Załącznik nr 1

do Procedury zarządzania ryzykiem

Kwestionariusz zarządzania ryzykiem

.....

Nazwa komórki organizacyjnej

Cele i zadnia komórki organizacyjnej	**Identyfikacja ryzyka**	**Analiza ryzyka**		**Reakcja na ryzyko**	**Nadzór i monitorowanie**
		Wpływ	prawdopodobieństwo		
1	2	3	4	5	6

Data sporządzenia .....

Podpis i pieczęć osoby sporządzającej .....

Instrukcja:

1. Należy wpisać najważniejsze cele i zadania komórki organizacyjnej.
2. Należy zidentyfikować ryzyka towarzyszące celom i zadaniom.

3 i 4. Należy dokonać analizy ryzyka, czyli wpływu zidentyfikowanego ryzyka na działanie komórki lub jednostki wpisując odpowiednią wagę wpływu oraz określić wagę prawdopodobieństwa wystąpienia ryzyka.

Wpływ	**Waga wpływu**
Nieznaczny	1
Mały	2
Średni	3
Poważny	4
Katastrofalny	5

Prawdopodobieństwo	**Waga prawdopodobieństwa**
Rzadkie	1
Mało prawdopodobne	2
Średnie	3
Prawdopodobne	4
Prawie pewne	5

5. Należy określić działania które zostały podjęte lub należy podjąć w celu zmniejszenia danego ryzyka do akceptowanego poziomu, np.: wdrożenie odpowiednich mechanizmów kontrolnych

   Reakcja na ryzyko może przybierać formy:

   a) zmniejszenia ryzyk, np.: poprzez zaprojektowanie i wdrożenie mechanizmów kontroli;

b) przeniesienia ryzyk, np.: wykupienie ubezpieczeń;
c) akceptacji istniejącego ryzyka.

Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do akceptowanego poziomu poprzez zmniejszenie prawdopodobieństwa jego ziszczenia się. W celu określenia metody przeciwdziałania ryzyku należy przeanalizować:

- przyczyny ryzyka i możliwe scenariusze rozwoju wydarzeń;
- istnienie mechanizmów kontroli stosowanych w celu ograniczenia lub uniknięcia tego ryzyka;
- skuteczność istniejących mechanizmów kontroli, tj. zakres w jakim przeciwdziałają ryzyku, a poprzez to ułatwiają realizację ustalonych celów i zadań.

6. Należy wpisać, w jaki sposób monitorowane jest zidentyfikowane ryzyko

Monitoring ryzyka obejmuje:

- przynajmniej raz w roku wykonanie przeglądu, w celu określenia czy pojawiły się nowe ryzyka; i czy uległy zmianie;
- sprawdzenie czy ocena ryzyka jest wciąż odpowiednia;
- zapewnienie skuteczności dotychczasowych mechanizmów kontroli;
- monitorowanie rozwoju uzgodnionych działań w zakresie zarządzania ryzykiem

Załącznik nr 2

do Procedury zarządzania ryzykiem

Rejestr ryzyk

Numer ryzyka	Właściciel ryzyka	Kategoria ryzyka	Opis ryzyka	W	P	Punktowa ocena ryzyka	Funkcjonujące mechanizmy kontrolne	Wymagane działania	Termin wykonania
1	2	3	4	5	6	7	8	9	10
1.									
2.									

Instrukcja:

Rejestr ryzyk sporządza się na podstawie „Kwestionariuszy zarządzania ryzykiem".

1. Należy wpisać odpowiednią liczbę porządkową oznaczającą zidentyfikowane ryzyko.

2. Należy wpisać nazwę komórki organizacyjnej Starostwa Powiatowego w Ząbkowicach Śląskich, która zidentyfikowała ryzyko i jest odpowiedzialna za jego monitoring.

3. Należy wpisać odpowiednią kategoria ryzyka tj. pogrupowane czynniki ryzyka np.: zewnętrzne, wewnętrzne, strategiczne tj.: polityczne, ekonomiczne, społeczne, technologiczne, legislacyjne, środowiskowe itp., operacyjne tj.: finansowe, prawne, zawodowe, umowne, technologiczne, środowiskowe itp.,

4. Należy krótko scharakteryzować zidentyfikowane ryzyko.

5. Należy wpisać wagę wpływu zidentyfikowanego ryzyka na działanie komórki lub jednostki

6. Należy wpisać wagę prawdopodobieństwa wystąpienia ryzyka.

7. Należy dokonać punktowej oceny ryzyka, którą jest iloczyn wpływu i prawdopodobieństwa.

8. Należy wyszczególnić wdrożone w komórce lub jednostce mechanizmy kontrolne.

9. Należy wpisać działania, które należy podjąć w celu ograniczenia ryzyka do akceptowanego poziomu.

10. Należy podać termin wykonania działań o których mowa w punkcie 9.

Załącznik nr 3

do Procedury zarządzania ryzykiem

Matryca punktowej analizy ryzyka

Wpływ	**waga**						
Katastrofalny	**5**	5	10				
Poważny	**4**	4	8	12			
Średni	**3**	3	6	8	10		
Mały	**2**	2	4	6	8	10	
Nieznaczny	**1**	1	2	3	4	5	
	0	**1**	**2**	**3**	**4**	**5**	**Waga**
		Rzadkie	**Mało prawdopodobne**	**Średnie**	**Prawdopodobne**	**Prawie pewne**	**Prawdopodobieństwo**

Instrukcja:

1. Matrycę punktowej analizy ryzyka sporządza się na podstawie Rejestru ryzyk.
2. Każde ryzyko należy umieścić w odpowiednim przedziale zgodnie z określonymi wagami wpływu i prawdopodobieństwa wystąpienia.
3. Ryzyka znajdujące się w obszarze zaznaczonym na czerwono, należy traktować jako ryzyka o największym prawdopodobieństwie wystąpienia i największym wpływie na komórkę lub jednostkę, w związku z powyższym należy objąć je szczególnym nadzorem.

Ryzyka znajdujące się w obszarze zaznaczonym na zielono, należy traktować jako ryzyka o najmniejszym prawdopodobieństwie wystąpienia i najmniejszym wpływie na komórkę lub jednostkę.

Hierarchizacja ryzyka;
Ocena ryzyka umożliwia uporządkowanie rodzajów ryzyka według ich wagi oraz przyznanych ocen. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa ziszczenia się ryzyka ustalany jest poziom istotności ryzyka:

a) **ryzyko poważne** – wymaga szybkiej reakcji. Ryzyko poważne charakteryzuje się
   - wpływem katastrofalnym i prawdopodobieństwem na poziomie: średnie, prawdopodobne lub prawie pewne,
   - wpływem poważnym i prawdopodobieństwem na poziomie: prawdopodobne lub prawie pewne,
   - wpływem średnim i prawdopodobieństwem na poziomie: prawie pewne.

b) **ryzyko umiarkowane** – należy omówić i monitorować. Ryzyko umiarkowane charakteryzuje się:
   - wpływem katastrofalnym i prawdopodobieństwem na poziomie: mało prawdopodobne i rzadkie,
   - wpływem poważnym i prawdopodobieństwem na poziomie: średnie, mało prawdopodobne i rzadkie,
   - wpływem średnim i prawdopodobieństwem na poziomie: prawdopodobne, średnie i mało prawdopodobne,
   - wpływem małym i prawdopodobieństwem na poziomie: prawie pewne, prawdopodobne i średnie,
   - wpływem nieznacznym i prawdopodobieństwem na poziomie: prawie pewne i prawdopodobne.

c) **ryzyko nieznaczne** – najniższe zagrożenie. Ryzyko nieznaczne charakteryzuje się:
   - wpływem średnim i prawdopodobieństwem na poziomie: rzadkie,
   - wpływem małym i prawdopodobieństwem na poziomie: mało prawdopodobne i rzadkie,
   - wpływem nieznacznym i prawdopodobieństwem na poziomie: średnie, mało prawdopodobne i rzadkie.

Iloczyn przyznanych konkretnemu ryzyku punktów wpływu i prawdopodobieństwa - łączna punktowa ocena ryzyka - pozwala na umiejscowienie go na mapie punktowej oceny ryzyka.

Załącznik
do Zarządzenia Nr 47/2011
Starosty Ząbkowickiego
z dnia 14.10.2011

Procedura zarządzania ryzykiem

§ 1

Określenia stosowane w niniejszej procedurze:

1. **ryzyko** - możliwość zaistnienia dowolnego zdarzenia, działania lub zaniechania działania, mierzone wpływem (siłą oddziaływania) oraz prawdopodobieństwem wystąpienia, które będzie miało wpływ na osiągnięcie celów i zadań jednostki, na kształtowanie jej wizerunku lub uszczuplenie jej majątku,

2. **czynnik ryzyka** – zdarzenie, działanie lub zaniechanie, które może spowodować wystąpienie ryzyka (przykładowe czynniki ryzyka zamieszczono w Załączniku nr 4 do niniejszej procedury),

3. **zarządzanie ryzykiem** - proces ograniczania ryzyka poprzez jego identyfikację, ocenę potencjalnego wpływu i prawdopodobieństwa wystąpienia oraz racjonalny dobór środków przeciwdziałających skutkom ryzyka; proces mający na celu optymalizację funkcjonowania komórki lub jednostki organizacyjnej,

4. **identyfikacja ryzyka** - przypisanie poszczególnych rodzajów czynników ryzyka do realizowanych celów i zadań,

5. **analiza ryzyka** - przypisanie dla każdego zidentyfikowanego ryzyka prawdopodobieństwa jego wystąpienia i dokonanie oceny jego wpływu na działanie komórki lub jednostki organizacyjnej,

6. **reakcja na ryzyko** - podjęcie adekwatnych, zasadnych, efektywnych i skutecznych działań (decyzji) zmierzających do ograniczenia lub wyeliminowania ryzyka,

7. **mechanizmy kontrolne** – procedury, instrukcje, wytyczne, standardy itp., których celem jest powstrzymanie lub minimalizacja negatywnych skutków ryzyka.

8. **nadzór i monitorowanie** - ciągła ocena skuteczności wprowadzonych działań, w tym badanie odstępstw i niezwłoczne reagowanie na nie,

§ 2

Do zadań kierowników komórek organizacyjnych w procesie zarządzania ryzykiem należy:

1. Określenie celów realizowanych przez podległe im komórki organizacyjne,

2. Zidentyfikowanie ryzyk, jakie mogą zagrozić osiągnięciu poszczególnych celów,

3. Analiza zidentyfikowanych ryzyk w celu określenia prawdopodobieństwa i możliwych skutków (efektów lub rezultatów) wystąpienia danego ryzyka,

4. Podjęcie działań w celu zmniejszenia wpływu i prawdopodobieństwa wystąpienia zidentyfikowanych ryzyk, tj. zastosowanie odpowiednich mechanizmów kontroli,

5. Dokumentowanie procesu analizy i oceny ryzyka poprzez wypełnienie *Kwestionariusza zarządzania ryzykiem* zgodnie ze wzorem zamieszczonym w załączniku nr 1 do niniejszej procedury,

6. Przekazanie Zespołowi ds. zarządzania ryzykiem *Kwestionariusza zarządzania ryzykiem* w terminie do końca stycznia każdego roku kalendarzowego,

7. Zgłaszanie Zespołowi postrzeganych zagrożeń nie związanych bezpośrednio z wykonywaną pracą, a dotyczących Jednostki.

§ 3

Do zadań Zespołu ds. zarządzania ryzykiem należy:

1. Weryfikacja otrzymanych od kierowników komórek organizacyjnych Kwestionariuszy zarządzania ryzykiem, tj.:

   1) analiza zidentyfikowanych ryzyk i reakcji na ryzyko,

   2) ocena adekwatności i efektywności zaproponowanych mechanizmów kontrolnych mających na celu ograniczenie ryzyka,

   3) ocena adekwatności i efektywności sposobu monitorowania ryzyka,

2. Sporządzenie *Rejestru ryzyk*, zgodnie ze wzorem zamieszczonym w załączniku nr 2 do niniejszej procedury,

3. Sporządzenie *Matrycy punktowej analizy ryzyka* zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszej procedury,

4. Przekazanie Staroście Ząbkowickiemu sprawozdania dotyczącego zarządzania ryzykiem do końca lutego każdego roku kalendarzowego,

5. Monitorowanie ryzyk o największym wpływie i prawdopodobieństwie wystąpienia oraz inicjowanie działań zmierzających do ich ograniczenia,

6. Informowanie Starosty Ząbkowickiego o najważniejszych ryzykach i działaniach podejmowanych w celu ich minimalizacji,

7. Okresowe przeglądy i aktualizacja *Rejestru ryzyk* oraz *Matrycy punktowej analizy ryzyka*.

Lista załączników do Procedury zarządzania ryzykiem:

Załącznik nr 1 – *Kwestionariusz zarządzania ryzykiem.*

Załącznik nr 2 - *Rejestr ryzyk.*

Załącznik nr 3 - *Matryca punktowej analizy ryzyka.*

Załącznik nr 4 – Przykładowe czynniki ryzk

Załącznik nr 4

do Procedury zarządzania ryzykiem

Przykładowe czynniki ryzyka

1. **Czynniki ryzyka dotyczące systemów informatycznych, w szczególności związane z:**

   1) utrzymaniem ciągłości pracy systemów informatycznych, np.: zatrzymanie pracy systemów informatycznych, brak przepływu informacji o błędach w systemach informatycznych,

   2) dostępem do zasobów informatycznych jednostki, np.: wypływ danych z systemów, włamania do systemów,

   3) wykorzystywaniem infrastruktury informatycznej, np.: awaria sprzętu, niedopasowanie systemów do bazy sprzętowej, wykorzystywanie nielegalnego oprogramowania,

   4) rozwojem i wdrożeniem nowych systemów informatycznych, np. nieuprawnione wdrożenie zmian w oprogramowaniu i bazach danych.

2. **Czynniki ryzyka o charakterze finansowym związane z:**

   1) wielkością środków finansowych jednostki, np.: zmiany wysokości dochodów, przychodów, środków z Unii Europejskiej, wydatków, rozchodów,

   2) płynnością finansową,

   3) inwestycjami, np.: niewłaściwe decyzje inwestycyjne, wzrost kosztów inwestycji, brak źródeł finansowania, opóźnienia w realizacji,

   4) nieproduktywną stratą środków, np.: oszustwo, kradzież, kary umowne, grzywny,

   5) sprawozdawczością finansową, np.: niedawne zmiany w systemie księgowania, częste zmiany pracowników odpowiedzialnych za sprawozdania.

3. **Czynniki ryzyka wynikające z charakteru prowadzonej działalności związane z:**

   1) działalnością podstawową jednostki, np.: stopień skomplikowania działalności, niewystarczające kompetencje pracowników, niedawne zmiany kluczowych pracowników, brak motywacji u pracowników,

2) przetwarzaniem informacji, np.: nieadekwatność informacji, na podstawie których podejmuje się decyzje, utrata informacji, naruszenie poufności informacji,

3) stabilnością działalności jednostki lub zatrudnienia, np.: ograniczenie lub znaczny wzrost zadań jednostki, zmiany procesów operacyjnych, decentralizacja działalności,

4) technologią, np.: zakłócenia w działaniu systemów informatycznych, powstanie nowych technologii, wdrażanie nowych technologii

5) projektami prowadzonymi przez jednostkę, np.: niewłaściwe planowanie projektu, wzrost kosztów realizacji projektu, opóźnienia w realizacji projektu, brak środków na realizację projektu, niepowodzenie projektu,

6) nowymi zadaniami i programami, np.: brak odpowiednich zasobów (środków finansowych, pracowników, wyposażenia, informacji), krótki termin realizacji, konieczność współpracy z innymi podmiotami,

7) innowacyjnością, np.: opór pracowników, brak skłonności do zmian, wdrażanie niesprawdzonych rozwiązań,

8) reputacją jednostki, np.: spadek reputacji na skutek niewłaściwego działania lub zaniedbań pracowników, niewłaściwej realizacji zadań przez jednostkę, złego zarządzania.

4. Czynniki sprzyjające wystąpieniu ryzyka związanego z zarządzaniem:

1) jakość zespołu zarządzającego, np.: niewystarczające kwalifikacje kierownictwa, częste zmiany na stanowiskach kierowniczych, zbyt mała liczba osób na stanowiskach kierowniczych,

2) organizacja jednostki, np.: nieadekwatna struktura organizacyjna, brak zakresów obowiązków kierownictwa i pracowników, nieefektywny system przepływu informacji, znaczne zmiany w zakresie odpowiedzialności kierownictwa,

3) zarządzanie zasobami ludzkimi, np.: niesprawiedliwa praktyka wynagradzania, niskie wynagrodzenia, brak działań motywujących pracowników, nie zapewnienie odpowiednich szkoleń, niewystarczające możliwości rozwoju zawodowego pracowników, nieefektywna rekrutacja.

5. Inne czynniki, mogące zwiększyć ryzyko:

1) niepowodzenia w osiąganiu celów w przeszłości, np.: niezrealizowanie projektu lub programu, przekroczenie planowanych wydatków, naruszenie lub obejście procedur kontrolnych, naruszenie prawa lub regulacji wewnętrznych,

2) czynniki ryzyka wrodzonego (wewnętrznego), np.: charakter działalności, wielkość jednostki, liczba pracowników, wielkość majątku trwałego, liczba transakcji, wielkość budżetu.

6. **Czynniki zewnętrzne związane z:**

1) infrastrukturą tj.: zakłócenia w dostawach energii, przerwy w łączności telefonicznej, przerwy w dostępie do Internetu i poczty elektronicznej,

2) zewnętrznymi warunkami ekonomicznymi tj.: zmiany stóp procentowych, kursów walut, inflacji, długu publicznego,

3) zmianami politycznymi tj.: zmiany na stanowiskach istotnych dla funkcjonowania jednostki,

4) środowiskiem prawnym, tj.: nowe przepisy prawa, zmiana przepisów, brak regulacji prawnej w danym zakresie, skomplikowane lub niejasne przepisy,

5) środowiskiem naturalnym, tj.: zanieczyszczenie środowiska, katastrofa ekologiczna, protesty społeczne,

6) „siłą wyższą", tj.: pożar, powódź, huragan,

7) innymi zagrożeniami i naciskami zewnętrznymi, tj.: działania przestępcze, terroryzm, presja polityczna, społeczna, naciski grup interesu, działalność lobbingowa,

8) dostawcami i usługodawcami, tj.: niestabilni dostawcy, monopolistyczna pozycja dostawców.

Baza przykładowych ryzyk

L.p.	Ryzyko	Czynniki ryzyka
1	Utrata danych z serwera jednostki	Wprowadzenie wirusa, atak hakerów, awaria systemu
2	Utrata danych osobowych pracowników/ klientów	Wirus w sieci, awaria systemu, awaria serwera, atak hakerów
3	Udostępnienie danych osobom nieuprawnionym	Umyślne działanie pracownika, brak procedur udostępniania danych oraz dostępu do danych, awaria systemu komputerowego, brak fizycznego zabezpieczenia dokumentów/ sprzętu komputerowego, złe ustawienie monitora komputera

4	Niezadowolenie klienta/ interesanta	Brak kompetentnej obsługi przez pracowników z powodu braku wiedzy/ braku procedur wykonywania danego zadania/ nieodpowiedniego zachowania pracownika/, Brak prawnych/ finansowych/ faktycznych/ fizycznych/ możliwości spełnienia oczekiwań klienta/ interesanta
5	Niewykonanie zadania	Nieuwaga pracownika, brak procedur realizacji zadania, nieprawidłowa informacja i komunikacja w jednostce, brak wiedzy/ umiejętności/ pracownika, awaria systemu komputerowego, awaria sprzętu, brak prądu, brak specjalistów z danego zakresu, brak środków finansowych, brak odpowiedniego sprzętu
6	Przekroczenie terminu realizacji zadania	Nieuwaga pracownika, brak procedur realizacji zadania, nieprawidłowa informacja i komunikacja w jednostce, awaria systemu komputerowego, awaria sprzętu, brak prądu
7	Sporządzenie sprawozdania finansowego niezgodnie z urządzeniami księgowymi	Nieuwaga pracownika, brak wiedzy pracownika, nieprawidłowa informacja i komunikacja w jednostce
8	Nieprawidłowe rozliczenie inwestycji	Nieuwaga pracownika, brak wiedzy pracownika, nieprawidłowa informacja i komunikacja wewnętrzna i zewnętrzna, niewywiązywanie się z umowy inspektora nadzoru inwestorskiego, zmowa wykonawcy i inspektora nadzoru, korupcja pracownika,
9	Dokonanie zamówienia publicznego niezgodnie z obowiązującym prawem	Nieuwaga pracownika, brak wiedzy pracownika, nieprawidłowa informacja i komunikacja wewnątrz jednostki, brak wykwalifikowanych pracowników, zmiana w przepisach dotyczących zamówień publicznych
10	Nieterminowe wykonanie inwestycji w stosunku do planu	Niesolidny wykonawca, brak nadzoru ze strony pracowników jednostki, niekorzystne warunki atmosferyczne, brak środków finansowych, roboty dodatkowe
11	Przesunięcie inwestycji w czasie	Brak wykonawców, brak środków

		finansowych, protesty społeczne
12	Brak środków finansowych na bieżącą działalność	Załamanie finansowania zewnętrznego, drastyczne zmniejszenie dochodów
13	Uszczerbek na zdrowiu pracownika/ klienta/ interesanta	Bbrak szkolenia BHP, nieprzestrzeganie obowiązujących zasad BHP, uszkodzone schody, niesprawne urządzenia/ wyposażenie, nieuwaga pracownika
14	Utrata/ uszkodzenie mienia	Kradzież, celowe zniszczenie, nieuwaga, pożar, zalanie, wichura, brak zabezpieczenia, brak procedur korzystania z powierzonego mienia
15	Strata finansowa/ dodatkowe koszty	Kradzież, wypłata odszkodowania, brak procedur wewnętrznych, brak nadzoru
16	Naruszenie obowiązującego prawa	Nieuwaga pracownika, niewiedza pracownika, częste zmiany przepisów powszechnie obowiązujących, brak wykwalifikowanych pracowników, zła organizacja pracy
17	Zakłócenie ciągłości działania jednostki	Brak systemu zastępstw, brak planów urlopów pracowników, zła organizacja pracy, awaria systemu informatycznego,
18	Utrata dobrego wizerunku	Niekompetentna obsługa klienta/ interesanta, zaniechanie rozpoczętej inwestycji
19	Zaciągnięcie zobowiązań planowany limit	Brak wykwalifikowanej kadry, brak procedur, brak kontroli zarządczej, brak zarządzania długiem
20	Naruszenie dyscypliny finansów publicznych	Nieznajomość prawa, brak wiedzy pracownika, brak szkoleń, nieprzestrzeganie procedur kontroli zarządczej, brak nadzoru ze strony kierownictwa, brak wykwalifikowanej kadry
21	Utrata wykwalifikowanych pracowników	Niskie płace, złe warunki pracy, konflikt z przełożonym/ pracownikami, zmiana miejsca zamieszkania
22	Duża rotacja pracowników	Zły system wynagradzania, zła organizacja pracy, brak możliwości awansu
23	Powódź	Brak zabezpieczeń/ wałów przeciwpowodziowych, brak systemu

		wczesnego ostrzegania, brak zbiornika retencyjnego
24	Błędne wprowadzenie do ksiąg rachunkowych kwoty wykazanej na fakturze	Nieuwaga pracownika, okresowe spiętrzenie zadań, celowe działanie pracownika, brak odpowiednich kwalifikacji pracownika
25	Błędy w planowaniu	Brak wykwalifikowanych pracowników, nieuwaga pracownika, brak nadzoru, brak odpowiednich procedur,
26	Niestosowanie procedur kontroli zarządczej	Sporządzenie procedur bez analizy ryzyka w jednostce, brak nadzoru i monitoringu ze strony przełożonych, niewiedza pracownika
27	Błędne zaksięgowanie operacji finansowej/ gospodarczej	Brak wiedzy pracownika, nieuwaga pracownika, brak nadzoru ze strony przełożonego, brak odpowiednich procedur wewnętrznych
28	Dokonanie podwójnej zapłaty dostawcy	Nieprawidłowa komunikacja wewnętrzna, nieuwaga pracownika, nieprawidłowe procedury sposobu regulowania zobowiązań,
29	Wydanie Decyzji z naruszeniem prawa	Nieuwaga pracownika, korupcja, brak wykwalifikowanych pracowników, zmiany w prawie
30	Niewprowadzenie korespondencji do systemu ewidencji	Nieuwaga pracownika, brak stosownych procedur, zagubienie korespondencji, spiętrzenie prac w jednym czasie
31	Niewykonanie remontu	Brak środków finansowych, nieujęcie remontu w planie, brak wykonawców, za mała ilość środków ujętych w planie,
32	Nieterminowe rozliczenie dotacji	Nieuwaga pracownika, brak procedur realizacji zadania, brak nadzoru, brak wiedzy pracownika, zła komunikacja wewnętrzna
33	Prowadzenie ewidencji księgowej z naruszeniem ustawy o rachunkowości	Duża rotacja pracowników, brak odpowiednio wykwalifikowanych pracowników, brak stosownych procedur wewnętrznych, brak podziału obowiązków, brak nadzoru
34	Przekroczenie określonego w ustawie limitu zadłużenia	Brak procedur wewnętrznych, brak prawidłowej komunikacji i informacji

		wewnętrznej, zmiana przepisów ustawowych, brak kompetentnych pracowników, brak zarządzania długiem
35	Niezgodne z przeznaczeniem wykorzystanie otrzymanej dotacji	Brak wiedzy pracownika, nieuwaga pracownika, brak procedur realizacji zadania, celowe działanie, za krótki termin na wykorzystanie dotacji