO INFORMACJI, b) CZYNNOŚCI ZMIERZAJĄCE DO WYKRYCIA NIEAUTORYZOWANYCH DZIAŁAŃ ZWIĄZANYCH Z PRZETWARZANIEM INFORMACJI, c) ZAPEWNIENIE ŚRODKÓW UNIEMOŻLIWIAJĄCYCH NIEAUTORYZOWANY DOSTĘP NA POZIOMIE SYSTEMÓW OPERACYJNYCH, USŁUG SIECIOWYCH I APLIKACJI 3) ZABEZPIECZENIE INFORMACJI W SPOSÓB UNIEMOŻLIWIAJĄCY NIEUPRAWNIONEMU JEJ UJAWNIENIE, MODYFIKACJE, USUNIĘCIE LUB ZNISZCZENIE 4) ZAPEWNIENIA ODPOWIEDNIEGO POZIOMU BEZPIECZEŃSTWA W SYSTEMACH TELEINFORMATYCZNYCH, POLEGAJĄCEGO W SZCZEGÓLNOŚCI NA: a) DBAŁOŚCI O AKTUALIZACJĘ OPROGRAMOWANIA, b) MINIMALIZOWANIU RYZYKA UTRATY INFORMACJI W WYNIKU AWARII, c) OCHRONIE PRZED BŁĘDAMI, UTRATĄ, NIEUPRAWNIONĄ MODYFIKACJĄ, d) STOSOWANIU MECHANIZMÓW KRYPTOGRAFICZNYCH W SPOSÓB ADEKWATNY DO ZAGROŻEŃ LUB WYMOGÓW PRZEPISU PRAWA, e) ZAPEWNIENIU BEZPIECZEŃSTWA PLIKÓW SYSTEMOWYCH, f) REDUKCJI RYZYK WYNIKAJĄCYCH Z WYKORZYSTANIA OPUBLIKOWANYCH PODATNOŚCI TECHNICZNYCH SYSTEMÓW TELEINFORMATYCZNYCH, g) NIEZWŁOCZNYM PODEJMOWANIU DZIAŁAŃ PO DOSTRZEŻENIU NIEUJAWNIONYCH PODATNOŚCI SYSTEMÓW TELEINFORMATYCZNYCH NA MOŻLIWOŚĆ NARUSZENIA BEZPIECZEŃSTWA, h) KONTROLI ZGODNOŚCI SYSTEMÓW TELEINFORMATYCZNYCH Z ODPOWIEDNIMI NORMAMI I POLITYKAMI BEZPIECZEŃSTWA 5) BEZZWŁOCZNE ZGŁASZANIE INCYDENTÓW NARUSZENIA BEZPIECZEŃSTWA INFORMACJI W OKREŚLONY I Z GÓRY

				USTALONY SPOSÓB, UMOŻLIWIAJĄCY SZYBKIE PODJĘCIE DZIAŁAŃ KORYGUJĄCYCH W w/w zakresie przedstawiono obszerny materiał informacyjny dot. m.in.: haseł, sposobu ustawiania monitorów, UPS-ów, ściągania nowych wersji oprogramowania. Uwagę należy zwrócić też na socjotechniki - wywieranie wpływu na ludzi i stosowanie perswazji w celu oszustwa. Zwykle celem socjotechnika jest uwiarygodnienie osoby, za którą się podaje stworzonej na potrzeby manipulowania tożsamością. Przy pomocy tej metody socjotechnik jest w stanie uzyskać poszukiwane informację od rozmówcy, zarówno przy użyciu innych metod technologicznych, jak i bez takiej możliwości. Poniższy materiał ma jedynie charakter informacyjny. Komputery pracujące w systemach komputerowych są na co dzień narażone na różnego rodzaju zagrożenia. W obecnych czasach, gdy te systemy mają tak wielkie znaczenie w zapewnieniu ciągłości pracy, słowo zagrożenie ma kluczowe znaczenie, a bezpieczeństwo tychże systemów powinno być traktowane priorytetowo. Należy zwrócić uwagę, że większość sytuacji związanych z utratą dostępu do danych we wszystkich systemach komputerowych jest powodowane problemami ze sprzętem. Uszkodzenia systemów dyskowych niosą za sobą największe ryzyko związane z utratą dostępu do danych, a nawet z ich bezpowrotną stratą. Innym czynnikiem, który może mieć duży wpływ na bezpieczeństwo danych jest potencjalna możliwość kradzieży (zniszczenia danych) sprzętu. Skradziony lub uszkodzony sprzęt zazwyczaj może być w dość krótkim okresie czasu zastąpiony przez nowy, bez większej szkody, ale niemożliwy jest taki sam scenariusz postępowania, gdy mamy do czynienia z danymi kluczowymi dla działania jednostki. Ich odtworzenie może być procesem długotrwałym, a w skrajnych przypadkach nawet niemożliwym. Bezpieczeństwo systemów komputerowych to ogół działań mających na celu zabezpieczać dane przechowywane w komputerze, tak by nie mogły zostać wykorzystane przez niepowołane osoby czy też narażone na trwałą utratę. W przypadku procesów związanych z bezpieczeństwem analiza zagrożeń jest niezbędna do opracowania systemu o możliwie najwyższej efektywności, przy jednoczesnym zapewnieniu racjonalnych kosztów

				ponoszonych na ochronę. Sprowadza się to do wyboru i wdrożenia narzędzi służących zapewnieniu bezpieczeństwa. Dobór zabezpieczeń jest tym elementem, który determinuje - często na długie lata - sprawność i efektywność systemu. Mamy do wyboru rozwiązania zróżnicowane zarówno pod względem jakości, parametrów technicznych, jak i wreszcie ceny. Na tym etapie konieczne jest współdziałanie osoby odpowiedzialnej za bezpieczeństwo systemów informatycznych oraz osoby odpowiedzialnej za gospodarkę finansową. Istotną kwestię stanowi sposób umieszczenia monitorów komputerowych. Okazuje się, że może to stanowić spore ryzyko, bowiem istnieje możliwość podglądu wyników pracy, możliwość podglądu danych. Konieczne jest ustawienie monitorów tak, że interesanci nie będą mieli wglądu w dane umieszczone na monitorze. Zapobieżenie skutkom nieprzewidzianych przerw w dostawie energii elektrycznej może technicznie być realizowane na wiele sposobów. Najbardziej rozpowszechnioną metodą jest stosowanie zasilaczy awaryjnych tzw. UPS-ów lub np. agregatów prądotwórczych. Bardzo istotną czynnością w zakresie zabezpieczenia działania systemów IT jest regularnie sprawdzanie działanie systemów UPS. Osoba, której przydzielono sprzęt powinna zadbać, aby dostęp do systemów na których pracuje, został zabezpieczony hasłem. Pracownicy posiadają zabezpieczenia w postaci haseł dostępu do swoich komputerów. Ponieważ systemy informatyczne nie zawsze wymuszają konieczności zmiany hasła po upływie określonego terminu, należałoby zastosować przynajmniej hasła spełniające wymogi „haseł bezpiecznych" (duże i małe litery, liczby itp.). Jedną z zasad bezpieczeństwa jest nie udostępnianie swoich haseł innym osobom. Główna zasada związana z właściwym zarządzaniem hasłami brzmi: hasła nie powinny być nigdzie zapisywane – ani w komputerze w formie jawnej. Wystarczy wspomnieć żółte karteczki na monitorze czy pod klawiaturą. Wyjątkiem jest hasło administratora. Ze względu na ciągłość działania systemu informatycznego hasło głównego administratora powinno zostać zapisane i właściwie zabezpieczone. Ma to zapobiec sytuacji, gdy administrator zdecyduje się opuścić szeregi pracowników naszej organizacji lub przytrafi mu się jakieś nieszczęście i nie będziemy mogli wykonać żadnych czynności administracyjnych. Najczęściej hasła administracyjne

				zapisywane są na kartce, a następnie umieszczane w specjalnie do tego celu przygotowanych kopertach, uniemożliwiających podejrzenie hasła, jak również zapewniających, że każda próba otwarcia koperty zostawi widoczne ślady. Kopertę trzeba umieścić w sejfie. W dalszych krokach należy zadbać o ograniczony dostęp do tego sejfu, właściwe zarządzanie kluczami do sejfu itp. Hasła użytkowników powinny być utrzymywane w tajemnicy i nie powinny być ujawniane innym osobom, jak również zapisywane, chyba że mogą być przechowywane w sposób bezpieczny, a metoda ta zostanie zatwierdzona. Wybierane przez użytkowników hasła powinny być łatwe do zapamiętania, dobrej jakości, o wystarczającej minimalnej długości, zmieniane w regularnych odstępach czasu. Zaleca się nie powtarzać haseł ani nie korzystać z nich cyklicznie. Wybierane przez użytkowników hasła nie powinny być oparte na prostych skojarzeniach związanych z użytkownikiem, np. imionach, numerach telefonów, datach urodzin, imienin itp., jak również nie powinny być podatne na atak słownikowy. Zaleca się stosowanie haseł składających się z różnych grup znaków. Po otrzymaniu hasła tymczasowego od administratora, użytkownik powinien dokonać jego zmiany przy pierwszym logowaniu do systemu. Hasło powinno być również zmienione w przypadku jego ujawnienia lub nawet podejrzenia jego kompromitacji. Zaleca się, aby nie korzystać z tego samego hasła w celach służbowych i niezwiązanych z pracą. Norma zaleca również, aby do przechowywania haseł nie korzystać ze zautomatyzowanych procesów, np. przypisania hasła do klawiszy funkcyjnych. Często hasła są przekazywane w czasie nieobecności pracownika, np. w czasie choroby, urlopu. Praktyka taka nie jest właściwa. Najlepszym rozwiązaniem jest rozszerzenie uprawnień osobie zastępującej danego pracownika, tak aby z poziomu swojego konta mogła wykonać wszystkie wymagane operacje – jeśli w danym systemie jest to możliwe. Podobnie rozwiązać można problem z pocztą elektroniczną, przekierowując pocztę na inne konto pocztowe. Należy pamiętać o udokumentowaniu zmiany uprawnień, a następnie o przywróceniu stanu pierwotnego po ustaniu czasu pełnienia zastępstwa. Obecnie prawie wszystkie zabezpieczenia wbudowane w systemy operacyjne mogą być stosunkowo łatwo ominięte. Informacje o sposobach obejścia danego zabezpieczenie dostępne są w wielu witrynach internetowych czy też na grupach dyskusyjnych. Do najbardziej

				popularnych zagrożeń należą niewątpliwie wirusy komputerowe. Obecnie źródłem zagrożenia mogą być także inne aplikacje. Wielu użytkowników ulega pokusie ściągania nowych wersji oprogramowania komercyjnego całkowicie za „darmo" z niesprawdzonych źródeł. Te właśnie źródła są powodem późniejszych kłopotów. Prócz pozornie „darmowego" oprogramowania otrzymuje się w zamian programy szpiegujące i wysyłające o nas informacje, lub co gorsze przesyłające pliki z naszego systemu bez wiedzy użytkownika. Najbardziej wyrafinowane potrafią przekazać kontrolę nad naszym komputerem osobom trzecim, które mogą w łatwy sposób utrudnić / uniemożliwić nam pracę. Ochrona przed pewnymi typami zagrożenia wymagać może wdrożenia wielu różnych zabezpieczeń, których funkcjonalność wzajemnie się uzupełnia. Dzieje się tak wówczas, gdy pojedynczy rodzaj zabezpieczenia nie gwarantuje ochrony na wymaganym poziomie. Oczywiście, aby dokonać właściwego doboru zabezpieczeń, należy być świadomym zarówno ich słabości, jak i własnych wymagań dotyczących ochrony zasobów. Uwagę należy zwrócić też na socjotechniki. **Socjotechnika** jest wywieraniem wpływu na ludzi i stosowanie perswazji w celu oszustwa, zwykle celem socjotechnika jest uwiarygodnienie osoby, za którą się podaje stworzonej na potrzeby manipulowania tożsamością. Przy pomocy tej metody socjotechnik jest w stanie uzyskać poszukiwane informację od rozmówcy, zarówno przy użyciu innych metod technologicznych, jak i bez takiej możliwości. Przykłady Fałszywe Pisma/Faktury/Dokumenty Jednostka, przelała pieniądze na podstawione konto bankowe. Komputer nie był zainfekowany i nikt go nie „zhackował". Po prostu uwierzyli w fałszywe pismo o zmianie numeru rachunku. Środki Bezpieczeństwa: • Pracownik Organizacji jest zobowiązany zachować poufność przetwarzanych danych oraz sposobów ich zabezpieczenia. • Dane można wykorzystywać wyłącznie do celów, dla których zostały udostępnione. • Dokumenty zawierające informacje podlegające ochronie powinny być przechowywane na biurku i innych miejscach do tego

				przeznaczonych, w taki sposób, aby osoba nieuprawniona nie miała do nich dostępu. • Nośniki informacji (w formie papierowej i elektronicznej) z danymi podlegającymi ochronie nie można pozostawiać w miejscach ogólnodostępnych i niezabezpieczonych oraz nie należy udostępniać osobom nieupoważnionym. • Dokumenty wydrukowane w nadmiernej ilości, a także zawierające błędy lub, które nie są wykorzystywane do żadnych celów należy trwale zniszczyć w sposób uniemożliwiający odtworzenie treści. • Dokumenty zawierające informacje podlegające ochronie, przed wyrzuceniem do kosza należy zanonimizować, w taki sposób, aby nie można było odtworzyć ich treści i zidentyfikować osoby, której dane dotyczą, lub zniszczyć za pomocą niszczarki. • Monitor należy usytuować w taki sposób, aby osoby nieupoważnione wchodzące do pomieszczenia nie miały wglądu do danych na nim wyświetlanych. • Przed zalogowaniem się do systemu stacji roboczej należy upewnić się, że w pobliżu nie ma osób trzecich lub urządzeń nagrywających mogących zarejestrować hasła dostępowe do systemów, z których zamierzamy skorzystać. Jeśli występuje takie zagrożenie należy zastosować szczególne środki ostrożności uniemożliwiające zarejestrowanie wpisywanego hasła • Oprogramowanie instaluje tylko i wyłącznie administrator systemu informatycznego, nigdy nie należy robić tego samodzielnie. • Używanych identyfikatorów i haseł nie należy udostępniać innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, należy dokonać ich zmiany zgodnie z obowiązującymi procedurami. • Logowanie do systemu pocztowego przy pomocy internetowej przeglądarki powinno być przeprowadzone na osobistym komputerze, laptopie posiadającym zabezpieczenie antywirusowe. • W przypadku opuszczania stanowiska pracy należy zastosować systemową blokadę komputera, laptopa lub innego elektronicznego nośnika informacji. • Przy opuszczaniu miejsca pracy należy zachować „zasadę czystego biurka" - nośniki informacji umieścić w szafach, szufladach i innych do tego przeznaczonych miejscach oraz upewnić się, że pokój jest zamknięty, gdy jesteśmy jedyną osobą opuszczającą pomieszczenie.

				• Nośniki elektroniczne zawierające informacje podlegające ochronie, poza miejscem pracy należy zabezpieczyć za pomocą środków kryptograficznych. • Poza miejscem pracy, szczególnie w miejscach publicznych unikać należy rozmów dotyczących informacji służbowych podlegających ochronie. • Hasła dostępowe do konta pocztowego, systemów informatycznych należy chronić przed dostępem osób trzecich. Nie zaleca się zapamiętywania ich w przeglądarkach internetowych. • Po zakończeniu pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy. • Nie należy przesyłać informacji służbowych z wykorzystaniem prywatnych nośników oraz wykorzystywać służbowych urządzeń (tj. komputerów, laptopów, telefonów) do prywatnych celów. • Przed zalogowaniem się do systemu stacji roboczej należy upewnić się, że w pobliżu nie ma osób trzecich lub urządzeń nagrywających mogących zarejestrować hasła dostępowe do systemów, z których zamierzamy skorzystać. Jeśli występuje takie zagrożenie należy zastosować szczególne środki ostrożności uniemożliwiające zarejestrowanie wpisywanego hasła. 6) USTANOWIENIE PODSTAWOWYCH ZASAD GWARANTUJĄCYCH BEZPIECZNĄ PRACĘ PRZY PRZETWARZANIU MOBILNYM I PRACY NA ODLEGŁOŚĆ USTALENIA ZASAD POSTĘPOWANIA Z INFORMACJAMI, ZAPEWNIAJĄCYCH MINIMALIZACJĘ WYSTĄPIENIA RYZYKA KRADZIEŻY INFORMACJI I ŚRODKÓW PRZETWARZANIA INFORMACJI, W TYM URZĄDZEŃ MOBILNYCH W w/w zakresie przedstawiono obszerny materiał informacyjny. Mnogość i różnorodność danych pochodzących z internetu, nośników przenośnych czy nowo zainstalowanego oprogramowania jest zazwyczaj źródłem niepożądanych programów, których działanie może przyczynić się w wydatny sposób do utraty poufności, a w rzadkich przypadkach do fizycznego zniszczenia danych znajdujących się w komputerze.

				Pracodawca nie może bagatelizować działań swoich podwładnych związanych z pobieraniem plików w sieci, zwłaszcza gdy są to treści objęte prawem autorskim. Pracodawca, jest zobowiązany do przestrzegania prawa, pomimo panującego w znacznej części społeczeństwa liberalnego podejścia do kwestii ochrony praw autorskich i np. wprowadzić blokadę ściągania poprzez www nielegalnych filmów fabularnych i muzyki. Poważnym zagrożeniem jest wyciek wrażliwych danych - o interesantach, transakcjach czy finansach - za pośrednictwem poczty elektronicznej, powodowany przez pracowników. To właśnie przez firmową skrzynkę pocztową dociera do firmy większość szkodliwych programów, chociaż nie jest to jedyny problem. Coraz częściej programy z wbudowanymi ukrytymi funkcjami, które pozwalają przejąć kontrolę nad komputerem i wykraść dane - występują pod postacią darmowych, pozornie pożytecznych programów, które pracownicy sami pobierają z Internetu i instalują na firmowym komputerze. Systemy pocztowe muszą być chronione przed tego rodzaju zagrożeniami, a także zabezpieczane na wypadek awarii. Spam ciągle jest zjawiskiem bardzo dokuczliwym, a jednym ze sposobów walki z tym zjawiskiem są bramy zarządzające ruchem przenoszącym spam, ograniczające zakres pasma sieci, jaki ruch ten może wykorzystać. Urządzenie wpięte do sieci pomiędzy serwerami pocztowymi i internetem klasyfikuje ruch pocztowy, opierając się na historii spamu związanej z adresem źródła. W walce z wyciekiem danych stosowane są specjalne rozwiązania do monitorowania wrażliwej informacji i blokowania poczty wychodzącej, w której stwierdzono jej obecność. Najczęstsze nadużycia internetu: • robienie zakupów w sklepach i serwisach aukcyjnych, • naruszanie praw autorskich (nielegalne pobieranie bądź udostępnianie plików), • marnotrawienie czasu na przeglądaniu stron www niezwiązanych z pracą, • infekowanie sieci firmowej wirusami pobieranymi z plikami z internetu, • korzystanie z poczty elektronicznej w sprawach prywatnych. Ponadto wiele podmiotów wciąż nie traktuje komunikatorów jako potencjalnego zagrożenia bezpieczeństwa. Tego typu

				oprogramowanie pozwala na prowadzenie swobodnych rozmów, a z tego względu, że komunikacja odbywa się w trybie pisanym, użytkownik nabiera przekonania, iż nie jest ani podsłuchiwany, ani kontrolowany. W tych okolicznościach często dochodzi do nawiązywania dość bliskich znajomości i prowadzenia całkiem zażyłych konwersacji, podczas których przez nieuwagę ujawniane mogą być poufne dane. Pracownikom może zdarzyć się przesłać ważne wiadomości nie do tego odbiorcy, co trzeba - jeśli jest to osoba z tej samej jednostki, nie jest jeszcze tak źle, gorzej, gdy informacja wydostaje się na zewnątrz. Mało oficjalne pogawędki internetowe prowadzą również do sytuacji, kiedy nie zdając sobie z tego sprawy, można powiedzieć o jedno słowo za dużo i w ten sposób udostępnić informację traktowaną w jednostce jako tajemnicę. Częściej jednak zdarza się, że pracownicy wymieniają się takimi informacjami/tajemnicami, bo zwyczajnie nie wiedzą bądź nie zdają sobie sprawy z faktu, że są to dane tajne. W tym przypadku wina leży po stronie pracodawcy, który zaniechał obowiązku przeszkolenia pracownika w kwestiach polityki bezpieczeństwa. Tak jak w przypadku kontroli poczty elektronicznej, pracownik musi zostać poinformowany o tym, jaka jest polityka firmy, jeśli chodzi o przeglądanie stron www. Są jednak jednostki, które nie tyle zakazują przeglądania pewnych witryn, ile je blokują. Niewątpliwie opcja filtrowania przeglądanych zawartości zapobiega przedostawaniu się do sieci wewnętrznej elementów potencjalnie niebezpiecznych. Pozwala to w prosty sposób wyeliminować zbędny ruch w sieci lokalnej i odciążyć pracujące w niej systemy. Coraz bardziej zwiększa się skala problemu, który dotyczy użytkowników korzystających z internetu podczas pracy. Liczba zagrożeń związanych z wykorzystywaniem internetu w pracy powoduje, że prowadzenie ciągłego monitoringu bezpieczeństwa systemu teleinformatycznego jest koniecznością. Zagrożenia związane są głównie z ochroną informacji, złośliwym oprogramowaniem oraz próbami przełamania stosowanych zabezpieczeń. Monitoring powinien skupiać się na ocenie zagrożeń oraz wykrywaniu incydentów, a nie jedynie na kontroli aktywności pracowników. Ważne jest jasne zdefiniowanie polityki bezpieczeństwa i procedur określających zasady postępowania z informacjami oraz korzystania z internetu. Dzięki temu pracownicy wykorzystują w sposób świadomy dostęp do zasobów internetu, przy zachowaniu zasad bezpieczeństwa.

				Wszyscy zatrudnieni powinni zostać zobowiązani do znajomości zasad korzystania z internetu oraz poczty elektronicznej i przestrzegania ich w codziennej pracy. Dostęp do internetu powinni mieć pracownicy, którzy wykorzystują go w pełnieniu obowiązków służbowych. Stosowane powinno być także zaawansowane filtrowanie treści, eliminujące ryzyko związane z odwiedzaniem przez pracowników niebezpiecznych witryn. Używane powinny być systemy ochrony antywirusowej i wykrywania włamań. Opierając się na tych systemach, prowadzony byłby całodobowy monitoring bezpieczeństwa systemu teleinformatycznego, który obejmowałby także ryzyko związane z dostępem pracowników do internetu. Przy takim podejściu kontrola aktywności pracowników byłaby przeprowadzana tylko w uzasadnionych przypadkach. Gdy podejrzewałoby się naruszenie obowiązujących zasad bezpieczeństwa, prowadzący postępowanie wyjaśniające mógłby uzyskać dostęp do logów z www systemów oraz z systemu rejestrującego połączenia z internetem. W sprawozdaniu przedstawiono także interpretację Ministerstwa Finansów dotyczącą audytu bezpieczeństwa informacji: Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji. Zawarte w sprawozdaniu rady, określenie ryzyk i zalecenia pomagające zabezpieczyć system komputerowy przez niepowołanym dostępem, próbami manipulowania danymi czy ich zniszczeniem, do których może zastosować się przeciętny użytkownik, aby osiągnąć minimalny poziom bezpieczeństwa – nie pozwolą danym ani systemowi stać się całkowicie bezpiecznym, ale mogą stać się podstawą ogólnego zabezpieczenia. Wiele zagrożeń dla informacji może być znacznie ograniczone przez podjęcie odpowiednich działań. Główne zasady systemów zarządzania i kontroli przewidują wyraźne zdefiniowanie zadań i podział funkcji. Kryteria mające szczególnie istotne znaczenie przy ocenie systemu kontroli wewnętrznej to: 1) istnienie pisemnych procedur, 2) podział obowiązków, 3) czynności kontrolne,

				4) bezpieczeństwo i ochrona danych. Celem niniejszego audytu była analiza czy system jest właściwie chroniony przed niepożądanymi zdarzeniami, natomiast w wypadku ich wystąpienia są one na czas wykrywane, a skutki ich na bieżąco korygowane. W oparciu o przeprowadzoną analizę, ryzyka audytor wewnętrzny przeprowadził przedmiotowy audyt w obszarach najistotniejszych dla realizacji celów jednostki. Analizę systemu dokonano w oparciu o należytą staranność (standardy audytu wewnętrznego) i wiedzę audytora wewnętrznego w badanym zakresie. W sprawozdaniu przedstawiono charakterystykę wybranego na podstawie analizy obiektu audytu. Na postawie ustaleń oraz analizy przyczyn i skutków uchybień, audytor sugeruje wykonanie działań wskazanych w sprawozdaniu. Zaprezentowano szereg pozytywnie wykonywanych czynności dotyczących poprawy funkcjonowania kontroli zarządczej, ale też zagrożeń/ryzyk, które mogą mieć negatywny wpływ na organizację. Podsumowując, audytor udziela zapewnienia, że w wystarczającym stopniu funkcjonuje adekwatna, skuteczna i efektywna kontrola zarządcza.

4.	Funkcjonowanie kontroli zarządczej w jednostkach organizacyjnych podległych Gminie Brusy	(D)	Wzrost efektywności i skuteczności działania	Zakres działalności, jaki poddany został audytowi wewnętrznemu to działania, procesy i procedury, do których odnoszą się zapisy art. 68 – 71 ustawy o finansach publicznych oraz standardy kontroli zarządczej. Ocena konstrukcji mechanizmów i systemu kontroli polegała na analizie i identyfikacji kluczowych kontroli oraz weryfikacji atutów i słabości kontroli. Jako główne obiekty audytu wyróżniono: 1) analizę systemu kontroli zarządczej – zgodność wewnętrznych procedur oraz zasad postępowania ze standardami kontroli zarządczej, 2) samoocenę kontroli zarządczej, 3) zarządzanie ryzykiem, 4) oświadczenia o stanie kontroli zarządczej. Zasady i mechanizmy funkcjonowania poszczególnych procesów zostały opracowane w postaci opisowej i tabelarycznej. Potwierdzenie zawartych ustaleń dokonano poprzez użycie niżej wymienionych technik: analiza zgodności procesów z procedurami, kwestionariusz samooceny kontroli zarządczej, badanie dokumentów źródłowych, rozmowy z pracownikami, badanie istniejących mechanizmów kontroli, testowanie zgodności posiadanych informacji z rzeczywistością, uzupełniające informacje w stosunku do informacji zgromadzonych za pomocą innych technik w celu ich potwierdzenia, uzupełnienia, wyjaśnienia dla pozyskania wystarczających dowodów badania, sprawdzenie zgodności z przepisami prawa, oświadczenia o stanie kontroli zarządczej. Czynniki ryzyka w zakresie zarządzania niniejszym obszarem mogą być następujące: 1) brak lub nieskuteczna kontrola wewnętrzna, 2) nieprzestrzeganie obowiązujących przepisów, 3) brak procedur wewnętrznych, 4) nieskuteczne realizowanie wewnętrznych procedur, 5) nie zapoznanie pracowników z wewnętrznymi procedurami, 6) złożoność procedur, 7) czynnik ludzki - pomyłki i niedopatrzenia, 8) niezgodne z obowiązującymi przepisami wykonywanie obowiązków, 9) brak procedur bezpieczeństwa bądź ich lekceważenie, 10) dostęp do dokumentów przez osoby nieupoważnione, 11) brak systemu wyznaczania celów i zadań dla jednostki, komórek organizacyjnych,

				12) brak skutecznego monitoringu realizacji celów i zadań, 13) niewłaściwa jakość pracy, 14) brak skutecznego systemu sprawozdawania o realizacji celów jednostki, 15) błędy w sporządzanych sprawozdaniach, 16) przypadki wystąpienia znacznych strat w majątku jednostki, spowodowane np. dostępem osób nieuprawnionych, 17) utrata informacji chronionych (niejawne, tajemnica, dane osobowe), 18) brak polityki bezpieczeństwa informacji lub jej nieprzestrzeganie, 19) brak odpowiednich zabezpieczeń informacji, systemów informatycznych i dokumentów, 20) brak przestrzegania i promowania zasad etycznego postępowania, 21) brak efektywności i skuteczności przepływu informacji, 22) brak formalnego systemu zarządzania ryzykiem, 23) brak identyfikacji i radzenia sobie z pojawiającymi się ryzykami, 24) brak wykorzystania szans pojawiających się w otoczeniu, 25) możliwość pominięcia istotnych zagadnień, a w konsekwencji brak właściwej reakcji na ryzyko, 26) niewłaściwa hierarchizacja rodząca ryzyko niewłaściwej reakcji oraz podjęcia odpowiednich działań kontrolnych, 27) nienależyta reakcja na ryzyko oraz nieadekwatność mechanizmu kontrolnego do poziomu ryzyka, 28) brak polityk, procedur, rejestrów ryzyka, 29) brak określenia akceptowalnego poziomu ryzyka, 30) brak świadomości pracowników dot. osiągania wyznaczonych celów i zadań, 31) nieprawidłowe definiowanie celów i zadań, 32) brak zdefiniowanych mierników realizacji celów i zadań. Obowiązująca od 1 stycznia 2010 r. ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych wprowadziła nowy rodzaj kontroli – kontrolę zarządczą. Należy zwrócić uwagę, że art. 69 ust. 1 ustawy o finansach publicznych nakłada na kierownika jednostki sektora finansów publicznych obowiązek zapewnienia funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej. Adekwatność kontroli zarządczej oznacza dostosowanie funkcjonujących rozwiązań, przede wszystkim, do rozmiaru organizacji i zakresu wykonywanych zadań. Skuteczność kontroli zarządczej oznacza koncentrację na zapewnianiu osiągania przez organizację jej celów. Efektywność kontroli zarządczej oznacza jej sprawność – dobre działanie wszystkich jej elementów

				opisanych w standardach kontroli zarządczej połączone z minimalizowaniem poświęconych temu nakładów. Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Zapewnienie osiągnięcia celów i zadań oznacza nacisk na skuteczność działania. W myśl powyższej definicji cele organizacji mają być osiągnięte w sposób: 1) zgodny z prawem, 2) efektywny, co oznacza zapewnienie najlepszej możliwej relacji pomiędzy ponoszonymi nakładami i osiąganymi efektami, 3) oszczędny, co oznacza zapewnienie najniższego możliwego kosztu realizacji celów i zadania przy założeniu odpowiedniej jakości wykonania, 4) terminowy, co oznacza wykonanie celów i zadań w odpowiednim czasie bez wzrostu nakładów lub utraty jakości. Kontrola zarządcza w Gminie Brusy zorganizowana jest na dwóch poziomach: 1) I poziom – jest to podstawowy poziom kontroli zarządczej realizowanej przez jednostki organizacyjne Gminy Brusy. Za funkcjonowanie kontroli zarządczej w jednostkach organizacyjnych odpowiedzialni są Kierownicy/Dyrektorzy, 2) II poziom – to kontrola jednostek organizacyjnych Gminy Brusy w zakresie nadzoru. Celem prowadzonej kontroli zarządczej jest zapewnienie: 1) zgodności działania z przepisami prawa oraz procedurami wewnętrznymi, 2) skuteczności i efektywności działania, 3) wiarygodności sprawozdań, 4) ochrony zasobów, 5) przestrzegania i promowania zasad etycznego postępowania, 6) efektywności i skuteczności przepływu informacji, 7) zarządzania ryzykiem. Ogólne wskazówki dotyczące zasad budowania systemów kontroli zarządczej w sektorze finansów publicznych zostały wydane w Komunikacie Ministra Finansów w sprawie standardów kontroli zarządczej dla sektora finansów publicznych, który ukazał się w Dzienniku Urzędowym Ministra Finansów nr 15, pozycja nr 84 z dnia 30 grudnia 2009 r. oraz na stronie internetowej Ministerstwa

				Finansów. W roku 2011 wydane zostały wytyczne w zakresie samooceny kontroli zarządczej dla jednostek sektora finansów publicznych. Natomiast pod koniec grudnia 2012 r. Minister Finansów wydał Wytyczne w zakresie planowania i zarządzania ryzykiem. W trakcie realizacji audytu dokonano weryfikacji działań w celu potwierdzenia efektywności wdrożonych systemów zarządzania i kontroli. Przeprowadzony audyt systemów zarządzania i kontroli skierowany był głównie na określenie, czy systemy działają efektywnie w celu zapobiegania nieprawidłowościom oraz czy tam gdzie mogą pojawić się ewentualne błędy i nieprawidłowości, systemy efektywnie wykryją je i skorygują. Ocena konstrukcji mechanizmów kontroli i systemu kontroli polegała na identyfikacji celów, analizie konkretnych ryzyk, identyfikacji kluczowych kontroli, ocenie atutów i słabości kontroli oraz dokonaniu oceny systemu kontroli. Przedstawiona w sprawozdaniu opinia audytora jest rezultatem zebranych dowodów oraz własnego osądu. Opiera się o procedury audytowe oraz ustalone fakty i ma na celu poszukiwanie możliwości ewentualnych usprawnień. Zgodnie z udzielonymi pisemnie informacjami, w każdej Jednostce odpowiedzialność za funkcjonowanie kontroli zarządczej ponosi Dyrektor Jednostki. Nie powoływano koordynatorów kontroli zarządczej w osobie pracowników jednostek. Do jednostek organizacjach podległych Gminie Brusy zostało skierowane pismo z prośbą o wypełnienie zestawienia: „Analiza systemu kontroli zarządczej – zgodność wewnętrznych procedur ze standardami kontroli zarządczej". Dyrektorów Jednostek poproszono także o uzupełnienie Kwestionariusza kontroli wewnętrznej. **<u>Analiza systemu kontroli zarządczej – zgodność wewnętrznych procedur oraz zasad postępowania ze standardami kontroli zarządczej:</u>** W zaleceniach wskazano, że Jednostki organizacyjne podległym Gminie Brusy powinny zapoznać się z katalogiem procedur odnoszących się do poszczególnych standardów kontroli zarządczej – zaprezentowanym szczegółowo w sprawozdaniu z audytu.

				Ponadto należy przypomnieć o konieczności systematycznego sprawdzania wewnętrznych procedur pod kątem ich zgodności z obowiązującymi przepisami prawa. Uwagę należy zwracać przede wszystkim na podstawy prawne, jakie wskazano w treści wewnętrznych procedur. Nie można uznać za obowiązującą procedury wskazującej w podstawie prawnej np. ustawę o finansach publicznych z 2005 r. ponieważ ustawa ta została całkowicie zmieniona wydaną w roku 2009 ustawą o finansach publicznych. Dodać należy także o konieczności analizy wewnętrznych procedur wskazujących wprost z imienia i nazwiska lub stanowiska, osoby powołane do wykonywania określonych czynności. Audytor niejednokrotnie spotykał się w swojej pracy z utrzymywaniem, przez Dyrektorów Jednostek, za aktualne procedur wskakujących osoby nie będące pracownikami Jednostki (np. z powodu przejścia na emeryturę/zwolnienia z pracy, a nawet osoby nieżyjące). Zdaniem audytora przegląd procedur powinien następować przynajmniej raz w roku przed podpisaniem oświadczenia o stanie kontroli zarządczej. W sprawozdaniu przedstawiono szczegółową analizę zagadnień do każdego Standardu kontroli zarządczej, wskazującą podjęte w Jednostkach procedury. Wskazano też ewentualne procedury odnoszące się do Standardów, które w kolejnych latach mogłyby być w Jednostkach wprowadzane. <u>Przestrzeganie wartości etycznych</u> Przykładem wewnętrznej procedury jaką dodatkowo można podjąć w zakresie opisywanego standardu jest procedura przeciwdziałania mobbingowi. <u>Kompetencje zawodowe</u> Jednostkom przypomina się o konieczności systematycznej aktualizacji (w razie potrzeb) zakresów czynności i odpowiedzialności pracowników. <u>Misja</u> <u>Określanie celów i zadań, monitorowanie i ocena ich realizacji</u> <u>Identyfikacja ryzyka</u> <u>Analiza ryzyka</u> <u>Reakcja na ryzyko</u> Jednostki powinny niezwłocznie wprowadzić procedury regulujące zasady zarządzania ryzykiem.

				Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych Wprowadzić można procedury regulujące m.in.: 1) zasady wstępnej oceny celowości zaciągania zobowiązań i zasad dokonywania wydatków, 2) procedury udzielanie zamówień publicznych, 3) procedury używania do celów służbowych samochodów osobowych nie będących własnością pracodawcy. Mechanizmy kontroli dotyczące systemów informatycznych Przypomina się, że od 25 maja 2018 r. w ochronie danych osobowych nic nie będzie już takie samo. Firmy i urzędy/jednostki muszą spełnić szereg restrykcyjnych wymogów. Za ich niespełnienie można zapłacić karę. Rozporządzenie o Ochronie Danych Osobowych (RODO), to nowe unijne prawo, które w zupełnie inny, niż dotychczas, sposób definiuje zasady przetwarzania, wykorzystywania i przechowywania danych osobowych. Trzeba je wdrożyć do 25 maja przyszłego roku. Przepisy obejmują wszystkie podmioty, które gromadzą i wykorzystują dane dotyczące osób fizycznych. Nadchodzące zmiany będą dotyczyły zarówno firm, jak i administracji. Co ważne – RODO będą musiały wdrożyć wszystkie organy administracji publicznej. Zarówno te duże firmy, czy urzędy jak i te małe kilku - czy kilkunastoosobowe firmy, sklepy internetowe, szkoły, ośrodki pomocy społecznej czy domy kultury itp. muszą przetwarzać dane osobowe zgodnie z prawem. Nowe przepisy wprowadzają szereg obowiązków, nowe rodzaje odpowiedzialności ale też sankcje finansowe. **Samoocena kontroli zarządczej** Analizując zagadnienia samooceny kontroli zarządczej przeprowadzanej w Jednostkach organizacyjnych podległych Gminie Brusy, stwierdzić należy że: 1) we wszystkich Jednostkach przeprowadzona została samoocena kontroli zarządczej, 2) metodą przeprowadzenia samooceny było wykorzystanie do tego celu ankiet, 3) ankiety zostały skierowane do Dyrektora Jednostki, jedynie w dwóch Jednostkach ankiety zostały skierowane do pracowników placówki.

				Przypomina się, że samoocena kontroli zarządczej, to proces, w którym dokonywana jest ocena funkcjonowania kontroli zarządczej przez pracowników i kierownictwo jednostki. Jak wynika z odpowiedzi udzielonych w KKW, w zdecydowanej większości Jednostek wypełniane są jedynie przez Dyrektora placówki. Poprzez udział w procesie samooceny pracownicy jednostki są bezpośrednio zaangażowani w ocenę ryzyka i mechanizmów kontroli, co może przyczyniać się do stałego doskonalenia systemu kontroli zarządczej, w tym zarządzania ryzykiem. Należy bowiem pamiętać, że w jednostce zawsze istnieją obszary, które mogą lepiej i sprawniej funkcjonować, a samoocena może te obszary wskazywać. Jest to narzędzie, które w stosunkowo krótkim czasie może dać ogólny obraz funkcjonowania kontroli zarządczej. Za cel przeprowadzania samooceny można uznać fakt, iż jej wyniki mogą być jednym ze źródeł wiedzy o funkcjonowaniu kontroli zarządczej, będących podstawą do podpisania oświadczenia o stanie kontroli zarządczej. **<u>Zarządzanie ryzykiem</u>** W Jednostkach nie prowadzi się identyfikacji i analizy ryzyka, tym, samym brak informacji czy określenie w latach poprzednich ryzyka i sposobu reakcji na ryzyko pozwoliło go uniknąć lub zminimalizować w kolejnych latach. Nie sporządza się okresowych sprawozdań z przebiegu zarządzania ryzykiem. Jednostki powinny niezwłocznie wprowadzić procedury regulujące zasady zarządzania ryzykiem. Na dokumentację dot. zarządzania ryzykiem składać się powinna: 1) procedura zarządzania ryzykiem, 2) dokumentacja związana z analizą ryzyka prowadzoną co najmniej raz w roku, której efektem finalnym jest rejestr ryzyka, 3) roczny raport dot. zarządzania ryzykiem.

				Celem dokumentacji związanej z analizą ryzyka powinno być określenie: 1) listy głównych celów i zadań w odniesieniu do działalności jednostki, 2) sposobu postępowania przy identyfikowaniu i analizie ryzyka, 3) sposobu postępowania ze zidentyfikowanym ryzykiem, 4) zakresu przeglądu ryzyka i sprawozdawczości, 5) sposobu praktycznego zarządzania ryzykiem, 6) struktury zarządzania ryzykiem, w tym danych o wszystkich zespołach i osobach ponoszących odpowiedzialność za ryzyko, 7) sposobu oceny procesu zarządzania ryzykiem. Wynikiem corocznego raportu powinny być zmiany lub usprawnienia kluczowych elementów podstaw zarządzania ryzykiem w jednostce. Roczny raport opierać się powinien na analizie sukcesów i porażek w dziedzinie zarządzania ryzykiem. W sprawdzaniu przedstawiono szczegółowy opis dot. procesu zarzadzania ryzykiem – celem zapoznania. Nowoczesne zarządzanie jednostką zmusza, aby patrzeć z wyprzedzeniem w przyszłość, być dynamiczne, reagować na zmiany i optymalnie wykorzystywać dostępne możliwości. Zarządzanie ryzykiem stanowi podstawę takiego działania. Coraz powszechniej uznaje się, iż zarządzanie ryzykiem może pomóc organizacji w poprawie jakości świadczenia usług i wykorzystaniu dostępnych możliwości. Oczekiwania wobec sektora publicznego są takie, że zgodnie ze swoim ustawowym zobowiązaniem sektor ten będzie zarządzał ryzykiem i tym samym chronił środki publiczne. Zarządzanie ryzykiem to zadanie każdego pracownika, nie tylko nielicznych specjalistów. Proces ten należy postrzegać jako podstawowy obowiązek zarządzających, którzy powinni zachęcać pracowników świadczących usługi do stosowania podejścia opartego na świadomości występowania ryzyka. **<u>Oświadczenie o stanie kontroli zarządczej</u>** Składanie oświadczeń o stanie kontroli zarządczej ma na celu podkreślenie roli i znaczenia kontroli zarządczej w skutecznym zarządzaniu jednostkami sektora finansów publicznych oraz podkreślenie odpowiedzialności osób składających oświadczenia za funkcjonowanie adekwatnej, skutecznej i efektywnej kontroli zarządczej.

				W sprawdzaniu przedstawiono szczegółowy opis dot. sporządzania oświadczeń o stanie kontroli zarządczej – celem zapoznania. W trakcie realizacji działań audytor dokonał weryfikacji przedsięwzięć w celu potwierdzenia efektywności wdrożonych systemów zarządzania. Ocena konstrukcji mechanizmów kontroli i systemu kontroli polegała na identyfikacji celów, analizie konkretnych ryzyk, identyfikacji kluczowych kontroli, ocenie atutów i słabości kontroli oraz dokonaniu oceny systemu kontroli. Przedstawiona w niniejszym dokumencie opinia audytora jest rezultatem zebranych dowodów oraz własnego osądu i opiera się o procedury audytowe i ustalone fakty. Analizę systemu dokonano w oparciu o należytą staranność (standardy audytu wewnętrznego) i wiedzę audytora wewnętrznego w badanym zakresie. Podsumowując, z uwagi na brak realizacji zagadnień dotyczących zarzadzania ryzykiem w kilku Jednostkach podległych Gminie Brusy, nie sposób uznać że w wystarczającym stopniu funkcjonuje adekwatna, skuteczna i efektywna kontrola zarządcza. W niniejszej opinii przedstawiono charakterystykę wybranych na podstawie analizy - 4 obiektów audytu. Zaprezentowano szereg pozytywnie wykonywanych czynności dotyczących poprawy funkcjonowania kontroli zarządczej, ale też nieprawidłowości, które mogą mieć negatywny wpływ na organizację. Wprowadzenie zaprezentowanych zaleceń ma za zadanie przyczynić się do usprawnienia opisywanych procesów. Audyt stanowi diagnozę stanu istniejącego oraz projekt rozwiązań poprawiających funkcjonowanie kontroli zarządczej.

5. Niezrealizowane zaplanowane zadania audytowe

Lp.	*Temat zadania zapewniającego, lub przedmiot czynności doradczej*	*Zadanie zapewniające (Z), czynność doradcza (D)*	*Przyczyna niezrealizowania zadania*
1.	----	----	---

7. Inne istotne informacje związane z funkcjonowaniem audytu wewnętrznego w jednostce w roku poprzednim, w tym dotyczące przeprowadzenia oceny wewnętrznej i zewnętrznej audytu wewnętrznego

------- ----- -----

.....

30.11.2017 r.

.....
(data)

AUDYTOR

.....
(podpis audytora wewnętrznego)

30.11.2017 r.

.....
(data)

BURMISTRZ

dr inż. Witold Ossowski

.....
(podpis Burmistrza)