

Oświadczenie o stanie kontroli zarządczej

Ministra Finansów ¹⁾

za rok 2022

(rok, za który składane jest oświadczenie)

Dział ²⁾

Jako osoba odpowiedzialna za zapewnienie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej, tj. działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy, a w szczególności dla zapewnienia:

- zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi,
- skuteczności i efektywności działania,
- wiarygodności sprawozdań,
- ochrony zasobów,
- przestrzegania i promowania zasad etycznego postępowania,
- efektywności i skuteczności przepływu informacji,
- zarządzania ryzykiem,

oświadczam, że w **kierowanych przez mnie działach administracji rządowej: budżet, finanse publiczne, instytucje finansowe**

Część A ³⁾

w wystarczającym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

Część B ⁴⁾

w ograniczonym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

Zastrzeżenia dotyczące funkcjonowania kontroli zarządczej wraz z planowanymi działaniami, które zostaną podjęte w celu poprawy funkcjonowania kontroli zarządczej, zostały opisane w dziale II oświadczenia.

Część C ⁵⁾

nie funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.

Zastrzeżenia dotyczące funkcjonowania kontroli zarządczej wraz z planowanymi działaniami, które zostaną podjęte w celu poprawy funkcjonowania kontroli zarządczej, zostały opisane w dziale II oświadczenia.

Część D

Niniejsze oświadczenie opiera się na mojej ocenie i informacjach dostępnych w czasie sporządzania niniejszego oświadczenia pochodzących z: ⁶⁾

- monitoringu realizacji celów i zadań,
- samooceny kontroli zarządczej przeprowadzonej z uwzględnieniem standardów kontroli zarządczej dla sektora finansów publicznych⁷⁾,
- procesu zarządzania ryzykiem,
- audytu wewnętrznego,
- kontroli wewnętrznych,
- kontroli zewnętrznych,
- innych źródeł informacji:
 - Opinii Komitetu Audytu o funkcjonowaniu kontroli zarządczej w działach: budżet, finanse publiczne, instytucje finansowe w 2022 r.;
 - Sprawozdania z wykonania planu działalności Ministra Finansów za rok 2022 dla działów administracji rządowej: budżet, finanse publiczne, instytucje finansowe;
 - Raportu z realizacji kierunków działania i rozwoju Krajowej Administracji Skarbowej za rok 2022;
 - Sprawozdań z wykonania planów działalności: Centrum Informatyki Resortu Finansów za rok 2022, Polskiej Agencji Nadzoru Audytowego za rok 2022, Instytutu Finansów za rok 2022;
 - Oświadczeń o stanie kontroli zarządczej za rok 2022 – Dyrektora Generalnego Ministerstwa Finansów, Szefa Krajowej Administracji Skarbowej, Dyrektora Centrum Informatyki Resortu Finansów, Prezesa Polskiej Agencji Nadzoru Audytowego, Dyrektora Instytutu Finansów.

Jednocześnie oświadczam, że nie są mi znane inne fakty lub okoliczności, które mogłyby wpłynąć na treść niniejszego oświadczenia.

Magdalena Rzeczkowska

Minister Finansów

Warszawa, dnia 28 kwietnia 2023 r.
(miejscowość, data)

/-podpisano kwalifikowanym podpisem elektronicznym/

Dział II⁸⁾

1. Zastrzeżenia dotyczące funkcjonowania kontroli zarządczej w roku ubiegłym.

Na podstawie wyników kontroli i audytów przeprowadzonych w 2022 roku oraz podsumowania wyników procesu samooceny ryzyka operacyjnego w MF przeprowadzonej w 2022 roku stwierdzono słabości kontroli zarządczej w zakresie: celów i zarządzania ryzykiem, mechanizmów kontroli.

Należy opisać przyczyny złożenia zastrzeżeń w zakresie funkcjonowania kontroli zarządczej, np. istotną słabość kontroli zarządczej, istotną nieprawidłowość w funkcjonowaniu jednostki sektora finansów publicznych albo działu administracji rządowej, istotny cel lub zadanie, które nie zostały zrealizowane, niewystarczający monitoring kontroli zarządczej, wraz z podaniem, jeżeli to możliwe, elementu, którego zastrzeżenia dotyczą, w szczególności: zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczności i efektywności działania, wiarygodności sprawozdań, ochrony zasobów, przestrzegania i promowania zasad etycznego postępowania, efektywności i skuteczności przepływu informacji lub zarządzania ryzykiem.

2. Planowane działania, które zostaną podjęte w celu poprawy funkcjonowania kontroli zarządczej.

- 1) wdrożenie zarządzania ryzykiem operacyjnym w Centrum Informatyki Resortu Finansów – termin realizacji: 30 czerwca 2024 r.;
- 2) integracja podejścia do zarządzania ryzykiem operacyjnym pomiędzy Ministerstwem Finansów i Centrum Informatyki Resortu Finansów – termin realizacji: 30 czerwca 2024 r.;
- 3) przeprowadzenie analizy w zakresie możliwości uwzględnienia w modelu współpracy z Centrum Informatyki Resortu Finansów Kluczowych Wskaźników Ryzyka – termin realizacji: 31 grudnia 2023 r.;
- 4) opracowanie koncepcji realizacji w Centrum Informatyki Resortu Finansów niezależnych audytów w zakresie cyberbezpieczeństwa oraz zarządzania infrastrukturą IT (minimum zarządzanie incydentami IT i awariami) – termin realizacji: 31 grudnia 2023 r.;
- 5) wdrożenie rozwiązania systemowego do monitorowania instalowanego oprogramowania przez pracowników z uprawnieniami administratorów – termin realizacji: 31 grudnia 2023 r.;
- 6) opracowanie kompleksowej koncepcji zarządzania strukturą informatyczną, w tym w obszarze zarządzania oprogramowaniem komputerowym i licencjami na oprogramowanie komputerowe – termin realizacji: 31 grudnia 2023 r.

Należy opisać kluczowe działania, które zostaną podjęte w celu poprawy funkcjonowania kontroli zarządczej w odniesieniu do złożonych zastrzeżeń, wraz z podaniem terminu ich realizacji.

Dział III⁹⁾

Działania, które zostały podjęte w ubiegłym roku w celu poprawy funkcjonowania kontroli zarządczej.

1. Działania, które zostały zaplanowane na rok, którego dotyczy oświadczenie:

- 1) w ramach dokonania przeglądu, aktualizacji oraz wdrożenia zmian *Systemu Zarządzania Bezpieczeństwem Informacji* (SZBI) ze szczególnym uwzględnieniem bezpieczeństwa pracy hybrydowej i zdalnej, nowego modelu funkcjonowania służby IT:
 - a) przeprowadzono niezależną, udokumentowaną analizę ryzyka obejmującą podatności, dotyczące wykorzystywania komputerów prywatnych do celów służbowych;
 - b) opracowano i wdrożono procedury zarządzania ryzykiem bezpieczeństwa informacji;
 - c) ustalono i przedstawiono do akceptacji Dyrektora Generalnego realny plan opracowania nowego SZBI, uwzględniającego wyniki analizy ryzyka, obejmującej podatności dotyczące wykorzystania komputerów prywatnych do celów służbowych;
 - d) opracowano i wdrożono nowe dokumenty *Polityka Bezpieczeństwa Informacji Resortu Finansów* (PBIRF), *Polityka Bezpieczeństwa Teleinformatycznego Resortu Finansów* (PBTRF) oraz dokumenty powiązane uwzględniające pracę w warunkach zdalnych oraz nowy model funkcjonowania służb IT;
 - e) opracowano, zatwierdzono i wdrożono poniższe dokumenty:
 - *Polityka Zarządzania Ciągłością Działania;*
 - *Procedura zarządzania upoważnieniami do przetwarzania danych osobowych;*
 - *Procedura powierzenia przetwarzania danych osobowych;*
 - *Procedura Zarządzania Incydentami Bezpieczeństwa Informacji;*
 - *Procedura wykonywania i zarządzania kopiami zapasowymi;*
 - *Instrukcja dotycząca oceny podmiotów zewnętrznych;*
 - *Instrukcja anonimizowania dokumentów;*
 - *Polityka Bezpieczeństwa Teleinformatycznego Resortu Finansów*

- *Procedura zarządzania uprawnieniami w systemach teleinformatycznych służących do przetwarzania danych osobowych* - opracowano dokument określający wymagania w tym obszarze – „Zasady zarządzania uprawnieniami”, nowy wzór „Instrukcji Zarządzania Systemem Informatycznym” oraz określono wymagania w PBTRF;
 - *Procedura zarządzania ryzykiem dot. danych osobowych* - została wprowadzona jako element zarządzania systemem informatycznym w ramach zasad i procedur związanych z realizacją dokumentacji bezpieczeństwa dla systemów informatycznych.
- f) opracowano procedury szybkiego blokowania kont systemowych użytkownika w sytuacjach awaryjnych z określeniem ról i odpowiedzialności w procesie oraz kanału zgłaszania takich sytuacji;
- g) przygotowano i wstępnie uzgodniono procedury (działania realizowane przez CIRF):
- *Procedura zarządzania dostępem do nośników danych;*
 - *Procedura zarządzania i eksploatacji nośników informacji.*
- Wymagania odnośnie korzystania z przyrządów urządzeń peryferyjnych oraz zarządzania dostępem do nośników danych zostały również określone w zatwierdzonej 30.12.2022 roku PBTRF.
- h) zapewniono, że program ABI zawiera odwzorowania cyfrowe wydanych upoważnień tak, że w 100% są zgodne z papierową wersją upoważnienia oraz usunięto z programu wszystkie inne upoważnienia, które nie są zgodne z faktycznie wydanymi upoważnieniami;
- i) zatwierdzono *Politykę Zarządzania Incydentami Bezpieczeństwa Informacji w Ministerstwie Finansów i jednostkach organizacyjnych Resortu Finansów (PZIBI)*, w tym określono kategorię incydentów bezpieczeństwa, opracowano procedury obsługi incydentów, w szczególności dotyczących informacji przetwarzanych w centralnych systemach teleinformatycznych;
- j) przekazano do stosowania po zatwierdzeniu *Polityki Zarządzania Incydentami Bezpieczeństwa Informacji w Ministerstwie Finansów i jednostkach organizacyjnych Resortu Finansów (PZIBI)*.
- 2) w ramach opracowania i wdrożenia zasad sprawowania nadzoru nad CIRF w zakresie planowania oraz rozliczania z działalności i osiąganych wyników, w tym w zakresie bezpieczeństwa informacji:
- a) opracowano plan nadzoru nad CIRF i Aplikacjami Krytycznymi (AK), od stycznia 2022 r. przygotowywano *Raport Okresowy CIRF i AK* w sekwencji miesięcznej, a od lipca 2022 r. przygotowywano *Raport nadzoru* w sekwencji dwumiesięcznej. Od stycznia 2023 r. raportowanie przez CIRF odbywać się będzie w sekwencji miesięcznej, a AK będzie monitorowane w ramach cotygodniowych spotkań PMO i Komitetów Sterujących.
- b) zweryfikowano i wdrożono (CIRF) 10 działań naprawczych zaproponowanych przez Departament Zarządzania Informatyzacją (DZI) w *Raporcie nadzoru*;
- c) dokonano przeglądu 107 usług w katalogu usług IT aktywnych centralnych /pozostałych oraz zgłoszono potrzeby aktualizacji do CIRF;
- d) uregulowano kwestie prawne prowadzenia audytów bezpieczeństwa w ramach realizacji zadania dot. zarządzania bezpieczeństwem informacji w MF i koordynowania tego procesu w jednostkach organizacyjnych podległych Ministrowi lub przez niego nadzorowanych oraz zasady realizacji audytów w PBIRF;
- e) dokonano przeglądu i aktualizacji standardów w zakresie bezpieczeństwa teleinformatycznego;
- f) zrealizowano audyty bezpieczeństwa w CIRF.
- 3) w ramach wdrożenia w organizacji Systemu Zarządzania Ciągłością Działania:
- a) zatwierdzono uzgodniony model architektury procesów Krajowej Administracji Skarbowej (KAS);
- b) zidentyfikowano procesy i wykorzystywane w ich realizacji zasoby w kolejnych komórkach organizacyjnych MF (Departament Finansowania Sfery Budżetowej, Departament Finansowania Sfery Gospodarczej, Departament Poboru Opłat Drogowych) do dalszych prac związanych z ciągłością działania, w tym wytypowania procesów krytycznych;
- c) opracowano strategię ciągłości działania dla procesów krytycznych wytypowanych w Departamencie Długu Publicznego;
- d) opracowano plany ciągłości działania dla procesów krytycznych wytypowanych w Departamencie Długu Publicznego;
- e) przeprowadzono analizę wpływu na działalność (BIA) oraz analizę ryzyka dla wstępnie wytypowanych 18 krytycznych procesów KAS;
- f) przekazano do jednostek organizacyjnych resortu finansów zbiorczego raportu o procesach krytycznych realizowanych w KAS;
- g) opracowano plany ciągłości działania dla wytypowanych po uzgodnieniach 14 procesów krytycznych KAS;
- h) przekazano do jednostek organizacyjnych resortu finansów opracowanych planów ciągłości działania dla 14 procesów krytycznych KAS - zebrano uwagi i sugestie;
- i) opracowano plany ciągłości działania dla procesów krytycznych z obszaru realizacji budżetu państwa;
- j) opracowano listę procesów realizowanych w obszarze poboru opłat drogowych (kontynuacja zadania w 2023 roku mająca na celu opracowanie planów ciągłości działania dla procesów krytycznych z obszaru poboru opłat drogowych);
- k) przeprowadzono testy wybranego planu ciągłości działania dla procesu krytycznego wytypowanego w Departamencie Długu Publicznego oraz sporządzono raport z tego testu.

Należy opisać najistotniejsze działania, jakie zostały podjęte w roku, którego dotyczy niniejsze oświadczenie w odniesieniu do planowanych działań wskazanych w dziale II oświadczenia za rok poprzedzający rok, którego dotyczy niniejsze oświadczenie.

2. Pozostałe działania:

Należy opisać najistotniejsze działania, niezaplanowane w oświadczeniu za rok poprzedzający rok, którego dotyczy niniejsze oświadczenie, jeżeli takie działania zostały podjęte.

Objaśnienia:

- ¹⁾ Należy podać nazwę pełnionej funkcji oraz nazwę komórki organizacyjnej.
- ²⁾ W dziale I, w zależności od wyników oceny stanu kontroli zarządczej, wypełnia się tylko jedną część z części A albo B, albo C przez zaznaczenie znakiem "X" odpowiedniego wiersza. Pozostałe dwie części wykreśla się. Część D wypełnia się niezależnie od wyników oceny stanu kontroli zarządczej.
- ³⁾ Część A wypełnia się w przypadku, gdy kontrola zarządcza w wystarczającym stopniu zapewniła łącznie wszystkie następujące elementy: zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczność i efektywność działania, wiarygodność sprawozdań, ochronę zasobów, przestrzeganie i promowanie zasad etycznego postępowania, efektywność i skuteczność przepływu informacji oraz zarządzanie ryzykiem.
- ⁴⁾ Część B wypełnia się w przypadku, gdy kontrola zarządcza nie zapewniła w wystarczającym stopniu jednego lub więcej z wymienionych elementów: zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczności i efektywności działania, wiarygodności sprawozdań, ochrony zasobów, przestrzegania i promowania zasad etycznego postępowania, efektywności i skuteczności przepływu informacji lub zarządzania ryzykiem, z zastrzeżeniem przypisu 6.
- ⁵⁾ Część C wypełnia się w przypadku, gdy kontrola zarządcza nie zapewniła w wystarczającym stopniu żadnego z wymienionych elementów: zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi, skuteczności i efektywności działania, wiarygodności sprawozdań, ochrony zasobów, przestrzegania i promowania zasad etycznego postępowania, efektywności i skuteczności przepływu informacji oraz zarządzania ryzykiem.
- ⁶⁾ Znakiem "X" zaznaczyć odpowiednie wiersze. W przypadku zaznaczenia punktu "inne źródła informacji" należy je wymienić.
- ⁷⁾ Standardy kontroli zarządczej dla sektora finansów publicznych ogłoszone przez Ministra Finansów na podstawie art. 69 ust. 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.
- ⁸⁾ Dział II sporządzany jest w przypadku, gdy w dziale I niniejszego oświadczenia zaznaczono część B albo C.
- ⁹⁾ Dział III sporządza się w przypadku, gdy w dziale I oświadczenia za rok poprzedzający rok, którego dotyczy niniejsze oświadczenie, była zaznaczona część B albo C lub gdy w roku, którego dotyczy niniejsze oświadczenie, były podejmowane inne niezaplanowane działania mające na celu poprawę funkcjonowania kontroli zarządczej.