RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

SZEF KRAJOWEJ ADMINISTRACJI SKARBOWEJ

DAS10.9011.6.2018.PZD.3

Sprawozdanie

Z AUDYTU GŁÓWNEGO SYSTEMU INFORMATYCZNEGO SL2014 WYKORZYSTYWANEGO PRZY WDRAŻANIU PROGRAMÓW OPERACYJNYCH W PERSPEKTYWIE FINANSOWEJ 2014-2020

Warszawa, luty 2019 r.

Spis treści

I. WSTĘP

I.1. CEL SPRAWOZDANIA

Art. 127 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. *ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie Rady (WE) nr 1083/2006* (dalej: rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013), nakłada na Instytucję Audytową obowiązek prowadzenia audytów systemu zarządzania i kontroli.

Zgodnie z art. 127 ust. 5 lit. a i b rozporządzenia 1303/2013 Instytucja Audytowa sporządza:

a) opinię audytową zgodnie z art. 63 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniającego rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylającego rozporządzenie (UE, Euratom) nr 966/2012;
b) sprawozdanie z kontroli, przedstawiające główne wyniki audytów przeprowadzonych zgodnie z ust. 1, w tym ustalenia dotyczące defektów stwierdzonych w systemach zarządzania i kontroli oraz proponowane i wdrożone działania naprawcze.

Zgodnie z art. 63 ust. 7 rozporządzenia finansowego dokumenty, o których mowa powyżej, przekazywane są Komisji do dnia 15 lutego każdego roku budżetowego.

W badanym systemie informatycznym SL2014 znajdują się dane finansowe dotyczące realizowanych projektów w ramach:

- Regionalnego Programu Operacyjnego Województwa Dolnośląskiego,
- Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego,
- Regionalnego Programu Operacyjnego Województwa Lubelskiego,
- Regionalnego Programu Operacyjnego Województwa Lubuskiego,
- Regionalnego Programu Operacyjnego Województwa Łódzkiego,
- Regionalnego Programu Operacyjnego Województwa Małopolskiego,
- Regionalnego Programu Operacyjnego Województwa Mazowieckiego,
- Regionalnego Programu Operacyjnego Województwa Opolskiego,
- Regionalnego Programu Operacyjnego Województwa Podkarpackiego,
- Regionalnego Programu Operacyjnego Województwa Podlaskiego,

- Regionalnego Programu Operacyjnego Województwa Pomorskiego,
- Regionalnego Programu Operacyjnego Województwa Śląskiego,
- Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego,
- Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego,
- Regionalnego Programu Operacyjnego Województwa Wielkopolskiego,
- Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego,
- Programu Operacyjnego Polska Cyfrowa,
- Programu Operacyjnego Wiedza Edukacja Rozwój,
- Programu Operacyjnego Polska Wschodnia,
- Programu Operacyjnego Pomoc Techniczna,
- Programu Operacyjnego Inteligentny Rozwój,
- Programu Operacyjnego Infrastruktura i Środowisko,
- Programów Europejskiej Współpracy Terytorialnej:
  - Programu INTERREG V-A Polska – Dania – Niemcy – Litwa – Szwecja (Południowy Bałtyk),
  - Programu INTERREG V-A Polska – Słowacja,
  - Programu INTERREG V-A Polska – Saksonia,
- Programów Europejskiego Instrumentu Sąsiedztwa:
  - Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina,
  - Programu Współpracy Transgranicznej Polska – Rosja.

Systemy zarządzania i kontroli ww. programów w perspektywie finansowej 2014-2020 oparte są na przepisach rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013. Sprawozdanie przedstawia zakres i wyniki czynności sprawdzających wykonanych przez pracowników Departamentu Audytu Środków Publicznych w Ministerstwie Finansów.

I.2. ORGAN ODPOWIEDZIALNY ZA SPORZĄDZENIE SPRAWOZDANIA

Wykonywanie zadań instytucji odpowiedzialnej za przeprowadzenie audytu systemu zostało powierzone Szefowi Krajowej Administracji Skarbowej, który pełni funkcję Instytucji Audytowej dla programów operacyjnych.

Szef Krajowej Administracji Skarbowej wykonuje swoje zadania za pośrednictwem Departamentu Audytu Środków Publicznych w Ministerstwie Finansów. Jest on również odpowiedzialny za zatwierdzenie przedmiotowego sprawozdania.

I.3. PODSUMOWANIE USTALEŃ

Kryterium oceny nr 15 (4.1)

W wyniku badania *kryterium oceny nr 15 (4.1) – Kontrole zarządcze zawierają kontrole administracyjne i kontrole na miejscu* wydano 5 rekomendacji w kategorii 1. Kryterium ostatecznie ocenione zostało w **kategorii 1 – system funkcjonuje prawidłowo, tylko niewielkie usprawnienia są potrzebne.**

Kryterium oceny nr 23 (6.1)

W ramach badania kryterium oceny nr 23 (6.1) wydano łącznie 5 rekomendacji – (1 rekomendacja w kategorii 1 oraz 4 rekomendacje w kategorii 2). Dwie rekomendacje wydane w latach ubiegłych nie zostały wdrożone.

Lp.	Ocena w ramach badania przeprowadzonego w 2018 r.	Liczba wydanych rekomendacji oraz kategorie				Ocena podsumowująca badany obszar
		1	2	3	4	
1	Regionalny Program Operacyjny Województwa Śląskiego	-	2	-	-	2
2	Program Operacyjny Infrastruktura i Środowisko	1	1	-	-	2
3	Program Operacyjny INTERREG V-A Polska – Saksonia 2014-2020	-	1	-	-	2

Lp.	Ocena w ramach badania follow-up	Liczba wydanych rekomendacji oraz kategorie				Ocena podsumowująca badany obszar
		1	2	3	4	
1	Program Operacyjny Inteligentny Rozwój	-	1	-	-	2
2	Regionalny Program Operacyjny Województwa Zachodniopomorskiego	1	-	-	-	1

Kryterium oceny nr 24 (6.2)

W ramach badania kryterium oceny nr 24 (6.2) nie stwierdzono nieprawidłowości – zostało ocenione w **kategorii 1 – system funkcjonuje prawidłowo.**

Kryterium oceny nr 25 (6.3)

Dla kryterium oceny nr 25 (6.3) wydano łącznie 2 rekomendacje w kategorii 1.

Dodatkowo przeprowadzono audyt follow-up rekomendacji otwartych, wydanych w latach ubiegłych. Potwierdzono wdrożenie 4 rekomendacji. Jedna rekomendacja w kategorii 2 nie została wdrożona.

Poniżej dokonano oceny podsumowującej na poziomie poszczególnych obszarów Normy PN-ISO/IEC27002:2014.

Oceny dla poszczególnych badanych obszarów, w których wydano rekomendacje:

Lp.	Badane obszary	Liczba wydanych rekomendacji				Ocena podsumowująca badany obszar
		Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4	
1	Polityki bezpieczeństwa informacji	-	-	-	-	1
2	Organizacja bezpieczeństwa informacji	-	-	-	-	1
3	Bezpieczeństwo zasobów ludzkich	-	-	-	-	1
4	Kontrola dostępu	-	-	-	-	1
5	Bezpieczeństwo eksploatacja	2	-	-	-	1
6	Pozyskiwanie, rozwój i utrzymanie systemów	-	-	-	-	1
7	Relacje z dostawcami	-	-	-	-	1

W związku z powyższym kluczowy wymóg kontrolny nr 6 został oceniony w **kategorii 2 – system funkcjonuje, potrzebne są jednak pewne usprawnienia**, zgodnie z wytyczną KE *Guidance for the Commission and Member States on a common methodology for the assessment of management and control systems in the Member States (EGESIF_14-0010-final)*. Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie następnego audytu systemu zarządzania i kontroli.

II. METODYKA I ZAKRES PRAC AUDYTOWYCH

II.1. RAMY CZASOWE AUDYTU

Audyt przeprowadzony zostały w okresie czerwiec – grudzień 2018 r.

II.2. ZAKRES WYKONANYCH PRAC

Prace przeprowadzone zostały w Agencji Restrukturyzacji i Modernizacji Rolnictwa, Instytucjach Zarządzających programami operacyjnymi właściwymi w zakresie swoich kompetencji oraz w Ministerstwie Inwestycji i Rozwoju – właścicielu systemu SL2014.

Celem przeprowadzonych prac było zapewnienie, iż spełniony jest kluczowy wymóg kontrolny nr 4 (4.1) oraz 6 (6.1, 6.2, 6.3).

System oceniony został w następujących kryteriach:

- Kryterium oceny nr 15 (4.1) – Kontrole zarządcze obejmują:

  a) weryfikacje administracyjne w odniesieniu do każdego złożonego przez beneficjentów wniosku o refundację,

  b) kontrole operacji na miejscu. Kontrole na miejscu powinny być przeprowadzone przez instytucję zarządzającą i jej instytucje pośredniczące w momencie kiedy projekt jest już w zaawansowanej fazie realizacji, zarówno pod względem zaawansowania fizycznego, jak i finansowego (np. w przypadku działań szkoleniowych).

- Kryterium oceny nr 23 (6.1) – Istnienie skomputeryzowanego systemu zdolnego do gromadzenia, rejestrowania i przechowywania danych w odniesieniu do każdej operacji, wymaganych w załączniku III rozporządzenia delegowanego Komisji (UE) nr 480/2014 z dnia 3 marca 2014 r. *uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego* [dalej rozporządzenia delegowanego Komisji (UE) nr 480/2014], w tym danych dotyczących wskaźników i celów pośrednich oraz danych na temat postępów programu w osiąganiu celów przekazanych przez instytucję zarządzającą na podstawie art. 125 ust. 2 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013. Jeśli operacja jest objęta wsparciem z EFS, system musi również obejmować dane dotyczące poszczególnych uczestników oraz, jeśli jest to wymagane przez EFS, podział danych odnoszących się do wskaźników według płci.

- Kryterium oceny nr 24 (6.2) – Istnieją odpowiednie procedury, aby umożliwić agregowanie danych, gdy jest to konieczne dla celów

ewaluacji, audytu, jak również w odniesieniu do wniosków o płatność i zestawień wydatków, rocznych sprawozdań podsumowujących, rocznej realizacji oraz sprawozdań końcowych, w tym sprawozdań dotyczących danych finansowych, przekazanych Komisji.

– Kryterium oceny nr 25 (6.3) – Istnieją odpowiednie procedury, aby zapewnić:

a) zabezpieczenie i konserwację takiego skomputeryzowanego systemu, spójność danych, uwzględniając przyjęte międzynarodowe standardy jak na przykład ISO/IEC27001:2013 i ISO/IEC27002:2013, poufność danych, weryfikację nadawcy oraz przechowywanie dokumentów i danych, w szczególności zgodnie z art. 122 ust. 3, art. 125 ust. 4 lit. d), art. 125 ust. 8 i art. 140 rozporządzenia Parlamentu Europejskiego i Rady UE nr 1303/2013,

b) ochronę osób fizycznych w zakresie przetwarzania danych osobowych.

Wykonane czynności:

Przeprowadzono analizę dokumentów:

- Raportów miesięcznych z usług utrzymania systemów informatycznych;
- Karty audytu wewnętrznego;
- Rejestru zmian w dokumentacji SZBI dla CST;
- Karty przeglądu dokumentacji SZBI;
- Protokołu z przeglądu zarządzania nr 1/2018;
- Planu działania 2018 r.;
- Deklaracji stosowania dla CST;
- Procedury obsługi zgłoszeń w ServiceDesk centralnego systemu teleinformatycznego;
- Procedury uruchomienia SL2014 w infrastrukturze MIiR;
- Planu ciągłości działania CST;
- Procedury Systemu Zarządzania Bezpieczeństwem Informacji dla CST;
- Polityki Systemu Zarządzania Bezpieczeństwem Informacji dla CST;
- Karty klasyfikacji zasobów i aktywów informacyjnych;
- Harmonogramu audytu wewnętrznego 2018;
- Programu audytów wewnętrznych 2018;
- Regulaminu bezpieczeństwa informacji przetwarzanych w CST;
- Regulaminu bezpieczeństwa informacji przetwarzanych w aplikacji głównej CST;
- Regulaminu bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych MIiR;
- Zarządzenia nr 20 Ministra Rozwoju z 11.04.2016 r. w sprawie wyznaczenia pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni MR;
- Instrukcji testowania oprogramowania przez Administratorów;

- Raportu – Przegląd aktywności;
- Monitoringu i ocena systemu pod kątem dostępności, integralności i rozliczalności działania CST;
- Procedury monitorowania wydajności, podatności i pojemności;
- Procedury migracji CST do Oracle Cloud;
- Wytycznych do zarządzania usługami IT w systemie CST świadczonymi przez firmę zewnętrzną;
- Polityki Bezpieczeństwa Systemów Teleinformatycznych w MR z 06.06.2016 r.;
- Polityki Ochrony Danych Osobowych w MIiR;
- SL2014 Dokument Architektury Oprogramowania wersja 2.4;
- Wytycznych w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020 wraz z załącznikami;

oraz przeprowadzono testy na dokumentacji dotyczącej projektów wytypowanych w ramach każdego programu operacyjnego, wskazanych w załącznikach 1-25 do niniejszego sprawozdania.

III. WYNIKI OCENY

III.1. KRYTERIUM OCENY NR 15 (4.1) KLUCZOWEGO WYMOGU KONTROLNEGO NR 4

W zakresie objętym audytem dotyczącym kryterium oceny nr 15 (4.1) - na podstawie przeprowadzonego badania stwierdzono:

Informacje ogólne:

W zakresie funduszy strukturalnych, Wspólnej Polityki Rybołówstwa oraz płatności non-IACS w ramach Wspólnej Polityki Rolnej wykorzystywane są dwa systemy informatyczne służące do przeprowadzania kontroli krzyżowych.

Pierwszym z nich jest system Ministerstwa Inwestycji i Rozwoju (MIiR) Centralny System Teleinformatyczny (CST), który agreguje dane w zakresie regionalnych programów operacyjnych oraz krajowych programów operacyjnych, funkcjonujący od początku perspektywy 2014-2020.

Drugi system to CKK (Centrum Kontroli Krzyżowych) Agencji Restrukturyzacji i Modernizacji Rolnictwa, agregujący dane w zakresie płatności non-IACS w ramach Wspólnej Polityki Rolnej oraz Programu Operacyjnego Rybactwo i Morze.

Agencja Restrukturyzacja i Modernizacji Rolnictwa podpisała z Ministerstwem Inwestycji i Rozwoju porozumienie, którego celem było nawiązanie współpracy w zakresie wymiany danych na temat beneficjentów realizujących projekty/ operacje/ przedsięwzięcia w programach operacyjnych w ramach polityki spójności na lata 2014-2020, płatności non-IACS w ramach Wspólnej Polityki Rolnej oraz Programu Operacyjnego Rybactwo i Morze i uregulowanie w porozumieniu warunków tej współpracy pomiędzy ARiMR a MIiR w zakresie realizacji kontroli krzyżowych

mających na celu wykrywanie i eliminowanie podwójnego finansowania wydatków w ramach polityki spójności (PS), WPR i PO RYBY14-20.

Wymiana danych pomiędzy systemami:

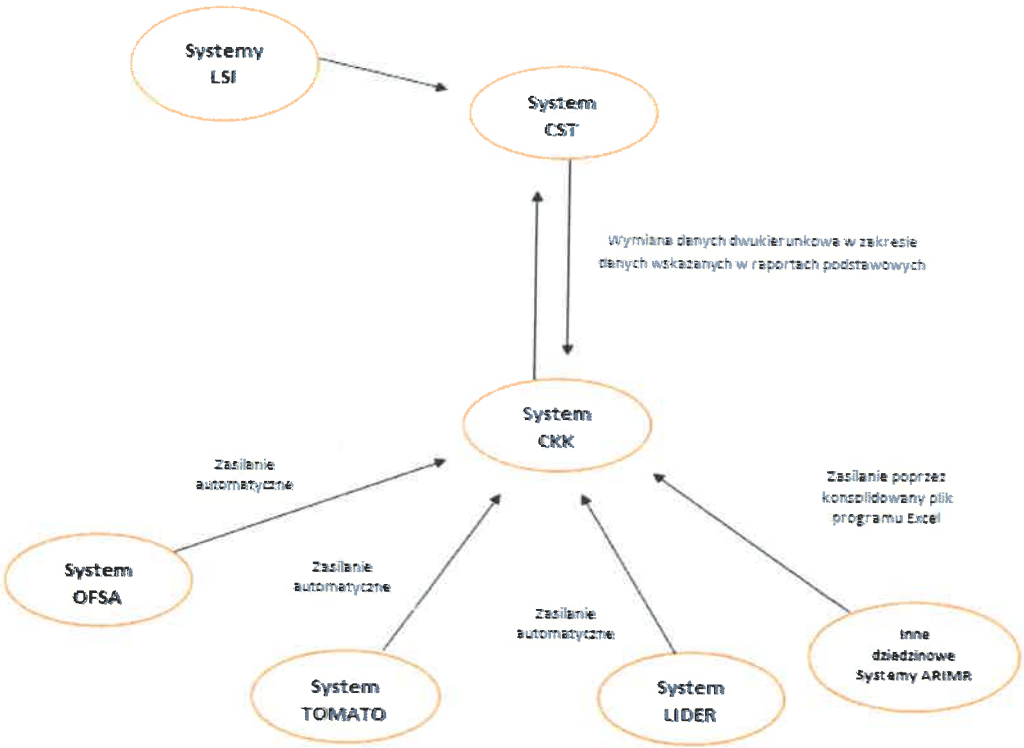
W ramach zawartego porozumienia:

- MIiR zobowiązało się do udostępnienia 120 osobom realizującym kontrole krzyżowe w ramach PROW14-20 i PO RYBY14-20, w tym pracownikom Samorządów Województw, danych zgromadzonych w Centralnym Systemie Teleinformatycznym za pośrednictwem hurtowni danych (aplikacji raportującej), tj. SRHD, jako użytkownikom CST,
- ARiMR zobowiązało się do udostępnienia 120 osobom przeprowadzającym kontrole krzyżowe w ramach PS, w tym pracownikom Samorządów Województw, danych zgromadzonych w systemach informatycznych ARiMR za pośrednictwem CKK, jako użytkownikom CKK. Każdy ze zgłoszonych użytkowników otrzyma dostęp do środowiska szkoleniowego i produkcyjnego CKK. Dostępu do systemu CKK nie posiadają pracownicy Instytucji Pośredniczących wdrażających programy operacyjne w ramach PS.

Podstawowym mechanizmem umożliwiającym wykonanie horyzontalnej kontroli krzyżowej w ramach środków wydatkowanych z budżetu UE w Polsce jest wymiana danych pomiędzy systemami CST oraz CKK. Wymiana danych pomiędzy systemami CST i CKK jest dwukierunkowa, poprzez usługi sieciowe, wyzwalana automatycznie raz dziennie. Wymiana danych następuje w zakresie raportów podstawowych, których zakres obejmuje następujące dane:

- NIP;
- Nazwa działania;
- Nazwa poddziałania;
- Nazwa instytucji podpisującej umowę o dofinansowanie;
- Cel operacji/tytuł projektu;
- Data rozpoczęcia realizacji operacji;
- Data zakończenia realizacji operacji;
- Numer projektu;
- Numer wniosku o płatność;
- Typ (wartość stała U lub S);
- System (wartość stała CKK);
- Beneficjentów, którzy mają zarejestrowane zatwierdzone wnioski o płatność rozliczające wydatki (wnioski o refundację lub rozliczenie zaliczki).

Rysunek 1. Schemat wymiany danych.



System CST zasilany jest (w zależności od zakresu danych) danymi pochodzącymi z Lokalnych Systemów Informatycznych wykorzystywanych w ramach wdrażania poszczególnych programów operacyjnych lub ręcznie poprzez spersonalizowane konta użytkowników/ beneficjentów.

System CKK zasilany jest danymi poprzez automatyczny mechanizm w zakresie danych pochodzących z systemów OFSA PROW 2014-2020 (dla działania 4 *Inwestycje w środki trwałe* i działania 6 *Rozwój gospodarstw i działalności gospodarczej*), OFSA-PROW-DD (dla działania 7 *Podstawowe usługi i odnowa wsi na obszarach wiejskich*), LIDER (dla PO *RYBY* 2014-2020) oraz TOMATO (dla grup i organizacji producentów). W przypadku niektórych działań, tj. *Pomoc Techniczna PROW 2014-2020,* Działanie 19 *Wsparcie dla rozwoju lokalnego w ramach inicjatywy LEADER* oraz *poddziałania 3.2 Wsparcie na działania informacyjne i promocyjne realizowane przez grupy producentów na rynku wewnętrznym,* dane do systemu CKK importowane są z pliku Ms Excel.

Zasady przeprowadzania kontroli krzyżowych:

Podstawowe wytyczne w zakresie przeprowadzania kontroli krzyżowych dla środków wydatkowanych z budżetu Unii Europejskiej zostały zawarte w *Wytycznych Ministra Inwestycji i Rozwoju w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020 z dnia 3 marca 2018 r.* Ze względu na cele kontroli krzyżowej wyróżnia się:

- kontrolę krzyżową programu, której celem jest wykrywanie i eliminowanie podwójnego finansowania wydatków w ramach jednego programu operacyjnego;
- kontrolę krzyżową horyzontalną, której celem jest wykrywanie i eliminowanie podwójnego finansowania wydatków w ramach różnych PO realizowanych w ramach Umowy Partnerstwa w tym PROW 2014-20 i PO RYBY;
- kontrolę krzyżową międzyokresową, której celem jest wykrywanie i eliminowanie podwójnego finansowania wydatków w ramach Programu Operacyjnego dwóch perspektyw finansowych.

Kontrola krzyżowa horyzontalna realizowana jest przez:

1. Ministra właściwego ds. rozwoju regionalnego (DCD), który wybiera cyklicznie raz na kwartał próbę spośród beneficjentów realizujących:
    - projekty w co najmniej dwóch PO;
    - projekty w ramach dwóch perspektyw finansowych.

Minimalna wielkość próby jest określona w *Procedurze prowadzenia kontroli krzyżowych horyzontalnych realizowanych w perspektywie finansowej z dnia 5 stycznia 2018 r.* Zgodnie z ww. procedurą minimalna próba beneficjentów do kontroli wynosi 5%, naczelnik wydziału może podjąć decyzję o rozszerzeniu próby beneficjentów do kontroli. Weryfikacji krzyżowej podlegają wydatki zawarte we wszystkich zatwierdzonych wnioskach o płatność kontrolowanego beneficjenta, nie dotyczą projektów realizowanych jednocześnie w ramach programów operacyjnych Polityki Spójności i PROW 14-20 lub PO RYBY.

2. Właściwą Instytucję Zarządzającą, która przeprowadza kontrolę krzyżową horyzontalną z PROW oraz PO RYBY spośród beneficjentów realizujących co najmniej 2 projekty w ramach jednego PO.

Ponadto, zgodnie z *Wytyczną Ministra Inwestycji i Rozwoju w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020 z dnia 3 marca 2018 r.*, Instytucja Koordynująca Umowę Partnerstwa może przeprowadzić kontrolę krzyżową koordynowaną wraz z właściwą komórką organizacyjną, o której mowa w pkt 7 lit b, ww. wytycznych we współpracy z właściwymi IZ.

Zgodnie z *Wytyczną Ministra Inwestycji i Rozwoju w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020 z dnia 3 marca 2018 r. Podrozdział 5.3 pkt. 8*, każda z Instytucji Zarządzających powinna opracować pisemne szczegółowe procedury prowadzenia kontroli.

Zgodnie ze stwierdzonym stanem faktycznym kontrola krzyżowa horyzontalna wykonywana jest w dwóch etapach. Pierwszym z nich jest wygenerowanie z systemu informatycznego raportu podstawowego, zawierającego zidentyfikowanych beneficjentów realizujących projekty równocześnie w PS, PROW i PO RYBY. W przypadku zidentyfikowania podejrzenia podwójnego dofinansowania generowany jest raport pogłębiony zawierający dane szczegółowe umożliwiające zidentyfikowanie czy nastąpiło podwójne dofinansowanie. Pracownicy wdrażający programy w ramach PS generują raport pogłębiony w systemie CKK, natomiast pracownicy wdrażający WPR oraz PO RYBY generują raport pogłębiony w systemie CST.

Zasady przeprowadzania kontroli krzyżowych Instrumentów Finansowych:

Prowadzenie kontroli krzyżowej instrumentów finansowych (dalej również jako KK IF) wynika z art. 65 ust. 11 rozporządzenia ogólnego oraz wytycznych KE *Guidance for Member States on Article 37 (7) (8) (9) CPR - Combination of support from a financial instrument with other support* (EGESIF 15 0012-02) kontrola krzyżowa instrumentów finansowych stanowi dodatkowy mechanizm kontroli eliminujący niewłaściwe łączenie wsparcia IF i wsparcia dotacyjnego. Jako część kontroli krzyżowej horyzontalnej jest ona prowadzona przez Departament Certyfikacji i Desygnacji Ministerstwa Inwestycji i Rozwoju. Dane do prowadzenia KK IF przekazywane są przez beneficjenta i zatwierdzane bez zbędnej zwłoki przez IZ lub IP (której IZ delegowała część kompetencji) w module instrumenty finansowe w systemie SL2014. Losowanie odbywa się w cyklach półrocznych (luty sierpień). Próba obejmuje min 5% podmiotów spośród grup zdefiniowanych:

- ostatecznych odbiorców wsparcia IF, którzy jednocześnie realizują projekt dotacyjny;
- podmiotów które podpisały co najmniej umowy, w ramach których korzystają ze środków unijnych w ramach IF.

Wyodrębnienie wyżej wymienionych podmiotów dokonywane jest na podstawie:

- danych ujętych w raporcie pn. Instrumenty finansowe - ostateczni odbiorcy zdefiniowanym w OBIEE przez Administratorów Merytorycznych IK UP,
- analizy tworzonej w OBIEE przez pracowników DCD w celu wyłonienia numerów NIP rozliczających niezerowe wnioski o płatność w ramach perspektywy finansowej 2014-2020 w okresie objętym losowaniem (poprzednie półrocze roku obrachunkowego).

Przygotowanie danych do losowania następuje w arkuszu kalkulacyjnym Ms Excel, a samo losowanie próby przeprowadzane jest z wykorzystaniem generatora liczb losowych przegotowanego również w arkuszu programu Ms Excel. Wyniki kontroli podlegają rejestracji w SL2014, w module *kontrole krzyżowe*. Za pośrednictwem modułu dane odnośnie wyników kontroli krzyżowych IF udostępniane są poszczególnym Instytucjom Certyfikującym i Instytucjom Zarządzającym Programami Operacyjnymi Polityki Spójności.

W trakcie prac audytowych ustalono, iż:

Ustalenie nr 1	Moduł kontrole krzyżowe SL 2014 nie jest dostosowany do rejestrowania wyników w zakresie kontroli krzyżowych instrumentów finansowych (numer NIP, oraz wniosek o płatność stanowi/ wskazuje na dane beneficjenta a nie ostatecznego odbiorcy).
Kategoria	Kategoria 1 – System działa, tylko niewielkie usprawnienia są konieczne.
Rekomendacja	Zaleca się dostosowanie modułu kontroli krzyżowych w SL 2014 tak aby umożliwić przechowywanie wiarygodnych danych wynikających z procedury prowadzenia kontroli krzyżowych w ramach instrumentów finansowych w perspektywie finansowej 2014-2020
Odpowiedź MIiR	Instytucja Koordynująca UP rozpoczęła prace rozwojowe (modyfikację systemu) we wskazanym zakresie.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

Ustalenie nr 2	Próba losowa w ramach kontroli krzyżowej instrumentów finansowych wybierana jest na podstawie danych ujętych w raportach zdefiniowanych w OBIEE (raport zawiera dane ostatecznych odbiorców zatwierdzonych przez właściwe IZ). Następnie departament DCD dokonuje wyboru próby min. 5% z populacji spełniającej określone kryteria za pośrednictwem arkusza programu Ms Excel, co nie zapewnia zachowania właściwej ścieżki audytowej. Kroki przedsiębrane dla każdego etapu wyboru próby powinny być archiwizowane w jednym miejscu co pozwoli na odtworzenie ścieżki audytu dokonania wyboru (np. jako załączniki do dokumentacji z wyboru próby/kontroli krzyżowej).
Kategoria	Kategoria 1 – System działa, tylko niewielkie usprawnienia są konieczne.
Rekomendacja	Zaleca się zapewnienie ścieżki audytowej w procesie wyboru próby w ramach kontroli krzyżowej instrumentów finansowych.
Odpowiedź MIiR	Procedura prowadzenia kontroli krzyżowych w ramach Instrumentów Finansowych w perspektywie finansowej 2014-2020 z dnia 18 czerwca 2018 r. opisuje etapy, w tym czynności

	oraz rodzaje raportów, mające na celu wybór próby do kontroli krzyżowej IF. Wszystkie procesy oraz raporty, włącznie z wyborem próby losowej są generowane/wykonywane zgodnie z pkt. 1.1 ww. procedury, a wszystkie pliki archiwizowane są na dysku wspólnym DCD, w dedykowanym do tego celu folderze. Realizacja ww. etapów procedury pozwala na zachowanie właściwej ścieżki audytu. Niemniej jednak IK UP, wraz z właściwym departamentem odpowiedzialnym za przeprowadzenie kontroli krzyżowych podejmie stosowne kroki i dokona analizy stosowanych rozwiązań w zakresie zapewnienia ścieżki audytowej w procesie wyboru próby do kontroli krzyżowej w ramach instrumentów Finansowych.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

Ustalenie nr 3	Zgodnie z zapisami rozdziału 6 punkt 12 *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020* dane do przeprowadzenia kontroli krzyżowej IF przekazywane są przez beneficjenta i zatwierdzane bez zbędnej zwłoki przez IZ lub IP. Wskazany nieprecyzyjny termin zatwierdzenia „bez zbędnej zwłoki" powoduje ryzyko powstawania opóźnień w zatwierdzaniu dokumentów co wpływa na wielkość populacji danych wykorzystywanej w ramach kontroli krzyżowej IF.
Kategoria	Kategoria 1 – System działa, tylko niewielkie usprawnienia są konieczne.
Rekomendacja	Zaleca się ujednolicenie sposobu i zakresu przekazywania danych niezbędnych do przeprowadzenia kontroli krzyżowej IF w zakresie terminu zatwierdzania danych.
Odpowiedź MIR	IK UP jeszcze w lutym br. planuje przeprowadzić aktualizacje *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020*. Zmiany zapisów obejmą swym zakresem kwestie dotyczące kontroli krzyżowych zgodnie z rekomendacją IA. Zakończenie procedury aktualizacji dokumentu planowane jest na 3 lub 4 kwartał br.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

Ustalenie nr 4	Zgodnie z zapisami *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020* podrozdział 5.3 punkt 3 kontrolą:

	– krzyżową programu; – kontrolą krzyżową horyzontalną; – kontrolą krzyżową międzyokresową; należy objąć próbę minimum 5% beneficjentów, którzy w danym cyklu realizują: – co najmniej 2 projekty w ramach jednego PO; – projekty w co najmniej dwóch PO; – projekty w ramach dwóch perspektyw finansowych. Cykle (częstotliwość przeprowadzania kontroli) zgodnie z przekazanymi IA informacjami są uszczegółowiane w dedykowanych procedurach IKUP/ DCD i IZ. Brak określenia w Wytycznych szczegółowych informacji o minimalnej częstotliwości cykli powoduje ryzyko, że podejście do przeprowadzania KK nie będzie spójne w ramach programów Operacyjnych.
Kategoria	Kategoria 1 – System działa, tylko niewielkie usprawnienia są konieczne.
Rekomendacja	Zaleca się określenie w wytycznych szczegółowych informacji o minimalnej częstotliwości cykli przeprowadzanych kontroli krzyżowych.
Odpowiedź MIiR	IK UP jeszcze w lutym br. planuje przeprowadzić aktualizacje *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020*. Zmiany zapisów obejmą swym zakresem kwestie dotyczące kontroli krzyżowych zgodnie z rekomendacją IA. Zakończenie procedury aktualizacji dokumentu planowane jest na 3 lub 4 kwartał br.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

Ustalenie nr 5	Zgodnie z zapisami *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020* kontrole krzyżowe są realizowane na próbie 5% beneficjentów spełniających określone kryteria. Wytyczne wskazują jedynie minimalną ilość kontroli bez możliwości zastosowania innych czynników ryzyka.
Kategoria	Kategoria 1 – System działa, tylko niewielkie usprawnienia są konieczne.

Rekomendacja	Zaleca się zintensyfikowanie kontroli w ramach ww. 5% na obszarach szczególnie wrażliwych (np. innowacyjność) lub zwiększenie ilości prowadzonych kontroli krzyżowych na podstawie przeprowadzonej analizy ryzyka uwzględniającej takie obszary.
Odpowiedź MIiR	IK UP jeszcze w lutym br. planuje przeprowadzić aktualizacje *Wytycznych w zakresie kontroli realizacji programów operacyjnych na lata 2014-2020*. Zmiany zapisów obejmą swym zakresem kwestie dotyczące kontroli krzyżowych zgodnie z rekomendacją IA. Zakończenie procedury aktualizacji dokumentu planowane jest na 3 lub 4 kwartał br.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

III.2. KRYTERIUM OCENY NR 23 (6.1) KLUCZOWEGO WYMOGU KONTROLNEGO NR 6

Ocena podsumowująca wyniki kryterium oceny (6.1).

Program operacyjny	kategoria oceny
Regionalny Program Operacyjny Województwa Dolnośląskiego	kategoria 1
Regionalny Program Operacyjny Województwa Kujawsko-Pomorskiego	kategoria 1
Regionalny Program Operacyjny Województwa Lubelskiego	kategoria 1
Regionalny Program Operacyjny Województwa Lubuskiego	kategoria 1
Regionalny Program Operacyjny Województwa Łódzkiego	kategoria 1
Regionalny Program Operacyjny Województwa Małopolskiego	kategoria 1
Regionalny Program Operacyjny Województwa Mazowieckiego	kategoria 1
Regionalny Program Operacyjny Województwa Opolskiego	kategoria 1
Regionalny Program Operacyjny Województwa Podkarpackiego	kategoria 1
Regionalny Program Operacyjny Województwa Podlaskiego	kategoria 1
Regionalny Program Operacyjny Województwa Pomorskiego	kategoria 1
Regionalny Program Operacyjny Województwa Śląskiego	kategoria 2

Regionalny Program Operacyjny Województwa Świętokrzyskiego	kategoria 1
Regionalny Program Operacyjny Województwa Warmińsko-Mazurskiego	kategoria 1
Regionalny Program Operacyjny Województwa Wielkopolskiego	kategoria 1
Program Operacyjny Województwa Zachodniopomorskiego	kategoria 1
Program Operacyjny Infrastruktura i Środowisko	kategoria 2
Program Operacyjny Inteligentny Rozwój	kategoria 2
Program Operacyjny Wiedza Edukacja Rozwój	kategoria 1
Program Operacyjny Polska Cyfrowa	kategoria 1
Program Operacyjny Polska Wschodnia	kategoria 1
Program Operacyjny Pomoc Techniczna	kategoria 1
Program Operacyjny INTERREG V-A Polska – Dania – Niemcy – Litwa – Szwecja (Południowy Bałtyk) 2014-2020	kategoria 1
Program Operacyjny INTERREG V-A Polska – Saksonia 2014-2020	kategoria 2
Program Operacyjny INTERREG V-A Polska – Słowacja 2014-2020	kategoria 1

W załącznikach do niniejszego sprawozdania ujęte zostały szczegółowe wyniki badania kryterium oceny (6.1) w podziale na poszczególne programy operacyjne:

- Załącznik 1 - Regionalny Program Operacyjny Województwa Dolnośląskiego;
- Załącznik 2 - Regionalny Program Operacyjny Województwa Kujawsko-Pomorskiego;
- Załącznik 3 - Regionalny Program Operacyjny Województwa Lubelskiego;
- Załącznik 4 - Regionalny Program Operacyjny Województwa Lubuskiego;
- Załącznik 5 - Regionalny Program Operacyjny Województwa Łódzkiego;
- Załącznik 6 - Regionalny Program Operacyjny Województwa Małopolskiego;
- Załącznik 7 - Regionalny Program Operacyjny Województwa Mazowieckiego;
- Załącznik 8 - Regionalny Program Operacyjny Województwa Opolskiego;
- Załącznik 9 - Regionalny Program Operacyjny Województwa Podkarpackiego;
- Załącznik 10 - Regionalny Program Operacyjny Województwa Podlaskiego;

- Załącznik 11 - Regionalny Program Operacyjny Województwa Pomorskiego;
- Załącznik 12 - Regionalny Program Operacyjny Województwa Śląskiego,
- Załącznik 13 - Regionalny Program Operacyjny Województwa Świętokrzyskiego;
- Załącznik 14 - Regionalny Program Operacyjny Województwa Warmińsko-Mazurskiego;
- Załącznik 15 - Regionalny Program Operacyjny Województwa Wielkopolskiego;
- Załącznik 16 - Program Operacyjny Województwa Zachodniopomorskiego;
- Załącznik 17 - Program Operacyjny Infrastruktura i Środowisko;
- Załącznik 18 - Program Operacyjny Inteligentny Rozwój;
- Załącznik 19 - Program Operacyjny Wiedza Edukacja Rozwój;
- Załącznik 20 - Program Operacyjny Polska Cyfrowa;
- Załącznik 21 - Program Operacyjny Polska Wschodnia;
- Załącznik 22 - Program Operacyjny Pomoc Techniczna;
- Załącznik 23 - Program Operacyjny INTERREG V-A Polska – Dania – Niemcy – Litwa – Szwecja (Południowy Bałtyk) 2014-2020;
- Załącznik 24 - Program Operacyjny INTERREG V-A Polska – Saksonia 2014-2020;
- Załącznik 25 - Program Operacyjny INTERREG V-A Polska – Słowacja 2014-2020.

III.3. KRYTERIUM OCENY NR 24 (6.2) KLUCZOWEGO WYMOGU KONTROLNEGO NR 6

Jednym z podstawowych systemów informatycznych, w którym odbywa się ewidencja oraz obsługa projektów, wniosków o dofinansowanie, zawartych umów z beneficjentami, jak również wniosków o płatność w ramach Programów Operacyjnych perspektywy finansowej 2014-2020 jest system SL2014. Niniejszy system jest wykorzystywany przy wdrażaniu programów operacyjnych finansowanych z Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności. W ramach weryfikacji kryterium oceny 6.2 *Istnieją odpowiednie procedury, aby umożliwić agregowanie danych, gdy jest to konieczne dla celów ewaluacji, audytu, jak również w odniesieniu do wniosków o płatności i zestawień wydatków, rocznych sprawozdań podsumowujących, rocznej realizacji oraz sprawozdań końcowych, w tym sprawozdań dotyczących danych finansowych, przekazanych Komisji* zidentyfikowano następujący dokument określający zasady przetwarzania w systemie danych:

- Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020 wraz z załącznikami:
  - Załącznik 1 Główne procedury w zakresie wykorzystania centralnego systemu teleinformatycznego;

- Załącznik 2 Opis tworzenia jednolitego identyfikatora dokumentów w SL2014 oraz w lokalnych systemach informatycznych;
- Załącznik 3 Wnioski o nadanie/zmianę/wycofanie dostępu dla osoby uprawnionej;
- Załącznik 4 Procedura zgłaszania osób uprawnionych w ramach projektu;
- Załącznik 5 Wzór wniosku o płatność Beneficjenta w ramach projektu współfinansowanego ze środków EFRR i FS;
- Załącznik 6 Wzór wniosku o płatność Beneficjenta w ramach projektów współfinansowanych ze środków EFS;
- Załącznik 7 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie danych o naborze;
- Załącznik 8 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie wniosku o dofinansowanie projektu;
- Załącznik 9 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie umowy o dofinansowanie projektu w ramach projektów współfinansowanych ze środków EFRR i FS;
- Załącznik 10 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie umowy o dofinansowanie projektu w ramach projektów współfinansowanych ze środków EFS;
- Załącznik 11 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie wniosku o płatność na potrzeby certyfikacji w ramach projektów współfinansowanych ze środków EFRR i FS;
- Załącznik 12 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie wniosku o płatność na potrzeby certyfikacji dla projektów współfinansowanych ze środków EFS;
- Załącznik 13 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie uczestników projektów;
- Załącznik 14 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie kontroli projektu;
- Załącznik 15 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie bazy personelu;
- Załącznik 16 Minimalny zakres danych koniecznych do wprowadzenia do SL2014 w zakresie instrumentów finansowych;
- Załącznik 17 Wzór harmonogramu płatności w ramach projektu współfinansowanego ze środków EFRR, FS i EFS;
- Załącznik 18 Wzór powołania do pełnienia funkcji Administratora Merytorycznego;
- Załącznik 19 Wzór odwołania z funkcji Administratora Merytorycznego.

Uzupełnieniem dokumentacji są procedury operacyjne funkcjonujące na poziomie Departamentu Informatyki Ministerstwa Inwestycji i Rozwoju oraz wewnętrzne procedury usługodawcy zewnętrznego Atos S.A.

III.4. KRYTERIUM OCENY NR 25 (6.3) KLUCZOWEGO WYMOGU KONTROLEGO NR 6

Obszar audytu systemu informatycznego SL2014 w Ministerstwie Inwestycji i Rozwoju został określony na podstawie analizy ryzyka, w której uwzględniono:

- Sprawozdanie z audytu bezpieczeństwa systemu SL2014 z 2017 r.,
- arkusz Ministerstwa Inwestycji i Rozwoju zawierający zmiany w poszczególnych obszarach/domenach normy ISO/IEC27002, które stwierdzono od ostatniego pełnego badania systemu,
- przegląd wstępny przeprowadzony w ramach wizyty audytora w Ministerstwie Inwestycji i Rozwoju.

Zakres audytu stanowią następujące zagadnienia:

1. Polityki bezpieczeństwa informacji,
2. Organizacja bezpieczeństwa informacji,
3. Bezpieczeństwo zasobów ludzkich,
4. Kontrola dostępu,
5. Bezpieczna eksploatacja,
6. Relacje z dostawcami.

Ustalenia opisane w dalszej części sprawozdania odzwierciedlają stan rzeczywisty zweryfikowany przez Instytucję Audytową na podstawie analizy dokumentów, wywiadów z pracownikami instytucji oraz testów potwierdzających działanie mechanizmów kontrolnych.

W wyniku przeprowadzonych prac audytowych ustalono:

1. Polityki bezpieczeństwa informacji

1.1. Kierunki bezpieczeństwa informacji określane przez kierownictwo

1.1.1. Przegląd polityki Bezpieczeństwa informacji

Zgodnie z pkt *3.1.2 Przegląd polityki bezpieczeństwa Polityki Bezpieczeństwa Systemów Teleinformatycznych w Ministerstw Rozwoju* (wersja 5.0) w celu zapewnienia właściwego wdrażania, skuteczności oraz adekwatności w odniesieniu do zmian środowiska organizacyjnego, warunków działalności, prawnych i środowiska technicznego Ministerstwa, dokonuje się przeglądu polityk bezpieczeństwa raz do roku lub jeśli wynika to z analizy i oceny ryzyka bezpieczeństwa teleinformatycznego lub gdy wystąpią zmiany istotne. Danymi do przeglądu są m.in.: wyniki przeprowadzonych audytów, doraźnych kontroli, okresowe raporty, zapisy dotyczące reagowania na incydenty i zgłaszane podatności.

Metody i wynikające z ich zastosowania czynności wykonywane podczas przeglądu określone zostały w *Procedurze systemu zarządzania bezpieczeństwem informacji dla CST (SZBI.CST.P.05 v1.3).* W ww. dokumencie opisano m. in. procedury: nadzór nad dokumentacją, nadzór nad zapisami, przegląd zarządzania, zarządzanie incydentami.

Zgodnie z procedurą *Nadzoru nad dokumentacją,* której celem jest zapewnienie, że wszystkie dokumenty potrzebne do funkcjonowania SZBI są zatwierdzone i aktualizowane, a ich odpowiednie wersje są dostępne upoważnionym użytkownikom, cała dokumentacja SZBI powinna zostać przejrzana pod względem aktualności i adekwatności w regularnych odstępach czasu, nie rzadziej niż raz w roku. Za przegląd odpowiada pełnomocnik ds. SZBI. Przeglądu dokonuje się na formularzu SZBI/CST/P-05/zal2 – *Karta przeglądu dokumentacji SZBI.*

Ostatni przegląd dokumentacji przeprowadzony w 2018 r. potwierdza *Karta przeglądu dokumentacji SZBI* nr 1/2018 r., zgodnie z którą w 2018 r. zaktualizowano dokumentację m. in. z uwagi na zapisy RODO. Zmiany wersji dokumentacji wraz z zakresem zmiany oraz terminem wprowadzenia zmiany uwzględniono w *Rejestrze zmian w dokumentacji SZBI dla CST.*

Ponadto zgodnie z procedurą *Przegląd zarządzania*, której celem jest właściwe zarządzanie i monitorowanie systemu SZBI, dane wejściowe są przygotowywane przez Zespół ds. SZBI w formie projektów, które zawierają:

- dane i wyniki analiz ryzyka bezpieczeństwa informacji,
- ustalanie i ocenę realizacji celów dotyczących bezpieczeństwa informacji,
- informacje zwrotne od interesantów (skargi i zażalenia w zakresie BI – jeśli wystąpiły),
- opis funkcjonowania procesów i zgodności usług w zakresie BI,
- status działań zapobiegawczych i korygujących podejmowanych w obszarze BI,
- ocenę skuteczności działań podjętych w wyniku poprzednich przeglądów zarządzania BI,
- propozycję zmian przydatnych do doskonalenia SZBI.

Przeglądu zarządzania dokonuje Kierownictwo DI przy współudziale Pełnomocnika ds. SZBI. Wykonanie przeglądu potwierdzają zapisy:

- Protokołu przeglądu zarządzania (SZBI/CST/P-05/zal10),
- zatwierdzonego przez Kierownictwo Planu Działania (SZBI/CST/P-03/zal3).

Powyższe potwierdzono *Protokołem z przeglądu zarządzania* nr 1/2018 z 04.12.2018 r. oraz *Planem Działania* zatwierdzonym 04.12.2018 r.

2. Organizacja bezpieczeństwa informacji

2.1. Organizacja wewnętrzna

2.1.1. Role i odpowiedzialności za bezpieczeństwo informacji

Dokument *Polityka Systemu Zarządzania Bezpieczeństwem Informacji dla CST* określa ogólne zasady i definicje związane z ochroną informacji w Ministerstwie Inwestycji i Rozwoju. SZBI obejmuje wszystkie wydziały DI biorące udział w obsłudze CST oraz dotyczy wszystkich wyznaczonych osób Departamentu Informatyki biorących udział w sposób bezpośredni lub pośredni w gromadzeniu, przetwarzaniu danych, w tym danych osobowych w ramach funkcjonowania CST.

Zgodnie z pkt 1 PBI Dyrektor Departamentu Informatyki jest odpowiedzialny za utrzymanie, rozwój i nadzór nad systemem CST i wyznacza:

- Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (PSBI), sprawującego nadzór w imieniu Dyrektora DI nad wdrożonym systemem zarządzania, opartym na wymogach normy ISO/IEC 27001,
- Administratora Technicznego odpowiadającego za bezpieczeństwo CST (ATB) dbającego o bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w ramach CST.

Natomiast w pkt 3 PBI określono zadania PSBI, ATB i Zespołu ds. SZBI systemu CST.

Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji (PSBI) odpowiedzialny jest za:

- nadzór nad realizacją Polityki SZBI,
- nadzór nad dokumentacją SZBI na etapie jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania,
- zarządzanie analizą ryzyka jako kluczowym narzędziem SZBI,
- inicjowanie procesu szacowania ryzyka,
- zarządzanie zabezpieczeniami aktywów informacji w sposób adekwatny do celów stosowania zabezpieczeń,
- zapewnienie, że procesy potrzebne w Systemie Zarządzania Bezpieczeństwem Informacji są ustanowione, wdrożone i utrzymywane,
- planowanie prac dotyczących systemu zarządzania i nadzór nad ich realizacją,
- przedstawienie do Dyrektora Departamentu sprawozdań dotyczących funkcjonowania SZBI oraz realizacji celów, jak również informowanie o skuteczności funkcjonującego SZBI,
- zarządzanie audytami wewnętrznymi w zakresie nadzorowania zespołu audytorów, planowania audytów i nadzór nad ich realizacją oraz działaniami poaudytowymi,
- inicjowanie oraz nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych,
- nadzorowanie działań związanych z wykrytymi incydentami,
- organizacje przeglądów SZBI oraz nadzór nad realizacją ustaleń wynikających z przeglądów,
- powiadamianie kierownictwa o działalności niezgodnej z obowiązującą w Systemie Zarządzania Bezpieczeństwem Informacji,
- nadzorowanie szkoleń z zakresu SZBI.

Pełnomocnik do spraw Systemu Zarządzania Bezpieczeństwem Informacji uprawniony jest do:

- wydawania poleceń wszystkim pracownikom organizacji z obszaru objętego SZBI w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem SZBI,
- rozstrzygania sporów dotyczących stosowania wymagań zawartych w dokumentacji SZBI oraz wydawania wiążących decyzji w tym zakresie,
- dostępu do wszystkich dokumentów występujących w organizacji, których treść może być istotna z punktu widzenia funkcjonowania SZBI (zgodnie z posiadanymi upoważnieniami),
- uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach Systemu Zarządzania Bezpieczeństwem Informacji,
- podejmowania decyzji w kwestiach bezpieczeństwa informacji, w zakresie nierodzącym zobowiązań finansowych.

Administrator Techniczny odpowiadający za bezpieczeństwo CST (ATB) odpowiedzialny jest za:

- zarządzanie systemem CST w sposób gwarantujący utrzymanie poufności, dostępności i integralności gromadzonych w nich danych na poziomie pozwalającym zachować zgodność z wymogami prawnymi i organizacyjnymi,
- wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych,
- nadzór nad funkcjonowaniem zabezpieczeń systemu CST,
- podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa, zgodnie z procedurami nadzoru nad incydentami bezpieczeństwa oraz utrzymania ciągłością działania,
- prowadzenie, uaktualnianie na bieżąco oraz przygotowywanie rejestru dotyczącego zdarzeń wpływających na bezpieczeństwo systemu CST, w tym m.in. wykrytego oprogramowania złośliwego lub szpiegującego, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzania faktu korzystania z systemu informatycznego przez osobę niepowołaną; ww. zdarzenia brane są pod uwagę podczas przeprowadzania procesu szacowania ryzyka.

Zespół ds. Systemu Zarządzania Bezpieczeństwem Informacji – Członkowie Zespołu ds. SZBI wspierają działania Pełnomocnika ds. SZBI w zakresie przez niego wskazanym m.in.:

- monitorowanie funkcjonowanie SZBI dla CST,
- przeprowadzanie procesu szacowania ryzyka,
- raportowanie wyników prowadzonych audytów wewnętrznych,
- proponowanie i wprowadzanie działań korygujących i zapobiegawczych.

W skład Zespołu ds. SZBI wchodzą:

- Pełnomocnik ds. SZBI,
- Pełnomocnik ds. bezpieczeństwa Cyberprzestrzeni MR,
- Administratorzy Techniczni odpowiadający za bezpieczeństwo CST,

- dodatkowe osoby wyznaczone przez Dyrektora Departamentu Informatyki.

Ponadto pozostałe role dotyczące bezpieczeństwa, obejmujące swoim działaniem również CST, zostały opisane w dokumentach:

- Polityce Bezpieczeństwa Systemów Teleinformatycznych w Ministerstwie Rozwoju, pkt 4.1.,
- Zarządzeniu nr 20 Ministra Rozwoju z dnia 11 kwietnia 2016 r. w sprawie wyznaczenia pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni Ministerstwa Rozwoju,
- Regulaminie bezpieczeństwa informacji przetwarzanych w centralnym systemie teleinformatycznym,
- Regulaminie bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego,
- Procedurze obsługi zgłoszeń w Service Desk centralnego systemu teleinformatycznego.

3. Bezpieczeństwo zasobów ludzkich

3.1.1. Odpowiedzialność kierownictwa

Zgodnie z pkt 1 *Polityki Systemu Zarządzania Bezpieczeństwem Informacji dla CST* Dyrektor Departamentu Informatyki odpowiedzialny za utrzymanie, rozwój i nadzór nad Centralnym Systemem Teleinformatycznym zgodnie z obowiązującymi wymogami prawa i rynku wprowadza System Zarządzania Bezpieczeństwem Informacji w zarządzaniu Centralnym Systemem Teleinformatycznym oraz deklaruje pełne wsparcie dla podejmowanych działań uzasadnionych realizacją celów zabezpieczenia przetwarzanych danych w CST. Ponadto podejmuje się uświadamiania podległym pracownikom wagi prowadzonych działań mających na celu zabezpieczenie danych i ich roli w systemie. Deklaruje również wsparcie dla wdrożonego systemu zarządzania i podejmowanie odpowiednich reakcji na zaistniałe sytuacje zagrażające bezpieczeństwu informacji przetwarzanych w ramach systemów należących do CST.

4. Kontrola dostępu

4.1. Zarządzanie dostępem użytkowników

4.1.1. Rejestrowanie i wyrejestrowanie użytkowników

W przedmiotowym obszarze funkcjonują *Wytyczne w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020*. Zgodnie z ww. wytycznymi wyróżnia się następujące rodzaje użytkowników:

- Użytkownicy B (osoby wskazane przez Beneficjenta i upoważnione do obsługi SL2014) – mające dostęp do SL2014, na podstawie wniosków o nadanie, zmianę i wycofanie uprawnień (załącznik nr 3 do ww. wytycznych), składanych zgodnie z *Procedurą zgłaszania osób uprawnionych*, stanowiącą załącznik nr 4 do ww. wytycznych. Zgodnie z procedurą zgłoszenie osoby uprawnionej następuje przy podpisaniu umowy o dofinansowanie. Następnie instytucja

podpisująca umowę o dofinansowanie z Beneficjentem przed wprowadzeniem danych do SL2014 weryfikuje poprawność zgłoszenia. Po weryfikacji dane wprowadzane są do SL2014.

Aktualizacja listy osób uprawnionych w SL2014 na podstawie wniosków o nadanie/zmianę/wycofanie uprawnień może nastąpić po przekazaniu przez Beneficjenta zgłoszenia aktualizacji listy osób uprawnionych, w ramach edycji umowy o dofinansowanie lub w zależności od decyzji instytucji, po podpisaniu aneksu/zmiany do umowy o dofinansowanie.

– Użytkownicy I (m.in. pracownicy IK, pracownicy IZ, pracownicy IP lub IW) – mający dostęp do SL2014 lub SL2014 wraz z SRHD, na podstawie wniosków o nadanie uprawnień, zgodnie z procedurą 1 określoną w załączniku nr 1 do ww. wytycznych. Zgodnie z procedurą, zaakceptowany przez kierownika właściwej komórki organizacyjnej lub osobę upoważnioną wniosek zostaje przesłany za pośrednictwem poczty e-mail do Administratora Merytorycznego Instytucji Zarządzającej (AM IZ). Po akceptacji AM IZ wniosek przekazywany jest do akceptacji Administratora Merytorycznego Instytucji Koordynującej (AM IK). AM IK po akceptacji wniosku, nadaje uprawnienia oraz przesyła informacje do użytkownika, dla którego zrealizowano wniosek.

  Wycofanie uprawnień określone zostało w *Procedurze wycofania i czasowego wycofania uprawnień Użytkowników I w CST* opisanej w załączniku nr 1 do ww. wytycznych. Zgodnie z procedurą kierownik właściwej komórki organizacyjnej (IW/IZ/IP/IK) lub osoba upoważniona akceptuje wniosek o wycofanie/czasowe wycofanie uprawnień oraz przesyła go za pośrednictwem skrzynki mailowej do realizacji przez AM IK. Po weryfikacji i akceptacji AM IK realizuje zgłoszenie i przesyła informacje o wycofaniu/czasowym wycofaniu uprawnień do Użytkownika I.

W trakcie audytu okazano m.in. wniosek o nadanie uprawnień (plik Ms Excel), wniosek o wycofanie i czasowe wycofanie (plik Ms Excel), korespondencję mailowa akceptującą wniosek o wycofanie uprawnień do SL2014, skan Upoważnienia/ Pełnomocnictwa z 22 sierpnia 2018 r. do wydawania upoważnień do przetwarzania danych osobowych w zbiorze - Centralny System Teleinformatyczny.

4.1.2. Przegląd praw dostępu

Zgodnie z pkt 7.2.3 *Przegląd Praw dostępu użytkowników Polityki Bezpieczeństwa Systemów Teleinformatycznych w Ministerstwie Rozwoju* Administratorzy okresowo wykonują przeglądy uprawnień użytkowników w celu wykrycia kont pracowników, którzy zostali zwolnieni, zakończyli prace (staż, praktykę, wolontariat, usługę ekspercką) w Ministerstwie, nie wykazywali aktywności logowań na konto i podjęcia stosownych działań opisanych w Procedurze zarządzania uprawnieniami użytkowników.

Zgodnie z *Procedurą przeglądów aktywności użytkowników I* (załącznik nr 1 do *Wytycznych w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020)* Administrator Merytoryczny właściwy dla danego programu operacyjnego odpowiada za wykonanie raportu przedstawiającego stan aktywności użytkowników w poszczególnych programach operacyjnych. Następnie przekazuje notatkę w formie elektronicznej do Administratora Merytorycznego Instytucji Koordynującej ze stanem aktywności

użytkowników w systemie. Za wycofanie uprawnień dla Użytkowników I, których konta nie były aktywne przez 4 miesiące, odpowiedziany jest Administrator Merytoryczny IZ.

Za przegląd praw dostępu w CST jest odpowiedzialny Departament Koordynacji Wdrażania Funduszy Unii Europejskiej. W trakcie audytu wykonano raport, przedstawiający informacje o użytkownikach, którzy się jeszcze nie logowali do SL2014 lub logowali w okresie od 18.08.2018 r. do 18.12.2018 r. Następnie przedstawiono wniosek o wycofanie i czasowe wycofanie uprawnień przekazany drogę elektroniczną (e-mail) do akceptacji oraz akceptację wniosku o wycofanie uprawnień po wykonanym przeglądzie.

4.1.3. Odbieranie lub dostosowywanie praw dostępu

Za odbieranie lub przydzielanie uprawnień w CST jest odpowiedzialny Departament Koordynacji Wdrażania Funduszy Unii Europejskiej Ministerstwa Inwestycji i Rozwoju. Odbieranie lub zmiana praw dostępu Administratorów Technicznych CST odbywa się według *Procedury zarządzania uprawnieniami użytkowników*. Opisane w pkt 4.1.1. Jednakże zgodnie z uzyskanymi informacjami najczęściej odbieranie uprawnień odbywa się w wyniku przeprowadzanych przeglądów aktywności użytkowników w SL2014.

4.2. Kontrola dostępu do systemów i aplikacji

4.2.1. Kontrola dostępu do kodów źródłowych programów

Departament Informatyki, zgodnie z zapisami umowy utrzymaniowej CST, ma dostęp do kodów źródłowych CST oraz przechowuje kopie zapasowe kodów źródłowych. Dostęp odbywa się zgodnie z załącznikiem nr 1 do *Procedury archiwizacji produktów w procesie rozwoju oprogramowania CST.*

Zgodnie z *Procedurą archiwizacji produktów w procesie rozwoju oprogramowania CST* wykonawca łączy się z serwerem (serwer przesiadkowy), na którym umieszcza kody źródłowe aplikacji CST za pomocą szyfrowanego kanału VPN, skąd wyznaczeni pracownicy DI (Wydział Centralnego Systemu Teleinformatycznego) kopiują kody źródłowe aplikacji CST na serwer stanowiącym repozytorium SVN. Zapisane kody na obu serwerach nie są usuwane.

5. Bezpieczna eksploatacja

5.1. Kopie zapasowe

5.1.1. Zapasowe kopie informacji

Polityka tworzenia kopii zapasowych dla CST tworzona jest na podstawie centralnej procedury Ministerstwa opisanej w *Polityce bezpieczeństwa systemów teleinformatycznych w Ministerstwie Rozwoju* rozdział 10.3, z której wynika iż w Ministerstwie funkcjonuje centralny system wykonywania kopii zapasowych i archiwizacji. Zgodnie z uzyskanymi informacjami, za wykonywanie kopii zapasowych odpowiedzialny jest system AVAMAR, w którym kopie bezpieczeństwa bazy Oracle dla grupy D_ORCL_STD_GRP1 tworzone są w każdą środę, piątek, niedzielę z retencją danych 14 dni, a dla grupy H_ORCL_STD_GRP1 tworzone są codziennie z retencją danych 14 dni, oraz backup systemu plików dla grupy D_FILE_STD_GRP1 również tworzony jest codziennie z retencją danych 30 dni.

Jednocześnie na podstawie umowy DI/BDG-III/4/2016 zawartej 16.06.2016 r. kopie zapasowe baz danych oraz kody źródłowe przekazywane są raz na pół roku przez firmę Atos Polska S.A. Powyższe potwierdzają *Protokoły przekazania* z dnia 10.01.2018 r. oraz z dnia 26.07.2018 r. Następnie potwierdzono, że przekazane kopie przechowywane są w zamkniętym pomieszczeniu, w sejfie. Pomieszczenie zostało wyposażone w elektroniczny system kontroli dostępu.

W trakcie prac audytowych ustalono, iż:

Ustalenie nr 6	Brak formalnych procedur określających sposób postępowania po otrzymaniu kopii zapasowych baz danych oraz kodów źródłowych od firmy Atos. Jednocześnie stwierdzono, iż Protokoły przekazania kopii zapasowych zawierają informacje, jakie dane przekazywane są na dyskach HDD, jednakże z uwagi na przechowywanie Protokołów przekazania i dysków HDD w różnych miejscach, dyski HDD nie są w odpowiedni sposób opisywane.
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne.
Rekomendacja	Zaleca się sformalizowanie procesu przechowywania dysków zawierających kopie zapasowe baz danych oraz kody źródłowe.
Odpowiedź MIiR	Procedura *SZBI.CST.P – 12 Procedura archiwizacji produktów w procesie rozwoju oprogramowania CST* zostanie uzupełniona o zapisy regulujące oznaczanie i postepowanie z dyskami i kodami źródłowymi. Termin realizacji 1 miesiąc.
Stanowisko IA	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up. MIiR powinno wdrożyć rekomendację w przeciągu 6 miesięcy.

Ustalenie nr 7	MIiR jest w trakcie budowy środowiska zapasowego Centralnego Systemu Teleinformatycznego w chmurze Oracle. W trakcie wykonywania czynności w ramach audytu przedstawiono zaakceptowaną przez Dyrektora Departamentu Informatyki Procedurę migracji CST do Oracle Cloud, zawierającą opisy procedur, kluczowych ról, niezbędnych zasobów do przeprowadzenia migracji.
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne.
Rekomendacja	Zaleca się przyspieszenie podejmowanych działań i uruchomienie środowiska zapasowego CST zgodnie z zapisami zawartymi w *Procedurze migracji CST do Oracle Cloud.*

odpowiedź MIiR	Środowisko zapasowe w Oracle Cloud jest już uruchomione i w gotowości operacyjnej do przeprowadzenia migracji zgodnie z tą procedurą.
Stanowisko IA	IA zapoznała się ze stanowiskiem MIiR. Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.

5.2. Wymagania związane z bezpieczeństwem systemów informacyjnych

5.2.1. Analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji

Zgodnie z *Polityką bezpieczeństwa systemów teleinformatycznych w Ministerstwie Rozwoju* rozdział 12.1.1. *Analiza i specyfikacja wymagań bezpieczeństwa teleinformatycznego*, specyfikacje istotnych warunków zamówienia, dotyczące nowych systemów teleinformatycznych zamawianych przez Ministerstwo u zewnętrznych dostawców, muszą zawierać wymagania bezpieczeństwa tych systemów. Wymagania te są włączane do umów z dostawcami. W procesie zamawiania przez Ministerstwo systemów teleinformatycznych sprawdza się, czy spełniają one następujące wymagania:

- sprawdzanie poprawności danych wejściowych,
- potwierdzanie poprawności przetwarzania w celu wykrywania naruszenia integralności danych w wyniku błędów przetwarzania lub działań umyślnych,
- zabezpieczenia integralności danych,
- sprawdzanie poprawności danych wyjściowych,
- logowanie następujących zdarzeń: logowanie i wylogowanie użytkownika, krytyczne operacje w systemie teleinformatycznym.

Z kolei, zgodnie z pkt 12.2 *Bezpieczeństwo w procesach rozwoju i wsparcia*, wszystkie zmiany w systemach teleinformatycznych i sieciowych podlegają kontroli. Po dokonaniu zmian w systemach operacyjnych lub aplikacjach są przeprowadzane testy i przeglądy aplikacji, aby uzyskać pewność, że wprowadzone zmiany nie mają niekorzystnego wpływu na funkcjonalność, wydajność i bezpieczeństwo systemów teleinformatycznych Ministerstwa.

W ramach audytu zbadano nowe moduły, które zostały zaimplementowane w aplikacji od ostatniego audytu przeprowadzonego przez IA, tj.: moduł baza personelu, moduł dokumentacja oraz moduł instrumenty finansowe.

W trakcie czynności ustalono, iż w systemie zaimplementowano szereg mechanizmów kontrolnych uniemożliwiających wprowadzenie błędnych danych w tym m. in.:

- walidacja pól dotyczących wymiaru czasu pracy z uwagi na przekroczenie 276 godzin miesięcznie przez osobę o danym numerze PESEL oraz z uwagi na podaną większą liczbę godzin czasu pracy od podanej dla danego stanowiska liczby godzin w miesiącu,

- walidacja pola PESEL,
- walidacja pola dotyczącego okresu zaangażowania (pole wymagane) oraz podawanych dat (data w „polu do" nie może być wcześniejsza od daty rozpoczęcia zaangażowania w projekcie „pole od", data rozpoczęcia konkursu nie może być większa od daty zakończenia),
- brak możliwości dodania do modułu dokumentacja ponownie tego samego pliku (plik o takiej samej nazwie lub identyfikatorze) lub pliku wykonywalnego,
- data podpisania umowy nie może być wcześniejsza od daty rozpoczęcia projektu (formatka instrumenty finansowe).

6. Relacje z dostawcami

6.1. Zarządzanie usługami świadczonymi przez dostawców

6.1.1. Monitorowanie i przegląd usług świadczonych przez dostawców

Ministerstwo monitoruje dostawców usług pod kątem zgodności działania usługi z prawem polskim. W umowach z firmą utrzymującą system CST są uwzględnione kwestie raportowania w formie formularza *Raportu miesięcznego świadczenia usługi utrzymania systemów informatycznych*. Dane przekazywane w *Raporcie miesięcznym świadczenia usługi utrzymania systemów informatycznych* są weryfikowane pod względem merytorycznym przez pracowników Wydziału Centralnego Systemu Teleinformatycznego Departamentu Informatyki m.in. za pomocą Google Analytics, internetowego darmowego narzędzia do analizy statystyk serwisów WWW, udostępnianego przez firmę Google.

7. Audyt stanu wdrożenia rekomendacji otwartych z lat ubiegłych

Poniższe rekomendacje zostały ujęte w Sprawozdaniu z audytu Głównego Systemu Informatycznego wykorzystywanego przy wdrażaniu programów operacyjnych w perspektywie finansowej 2014-2020, przeprowadzonego w grudniu 2017 r.

Ustalenie nr 9	Domena, pod którą dostępny jest system SL2014 https://sl.gov.pl/ i https://slowniki.sl.gov.pl/ umożliwia nawiązanie połączenia pomiędzy klientem i serwerem z wykorzystaniem protokołu TLS w wersji 1.0.
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne
Rekomendacja	Zaleca się wyłączenie obsługi protokołu TLS 1.0 z uwagi na podatność na ataki POODLE.
Odpowiedź jednostki	Po uprzednim poinformowaniu LSI o zmianach w komunikacji z SL2014, zostaną wyłączone przez Wykonawcę podatne protokoły. Termin realizacji: 6 m-cy
Stanowisko	Stan wdrożenia rekomendacji będzie przedmiotem audytu

Instytucji Audytowej	follow-up.
Stan wdrożenia rekomendacji wg MIiR	W trakcie wdrożenia – zmiana wejdzie na produkcję 15 grudnia 2018 r.
Stan wdrożenia 2018 r.	**Rekomendacja wdrożona, zamknięta**

Ustalenie nr 10	Słowniki proste udostępniane dla systemów LSI nie posiadają identyfikatorów (kluczy) tak, aby jednoznacznie wskazać daną pozycję słownikową. Dane identyfikowane są po nazwach (stringach).
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne
Rekomendacja	Zaleca się wprowadzenie identyfikatorów w słownikach prostych udostępnianych LSI.
Odpowiedź jednostki	W przypadku słowników prostych unikalnym identyfikatorem jest jego wartość, dlatego też niezasadne jest dodawanie klucza sztucznego w postaci dodatkowego identyfikatora.
Stanowisko Instytucji Audytowej	Rekomendacja podtrzymana. Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.
Stan wdrożenia rekomendacji wg MIiR	Rekomendacja wdrożona w Zleceniu SL2014/ZUD/12/2018, instalacja na produkcji 10.05.2018 r.
Stan wdrożenia 2018 r.	**Rekomendacja wdrożona, zamknięta**

Ustalenie nr 11	Aktualizowanie słowników wiąże się z usuwaniem nieaktualnych wpisów (dotyczy nazw miejscowości). Ponadto w przypadku nazw ulic usuwane są poszczególne rekordy ze słownika z nazwami, a następnie dodawana jest nowa pozycja w słowniku bez możliwości mapowania starej nazwy ulicy z nową.
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne
Rekomendacja	Zaleca się aby pozycje słownikowe ulegające zmianie nie były usuwane ze słownika (przejmowały znacznik aktywny/ nieaktywny). Dodatkowo w odniesieniu do nazw ulic zaleca się, aby w przypadku zmiany nazwy ulicy (usunięciu starego rekordu i dodania nowego) nowy rekord zawierał również ID rekordu

	zastępowanego, umożliwiając zidentyfikowanie wartości zmiany.
Odpowiedź jednostki	Zostanie zrealizowana modyfikacja słowników: miejscowości (slMiejscowości), ulic (slUlice) oraz jednostek geograficznych (slJednostkiGeo), mająca na celu wprowadzenie przechowywania starej nazwy miejscowości/ ulicy/ gminy/ powiatu w sytuacji, gdy nazwa ulega zmianie w momencie aktualizacji danych z TERYT oraz daty tej zmiany i wystawienie tych informacji użytkownikom przez webservice (SOLR). Wartości prezentowane będą tylko w przypadku elementów, które uległy zmianie. Termin realizacji: 6 m-cy
Stanowisko Instytucji Audytowej	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.
Stan wdrożenia rekomendacji wg MIiR	Rekomendacja wdrożona w Zleceniu SL2014/ZUD/12/2018, instalacja na produkcji 10.05.2018 r.
Stan wdrożenia 2018 r	**Rekomendacja wdrożona, zamknięta**

Ustalenie nr 13	W planach ciągłości działania CST określono, iż decyzję o podjęciu działań w przypadku awarii krytycznych i uruchomieniu planu awaryjnego podejmuje wykonawca, upoważniony przez niego pracownik lub Kierownik projektu: Rozwój i utrzymanie systemów informatycznych Ministerstwa Rozwoju wspierających realizację programów operacyjnych współfinansowanych ze środków UE, w tym centralnego systemu teleinformatycznego, podczas gdy plan odnosi się wyłącznie do działań podejmowanych przez Ministerstwo Rozwoju. Ponadto w dokumencie brakuje danych kontaktowych do osób zaangażowanych w zapewnienie ciągłości działania.
Kategoria	Kategoria 1 – System działa dobrze, tylko niewielkie usprawnienia są potrzebne
Rekomendacja	Zaleca się przegląd dokumentu oraz doprecyzowanie/usunięcie zbędnych zapisów, a także uzupełnienie dokumentu o dane kontaktowe do osób zaangażowanych w zapewnienie ciągłości działania.
Odpowiedź jednostki	Dokument zostanie przejrzany i uzupełniony. Termin realizacji: 6 m-cy
Stanowisko Instytucji	Stan wdrożenia rekomendacji będzie przedmiotem audytu

Audytowej	follow-up.
Stan wdrożenia rekomendacji	Aktualizacja dokumentu do wersji 1.5 z dnia 25.05.2018 r.
Stan wdrożenia 2018 r	**Rekomendacja wdrożona, zamknięta**

Ustalenie nr 14	Instytucja Audytowa otrzymała raport z odtwarzania źródeł aplikacji systemu SL2014 na infrastrukturze MR, jednak nie udało się potwierdzić testowania planów ciągłości działania zarówno tych utworzonych przez MR, jak i BCM firmy ATOS.
Kategoria	Kategoria 2 – System działa, ale konieczne są usprawnienia
Rekomendacja	Zaleca się przetestowanie planów ciągłości działania i udokumentowanie ich.
Odpowiedź jednostki	Plany zostaną przetestowane (SZBI) lub zostaną dostarczone dowody zgodnie z procedurą (Atos). Termin realizacji: 9 m-cy.
Stanowisko Instytucji Audytowej	Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.
Stan wdrożenia rekomendacji	MIiR jest w trakcie modyfikacji planów ciągłości działania pod kątem uwzględnienia budowanego środowiska zapasowego CST w chmurze Oracle. Atos przedstawił załączone wyjaśnienie w sprawie planów ciągłości działania.
Stan wdrożenia 2018 r	**Stan wdrożenia rekomendacji będzie przedmiotem audytu follow-up.**

Z upoważnienia
Szefa Krajowej Administracji Skarbowej

Paweł Cybulski

Zastępca Szefa Krajowej Administracji Skarbowej
/podpisano kwalifikowanym podpisem elektronicznym/