Warszawa, 03 października 2008 r.

Ministerstwo Finansów
Generalny Inspektor Kontroli Skarbowej

DO2/9013/14/593/JBG/08/1901

Pan
Dirk Ahner
Dyrektor
Dyrekcja Generalna
ds. Polityki Regionalnej
Komisja Europejska
Avenue de Tervueren 41
B-1049 Brussels
Belgium

Zgodnie z art. 71 ust. 2 *rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999* przekazuję w załączeniu następujące dokumenty:

- Sprawozdanie z audytu zgodności Regionalnego Programu Operacyjnego Województwa Podlaskiego;
- Opinię w sprawie zgodności systemów zarządzania i kontroli;
- Oświadczenie o kompetencji i niezależności działania.

PODSEKRETARZ STANU
Generalny Inspektor Kontroli Skarbowej

Andrzej Parafianowicz

Do wiadomości: (bez załącznika)

1. Pan Jan Tombiński – Ambasador, Stały Przedstawiciel RP przy Unii Europejskiej, Avenue de Tervueren 282-284, 1150 Brussels, Belgium

RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

GENERALNY INSPEKTOR KONTROLI SKARBOWEJ

DO2/9013/14/593/JBG/08/190.1

Sprawozdanie z audytu zgodności Regionalnego Programu Operacyjnego Województwa Podlaskiego

(nr kodu CCI 2007 PL 16 1 PO 014)

Warszawa, październik 2008 r.

Spis treści

1. WSTĘP

1.1. Cel sprawozdania

Art. 71 ust 2 rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999 oraz art. 25 rozporządzenia Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006 r. ustanawiającego szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 nakładają na państwo członkowskie obowiązek przeprowadzenia badania audytowego w celu uzyskania zapewnienia, że systemy zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58-62 rozporządzenia Rady (WE) nr 1083/2006 i przepisami sekcji 3 rozporządzenia Komisji (WE) nr 1828/2006.

Sprawozdanie prezentuje wyniki czynności sprawdzających wykonanych przez pracowników Departamentu Ochrony Interesów Finansowych Unii Europejskiej Ministerstwa Finansów w Departamencie Instytucji Certyfikującej (pełniącym funkcję Instytucji Certyfikującej) w Ministerstwie Rozwoju Regionalnego (MRR) oraz inspektorów i pracowników Urzędu Kontroli Skarbowej w Białymstoku w Urzędzie Marszałkowskim Województwa Podlaskiego (pełniącym funkcję Instytucji Zarządzającej) oraz w Podlaskim Urzędzie Wojewódzkim w Białymstoku (pełniącym funkcję Instytucji Pośredniczącej w Certyfikacji).). Ponadto w sprawozdaniu przedstawiono wyniki samooceny dokonanej przez Instytucję Audytową.

Celem niniejszego sprawozdania jest przedstawienie zakresu i wyników prac będących podstawą oceny systemów zarządzania i kontroli w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego, a tym samym potwierdzenie, że systemy zarządzania i kontroli ustanowione zostały zgodnie z wymogami wspólnotowymi (tj. art. 58-62 rozporządzenia Rady (WE) nr 1083/2006 i przepisami sekcji 3 rozporządzenia Komisji (WE) nr 1828/2006).

1.2. Zakres sprawozdania

Sprawozdanie obejmuje wyniki prac audytowych będących podstawą oceny systemów zarządzania i kontroli w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego, finansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego, ustanowionego w Instytucji Zarządzającej (Zarząd Województwa Podlaskiego), Instytucji Certyfikującej (Departament Instytucji Certyfikującej w MRR) oraz Instytucji Pośredniczącej w Certyfikacji (Wojewoda Podlaski). Ponadto w sprawozdaniu przedstawiono wyniki samooceny dokonanej przez Instytucję Audytową.

1.3. Organ odpowiedzialny za sporządzenie sprawozdania

Wykonywanie zadań instytucji odpowiedzialnej za przeprowadzenie audytu zgodności zostało powierzone Generalnemu Inspektorowi Kontroli Skarbowej, który pełni również funkcję Instytucji Audytowej dla programów operacyjnych. Generalny Inspektor Kontroli Skarbowej wykonuje swoje zadania za pośrednictwem Departamentu Ochrony Interesów Finansowych Unii Europejskiej Ministerstwa Finansów oraz 16 urzędów kontroli skarbowej (w szczególności Urzędu Kontroli Skarbowej w Białymstoku w odniesieniu do Regionalnego Programu Operacyjnego Województwa Podlaskiego). Jest on również odpowiedzialny za zatwierdzenie przedmiotowego sprawozdania, które jest opracowywane przez pracowników Departamentu Ochrony Interesów Finansowych Unii Europejskiej.

1.4. Niezależność instytucji audytowej

Zgodnie z art. 59 rozporządzenia 1083/2006, Instytucja Audytowa powinna być funkcjonalnie niezależna od Instytucji Zarządzającej i od Instytucji Certyfikującej.

Funkcję Instytucji Audytowej oraz organu odpowiedzialnego za przeprowadzenie audytu zgodności pełni Generalny Inspektor Kontroli Skarbowej, usytuowany w strukturze Ministerstwa Finansów, który jest organem niezależnym od instytucji zaangażowanych we wdrażanie Regionalnego Programu Operacyjnego Województwa Podlaskiego tj.

- Instytucji Zarządzającej programem operacyjnym (Zarząd Województwa Podlaskiego);
- Instytucji Certyfikującej (Departament Instytucji Certyfikującej w Ministerstwie Rozwoju Regionalnego) oraz
- Instytucji Pośredniczącej w Certyfikacji (Wojewoda Podlaski).

Departament Ochrony Interesów Finansowych Unii Europejskiej w Ministerstwie Finansów oraz Urząd Kontroli Skarbowej w Białymstoku, wykonujące zadania Generalnego Inspektora Kontroli Skarbowej, są niezależne od ww. instytucji wyznaczonych do wdrażania Regionalnego Programu Operacyjnego Województwa Podlaskiego.

2. METODYKA I ZAKRES PRAC AUDYTOWYCH

2.1. Ramy czasowe audytu oraz skład zespołu audytowego

Opis systemu zarządzania i kontroli wraz z towarzyszącą dokumentacją został przekazany do organu odpowiedzialnego za przeprowadzenie audytu zgodności w lutym 2008 r. Druga wersja OSZiK została przekazana w lipcu 2008r.

Ostateczna wersja OSZiK została przekazana do Instytucji Audytowej w dniu 4 września 2008 r.

Czynności audytowe prowadzone były w terminie od 4 lutego do 30 września 2008 r.

Audyt był realizowany przez zespół składający się z 31 osób.

2.2. Zakres wykonanych prac

Audyt zgodności był realizowany w Instytucji Zarządzającej (IZ), Instytucji Certyfikującej (IC) oraz Instytucji Pośredniczącej w Certyfikacji, w oparciu o program badania opracowany między innymi na podstawie wytycznych Komisji Europejskiej.

W trakcie audytu zgodności badano, czy ustanowiony system zarządzania i kontroli RPO WPo zapewnia:

- określenie funkcji podmiotów związanych z zarządzaniem i kontrolą oraz przydziału funkcji w obrębie każdego podmiotu;
- zgodność z zasadą rozdzielenia funkcji pomiędzy tymi podmiotami i w ich obrębie;
- procedury dla zapewnienia zasadności i prawidłowości wydatków zadeklarowanych w ramach programu operacyjnego;
- wiarygodne, skomputeryzowane systemy rachunkowości i księgowości, monitorowania i sprawozdawczości finansowej;
- system sprawozdawczości i monitorowania, w przypadku gdy podmiot odpowiedzialny powierza wykonanie zadań innemu podmiotowi;
- ustalenia dotyczące audytu funkcjonowania systemów;
- systemy i procedury w celu zapewnienia stosowania właściwej ścieżki audytu;
- procedury sprawozdawczości i monitorowania nieprawidłowości oraz odzyskiwania kwot nienależnie wypłaconych.

W trakcie audytu zgodności w Instytucji Zarządzającej zbadano, czy:

- zapewniono, że operacje są wybierane do finansowania zgodnie z kryteriami mającymi zastosowanie do programu operacyjnego oraz że spełniają one mające zastosowanie zasady wspólnotowe i krajowe przez cały okres ich realizacji;
- zapewniono weryfikację, że współfinansowane towary i usługi będą dostarczone oraz że wydatki zadeklarowane przez beneficjentów

na operacje zostały rzeczywiście poniesione i są zgodne z zasadami wspólnotowymi i krajowymi;

- zapewniono istnienie informatycznego systemu rejestracji i przechowywania zapisów księgowych dla każdej operacji w ramach programu operacyjnego oraz czy zapewniono, że dane na temat realizacji, niezbędne do celów zarządzania finansowego, monitorowania, weryfikacji, audytu i oceny są gromadzone;
- zapewniono utrzymywanie przez beneficjentów i inne podmioty uczestniczące w realizacji operacji odrębnego systemu księgowego albo odpowiedniego kodu księgowego dla wszystkich transakcji związanych z operacją, bez uszczerbku dla krajowych zasad księgowych;
- zapewniono, że oceny programów operacyjnych, o których mowa w art. 48 ust. 3 RR 1083/2006, są przeprowadzane zgodnie z art. 47;
- ustanowiono procedury dla zapewnienia, że wszystkie dokumenty dotyczące wydatków i audytów, wymagane do realizacji właściwej ścieżki audytu, są przechowywane zgodnie z wymogami art. 90 RR 1083/2006;
- zapewniono otrzymywanie przez instytucję certyfikującą wszystkich niezbędnych informacji o procedurach i weryfikacjach prowadzonych w odniesieniu do wydatków na potrzeby poświadczania;
- zapewniono kierowanie pracą komitetu monitorującego i dostarczanie mu dokumentacji wymaganej w celu umożliwienia monitorowania jakościowego realizacji programu operacyjnego w świetle jego szczegółowych celów;
- zapewniono opracowywanie i przedkładanie Komisji rocznych i końcowych sprawozdań z realizacji, po ich uprzednim zatwierdzeniu przez komitet monitorujący;
- zapewniono przestrzeganie wymogów w zakresie informacji i promocji ustanowionych w art. 69 RR 1083/2006;
- zapewniono dostarczanie Komisji informacji umożliwiających jej dokonanie oceny dużych projektów;
- systemy informatyczne (KSI SIMIK 07-13 oraz system finansowo-księgowy) funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych, są ustanowione zgodnie z wymogami art. 58d) oraz 60c) RR 1083/2006.

W trakcie audytu zgodności w Instytucji Certyfikującej i Instytucji Pośredniczącej w Certyfikacji zbadano, czy istnieją procedury zapewniające:

- opracowywanie i przedkładanie Komisji poświadczonych deklaracji wydatków i wniosków o płatność;
- poświadczanie, że:
  - deklaracja wydatków jest dokładna, wynika z wiarygodnych systemów księgowych i jest oparta na weryfikowalnej dokumentacji uzupełniającej;
  - zadeklarowane wydatki są zgodne z mającymi zastosowanie zasadami wspólnotowymi i krajowymi oraz zostały poniesione w związku

z operacjami wybranymi do finansowania zgodnie z kryteriami mającymi zastosowanie do programu i spełniają zasady wspólnotowe i krajowe;

- otrzymywanie, do celów poświadczenia, od instytucji zarządzającej odpowiednich informacji na temat procedur i weryfikacji prowadzonych w związku z wydatkami zawartymi w deklaracjach wydatków;
- uwzględnianie, do celów poświadczenia, wyników wszystkich audytów przeprowadzanych przez instytucję audytową lub na jej odpowiedzialność;
- utrzymywanie w formie elektronicznej zapisów księgowych dotyczących wydatków zadeklarowanych Komisji;
- prowadzenie ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych po anulowaniu całości lub części wkładu dla operacji.

Zespół audytowy przeprowadził czynności sprawdzające w oparciu o program badania audytu zgodności. Głównymi obszarami badania były:

- struktura organizacyjna jednostki;
- zasoby ludzkie;
- procedury zarządzania ryzykiem;
- mechanizmy kontrolne, które eliminują bądź ograniczają zidentyfikowane ryzyka;
- system księgowy;
- system monitoringu;
- procesy związane z informacją i komunikacją.

W trakcie audytu zgodności wykorzystywane były następujące techniki:

- analiza przepisów prawnych, procedur, wytycznych, instrukcji i programów operacyjnych;
- rozmowy i wywiady z kierownictwem oraz pracownikami instytucji zaangażowanych we wdrażanie Programu.

W związku z faktem, że funkcja instytucji odpowiedzialnej za przeprowadzenie audytu zgodności została powierzona Generalnemu Inspektorowi Kontroli Skarbowej, który pełni również funkcję Instytucji Audytowej dla programów operacyjnych, Instytucja Audytowa dokonała samooceny przygotowania do realizacji zadań określonych w art. 62 rozporządzenia 1083/2006.

2.2.1. ZAKRES PRAC WYKONANYCH W INSTYTUCJI ZARZĄDZAJĄCEJ

W trakcie czynności związanych z przeprowadzeniem audytu zgodności w Instytucji Zarządzającej Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007 – 2013, dokonano analizy następujących dokumentów:

- Rozporządzenie Parlamentu Europejskiego (WE) z dnia 5 lipca 2006 r. nr 1080/2006 w sprawie Europejskiego Funduszu Rozwoju Regionalnego i uchylające rozporządzenie (WE) nr 1783/1999;
- Rozporządzenie Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju

Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylające rozporządzenie (WE) nr 1260/1999;

- Rozporządzenie Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006 r. ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999;
- Regionalny Program Operacyjny Województwa Podlaskiego na lata 2007-2013,Szczegółowy Opis Priorytetów RPO WPo na lata 2007-2013- przyjęty Uchwałą Zarządu Województwa Podlaskiego Nr 88/1210/08 z dnia 13 maja 2008r.,
- Opis Systemu Zarządzania i Kontroli Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013- przyjęty Uchwałą Zarządu Województwa Podlaskiego Nr 94/1268/08 z dnia 03 czerwca 2008r.,
- Instrukcja Wykonawcza IZ RPO WPo na lata 2007-2013,
- Kryteria wyboru projektów przyjęte przez Komitet Monitorujący RPO WPo:
  - Kryteria formalne oceny wniosków w ramach RPO WPo na lata 2007-2013,
  - Kryteria merytoryczno-techniczne dopuszczające (wstępne),
  - Kryteria merytoryczno-techniczne ogólne,
  - Kryteria merytoryczno – techniczne szczegółowe dla Osi Priorytetowych I-VI,
  - Kryteria formalno-merytoryczne dla Priorytetu VII Pomoc Techniczna,
- Podręcznik dla Beneficjenta RPO WPo na lata 2007-2013 – z marca 2008r. opublikowany na stronie internetowej Urzędu Marszałkowskiego Województwa Podlaskiego w dniu 16 kwietnia 2008r.,
- Regulamin Organizacyjny Urzędu Marszałkowskiego Województwa Podlaskiego w Białymstoku, przyjęty Uchwałą Zarządu Województwa Podlaskiego Nr 74/941/08 z dnia 11 marca 2008r., zmieniony Uchwałą Nr 101/1388/08 z dnia 01 lipca 2008r.,
- Wytyczne w zakresie kwalifikowania wydatków w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013 – przyjęte Uchwałą Zarządu Województwa Podlaskiego Nr 108/1487/08 z dnia 05 sierpnia 2008r.,
- Instrukcję w sprawie organizacji i zakresu działania archiwum zakładowego oraz zasad i trybu postępowania z dokumentacją w Urzędzie Marszałkowskim Województwa Podlaskiego wprowadzonej Zarządzeniem nr 11/03 Marszałka Województwa Podlaskiego z dnia 10.03.2003r.,
- „Zasady (polityka) rachunkowości w zakresie funduszy pomocowych dla Urzędu Marszałkowskiego jako jednostki budżetowej",
- Plan Komunikacji Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013,
- zakresy obowiązków pracowników i opisy stanowisk,

- indywidualne karty szkoleń pracowników zaangażowanych w realizację zadań związanych z RPO WPo,
- plan zatrudnienia, formularze zapotrzebowania na pracowników,
- sprawozdanie z audytu wewnętrznego, zadanie audytowe nr 08/2007 „Audyt zgodności systemów zarządzania i kontroli RPO WPo na 2007-2013", Białystok, wrzesień 2007,
- Wytyczne Ministerstwa Rozwoju Regionalnego w zakresie:
  - kwalifikowania wydatków w ramach RPO WPo na lata 2007-2013,
  - gromadzenia i przekazywania danych w formie elektronicznej,
  - informacji i promocji,
  - szczegółowego opisu priorytetów programu operacyjnego,
  - jednolitego systemu zarządzania i monitoringu projektów indywidualnych zgodnych z art. 28 ust. 1 pkt 1 Ustawy z dnia 6 grudnia 2006r. o zasadach prowadzenia polityki rozwoju,
  - procesu kontroli w ramach obowiązków Instytucji Zarządzającej Programem Operacyjnym,
  - wybranych zagadnień związanych z przygotowaniem projektów inwestycyjnych, w tym projektów generujących dochód,
  - warunków certyfikacji oraz przygotowania wniosków o płatność do Komisji Europejskiej w Programach Operacyjnych w ramach NSRO na lata 2007-2013,
  - sprawozdawczości,
- Strategię Komunikacji Funduszy Europejskich w Polsce na lata 2007-2013,
- Rozporządzenie Prezesa Rady Ministrów z dnia 18 grudnia 1998 w sprawie instrukcji kancelaryjnej dla organów samorządu województwa,
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 1999 zmieniającym rozporządzenie w sprawie instrukcji kancelaryjnej dla organów samorządu województwa.

W trakcie audytu sprawdzono, czy:

- istnieją pisemne procedury regulujące proces wdrażania i zarządzania Regionalnym Programem Operacyjnym Województwa Podlaskiego;
- zachowana została zasada rozdziału funkcji w ramach Instytucji Zarządzającej;
- pracownicy zaangażowani w realizację zadań mają określone zakresy obowiązków;
- pracownicy są przygotowani merytorycznie do realizacji zadań;
- procedury określają sposób informowania pracowników o aktualizacji dokumentów niezbędnych do prawidłowego wykonywania zadań;
- procedury zapewniają dokonywanie okresowych przeglądów procedur i ich aktualizację, wyznaczenie osób odpowiedzialnych za te procesy;
- procedury zapewniają uwzględnianie dla celów zarządzania finansowego programem operacyjnym wszystkich audytów przeprowadzanych przez IA;

- procedury zapewniają podejmowanie czynności usprawniających w przypadku wykrycia przez Instytucję Audytową lub inne instytucje, słabości w systemie;
- Instytucja Zarządzająca zarządza ryzykiem wewnętrznym.

Zbadano procesy związane z:

- ogłaszaniem konkursów i naborem wniosków o dofinansowanie projektów konkursowych,
- oceną formalną i merytoryczną wniosków konkursowych i indywidualnych oraz zatwierdzaniem projektów konkursowych i indywidualnych,
- podpisywaniem i aneksowaniem umów o dofinansowanie projektów,
- sprawozdawczością i monitorowaniem realizacji projektu,
- zapewnieniem bezpieczeństwa systemów informatycznych,
- weryfikacją wniosków o płatność beneficjentów,
- dokonywaniem płatności na rzecz beneficjentów,
- sporządzaniem, poświadczaniem i przedkładaniem do Instytucji Certyfikującej poświadczeń i deklaracji dokonanych wydatków,
- prowadzeniem ewidencji księgowej wydatków zadeklarowanych do Instytucji Certyfikującej,
- prowadzeniem ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych (prowadzeniem „rejestru dłużników"),
- odzyskiwaniem nieprawidłowo wydatkowanych środków,
- planowaniem i realizacją kontroli projektów,
- pozyskiwaniem i analizowaniem w procesie zarządzania wdrażaniem RPO WPo wyników kontroli i audytów przez inne instytucje upoważnione,
- opiniowaniem i akceptacją Instrukcji Wykonawczej Instytucji Zarządzającej RPO WPo na lata 2007-2013,
- wprowadzaniem zmian do Instrukcji Wykonawczej,
- informacją, promocją i szkoleniami,
- archiwizacją dokumentów.

W trakcie audytu zgodności realizowanego w Instytucji Zarządzającej przeprowadzono wywiady (w sumie 7 spotkań) z kierownictwem (zastępcą dyrektora departamentu,, kierownikami referatów) oraz 3 pracownikami Urzędu Marszałkowskiego Województwa Podlaskiego. W trakcie wywiadów poruszano w szczególności następujące zagadnienia:

- proces obsługi wniosków od momentu ogłoszenia konkursu (tryb konkursowy) lub podpisania pre-umowy z beneficjentami realizującymi projekty indywidualne do rozliczenia wniosków o płatność końcową w ramach projektu;

- zagadnienia z zakresu sprawozdawczości na poziomie IZ oraz działań informacyjnych i promocyjnych podejmowanych przez IZ w ramach jej obowiązków;
- proces sporządzania sprawozdań z realizacji RPO WPo, sporządzania poświadczeń i deklaracji wydatków oraz wniosków o płatność od IZ do IC, działań monitoringowych.

Ponadto w IZ przeprowadzony został przegląd systemów informatycznych wykorzystywanych przy dystrybucji środków finansowych RPOPo oraz ogólnego środowiska informatycznego, w jakim one funkcjonują.

Celem tego badania było uzyskanie zapewnienia, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych, są ustanowione zgodnie z wymogami rozporządzenia 1083/2006.

Szczegóły badania zostały przedstawione w *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Urzędu Marszałkowskiego Województwa Podlaskiego* (załącznik nr 1 do niniejszego sprawozdania).

2.2.2. ZAKRES PRAC WYKONANYCH W INSTYTUCJI CERTYFIKUJĄCEJ

W zakresie wykonanych prac dokonano przeglądu i oceny następujących dokumentów:

- Rozporządzenie Parlamentu Europejskiego (WE) z dnia 5 lipca 2006 r. nr 1080/2006 w sprawie Europejskiego Funduszu Rozwoju Regionalnego i uchylające rozporządzenie (WE) nr 1783/1999;
- Rozporządzenie Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylające rozporządzenie (WE) nr 1260/1999;
- Rozporządzenie Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006 r. ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999;
- Instrukcji Wykonawczej Instytucji Certyfikującej (IW IC),
- Zarządzenia nr 1 Prezesa Rady Ministrów z dnia 5 stycznia 2007r. w sprawie nadania statutu Ministerstwu Rozwoju Regionalnego;
- Zarządzenia nr 7 Prezesa Rady Ministrów z dnia 2008.01.29 w sprawie nadania statutu Ministerstwu Rozwoju Regionalnego;
- Podziału zadań w kierownictwie MRR;
- Regulaminu organizacyjnego Ministerstwa Rozwoju Regionalnego;
- Regulaminu wewnętrznego Departamentu Instytucji Certyfikującej;
- Schematu organizacyjnego Departamentu Instytucji Certyfikującej;

- Opisów stanowisk pracowników Departamentu Instytucji Certyfikującej;
- Dokonanej w 2007r. przez Departament Instytucji Certyfikującej analizy ryzyka;
- Analizy ryzyka i określenia kolejności wizyt sprawdzających w IZ;
- Rocznego planu wizyt Instytucji Certyfikującej na rok 2008;
- Ogólnego wzoru tabeli IC do celów przeliczania poniesionych wydatków z PLN na EUR - Tabela A;
- Wzoru tabeli IC do celów monitorowania poniesionych wydatków w EUR - Tabela B;
- Wytycznych w zakresie warunków certyfikacji oraz przygotowania prognoz wniosków o płatność do Komisji Europejskiej w Programach Operacyjnych w ramach Narodowych Strategicznych Ram Odniesienia na lata 2007-2013;
- Instrukcji wypełniania załącznika nr 3 do Wytycznych w zakresie certyfikacji oraz przygotowania prognoz wniosków o płatność do Komisji Europejskiej w Programach Operacyjnych w ramach Narodowych Strategicznych Ram Odniesienia na lata 2007-2013 (Poświadczenie i deklaracja wydatków oraz wniosek o płatność okresową od Instytucji Zarządzającej do Instytucji Certyfikującej dla programów krajowych);
- Wytycznych w zakresie sposobu postępowania w razie wykrycia nieprawidłowości w wykorzystaniu funduszy strukturalnych i Funduszu Spójności w okresie programowania 2007-2013;
- Opisu rejestru kwot do odzyskania, kwot odzyskanych oraz kwot wycofanych (tzw. „rejestr dłużników");
- Propozycji opisu trybu postępowania w przypadku wystąpienia nieprawidłowości skutkującej obowiązkiem zwrotu środków przez beneficjenta.

W trakcie audytu sprawdzono, czy:

- istnieją pisemne procedury regulujące proces certyfikacji;
- zachowana została zasada rozdziału funkcji pomiędzy Instytucją Certyfikującą a Instytucją Zarządzającą, a także rozdziału funkcji w ramach Instytucji Certyfikującej;
- pracownicy zaangażowani w realizację zadań mają określone zakresy obowiązków;
- pracownicy są przygotowani merytorycznie do realizacji zadań;
- procedury zapewniają uwzględnianie dla celów poświadczania wyników wszystkich audytów przeprowadzanych przez IA;
- procedury zapewniają dokonywanie okresowych przeglądów procedur i ich aktualizację, wyznaczenie osób odpowiedzialnych za te procesy;
- Instytucja Certyfikująca zarządza ryzykiem wewnętrznym;
- procedury zapewniają podejmowanie czynności usprawniających w przypadku wykrycia przez Instytucję Audytową lub inne instytucje słabości w systemie;

- zaprojektowano odpowiednie mechanizmy kontrolne minimalizujące nieodpowiednie wykonywanie zadań przez Instytucję Certyfikującą.

Zbadano procesy związane z:

- sporządzaniem, certyfikacją i przedkładaniem do Komisji Europejskiej wniosków o płatność;
- prowadzeniem ewidencji księgowej wydatków zadeklarowanych do Komisji Europejskiej;
- monitorowaniem dostępności środków w ramach alokacji i środków krajowych przeznaczonych na współfinansowanie;
- zastosowaniem Krajowego Systemu Informatycznego;
- prowadzeniem ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych (prowadzeniem „rejestru dłużników");
- odzyskiwaniem nieprawidłowo wydatkowanych środków;
- wizytami sprawdzającymi;
- pozyskiwaniem i analizowaniem w procesie certyfikacji wyników kontroli i audytów przez inne instytucje upoważnione;
- opiniowaniem i akceptacją instrukcji wykonawczych oraz oceną systemu zarządzania i kontroli przez Instytucję Certyfikującą;
- wprowadzaniem zmian do podręcznika.

W trakcie audytu zgodności realizowanego w Instytucji Certyfikującej zostały przeprowadzone wywiady (w sumie 5 spotkań) z kierownictwem (dyrekcją i naczelnikami) oraz pracownikami Departamentu Instytucji Certyfikującej w MRR. W trakcie wywiadów poruszano następujące zagadnienia:

- system księgowy;
- rejestr kwot wycofanych;
- proces poświadczania wydatków;
- funkcjonalność systemu KSI;
- generowanie raportów przy użyciu aplikacji Oracle discoverer.

2.2.3. ZAKRES PRAC WYKONANYCH W INSTYTUCJI POŚREDNICZĄCEJ W CERTYFIKACJI

W zakresie wykonanych prac dokonano przeglądu i oceny następujących dokumentów:

- Rozporządzenie Parlamentu Europejskiego (WE) z dnia 5 lipca 2006 r. nr 1080/2006 w sprawie Europejskiego Funduszu Rozwoju Regionalnego i uchylające rozporządzenie (WE) nr 1783/1999;
- Rozporządzenie Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylające rozporządzenie (WE) nr 1260/1999;

- Rozporządzenie Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006 r. ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999;
- Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013,
- Szczegółowego opisu priorytetów Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013,
- Wytycznych w zakresie warunków certyfikacji oraz przygotowania prognoz wniosków o płatność do Komisji Europejskiej w Programach Operacyjnych w ramach Narodowych Strategicznych Ram Odniesienia na lata 2007-2013,
- Wytycznych w zakresie sprawozdawczości,
- Wytycznych w zakresie sposobu postępowania w razie wykrycia nieprawidłowości w wykorzystaniu funduszy strukturalnych i Funduszu Spójności w okresie programowania 2007-2013,
- Wytycznych w zakresie warunków gromadzenia i przekazywania danych w formie elektronicznej,
- Warunkowej Deklaracji Gotowości do audytu IPOC z dnia 06.12.2007r.,
- Porozumienia z dn. 04.07.2007r. między Ministrem Rozwoju Regionalnego a Wojewodą w sprawie przekazania zadań z zakresu certyfikacji prawidłowości poniesienia wydatków w ramach Regionalnego Programu Operacyjnego,
- Instrukcji wypełniania załączników nr 4a oraz 4b do Wytycznych w zakresie certyfikacji oraz przygotowywania prognoz wniosków o płatność do Komisji Europejskiej w Programach Operacyjnych w ramach Narodowych Strategicznych Ram Odniesienia na lata 2007-2013 zatwierdzonych w dniu 07.02.2008r.,
- Instrukcji wykonawczej Instytucji Pośredniczącej w Certyfikacji,
- Zarządzenia nr 158/07 Wojewody Podlaskiego z dnia 27 września 2007r. zmieniającego zarządzenie w sprawie ustalenia regulaminu Podlaskiego Urzędu Wojewódzkiego w Białymstoku,
- Zarządzenia nr 197/07 Wojewody Podlaskiego z dnia 4 grudnia 2007r. zmieniającego zarządzenie w sprawie nadania statutu Podlaskiemu Urzędowi Wojewódzkiemu w Białymstoku,
- Zarządzenia nr 10/08 Wojewody Podlaskiego z dnia 21 stycznia 2008r. zmieniającego zarządzenie w sprawie ustalenia regulaminu Podlaskiego Urzędu Wojewódzkiego w Białymstoku,
- Planu dochodzenia do pełnej gotowości operacyjnej IPOC Podlaskiego Urzędu Wojewódzkiego,
- Systemu informowania o nieprawidłowościach finansowych w wykorzystaniu funduszy strukturalnych i Funduszu Spójności w latach 2007-2013 - Pełnomocnik Rządu do Spraw Zwalczania Nieprawidłowości Finansowych na Szkodę Rzeczpospolitej Polskiej lub Unii Europejskiej,

- Arkusza identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku sporządzonego przez oddział IPOC,
- Instrukcji użytkownika obsługi KSI SIMIK 07-13,
- zakresów czynności pracowników Wydziału IPOC,
- opisów stanowisk pracy pracowników Wydziału IPOC.

W trakcie audytu sprawdzono czy:

- wszystkie funkcje przypisane IPOC na mocy porozumienia Wojewody Podlaskiego z Ministrem Rozwoju Regionalnego z dnia 4 lipca 2007r zostały przydzielone komórkom organizacyjnym w ramach struktury IPOC,
- zachowano zasadę właściwego rozdziału funkcji pomiędzy IPOC a IZ, a także zasadę rozdziału funkcji w ramach IPOC,
- określono zakresy obowiązków pracowników zaangażowanych w realizację zadań,
- pracownicy są przygotowani merytorycznie do realizacji zadań;
- istnieją pisemne procedury regulujące proces certyfikacji zapewniające zasadność i prawidłowość wydatków zadeklarowanych w ramach programu operacyjnego,
- IPOC posiada dostęp do wiarygodnych i skomputeryzowanych systemów rachunkowości i księgowości, monitorowania i sprawozdawczości finansowej (Krajowego Systemu Informatycznego – KSI),
- wdrożono system sprawozdawczości i monitorowania wykonywania zadań IPOC przez IC (czy istnieje system wymiany informacji),
- zapewniono uwzględnianie dla celów poświadczania wyników wszystkich audytów przeprowadzanych przez Instytucję Audytową,
- zapewniono podejmowanie czynności usprawniających w przypadku wykrycia przez Instytucję Audytową lub inne instytucje słabości w systemie,
- istnieją procedury zapewniających właściwą ścieżkę audytu,
- istnieją procedury sprawozdawczości i monitorowania nieprawidłowości oraz odzyskiwania kwot nienależnie wypłaconych,
- istnieją procedury zapewniające dokonywanie okresowych przeglądów Instrukcji wykonawczej i jej aktualizację, wyznaczenie osób odpowiedzialnych za te procesy;
- istnieją procedury regulujące zarządzanie ryzykiem wewnętrznym przez IPOC.

Zbadano procesy związane z:

- sporządzaniem, certyfikacją i przedkładaniem do Instytucji Certyfikującej Poświadczenia i deklaracji wydatków oraz wniosków o płatność,
- częściowym i końcowym zamknięciem pomocy,
- prowadzeniem ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych (prowadzeniem „rejestru dłużników"),

- wizytami sprawdzającymi,
- pozyskiwaniem i analizowaniem w procesie certyfikacji wyników kontroli i audytów przeprowadzonych przez inne upoważnione instytucje,
- opiniowaniem i akceptacją instrukcji wykonawczych oraz oceną systemu zarządzania i kontroli przez Instytucję Pośredniczącą w Certyfikacji,
- okresowymi przeglądami procedur,
- zarządzaniem ryzykiem,
- zastosowaniem Krajowego Systemu Informatycznego.

W trakcie audytu zgodności realizowanego w Instytucji Pośredniczącej w Certyfikacji zostały przeprowadzone wywiady (w sumie 6 spotkań) z kierownictwem (dyrekcją i kierownikami) oraz pracownikami Podlaskiego Urzędu Wojewódzkiego w Białymstoku. W trakcie wywiadów poruszano następujące zagadnienia:

- przygotowanie IPOC do audytu,
- przebieg procesu certyfikacji w IPOC,
- zapisy Instrukcji Wykonawczej IPOC w świetle procesów przebiegających w IPOC, zadań przekazanych przez IC oraz wymogów prawnych Wspólnoty Europejskiej dotyczących roli i zadań IPOC,
- zapisy Instrukcji Wykonawczej IPOC regulujące proces certyfikacji w świetle wymogów dotyczących kwalifikowalności wydatków, zasad wspólnotowych (pomocy publicznej, ochrony środowiska, równości kobiet i mężczyzn, informacji i promocji) oraz zasad udzielania zamówień publicznych,
- zarządzanie ryzykiem w IPOC.

2.2.4. ZAKRES PRAC WYKONANYCH W ODNIESIENIU DO KRAJOWEGO SYSTEMU INFORMATYCZNEGO

Przedmiotem audytu zgodności było uzyskanie zapewnienia, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58d) oraz 60c) rozporządzenia 1083/2006.

W ramach wykonanych prac audytowych dokonano przeglądu Krajowego Systemu Informatycznego SIMIK 07-13 oraz ogólnego środowiska informatycznego, w jakim on funkcjonuje.

Szczegóły badania zostały przedstawione w *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Ministerstwa Rozwoju Regionalnego* (załącznik nr 2 do niniejszego sprawozdania).

2.2.5. ZAKRES PRAC WYKONANYCH W INSTYTUCJI AUDYTOWEJ

W zakresie wykonanych prac dokonano przeglądu i oceny w szczególności następujących dokumentów:

- Rozporządzenie Parlamentu Europejskiego (WE) z dnia 5 lipca 2006 r. nr 1080/2006 w sprawie Europejskiego Funduszu Rozwoju Regionalnego i uchylające rozporządzenie (WE) nr 1783/1999;
- Rozporządzenie Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylające rozporządzenie (WE) nr 1260/1999;
- Rozporządzenie Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006 r. ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999;
- Ustawa z dnia 28 września 2001 r. o kontroli skarbowej (tekst jednolity Dz. U. z 2004 r., Nr 8, poz. 65, ze zm.);
- Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (teks jednolity Dz. U 2005 Nr 8; poz. 60 ze zm.)
- Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (tekst jednolity Dz. U z 2007, Nr 65, poz. 437 ze zm.);
- Rozporządzenie Ministra Finansów z dnia 28 czerwca 2002 r. w sprawie organizacji urzędów kontroli skarbowej (Dz. U. z 2002 r. Nr 96, poz. 856 ze zm.)
- Rozporządzenie Ministra Finansów z dnia 7 grudnia 1998 r. w sprawie określenia siedzib i terytorialnego zasięgu działania urzędów kontroli skarbowej (Dz. U. z 1998 r., Nr 153, poz. 995)
- Zarządzenie Nr 68 Prezesa Rady Ministrów z dnia 24 czerwca 2008 r. w sprawie nadania Statutu Ministerstwa Finansów (M.P. z 2008 r.; Nr 48, poz.431);
- Zarządzenie Nr 10 Ministra Finansów z dnia 10 lipca 2008 r. w sprawie nadania regulaminu organizacyjnego Ministerstwa Finansów;
- Zarządzenie nr 2 Dyrektora Departamentu Certyfikacji i Poświadczeń Środków z Unii Europejskiej z dnia 28 sierpnia 2007 r. w sprawie wprowadzenia wewnętrznego regulaminu organizacyjnego Departamentu Certyfikacji i Poświadczeń Środków z Unii Europejskiej,
- Decyzja Ministra Finansów w sprawie podziału kompetencji w Kierownictwie Ministerstwa Finansów;
- regulaminy organizacyjne urzędów kontroli skarbowej;
- Protokół nr 22/2006 z posiedzenia Komitetu Europejskiego Rady Ministrów z dnia 17 marca 2006 r. w sprawie wyznaczenia jednostki pełniącej funkcję Instytucji Audytowej oraz podmiotu odpowiedzialnego za dokonanie oceny

zgodności systemów zarządzania i kontroli funduszy strukturalnych i Funduszu Spójności w okresie programowania 2007-2013;

- Procedury Instytucji Audytowej:
  - Podręcznik audytu,
  - Strategia audytu,
  - Upoważnianie do audytu,
  - Audyt systemów,
  - Audyty operacji,
  - Wybór próby,
  - Sprawozdanie i opinia,
  - Udostępnianie wyników audytu,
  - Zamknięcie pomocy,
  - Zapewnienie jakości.
- Norma PN-ISO/IEC 17799:2007,
- Metodologia COBiT (Control Objectives for Information and related Technology)
- Opisy stanowisk pracowników Instytucji Audytowej,
- Zestawienie szkoleń/kwalifikacji pracowników IA.

W trakcie audytu sprawdzono, czy:

- wyznaczono Instytucję Audytową dla programu operacyjnego;
- powyższe instytucje funkcjonowały w perspektywie 2000-2006;
- dostępny jest schemat organizacyjny IA wskazujący ilość etatów przypisanych do poszczególnych wydziałów;
- określone zostały minimalne wymagania dotyczące kwalifikacji pracowników IA;
- zachowana została zasada rozdziału funkcji pomiędzy Instytucją Audytową a instytucjami zaangażowanymi we wdrażanie programu;
- ustanowione zostały odpowiednie ścieżki raportowania;
- pracownicy zaangażowani w realizację zadań IA mają określone zakresy obowiązków;
- pracownicy IA są przygotowani merytorycznie do realizacji zadań;
- opracowano procedury audytu; czy są one zgodne z międzynarodowymi standardami audytu;
- ustanowiono procedury dotyczące monitorowania zaleceń oraz follow-up;
- ustanowiono procedury umożliwiające przygotowanie rocznego sprawozdania audytowego, opinii oraz deklaracji zamknięcia pomocy;

- istnieją procedury sporządzania deklaracji częściowego zamknięcia pomocy;
- dostępny jest schemat obrazujący w jaki sposób IA zamierza wywiązywać się z wymogów Art. 62 Rozp. 1083/2006;
- przygotowano strategię audytu.

2.3. Wykorzystanie prac z poprzednich audytów oraz audytów przeprowadzonych przez inne jednostki

Zgodnie z przyjętą metodyką i programem badania, audyt zgodności został przeprowadzony we wszystkich instytucjach zaangażowanych we wdrażanie Regionalnego Programu Operacyjnego Województwa Podlaskiego (Instytucji Zarządzającej, Instytucji Certyfikującej oraz Instytucji Pośredniczącej w Certyfikacji).

Dla potrzeb oceny systemów zarządzania i kontroli opracowanych dla perspektywy 2007-2013 nie korzystano z wyników prac audytowych prowadzonych w ramach okresu programowania 2000-2006 (w przypadku Polski 2004-2006).

Jednakże, obszary ryzyka stwierdzone w trakcie audytów prowadzonych w ramach poprzedniego okresu programowania, zostały uwzględnione w analizie ryzyka sporządzonej dla potrzeb audytu zgodności.

W trakcie audytu zgodności nie korzystano z wyników prac audytowych innych jednostek.

2.4. Procedura kontradyktoryjna

Przed sporządzeniem przedmiotowego sprawozdania miała zastosowanie procedura kontradyktoryjna. Wstępne wersje sprawozdań z audytu zgodności zostały sporządzone osobno dla Instytucji Zarządzającej, Instytucji Certyfikującej oraz Instytucji Pośredniczącej w Certyfikacji i przekazane tym instytucjom w celu ustosunkowania się do stwierdzonych ustaleń i rekomendacji. Odpowiedzi instytucji oraz stanowisko Instytucji Audytowej zostały włączone do sprawozdań końcowych przekazanych instytucjom. Instytucja Audytowa przeprowadziła czynności sprawdzające stan wdrożenia wydanych rekomendacji. Na podstawie wyników wszystkich wykonanych czynności audytowych sporządzono niniejsze sprawozdanie z audytu zgodności w RPO WPo. Sprawozdanie zostało przekazane Instytucji Zarządzającej w celu zgłoszenia uwag do jego treści.

2.5. Jakość prac audytowych

Z uwagi na fakt, iż audyt zgodności był realizowany przez Instytucję Audytową, która sporządziła również przedmiotowe sprawozdanie, sprawozdaniu temu towarzyszy dodatkowo *Oświadczenia o kompetencji i niezależności działania.*

Czynności badawcze zostały wykonane zgodnie z międzynarodowo uznanymi standardami audytu.

W trakcie audytu nie ograniczono zakresu badania.

3. WYNIKI OCENY

Nr kodu CCI	Instytucja (Nazwa i rodzaj: IZ/ IC/IPOC/IA)	Kompletność i dokładność OSZiK (Tak/Nie)	Wnioski (bez zastrzeżeń/z zastrzeżeniami/ negatywne)	Uchybienia	Osie priorytetowe	Kluczowe / pomocnicze elementy	Rekomendacje / środki naprawcze
2007/PL161PO014	Instytucja Zarządzająca – Zarząd Województwa Podlaskiego	Tak	Bez zastrzeżeń	Brak kluczowych i innych uchybień	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów kluczowych i pomocniczych	Brak kluczowych i innych rekomendacji
2007/PL161PO014	Instytucja Certyfikująca – Departament Instytucji Certyfikującej w MRR	Tak	Bez zastrzeżeń	Brak kluczowych uchybień.	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów kluczowych	Brak kluczowych rekomendacji.
				Uchybienia nie wpływające na opinię o zgodności wskazano w pkt 3.2 sprawozdania	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów pomocniczych	Środki naprawcze do podjęcia w odniesieniu do uchybień nie wpływających na opinię o zgodności wskazano w pkt 3.2. sprawozdania
2007/PL161PO014	Instytucja Pośrednicząca w Certyfikacji – Wojewoda	Tak	Bez zastrzeżeń	Brak kluczowych uchybień.	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów kluczowych	Brak kluczowych rekomendacji.

	Podlaski			Uchybienia nie wpływające na opinię o zgodności wskazano w pkt 3.3. sprawozdania	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów pomocniczych	Środki naprawcze do podjęcia w odniesieniu do uchybień nie wpływających na opinię o zgodności wskazano w pkt 3.3. sprawozdania
2007/PL161PO014	Instytucja Audytowa – Generalny Inspektor Kontroli Skarbowej	Tak	Bez zastrzeżeń	Brak kluczowych i innych uchybień	Dotyczy wszystkich osi priorytetowych	Dotyczy wszystkich elementów kluczowych i pomocniczych	Brak kluczowych i innych rekomendacji

3.1. Instytucja Zarządzająca

W trakcie audytu w IZ ustalono, że

- Opis systemu zarządzania i kontroli zawiera wszystkie wymagane elementy;
- wyznaczono Instytucję Zarządzającą oraz wyszczególniono jej funkcje i zadania zgodnie z przepisami wspólnotowymi;
- określono schemat organizacyjny IZ oraz zakresy obowiązków ich pracowników;
- zapewniony został rozdział funkcji między IZ a pozostałymi instytucjami zaangażowanymi we wdrażanie RPO WPo oraz w obrębie IZ;
- opracowano podręczniki procedur dla IZ, zawierające również procedury ich aktualizacji;
- przygotowano wytyczne niezbędne do wdrażania RPO WPo;
- ustalono zasady kwalifikowania wydatków w RPO WPo zgodne z przepisami prawa wspólnotowego;
- opracowano procedury ogłaszania naboru wniosków aplikacyjnych, wyboru i zatwierdzania operacji zgodnie z wymogami prawa wspólnotowego;
- procedury dają racjonalne zapewnienie, że zostanie dokonana weryfikacja dostarczonych produktów/usług w celu sprawdzenia rzeczywistego poniesienia wydatków oraz weryfikacji wydatków pod kątem zgodności z zasadami kwalifikowalności UE i krajowymi;
- procedury zapewniają dokonanie weryfikacji (formalnej i merytorycznej) złożonych wniosków przez beneficjentów oraz dołączonej dokumentacji a także przeprowadzenie weryfikacji na miejscu w trakcie trwania projektu i sprawdzenie postępu rzeczowego oraz finansowego;
- procedury zapewniają że przeprowadzone weryfikacje (formalne, merytoryczne oraz kontrole na miejscu) będą dokumentowane i zawierają wzory list sprawdzających/raportów;
- procedury gwarantują przechowywanie wyników przeprowadzonych weryfikacji formalnej i merytorycznej oraz kontroli na miejscu;
- procedury zapewniają, iż kontrolą objęte będą wszystkie projekty realizowane w ramach RPO WPo;
- procedury zapewniają istnienie ścieżki audytu i przechowywanie wymaganej dokumentacji zgodnie z przepisami UE;
- opracowano procedury sprawozdawczości i monitorowania w przypadku stwierdzenia nieprawidłowości, raportowania do KE, prowadzenia i regularnego przeglądu rejestru kwot odzyskanych/do odzyskania, odzyskiwania kwot nieprawidłowo wypłaconych;
- opracowano procedury poświadczania i deklarowania wydatków do KE oraz składania wniosków o płatność; zapewniono przekazywanie

do Instytucji Certyfikującej wszystkich niezbędnych informacji o procedurach i weryfikacjach prowadzonych odniesieniu do wydatków na potrzeby poświadczania;

- systemy informatyczne funkcjonujące w ramach systemu zarządzania i kontroli RPO WPo są ustanowione zgodnie z wymogami rozporządzenia 1083/2006 (szczegółowe ustalenia zostały zawarte w *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Urzędu Marszałkowskiego Województwa Podlaskiego* stanowiącym załącznik nr 1 do niniejszego sprawozdania oraz *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Ministerstwa Rozwoju Regionalnego* stanowiącym załącznik nr 2 do niniejszego sprawozdania);
- procedury zapewniają uzyskanie z zapisów księgowych odpowiednio szczegółowych informacji o poziomie aktualnych wydatków w każdym współfinansowanym projekcie beneficjenta; dane, o których mowa w zał. III rozporządzenia Komisji (WE) nr 1828/2006 gromadzone będą w Krajowym Systemie Informatycznym (KSI);
- zaimplementowano mechanizmy zapewniające, że utrzymywany przez beneficjenta system księgowy gwarantuje identyfikację każdej poszczególnej operacji finansowej;
- procedury określają odpowiednie zasady prowadzenia kampanii informacyjnej dotyczącej RPO WPo, opracowany został plan działań dotyczących promocji.

Ustalenia dotyczące systemów informatycznych funkcjonujących w ramach systemu zarządzania i kontroli RPO WPo zostały przedstawione *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Urzędu Marszałkowskiego Województwa Podlaskiego* stanowiącym załącznik nr 1 do niniejszego sprawozdania oraz *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Ministerstwa Rozwoju Regionalnego* stanowiącym załącznik nr 2 do niniejszego sprawozdania.

Dokonane ustalenia, ze względu na wagę, nie stanowią podstawy do zastrzeżeń w opinii o zgodności.

Stan wdrożenia wydanych w zakresie systemów informatycznych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

Na dzień sporządzenia niniejszego sprawozdania, rekomendacje wydane w pozostałym zakresie zostały wdrożone, co zostało sprawdzone w trakcie czynności sprawdzających „follow –up". Nie pozostały rekomendacje wymagające podejmowania dalszych działań naprawczych przez IZ.

3.2. Instytucja Certyfikująca

W trakcie audytu w IC ustalono, że:

- Opis systemu zarządzania i kontroli zawiera wszystkie wymagane elementy;

- wyznaczono Instytucję Certyfikującą oraz wyszczególniono jej funkcje i zadania zgodnie z przepisami wspólnotowymi;
- wyraźnie wskazano funkcje oddelegowane do Instytucji Pośredniczącej w Certyfikacji oraz wprowadzono system raportowania i monitorowania realizacji przez nią powierzonych zadań;
- określono schemat organizacyjny IC oraz zakresy obowiązków ich pracowników;
- zapewniony został rozdział funkcji między IC a pozostałymi instytucjami zaangażowanymi we wdrażanie RPO WPo oraz w obrębie IC;
- opracowano podręczniki procedur dla IC, zawierające również procedury ich aktualizacji;
- opracowano procedury poświadczania i deklarowania wydatków do KE oraz składania wniosków o płatność;
- procedury dotyczące poświadczania zapewniają:
  - wychwycenie, na etapie weryfikacji złożonych deklaracji i wniosków, wielokrotne ujęcie tej samej płatności oraz błędów rachunkowych;
  - pomniejszenie wniosku o kwoty stwierdzonych nieprawidłowości/kwoty odzyskane;
  - weryfikację wniosku pod kątem zawarcia w nim tylko wydatków kwalifikowanych poniesionych w danym okresie;
  - że nie zostaną dokonane żadne nieuprawnione zmiany we wnioskach na etapie certyfikacji;
  - przesłanie wszystkich certyfikowanych pozytywnie wniosków do KE i nie przesyłanie wielokrotnie tych samych wniosków;
- procedury zapewniają korzystanie w procesie sporządzania poświadczeń i deklaracji wydatków z KSI oraz zgodność danych wykazanych w poświadczeniu i deklaracji wydatków z KSI;
- opracowano procedury sprawozdawczości i monitorowania w przypadku stwierdzenia nieprawidłowości, raportowania do KE, prowadzenia i regularnego przeglądu rejestru kwot odzyskanych/do odzyskania, odzyskiwania kwot nieprawidłowo wypłaconych;
- procedury zapewniają korzystanie w procesie poświadczania wydatków z informacji na temat wyników kontroli i audytów związanych z wydatkami zawartymi w deklaracjach wydatków, przeprowadzonych przez IZ, oraz IA;
- dostępny jest opis systemu będącego podstawą poświadczania wydatków do KE (KSI);
- IC posiada dostęp do KSI;
- procedury zapewniają utrzymywanie w formie elektronicznej zapisów księgowych dotyczących wydatków zadeklarowanych Komisji,

- procedury zapewniają prowadzenie ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych po anulowaniu całości lub części wkładu do operacji.

Na dzień sporządzenia niniejszego sprawozdania, rekomendacje wydane IC w trakcie audytu zgodności, za wyjątkiem poniżej wskazanych, zostały wdrożone, co zostało sprawdzone w trakcie czynności sprawdzających „follow –up".

Poniższe ustalenie, ze względu na wagę, nie stanowi podstawy do zastrzeżeń w opinii o zgodności. IC opracowała procedury (podręczniki, wytyczne, standardowe dokumenty, listy sprawdzające) niezbędne do realizacji zadań, o których mowa w art. 61 rozporządzenia 1083/2006. Ustalenie wskazuje, że ustanowione procedury wymagają jedynie poniżej wskazanego uszczegółowienia:

Ustalenie:	IC posiada procedury w zakresie postępowania w związku z częściowym zamknięciem pomocy. Procedury te są jednak ogólne i wymagają uszczegółowienia. IC nie posiada odrębnej listy sprawdzającej do wniosków o płatność w ramach częściowego zamknięcia pomocy. IC poinformowała, że procedury zostaną uzupełnione po otrzymaniu z KE wytycznych.
Rekomendacja:	Po otrzymaniu od KE stosownych wytycznych zaleca się doprecyzować procedury dotyczące częściowego zamknięcia pomocy, zwłaszcza uzupełnienie o listę sprawdzającą, która ma stanowić załącznik do Instrukcji Wykonawczej.

Stan wdrożenia powyższego zalecenia będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

3.3. Instytucja Pośrednicząca w Certyfikacji

W trakcie audytu w IPOC ustalono, że:

- Opis systemu zarządzania i kontroli zawiera wszystkie wymagane elementy;
- wyznaczono Instytucję Pośredniczącą w Certyfikacji oraz wyszczególniono jej funkcje i zadania zgodnie z przepisami wspólnotowymi;
- wyraźnie wskazano funkcje oddelegowane do Instytucji Pośredniczącej w Certyfikacji oraz wprowadzono system raportowania i monitorowania realizacji przez nią powierzonych zadań;
- określono schemat organizacyjny IPOC oraz zakresy obowiązków ich pracowników;
- zapewniony został rozdział funkcji między IPOC a pozostałymi instytucjami zaangażowanymi we wdrażanie RPO WPo oraz w obrębie IPOC;
- opracowano podręczniki procedur dla IPOC, zawierające również procedury ich aktualizacji;

- opracowano procedury poświadczania i deklarowania wydatków do KE oraz składania wniosków o płatność;
- procedury dotyczące poświadczania zapewniają:
  - wychwycenie, na etapie weryfikacji złożonych deklaracji i wniosków, wielokrotne ujęcie tej samej płatności oraz błędów rachunkowych;
  - pomniejszenie wniosku o kwoty stwierdzonych nieprawidłowości/kwoty odzyskane;
  - weryfikację wniosku pod kątem zawarcia w nim tylko wydatków kwalifikowanych poniesionych w danym okresie;
  - że nie zostaną dokonane żadne nieuprawnione zmiany we wnioskach na etapie certyfikacji;
  - przesłanie wszystkich certyfikowanych pozytywnie wniosków do KE i nie przesyłanie wielokrotnie tych samych wniosków;
- procedury zapewniają korzystanie w procesie sporządzania poświadczeń i deklaracji wydatków z KSI oraz zgodność danych wykazanych w poświadczeniu i deklaracji wydatków z KSI;
- opracowano procedury sprawozdawczości i monitorowania w przypadku stwierdzenia nieprawidłowości, raportowania do KE, prowadzenia i regularnego przeglądu rejestru kwot odzyskanych/do odzyskania, odzyskiwania kwot nieprawidłowo wypłaconych;
- procedury zapewniają korzystanie w procesie poświadczania wydatków z informacji na temat wyników kontroli i audytów związanych z wydatkami zawartymi w deklaracjach wydatków, przeprowadzonych przez IZ oraz IA;
- dostępny jest opis systemu będącego podstawą poświadczania wydatków do KE (KSI).
- IPOC posiada dostęp do KSI,
- procedury zapewniają prowadzenie ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych po anulowaniu całości lub części wkładu do operacji.

Na dzień sporządzenia niniejszego sprawozdania, rekomendacje wydane IPOC w trakcie audytu zgodności, za wyjątkiem poniżej wskazanych, zostały wdrożone, co zostało sprawdzone w trakcie czynności sprawdzających „follow –up".

Poniższe ustalenie, ze względu na wagę, nie stanowi podstawy do zastrzeżeń w opinii o zgodności. IPOC opracowała procedury (podręczniki, wytyczne, standardowe dokumenty, listy sprawdzające) niezbędne do realizacji zadań, o których mowa w art. 61 rozporządzenia 1083/2006. Ustalenie wskazuje, że ustanowione procedury wymagają jedynie poniżej wskazanego uszczegółowienia:

Ustalenie:	IPOC posiada procedury w zakresie postępowania w związku z częściowym zamknięciem pomocy. Procedury te są jednak ogólne i wymagają uszczegółowienia. IPOC nie

posiada odrębnej listy sprawdzającej do wniosków o płatność w ramach częściowego zamknięcia pomocy. IPOC poinformowała, że procedury zostaną uzupełnione po otrzymaniu stosownych wytycznych.

Rekomendacja: Po otrzymaniu stosownych wytycznych zaleca się doprecyzować procedury dotyczące częściowego zamknięcia pomocy, zwłaszcza uzupełnienie o listę sprawdzającą, która ma stanowić załącznik do Instrukcji Wykonawczej.

Stan wdrożenia powyższego zalecenia będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

3.4. Instytucja Audytowa

W wyniku dokonanej samooceny Instytucji Audytowej potwierdzono, że:

- wyznaczono jedną Instytucję Audytową dla wszystkich programów oraz wyszczególniono jej funkcje i zadania zgodnie z przepisami wspólnotowymi;
- instytucja wyznaczona do pełnienia roli IA wykonywała zadania określone w art. 10 i 15 rozporządzenia 438/2001 oraz art. 9 i 15 rozporządzenia 1386/2002;
- określono schemat organizacyjny IA, zakresy obowiązków jej pracowników i wymagania dotyczące kwalifikacji;
- zapewniony został rozdział funkcji między IA a pozostałymi instytucjami zaangażowanymi we wdrażanie programu;
- Generalny Inspektor Kontroli Skarbowej jest funkcjonalnie niezależny od pozostałych instytucji zaangażowanych we wdrażanie programu co posiada walor adekwatności;
- opracowano procedury IA zgodne z międzynarodowymi standardami audytu;
- procedury IA zapewniają odpowiednie ścieżki raportowania;
- ustanowiono procedury dotyczące monitorowania zaleceń oraz follow-up;
- Instytucja Audytowa posiada dostęp do danych gromadzonych w Krajowym Systemie Informatycznym;
- ustanowiono procedury umożliwiające przygotowanie rocznego sprawozdania audytowego, opinii oraz deklaracji zamknięcia pomocy;
- istnieją procedury sporządzania deklaracji częściowego zamknięcia pomocy;
- dostępny jest schemat obrazujący, w jaki sposób IA zamierza wywiązywać się z wymogów Art. 62 Rozp. 1083/2006;
- przygotowano strategię audytu.

4. WNIOSKI OGÓLNE

W wyniku prac audytowych potwierdzono, że systemy zarządzania i kontroli w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego ustanowiono zgodnie z wymogami wspólnotowymi (tj. art. 58-62 rozporządzenia Rady (WE) nr 1083/2006 i przepisami sekcji 3 rozporządzenia Komisji (WE) nr 1828/2006).

W trakcie czynności audytowych, w odniesieniu do wszystkich instytucji potwierdzono, że:

- Opis systemu zarządzania i kontroli zawiera wszystkie wymagane elementy;
- wyznaczono Instytucję Zarządzającą, Instytucję Certyfikującą i Instytucję Pośredniczącą w Certyfikacji dla RPO WPo oraz wyszczególniono ich funkcje i zadania;
- wyraźnie wskazano funkcje oddelegowane do Instytucji Pośredniczącej w Certyfikacji oraz wprowadzono system monitorowania realizacji przez nią powierzonych zadań;
- określono schematy organizacyjne wyznaczonych instytucji oraz zakresy obowiązków ich pracowników;
- zapewniony został rozdział funkcji między instytucjami zaangażowanymi we wdrażanie RPO WPo oraz w obrębie tych instytucji;
- opracowano podręczniki procedur dla poszczególnych instytucji, zawierające również procedury ich aktualizacji;
- przygotowano wytyczne niezbędne do wdrażania RPO WPo;
- zapewniono procedury przepływu informacji pomiędzy instytucjami zaangażowanymi we wdrażanie RPO WPo;
- ustalono zasady kwalifikowania wydatków w RPO WPo zgodne z przepisami prawa wspólnotowego;
- opracowano procedury ogłaszania naboru wniosków aplikacyjnych, wyboru i zatwierdzania operacji zgodnie z wymogami prawa wspólnotowego;
- procedury dają racjonalne zapewnienie, że zostanie dokonana weryfikacja dostarczonych produktów/usług w celu sprawdzenia rzeczywistego poniesienia wydatków oraz weryfikacji wydatków pod kątem zgodności z zasadami kwalifikowalności UE i krajowymi;
- procedury zapewniają dokonanie weryfikacji (formalnej i merytorycznej) złożonych wniosków przez beneficjentów oraz dołączonej dokumentacji a także przeprowadzenie weryfikacji na miejscu w trakcie trwania projektu i sprawdzenie postępu rzeczowego oraz finansowego;
- procedury gwarantują przechowywanie wyników przeprowadzonych weryfikacji formalnej i merytorycznej oraz kontroli na miejscu;
- procedury zapewniają, iż kontrolą objęte będą wszystkie projekty realizowane w ramach RPO WPo;

- procedury zapewniają istnienie ścieżki audytu i przechowywanie wymaganej dokumentacji zgodnie z przepisami UE;
- opracowano procedury sprawozdawczości i monitorowania w przypadku stwierdzenia nieprawidłowości, raportowania do KE, prowadzenia i regularnego przeglądu rejestru kwot odzyskanych/do odzyskania, odzyskiwania kwot nieprawidłowo wypłaconych;
- opracowano procedury poświadczania i deklarowania wydatków do KE oraz składania wniosków o płatność;
- procedury dotyczące poświadczania zapewniają:
  - wychwycenie, na etapie weryfikacji złożonych deklaracji i wniosków, wielokrotne ujęcie tej samej płatności oraz błędów rachunkowych;
  - pomniejszenie wniosku o kwoty stwierdzonych nieprawidłowości/kwoty odzyskane;
  - weryfikację wniosku pod kątem zawarcia w nim tylko wydatków kwalifikowanych poniesionych w danym okresie;
  - że nie zostaną dokonane żadne nieuprawnione zmiany we wnioskach na etapie certyfikacji;
  - przesłanie wszystkich certyfikowanych pozytywnie wniosków do KE i nie przesyłanie wielokrotnie tych samych wniosków;
- procedury zapewniają korzystanie w procesie poświadczania wydatków z informacji na temat wyników kontroli i audytów związanych z wydatkami zawartymi w deklaracjach wydatków, przeprowadzonych przez IZ, IP oraz IA;
- systemy informatyczne funkcjonujące w ramach systemu zarządzania i kontroli RPO WPo są ustanowione zgodnie z wymogami art. 58d), 60c) oraz 61e) rozporządzenia 1083/2006 (szczegółowe ustalenia zostały zawarte w *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Urzędu Marszałkowskiego Województwa Podlaskiego* stanowiącym załącznik nr 1 do niniejszego sprawozdania oraz *Sprawozdaniu z czynności sprawdzających w zakresie audytu zgodności systemów informatycznych Ministerstwa Rozwoju Regionalnego* stanowiącym załącznik nr 2 do niniejszego sprawozdania);
- dla celów zarządzania i sprawozdawczości w instytucjach zaangażowanych we wdrażanie programu obligatoryjnie wykorzystywane są podstawowe systemy informatyczne tj.: KSI (SIMIK 07-13) oraz system finansowo-księgowy; Lokalne Systemy Informatyczne mogą być wykorzystywane opcjonalnie;
- procedury zapewniają uzyskanie z zapisów księgowych odpowiednio szczegółowych informacji o poziomie aktualnych wydatków w każdym współfinansowanym projekcie beneficjenta; dane, o których mowa w zał. III rozporządzenia Komisji (WE) nr 1828/2006 gromadzone będą w Krajowym Systemie Informatycznym (KSI);
- dostępny jest opis systemu będącego podstawą poświadczania wydatków do KE (KSI);

- procedury zapewniają utrzymywanie w formie elektronicznej zapisów księgowych dotyczących wydatków zadeklarowanych Komisji;
- zaimplementowano mechanizmy zapewniające, że utrzymywany przez beneficjenta system księgowy gwarantuje identyfikację każdej poszczególnej operacji finansowej;
- wyznaczona została niezależna od pozostałych instytucji zaangażowanych we wdrażanie RPO WPo Instytucja Audytowa odpowiedzialna za wykonywanie audytów systemów zarządzania i kontroli i audytów operacji; strategia audytu została przekazana do KE w terminie;
- procedury zapewniają prowadzenie ewidencji kwot podlegających procedurze odzyskiwania i kwot wycofanych po anulowaniu całości lub części wkładu do operacji;
- procedury określają odpowiednie zasady prowadzenia kampanii informacyjnej dotyczącej RPO WPo, opracowany został plan działań dotyczących promocji.

W trakcie audytu zgodności nie dokonano ustaleń, które stanowiłyby podstawę do sformułowania zastrzeżeń w opinii o zgodności.

Ustalenia, które nie mają wpływu na opinię o zgodności oraz działania naprawcze, które powinny zostać podjęte przez poszczególne jednostki wskazano w pkt 3.1 – 3.3 sprawozdania.

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

Instytucja Audytowa pozyska od jednostek audytowanych informacje o stanie wdrożenia zaleceń zawartych w niniejszym sprawozdaniu i przekaże je do Komisji Europejskiej do 31 grudnia 2008 r.

5. WYKAZ SKRÓTÓW

DO	Departament Ochrony Interesów Finansowych Unii Europejskiej w Ministerstwie Finansów
IA	Instytucja Audytowa
UKS	Urząd Kontroli Skarbowej
IZ	Instytucja Zarządzająca
IC	Instytucja Certyfikująca
IPOC	Instytucja Pośrednicząca w Certyfikacji
IW	Instrukcja Wykonawcza
KE	Komisja Europejska
KSI	Krajowy System Informatyczny
MRR	Ministerstwo Rozwoju Regionalnego
OSZiK	Opis Systemu Zarządzania i Kontroli
RPO WPo	Regionalny Program Operacyjny Województwa Podlaskiego
UE	Unia Europejska

PODSEKRETARZ STANU
Generalny Inspektor Kontroli Skarbowej
.....
Andrzej Parafianowicz
Pieczątka i podpis osoby
zatwierdzającej sprawozdanie

RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

GENERALNY INSPEKTOR KONTROLI SKARBOWEJ

Sprawozdanie

z czynności sprawdzających w zakresie

audytu zgodności

systemów informatycznych

Urzędu Marszałkowskiego

Województwa Podlaskiego

SPIS TREŚCI

1. WPROWADZENIE

Art. 70 i 71 *rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999*[1], nakładają na państwo członkowskie obowiązek uzyskania zapewnienia, że systemy zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58-62 tego *rozporządzenia* oraz że funkcjonują skutecznie. Audyt zgodności, zgodnie z art. 71 ust. 1 w zw. z ust. 2 *rozporządzenia 1083/2006* powinien zostać zakończony przed złożeniem przez Polskę pierwszego wniosku o płatność pośrednią do KE, lub nie później niż w terminie 12 miesięcy od zatwierdzenia przez KE każdego programu operacyjnego.

Zasadniczym celem niniejszego audytu jest uzyskanie zapewnienia, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych, są ustanowione zgodnie z wymogami art. 58d) oraz 60c) ww. *rozporządzenia.*

Instytucją Zarządzającą Regionalnego Programu Operacyjnego Województwa Podlaskiego jest Zarząd Województwa Podlaskiego, który pełni tą funkcję przy pomocy Urzędu Marszałkowskiego Województwa Podlaskiego.

Instytucją Pośredniczącą Programu Operacyjnego Kapitał Ludzki jest Urząd Marszałkowski Województwa Podlaskiego.

W ramach wykonanych prac audytowych dokonano przeglądu systemów informatycznych Urzędu Marszałkowskiego Województwa Podlaskiego wykorzystywanych przy dystrybucji środków finansowych RPO WP i PO KL oraz ogólnego środowiska informatycznego, w jakim one funkcjonują.

Środowisko informatyczne Urzędu Marszałkowskiego, zgodnie z metodologią COBIT 4.1 zostało ujęte w następujące obszary:

- *Kontrole Aplikacyjne;*
- *Planowanie i Organizacja*;
- *Zakup i Wdrożenie;*
- *Dostarczanie i Wsparcie*;
- *Monitorowanie i Ocena.*

Każdy z tych obszarów został podzielony na procesy w oparciu o metodologię COBIT 4.1 przy wykorzystaniu standardów Stowarzyszenia ds. audytu i kontroli systemów informatycznych ISACA.

W ramach dokumentowania stanu faktycznego, szczególna uwaga została poświęcona identyfikacji mechanizmów kontrolnych odnoszących się do ryzyka utraty poufności danych (*Confidentiality Risk*), ryzyka utraty integralności danych (*Integrity Risk*), oraz ryzyka braku dostępności danych (*Availability Risk*). Zidentyfikowane mechanizmy kontrolne zostały następnie poddane testom, na podstawie których została oceniona efektywność ich funkcjonowania.

[1] Dz.U.UE.L.06.210.25

Prace audytowe zostały przeprowadzone w dniach 26-27.02.2008 w siedzibie Urzędu Marszałkowskiego Województwa Podlaskiego, ul. Wyszyńskiego 1.

Wyniki przeprowadzonych prac zostały oparte na dokumentach dostarczonych przez pracowników Urzędu Marszałkowskiego, wydrukach z badanych systemów i aplikacji oraz informacjach przekazanych w rozmowach, a także obserwacjach procesów i operacji wykonywanych w systemach informatycznych. Wyniki prac opierają się na założeniu, że wszystkie przekazywane informacje zostały przedstawione zgodnie z najlepszą wiedzą pracowników Urzędu, w sposób kompletny, rzetelny i prawdziwy.

Sprawozdanie zostało sporządzone według stanu na dzień 28 lutego 2008 r. i może być rozpatrywane tylko w świetle kwestii i faktów w nim przedstawionych. Zawarte w *Sprawozdaniu* ustalenia odzwierciedlają stan rzeczywisty stwierdzony podczas przeglądu aplikacji wykorzystywanych do obsługi środków w ramach funduszy strukturalnych.

2. OPIS STANU FAKTYCZNEGO – STRESZCZENIE

W Urzędzie Marszałkowskim Województwa Podlaskiego proces obsługi środków wydatkowania funduszy strukturalnych w ramach perspektywy na lata 2007-2013, który był przedmiotem badania, wygląda następująco:

- w aplikacji EUROBUDŻET odbywać się będą rozliczenia finansowo-księgowe;
- do rozliczeń bankowych będzie używany system VIDEOTEL.

Do celów ewidencji i rozliczeń księgowych oraz sprawozdawczości finansowej wykorzystywany będzie system finansowo-księgowy EUROBUDŻET, oparty na bazie danych MS SQL 2000. System jest produktem opracowanym przez firmę MICOMP, która na podstawie formalnej umowy dostosowała go do specyfikacji rozliczeń środków unijnych, przeprowadziła szkolenie jego użytkowników i zapewnia wsparcie oraz aktualizację dostarczonego oprogramowania. Obecnie odbywa się już w tym systemie księgowanie środków w ramach PO KL, księgowanie środków pochodzących z RPO WP rozpocznie się z chwilą otrzymania pierwszej płatności.

Do rozliczeń bankowych używany jest system VIDEOTEL. Dane do tego systemu są wprowadzane ręcznie na podstawie otrzymanych zleceń płatności. Planuje się zintegrowanie systemów EUROBUDŻET oraz VIDEOTEL tak, aby przekaz danych odbywał się bez ingerencji użytkownika.

Urząd Marszałkowski Województwa Podlaskiego nie posiada Lokalnego Systemu Informatycznego, służącego do ewidencji projektów, wniosków, umów o dofinansowanie oraz generowania zleceń płatności. Zgodnie z uzyskanymi informacjami obecnie trwają prace nad opracowaniem podstawowych założeń, po czym nastąpi podjęcie decyzji, czy system będzie opracowywany wewnętrznie, czy zlecony wykonawcy zewnętrznemu. Wstępne uruchomienie systemu planowane jest na okres lipiec – wrzesień br., natomiast uzyskanie pełnej funkcjonalności ma nastąpić do końca 2008 r. Do tego czasu obsługa wniosków będzie obywać się wyłącznie w formie papierowej.

Szczegółowe informacje dotyczące przeprowadzonych testów aplikacyjnych systemów zostały opisane w części *Kontrole aplikacyjne*.

Wyniki wykonanych prac tj. opis stanu faktycznego oraz zidentyfikowane kwestie zostały przedstawione w dalszej części niniejszego *Sprawozdania* w podziale na poszczególne obszary prac.

Na podstawie przeprowadzonego audytu, pomimo zastrzeżeń opisanych w części *8. Ustalenia i rekomendacje* niniejszego *Sprawozdania*, uzyskano zapewnienie, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58d) oraz 60c) *rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999.*

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

3. KONTROLE APLIKACYJNE

Całość księgowania środków zarządzanych przez Urząd Marszałkowski Województwa Podlaskiego i pochodzących z Programu Operacyjnego Kapitał Ludzki oraz Regionalnego Programu Operacyjnego Województwa Podlaskiego będzie dokonywać się w systemie EUROBUDŻET. Docelowo w systemie EUROBUDŻET będzie dokonywane księgowanie wszystkich środków finansowych Urzędu (także nie związanych z funduszami strukturalnymi UE).

Obecnie trwają prace nad ostatecznym wdrożeniem i rozpoczęciem korzystania z systemu, na przełomie marca/kwietnia nastąpi wizyta w UM przedstawicieli MiCOMP – twórcy systemu i właściciela praw autorskich, którzy dokonają aktualizacji funkcjonalności związanej z dystrybucją środków unijnych RPO WP (stworzenie odpowiednich formatek, uzupełnienie planów kont o uwzględniające poddziałania RPO WP itp.) oraz przeszkolą pracowników księgowości w tym zakresie.

Zgodnie z otrzymanymi informacjami obecnie odbywa się już w systemie księgowanie środków pochodzących z PO KL. Po otrzymaniu pierwszej płatności środków RPO WP (co ma nastąpić w kwietniu) środki te będą księgowane w systemie EUROBUDŻET i równolegle w obecnie wykorzystywanym systemie KWANT. Po ok. 3 miesiącach, przy poprawnym działaniu systemu, pracownicy będą wykorzystywać jedynie system EUROBUDŻET.

Serwer aplikacyjny, na którym zainstalowany jest system EUROBUDŻET działa pod kontrolą systemu operacyjnego *Windows 2000 Server Advanced*. Serwer bazodanowy z zainstalowanym oprogramowaniem *Microsoft SQL Server 2000 Enterprise Edition* działa w konfiguracji klastra.

System jest zainstalowany obecnie na komputerach 13 użytkowników (tylko w księgowości), docelowo będzie posiadał ok. 18-20 użytkowników. Uprawnienia administratora aplikacji posiada wyznaczona osoba, która zarządza aplikacją poprzez wbudowany moduł „Administrator" – nadaje i odbiera uprawnienia dostępu (na podstawie wniosku o dostęp do systemów informatycznych) oraz przywileje w aplikacji, ustawia i zmienia hasła pracownikom, konfiguruje system, kontaktuje się z dostawcą w przypadku awarii lub konieczności aktualizacji w wyniku zmian przepisów prawnych, rozbudowy itp., kontaktuje się z departamentem informatycznym w sprawie obsługi informatycznej. W trakcie audytu nie zidentyfikowano szczegółowych formalnych procedur zarządzania aplikacją.

Rekomendacja 1. Kontrole aplikacyjne – System księgowy

Do aplikacji stworzono odrębne od domenowego logowanie, użytkownicy aplikacji posiadają unikalny identyfikator (imię.nazwisko). Do zalogowania konieczne jest podanie hasła, które nadaje za formalnym potwierdzeniem administrator aplikacji. System wymusza zmianę hasła przy pierwszym logowaniu. W systemie nie są wykorzystywane konta grupowe.

W systemie „zaszyte" są aplikacyjne mechanizmy kontrolne – do pola numerycznego (jak np. kwota) można wprowadzić jedynie wartości liczbowe, do pola daty – datę w odpowiednim formacie. Wartości w polach wyliczane są w oparciu o wprowadzone

dane stałe (np. stawka VAT), zwykły użytkownik nie ma możliwości zmiany danych stałych.

Zachowana jest pełna ścieżka audytu – każda operacja w systemie EUROBUDŻET skutkująca zmianą statusu jest zapisywana w historii, w której widoczna jest m.in. data operacji oraz login użytkownika, który jej dokonał. Księgowanie następuje etapowo – po wprowadzeniu danych płatność ma status „wprowadzona", a następnie dokonywana płatność musi być zweryfikowana (zmiana statusu na „do zaksięgowania") i dopiero wtedy następuje księgowanie (zmiana statusu na „zaksięgowana"). Użytkownik nie ma możliwości usunięcia zaksięgowanej płatności, nie ma również możliwości zmiany/usunięcia historii operacji.

Wprowadzanie danych podlega kontroli formalnej – podstawą wprowadzenia danych do systemu jest Lista Płatności, otrzymana z Departamentu Funduszy Strukturalnych UM. Lista Płatności musi zostać formalnie zaakceptowana przez szereg osób – m .in. przez Dyrektora Departamentu Funduszy Strukturalnych, dyrektora Departamentu Finansów oraz podpisana przez Główną Księgową. Następnie wypełniana jest karta Listy Sprawdzającej – checklista, w której zawarto pytania dotyczące m.in. formalnej akceptacji, poprawności wprowadzonych kwot. Jeśli na tym etapie pojawią się wątpliwości, dane z Listy Płatności nie są wprowadzane do systemu, a Lista jest zwracana do Departamentu Funduszy Strukturalnych. W przypadku akceptacji Listy Płatności, następuje wprowadzenie danych do systemu, obie Listy (Płatności i Sprawdzająca) są archiwizowane.

Zgodnie z otrzymanymi informacjami, system EUROBUDŻET będzie umożliwiał generowanie raportów służących monitorowaniu stanu środków finansowych. Przykładowo będzie możliwe uzyskanie informacji o wartości środków zaksięgowanych na odpowiednich kontach, działaniach, priorytetach, przeznaczonych na dany projekt, umowę itp. System umożliwia także generowanie dokumentów (np. faktur w wersji elektronicznej i zapisanie ich w wybranym formacie). Ze względu na brak środowiska testowego nie była możliwa weryfikacja modułu generowania raportów na temat stanu środków finansowych, dotyczących monitorowania i sprawozdawczości finansowej.

Rekomendacja 2. Kontrole aplikacyjne – System księgowy

W dalszej perspektywie planowana jest integracja systemu EUROBUDŻET z systemem VIDEOTEL, wykorzystywanym do rozliczeń bankowych (poprzez bezpośredni eksport/import danych, bez ingerencji użytkownika). Obecnie dane do systemu VIDEOTEL wprowadzane są osobno, na podstawie Listy Płatności.

System VIDEOTEL jest zainstalowany na komputerach 6 użytkowników. Do zalogowania w systemie konieczne jest podanie unikalnego identyfikatora użytkownika (pierwsza litera imienia.nazwisko) oraz hasła. W systemie zapewniona jest ścieżka audytu oraz pełna historia operacji. Użytkownik nie ma możliwości zmiany wykonanych przelewów.

Planowana jest również integracja systemu EUROBUDŻET z opracowywanym w Departamencie Funduszy Strukturalnych systemem SOWA. Będzie to Lokalny System Informatyczny (w rozumieniu wytycznych Ministerstwa Rozwoju Regionalnego) służący do ewidencji projektów, wniosków, umów o dofinansowanie oraz generowania zleceń płatności, przesyłanych do sytemu księgowego.

Z uzyskanych informacji wynika, iż trwają prace nad opracowaniem podstawowych założeń, po czym nastąpi podjęcie decyzji, czy system będzie opracowywany wewnętrznie, czy zlecony wykonawcy zewnętrznemu. Na chwilę obecną brak jest formalnych dokumentów i zatwierdzonych zasad budowy/opracowania tego systemu.

Rekomendacja 3. Kontrole aplikacyjne - Lokalny System Informatyczny

Wstępne uruchomienie takiego systemu planowane jest na okres lipiec – wrzesień br., uzyskanie pełnej funkcjonalności – do końca 2008 r. Do tego czasu obsługa wniosków będzie obywać się tylko w formie papierowej (poza doraźnymi sprawozdaniami i raportami opracowywanymi w arkuszu kalkulacyjnym MS Excel).

4. PLANOWANIE I ORGANIZACJA

Zasady zarządzania oraz organizacja bezpieczeństwa informacji w Urzędzie Marszałkowskim Województwa Podlaskiego zostały określone w następujących dokumentach:

- *Instrukcja Bezpieczeństwa Systemów Informatycznych w Urzędzie Marszałkowskim Województwa Podlaskiego,* formalnie zaakceptowana oraz wprowadzona Zarządzeniem wewnętrznym nr 2/04 Marszałka Województwa Podlaskiego z dnia 5.02.2004 r.;
- *Polityka Bezpieczeństwa z 2003 r.*, dostarczona przez dostawcę oprogramowania.

Od momentu zatwierdzenia *Polityka Bezpieczeństwa* oraz *Instrukcja Bezpieczeństwa Systemów Informatycznych* nie były przeglądane ani uaktualniane. Obecnie przygotowywana jest nowa, kompleksowa wersja *Polityki Bezpieczeństwa*, która zostanie przekazana Marszałkowi Województwa Podlaskiego w połowie marca 2008 r. do weryfikacji i zatwierdzenia. Zgodnie z otrzymanymi informacjami nowa *Polityka bezpieczeństwa* zastąpi dotychczas istniejące dokumenty.

Nowa *Polityka bezpieczeństwa* składać się będzie z dwóch części – części ogólnej, precyzującej obowiązki użytkowników i administratorów systemów oraz zawierającej ogólne polityki wykorzystania systemów informatycznych Urzędu oraz części technicznej, zawierającej ustawienia i parametry bezpieczeństwa systemów.

Rekomendacja 4. Planowanie i organizacja – Polityka Bezpieczeństwa

Wymienione powyżej dokumenty są formalnymi procedurami, w oparciu o które odbywa się zarządzanie systemami informatycznymi w UM WP.

W ramach dostarczonej *Polityki Bezpieczeństwa* wykonano wstępną analizę ryzyka i identyfikację zagrożeń dla systemów informatycznych UMWP. Wykonana analiza ryzyka zawiera m.in.:

- Analizę systemu informatycznego – strukturę sprzętową systemu informatycznego UMWP oraz wyszczególnienie wszystkich zasobów sprzętowych oraz zainstalowanego oprogramowania systemowego i aplikacyjnego;
- Analizę procesów biznesowych – wyszczególnienie podstawowych grup procesów biznesowych realizowanych przez UMWP;
- Identyfikację zagrożeń w podziale na odpowiednie kategorie:
  - *Awarie techniczne sprzętu komputerowego*,
  - *Awarie (zawieszenie, destrukcja) systemów operacyjnych poszczególnych komputerów* (krytyczne i niekrytyczne),
  - *Awarie aplikacji użytkowych* (awarie klienta i awarie serwera aplikacji) pojawiające się wskutek ujawnienia się błędu programu lub awarii środowiska (systemu operacyjnego, łączności z serwerami aplikacji),
  - *Utrata konsystencji danych lokalnych i centralnych*,
  - *Utrata danych lokalnych i centralnych*,

- *Atak na system informatyczny pochodzący z zewnątrz*,
- *Atak na system informatyczny pochodzący z wewnątrz* (np. nieuprawniony dostęp do aplikacji i informacji),
- *Zatrzymanie systemu informatycznego w wyniku braku zasilania*,
- *Zainfekowanie serwerów/komputerów stanowiskowych wirusami komputerowymi*.

- Analizę ryzyka z uwzględnieniem zidentyfikowanych zagrożeń.

W *Polityce Bezpieczeństwa* zawarto schemat klasyfikacji danych w UMWP. Klasyfikacja informacji została oparta na następujących kryteriach: dostępność, wrażliwość, dodatkowe (wynikające np. z przyjętych ustaw i rozporządzeń – ustawy o ochronie danych osobowych oraz ustawy o ochronie informacji niejawnych, ustawie o dostępie do informacji publicznej).

Polityka Bezpieczeństwa definiuje formalną strukturę organizacji bezpieczeństwa informacji w instytucji. Zgodnie z jej zapisami w strukturze Urzędu Marszałkowskiego wyodrębniono:

- *Zarządcę Systemu Informatycznego,* który pełni nadzór nad prawidłowym funkcjonowaniem całego systemu;
- *Administratora Systemu Informatycznego*, odpowiedzialnego za bieżące zarządzanie i administrowanie całością systemu;
- *Administratora Bezpieczeństwa Systemu Informatycznego UMWP,* do którego obowiązków należy m.in. nadzór nad okresowym składowaniem danych, wykonywanie i przechowywanie kopii bezpieczeństwa, bieżąca analiza logów, opiniowanie konfiguracji elementów bezpieczeństwa systemów;
- *Audytora Bezpieczeństwa Systemu Informatycznego*, który dokonuje okresowych ocen funkcjonowania systemu bezpieczeństwa – obecnie tą funkcję pełnią pracownicy Zespołu Audytu Wewnętrznego w ramach wykonywanych zadań;
- *Właścicieli Aplikacji* - Dyrektorów Departamentów/Kierowników poszczególnych komórek organizacyjnych, odpowiedzialnych za zarządzanie powierzonym im aplikacjami.

W odniesieniu do aplikacji służących do księgowania i monitorowania środków finansowych pochodzących z funduszy strukturalnych funkcję Właścicieli Aplikacji pełnią Dyrektor Departamentu Finansów w zakresie systemów księgowych EUROBUDŻET oraz KWANT oraz Dyrektor Departamentu Funduszy Strukturalnych w zakresie powstającego systemu monitoringu i sprawozdawczości (LSI).

Polityka Bezpieczeństwa zawiera podstawowe wytyczne dotyczące ochrony i zabezpieczenia systemu informatycznego Urzędu. Obejmuje ona m.in.:

- wytyczne dotyczące ochrony stanowisk pracy (pomieszczenia serwerowni, zabezpieczania komputerów hasłem dostępu);
- wytyczne dotyczące bezpieczeństwa i ochrony komputerów przenośnych, dysków i nośników danych;
- zasady przydzielania i odbierania praw dostępu i uwierzytelniania użytkowników;

- zasady ochrony systemów informatycznych Urzędu przed nieupoważnionymi działaniami użytkowników;
- zasady zabezpieczenia serwerów, urządzeń sieciowych oraz kont administratorów;
- zabezpieczenia przed awariami systemu, reakcje na sytuacje nadzwyczajne i instrukcje postępowania w przypadku awarii;
- zasady tworzenia kopii zapasowych i kopii awaryjnych.

Instrukcja bezpieczeństwa precyzuje zapisy Polityki Bezpieczeństwa w odniesieniu do zarządzania bezpieczeństwem systemów informatycznych. *Instrukcja bezpieczeństwa* zawiera m.in.:

- zasady kontroli dostępu do sieci i systemu informatycznego;
- zasady stosowanej w Urzędzie polityki haseł i kont;
- obowiązki i odpowiedzialności osób odpowiedzialnych za zapewnienie bezpieczeństwa informacji oraz użytkowników systemu informatycznego Urzędu Marszałkowskiego;
- wytyczne dotyczące korzystania z Internetu oraz poczty elektronicznej;
- procedurę zarządzania incydentami naruszenia bezpieczeństwa informacji

Pracownicy podpisują oświadczenia o zapoznaniu się z obowiązującymi zasadami bezpieczeństwa informacji i zobowiązują się do ich przestrzegania – wzór takiego oświadczenia stanowi załącznik do *Instrukcji Bezpieczeństwa.*

5. ZAKUP I WDROŻENIE

Wprowadzanie zmian i aktualizacji oraz utrzymanie systemu EUROBUDŻET odbywa się na podstawie formalnej umowy nr WR/17/07/07 zawartej w Białymstoku w dniu 31.07.2007 pomiędzy Województwem Podlaskim a firmą MiCOMP Systemy Komputerowe – producentem i dostawcą oprogramowania. Przedmiotem umowy jest objęcie nadzorem autorskim oprogramowania EUROBUDŻET. W ramach nadzoru autorskiego firma MiCOMP zobowiązała się do:

- opracowania i wdrożenia aktualizacji oprogramowania, w szczególności dostarczania aktualizacji zapewniających zgodność systemu EUROBUDŻET z obowiązującymi przepisami prawnymi;
- gotowość przyjmowania propozycji modyfikacji oprogramowania oraz odpłatnego ich wykonania, zgodnie z wymaganiami Urzędu Marszałkowskiego;
- usuwania błędów i usterek występujących w trakcie eksploatacji oprogramowania;
- udzielanie konsultacji telefonicznych oraz w siedzibie Urzędu Marszałkowskiego umożliwiających rozwiązywanie problemów występujących w trakcie eksploatacji systemu EUROBUDŻET (usługa Helpdesku);
- przekazywania informacji pozwalających pracownikom Urzędu Marszałkowskiego w pełni wykorzystać oprogramowanie.

Aktualizacja oprogramowania odbywa się poprzez udostępnienie na serwerze FTP najnowszej wersji systemu, wraz ze szczegółową instrukcją postępowania podczas instalacji oraz pisemnym wykazem zmian w oprogramowaniu w stosunku do poprzednich wersji. Instalacja oprogramowania jest przeprowadzana przez pracownika Urzędu.

Firma MiCOMP jest posiadaczem pełni praw autorskich dotyczących kodu źródłowego systemu EUROBUDŻET. Zawarta umowa nie zawiera postanowień „code escrow".

Umowa została zawarta na rok czasu, obowiązuje do 30.06.2008 r.

W zawartej umowie zdefiniowano obowiązki obydwu stron w zakresie objęcia nadzorem autorskim systemu EUROBUDŻET oraz podstawowe warunki świadczenia usług. Uzgodniono również system zgłaszania uwag i pytań. Obydwie strony umowy uzgodniły, iż zgłoszenia będą klasyfikowane pod względem dwóch priorytetów. W przypadku zgłoszenia błędu o priorytecie wyższym „A" czas reakcji wykonawcy nie może przekroczyć 1 dnia roboczego, a czas całkowitego rozwiązania problemu powinien zająć maksymalnie 3 dni robocze. W przypadku zgłoszenia błędu o niższym priorytecie „B" czas rozwiązania problemu, lub zaproponowania zastępczej metody pracy, wynosi 7 dni. W przypadku niedotrzymania tych terminów Wykonawcę obowiązują określone w umowie kary umowne.

Formularz zgłoszenia problemu stanowi załącznik do umowy.

W umowie zawarto zapis dotyczący możliwości przekazania fragmentów lub całości baz danych do Wykonawcy oprogramowania, poza siedzibę Urzędu Marszałkowskiego. Umowa zawiera zobowiązanie Wykonawcy do zapewnienia poufności i utrzymania w tajemnicy uzyskanych informacji oraz dokumentacji technicznej.

Zgodnie z zapisami umowy pracownicy Urzędu Marszałkowskiego są zobowiązani do nie dokonywania samodzielnie żadnych zmian w konfiguracji oprogramowania i sprzętu komputerowego, na którym jest zainstalowany system EUROBUDŻET, w tym nie dokonywanie nieautoryzowanych modyfikacji zawartości baz danych.

Zarządzanie zmianą w aplikacji EUROBUDŻET w Urzędzie Marszałkowskim zostało zredukowane do konieczności instalacji aktualizacji zamieszczanych na serwerze FTP firmy MiCOMP. Zgodnie z otrzymanymi informacji jest to obowiązkiem osoby wyznaczonej do zarządzania systemem EUROBUDŻET. Zawarta umowa nie przewiduje formalnej akceptacji zmian oprogramowania przez przedstawiciela Urzędu Marszałkowskiego przed wprowadzeniem ich do środowiska produkcyjnego, nie opisuje konieczności wcześniejszego dokonywania testów aplikacji oraz testów zgodności oraz nie obliguje dostawcy oprogramowania do dostarczenia środowiska testowego na użytek Urzędu. Całość procesu wprowadzania zmian i poprawek do systemu EUROBUDŻET znajduje się w obowiązkach dostawcy oprogramowania, który jest odpowiedzialny za ww. czynności.

Środowisko testowe systemu EUROBUDŻET nie jest wykorzystywane w Urzędzie Marszałkowskim.

Rekomendacja 5. Zakup i wdrożenie – Zarządzanie zmianą

Aktualizacja systemów operacyjnych stacji roboczych i serwerów, na których jest zainstalowany system EUROBUDŻET odbywa się automatycznie przy wykorzystaniu narzędzia *Windows Server Update Services*. Poprawki i aktualizacje systemów operacyjnych pobierane są automatycznie przez serwer, a następnie udostępniane komputerom znajdującym się w sieci LAN. Proces instalacji poprawek przebiega bez udziału użytkownika, który nie ma możliwości zablokowania/wyłączenia automatycznej aktualizacji.

6. DOSTARCZANIE I WSPARCIE

Zawarta umowa z dostawcą systemu EUROBUDŻET oraz postanowienia dotyczące zapewnienia poziomu świadczonych usług zostały opisane w części *5. Zakup i wdrożenie*. W Urzędzie Marszałkowskim została formalnie wyznaczona osoba zarządzająca aplikacją, która jest odpowiedzialna za utrzymywanie kontaktów z dostawcą, zgłaszanie błędów i propozycji modyfikacji oraz monitorowanie działań podejmowanych przez producenta systemu.

Proces nadawania praw dostępu do systemu informatycznego jest w Urzędzie Marszałkowskim sformalizowany – każdy użytkownik musi wypełnić *Wniosek o nadanie praw dostępu do zasobów sieciowych*, którego wzór stanowi załącznik do *Instrukcji Bezpieczeństwa.* Na wniosku podpisuje się użytkownik, Dyrektor Departamentu/Biura, któremu użytkownik podlega służbowo oraz administrator systemu zakładający konto. Wniosek jest uzupełniany o nr w ewidencji pracowników i osób uprawnionych do korzystania z systemów informatycznych, którą prowadzi Referat Kadr i Szkoleń.

Na wniosku odnotowane są dane użytkownika, jego unikalny login nadawany w momencie utworzenia konta oraz czas ważności konta (nieokreślony, określony czas zatrudnienia). Na podstawie formalnego wniosku administrator dokonuje założenia i konfiguracji konta w ustawieniach domenowych.

W przypadku, gdy prawa dostępu są przyznawane na czas określony (np. dla praktykantów, stażystów, serwisantów, pracowników firm zewnętrznych itp.) po upływie czasu określonego na wniosku system automatycznie wymusza blokadę konta i w celu przedłużenia jego ważności wypełniany jest kolejny wniosek.

Wszystkie wnioski są archiwizowane w Departamencie Informatyki w pokoju administratora systemu.

Odebranie praw dostępu i blokada konta w domenie następuje na podstawie obiegówki pokazywanej administratorowi przez odchodzącego użytkownika, lub w sytuacjach nadzwyczajnych na wniosek Dyrektora Departamentu, któremu użytkownik podlega służbowo (np. w sprawach dyscyplinarnych). W Urzędzie Marszałkowskim nie obowiązują inne formalne zasady odbierania praw dostępu.

Proces nadawania praw dostępu do poczty elektronicznej jest również sformalizowany – wypełniany jest *Wniosek o skonfigurowanie konta poczty elektronicznej*, stanowiący załącznik do *Instrukcji Bezpieczeństwa*. Procedura postępowania jest identyczna jak w przypadku *Wniosków o nadanie praw dostępu*.

Wszystkie komputery pracujące w sieci Urzędu Marszałkowskiego objęte są systemem ochrony antywirusowej *McAfee*, zainstalowanym na serwerach i stacjach roboczych użytkowników. Każdorazowo raz dzienne wykonywane jest zaplanowane skanowanie systemu w celu wykrycia i zlikwidowania nieautoryzowanego lub szkodliwego oprogramowania. Odbierana i wysyłana poczta skanowana jest na serwerach pocztowych oraz lokalnie, na komputerach użytkowników.

Do dystrybucji definicji sygnatur wirusów i aktualizacji oprogramowania stosowana jest centralna aplikacja ułatwiająca zarządzanie aktualizacją oprogramowania antywirusowego.

W przypadku jej awarii, oprogramowanie stacji roboczych i serwerów zostało tak skonfigurowane, aby automatycznie łączyć się przy starcie systemu z serwerem dystrybucji aktualizacji oraz pobierać i instalować najnowsze wersje sygnatur.

W trakcie audytu stwierdzono, iż data bazy danych sygnatur wirusów na komputerze administratora systemu nie była aktualizowana przez okres ostatnich trzech tygodni.

Rekomendacja 6. Dostarczanie i wsparcie – Oprogramowanie antywirusowe

W celu zapewnienia kontroli dostępu w Urzędzie Marszałkowskim są stosowane hasła dostępu do systemu operacyjnego. Identyfikacja użytkownika w systemie operacyjnym odbywa się na podstawie indywidualnego, imiennego loginu skojarzonego z hasłem. Z identyfikatorem związane są prawa dostępu określające uprawnienia użytkownika. Zwykli użytkownicy, w tym osoby obsługujące system EUROBUDŻET, posiadają uprawnienia użytkownika na stacjach roboczych.

System wymusza (ustawienia domenowe) następujące wymogi dotyczące haseł użytkowników:

- minimalna długość hasła – 6 znaków;
- hasło musi spełniać wymagania dotyczące złożoności – musi być kombinacją liter i cyfr;
- hasło musi zostać zmienione każdorazowo po upływie 40 dni;
- hasło nie może być takie samo jak dwa poprzednio użyte;

W systemie nie włączono opcji automatycznego blokowania konta użytkownika po danej ilości prób logowania się do systemu.

Rekomendacja 7. Dostarczanie i wsparcie – Ustawienia domenowe

W przypadku zapomnienia hasła przez użytkownika, administrator ustawia nowe hasło (po potwierdzeniu tożsamości zgłaszającej osoby) i wymuszana jest automatyczna zmiana tego hasła przy pierwszym logowaniu. Chroniony hasłem wygaszasz ekranu włącza się automatycznie po 10 min. bezczynności systemu.

Zgodnie z zasadami bezpieczeństwa hasło nie powinno być przechowywane w niechronionej postaci, do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury, tzw. „koperty bezpieczne”. Koperty z hasłami w postaci bezpiecznej (m.in. hasła konfiguracyjne switchy, routerów, firewalli oraz do innych krytycznych elementów sieci, główne hasła administracyjne systemów, aplikacji i baz danych, hasła BIOS) przechowywane są w zamkniętym sejfie, w pokoju administratora.

Po odejściu administratora z pracy, zgodnie z *Polityką Bezpieczeństwa*, musi nastąpić zmiana wszystkich haseł.

W celu zapewnienia bezpieczeństwa systemu informatycznego Urzędu Marszałkowskiego oraz ciągłości jego działania wykonywane są regularnie przez administratora

bezpieczeństwa kopie zapasowe. Kopie zapasowe z najważniejszych baz danych (w tym z baz danych systemów księgowych EUROBUDŻET i KWANT) dokonywane są przyrostowo co 2 godziny, na zakończenie dnia wykonywana jest kopia całościowa. Raz w tygodniu, w dzień wolny od pracy, dokonywana jest kopia całościowa zawartości wszystkich serwerów i baz danych.

Dodatkowo w odniesieniu do systemu EUROBUDŻET na koniec każdego kwartału/roku wykonywana jest kopia archiwalna na płytach CD/DVD.

Kopie zapasowe wykonywane są za pomocą zautomatyzowanego narzędzia w cyklu tygodniowym, po czym następuje nadpisanie odpowiedniej tasiemki (oznaczonej etykietami: poniedziałek – piątek, weekend). Kopie zapasowe przechowywane są niedaleko serwerowni (klika pomieszczeń dalej na tym samym piętrze), w zamkniętej szafie w pokoju, do którego dostęp mają jedynie administratorzy. Kopie zapasowe nie są regularnie odtwarzane i testowane, poza ogólnymi uregulowaniami *Instrukcji Bezpieczeństwa* nie istnieją formalne procedury dotyczące tego obszaru.

Rekomendacja 8. Dostarczanie i wsparcie – Kopie zapasowe

Z uzyskanych informacji wynika, iż kilka razy w przeszłości zaistniała konieczność odtworzenia bazy danych z kopii zapasowej. Wszystkie operacje odtworzenia danych zakończyły się pomyślnie.

W Urzędzie Marszałkowskim brak formalnego schematu sieci informatycznej.

Zgodnie z otrzymanymi informacjami istnieją dwa punkty styku sieci wewnętrznej z siecią Internet (jeden w odniesieniu do systemów i sieci LAN Urzędu Marszałkowskiego i jeden w odniesieniu do systemu wojewódzkiego, istnieje możliwość przełączania ruchu pomiędzy routerami). W celu ochrony sieci w jej obszarze wydzielono strefy DMZ, sieć LAN i serwery bazodanowe znajdują się za firewallem sprzętowym (*CISCO PIX*).

Rekomendacja 9. Dostarczanie i wsparcie – Bezpieczeństwo sieci

Firewall został skonfigurowany przez administratora sieci w taki sposób, aby blokować komunikację na portach niezwiązanych z usługami dostępu do internetu oraz poczty elektronicznej. W system włączona jest sonda *Intrusion Detection System*, skanująca ruch w sieci i wykrywająca potencjalne ataki. Administrator sieci dokonuje codziennych przeglądów logów z tej sondy oraz logów z firewalla sprzętowego. Przegląd tych logów dokonywany jest za pomocą aplikacji *CISCO Event Viewer*, która umożliwia automatyczną priorytetyzację alarmów (zaznaczonych kolorem czerwonym na ekranie przeglądu logów). W przypadku podejrzenia wystąpienia incydentu naruszenia bezpieczeństwa sieci powiadamiany jest administrator bezpieczeństwa.

Z otrzymanych informacji wynika, iż dotychczas nie zanotowano udanych prób włamań do sieci LAN Urzędu Marszałkowskiego.

Nie wszystkie urządzenia sieciowe są całkowicie zarządzalne (tzn. nie wszędzie występuje przypisanie gniazdek sieciowych do adresów urządzeń) – istnieje teoretyczna możliwość wpięcia urządzenia zewnętrznego w sieć Urzędu.

Dla wybranych pracowników Urzędu (m.in. Marszałek, Dyrektor Departamentu Informatyki) istnieje możliwość dostępu zdalnego do wybranych aplikacji i poczty elektronicznej – przez szyfrowane połączenie VPN realizowane za pomocą koncentratora VPN. W przypadku konieczności takiego dostępu administrator zestawia i konfiguruje połączenie oraz udostępnia odpowiednie usługi oraz porty komunikacyjne na serwerach. Brak jakichkolwiek formalnych procedur dotyczących tego obszaru (procedury wydawania zezwoleń na utworzenie dostępu zdalnego, wniosków o dostęp zdalny do zasobów, itp.).

Rekomendacja 10. Dostarczanie i wsparcie – Bezpieczeństwo sieci

Podstawowe wytyczne dotyczące fizycznych zabezpieczeń systemów informatycznych Urzędu zostały określone w *Instrukcji Bezpieczeństwa*. Zgodnie z § 5 ust.3 tego dokumentu zabezpieczenia fizyczne realizowane są poprzez odpowiednią lokalizację, bezpieczeństwo fizyczne pomieszczeń informatycznych oraz utworzenie stref specjalnej ochrony. W skład stref specjalnej ochrony wchodzi serwerownia, pomieszczenia z szafami z nośnikami magnetycznymi zawierającymi kopie danych, pomieszczenia z urządzeniami teletransmisyjnymi, wyłącznikami zasilania elektrycznego oraz pomieszczenia administratorów systemu informatycznego.

Obydwie serwerownie Urzędu Marszałkowskiego znajdują się na IV piętrze budynku, obok siebie, w pobliżu pomieszczeń biurowych pracowników Departamentu Informatyki. Wejście na piętro nie jest zamknięte i jest dostępne dla osób trzecich (poza godzinami pracy wejście na piętro jest zamykane przez ochronę budynku). Dane osób wchodzących do budynku Urzędu Marszałkowskiego nie są rejestrowane.

Rekomendacja 11. Dostarczanie i wsparcie – Bezpieczeństwo fizyczne

Wejście do obu pomieszczeń serwerowni jest zamknięte wzmocnionymi zamkami, monitorowane przez kamery CCTV, z których sygnał na bieżąco jest przekazywany do administratora i rejestrowany. Dostęp do pomieszczenia serwerowni uzyskuje się poprzez kartę elektroniczną, którą posiadają uprawnieni administratorzy. Dla osób trzecich (serwisantów, audytorów) oraz osób, które nie posiadają uprawnień stałego dostępu, pobyt w serwerowni jest możliwy wyłącznie w obecności upoważnionego administratora.

Osoby trzecie (serwisanci, audytorzy itp.) uzyskujący dostęp do serwerowni nie muszą wypełniać formalnych wniosków o dostęp.

Prowadzony jest elektroniczny rejestr wejść do serwerowni, w postaci danych pochodzących z systemu dostępu. W rejestrze odnotowana jest osoba wchodząca (dane są sczytywane z karty magnetycznej administratora) oraz godzina wejścia/wyjścia.

W celu ochrony znajdującego się tam okablowania i przewodów transmisyjnych obie serwerownie posiadają podniesione podłogi. Serwerownie wyposażone są w systemy monitorowania pracy zasilaczy UPS oraz w systemy monitorowania warunków środowiskowych - wilgotności i temperatury powietrza. Administrator ma możliwość stałego podglądu tych danych, po przekroczeniu założonych wartości krytycznych uruchamiany jest automatyczny alarm. Serwery znajdują się w szafach o podniesionych półkach, zabezpieczonych dodatkowo zamykanymi drzwiami. Czujniki monitorujące wilgotność i temperaturę powietrza są zlokalizowane w każdej szafie z serwerami.

Obie serwerownie wyposażone są w klimatyzatory oraz systemy gaszenia gazem.

Zgodnie z otrzymanymi informacjami zużyte nośniki optyczne są niszczone przez administratorów, zaś wycofane z eksploatacji lub uszkodzone dyski twarde serwerów i stacji roboczych składowane w zamkniętej szafie. Urząd Marszałkowski nie przekazuje sprzętu komputerowego zawierającego dane do osób trzecich.

W Urzędzie Marszałkowskim nie istnieje szczegółowy plan zapewnienia ciągłości działania w odniesieniu do systemu EUROBUDŻET tj. plan zawierający szczegółowe procedury zapewniające utrzymanie ciągłości księgowania środków w przypadku wystąpienia katastrofy lub rozległej awarii. Ogólne wytyczne dotyczące postępowania w sytuacjach nadzwyczajnych oraz procedury awaryjne zostały zawarte w *Polityce Bezpieczeństwa* oraz *Instrukcji bezpieczeństwa systemów informatycznych*, jak również zawarte w postanowieniach umowy z dostawcą oprogramowania.

Rekomendacja 12. Dostarczanie i wsparcie – Plan zapewnienia ciągłości działania

7. MONITOROWANIE I OCENA

Zgodnie z zapisami *Polityki Bezpieczeństwa* w Urzędzie Marszałkowskim Województwa Podlaskiego prowadzony jest bieżący monitoring systemu informatycznego, polegający na analizie przez upoważnionych pracowników (administratorów sieci oraz administratorów aplikacji) raportowanych zdarzeń pochodzących z urządzeń i systemów (m.in. sondę IDS i firewall, dzienniki zdarzeń każdego komputera, logi i historie aplikacji).

Dodatkowo, mechanizmem pozwalającym na okresową, niezależną analizę i ocenę stanu bezpieczeństwa i wiarygodności systemów informatycznych są audyty realizowane przez Zespół ds. Audytu Wewnętrznego. Zgodnie z otrzymanymi informacjami ostatni audyt informatyczny został przeprowadzony ok. rok temu, brak jest jednakże formalnych raportów i sprawozdań z tych audytów.

8. USTALENIA I REKOMENDACJE

Niniejszy rozdział podsumowuje rekomendacje, które są wynikiem przeprowadzonych prac w Urzędzie Marszałkowskim Województwa Podlaskiego.

Poszczególne kwestie analizowane były z perspektywy potencjalnego wpływu, jaki mogą mieć na działalność Urzędu w zakresie obsługi informatycznej Regionalnego Programu Operacyjnego Województwa Podlaskiego oraz Programu Operacyjnego Kapitał Ludzki. Poszczególnym kwestiom nadane zostały priorytety zgodne z następującymi definicjami:

- Wysoki – zagadnienia wymagające natychmiastowej reakcji kierownictwa jednostki podlegającej badaniu, ustalenia mają wpływ na zastrzeżenia w opinii z audytu zgodności.
- Średni – zagadnienia istotne w kontekście środowiska kontroli jednostek podlegających audytowi i wymagające zajęcia się nimi przez kierownictwo jednostki, ustalenia pośrednio mogą mieć wpływ na zastrzeżenia w opinii z audytu zgodności.
- Niski – zagadnienia wymagające podjęcia działań zmierzających do poprawy efektywności systemu zarządzania i kontroli

W trakcie naszych prac zostało zidentyfikowanych łącznie: 7 kwestii o priorytecie średnim i 5 kwestii o priorytecie niskim.

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

1. Kontrole aplikacyjne – System księgowy

Priorytet	Niski
Ustalenia	Proces zarządzania systemem EUROBUDŻET jest częściowo sformalizowany – nadawania i odbieranie uprawnień dostępu odbywa się na podstawie wniosku o dostęp do systemów informatycznych, zaś użytkownicy potwierdzają odbiór hasła i loginu. Brak jest jednakże szczegółowych procedur zarządzania i formalnych wytycznych dotyczących korzystania z systemu (np. procedur eksploatacyjnych).
Implikacje	Brak formalnych wytycznych dotyczących zarządzania i wykorzystania systemu EUROBUDŻET zwiększa podatność systemu na niewłaściwe użycie, będące skutkiem błędu lub celowego działania.
Rekomendacje	Zaleca się opracowanie i wdrożenie formalnych zasad i wytycznych dotyczących zarządzania i wykorzystywania systemu EUROBUDŻET.
Odpowiedź Urzędu	Sformalizowane procedury zarządzania systemem Eurobudżet oraz procedury eksploatacyjne zostaną opracowane i wdrożone w oparciu o *Instrukcję bezpieczeństwa systemów informatycznych UMWP* i zatwierdzone przez Właściciela systemu.
Termin wdrożenia	31.05.2008

2. Kontrole aplikacyjne – System księgowy

Priorytet Średni

Ustalenia System EUROBUDŻET będzie umożliwiał generowanie raportów służących monitorowaniu stanu środków finansowych. Przykładowo będzie możliwe uzyskanie informacji o wartości środków zaksięgowanych na odpowiednich kontach, działaniach, priorytetach, przeznaczonych na dany projekt, umowę itp.

Ze względu na brak środowiska testowego nie była możliwa weryfikacja modułu generowania raportów na temat stanu środków finansowych, dotyczących monitorowania i sprawozdawczości finansowej.

Implikacje Brak modułu sprawozdawczości finansowej w systemie lub niewłaściwe jego funkcjonowanie może prowadzić do nie spełniania wymogów prawnych określonych w prawie krajowym i wspólnotowym.

Rekomendacje Zaleca się dokonanie weryfikacji działania systemu EUROBUDŻET w zakresie modułu generowania raportów na temat stanu środków finansowych i uzyskanie potwierdzenia, iż system ten może być wykorzystywany do celów monitoringu i sprawozdawczości finansowej.

Odpowiedź Urzędu W ankiecie dotyczącej informacji nt. środowiska informatycznego funkcjonującego w Urzędzie Marszałkowskim Województwa Podlaskiego opisano aplikacje (moduły) wchodzące w skład systemu Eurobudżet, w tym Sprawozdawczość.

W dniach 31.03.2008-02.04.2008r. przeprowadzono wdrożenie systemu Eurobudżet w zakresie funduszy pomocowych, z udziałem przedstawiciela firmy MiCOMP. Sprawdzone zostały następujące obszary działania systemu:

- wprowadzanie w module Księga Główna danych na podstawie dokumentów źródłowych dotyczących przepływów środków finansowych (Wyciągi bankowe) oraz stanowiących podstawę wypłaty środków (FV, R-ki, Listy płac, dyspozycje, itp.) w ramach Działania 10.1 PO KL;
- generowanie wydruków z poszczególnych kont

księgowych, celem uzyskania informacji niezbędnych do monitorowania stanu środków, oraz zrealizowanych wydatków w ramach poszczególnych grup rocznego planu działań PT PO KL;

- generowanie obowiązujących sprawozdań finansowych w module Sprawozdawczość na podstawie danych finansowych wprowadzonych w module Księga Główna.

Termin wdrożenia

Do 15.05.2008 r. zostanie zakończone wprowadzanie danych finansowych i sprawdzenie w/w funkcjonalności systemu w ramach Priorytetu 7 RPOWP. Dalsze prace nad wdrożeniem systemu, w zakresie poszczególnych działań PO KL i RPO WP będą następować sukcesywnie w miarę napływu środków finansowych oraz realizowanych płatności na rzecz Beneficjentów.

Stanowisko Instytucji Audytowej

W odpowiedzi na pismo nr DO5/9017/3/MDQ/221/08/540 przesłano do Instytucji Audytowej wygenerowane z programu EUROBUDŻET formularze *Zestawień obrotów i sald* na kontach o nr 130 oraz 137 oraz formularze *Sprawozdań z wykonania planu wydatków budżetowych jednostki samorządu terytorialnego RB-28s*.

Po otrzymaniu odpowiedzi obniżono status rekomendacji. Wdrożenie rekomendacji będzie przedmiotem audytu sprawdzającego.

3. Kontrole aplikacyjne - Lokalny System Informatyczny

Priorytet	Średni
Ustalenia	W Urzędzie Marszałkowskim Województwa Podlaskiego trwają prace nad wdrożeniem Lokalnego Systemu Informatycznego, służącego do ewidencji projektów, wniosków, umów o dofinansowanie oraz generowania zleceń płatności. Zgodnie z uzyskanymi informacjami obecnie opracowywane są podstawowe założenia, po czym nastąpi podjęcie decyzji, czy system będzie budowany wewnętrznie, czy zlecony wykonawcy zewnętrznemu. Na chwilę obecną brak jest formalnych dokumentów i zatwierdzonych zasad budowy/opracowania tego systemu.
Implikacje	Brak formalnych zasad budowy/opracowania Lokalnego Systemu Informatycznego, przy założonych terminach jego wykonania, zwiększa ryzyko nie wdrożenia systemu w określonym terminie lub implementację systemu nie w pełni funkcjonalnego.
Rekomendacje	Zaleca się opracowanie i zatwierdzenie formalnych wymogów i założeń dotyczących Lokalnego Systemu Informatycznego, służącego do ewidencji projektów, wniosków, umów o dofinansowanie oraz generowania zleceń płatności.
Odpowiedź Urzędu	Lokalny System Informatyczny dla wspierania zarządzania EFRR w ramach RPO WP jest na etapie zatwierdzania funkcjonalności. Planuje się zakończenie prac nad dokumentacja projektowa do końca maja 2008 roku. Produkcyjne wdrożenie Generatora Wniosków jest przewidziane na koniec czerwca 2008 roku. Uruchomienie pierwszego modułu LSI do końca sierpnia 2008 roku. Uruchomienie drugiego (ostatniego) modułu do końca grudnia 2008 roku.
Termin wdrożenia	Do końca grudnia 2008 roku planowane jest zakończenie prac i wdrożenie systemu LSI.

4. Planowanie i organizacja – Polityka Bezpieczeństwa

Priorytet Średni

Ustalenia Od momentu zatwierdzenia *Polityka Bezpieczeństwa* oraz *Instrukcja Bezpieczeństwa Systemów Informatycznych* nie były przeglądane ani uaktualniane. Dokumenty te zostały formalnie zaakceptowane odpowiednio w 2003 oraz w 2004 r.

Zgodnie z uzyskanymi informacjami obecnie przygotowywana jest nowa, kompleksowa wersja *Polityki Bezpieczeństwa*, która zostanie przekazana Marszałkowi Województwa Podlaskiego w połowie marca 2008 r. do weryfikacji i zatwierdzenia. Zgodnie z otrzymanymi informacjami nowa *Polityka Bezpieczeństwa* zastąpi dotychczas istniejące dokumenty.

Implikacje Brak zaktualizowanych dokumentów dotyczących zasad bezpieczeństwa informacyjnego utrudnia tworzenie kompleksowych, sprawnych i skutecznych mechanizmów zapewniających odpowiedni poziom bezpieczeństwa oraz uniemożliwia zapewnienie spójności pomiędzy poszczególnymi procedurami regulującymi kwestie bezpieczeństwa.

Rekomendacje Zaleca się opracowanie i wdrożenie aktualnych dokumentów wyznaczających system zarządzania bezpieczeństwem informacji w instytucji.

Zaleca się regularny przegląd i aktualizację *Polityki Bezpieczeństwa* oraz wynikających z niej szczegółowych zasad zarządzania systemami informatycznymi.

Odpowiedź Urzędu Zatwierdzona *Polityka Bezpieczeństwa* oraz *Instrukcja Bezpieczeństwa Systemów Informatycznych* z 2003 oraz z 2004 roku regulują zagadnienia związane z zabezpieczeniem funkcjonowania systemów informatycznych w zakresie bezpieczeństwa organizacyjnego i technicznego. Zapisy dotyczące zabezpieczeń technicznych są nadal aktualne, natomiast regulacje dot. bezpieczeństwa organizacyjnego muszą uwzględnić wprowadzone zmiany organizacyjne Urzędu z drugiej połowy marca 2008. Departament odpowiedzialny za sprawy informatyczne uległ reorganizacji, w ramach której rozszerzono zakres działania i odpowiedzialności tej komórki.

	Obecnie są przygotowane projekty polityk bezpieczeństwa i trwają prace nad procedurami do tych polityk. Aktualna forma dokumentów związanych z bezpieczeństwem została stworzona w takim brzmieniu, aby kolejne zmiany organizacyjne nie powodowały konieczności zmiany treści tych dokumentów. Zasady przeglądów i aktualizacji polityk bezpieczeństwa będą wynikały z treści procedur. Kompleksowe wdrożenie polityk bezpieczeństwa wraz z tworzonymi procedurami zostało ujęte w programie działania UMWP na 2008 rok, którego realizacja została wpisana na II półrocze 2008 r.
Termin wdrożenia	II półrocze 2008 r.

5. Zakup i wdrożenie – Zarządzanie zmianą

Priorytet Średni

Ustalenia Zarządzanie zmianą w aplikacji EUROBUDŻET w Urzędzie Marszałkowskim zostało zredukowane do pobierania aktualizacji zamieszczanych na serwerze firmy MiCOMP i ich instalacji na środowisku produkcyjnym. Zawarta umowa nie przewiduje formalnej akceptacji zmian oprogramowania przez przedstawiciela Urzędu Marszałkowskiego przed wprowadzeniem ich do środowiska produkcyjnego oraz konieczności wcześniejszego szczegółowego testowania wprowadzanych zmian (lub możliwości uczestniczenia w testach przez przedstawiciela Urzędu).

Brak jest formalnych zasad zarządzania zmianą w odniesieniu do aplikacji EUROBUDŻET.

Środowisko testowe systemu EUROBUDŻET nie jest wykorzystywane w Urzędzie Marszałkowskim.

Implikacje Brak formalnych zasad zarządzania zmianą może prowadzić do nieautoryzowanego wprowadzania zmian w systemie, a w konsekwencji do braku integralności danych bądź niewłaściwego funkcjonowania całego systemu.

Dodatkowo brak środowiska testowo-szkoleniowego uniemożliwia prowadzenie wewnętrznych testów systemu i szkolenie nowych użytkowników.

Rekomendacje Zaleca się ustanowienie formalnych procedur zarządzania zmianami w systemie EUROBUDŻET zawierających m.in. konieczność szczegółowego testowania wprowadzanych zmian do systemu, formalną akceptację dokonywanych zmian, opracowanie scenariuszy testowych i planów testów.

Odpowiedź Urzędu Zarządzanie zmianami w celu ochrony przed nieautoryzowanym wprowadzeniem zmian w systemie Eurobudżet odbywa się poprzez:

1) Instalację nowych wersji systemu pochodzących wyłącznie od Wykonawcy systemu firmy MiCOMP Systemu Komputerowe Sp. z o.o. Aktualizacje posiadają unikatowy identyfikator wersji.
2) Pobieranie i wykonywanie aktualizacji lub innych

czynności wpływających na funkcjonalność systemu należy wyłącznie do administratora systemu. Zgodnie § 4 pkt 3 umowy nr WR/17/07/07 z dnia 31.07.2007 na nadzór autorski oprogramowania komputerowego firma MiCOMP udostępnia nowe wersje oprogramowania na serwerze FTP, o czym powiadamiany jest e-mailem administrator systemu. Dostęp do serwera FTP jest autoryzowany, należy wprowadzić nazwę użytkownika i hasło, które zna wyłącznie administrator systemu (nazwa użytkownika i hasło przechowywane są w zaklejonej kopercie w sejfie).

3) Nadanie uprawnień dostępu do baz systemu Eurobudżet, jak też folderu, w którym zainstalowany jest system. Aktualizacja systemu polega na uruchomieniu skryptów na bazie danych systemu Eurobudżet oraz aktualizacji plików wykonywalnych. Zarówno dostęp do serwera bazodanowego, jak i aplikacyjnego mają wyłącznie administratorzy.
4) Wykonywanie kopii awaryjnej systemu przed dokonaniem zmian w systemie, co umożliwi przywrócenie systemu do pierwotnego stanu w przypadku problemów występujących po wykonywaniu zmian.

Zawarta umowa nie przewiduje formalnej akceptacji zmian oprogramowania przez przedstawiciela Urzędu Marszałkowskiego (zmiany te wykonywane są nie tylko na potrzeby Urzędu i mają w szczególności zapewnić zgodność oprogramowania z obowiązującymi przepisami prawa). Wykonawca jest zobowiązany natomiast do zamieszczania na serwerze FTP wraz z nową wersją oprogramowania: wykazu wprowadzonych zmian w oprogramowaniu oraz szczegółową instrukcję postępowania podczas instalacji.

Odpowiednia procedura zarządzania zmianami w systemie Eurobudżet, uwzględniająca m.in. uzyskanie pisemnego potwierdzenia pozwolenia Właściciela systemu na dokonanie zmian lub innych czynności wpływających na funkcjonalność systemu oraz ich dokumentowania zostanie opracowana i wdrożona w oparciu o *Instrukcję bezpieczeństwa systemów informatycznych UMWP*.

Termin wdrożenia

31.05.2008

Stanowisko Instytucji Audytowej

W odpowiedzi na pismo nr nr DO5/9017/3/MDQ/221/08/540 do Instytucji Audytowej przesłano *Instrukcję zarządzania bezpieczeństwem systemu finansowo-księgowego EUROBUDŻET*, która w punkcie *5. Zarządzanie konfiguracją*

i zmianami zawiera procedury zarządzania zmianami w systemie EUROBUDŻET.

Ponadto Instytucja Audytowa została poinformowana, iż w nowej umowie zawartej z firmą MiCOMP Systemy Komputerowe na nadzór autorski oprogramowania komputerowego (Umowa nr 2/UMWP/07/2008 z dnia 4 lipca 2008 r.) wprowadzono zapis, iż „Wykonawca systemu zapewnia, że dostarczone aktualizacje oprogramowania zostaną sprawdzone i należycie przetestowane, tak by w żaden sposób nie spowodowały one pogorszenia działania programu lub utraty możliwości korzystania z poprawnie do tej pory działających opcji".

Po otrzymaniu odpowiedzi obniżono status rekomendacji. Wdrożenie rekomendacji będzie przedmiotem audytu sprawdzającego.

6. Dostarczanie i wsparcie – Oprogramowanie antywirusowe

Priorytet	Średni
Ustalenia	W trakcie audytu stwierdzono, iż data bazy danych sygnatur wirusów na komputerze administratora systemu nie była aktualizowana przez okres ostatnich trzech tygodni.
Implikacje	Brak regularnie aktualizowanego oprogramowania antywirusowego znacznie zwiększa ryzyko narażenia systemów Urzędu na ataki z użyciem kodu złośliwego.
Rekomendacje	Zaleca się dokonanie przeglądu procesu aktualizacji oprogramowania antywirusowego i instalację najnowszych wersji oprogramowania antywirusowego i baz danych sygnatur wirusów na wszystkich komputerach administratorów, stacjach roboczych użytkowników oraz serwerach.
Odpowiedź Urzędu	Od marca 2008 zrekonfigurowano centralne zarządzanie systemem antywirusowym Urzędu, dzięki czemu stacje robocze i serwery mają wymuszaną codzienną aktualizację baz antywirusowych.
Termin wdrożenia	marzec 2008

7. Dostarczanie i wsparcie – Ustawienia domenowe

Priorytet	Średni
Ustalenia	W ustawieniach domenowych w systemie nie włączono opcji automatycznego blokowania konta użytkownika po określonej liczbie nieudanych prób logowania się do systemu.
Implikacje	Brak blokady konta domenowego po określonej liczbie nieudanych prób logowania do systemu może powodować próby łamania haseł w systemach informatycznych Urzędu oraz nieautoryzowane wykorzystanie kont użytkowników.
Rekomendacje	Zaleca się wprowadzenie mechanizmu powodującego blokadę konta użytkownika po określonej liczbie błędnych prób logowania do systemu.
Odpowiedź Urzędu	Wprowadzono mechanizm powodujący blokadę użytkownika po 7 błędnych próbach logowania do systemu.
Termin wdrożenia	kwiecień 2008

8. Dostarczanie i wsparcie – Kopie zapasowe

Priorytet	Średni
Ustalenia	Kopie zapasowe danych przechowywane są w pobliżu serwerowni (kilka pomieszczeń dalej na tym samym piętrze), w zamkniętej szafie w pokoju, do którego dostęp mają jedynie administratorzy. Kopie zapasowe nie są regularnie odtwarzane i testowane. Poza ogólnymi uregulowaniami *Polityki Bezpieczeństwa* nie istnieją formalne procedury dotyczące tego obszaru.
Implikacje	Brak zasad testowania i odtwarzania kopii zapasowych oraz przechowywanie ich w pobliżu pomieszczeń serwerowni może uniemożliwić skuteczne odtworzenie danych po katastrofie lub rozległej awarii.
Rekomendacje	Zaleca się przechowywanie kopii zapasowych najważniejszych baz danych w bezpiecznej odległości (w miarę możliwości w innej fizycznej lokalizacji) od danych źródłowych, aby zapewnić skuteczne odtworzenie systemów po np. pożarze budynku. Zaleca się wdrożenie formalnych zasad regularnego testowania i odtwarzania kopii zapasowych.
Odpowiedź Urzędu	Obecne składowanie kopii bezpieczeństwa odbywa się w osobnym pomieszczeniu przeznaczonym wyłącznie do tego celu, posiadającym drzwi ogniotrwałe i antywłamaniowe. Pomieszczenie ponadto posiada system antypożarowy. Nośniki z backupem są przechowywane w kasetce zamykanej w metalowej szafie. Urząd nie posiada w chwili obecnej możliwości przeniesienia serwerowni backupowej do innej lokalizacji. Sformalizowanie zasad testowania i odtwarzania kopii zapasowych zostanie ujęte w tworzonych procedurach, które zgodnie z odpowiedzią do pkt4 zostaną wdrożone w II połowie 2008.
Termin wdrożenia	w zakresie zasad testowania i odtwarzania kopii zapasowych II połowa 2008

9. Dostarczanie i wsparcie – Bezpieczeństwo sieci

Priorytet	Niski
Ustalenia	Zgodnie z otrzymanymi informacjami istnieją dwa punkty styku sieci wewnętrznej z siecią Internet. W celu ochrony sieci w jej obszarze wydzielono strefy DMZ, sieć LAN i serwery bazodanowe znajdują się za firewallem filtrującym ruch. W Urzędzie Marszałkowskim Województwa Podlaskiego brak jest formalnego schematu sieci informatycznej.
Implikacje	Brak formalnego, regularnie aktualizowanego schematu sieci informatycznej zwiększa ryzyko dokonywania nieautoryzowanych zmian w infrastrukturze sieciowej Urzędu.
Rekomendacje	Zaleca się opracowanie schematu sieci informatycznej oraz dokonywanie jego regularnych aktualizacji przy każdorazowej zmianie konfiguracji sieci informatycznej.
Odpowiedź Urzędu	Schemat sieci informatycznej umieszczony jest w dokumentacji powykonawczej dostawcy sytemu informatycznego UMWP.
Termin wdrożenia	-

10. Dostarczanie i wsparcie – Bezpieczeństwo sieci

Priorytet	Niski
Ustalenia	Wybrani pracownicy Urzędu Marszałkowskiego posiadają możliwość dostępu zdalnego do wybranych aplikacji (innych niż wspierające wydatkowanie funduszy UE) i poczty elektronicznej – przez szyfrowane połączenie VPN. W przypadku konieczności takiego dostępu administrator zestawia i konfiguruje połączenie oraz udostępnia odpowiednie usługi oraz porty komunikacyjne na serwerach. Brak jest jakichkolwiek formalnych procedur dotyczących tego obszaru (procedury wydawania zezwoleń na utworzenie dostępu zdalnego, wniosków o dostęp zdalny do zasobów itp.).
Implikacje	Brak formalnego uregulowania zasad dostępu zdalnego do systemów Urzędu Marszałkowskiego zwiększa podatność sieci na ataki z zewnątrz.
Rekomendacje	Zaleca się opracowanie formalnych zasad nadawania i odbierania uprawnień dostępu zdalnego do systemów informatycznych Urzędu.
Odpowiedź Urzędu	Obecnie połączenia VPN są tworzone na wniosek kadry kierowniczej Urzędu. Na dzień dzisiejszy dostęp taki posiada 5 osób (połączenia związane z odbieraniem poczty). Zasady formalne nadawania i odbierania uprawnień do tego typu połączeń zostaną zawarte w procedurach, o których mowa w odpowiedzi do pkt 4.
Termin wdrożenia	II połowa 2008 r.

11. Dostarczanie i wsparcie – Bezpieczeństwo fizyczne

Priorytet	Niski
Ustalenia	Obydwie serwerownie Urzędu Marszałkowskiego znajdują się na IV piętrze budynku, obok siebie, w pobliżu pomieszczeń biurowych pracowników Departamentu Informatyki (w tym pomieszczeń administratorów systemu). Wejście na piętro nie jest zamknięte i jest dostępne dla osób trzecich (poza godzinami pracy wejście na piętro jest zamykane przez ochronę budynku). Dane osób wchodzących do budynku Urzędu Marszałkowskiego nie są rejestrowane.
Implikacje	Brak mechanizmu zabezpieczającego przed nieuprawnionym dostępem do piętra, na którym znajdują się pomieszczenia administratorów systemu informatycznego oraz serwerownie może powodować wystąpienie przypadków naruszenia bezpieczeństwa fizycznego Urzędu i nieautoryzowany dostęp do informacji.
Rekomendacje	Zaleca się wprowadzenie mechanizmu zabezpieczającego przed nieuprawnionym dostępem do piętra, na którym znajdują się pomieszczenia administratorów systemu informatycznego oraz serwerownie.
Odpowiedź Urzędu	Pomieszczenia serwerowni Urzędu posiadają monitoring wejść i wyjść do poszczególnych stref serwerowni. Zamknięcie pomieszczeń biurowych, w których pracują administratorzy systemów jest przewidziane w roku 2008.
Termin wdrożenia	II półrocze 2008 r.

12. Dostarczanie i wsparcie – Plan zapewnienia ciągłości działania

Priorytet Niski

Ustalenia Ogólne wytyczne dotyczące postępowania w sytuacjach nadzwyczajnych oraz procedury awaryjne zostały zawarte w *Polityce Bezpieczeństwa* oraz *Instrukcji bezpieczeństwa systemów informatycznych* oraz w postanowieniach umowy z dostawcą systemu EUROBUDŻET.

W Urzędzie Marszałkowskim nie istnieje szczegółowy plan zapewnienia ciągłości działania w odniesieniu do systemu EUROBUDŻET tj. plan zawierający szczegółowe procedury zapewniające utrzymanie ciągłości księgowania środków w przypadku wystąpienia katastrofy lub rozległej awarii.

Implikacje Brak szczegółowego planu zapewnienia ciągłości działania w odniesieniu do systemu EUROBUDŻET zwiększa ryzyko przerwania operacji biznesowych dokonywanych za pomocą tego systemu w przypadku katastrofy lub rozległej awarii.

Rekomendacje Zaleca się opracowanie i zatwierdzenie planu zapewnienia ciągłości działania w odniesieniu do systemu EUROBUDŻET, zawierającego szczegółowe procedury postępowania w przypadku wystąpienia katastrofy lub awarii i zapewniające ciągłość pracy Urzędu.

Odpowiedź Urzędu Zapewnieniu ciągłości działania systemu Eurobudżet oraz jego przywrócenia w przypadku wystąpienia katastrofy lub awarii służą wdrożone środki administracyjne, fizyczne, techniczne i programowe, opisane w *Instrukcji bezpieczeństwa systemów informatycznych UMWP*, gdyż ciągłość działania systemu jest ściśle uzależniona od całokształtu środków i działań zapewniających bezpieczeństwo sprzętu i danych zgromadzonych w SI UMWP. Szczególnej ochronie podlegają bazy danych, których kopie zapasowe wykonywane są 3 razy dziennie, tzn.: o godz. 10:00, 12:00 i 14:00.

Ponadto podpisana z firmą MiCOMP umowa na nadzór autorski gwarantuje m.in. w przypadku „uniemożliwienia użytkowania systemu w zakresie jego podstawowej funkcjonalności z jego przeznaczeniem, a w szczególności utratę danych lub naruszenie ich spójności, w wyniku której niemożliwe będzie poprawne działanie systemu", iż czas podjęcia przez Wykonawcę czynności zmierzających do

podjęcia przez Wykonawcę czynności zmierzających do naprawy błędu wyniesie 1 dzień roboczy od otrzymania zgłoszenia. Zgłoszenia dokonuje Administrator systemu na specjalnym formularzu stanowiącym Załącznik Nr 1 do umowy drogą elektroniczną bądź w razie trudności z wysłaniem e-maila faksem lub telefonicznie.

Uszczegółowione procedury postępowania w przypadku wystąpienia katastrofy lub awarii systemu Eurobudżet zostaną opracowane i zatwierdzone przez Właściciela systemu.

Termin wdrożenia 31.05.2008

PODSEKRETARZ STANU
Generalny Inspektor Kontroli Skarbowej
Andrzej Parafianowicz

RZECZPOSPOLITA POLSKA

MINISTERSTWO FINANSÓW

GENERALNY INSPEKTOR KONTROLI SKARBOWEJ

Sprawozdanie

z czynności sprawdzających w zakresie

audytu zgodności

systemów informatycznych

Ministerstwa Rozwoju Regionalnego

Wrzesień 2008

SPIS TREŚCI

1. WPROWADZENIE

Cel dokumentu

Art. 70 i 71 *rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999*[1], nakładają na państwo członkowskie obowiązek uzyskania zapewnienia, że systemy zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58-62 tego *rozporządzenia* oraz że funkcjonują skutecznie. Audyt zgodności, zgodnie z art. 71 ust. 1 w zw. z ust. 2 *rozporządzenia 1083/2006* powinien zostać zakończony przed złożeniem przez Polskę pierwszego wniosku o płatność pośrednią do KE, lub nie później niż w terminie 12 miesięcy od zatwierdzenia przez KE każdego programu operacyjnego.

Zasadniczym celem niniejszego audytu jest uzyskanie zapewnienia, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych, są ustanowione zgodnie z wymogami art. 58d), 60c) oraz 61e) ww. *rozporządzenia.*

W ramach wykonanych prac audytowych dokonano przeglądu Krajowego Systemu Informatycznego SIMIK 07-13 oraz ogólnego środowiska informatycznego, w jakim on funkcjonuje. Dokonano również przeglądu systemu rachunkowo - księgowego Ministerstwa Rozwoju Regionalnego, używanego do księgowania płatności w ramach zarządzanych Programów Operacyjnych.

Środowisko informatyczne Krajowego Systemu Informatycznego, zgodnie z metodologią COBIT 4.1 zostało ujęte w następujące obszary:

- *Kontrole Aplikacyjne;*
- *Planowanie i Organizacja*;
- *Zakup i Wdrożenie;*
- *Dostarczanie i Wsparcie*;
- *Monitorowanie i Ocena.*

Każdy z tych obszarów został podzielony na wybrane procesy w oparciu o metodologię COBIT 4.1 przy wykorzystaniu standardów Stowarzyszenia ds. audytu i kontroli systemów informatycznych ISACA.

W ramach dokumentowania stanu faktycznego, szczególna uwaga została poświęcona identyfikacji mechanizmów kontrolnych odnoszących się do ryzyka utraty poufności danych (*Confidentiality Risk*), ryzyka utraty integralności danych (*Integrity Risk*), oraz ryzyka braku dostępności danych (*Availability Risk*). Zidentyfikowane mechanizmy kontrolne zostały następnie poddane testom, na podstawie których została oceniona efektywność ich funkcjonowania.

[1] Dz.U.UE.L.06.210.25

Prace audytowe zostały przeprowadzone w dniach 01.05-26.06.2008 w Ministerstwie Rozwoju Regionalnego, Ministerstwie Finansów oraz siedzibach wybranych instytucji Zarządzających, Pośredniczących, Pośredniczących II stopnia oraz Certyfikujących zaangażowanych w wydatkowanie środków pochodzących z Programów Operacyjnych i Regionalnych Programów Operacyjnych na lata 2007-2013.

Dodatkowo w dniu 18.07.2008 r. przeprowadzono sprawdzenie dot. wdrożenia III grupy funkcjonalności systemu KSI SIMIK 07-13.

Wyniki przeprowadzonych prac zostały oparte na dokumentach dostarczonych przez pracowników instytucji obsługujących Krajowy System Informatyczny SIMIK 07-13, wydrukach z badanych modułów oraz informacjach przekazanych w rozmowach, a także obserwacjach procesów i operacji wykonywanych w systemie informatycznym. Wyniki opierają się na założeniu, że wszystkie przekazywane informacje zostały przedstawione zgodnie z najlepszą wiedzą pracowników instytucji, w sposób kompletny, rzetelny i prawdziwy.

Sprawozdanie zostało sporządzone według stanu na dzień 26 czerwca 2008 r. i może być rozpatrywane tylko w świetle kwestii i faktów w nim przedstawionych. Zawarte w *Sprawozdaniu* ustalenia odzwierciedlają stan rzeczywisty stwierdzony podczas przeglądu aplikacji wykorzystywanych do obsługi środków w ramach funduszy strukturalnych.

Na podstawie przeprowadzonego audytu, pomimo zastrzeżeń opisanych w części *8. Ustalenia i rekomendacje* niniejszego *Sprawozdania*, uzyskano zapewnienie, że systemy informatyczne funkcjonujące w ramach systemów zarządzania i kontroli programów operacyjnych są ustanowione zgodnie z wymogami art. 58d), 60c) oraz 61e) *rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającego rozporządzenie (WE) nr 1260/1999.*

2. STRESZCZENIE

Podstawowym systemem informatycznym, w którym odbywać się będzie ewidencja oraz obsługa projektów, wniosków o dofinansowanie i zawartych umów z beneficjentami w ramach Programów Operacyjnych perspektywy finansowej 2007-2013 jest Krajowy System Informatyczny SIMIK 07-13 (KSI SIMIK 07-13). Jest to system o zasięgu ogólnokrajowym, zbudowany na zasadzie aplikacji webowej, dostępnej przez sieć Internet. KSI SIMIK 07-13 zawiera funkcjonalności wspomagające proces programowania i monitorowania wdrażania realizowanych projektów UE w Polsce.

Dostęp do KSI SIMIK 07-13, zgodnie z wytycznymi MRR, mają zapewniony wszystkie podmioty uczestniczące w systemie zarządzania i kontroli:

- Ministerstwo Rozwoju Regionalnego, pełniące rolę **Instytucji Koordynującej** Narodowe Strategiczne Ramy Odniesienia;
- **Instytucje Zarządzające** (IZ) poszczególnymi programami operacyjnymi;
- Instytucje uczestniczące we wdrażaniu poszczególnych programów operacyjnych – **Instytucje Pośredniczące** (IP) oraz **Instytucje Pośredniczące II stopnia** (IP2);
- **Instytucje Certyfikujące** (IC) oraz **Instytucje Certyfikujące II Stopnia** (IC2);
- **Instytucja Audytowa**;
- oraz Departament Rozwoju Systemów Informatycznych Ministerstwa Finansów, odpowiedzialny za techniczna obsługę systemu.

Dane gromadzone w Krajowym Systemie Informatycznym pozwolą na uzyskanie pełnego wykazu informacji, o których mowa w załączniku III do r*ozporządzenia Komisji (WE) 1828/2006 z dnia 6 grudnia 2006 r. ustanawiającego szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006*) dla każdego Programu Operacyjnego oraz Regionalnych Programów Operacyjnych perspektywy finansowej 2007-2013.

Administracją Krajowego Systemu Informatycznego SIMIK 07-13 i jego merytoryczną obsługą zajmują się wyznaczeni pracownicy Ministerstwa Rozwoju Regionalnego. Pracownicy Departamentu Rozwoju Systemów Informatycznych Ministerstwa Finansów są odpowiedzialni za działanie systemu od strony technicznej oraz utrzymanie pomieszczeń służących do gromadzenia i przetwarzania danych.

Zasadniczym założeniem dotyczącym funkcjonalności KSI SIMIK 07-13 podczas tworzenia i budowania systemu, a także z punktu widzenia doświadczeń poprzedniego okresu programowania, było założenie, iż system ma gromadzić i przetwarzać minimalną ilość danych wymaganych przez regulacje wspólnotowe oraz akty prawa krajowego w zakresie monitorowania wykorzystania środków finansowych pochodzących z funduszy Unii Europejskiej. System powinien zawierać informacje, które po ich agregacji umożliwią wsparcie procesu tworzenia zestawień wydatków na wszystkich poziomach wdrażania. System powinien również umożliwiać wsparcie tworzenia bieżących sprawozdań dotyczących ilości aplikacji o środki finansowe, realizowanych projektów, zaangażowanych kwot, ewentualnego postępu wskaźników itp.

System KSI SIMIK 07-13 nie eliminuje obiegu dokumentacji papierowej, a jedynie rejestruje, magazynuje i agreguje niektóre dane z tej dokumentacji. Dane wprowadzone do systemu tworzą złożoną bazę danych, którą można filtrować i wydobywać z niej raporty

w dowolnych układach. Oryginalne dokumenty źródłowe, z których pochodzą dane wprowadzane do systemu, są przechowywane w odpowiednich Instytucjach oraz w siedzibach beneficjentów.

Zgodnie z zapisami *Założeń projektu „Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013”* w systemie SIMIK zarejestrowane są tylko wnioski formalnie poprawne, nie odnoszące się do Europejskiej Współpracy Terytorialnej.

Obecnie system KSI SIMIK 07-13 składa się z następujących części:

- podstawowy moduł KSI SIMIK 07-13, obsługiwany przez przeglądarkę internetową, posiadający system zarządzania bazami danych ORACLE;
- *Oracle Discoverer*, dedykowana aplikacja dostępna przez przeglądarkę internetową, służąca do generowania raportów z bazy danych dotyczących monitorowania i sprawozdawczości środków strukturalnych pochodzących z perspektywy 2007-2013;
- moduł SIMIKXML, służący do importu i walidacji plików XML, pochodzących z Lokalnych Systemów Informatycznych.

Od strony funkcjonalnej system KSI SIMIK obejmuje trzy podstawowe grupy użyteczności:

- I grupa funkcjonalności, zawierająca następujące moduły:
  - Administracja systemem KSI SIMIK 07-13;
  - Interfejsy komunikacyjne, obsługujące proces wymiany danych pomiędzy Lokalnymi Systemami Informatycznymi a Krajowym Systemem Informatycznym;
  - Obsługa cyklu życia projektu, ewidencjonowanie i obsługa danych dotyczących wniosków aplikacyjnych, umów o dofinansowanie oraz wniosków o płatność;
  - Moduł kontroli poszczególnych projektów;
- II grupa funkcjonalności, obejmującą:
  - Wsparcie obsługi dużych projektów;
  - Ewidencja danych dotyczących programów operacyjnych;
  - Przygotowanie deklaracji wydatków oraz wniosków o płatność;
  - Wspieranie procesu „monitorowania wdrażania” poprzez standardowe raporty umożliwiające przygotowanie zestawień wydatków z poziomu Instytucji Pośredniczącej oraz zestawień wydatków i wniosków o płatność na wszystkich wyższych poziomach;
  - Wspieranie procesu „monitorowania wdrażania” poprzez standardowe raporty umożliwiające uzyskanie prognoz wydatków;
- III grupa funkcjonalności, zawierająca następujące funkcjonalności:
  - Wprowadzenie słownika wskaźników postępu rzeczowego i ich ewidencjonowanie;
  - Ewidencjonowanie i rejestr kwot odzyskanych;
  - Zapewnienie mechanizmów definiowania niestandardowych raportów.

System KSI jest obecnie w pełni funkcjonalny w zakresie ww. grup funkcjonalności (wdrożone i utrzymywane środowisko produkcyjne) – wdrożenie trzeciej grupy

funkcjonalności nastąpiło po przeprowadzeniu pełnych testów i końcowym odbiorze w dniu 7.07.2008 r.

Księgi rachunkowe w Ministerstwie Rozwoju Regionalnego prowadzone są przy użyciu systemu informatycznego QWANT w wersji 4.00 firmy QNT Systemy Informatyczne Sp. z o.o. (wdrożony w MRR w październiku 2005 r.).

Podstawowe cechy programu to:

- definiowane przez użytkownika wykaz rejestrów księgowych, struktura konta, plan kont wraz z wykazem księgowań dozwolonych dla wskazanego konta;
- prowadzenie rejestrów bankowych, kasowych, poleceń księgowania;
- wielowalutowość, automatyczne obliczanie różnic kursowych;
- bieżące sprawdzanie poprawności wprowadzanych dokumentów;
- różnorodne zestawienia (analityczne, syntetyczne) finansowe, rozrachunkowe, kosztowe z dowolnych urządzeń księgowych i dokumentów;
- automatyczne tworzenie bilansu zamknięcia i otwarcia;
- obsługa programu za pomocą list zleceń (menu);
- rozbudowany system haseł i kontroli uprawnień użytkowników, pozwalający na dostosowanie do struktury organizacyjnej i kompetencji pracowników.

Cała funkcjonalność programu jest zorganizowana w postaci okien, dostępnych przez użycie odpowiedniej opcji menu programu. Menu jest wielopoziomowe. Okna programu służą do wprowadzania danych, umożliwiają dokonywanie ich przetwarzania, a także pozwalają na prezentację zestawień.

Ze względu na fakt, iż Krajowy System Informatyczny SIMIK 07-13 swoim zasięgiem obejmuje wszystkie Instytucje zaangażowane w proces dystrybucji środków finansowych pochodzących z Programów Operacyjnych w ramach perspektywy 2007-2013, wyniki prac audytowych zawarte w niniejszym *Sprawozdaniu* odnoszą się do wszystkich Programów Operacyjnych i mają wpływ na wydanie opinii, o której mowa w art. 71 ust. 2 rozporządzenia Rady (WE) 1083/2006 z dnia 11 lipca 2006 r.

W rozdziałach 3-7 niniejszego *Sprawozdania* zawarto szczegółowy opis stanu faktycznego stwierdzonego podczas audytu.

W trakcie naszych prac zostało zidentyfikowanych łącznie: 5 kwestii o priorytecie średnim oraz 36 kwestii o priorytecie niskim, szczegółowo opisanych w rozdziale 8 *Sprawozdania*.

Brak jest rekomendacji o priorytecie wysokim, które mogłyby mieć bezpośredni wpływ na zastrzeżenia w opinii z audytu zgodności.

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

3. PLANOWANIE I ORGANIZACJA

3.1. Określenie Architektury Informacyjnej

3.1.1 Model architektury informacyjnej instytucji

Podstawowy zarys architektury informatycznej systemu KSI SIMIK 07-13 został określony w roboczym dokumencie *Architektura techniczna systemu KSI SIMIK 07-13* oraz w szczegółowej dokumentacji administracyjnej systemu. Zgodnie z zapisami tych dokumentów system SIMIK 07-13 tworzony jest w technologii internetowej w architekturze klient-serwer, umożliwiającej użytkownikom zalogowanie się do aplikacji i wprowadzanie danych do systemu informatycznego poprzez dostępną przeglądarkę internetową. Użytkownicy logują się do aplikacji poprzez protokół HTTPS.

Na potrzeby systemu SIMIK 07-13 przygotowano cztery dedykowane serwery z zainstalowanym systemem operacyjnym *Windows Server 2003*. Aplikacja internetowa obsługująca system wykonana jest w technologii .NET Framework i jest zainstalowana na dwóch serwerach aplikacyjnych, podłączonych do Internetu poprzez strefę DMZ. Dwa serwery bazodanowe pracują w konfiguracji primary-standby, co oznacza, iż w przypadku awarii lub przestoju pierwszego serwera jego funkcję przejmuje drugi, a dane pomiędzy nimi są regularnie synchronizowane. Do obsługi baz danych obu serwerów wykorzystano system zarządzania bazami danych ORACLE w wersji 9i.

Na tych samych serwerach, lecz w oparciu o rozdzielne schematy baz danych, zainstalowane jest środowisko testowo-szkoleniowe.

System jest budowany w sposób umożliwiający ewentualną zmianę architektury technicznej i łatwą rozbudowę. Zgodnie z otrzymanymi informacjami docelowo system KSI SIMIK 07-13 składał się będzie z trzech serwerów aplikacyjnych bezpośrednio połączonych z dwoma serwerami bazodanowymi. Podstawowa baza produkcyjna będzie zainstalowana na dedykowanym serwerze, na drugim natomiast będzie zainstalowana regularnie synchronizowana baza w trybie standby i środowisko testowo-szkoleniowe. Na potrzeby rozbudowy systemu zakupiono już niezbędny sprzęt informatyczny Czas przebudowy systemu uzależniony jest od migracji do nowej serwerowni, co zostało szczegółowo opisane w części *5.9. Zarządzanie środowiskiem fizycznym.*

Zgodnie z otrzymanymi informacjami model architektury informacyjnej systemu KSI SIMIK nie został formalnie zatwierdzony przez Właściciela systemu – dokument *Architektura techniczna systemu KSI SIMIK 07-13* jest dostępny jedynie w wersji roboczej.

Rekomendacja 1. Planowanie i organizacja – Model architektury informacyjnej instytucji

3.1.2 Słowniki danych i reguły składni danych

W celu utrzymania integralności i poprawności przetwarzanych danych w systemie zdefiniowano szczegółowe słowniki danych i reguły składni danych, służące standaryzacji danych wprowadzanych do systemu a pochodzących z różnych Programów Operacyjnych.

Podstawową grupę słowników stanowią słowniki proste (np. jednostki miary, rodzaj formy prawnej beneficjenta, rodzaj podmiotu, rodzaj stosowanego wskaźnika postępu rzeczowego, typ projektu). Oprócz tego w systemie zdefiniowano m.in. słownik jednostek geograficznych (kody NUTS/NTS i GUS) i listę instytucji zaangażowanych w obsługę procesu wydatkowania środków pochodzących z funduszy strukturalnych perspektywy 07-13.

Z punktu widzenia funkcjonalności systemu jednym z najważniejszych zdefiniowanych słowników w systemie jest słownik poziomów wdrażania, który zawiera podział głównego węzła słownika – Narodowych Strategicznych Ram Odniesienia – na Program Operacyjny oraz poszczególne osie priorytetowe, działania i poddziałania. W ramach struktury tego słownika na poziomie Programu Operacyjnego przypisano również kod CCI (kod jednolitego dokumentu programowego - fr. Code commun d'identification).

Użytkownik wprowadzający informacje z danego wniosku o dofinansowanie, umowy bądź wniosku o płatność musi wybrać wartość z listy rozwijalnej pochodzącej ze słownika poziomów wdrażania i nie ma możliwości samodzielnej edycji tych informacji. Rozwiązanie takie pomaga zachować integralność przetwarzanych danych. Szczegółowe zabezpieczenia w tym zakresie zostały opisane w części *7.1. Kontrola w aplikacjach*.

Wymagania funkcjonalne dotyczące słowników zostały zdefiniowane w *Specyfikacjach przypadków użycia.* Zgodnie z tymi dokumentami każdy słownik składa się z głównego węzła oraz kilku poziomów, dla których zdefiniowano odpowiednie pola w bazie danych.

W trakcie audytu ustalono, iż za zarządzanie słownikami wbudowanymi w system odpowiada Administrator Merytoryczny w Instytucji Koordynującej. Jedyne wytyczne dotyczące zarządzania słownikami w systemie KSI zostały zawarte w Procedurach Wewnętrznych Wydziału Administracji i Audytu Systemów Informatycznych Departamentu Koordynacji i Zarządzania PWW MRR. Zgodnie z zapisami tego dokumentu Naczelnik Wydziału wyznacza pracownika odpowiedzialnego za wprowadzenie zmian w danych słownikowych w KSI. Następnie zmiana jest realizowana przez AM IK NSRO lub pracownika Ministerstwa Finansów, po czym Kierownictwo Departamentu zatwierdza dokumentację.

Opisana procedura nie zawiera jasno określonej ścieżki akceptacji zmian danych słownikowych (z treści procedury wynika, iż zatwierdzenie dokumentacji przez Kierownictwo Departamentu następuje po wprowadzeniu zmian do systemu) oraz szczegółowego wykazu, za jakie słowniki odpowiadają Administratorzy Merytoryczni IK NSRO, a za które ponoszą odpowiedzialność Administratorzy Techniczni w Ministerstwie Finansów.

Rekomendacja 2. Planowanie i organizacja – Słowniki danych i reguły składni danych

3.1.3 Schemat klasyfikacji danych

Zgodnie z *Założeniami projektu „Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013”* system KSI SIMIK 07-13 nie ma charakteru księgowego (nie służy do rejestracji zapisów księgowych i nie podlega wymogom ustawy o rachunkowości), nie zawiera również informacji niejawnych w rozumieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych[2] oraz danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3].

Przetwarzane dane w systemie są dostępne jedynie dla zarejestrowanych użytkowników systemu, po podaniu przez nich hasła logowania. Każdemu użytkownikowi został przypisany profil dostępowy, w którym skonfigurowano jego uprawnienia w sposób ograniczony do zakresu wykonywanych obowiązków. Obostrzenia dotyczą:

- poziomu wdrażania – użytkownicy aplikacji wprowadzający dane na poziomie Instytucji Pośredniczącej II stopnia mają dostęp do informacji tylko dla nich przeznaczonych; np. użytkownicy na poziomie Instytucji Pośredniczącej mają dostęp do danych przeznaczonych dla IP i podległych IP2, użytkownicy IZ mają pełny dostęp do informacji dotyczących danego Programu Operacyjnego);
- Programu Operacyjnego – użytkownicy przypisani do danego Programu Operacyjnego nie posiadają dostępu do informacji dotyczących innych Programów Operacyjnych;
- zróżnicowania terytorialnego – dane z poszczególnych jednostek terytorialnych są agregowane na poziomie centralnej Instytucji Zarządzającej.

System gromadzi dane określone w załączniku III do r*ozporządzenia Komisji (WE) 1828/2006 z dnia 6 grudnia 2006 r. ustanawiającego szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006*) dla każdego Programu Operacyjnego oraz Regionalnych Programów Operacyjnych perspektywy finansowej 2007-2013.

3.1.4 Zarządzanie integralnością

W celu zarządzania integralnością w systemie SIMIK 07-13 zostały ustalone i przyjęte *Polityka Bezpieczeństwa* oraz szczegółowe procedury monitorowania i wykorzystania systemu, opisane w dalszych częściach niniejszego *Sprawozdania*.

W samej aplikacji wbudowane zostały aplikacyjne mechanizmy kontrolne, których obecność zwiększa jakość i integralność danych wprowadzanych do systemu.

[2] Tekst jednolity: Dz. U. z 2005 r. Nr 196, poz. 1631 ze zm.
[3] Tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.

3.2. Szacowanie i Zarządzanie Ryzykiem IT

3.2.1 Szacowanie ryzyka

Podstawowym dokumentem dotyczącym szacowania ryzyk związanych z Krajowym Systemem Informatycznym jest *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13* (na podstawie metodologii CRAMM) opracowany wspólnie przez Ministerstwo Finansów oraz Ministerstwo Rozwoju Regionalnego i zatwierdzony przez Dyrektora Departamentu Rozwoju Systemów Informatycznych MF. Dokument ma zastosowanie do wszystkich elementów KSI SIMIK 07-13. Opracowany został na podstawie następujących dokumentów:

- *Polityka Bezpieczeństwa Informacji. Dokument Ramowy (PBI-DR-ramowy-z-v1.30);*
- *Polityka bezpieczeństwa <systemu informatycznego>. Wzór (PBI-SI-wzor-z-v1.30);*
- *Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji. Dokument ramowy (PBI-INB-ramowy-z-v1.30);*
- *Standard Budowy Dokumentu z Zakresu Eksploatacji Systemów Informatycznych i Bezpieczeństwa Informacji (OGO-STD-x-AD-x-x-z-MF_EI-v1.00);*
- *Założenia Projektu – wersja 3.0;*
- *Porozumienie o współpracy przy realizacji projektu;*
- *Plan zarządzania wymaganiami – wersja S713-Z-DIP-ZR;*
- *Specyfikacja niefunkcjonalna - wersja 1.13;*
- *Zasady bezpiecznego korzystania z sieci systemu informatycznego Monitoringu i Kontroli Finansowej Funduszy Strukturalnych i Funduszu Spójności SIMIK-NET.*

Zgodnie z *Polityką bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* dokument *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13* jest opracowywany przez Zespół do Spraw Bezpieczeństwa Informacji (ZBI) wraz z Administratorem Bezpieczeństwa Informacji (ABI). Dokument aktualizowany jest w zależności od zmieniających się zagrożeń i podatności.

Szacowanie ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13 zostało przeprowadzone przy użyciu metod ilościowych i jakościowych dla następujących elementów technicznych:

- serwerów aplikacyjnych i bazodanowych;
- urządzeń sieciowych.

Dla podanych powyżej urządzeń na podstawie występujących zagrożeń określone zostały przedziały szacunkowe ryzyka:

- Niskie;
- Średnie;

- Wysokie;
- Bardzo wysokie.

Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13 opisuje wymagane zachowania i niezbędne zabezpieczenia dla zasobu wynikające z otrzymanej oceny, przy oszacowanym poziomie ryzyka.

W analizie nie zostały uwzględnione ryzyka wynikające z procesów biznesowych mających bezpośredni wpływ na pracę systemu.

3.2.2 Reakcja na wystąpienie ryzyka

Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13 zawiera zastosowane zabezpieczenia w celu zminimalizowania wystąpienia ryzyka. Nie zostały jednak zidentyfikowane procesy odpowiedzi na występujące w systemie informacyjnym ryzyka w celu złagodzenia ewentualnych strat (przy uwzględnieniu takich strategii działania jak unikanie, redukcja, przeniesienie lub akceptacja).

3.2.3 Utrzymanie i monitorowanie planu postępowania w przypadku wystąpienia ryzyka

Nie został opracowany plan postępowania w przypadku wystąpienia ryzyka, który uwzględniałby takie elementy jak np.: odpowiedź na poszczególne ryzyka (z uwzględnieniem kosztów, potencjalnych korzyści, odpowiedzialności), zgodę właścicieli procesów na ryzyko wewnętrzne (szczątkowe) oraz na podejmowane działania zabezpieczające, monitorowanie wykonania planu, raportowanie wyjątków, itp.

Rekomendacja 3. Planowanie i Organizacja – Szacowanie i zarządzanie ryzykiem IT

4. ZAKUP I WDROŻENIE

4.1. Rozwój i Utrzymanie Oprogramowania Aplikacyjnego

4.1.1 Projektowanie szczegółowe

Podstawowym dokumentem wyznaczającym proces budowy i tworzenia systemu SIMIK 07-13 jest dokument *Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013 (SIMIK 07-13) – Założenia projektu*, uzgodniony i zaakceptowany przez Ministerstwo Rozwoju Regionalnego (Głównego Użytkownika) oraz Ministerstwo Finansów (Głównego Dostawcę) w dniu 23 lutego 2007 r. w dniu formalnego porozumienia. Zgodnie z zapisami tego dokumentu tworzenie aplikacji SIMIK odbywać się będzie zgodnie z metodyką zarządzania projektami PRINCE2.

Wykonawcą oprogramowania systemu KSI SIMIK 07-13 jest wybrana zgodnie z procedurą zamówień publicznych firma ComArch S.A.

Na całym etapie budowy systemu ustalono poszczególne podstawowe potrzeby udziałowców i użytkowników, ogólne funkcjonalności całego systemu oraz uzgodniono proponowaną strukturę projektową.

Szczegółowe projektowanie aplikacji KSI SIMIK 07-13 odbywało się zgodnie z metodyką procesu inżynierii oprogramowania *Rational Unified Process*. Jako jeden z dokumentów podrzędnych, wymaganych przez tą metodykę, został opracowany dokument *Kryteria jakości – odbioru* – dokument opisujący warunki, które muszą zostać spełnione podczas odbioru poszczególnych funkcjonalności. Zgodnie z zapisami tego dokumentu system KSI SIMIK 07-13 zostanie zaakceptowany jeżeli:

- będzie zgodny ze specyfikacją wymagań funkcjonalnych i niefunkcjonalnych;
- zostaną przedstawione scenariusze testowe właściwe dla aplikacji;
- zostanie przedstawiona pełna dokumentacja aplikacji w postaci instrukcji stanowiskowych i użytkownika;
- zostanie przedstawiona pełna dokumentacja aplikacji w postaci podręczników wykładowcy i studenta.

Dla każdej grupy funkcjonalności aplikacji określono szczegółowe *Scenariusze przypadków użycia*, definiujące zakres wymagań. Funkcjonalności systemu zostały określone z dokładnością do poszczególnych pól formularza. W opisie każdej funkcjonalności uwzględniono również logikę procesu biznesowego, która jest przez daną funkcjonalność wspierana.

Każdy ze *Scenariuszy testowych* został zaakceptowany w uzgodnionym kształcie przez Głównego Użytkownika (Ministerstwo Rozwoju Regionalnego) oraz przez Głównego Dostawcę (Ministerstwo Finansów). Wymagania zawarte w *Scenariuszach testowych* są przedmiotem szczegółowych testów i dopiero po pomyślnym ich przejściu następuje formalny odbiór danej części systemu.

W dniu 24.06.2008 r. Rada Projektu ostatecznie zaakceptowała wdrożenie III grupy funkcjonalności KSI SIMI, jednakże do dnia 26.06.2008 r. tj. dnia zakończenia prac

audytowych i przekazania wstępnej wersji sprawozdania nie przeprowadzono wdrożenia trzeciej grupy funkcjonalności, zawierającej m.in. moduły do obsługi Deklaracji wydatków, Rejestru kwot wycofanych, Rejestru obciążeń na projekcie

Zgodnie z ustaleniami przyjętymi na Radzie Projektu, między MRR (Główny Użytkownik) a MF (Główny Dostawca) środowisko produkcyjne miało zostać uruchomione po przygotowaniu przez Głównego Dostawcę – wspólnie z Wykonawcą tj. firmą Comarch odpowiednio skonfigurowanego oprogramowania, po instalacji którego prowadzane są m.in. standardowe testy oraz weryfikowana jest zgodność i spójność poszczególnych środowisk systemu.

Ostatecznie wdrożenie III grupy funkcjonalności na środowisku produkcyjnym systemu KSI SIMIK 07-13 nastąpiło w dniu 7.07.2008 r. co zostało potwierdzone podczas spotkania w dn. 18.07.2008 r.

4.1.2 Kontrola i audyt w aplikacji

Ze względu na dużą ilość podmiotów wprowadzających dane do systemu oraz przewidywaną dużą liczbę użytkowników KSI SIMIK 07-13 w poszczególnych Instytucjach zdecydowano, iż w systemie zostaną wbudowane mechanizmy kontrolne, służące walidacji i kontroli poprawności wprowadzanych danych. Dodatkowo dla każdej funkcjonalności powinna być dostępna historia zmian, obejmująca następujące informacje:

- kto dokonał zmiany;
- kiedy zmiana została dokonana;
- jakie pole podlegało zmianie;
- stara wartość pola;
- nowa wartość pola.

Wszystkie stosowane mechanizmy kontrolne w aplikacji zostały zapisane w *Specyfikacjach przypadków użycia* – dokumentach, na podstawie których opracowano poszczególne funkcjonalności i wygląd formatek. Szczegółowe informacje dotyczące tego zakresu zostały zawarte w części *7.1 Kontrola w aplikacjach* niniejszego *Sprawozdania*.

Ponadto w systemie zawarto również kontrole wspierające procesy biznesowe. Przykładowo w poprzednim okresie programowania dużym problemem było terminowe rozpatrywanie wniosków aplikacyjnych i szybkie zawieranie na ich podstawie umów o płatność z beneficjentami, co skutkowało opóźnieniami w alokacji środków finansowych. Dlatego podczas projektowania systemu KSI zdecydowano, iż zostaną w nim zawarte informacje pozwalające zweryfikować terminowość rozpatrywania aplikacji beneficjentów oraz dające informacje Instytucji Zarządzającej o stanie tego procesu. Przykładem takich informacji są np. data przyjęcia wniosku, data podpisania umowy o płatność – pola wymagalne, bez podania których system nie pozwoli zapisać danych.

4.1.3 Bezpieczeństwo i dostępność aplikacji

Podstawowe wymogi i ogólne założenia dotyczące bezpieczeństwa i dostępności systemu KSI SIMIK 07-13 zostały sprecyzowane już na etapie ustalania struktury projektowej, w dokumencie *Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013 (SIMIK 07-13) – Założenia*

projektu. Szczegółowe wymagania dotyczące tego obszaru zostały zawarte w *Specyfikacjach przypadków użycia – Specyfikacji niefunkcjonalnej*.

Zgodnie z zapisami tego dokumentu system powinien być w pełni kompatybilny z najbardziej rozpowszechnionymi przeglądarkami internetowymi (*Internet Explorer* w wersji 5.5 lub wyższej, *Mozilla Firefox* w wersji 2.0 lub wyższej). System powinien być dostępny dla użytkowników przez 7 dni w tygodniu, w godzinach 6-24. Docelowo system powinien obsługiwać do 1000 użytkowników jednocześnie.

System powinien być dostępny w trzech konfiguracjach:

- testowej, zawierającej środowisko testowe nowych funkcjonalności dla administratorów;
- testowo-produkcyjnej, zawierającej środowisko testowe dla użytkowników systemu;
- produkcyjnej, zawierającej środowisko właściwej pracy użytkowników.

Dostęp do systemu SIMIK uzyskuje się za pomocą szyfrowanego połączenia poprzez protokół HTTPS. Dostęp posiadają wyłącznie uwierzytelnieni użytkownicy za pomocą unikalnego loginu skojarzonego z hasłem. Użytkownik ma dostęp tylko do ściśle określonych funkcji systemu, zgodnie z przyznanymi jego profilowi uprawnieniami. Autoryzacja użytkownika następuje po pomyślnym zakończeniu procesu logowania.

Szczegółowe wymagania dotyczące monitorowania wydajności i dostępności systemu KSI SIMIK zostały opisane w części 5.*3. Zarządzanie pojemnością i wydajnością* niniejszego *Sprawozdania*.

4.1.4 Konfiguracja i implementowanie nabytego oprogramowania aplikacyjnego

Wdrożeniem oprogramowania KSI SIMIK 07-13 oraz bieżącą jego konfiguracją i utrzymaniem zajmują się wyznaczeni pracownicy Departamentu Rozwoju Systemów Informatycznych Ministerstwa Finansów.

Aby właściwie zarządzać konfiguracją podczas wdrażania systemu, zgodnie z metodologią *Rational Unified Process* przygotowano *Plan zarządzania konfiguracją*. Celem tego dokumentu jest określenie wszelkich działalności i kroków, jakie muszą być podjęte w trakcie prowadzenia projektu, aby skutecznie zarządzać konfiguracją. Zgodnie z zapisami tego dokumentu kierownik zarządzania konfiguracją określa środowisko, w którym prowadzony jest projekt i ustala politykę zarządzania konfiguracją, definiuje punkty kontrolne i tworzy raport o stanie projektu.

Zarządzanie konfiguracją i zmianami w systemie KSI SIMIK 07-13 odbywa się przy pomocy zautomatyzowanych narzędzi – oprogramowania *ClearQuest* oraz repozytorium *ClearCase*. Szczegółowy opis tych narzędzi i systemu zarządzania konfiguracją i zmianami został zawarty w dalszej części *Sprawozdania*.

4.1.5 Znaczące poprawki do istniejących systemów

W celu skutecznego zarządzania zmianami w systemie KSI SIMIK 07-13 opracowano *Plan zarządzania zmianami*, stanowiący załącznik do dokumentu inicjującego projekt *Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013*. W dokumencie tym ustalono zasady

gromadzenia, rejestrowania oraz nadzorowania zgłoszonych i wprowadzanych zmian we wszystkich produktach projektowych. Uczestnikami procesu implementacji zmian są zarówno Główny Dostawca (Ministerstwo Finansów) oraz Wykonawca Systemu (ComArch S.A.), jak i Główny Użytkownik (Ministerstwo Rozwoju Regionalnego).

Zgodnie z zapisami tego dokumentu wszystkie zmiany implementowane w systemie KSI SIMIK 07-13 muszą przejść formalną ścieżkę zgłaszania, rozpatrywania, opracowania rozwiązania oraz szczegółowego testowania i akceptacji proponowanych zmian w systemie. Dopiero po przejściu tego procesu i uzyskaniu akceptacji zarówno ze strony Głównego Dostawcy, jak i Głównego Użytkownika, zmiany są implementowane na środowisko produkcyjne.

Znaczące poprawki do systemu przechodzą również tą samą ścieżkę postępowania.

4.1.6 Rozwój oprogramowania aplikacyjnego

Rozwój oprogramowania, zgodnie z przyjętą strukturą projektową, opiera się o *Specyfikacje przypadków użycia*. Specyfikacje te zawierają opisy wszystkich funkcjonalności systemu KSI SIMIK 07-13 i zostały zaakceptowane; od strony technicznej przez Ministerstwo Finansów oraz od strony merytorycznej przez pracowników Ministerstwa Rozwoju Regionalnego.

Na podstawie tych zatwierdzonych funkcjonalności pracownicy Wykonawcy tworzą kody programu. Dostarczone wersje aplikacji są szczegółowo testowane w oparciu o scenariusze testowe a następnie implementowane.

Rozwój oprogramowania aplikacyjnego KSI SIMIK 07-13 oraz całego systemu jest przedmiotem umowy z dostawcą zewnętrznym, w której szczegółowo zdefiniowano wymogi dotyczące rozwoju oprogramowania systemu KSI SIMIK 07-13. Zagadnienia związane z umową na wykonanie Krajowego Systemu Informatycznego zostały szerzej opisane w rozdziałach *5.1. Zdefiniowanie i Zarządzanie Poziomem Usług* oraz *5.2. Zarządzanie Usługami Stron Trzecich*.

4.1.7 Zarządzanie wymaganiami aplikacyjnymi

Zarządzanie wymaganiami aplikacyjnymi odbywa się zgodnie z przyjęta strukturą projektową i zostało szczegółowo opisane w rozdziale *4.4. Zarządzanie zmianami* niniejszego *Sprawozdania*.

4.1.8 Utrzymanie oprogramowania aplikacyjnego

Formalne wytyczne dotyczące obsługi procesu utrzymania oprogramowania aplikacyjnego systemu KSI SIMIK 07-13 zostały opisane w punktach 4.1.1 – 4.1.7 niniejszego *Sprawozdania*.

W systemie KSI SIMIK nie istnieje odrębny dokument zawierający plan utrzymania oprogramowania aplikacyjnego, zasady i regulacje dotyczące tego zakresu zostały zawarte w procedurach zarządzania konfiguracją oraz zarządzania zmianą w systemie KSI SIMIK 07-13.

4.2. Rozwój i Utrzymanie Infrastruktury Technologicznej

4.2.1 Ochrona i dostępność zasobów infrastrukturalnych

Zasady konfiguracji oprogramowania na serwerach zostały opisane w rozdziale *4.3.1. Planowanie rozwiązań funkcjonalnych*. Po zainstalowaniu serwera dokonywany jest przegląd jego bieżących ustawień oraz wykonywane są zmiany zgodnie z zaleceniami z dokumentu *Hardering serwerów Windows 2003*, dostarczonego pracownikom MF przez firmę ComArch. Nie został on jednakże formalnie zatwierdzony przez kierownictwo departamentu zajmującego się obsługą systemu KSI. Zawiera on następujące elementy:

- Specyfikacja środowiska – serwery MS Windows 2003 Enterprise Edition;
- Plan działania;
- Wykonanie
  - Instalacja Service Packa 2;
  - Instalacja pozostałych hotfixów;
  - Wyłączenie nieużywanych usług;
  - Konfiguracja połączenia sieciowego;
  - Ustawienia zabezpieczeń lokalnych;
  - Konfiguracja Aktualizacji Automatycznych;
  - Zabezpieczenia IIS.

Hardening jest to proces zabezpieczenia serwerów pod kątem systemu operacyjnego i roli serwera aplikacji. Wykonywany jest na podstawie zaleceń firmy Microsoft oraz „Centre for Internet Security" (w uproszczonej formie). Konfiguracji i zabezpieczania serwerów dokują jedynie administratorzy systemu KSI zatrudnieni w Ministerstwie Finansów. Aktualizacje są wgrywane ręcznie. Administrator pobiera odpowiednie pliki ze strony producenta oprogramowania, po czym instaluje je na poszczególnych maszynach. Brak jest jednakże formalnie określonej odpowiedzialności za wykonywanie procesu zabezpieczania i aktualizacji oprogramowania.

Rekomendacja 4. Zakup i Wdrożenie – Ochrona i dostępność zasobów infrastrukturalnych

Zgodnie z otrzymanymi informacjami na serwerach nie jest instalowane żadne dodatkowe oprogramowanie, poza oprogramowaniem niezbędnym do spełniania roli przeznaczonej dla danego serwera.

W celu instalacji oprogramowania i zabezpieczania sprzętu używane są konta imienne administratorów, nie są natomiast wykorzystywane wbudowane systemowe konta „administrator/root". Hasła kont administracyjnych, zgodnie z *Procedurą zmiany i przechowywania haseł administracyjnych*, przechowywane są w zamkniętych kopertach w sejfie. Zmiana haseł administratora następuje nie rzadziej niż co 60 dni oraz każdorazowo po ujawnieniu hasła. Hasło powinno składać się z przynajmniej 8 znaków oraz powinno zawierać co najmniej jedną dużą literę, małe litery, co najmniej jedną cyfrę oraz co najmniej jeden znak specjalny. Hasło może być udostępnione wyłącznie za zgodą AI lub kierownika Projektu (lub jego zastępcy) lub osoby przez upoważnionej przez AI. Przypadki udostępnienia

haseł należy dokumentować w ewidencji (ewidencja powinna być przechowywana razem z kopertami w sejfie).

Zasady dostępu do serwerowni, w której znajdują się kluczowe elementy infrastruktury, zostały opisane w rozdziale *5.9. Zarządzanie Środowiskiem Fizycznym*.

4.2.2 Utrzymanie infrastruktury

Procedura zarządzania rozwojem w systemie KSI SIMIK 07-13 określa proces rozwoju systemu. Jej celem jest zdefiniowanie zasad monitoringu, kontroli i zarządzania wydajnością usług systemu, co ma pozwolić na zapewnienie założonego poziomu pojemności i wydajności systemu oraz ewolucję systemu zgodnie z potrzebami.

Zgodnie z tymi zapisami Zespół Infrastruktury Technicznej analizuje popyt na dostęp do systemu, tzn. ilość użytkowników systemu, ilość użytkowników pracujących jednocześnie, co ma wpływ na wydajność systemu. Rezultatem tego monitorowania jest sporządzenie raz w miesiącu *Raportu monitorowania obciążenia systemu KSI SIMIK 07-13*. Raport ten przedstawia informację z jednego pełnego tygodnia pracy systemu w zakresie logowania do systemu ze szczególnym uwzględnieniem czasów zwiększonego natężenia działań użytkowników. Powstaje on na podstawie logów systemu KSI SIMIK, dających informację o czasie operacji związanych z logowaniem się użytkowników do systemu.

Procedura zarządzania rozwojem w systemie KSI SIMIK 07-13 omawia ponadto zagadnienia monitorowania wydajności zasobów systemu (opisane szerzej w rozdziale *5.3. Zarządzanie Wydajnością i Pojemnością*).

Zgodnie z otrzymanymi informacjami ewentualne zmiany (w tym również awaryjne) będą wykonywane zgodnie z obowiązującymi procedurami zarządzania zmianami.

Obecnie jest realizowany zakup sprzętu na potrzeby systemu KSI. W dokumencie *Opis przedmiotu zamówienia SIMIK07-13* zostały określone elementy infrastruktury, które należy zakupić w celu prawidłowego funkcjonowania systemu SIMIK. Rozbudowa ta jest związana przede wszystkim z zapewnieniem backupu danych oraz z zakupem odpowiedniego oprogramowania wraz z licencjami. Ważnym czynnikiem jest też zapewnienie odpowiedniego poziomu dostępności systemu. Ze względu na skomplikowane procedury przetargowe związane z zakupem sprzętu, oprogramowania oraz z przeprowadzeniem szkoleń przewiduje się termin realizacji zamówień na dzień 31 października 2008 r.

4.3. Umożliwienie Funkcjonowania i Użytkowania

4.3.1 Planowanie rozwiązań funkcjonalnych

W celu użycia i wykorzystywania rozwiązań funkcjonalnych i technicznych został opracowany szereg procedur.

W odniesieniu do kwestii administracyjnych są to:

- *Dokumentacja administracyjna systemu SIMIK 07-13* (w Ministerstwie Finansów);
- *Procedury wewnętrzne w Wydziale Administracji i Audytu Systemów Informatycznych* (w Ministerstwie Rozwoju Regionalnego).

Dokumentacja administracyjna systemu SIMIK 07-13 opisuje następujące zagadnienia:

- Instalacja i konfiguracja serwera aplikacyjnego;
  - Instalacja aplikacji SIMIK 07-13;
  - Instalacja serwera IIS;
  - Instalacja pakietu uruchomieniowego Microsoft .NET Framework 2.0;
  - Instalacja Microsoft ASP.NET AJAX Extentions 1.0;
  - Instalacja ODAC;
  - Konfiguracja IIS na potrzeby aplikacji SIMIK 07-13;
  - Potwierdzenie poprawnego zainstalowania aplikacji;
  - Konfiguracja protokołu https;
- Instalacja bazy danych;
  - Instalacja serwera bazy danych oraz utworzenie bazy danych;
  - Utworzenie konfiguracji Primary – Standby;
  - Podstawowe operacje na serwerze Standby;
  - Przełączanie ról serwerów bazodanowych;
- Backup i odtwarzanie bazy danych.

Procedury wewnętrzne w Wydziale Administracji i Audytu Systemów Informatycznych opisują następujące kwestie:

- Podstawowa procedura obsługi zadań w Wydziale;
- Oracle Discoverer Plus – projektowanie raportów;
- Organizowanie szkoleń/spotkań/konferencji/itp.;
- Prowadzenie szkoleń;
- Lokalne Systemy Informatyczne (LSI);
- Obsługa zgłoszeń dotyczących problemów obsługowych, merytorycznych, technicznych oraz zleceń zmian;
- Obsługa zgłoszeń dotyczących incydentów naruszenia bezpieczeństwa informacji;
- Polityka bezpieczeństwa – prowadzenie szkoleń;
- Polityka bezpieczeństwa – monitorowanie szkoleń prowadzonych przez Administratorów Merytorycznych;
- SFC2007 - pełnienie funkcji MS Liaison, tj. koordynacja dostępu do systemu wśród Użytkowników krajowych;

- Opracowywanie i aktualizowanie dokumentacji dla Użytkownika KSI (SIMIK 07-13) lub procedur wewnętrznych Wydziału III lub procedur, zaleceń i wytycznych dla odbiorców zewnętrznych;
- Aktualizacja słowników KSI SIMIK 07-13;
- Aktualizacja XML Schema – informowanie właścicieli LSI;
- Audyt jakości danych w KSI SIMIK 07-13;
- Aktualizacja danych dotyczących Administratorów Merytorycznych;
- Aktualizacja danych dotyczących Użytkowników w Clear Quest;
- Nadawanie uprawnień Użytkownikowi KSI SIMIK 07-13 w bazie produkcyjnej i szkoleniowej;
- Nadanie/zmiana uprawnień Użytkownikowi w bazie szkoleniowej (bez „Wniosku o nadanie/zmianę uprawnień do Krajowego Systemu Informatycznego (SIMIK 07-13)";
- Nadawanie uprawnień AM IK NSRO w bazie produkcyjnej i szkoleniowej;
- Nadanie/zmiana/wygaśnięcie uprawnień Użytkownika KSI SIMIK 07-13 w Oracle Discoverer Plus;
- Zmiana uprawnień Użytkownikowi KSI SIMIK 07-13 w bazie produkcyjnej i szkoleniowej;
- Zmiana uprawnień AM IK NSRO w bazie produkcyjnej i szkoleniowej;
- Zmiana hasła Użytkownikowi przez AM IK NSRO (procedura obowiązuje w przypadku tymczasowego braku działania funkcjonalności „Przypomnienie hasła");
- Wygaśnięcie uprawnień Użytkownika KSI SIMIK 07-13 – zablokowanie konta w bazie produkcyjnej i szkoleniowej (zwykła procedura);
- Wygaśnięcie uprawnień AM IK NSRO – zablokowanie konta w bazie produkcyjnej i szkoleniowej (zwykła procedura);
- Natychmiastowe blokowanie konta Użytkownika ze względów bezpieczeństwa;
- Odblokowywanie konta Użytkownika KSI SIMIK 07-13 w bazie produkcyjnej i szkoleniowej;
- Nadanie/zmiana/wycofanie uprawnień Użytkownikowi w bazie testowej;
- Przygotowywanie wzorów wniosków o nadanie/zmianę uprawnień do KSI SIMIK 07-13;
- Archiwizacja danych na temat nadanych uprawnień;
- Przeprowadzanie okresowych przeglądów kont Użytkowników w bazie produkcyjnej i szkoleniowej;
- Aktualizowanie informacji zamieszczanych na stronach internetowych MRR w zakresie dotyczącym KSI SIMIK 07-13.

Została opracowana również *Instrukcja użytkownika Krajowego Systemu Informatycznego SIMIK 2007-2013*. Zawiera ona informacje przeznaczone dla każdego użytkownika systemu:

- Bezpieczeństwo;
  - Uczestnicy Polityki Bezpieczeństwa;
  - Polityka Bezpieczeństwa – Procedury udostępnione Użytkownikom;
  - Polityka Bezpieczeństwa – podstawowy schemat przepływu informacji w sytuacji naruszenia bezpieczeństwa informacji;
- Service Desk;
  - Service desk – elementy docelowe;
  - Service desk – procedury;

  - Service desk – zadania uczestników;
  - Service desk – Clear Quest;
  - Service desk – Baza wiedzy;
  - Service desk – Główne rodzaje zgłoszeń realizowanych w Service Desk;
  - Service desk – Podstawowy schemat przepływu informacji w Service Desk (po zakończeniu wdrożenia „Bazy wiedzy" oraz „ClearQuest");
- Start / pierwsze kroki;
  - Pierwsze logowanie do aplikacji;
  - Następne logowania do aplikacji;
  - Wybór profilu użytkownika;
  - Menu;
- Wnioski o dofinansowanie;
  - Rejestracja danych dotyczących wniosku o dofinansowanie;
  - Edycja danych dotyczących wniosku o dofinansowanie;
  - Zarządzanie danymi dotyczącymi wniosków o dofinansowanie;
- Duże projekty;
  - Rejestracja danych dotyczących wniosków o dofinansowanie dużych projektów;
  - Edycja danych dotyczących wniosków o dofinansowanie dużych projektów;
  - Zarządzanie danymi dotyczącymi wniosków o dofinansowanie dużych projektów;
- Umowy o dofinansowanie / decyzje;
  - Rejestracja danych dotyczących umowy o dofinansowanie / decyzji;
  - Rejestracja zmian do umowy o dofinansowanie / decyzji;
  - Edycja danych dotyczących umowy o dofinansowanie / decyzji;
  - Edytowanie wcześniejszych wersji umowy / decyzji;
  - Zarządzanie danymi dotyczącymi umów o dofinansowanie / decyzji;
- Wnioski o płatność;
  - Rejestracja danych dotyczących wniosku o płatność;
  - Edycja danych dotyczących wniosków o płatność;
  - Zarządzanie danymi dotyczącymi wniosków o płatność;
- Kontrole;
  - Rejestracja informacji o przeprowadzonej kontroli projektu;
  - Edycja danych dotyczących kontroli;
  - Zarządzanie danymi dotyczącymi kontroli;
- Programy operacyjne;
  - Informacja o Narodowych Strategicznych Ramach Odniesienia;
  - Informacja o Programie Operacyjnym;
  - Wprowadzanie i edycja danych dotyczących Informacji o PO;
- Oracle Discoverer;
- Prognozy wydatków;
  - Prognozy wydatków na podstawie danych z umów/decyzji o dofinansowanie oraz wniosków o płatność;
  - Prognozy wydatków w oparciu o szacunki instytucji;
  - Rejestracja danych dotyczących prognozy wydatków w oparciu o szacunki instytucji;
- Rejestr obciążeń na projekcie;
  - Wprowadzenie danych dotyczących obciążeń na projekcie;

- Walidacja i zapisanie danych.

Opisane powyżej dokumenty nie zawierają zapisów dotyczących odpowiedzialności za przeglądy i aktualizację treści procedur w przypadku nanoszenia zmian lub powstawania nowych systemów oraz częstotliwości wykonywania tego procesu.

Rekomendacja 5. Zakup i Wdrożenie – Planowanie rozwiązań funkcjonalnych

4.3.2 Transfer wiedzy do użytkowników końcowych

Ministerstwo Rozwoju Regionalnego z zakresu obsługi aplikacji KSI organizuje szkolenia dla Administratorów Merytorycznych z poszczególnych Instytucji Zarządzających. Następnie osoby te powinny przeszkolić pracowników swoich instytucji. W MRR prowadzony jest rejestr szkoleń w pliku arkusza kalkulacyjnego „Baza przeszkolonych użytkowników KSI SIMIK07-13.xls". Zgodnie z tym wykazem przeprowadzone były następujące szkolenia dla użytkowników:

- Spotkanie przedstawicieli Ministerstwa Rozwoju Regionalnego oraz użytkowników systemu SIMIK dotyczące wdrożenia I grupy funkcjonalności SIMIK 2007-13 – 326 osób;
- Obsługa narzędzia ORACLE DISCOVERER – 297 osób;
- Spotkanie Administratorów Merytorycznych IZ, wdrożenie II grupy funkcjonalności KSI SIMIK 07-13. Polityka bezpieczeństwa oraz procedury service desk – 35 osób;
- Instruktaż – Spotkanie Administratorów Merytorycznych IZ RPO, wdrożenie II grupy funkcjonalności, informacje o Programach Operacyjnych, Prognozy Wydatków – 24 osoby;
- Konferencja nt. „Zarządzanie zmianą w systemie KSI SIMIK 07-13" – 36 osób.

W rejestrze zawarte są na temat każdego z użytkowników takie informacje jak; login, imię i nazwisko, nazwa Instytucji, rola Instytucji, e-mail użytkownika, data szkolenia, temat szkolenia, miejsce szkolenia, uwagi.

Nie został jednakże opracowany formalny model procesu szkoleń dla pracowników. Szkolenia odbywają się jedynie po zgłoszeniu przez poszczególne instytucje oraz po wdrażaniu kolejnych grup funkcjonalności. Nie jest również weryfikowane, czy wszyscy pracownicy obsługujący system KSI zostali przeszkoleni.

Rekomendacja 6. Zakup i Wdrożenie – Transfer wiedzy do użytkowników końcowych

Uczestnicy szkoleń wypełniali ankiety oceniające szkolenia. Szkolenie nie kończy się żadnym testem praktycznym z umiejętności użycia systemu. Podczas szkoleń jest przekazywana również wiedza o istnieniu i sposobie kontaktowania się z Service-Deskiem mającym zapewnić wsparcie techniczne oraz Administratorami Merytorycznymi.

4.3.3 Transfer wiedzy do personelu wsparcia

Personel wsparcia technicznego (administratorzy) odbywają szkolenia z zakresu obsługi sprzętu w momencie dostawy tego sprzętu. Wymóg przeszkolenia pracowników jest zapisywany w umowach zawieranych z dostawcą.

Zasady działania wsparcia technicznego zostały opisane w dokumencie *Service Desk dla Krajowego Systemu Informatycznego SIMIK 07-13. Z*ostały w nim przedstawione zasady działania i sposób zorganizowania Service Desk składającego się z HelpDesku i Pomocy Technicznej. W szczególności dokument ten ma na celu opracowanie procesów, kluczowych ról, świadczonych usług oraz procedur w Service Desk dla KSI SIMIK 07-13. Obejmuje on takie zagadnienia jak:

- Zgłoszenie problemu merytorycznego/obsługowego/zmiany;
  - Role i zadania użytkownika;
  - Role i zadania Administratora Merytorycznego w Instytucji (pierwszy poziom wsparcia merytorycznego/obsługowego/opracowania zmiany dla użytkowników w Instytucji);
  - Role i zadania Administratora Merytorycznego w IZ (pierwszy poziom wsparcia merytorycznego/obsługowego/opracowania zmiany dla Użytkowników w IZ);
  - Role i zadania Administratora Merytorycznego w IK NSRO – Zespół Analityczny w MRR (pierwszy poziom wsparcia merytorycznego/obsługowego/opracowania zmiany dla Użytkowników w IK NSRO oraz pierwszy poziom wsparcia w opracowaniu zgłoszenia zmiany);
  - Role i zadania Koordynatora SIMIK;
  - Role i zadania Zespołu Projektowo-Technicznego MF (pierwszy poziom rozwiązania problemu merytorycznego oraz drugi poziom wsparcia w opracowaniu zgłoszenia zmiany);
  - Role i zadania Wykonawcy oprogramowania (drugi poziom rozwiązania problemu merytorycznego oraz realizacja zmiany);
  - Ścieżka obsługi (przepływu) zgłoszeń dot. problemu merytorycznego/ obsługowego/ zmiany;
- Zgłoszenie problemu technicznego;
  - Role i zadania użytkownika;
  - Role i zadania Koordynatora SIMIK (pierwszy poziom wsparcia technicznego);
  - Role i zadania Administratora Merytorycznego;
  - Role i zadania Służb informatycznych Instytucji użytkownika (drugi poziom wsparcia technicznego);
  - Role i zadania Zespołu Projektowo-Technicznego MF (rozwiązanie problemu technicznego);
  - Ścieżka obsługi (przepływu) zgłoszeń dot. problemu technicznego;
- Zgłoszenie incydentu dotyczącego bezpieczeństwa;
  - Role i zadania użytkownika;
  - Role i zadania Koordynatora SIMIK (pierwszy poziom obsługi incydentu);
  - Role i zadania Administratora Merytorycznego;
  - Role i zadania Służb informatycznych Instytucji użytkownika;
  - Role i zadania Administratora Bezpieczeństwa Informacji;
  - Role i zadania Administratora Technicznego;
  - Role i zadania Administratora Informacji;

  - Role i zadania Zespołu Kryzysowego;
  - Ścieżka obsługi (przepływu) zgłoszeń dot. incydentu dotyczącego naruszenia bezpieczeństwa informacji;
- Zakres usługi Service Desk;
- Rodzaje i obsługa zgłoszeń;
- Baza wiedzy;
- Aplikacja Clear Quest.

4.4. Zarządzanie Zmianami

4.4.1 Standardy i procedury zarządzania zmianami

Podstawowym dokumentem wyznaczającym proces zarządzania zmianami jest *Plan zarządzania zmianami dla Systemu Informatycznego SIMIK 07-13.* Celem tego dokumentu jest określenie wszelkich działalności i kroków, jakie muszą być podjęte w trakcie prowadzenia projektu, aby skutecznie zarządzać zmianą. Dokument ten i zawarte w nim procedury opisują:

- jak będą obsługiwane zmiany w projekcie;
- metody sprawowania nadzoru nad zmianami;
- zasady zarządzania zmianami.

Proces zarządzania zmianami jest wspomagany przez narzędzia i mechanizmy:

- *Repozytorium CC* – repozytorium ClearCase – przechowujące wszystkie informacje związane z projektem, w tym wszystkie obowiązujące przypadki użycia. Repozytorium CC służy również do wersjonowania aplikacji.
- *Narzędzie CQ* – narzędzie informatyczne ClearQuest – przechowujące wszystkie zgłoszenia, wspomagające proces obsługi procesu zarządzania zgłoszeniem. Docelowo obsługiwać będzie również zlecenia i defekty, czyli wszystkie żądania zmiany. Narzędzie to również może śledzić status zmiany.
- *Rejestr Jakości Projektu SIMIK 07-13* – baza informacji z kontroli jakości produktu zawierająca szczegółowe informacje na temat kontrolowanego produktu, metody kontroli jakości, osoby odpowiedzialnej za przeprowadzenie kontroli, planowanej i faktycznej daty przeprowadzenia kontroli, podjętego działania, wyniku kontroli wraz ze szczegółowym raportem z testów, planowanej i faktycznej dacie akceptacji produktu. Narzędzie wspiera arkusz „Realizacja testów danej Grupy Funkcjonalności" – zawierający szczegółowe informacje odnośnie przebiegu procesu testowania (która ze stron Główny Dostawca czy Użytkownik testuje dany produkt, czy produkt jest w trakcie nanoszenia poprawek przez Głównego Wykonawcę). Za prawidłowe prowadzenie rejestru jest odpowiedzialny administrator merytoryczny MF. Narzędzie to umożliwia śledzenie statusu zmiany.
- *Zlecenia usług developerskich* – zbiór dokumentacji zlecanych Głównemu Wykonawcy przez Głównego Dostawcę usług developerskich zgodnie z *Procedurą realizacji zleceń na usługi developerskie w ramach umowy z ComArch S.A.*" Dokumentacja ta zawiera, w podziale na konkretne produkty bądź zlecenia zmiany, zlecenie zmiany, a w nim m.in. harmonogram realizacje usługi, karty wymagań, wycenę oprogramowania w PF oraz dokumentację techniczną wraz z dokumentacją odbioru zlecenia, w tym raport z testów. Zbiór wykorzystywany jest w trakcie prac nad zleceniem i dokumentuje wszystkie przeprowadzone prace w ramach zlecenia.
- *Wersje podpisane* przypadki użycia [ang. Use Case] *(UC SIMIK 07-13)* – katalog wszystkich zaakceptowanych przez Głównego Użytkownika i Dostawcę wersji przypadków użycia specyfikujące wymagania Głównego Użytkownika. Zbiór podzielony został na Grupy Funkcjonalności i konkretne moduły systemu

KSI SIMIK 07-13. Zbiór utrzymywany jest w formie elektronicznej i papierowej.

Plan zarządzania zmianami nie zawiera informacji dotyczących konieczności opracowywania procedury odtworzenia systemu w przypadku instalacji wadliwego oprogramowania.

Plan ten nie posiada procedur dotyczących zarządzania zmianą procedur, procesami biznesowymi, usługami, zmianami w systemie jak również platformą sprzętową.

Rekomendacja 7. Zakup i Wdrożenie – Standardy i procedury zarządzania zmianami

Plan zarządzania zmianami definiuje role poszczególnych użytkowników, jak również ich odpowiedzialność dotyczącą pracy w systemie.

Procedura zarządzania zmianami od rejestracji problemu w aplikacji Clear Quest do zamknięcia problemu wraz z opisaniem ścieżki audytowej oraz współpraca z firmami zewnętrznymi została opisana w *Rozdziale 5.7.1 Identyfikacja i Klasyfikacja Problemów*.

4.4.2 Ocena wpływu, priorytetyzacja i autoryzacja

Wszystkie zgłoszenia dotyczące zarządzania zmianą są skatalogowane wg kategorii ważności dla systemu i jego funkcjonalności:

- Zgłoszenie – służy do rejestrowania i analizy problemów związanych z systemem KSI SIMIK 07-13;
- Zlecenie – służy do zdefiniowania zlecenia pracy dla Wykonawcy, przekazania tego zlecenia do wykonania, a następnie odnotowania wyniku testów oprogramowania dostarczonego w ramach tego Zlecenia.

Procedury planu zarządzania zmianami kategoryzują zmiany na odpowiednie grupy (problemy merytoryczne, problemy obsługowe, opracowanie zmiany, zgłoszenie dotyczącego incydentu naruszenia bezpieczeństwa) wraz z nadaniem im priorytetu.

Plan zarządzania zmianami nie definiuje wysokości priorytetu jaki może zostać nadany zdarzeniu, jednakże aplikacja, wykorzystywana do obsługi zmian, umożliwia nadanie zgłoszonym zdarzeniom przypisania błędowi trzech wartości tj. błąd błahy, błąd istotny, błąd krytyczny. W trakcie prac audytowych ustalono, że osoba zgłaszająca nadaje priorytet zdarzeniu, który następnie jest weryfikowany przez administratora merytorycznego.

Wszystkie zdarzenia, zarówno żądanie obsługi błędu, jak również zgłoszenia zmiany są oceniane i akceptowane przez Głównego Użytkownika, przy czym błędy są usuwane przez twórcę oprogramowania w ramach gwarancji natomiast zgłoszenia zmiany są szczegółowo analizowane przez Głównego Dostawcę - MF, a następnie po dokonaniu wyceny są akceptowane lub odrzucane przez Głównego Użytkownika – MRR. Wszystkie zgłoszenia zmian jak również żądania usunięcia błędów są również analizowane pod kątem bezpieczeństwa systemu, wymaganiami prawnymi i kontraktowymi.

4.4.3 Zmiany awaryjne

Zmiany awaryjne stanowią jeden z punktów dokumentu *Plan zarządzania zmianami dla Systemu Informatycznego SIMIK 07-13*.

W przypadku zgłoszenia zmian o charakterze krytycznym dla działania systemu dopuszcza się uruchomienie procesu zarządzania zmianami awaryjnymi, które nie są prowadzone w sposób określony *Procedurami zarządzania wymaganiami* – punkt *3.4 Awaryjne żądanie zmiany* ww. *Planu* określa ścieżkę postępowania.

4.4.4 Śledzenie statusu zmian i raportowanie

Wdrożone narzędzia informatyczne obsługujące bazę danych zgłoszeń błędów wspomagające proces zarządzania zmianami umożliwiają generowanie raportów, zestawień o stanie realizacji żądania zmiany czy defektu oraz sporządzanie statystyk na podstawie danych zgromadzonych w tychże bazach. Narzędzia te umożliwiają monitorowanie wpływu zarządzania zmianą na system i świadczone przez Głównego Wykonawcę i Dostawcę usługi.

Aplikacja wspierająca ClearQuest umożliwia śledzenie statusu zmian zarówno dla zgłoszenia błędu jak również dla zgłoszenia zmiany.

Aplikacja umożliwia również generowanie raportów dot. statusu obsługiwanych zgłoszeń. *Plan zarządzania zmianami* nie posiada procedury definiującej konieczność tworzenia i sprawdzania raportów z obsługi zdarzeń, jednakże w trakcie prac audytowych stwierdzono, że pracownicy wykonują sprawdzenia statusów obsługi zgłoszeń.

4.4.5 Zakończenie wprowadzania zmiany i dokumentowanie

Plan zarządzania zmianami dla Systemu Informatycznego SIMIK 07-13 definiuje strukturę katalogową służącą do utrzymywania wszystkich zaakceptowanych przez Głównego Użytkownika i Dostawcę wersji zmian – zgodnie z przypadkami użycia specyfikujących wymagania Głównego Użytkownika. Zbiór został podzielony na Grupy Funkcjonalności i konkretne moduły systemu KSI SIMIK 07-13. Zbiór utrzymywany jest również w formie papierowej.

Na podstawie przekazanych informacji ustalono, że istnieje i jest wdrożony podproces ewidencjonowania zakończenia zmiany i obsługi błędu. Przy zakończeniu zamknięciu problemu następuje aktualizacja dokumentacji. Za aktualizację dokumentacji użytkownika odpowiada MRR.

4.5. Wprowadzenie i Przypisywanie Rozwiązań i Zmian

4.5.1 Plan testów

Podstawowym dokumentem określającym wprowadzenie i przypisywanie testów w KSI SIMIK jest *Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13*. Dokument ten definiuje proces testowania oprogramowania, określa sposób przeprowadzenia testów wstępnych i akceptacyjnych oprogramowania, definiuje użytkowników biorących udział w procesie testowania produktu oraz przydziela im określone role i odpowiedzialność. *Plan* zawiera opis środowiska testowego oraz spis wymaganej dokumentacji.

Celem realizacji testów jest weryfikacja i walidacja funkcjonalności dostarczonego Oprogramowania na zgodność z wymaganiami Głównego Użytkownika. Pozytywne wyniki testów stanowią podstawę akceptacji Oprogramowania przez Głównego Użytkownika. Wykonawca oprogramowania po wykonaniu prac sporządza i przedstawia MF scenariusze testowe dla nowego produktu. Osoby odpowiedzialne ze strony MF za testowanie oprogramowania sprawdzają zgodność scenariuszy testowych ze specyfikacjami wymagań funkcjonalnych i niefunkcjonalnych Głównego Użytkownika, zebranych w formie specyfikacji przypadków użycia (Use Case). Dokument *Plan testów* został oficjalnie zaakceptowany przez kierownictwo.

4.5.2 Plan wdrożenia

Plan wdrożenia nie zawiera procedur dotyczących planu przywracania systemu (aplikacji) po wgraniu wadliwego oprogramowania.

Patrz Rekomendacja 7: Zakup i Wdrożenie – Standardy i procedury zarządzania zmianami

4.5.3 Środowisko testowe

Dokument definiuje środowisko testowe jako testową instancję bazy danych (nie mającą połączenia z bazą produkcyjną). Testowanie aplikacji odbywa się za pomocą przeglądarek internetowych IE oraz Mozilla Firefox.

Dostęp użytkowników do środowiska testowego został opisany w rozdziałach *5.5.3. Zarządzanie tożsamością* oraz *5.5.4. Zarządzanie kontami użytkowników*.

4.5.4 Testowanie zmian

Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13 zwiera procedury testowania wdrażanych zmian zgodnie ze sporządzonym planem testów (Use Cases), przed wprowadzeniem zmian do środowiska produkcyjnego. Oprogramowanie jest testowane wielostopniowo.

Testy wewnętrzne oprogramowania są dokonywane wstępnie przez producenta na podstawie zaakceptowanych przez MF scenariuszy testowych. Produktem testów jest raport z testów. W przypadku wystąpienia błędów podczas tych testów wykonawca zobowiązany jest do ich usunięcia i przeprowadzenia zakończonych pozytywnie retestów. Po pozytywnym zakończeniu testów wewnętrznych, co udokumentowane jest „Raportem z testów” Wykonawca przekazuje MF „Zgłoszenie gotowości do odbioru”.

Pracownicy MF, na podstawie scenariuszy testowych, przeprowadzają testy weryfikujące poprawność dostarczanego oprogramowania i sporządzają „Raportu z testów". Pozytywny wynik testów wstępnych pozwala na przesłanie Głównemu Użytkownikowi „Zgłoszenia gotowości do akceptacji modułu". Negatywny wynik testów skutkuje zgłoszeniem zastrzeżeń do Wykonawcy, który musi dokonać poprawek i procesu testowania rozpoczyna się od początku.

Pozytywny wynik testów wstępnych i dostarczenie aktualnej wersji dokumentacji upoważnia MF do podpisania „Protokołu odbioru dokumentacji" i „Protokołu odbioru oprogramowania".

Następnie na podstawie scenariuszy testowych Główny Użytkownik przeprowadza testy akceptacyjne. Pozytywny wynik testów skutkuje akceptacją Oprogramowania zainstalowanego na testowej instancji bazy danych.

Procedura określa również ścieżkę postępowania przy negatywnym wyniku testów.

4.5.5 Przeniesienie do środowiska produkcyjnego

Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13 nie definiuje procedur przeniesienia przetestowanego i odebranego oprogramowania do środowiska produkcyjnego.

Rekomendacja 8. Zakup i Wdrożenie – Przeniesienie do środowiska produkcyjnego

4.5.6 Przegląd powdrożeniowy

Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13 nie zawiera procedur dotyczących przeglądu systemu po wprowadzeniu do niego zmian.

Rekomendacja 9. Zakup i Wdrożenie – Przegląd powdrożeniowy

5. DOSTARCZANIE I WSPARCIE

5.1. Zdefiniowanie i Zarządzanie Poziomem Usług

5.1.1 Struktura zarządzania poziomem usług

Relacje z zewnętrznymi dostawcami usług odbywają się na podstawie formalnie zawieranych umów. Ze względu na ograniczenia nakładane przez wymogi prawne (Prawo zamówień publicznych), jak również z powodu negocjowania umów z każdym z usługodawców, nie jest możliwe określenie jednolitej struktury wszystkich umów.

Zawarta umowa na wykonanie Krajowego Systemu Informatycznego zawiera charakterystykę przedmiotu umowy, w tym m.in. określenie obowiązków Wykonawcy. Określone zostały również kary umowne przysługujące w przypadku ewentualnych opóźnień w wykonaniu przedmiotu umowy.

5.1.2 Umowy dotyczące poziomu świadczenia usług

W umowie na wykonanie Krajowego Systemu Informatycznego zostały określone pojęcia wady i wady krytycznej. W przypadku ujawnienia się tych wad, Wykonawca jest zobowiązany do ich usunięcia w określonych umową terminach.

Zostały również określone zasady przysługiwania prawa żądania kar umownych.

5.1.3 Monitorowanie i raportowanie poziomu świadczenia usług

W trakcie prac audytowych nie potwierdzono faktu wykonywania przeglądów dotyczących sprawdzenia wywiązywania się przez Wykonawcę z obowiązku zapewnienia poziomu jakości usług. Brak jest także formalnych wewnętrznych zasad (procedur) monitorowania poziomu usług dostawców zewnętrznych, nie zostały również określone kryteria raportowania poziomu usług.

Rekomendacja 10. Dostarczanie i Wsparcie – Monitorowanie i raportowanie poziomu świadczenia usług

5.1.4 Przegląd umów i kontraktów dotyczących poziomu świadczenia usług

Patrz punkty *5.1.1. Struktura zarządzania poziomem usług*, *5.1.2. Umowy dotyczące poziomu świadczenia usług*, *5.1.3. Monitorowanie i raportowanie poziomu świadczenia usług*.

5.2. Zarządzanie Usługami Stron Trzecich

5.2.1 Zarządzanie stosunkami z dostawcami

Zawieranie umów z kontrahentami zewnętrznymi odbywa się zgodnie z zasadami opisanymi w obowiązującym Prawie zamówień publicznych. W zawartej umowie na wykonanie Krajowego Systemu Informatycznego zostały określone obowiązki dostawcy. W ramach utrzymania i rozwoju oprogramowania SIMIK Wykonawca zobowiązany będzie do:

- świadczenia Usług Developerskich:
  - wykonania i przedłożenia do wglądu Zamawiającemu Projektu Technicznego (w tym scenariuszy testowych) zmian lub rozbudowy oprogramowania SIMIK, dokonywania implementacji tego projektu w oprogramowaniu SIMIK oraz przeprowadzenia testów technicznych nowych wersji oprogramowania SIMIK;
  - instalacji nowych wersji oprogramowania SIMIK na serwerach Zamawiającego wraz z niezbędną migracją danych i uzupełnieniem danych podstawowych, na testowej instancji bazy danych;
  - pomocy w trakcie wykonywania przez pracowników Zamawiającego lub inne osoby wskazane przez Zamawiającego, testów akceptacyjnych nowej wersji oprogramowania SIMIK;
  - instalacji nowych wersji oprogramowania SIMIK na serwerach Zamawiającego na produkcyjnej instancji bazy danych oraz przekazania kompletnej dokumentacji oprogramowania SIMIK, zgodnej z zakresem dokumentacji określonym w Zleceniu;
- świadczenia usług Asysty Technicznej:
  - wsparcia przy wdrażaniu nowych wersji oprogramowania SIMIK, zmian konfiguracji, analizy wydajności oraz optymalizacji oprogramowania systemowego (Windows Serwer 2003, Solaris, RDBMS Oracle), prowadzenia prezentacji i warsztatów dotyczących oprogramowania SIMIK;
  - udzielania konsultacji telefonicznych oraz za pośrednictwem poczty elektronicznej, dotyczących oprogramowania SIMIK;
  - świadczenia usług serwisowych polegających na usuwaniu wad i wad krytycznych.

Zgodnie z umową Wykonawca zobowiązał się do utrzymania prawidłowego funkcjonowania Systemu, tj. wolnego od wad i wad krytycznych w zakresie zmian i rozbudowy oprogramowania. Gwarancja na produkty wykonane w ramach Umowy udzielona została na okres 12 miesięcy.

5.2.2 Zarządzanie ryzykiem związanym z dostawcami

W umowie na wykonanie Krajowego Systemu Informatycznego zostały określone kary występujące w przypadku nie wywiązania się Wykonawcy z obowiązków zapisanych w umowie – tj. w przypadku opóźnienia w przekazaniu do odbioru Produktu albo w osiągnięciu Pozytywnego Wyniku Testów po zakończeniu testów akceptacyjnych. Dodatkowe kary zostały określone w przypadku, gdy ilość wad krytycznych stwierdzonych w wyniku testów oprogramowania jest wyższa niż

określona w umowie, jak również w przypadku naruszenia przez Wykonawcę obowiązku przekazania Zamawiającemu kodów źródłowych oprogramowania we wskazanym terminie oraz w przypadku niewykonania umowy w zakresie Asysty Technicznej.

Zgodnie z zawartą umową Wykonawca przekaże Zamawiającemu kody źródłowe zmian lub rozbudowy Oprogramowania wykonanych w ramach Umowy oraz wszelkie procedury niezbędne do przekształcenia kodu źródłowego do postaci wykonywalnej, z użyciem standardowych, dostępnych na rynku narzędzi informatycznych wraz z dostarczeniem Dokumentacji danego Zlecenia. Kod źródłowy Oprogramowania zostanie przekazany w formie elektronicznej (na nośniku zewnętrznym).

Ponadto tytułem zabezpieczenia należytego wykonania umowy Wykonawca złożył przed podpisaniem umowy gwarancję bankową, która zostanie częściowo zwolniona przez Zamawiającego w ciągu 30 dni od wykonania przez Wykonawcę wszystkich obowiązków wynikających z umowy, pozostała część kwoty gwarancji zostanie zwolniona w ciągu 15 dni od upływu okresu gwarancji po wywiązaniu się przez Wykonawcę z obowiązków gwarancyjnych.

Zgodnie z zapisami umowy, może ona zostać rozwiązana przez Zamawiającego bez wypowiedzenia, jeżeli Wykonawca zaprzestanie, bez należytego uzasadnienia, wykonywania obowiązków określonych w umowie lub jeżeli z przyczyn leżących po stronie Wykonawcy, w realizacji jakiegokolwiek obowiązku określonego w umowie, powstaną opóźnienia przekraczające 1 miesiąc.

Została również opracowana *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13*. W analizie tej brak jest jednakże elementów dotyczących szacowania ryzyka związanego z dostawcami zewnętrznymi.

Rekomendacja 11. Dostarczanie i Wsparcie – Zarządzanie ryzykiem związanym z dostawcami

5.2.3 Monitorowanie współpracy z dostawcami

W ramach budowy Krajowego Systemu Informatycznego nie został opracowany formalny proces monitorowania działań dostawców uwzględniający m.in. takie zagadnienia jak: wypełnianie obowiązków kontraktowych, dotrzymywanie poziomów świadczonych usług oraz spełnianie wymogów biznesowych przez dostawcę. Jednakże w trakcie swoich spotkań Rada Projektu dokonuje przeglądów współpracy z Wykonawcą oprogramowania.

W umowie na wykonanie KSI został określony obowiązek usuwania przez producenta oprogramowania wszelkich ujawnionych wad w określonych w umowie terminach, jak również kary w przypadku nie wywiązywania się z tego obowiązku.

5.3. Zarządzanie Wydajnością i Pojemnością

5.3.1 Planowanie wydajności i pojemności

Dokument *Procedura zarządzania rozwojem systemu w systemie SIMIK 07-13* jest dokumentem określającym zasady rozwoju systemu, zasady monitoringu, kontroli i zarządzania wydajnością usług systemu. Pozwala na ewaluację założonego poziomu wydajności systemu. Dokument ten definiuje osoby odpowiedzialne za monitoring i kontrolę wydajności systemu. Procedura ta określa monitorowanie systemu pod kątem wydajności. Brak jest natomiast procedur definiujących monitorowanie systemu pod kątem pojemności.

Z informacji uzyskanych podczas prac audytowych wynika, że nie ma w chwili obecnej regularnego procesu przeglądu dokumentu w celu jego aktualizacji.

Rekomendacja 12. Dostarczanie i Wsparcie – Planowanie wydajności i pojemności

5.3.2 Obecna wydajność i pojemność

Monitorowanie systemu pod kątem wydajności jest dokonywane raz w tygodniu, z procesu tego powstaje dokument *Notatka z monitorowania wydajności systemu SIMIK 07 -13*.

Do monitorowania stanu warstwy sprzętowej systemu służą aplikacje narzędziowe wbudowane w używany system operacyjny. Monitorowaniu podlegają serwery aplikacyjne i bazy danych dla systemu SIMIK w środowisku produkcyjnym. Procesowi monitorowania podlegają również czas procesora, średnia długość kolejki dysku, itp. Monitorowanie jest wykonywane w godzinach największego nasilenia pracy użytkowników systemu.

W przeprowadzonych rozmowach z administratorami ustalono, iż do chwili obecnej odbyły się cztery, udokumentowane powstaniem notatki, badania wydajności systemu. Na podstawie wykonanych badań systemu, administrator we wnioskach określił, że w chwili obecnej wydajność systemu SIMIK w okresach zwiększonego nasilenia pracy użytkowników tj. od godz. 10 do godz. 14 jest nie wystarczająca. Jednocześnie z udzielonych informacji wynika, że obecnie są prowadzone prace mające na celu wdrożenie nowej infrastruktury sprzętowej. Zakończenie procesu wdrożenia nowej platformy sprzętowej planowane jest na początek lipca 2008 r.

Uzyskane z monitoringu wyniki sporządzane w postaci notatek służą do opracowania *Raportu monitorowania obciążenia systemu KSI SIMIK 07-13*. Jest on przygotowywany raz w miesiącu przez zespół Infrastruktury Technicznej. Z udzielonych informacji ustalono, że do chwili obecnej powstał jeden miesięczny *Raport z monitorowania obciążenia systemu KSI SIMIK 07 – 13*. Na podstawie comiesięcznych raportów Zespół Infrastruktury Technicznej sporządza raz na pół roku *Raport o wydajności zasobów systemu,* zawierający:

- informację z cyklicznych notatek sporządzanych z monitorowania w okresie za jaki raport jest sporządzany;
- wnioski z przebiegu monitorowania w 6 miesięcznym okresie;

- wychwycone tendencje co do zwiększającego się obciążenia systemu w określonych zakresach;
- wnioski co do wykonywania kolejnych pomiarów wydajności;
- informację o osobach sporządzających raport.

Z uzyskanych informacji wynika, że miesięczny *Raport z monitorowania obciążenia systemu KSI SIMIK 07 – 13* został wykonany raz pierwszy.

Rekomendacja 13. Dostarczanie i Wsparcie – Obecna wydajność i pojemność

5.3.3 Docelowa wydajność i pojemność

Zespół Infrastruktury Technicznej MF porównuje zakres zadań planowanych do obsługi w systemie z aktualną wydajnością systemu i w przypadku stwierdzenia niskiego poziomu wydajności:

- Sporządzany jest plan potrzeb w zakresie infrastruktury sprzętowej i programowej;
- Przekazywane są wnioski do wykonawcy oprogramowania (zlecenia zmiany lub zgłoszenie błędu) o optymalizację działania aplikacji, bazy danych.

Z informacji uzyskanych od pracowników MF wynika, iż w chwili obecnej monitorowanie wydajności odbywa się za pomocą standardowych aplikacji dostarczonych i wbudowanych w system operacyjny, proces monitorowania pojemności systemu nie jest prowadzony. Z uzyskanych informacji wynika, że nie są dokonywane analizy przyszłego wykorzystania zasobów.

Rekomendacja 14. Dostarczanie i Wsparcie – Docelowa wydajność i pojemność

5.3.4 Dostępność zasobów

W trakcie prac uzyskano informacje o występujących w przeszłości problemach z dostępem do systemu SIMIK. Problemy te były spowodowane zbyt małą przepustowością sieci, która została wydzielona na potrzeby systemu. W chwili obecnej problem ten nie występuje - został usunięty w porozumieniu z wykonawcą systemu SIMIK.

5.3.5 Monitorowanie i raportowanie

Procedura zarządzania rozwojem systemu w systemie SIMIK 07-13 określa, że zespół obsługi technicznej powinien cyklicznie monitorować i sprawdzać wydajność systemu na poziomie MF. Zespół raz na pół roku sporządza *Raport o wykorzystaniu systemu*. Procedura określa dane, które powinny być prezentowane personelowi zarządzającemu tj.

- informację z cyklicznych notatek z monitorowania;
- wnioski z przebiegu monitorowania w 6 miesięcznym okresie;
- wychwycone tendencje co do zwiększającego się obciążenia systemu w określonych zakresach;
- wnioski co do wykonywania kolejnych pomiarów wydajności;
- informację o osobach sporządzających raport.

Ponadto zespół obsługi technicznej porównuje zakres zadań planowanych do obsługi w systemie z aktualną wydajnością systemu i w przypadku stwierdzenia niskiego poziomu wydajności:

- sporządza plan potrzeb w zakresie infrastruktury sprzętowej i programowej;
- sporządza wnioski do wykonawcy oprogramowania (zlecenia zmiany lub zgłoszenie błędu) o optymalizację działania aplikacji, bazy danych.

Z uzyskanych informacji wynika, że administrator dokonuje przeglądu wydajności systemu raz na tydzień w godzinach najwyższego obciążenia systemu tj. od godz. 10 do godz. 14. Po wykonaniu procesu monitorowania administrator sporządza notatkę dla kierownika projektu. W toku prac audytowych potwierdzono przekazywania informacji w formie notatek z monitorowania wydajności systemu kierownikowi projektu.

5.4. Zapewnienie Ciągłości Usług

5.4.1 Struktura zapewnienia ciągłości działania IT

Podstawowymi dokumentami wyznaczającymi proces zarządzania ciągłością działania w odniesieniu do systemu KSI SIMIK 07-13 są *Polityka bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* oraz *Plan ciągłości działania Krajowego Systemu Informatycznego SIMIK 07-13*, opracowane wspólnie przez pracowników Ministerstwa Rozwoju Regionalnego oraz Ministerstwa Finansów i zatwierdzone przez Kierownika Projektu i Dyrektora Departamentu Rozwoju Systemów Informatycznych Ministerstwa Finansów.

Celem *Planu ciągłości działania KSI* jest określenie działań niezbędnych do utrzymania ciągłości działania Krajowego Systemu Informatycznego SIMIK 07-13.

Polityka bezpieczeństwa definiuje formalną strukturę zarządzania ciągłością działania w systemie KSI. Zawiera postanowienia regulujące monitorowanie i raportowanie bezpieczeństwa systemu.

Zgodnie z jej zapisami wyodrębniona została specjalna komórka – Zespół Kryzysowy (ZK), do którego zadań należy m.in. podejmowanie działań w przypadku wystąpienia awarii krytycznych KSI SIMIK 07-13, aktualizacja *Planu ciągłości działania* i testowanie planu awaryjnego. W skład Zespołu wchodzą:

- Przedstawiciel(e) MF;
- Przedstawiciel(e) MRR;
- Przedstawiciele na zasadzie ekspertów: osoba z biura informacji niejawnych MF, osoba z biura prasowego MF, osoba z departamentu prawnego MF.

Decyzję o podjęciu działań w przypadku awarii krytycznych i uruchomieniu planu awaryjnego podejmuje Koordynator Zespołu Kryzysowego lub wyznaczony przez niego członek ZK. Skład ZK, zakresy zadań członków oraz dane kontaktowe zawarte są w odrębnym dokumencie *Zakresy zadań i dane kontaktowe ZK*.

Zgodnie z otrzymanymi informacjami szczegółowy skład Zespołu Kryzysowego jest na bieżąco aktualizowany.

Plan ciągłości działania zawiera szczegółowe zasady postępowania Zespołu Kryzysowego w sytuacjach awaryjnych.

5.4.2 Plany ciągłości działania IT

Dokument *Plan ciągłości działania KSI SIMIK 07-13* wymienia działania prewencyjne służące utrzymaniu ciągłości działania systemu oraz jednostkę organizacyjną odpowiedzialną za ich realizację. W szczególności *Plan ciągłości działania* wymienia działania prewencyjne w obszarze IT, podejmowane przez odpowiednich administratorów. W celu przeciwdziałania utracie ciągłości przetwarzania danych administratorzy techniczni zobowiązani są m.in. do regularnej aktualizacji bazy danych sygnatur oprogramowania antywirusowego zainstalowanego na serwerach, tworzenia i testowania kopii zapasowych, wykonywania regularnego przeglądu technicznego urządzeń systemu, sprawdzania stanu pomieszczeń serwerowni oraz testowania zasilania awaryjnego.

Plan ciągłości działania określa wpływ awarii systemu na krytyczne procesy biznesowe. Maksymalny dopuszczalny czas braku dostępności jakiegokolwiek modułu (krytycznego procesu biznesowego wspieranego przez KSI) ustalono na poziomie 1 dnia pracy.

Plan ciągłości działania zawiera również szczegółowy plan awaryjny, określający obowiązki i zadania osób zaangażowanych w proces zapewnienia ciągłości działania systemu KSI SIMIK 07-13. Są to działania związane między innymi z:

- awariami większej liczby komponentów systemu;
- awarią sprzętowych urządzeń sieciowych;
- awarią i nieprawidłowym funkcjonowaniem oprogramowania KSI SIMIK;
- awariami i niedostępnością serwera bazodanowego i systemu zarządzania bazami danych;
- awariami stacji roboczych;
- awariami zasilania serwerowni.

Plan awaryjny opisuje szczegółowe działania naprawcze, jakie należy podjąć w przypadku wystąpienia danej awarii oraz zawiera ogólne wytyczne związane z powiadamianiem osób zobowiązanych do podejmowania działań w przypadku awarii krytycznych, reagowaniem w sytuacjach kryzysowych oraz odtwarzaniem danych i systemu informatycznego.

5.4.3 Krytyczne zasoby IT

Plan ciągłości działania określa wpływ awarii systemu na krytyczne procesy biznesowe. Maksymalny dopuszczalny czas braku dostępności jakiegokolwiek modułu (krytycznego procesu biznesowego wspieranego przez KSI) ustalono na poziomie 1 dnia pracy.

W *Planie ciągłości działania* określono następujące priorytety postępowania podczas operacji awaryjnych:

- ochrona życia - wszelkie inne działania powinny być brane pod uwagę wyłącznie w przypadku, gdy życie osób nie jest zagrożone;
- utrzymanie bezpiecznego środowiska i ochrona aktywów,
- odtworzenie działalności biznesowej.

Krytyczne zasoby IT wskazane zostały w *Planie awaryjnym.* Natomiast *Plan ciągłości działania* koncentruje się na krytycznych procesach biznesowych określonych jako moduł.

5.4.4 Utrzymanie planu ciągłości działania IT

Aktualizację planu ciągłości działania, w tym planu awaryjnego oraz odpowiednich procedur, powinien przeprowadzać Zespół Kryzysowy. W dokumencie nie określono częstotliwości wymaganych przeglądów i aktualizacji. Ostatnia wersja dokumentu została zatwierdzona przez Dyrektora Departamentu MF/RI w dniu 29.02.2008 r.

Patrz Rekomendacja 15: Dostarczanie i Wsparcie – Zapewnienie ciągłości usług

5.4.5 Testowanie planu ciągłości działania IT

Zgodnie z *Planem ciągłości działania* testowanie planów awaryjnych powinno być przeprowadzane nie rzadziej niż raz do roku oraz każdorazowo po wprowadzeniu istotnych zmian w systemach. Testowanie planów awaryjnych przeprowadza Zespół Kryzysowy na podstawie listy kontrolnej opisanej w *Planie ciągłości działania*.

Po przeprowadzeniu testu Zespół Kryzysowy sporządza raport zawierający: zakres i czas trwania testu, wynik testu, zidentyfikowane problemy oraz opinię w sprawie konieczności aktualizacji planu.

Dotychczas *Plan ciągłości działania Krajowego Systemu Informatycznego SIMIK 07-13* nie został przetestowany.

Patrz Rekomendacja 15: Dostarczanie i Wsparcie – Zapewnienie ciągłości usług

5.4.6 Szkolenie z zakresu planu ciągłości działania IT

Plan ciągłości działania określa zakres tematyki i częstotliwość szkolenia członków Zespołu Kryzysowego oraz pozostałych osób uczestniczących w procesie zapewnienia ciągłości działania w przypadku wystąpienia incydentu lub katastrofy.

Szkolenia dla członków Zespołu Kryzysowego zgodnie z *Planem ciągłości działania* powinny obejmować następujące zagadnienia:

- definicje podstawowych pojęć: polityka bezpieczeństwa informacji, plan ciągłości działania, plan awaryjny, zarządzanie kryzysowe, zarządzanie ryzykiem, itp.;
- proces zarządzania ryzykiem, w tym analiza skutków biznesowych;
- strategie utrzymania ciągłości działania;
- proces tworzenia planów ciągłości działania oraz planów awaryjnych;
- tworzenie efektywnego środowiska niezbędnego do symulacji awarii dla celów testowych;
- proces zarządzania zmianami planów ciągłości działania;
- organizowanie efektywnego zespołu kryzysowego;
- analiza przykładowych rzeczywistych sytuacji kryzysowych, w tym omówienie typowych błędów przy realizacji planów awaryjnych oraz sposobów ich unikania.

Zgodnie z otrzymanymi informacjami szkolenia dotyczące *Planu ciągłości działania* nie były dotychczas przeprowadzane.

Rekomendacja 15. Dostarczanie i Wsparcie – Zapewnienie ciągłości usług

5.4.7 Rozpowszechnienie planu ciągłości działania IT

W *Polityce bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* znajduje się spis dokumentów wraz z określeniem osób/instytucji, które mogą zapoznać się i/lub korzystać z dokumentów. *Plan ciągłości działania* jest dostępny dla:

- Administratora Informacji;

- Administratora Bezpieczeństwa Informacji;
- Osób pisemnie upoważnionych przez AI;
- Członków Zespołu Bezpieczeństwa Informacji;
- Pracowników Ministerstwa Rozwoju Regionalnego pisemnie upoważnionych przez Właściciela Projektu.

Dla innych osób lub instytucji dokumenty dotyczące zapewnienia ciągłości działania nie są udostępniane.

W trakcie prac audytowych potwierdzono, iż *Plan ciągłości działania* jest znany i dostępny Administratorom Technicznym. Dokument jest przechowywany w sejfie w pokoju administratorów. Klucze do sejfu są przechowywane w bezpiecznym miejscu i wydawane upoważnionym osobom.

5.4.8 Odzyskiwanie i przywracanie zasobów IT

W *Planie ciągłości działania* zamieszczono plan awaryjny KSI SIMIK 07-13 obejmujący działania związane z reagowaniem w przypadku awarii krytycznych, elementy powiadamiania kluczowych osób oraz działania związane z odtwarzaniem systemu i danych.

Zasady powiadamiania osób zobowiązanych do podejmowania działań naprawczych, określa koordynator Zespołu Kryzysowego. Działania naprawcze wymienione są w porządku priorytetowym w ramach określonej awarii.

W przypadku awarii upoważnione osoby powinny postępować zgodnie z planem awaryjnym zawartym w *Planie ciągłości działania KSI SIMIK 07-13*. W trakcie prac audytowych uzyskano informacje, iż do chwili obecnej nie zaistniały awarie systemu SIMIK, w związku z powyższym nie zaistniała potrzeba realizacji *Planu ciągłości działania.*

Obecnie wszystkie zasoby KSI SIMIK 07-13 znajdują się w jednym pomieszczeniu. Kopie zapasowe są przechowywane w tym samym budynku w MF. Dostęp do kopii zapasowych posiadają jedynie upoważnieni administratorzy.

5.4.9 Lokalizacja zapasowa

Zgodnie z otrzymanymi w trakcie prac audytowych informacji KSI SIMIK 07-13 nie posiada lokalizacji zapasowej i stworzenie takiej lokalizacji nie jest planowane w przyszłości.

5.5. Zapewnienie Bezpieczeństwa Systemów

5.5.1 Zarządzanie bezpieczeństwem IT

Zarządzanie bezpieczeństwem informacji w systemie SIMIK 07-13 zostało zdefiniowane przez kierownictwo Ministerstw tworzących system już na etapie definiowania podstawowych funkcjonalności systemu i założeń wzajemnej współpracy. Zgodnie z Załącznikiem do *Porozumienia z dnia 23 lutego 2007 o współpracy przy realizacji projektu „Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013 (SIMIK 07-13)”*, zawartego pomiędzy Ministrem Finansów a Ministrem Rozwoju Regionalnego, budowany system powinien zapewniać odpowiedni poziom bezpieczeństwa, zgodny z powszechnie przyjętymi standardami.

5.5.2 Plan zapewnienia bezpieczeństwa IT

Podstawowym dokumentem opisującym zasady zarządzania bezpieczeństwem informacji jest *Polityka Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13,* która została formalnie zaakceptowana przez właściciela procesu biznesowego – Dyrektora Departamentu Rozwoju Systemów Informatycznych Ministerstwa Finansów. Obecnie obowiązuje wersja 1.3 *Polityki*, zaakceptowana w dn. 28.04.2008 r.

Polityka Bezpieczeństwa definiuje podstawowy cel wprowadzenia zasad zarządzania bezpieczeństwem informacji. Zgodnie z zapisami tego dokumentu celem polityki bezpieczeństwa jest zdefiniowanie zasad i środków ochrony wszystkich elementów Krajowego Systemu Informatycznego SIMIK 07-13 oraz informacji w nim przetwarzanych. *Polityka Bezpieczeństwa* KSI SIMIK 07-13 określa zasady ochrony wszystkich zasobów technicznych systemu oraz informacji przetwarzanych w tym systemie wraz z obszarami przetwarzania.

Polityka Bezpieczeństwa definiuje całościową strukturę organizacyjną zarządzania bezpieczeństwem informacji w KSI SIMIK 07-13 oraz role i zadania osób zaangażowanych w ten proces.

Polityka Bezpieczeństwa zawiera w formie załączników wzory dokumentów wykorzystywanych w procesie nadawania i odbierania uprawnień dla poszczególnych administratorów oraz wzory oświadczeń potwierdzających przyjęcie tych funkcji. Szczegółowe obowiązki poszczególnych administratorów zostały zawarte w politykach i procedurach wynikających z *Polityki Bezpieczeństwa* i uzupełniających ten dokument. Zgodnie z otrzymanymi informacjami są to następujące dokumenty:

- *Instrukcja Zarządzania Krajowym Systemem Informatycznym SIMIK 07-13;*
- *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13* oraz *Spis zagrożeń dla Krajowego Systemu Informatycznego SIMIK 07-13;*
- Instrukcje postępowania administratorów, koordynatorów i użytkowników w przypadku naruszenia bezpieczeństwa informacji;
- *Plan Ciągłości Działania Krajowego Systemu Informatycznego SIMIK 07-13;*

- Zalecenia dotyczące zabezpieczenia komputerów użytkowników;
- szczegółowe procedury zarządzania systemem KSI (m.in. procedura przechowywania haseł administracyjnych, procedura przechowywania i udostępniania dokumentacji technicznej, procedura postępowania z nośnikami informacji).

Zgodnie z zapisami *Polityki Bezpieczeństwa* wszystkie dokumenty składające się na politykę bezpieczeństwa w KSI SIMIK podlegają ochronie i są zastrzeżone zgodnie z zawartym w niej opisem. Oznacza to, iż dostęp do tych dokumentów jest zastrzeżony tylko dla osób uczestniczących w procesie tworzenia bezpieczeństwa systemu (odpowiednich administratorów wymienionych w załączniku nr 2 *Polityki* lub osób pisemnie upoważnionych przez AI lub MRR). Jest to sprzeczne z powszechnie przyjętą praktyką, która stanowi, iż główny dokument polityki bezpieczeństwa powinien zawierać m.in. ogólne oświadczenie o intencjach kierownictwa w stosunku do celów i zasad bezpieczeństwa informacji w systemie oraz stosowanych norm i zasad zabezpieczeń i jako taki powinien być powszechnie dostępny w formie właściwej i zrozumiałej dla wszystkich użytkowników systemu informatycznego.

Rekomendacja 16. Dostarczanie i wsparcie – Plan zapewnienia bezpieczeństwa IT

Polityka Bezpieczeństwa zawiera opis podstawowych zasad ochrony informacji w systemie. Zgodnie z tym dokumentem w KSI SIMIK 07-13 stosowane jest wyłącznie licencjonowane oprogramowanie Ministerstwa Finansów (urządzenia sieciowe, serwery aplikacyjne i bazodanowe). Ochrona sieci następuje poprzez zastosowanie odpowiednich zabezpieczeń technicznych (firewall, akcelerator SSL, sondy IPS posiadające funkcjonalność ochrony antywirusowej). Urządzenia służące do przetwarzania danych znajdują się w serwerowni Ministerstwa Finansów, w strefie zamkniętej. Każdy użytkownik dysponuje indywidualnym kontem o niepowtarzalnym loginie, chronionym unikalnym hasłem.

Polityka Bezpieczeństwa definiuje podstawowe zasady prowadzenia monitoringu systemu KSI. Zgodnie z tymi zapisami Administrator Bezpieczeństwa Informacji jest zobowiązany do składania kwartalnego raportu z prowadzonego monitorowania przestrzegania zasad *Polityki Bezpieczeństwa*. Administratorzy Techniczni monitorują poprawność funkcjonowania systemu informatycznego oraz elementy systemu mające wpływ na bezpieczeństwo przetwarzanych informacji. Wzory raportów składanych przez administratorów stanowią załączniki *Polityki Bezpieczeństwa*.

Polityka Bezpieczeństwa zawiera krótki opis systemu zarządzania incydentami. W przypadku wystąpienia takiego incydentu należy zachować się zgodnie z *Instrukcjami postępowania w sytuacji naruszenia bezpieczeństwa informacji.* Realizacja procedur awaryjnych powinna być każdorazowo udokumentowana wpisem w dzienniku systemu, z podaniem imienia i nazwiska osoby wykonującej procedurę, wykazu wykonywanych czynności oraz daty.

W *Polityce Bezpieczeństwa* nie został określony bezpośrednio Właściciel dokumentu – osoba odpowiedzialna za akceptację dokumentu oraz regularne (np. roczne) przeglądy i zatwierdzanie aktualizacji zasad zarządzania bezpieczeństwem informacji w KSI, dostosowujących *Politykę* i wynikające z niej szczegółowe procedury do aktualnego stanu technicznego, prawnego i organizacyjnego.

W *Polityce Bezpieczeństwa* zawarto jedynie ogólny zapis, iż za opracowanie i aktualizację dokumentu odpowiada Zespół do Spraw Bezpieczeństwa Informacji.

Rekomendacja 17. Dostarczanie i wsparcie – Plan zapewnienia bezpieczeństwa IT

Polityka Bezpieczeństwa zawiera podstawowe wytyczne dotyczące systemu szkoleń z zakresu bezpieczeństwa informacji dla pracowników MRR. Podczas szkoleń użytkownicy jedynie zapoznają się z wybranymi zapisami *PBI*. Na zakończenie szkolenia potwierdzają fakt zapoznania się z *Polityką Bezpieczeństwa* i obowiązującymi procedurami oraz zobowiązują się do przestrzegania tych postanowień. Wykazy przeszkolonych użytkowników przechowywane są w wyznaczonej komórce MRR.

Zgodnie z otrzymanymi informacjami Ministerstwo Rozwoju Regionalnego zorganizowało szkolenie osób pełniących rolę Administratorów Merytorycznych w Instytucjach Zarządzających, na którym zaprezentowano i szczegółowo omówiono zapisy *Polityki Bezpieczeństwa* oraz system obsługi zgłaszania problemów i incydentów dotyczących KSI SIMIK 07-13. System szkoleń z zapisów *Polityki Bezpieczeństwa* zakłada, iż dalsze szkolenia odbywać się będą kaskadowo – każdy Administrator Merytoryczny jest zobowiązany do przeszkolenia wszystkich Administratorów Merytorycznych w Instytucjach Pośredniczących i Instytucjach Pośredniczących II stopnia. Przeszkoleni Administratorzy Merytoryczni w Instytucjach przeprowadzają szkolenia dla wszystkich użytkowników KSI SIMIK 07-13 w Instytucji.

Wszyscy nowi użytkownicy KSI SIMIK 07-13 powinni być przeszkoleni z zapisów *Polityki Bezpieczeństwa* przez Administratorów Merytorycznych w Instytucjach nie później niż w ciągu 3 tygodni od daty podpisania *Wniosku o nadanie/zmianę uprawnień do Krajowego Systemy Informatycznego SIMIK 07-13*.

5.5.3 Zarządzanie tożsamością

Proces zarządzania tożsamością został sformalizowany, a jego opis został przedstawiony w punkcie *5.5.4. Zarządzanie kontami użytkowników*.

Wszyscy użytkownicy posiadają unikalny identyfikator (login) składający się z trzech pierwszych liter imienia oraz trzech pierwszych liter nazwiska.

Proces logowania do systemu rozpoczyna się wpisaniem odpowiedniego adresu w przeglądarce internetowej. Z punktu widzenia użytkownika różnica w sposobie logowania do bazy produkcyjnej i szkoleniowej polega jedynie na podawaniu odmiennych adresów w przeglądarce. Niezależnie od tego, do którego systemu użytkownik się loguje, po uruchomieniu przeglądarki internetowej użytkownik

proszony jest o podanie loginu i hasła. W systemie użytkownik może jedynie wykonywać operacje zgodnie z nadanymi prawami dostępu.

5.5.4 Zarządzanie kontami użytkowników

W Ministerstwie Rozwoju Regionalnego został opracowany dokument *Wytyczne w zakresie warunków gromadzenia i przekazywania danych w formie elektronicznej* zaakceptowany przez Ministra Rozwoju Regionalnego w dniu 10 stycznia 2008 r.

Zgodnie z ww. wytycznymi dostęp do KSI SIMIK 07-13 mają zapewniony wszystkie podmioty uczestniczące w systemie zarządzania i kontroli:

- Ministerstwo Rozwoju Regionalnego, pełniące rolę **Instytucji Koordynującej** Narodowe Strategiczne Ramy Odniesienia;
- **Instytucje Zarządzające** (IZ) poszczególnymi programami operacyjnymi;
- Instytucje uczestniczące we wdrażaniu poszczególnych programów operacyjnych – **Instytucje Pośredniczące** (IP) oraz **Instytucje Pośredniczące II stopnia** (IP2);
- **Instytucje Certyfikujące** (IC) oraz **Instytucje Certyfikujące II Stopnia** (IC2);
- **Instytucja Audytowa**;
- oraz Departament Rozwoju Systemów Informatycznych Ministerstwa Finansów, odpowiedzialny za techniczna obsługę systemu.

Załącznikiem do tego dokumentu jest *Procedura zgłaszania użytkownika do Krajowego Systemu Informatycznego (SIMIK 07-13) (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych*. Procedura ta zawiera następujące informacje:
- zakres stosowania procedury;
- instytucje stosujące procedurę;
- opis procedury;
  - Nadawanie i zmiana uprawnień użytkownika KSI (SIMIK 07-13);
  - Wygaśnięcie uprawnień użytkownika KSI (SIMIK 07-13);
  - Kopia bezpieczeństwa wersji elektronicznej uprawnień;
  - Uwagi;
- Zakres obowiązków Administratorów Merytorycznych.

Zgodnie z *Procedurą* pracownicy instytucji mający dostęp do KSI SIMIK 07-13 mogą w ramach wykonywania swoich obowiązków służbowych wykorzystywać ten system do wprowadzenia do niego informacji lub uzyskania z niego niezbędnych informacji o postępie wdrażania funduszy w wybranym zakresie.

Procedura określa, w jaki sposób instytucje uczestniczące w systemie zarzadzania i kontroli występują o nadanie uprawnień do KSI dla swoich pracowników. Procedurę stosuje się w następujących sytuacjach:
- w trakcie wdrażania KSI;
- zgłoszenia nowego użytkownika;
- zmiany uprawnień użytkownika wynikających ze zmiany obowiązków;
- wygaśnięcia uprawnień.

Nadanie praw dostępu do systemu następuje wskutek złożenia pisemnego *Wniosku o nadanie/zmianę uprawnień do krajowego Systemu Informatycznego (SIMIK 07-13)*. Wniosek ten zawiera następujące informacje:
- Nazwa instytucji wnioskującej;
- Użytkownik;
- Imię i nazwisko użytkownika;
- Adres poczty elektronicznej;
- Uprawnienia do funkcji systemu;
- Uprawnienia do zakresu danych;
- Data sporządzenia wniosku;
- Podpis osoby uprawnionej.

Wniosek musi zostać zaakceptowany przez kierownika jednostki organizacyjnej, w której zatrudniony jest dany pracownik. Akceptacja ta jest traktowana jako weryfikacja merytoryczna wniosku – wniosek nie jest merytorycznie sprawdzany przez administratora odpowiedzialnego za nadanie uprawnień. Za nadane użytkownikowi uprawnienia odpowiedzialny jest kierownik jednostki, który podpisał dany wniosek.

Proces odebrania uprawnień użytkownika KSI wygląda następująco:
- Wypełnienie formularza zgłaszającego wygaśnięcie uprawnień użytkownika;
- Podpisanie formularza przez Kierownika jednostki organizacyjnej;
- Skanowanie formularza;
- Archiwizacja podpisanego formularza;
- Przesłanie wersji elektronicznej formularza pocztą elektroniczną do IK NSRO oraz do IZ;
- Blokowanie dostępu do KSI dla wskazanego w zgłoszeniu użytkownika;
- Przesłanie pocztą elektroniczną do użytkownika oraz do wiadomości AM I i AM IZ, informacji o zablokowaniu dostępu;
- Archiwizacja wersji elektronicznej formularza na dysku lokalnym.

Po zaakceptowaniu wniosku o nadanie bądź odebranie uprawnień przez przełożonego danej osoby, wniosek ten jest skanowany i jego wersja elektroniczna jest przesyłana mailem na adres administratorów systemu. Administrator nadaje bądź odbiera użytkownikowi wymagane uprawnienia, po czym wniosek (elektroniczny) jest archiwizowany na dysku. Zawartość tego dysku jest zapisywana raz w miesiącu na kopiach zapasowych. Administrator prowadzi elektroniczny rejestr nadanych uprawnień wszystkim użytkownikom (w formie pliku w arkuszu Excel).

W *Procedurze zgłaszania użytkownika do Krajowego Systemu Informatycznego (SIMIK 07-13) (nadawanie, zmiana, wygaśniecie uprawnień) oraz zakres obowiązków Administratorów Merytorycznych* wskazane są również osoby odpowiedzialne za każdą czynność oraz termin, w jakim powinny być wykonane poszczególne czynności.

Zgodnie z otrzymanymi informacjami w systemie KSI nie zostały zdefiniowane predefiniowane profile kont, zawierające uprawnienia dla różnych typów użytkowników, ze względu na dużą liczbę możliwych kombinacji uprawnień nadawanych użytkownikom.

W chwili obecnej wykonywany jest jedynie przegląd uprawnień użytkowników na zgodność ze złożonymi wnioskami. Administratorzy cotygodniowo wybierają

losowo 10 użytkowników, dla których odbywa się weryfikacja złożonych wniosków i nadanych odpowiednio uprawnień. Po każdym przeglądzie sporządzany jest *Raport z okresowego przeglądu kont użytkowników KSI (SIMIK 07-13)*. Raport ten zawiera szczegółowe informacje na temat sprawdzanych kont użytkowników oraz nadanych im uprawnień. Podana jest informacja o dacie wykonanie oraz osobie dokonującej weryfikacji. Raport akceptowany jest przez Naczelnika Wydziału Administracji i Audytu Systemów Informatycznych.

W chwili obecnej nie są natomiast wykonywane regularne przeglądy kont użytkowników, przeprowadzane w celu zablokowania niewykorzystywanych przez dłuższy czas kont użytkowników.

Rekomendacja 18. Dostarczanie i Wsparcie – Zarządzanie kontami użytkowników

W Departamencie Koordynacji i Zarządzania Podstawami Wsparcia Wspólnoty Ministerstwa Rozwoju Regionalnego zostały opracowane *Procedury Wewnętrzne* w Wydziale Administracji i Audytu Systemów Informatycznych. Procedury te mają na celu określenie czynności związanych z wykonywaniem zadań w *Wydziale* w ramach poniższych procesów:

- Aktualizacja systemu KSI SIMIK 07-13 – analiza procesów biznesowych;
- Testowanie;
- Koordynacja prac nad wdrożeniem programów krajowych w zakresie KSI;
- Koordynacja prac nad wdrożeniem RPO w zakresie KSI;
- Obsługa audytów zewnętrznych;
- Weryfikacja instrukcji wykonawczych IZ PO Krajowych pod kątem KSI;
- Weryfikacja poziomu wdrożenia SIMIK;
- Weryfikowanie i opiniowanie wzorów dokumentów np. Wniosków o dofinansowanie umów pod kątem wymagań KSI.

W odniesieniu do systemu finansowo-księgowego QWANT uprawnienia dostępu dla pracowników Departamentu DEF nadawane są przez osoby administrujące oprogramowaniem QWANT, zatrudnione w Biurze Administracyjno-Informatycznym. W celu nadania uprawnień Dyrektor (lub Zastępca Dyrektora) Departamentu DEF przesyła do Biura Administracyjno-Informatycznego pismo informujące o zatrudnieniu nowej osoby oraz z prośbą o nadanie uprawnień dla pracownika danego Wydziału. Uprawnienia w systemie zostały pogrupowane w zależności od zakresu obowiązków poszczególnych Wydziałów.

5.5.5 Monitorowanie i testowanie bezpieczeństwa

W *Dokumencie Głównym Polityki Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* został zawarty opis ról i odpowiedzialności dotyczących monitorowania bezpieczeństwa systemu. Zgodnie z tymi zapisami Administrator Bezpieczeństwa Informacji monitoruje przestrzeganie zasad *PBI*, zgodnie z harmonogramem zatwierdzonym przez Administratora Informacji. ABI przygotowuje kwartalny raport z prowadzonego monitorowania i przekazuje go do AI. Do chwili obecnej ABI opracował jeden raport (noszący datę 24.04.2008) odnoszący się do zagadnień bezpieczeństwa – kolejne raporty powstaną w następnych kwartałach (ze względu na fakt, iż *PBI* została zaakceptowana

i wdrożona w dniu 28.04.2008). Raport przedstawia informację statystyczną o przebiegu logowania do systemu ze szczególnym uwzględnieniem nieudanych prób logowania do systemu KSI SIMIK, w okresie kwartalnym. Uwzględniono ponadto następujące zagadnienia: backup systemu, awarie sprzętu, incydenty związane z nieprawidłową pracą systemu. Brak jest jednakże harmonogramu zadań związanych z monitorowaniem zatwierdzonego przez AI, o którym jest mowa w PBI.

Rekomendacja 19. Dostarczanie i Wsparcie – Monitorowanie i testowanie bezpieczeństwa

Systemy posiadają funkcje logowania wykonywanych działań. Możliwe jest zweryfikowanie każdej operacji wykonywanej w systemie KSI.

5.5.6 Definicja incydentu bezpieczeństwa

Definicja incydentu naruszenia bezpieczeństwa w systemie KSI SIMIK 07-13 została zawarta w szczegółowych procedurach postępowania użytkowników, koordynatorów i poszczególnych administratorów w sytuacji wystąpienia takiego incydentu. Zgodnie z tymi zapisami przez naruszenie bezpieczeństwa informacji należy rozumieć wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata lub nieuzasadniona modyfikacja danych lub części danych, a także możliwość dostępu do danych dla osób nieupoważnionych.

Incydentem naruszenia bezpieczeństwa określa się każde określone zdarzenie lub działanie, naruszające bezpieczeństwo lub zasady ochrony informacji.

Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

- nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia);
- zaginięcie sprzętu lub nośników informacji (dyskietek, dokumentów papierowych, itp.);
- nieuzasadnione modyfikacje lub usunięcie danych, niezgodności w danych;
- nieprawidłowe lub nietypowe działanie systemu informatycznego (lub nietypowe komunikaty wyświetlane na monitorze);
- przypadki niskiej wydajności systemu;
- nietypowy przepływ danych;
- nietypowe czasy wykorzystywania systemu, duża liczba nieudanych prób logowania lub inne nietypowe zdarzenia występujące w logach systemu operacyjnego;
- zgłoszenie otrzymane od użytkownika, administratora lub koordynatora systemu SIMIK.

5.5.7 Ochrona technologii bezpieczeństwa

Dokumentem definiującym sposób postępowania przy naruszeniu bezpieczeństwa jest *Instrukcja postępowania Administratora Bezpieczeństwa Informacji w sytuacjach naruszenia bezpieczeństwa informacji dla KSI SIMIK 07-13*. Określa ona sposób postępowania administratora w przypadku wystąpienia incydentów naruszenia bezpieczeństwa, a także sposób zabezpieczenia dowodów incydentu oraz działania podejmowane w celu ograniczania skutków incydentu i przywracania stanu sprzed incydentu.

Przez naruszenie bezpieczeństwa informacji rozumie się wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie) lub nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych), a także możliwość dostępu do danych dla osób nieupoważnionych.

Działania związane z analizą skutków incydentu naruszenia bezpieczeństwa oraz opracowaniem zaleceń mających na celu podniesienie poziomu bezpieczeństwa systemu, przeprowadza ABI. Wyniki analizy incydentów, w formie raportu, ABI przedkłada AI lub kierownikowi Projektu (lub jego zastępcy).

Analiza incydentu obejmuje sprawdzenie i ustalenie, m.in.:
- Stanu zabezpieczeń fizycznych;
- Stanu informacji (czy została zmodyfikowana, utracona lub ujawniona);
- Czy miał miejsce dostęp osób nieupoważnionych do zasobów;
- Ustalenie sposobu i miejsca, z którego uzyskano nieuprawniony dostęp do systemu;
- Czy miało miejsce, celowe lub przypadkowe, niedopełnienie obowiązków lub przekroczenie uprawnień przez osoby upoważnione.

Ponadto, zależnie od rodzaju incydentu, należy wykonać (ABI zleca odpowiedniej osobie, w szczególności AT):

- Sprawdzenie dzienników systemowych oraz parametrów pracy systemu przed i po wystąpieniu incydentu;
- Sprawdzenie urządzenia oraz systemu operacyjnego, również pod kątem nowych, nieznanych elementów, oraz zachowań, które nie mieszczą się w typowych wzorcach;
- Sprawdzenie list dostępowych routerów, firewalli oraz wykazów kont i uprawnień użytkowników;
- Zapoznanie się z wynikami analizy ruchu w sieci z wykorzystaniem specjalistycznych narzędzi monitorowania sieci.

Jeśli incydent polegał na nieuprawnionym dostępie do systemu, to ABI ustala, czy dostęp uzyskano spoza Instytucji, z wykorzystaniem technik włamań do sieci i systemów informatycznych, czy też z jej obszaru, z wykorzystaniem sieci lokalnej lub urządzeń wchodzących w skład systemu. Należy także ustalić, czy incydent

został spowodowany nieprzestrzeganiem procedur lub błędnymi zapisami w procedurach.

Po dokonaniu analiz ABI sporządza raport, który powinien również zawierać opis wpływu incydentu na infrastrukturę systemu informatycznego, na stan zbiorów informacji oraz ocenę możliwych negatywnych przyszłych skutków incydentu. Raport, jeśli to możliwe, powinien zawierać opinię, czy incydent był przypadkowy, czy spowodowany celowo. Raport powinien zawierać również, w formie wniosków końcowych, zalecenia w celu podniesienia poziomu bezpieczeństwa oraz ograniczania skutków incydentów w przyszłości.

W przypadku stwierdzenia ujawnienia informacji chronionej osobie nieuprawnionej, kierownik Instytucji (lub AI lub kierownik Projektu (lub jego zastępca), jeśli incydent wydarzył się w MF) może powołać komisję do przeprowadzenia postępowania wyjaśniającego w celu pełnego zbadania przyczyn i skutków incydentu, ustalenia sprawcy oraz wielkości poniesionych strat. Powodem powołania komisji może być również: podejrzenie celowego uszkodzenia, zniszczenia bądź nieuprawnionej lub nieuzasadnionej modyfikacji zasobów oraz gdy miał miejsce nieuprawniony dostęp do zasobów systemu. Protokół z postępowania komisja przedkłada kierownikowi instytucji oraz AI lub kierownik Projektu (lub jego zastępca). Wszelkie dalsze działania podejmuje kierownik Instytucji lub AI lub kierownik Projektu (lub jego zastępca), jeśli incydent wydarzył się w MF.

W trakcie prac audytowych ustalono, że nie zanotowano udanych ataków na infrastrukturę informatyczną MF.

Zasady dostępu użytkowników do systemu zostały opisane w rozdziale *5.5.4 Zarządzanie kontami użytkowników*.

Bezpieczeństwo sieci zostało opisane w rozdziale *5.5.10 Bezpieczeństwo sieciowe*.

5.5.8 Zarządzanie kluczem kryptograficznym

W systemie SIMIK klucze kryptograficzne są używane w celu zabezpieczenia aplikacji, przed podsłuchaniem transmisji sieciowej. Proces generowania pary kluczy oraz sposób uzyskania certyfikatu został opisany w *Dokumentacji administracyjnej systemu SIMIK 07-13* oraz w *Instrukcji użytkownika Internet Information Service (IIS) 5.0 Użycie certyfikatów niekwalifikowanych w oprogramowaniu Microsoft IIS 5.0 PL*. Proces ten składa się z kilku etapów. W pierwszym kroku przygotowywana jest, tzw. prośba o certyfikat. Prośba o certyfikat zawiera w sobie klucz publiczny oraz informacje identyfikujące właściciela. W drugim etapie prośba o certyfikat jest wysyłana do urzędu certyfikacji, który odsyła gotowy certyfikat, który poza kluczem publicznym i informacjami identyfikującymi właściciela zawiera dodatkowo informacje o instytucji certyfikującej oraz jest przez tą instytucję podpisany. Urząd certyfikacji może być wyspecjalizowaną w tym celu instytucją lub może być utworzony na jednym z serwerów.

Ministerstwo Finansów zawarło z firmą Unizeto Technologies S.A. umowę na świadczenie niekwalifikowanych usług certyfikacyjnych, dotyczących Certyfikatów Serwerowych Trusted SSL. W ramach wykonania przedmiotu umowy wykonawca zapewnia:

- zgodność świadczonych usług za standardem X.509 v.3;

- wykorzystanie w ramach usług funkcji kryptograficznej RSA-SHA1;
- certyfikat urzędu automatycznie rozpoznawany jako zaufany w przeglądarkach internetowych;
- możliwość weryfikacji statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP.

Ważność certyfikatu, udzielonego w ramach świadczonych usług wynosi 24 miesiące i kończy się w dniu 19 listopada 2009 r. Długość klucza kryptograficznego wykorzystywanego przez system wynosi 1024 bitów (RSA).

Dokumentacja administracyjna systemu SIMIK 07-13 oraz Instrukcja użytkownika Internet Information Service (IIS) 5.0 Użycie certyfikatów niekwalifikowanych w oprogramowaniu Microsoft IIS 5.0 PL są stosowane w przypadku generacji, zmiany, tworzenia kopii zapasowej certyfikatów serwera lub wygaśnięcia kluczy kryptograficznych.

Zgodnie informacjami otrzymanymi w trakcie prac audytowych, do chwili obecnej nie została wdrożona procedura dotycząca przechowywania kluczy kryptograficznych w celu zapewnienia szybkiego dostępu w przypadku awarii sprzętu informatycznego oraz ochrony kluczy przed utratą.

Rekomendacja 20. Dostarczanie i Wsparcie – Zarządzanie kluczem kryptograficznym

Zgodnie z otrzymanymi w trakcie audytu informacjami klucze kryptograficzne przechowywane są w szafie pancernej w pokoju administratorów. Dostęp do nich posiadają jedynie upoważnione osoby.

5.5.9 Zapobieganie, detekcja i korekcja działań złośliwego oprogramowania

Zgodnie z otrzymanymi w trakcie audytu informacjami, w systemie KSI aktualizowane są zabezpieczenia systemowe. Administratorzy konfigurują usługi i zabezpieczenia systemowe oraz aktualizują systemy operacyjne serwerów zgodnie z dokumentem projektowym *Hardering serwerów Windows 2003* dostarczonym przez wykonawcę systemu SIMIK firmę ComArch S.A.. Poprawki i aktualizacje systemowe są wgrywane ręcznie. *Hardering* wymienia usługi wyłączone ze względów bezpieczeństwa. Dokument ten nie został zatwierdzony przez Administratora Informacji. Obecnie nie został wdrożony harmonogram wykonywania wymienionych operacji.

Ochrona przed szkodliwym oprogramowaniem (np. przed wirusami, robakami i koniami trojańskimi, spamem, oprogramowaniem szpiegującym) na stacjach roboczych znajdujących się w Ministerstwie Finansów jest realizowana przez Departament Eksploatacji Systemów Informatycznych. Serwery bazodanowe i aplikacyjne posiadają adresację z puli prywatnej, co powoduje, że nie są one bezpośrednio osiągalne z Internetu. Zabezpieczenia sieci wewnętrznej, w której znajdują się serwery systemu SIMIK, zostały opisane w rozdziale *5.5.10. Bezpieczeństwo sieciowe*.

Na serwerach nie został zainstalowany automatyczny program antywirusowy chroniący przed szkodliwym oprogramowaniem.

Rekomendacja 21. Dostarczanie i Wsparcie – Zapobieganie, detekcja i korekcja działań złośliwego oprogramowania

5.5.10 Bezpieczeństwo sieciowe

Architektura sieci zakłada istnienie sieci zewnętrznej, strefy DMZ z wydzielonymi wewnątrz strefy podsieciami VLAN oraz sieci intranet. Dostęp do sieci DMZ jest zabezpieczony za pomocą rozwiązań sprzętowych, bramki są zlokalizowane zarówno od strony sieci Internet jak i sieci wewnętrznej intranet. Pierwszy poziom kontroli dostępu do zasobów sieciowych stanowią routery ze skonfigurowanymi listami dostępu ACL, przekierowywują one ruch do odpowiednich VLANów, w których znajdują się udostępnione usługi. Druga linia kontroli dostępu do DMZ z sieci Internet, jak również z sieci intranet, stanowią urządzenia PIX.

Sieć jest monitorowana poprzez sondę IDS/IPS które umożliwia monitorowanie sieci pod kątem ewentualnych ataków.

Z informacji uzyskanych od administratorów sieciowych zarówno routery, jak również urządzenia PIX, mają możliwość zapisywania logów do dedykowanego serwera logów. Czas przetrzymywania logów wynosi 90 dni. Zadanie przeglądania logów zostało wpisane do zakresów obowiązków administratorów siec, jednakże brak jest mechanizmu kontrolnego pozwalającego potwierdzić wykonywanie tych obowiązków. Ponadto z informacji uzyskanych podczas prac wynika, że brak jest procedury testowania i przeprowadzania testów penetracyjnych umożliwiających uzyskanie odpowiedzi, czy wdrożone rozwiązania zachowują odpowiednio wysoki poziom bezpieczeństwa.

Rekomendacja 22. Dostarczanie i Wsparcie – Bezpieczeństwo sieciowe

5.5.11 Wymiana danych wrażliwych

Użytkownicy systemu KSI łączą się z bazami danych za pomocą przeglądarki internetowej, wykorzystując protokół HTTPS (ang. *HyperText Transfer Protocol Secure*). HTTPS jest rozszerzeniem protokołu HTTP o szyfrowanie przesyłanych danych. W protokole tym, zamiast używać w komunikacji klient-serwer niezaszyfrowanego tekstu, dane szyfrowane są za pomocą technologii SSL. Szyfrowanie to ma na celu niedopuszczenie do podsłuchania przesyłanych danych przez osoby trzecie. Dodatkowo poprzez analizę certyfikatów klient ma pewność, że serwer, z którym się połączył nie jest fałszywy. Ma to szczególne znaczenie w przypadku aplikacji, gdzie bardzo ważna jest poufność przesyłanych danych. Zapobiega to bowiem przechwytywaniu i zmienianiu tych danych. Użytkownicy systemu KSI otrzymują szczegółowe instrukcje dotyczące adresu, który należy wpisać w przeglądarce w celu podłączenia się w sposób bezpieczny do bazy danych.

5.6. Zarządzanie Konfiguracją

5.6.1 Repozytorium konfiguracji i uaktualnień

Rolę narzędzi wspierających i centralnego repozytorium o konfiguracji KSI SIMIK 07-13 pełnią narzędzia ClearCase (w zakresie zarządzania konfiguracją) i ClearQuest (w zakresie zarządzania zmianami).

5.6.2 Identyfikacja i utrzymanie elementów konfiguracji

Został opracowany *Plan Zarządzania Konfiguracją*. Celem tego dokumentu jest określenie wszelkich działalności i kroków, jakie muszą być podjęte w trakcie prowadzenia projektu, aby skutecznie zarządzać konfiguracją. Opisuje on:

- jakie elementy podlegać będą zarządzaniu konfiguracją i w jaki sposób;
- metody sprawowania nadzoru nad konfiguracją;
- politykę bezpieczeństwa;
- zasady zarządzania zmianami;
- wykorzystywane narzędzia;
- środowisko pracy.

5.6.3 Przegląd integralności konfiguracji

Zasady konfiguracji oprogramowania na serwerach zostały opisane w rozdziale *4.3.1. Planowanie rozwiązań funkcjonalnych*. Po zainstalowaniu serwera dokonywany jest przegląd jego obecnych ustawień oraz wykonywane są zmiany zgodnie z zaleceniami z dokumentu *Hardering serwerów Windows 2003*. Dokument ten został szerzej opisany w rozdziale *4.2.1. Ochrona i dostępność zasobów infrastrukturalnych*.

5.7. Zarządzanie Problemami

5.7.1 Identifikacja i klasyfikacja problemów

Podstawowym dokumentem opisującym zasady identyfikacji i klasyfikacji jest dokument *Service Desk dla Krajowego Systemu Informatycznego SIMIK 07-13*. Dokument określa zasady działania oraz sposób zorganizowania Service Desk i Pomocy Technicznej. W szczególności dokument ma na celu opracowanie procesów, kluczowych ról, usług świadczonych oraz procedur w Service Desk dla KSI SIMIK 07-13.

Procedury zawarte w dokumencie klasyfikują ze względu na krytyczność problemy występujące w systemie. Problemy są dzielone na grupy zadaniowe, tj.:

- problemy merytoryczne;
- problemy obsługowe;
- opracowanie zmiany;
- zgłoszenie dotyczącego incydentu naruszenia bezpieczeństwa.

Użytkownik przegląda bazę wiedzy udostępnioną na stronie internetowej, a w przypadku nie znalezienia rozwiązania problemu, zgłasza wystąpienie błędu poprzez wypełnienie Formularza Zgłoszeniowego w KSI i wysłanie go za pomocą poczty elektronicznej administratorowi merytorycznemu Instytucji Pośredniczącej przy jednoczesnym poinformowaniu odpowiedniego Koordynatora SIMIK.

W przypadku zmiany użytkownik sporządza jej opis i wysyła pocztą elektroniczną do administratora merytorycznego wraz z jednoczesnym poinformowaniem odpowiedniego Koordynatora SIMIK.

Zgłaszanie żądania usunięcia błędu jest zhierarchizowane, odpowiednie role oraz funkcje zostały określone i zdefiniowane w dokumencie *Service Desk dla Krajowego Systemu Informatycznego SIMIK 07-13*

5.7.2 Śledzenie i rozwiązanie problemu

Instrukcja *Service Desk dla Krajowego Systemu Informatycznego SIMIK 07 – 13* definiuje proces przekazywania informacji o zaistniałych problemach poprzez aplikację ClearQuest. Aplikacja ta umożliwia śledzenie zgłoszonych błędów od chwili ich rejestracji do momentu ich rozwiązania. Narzędzie to umożliwia śledzenie pełnej historii obsługi błędów. Dodatkowo rejestrowane są dodatkowe informacje takie jak użytkownik zgłaszający błąd, data zgłoszenia, opis błędu, data usunięcia błędu.

5.7.3 Zamknięcie problemu

Zawarte w ww. dokumencie procedury zgłaszania obsługi problemów umożliwiają zamknięcie zgłoszenia problemu po jego ujawnieniu i skutecznym rozwiązaniu. Zgłoszenia zaistnienia problemu zarejestrowane w aplikacji wspierającej mogą zostać odrzucenie przez administratorów merytorycznych w takim przypadku zgłoszenia takie zostaje również zamknięte. Zamknięcie zgłoszenia problemu jest autoryzowane przez administratora instytucji kontrolującej

5.8. Zarządzanie Danymi

5.8.1 Wymogi biznesowe dla zarządzania danymi

Dane wejściowe do systemu SIMIK są wprowadzane bezpośrednio przez użytkownika lub importowane z pliku XML. Wprowadzane przez użytkownika dane są sprawdzane poprzez system zgodnie z regułami walidacyjnymi przypisanymi do pól aplikacji polegającymi na zastosowaniu masek wprowadzania danych. Zastosowano również wymogi biznesowe na wczytywane. Szczegółowy opis reguł znajduje się w dokumencie *SIMIKXML - Reguły zgodności danych v1.4.1*.

Zgodnie z założeniami biznesowymi interfejs integracji systemu SIMIK składa się z dwóch etapów:

- import i walidacja pliku XML (pod względem schematu oraz reguł dodatkowych);
- ładowanie danych do tablic głównych.

W pierwszym etapie importu danych z pliku do systemu centralnego SIMIK 07-13 następuje sprawdzenie zgodności pliku XML z odpowiednim schematem XSD (XBRL). Jeśli operacja zakończy się powodzeniem następuje zaimportowanie zawartości pliku do bazy danych SIMIK i walidacja danych. W drugim etapie z prawidłowo zaimportowanych i poprawnie zwalidowanych plików XML odbywa się ładowanie danych do tablic aplikacji przy pomocy biznesowych reguł walidacyjnych. Reguły zostały oznaczone kodami, numerami oraz opisane słownie w dokumencie *SIMIKXML - Reguły zgodności danych v1.4.1*.

W trakcie importu wyróżniono błędy rejestrowane z poziomu bazy danych informujące np. o złym typie danych czy szerokości pola oraz błędy wynikające z walidacji reguł biznesowych zapisywane w postaci kodów i nazw błędów. W sytuacji wystąpienia błędnych danych żadne informacje pochodzące z danego pliku XML do systemu centralnego nie zostaną przeniesione. Wymagana jest korekta danych w pliku XML i ponowny ich import.

Administrator posiada możliwość nadzorowania mechanizmu importującego dane. Za pomocą ustawień systemowych ustala interwał wczytywania danych z plików. Podgląd wykonywanych operacji pozwala na określenie optymalnych parametrów pracy systemu. Pomocne są w tym również dane zbierane w systemie zawierające datę, czas przetwarzania operacji oraz numer importu.

Według administratorów dane są przetwarzane w odpowiednim czasie, jednakże w żadnym dokumencie nie zostały określone maksymalne czasy przetwarzania i wymagania na dostępność danych zgodne z potrzebami użytkowników.

Rekomendacja 23. Dostarczanie i Wsparcie – Wymogi biznesowe dla zarządzania danymi

Dane wyjściowe są zgodne z wymaganiami biznesowymi określonymi w dokumencie *Narodowe Strategiczne Ramy Odniesienia 2007-2013 – Wytyczne w zakresie warunków gromadzenia i przekazywania danych w formie elektronicznej*.

W czasie codziennej pracy nie istnieje konieczność przerywania działania systemu, tj. jego restartu. Raz dziennie po godzinach pracy użytkowników zamykana jest baza danych na czas wykonywania kopii zapasowych.

W obecnej chwili następuje kontrola prawidłowości wprowadzonych danych na podstawie automatycznych mechanizmów opisanych powyżej. Do tego celu ma być również używany Oracle Discovery. Weryfikacja jakości wprowadzonych danych następuje na podstawie procedury wewnętrznej opracowanej przez Wydział Administracji i Audytu Systemów Informatycznych Departamentu Koordynacji i Zarządzania Podstawami Wsparcia Wspólnoty MRR.

5.8.2 Procedury składowania i utrzymania danych

Zasady przechowywania nośników z kopiami danych z systemu zostały zdefiniowane w *Procedurze przechowywania nośników z kopiami awaryjnymi danych z systemu*. Wyznacza ona osoby odpowiedzialne za jej stosowanie oraz wskazuje sposób postępowania z nośnikami. Procedura przechowywania, utrzymania i archiwizowania danych jest zgodna z celami biznesowymi, wewnętrzną polityką bezpieczeństwa oraz wymaganiami prawnymi.

Zgodnie z *Procedurą przechowywania nośników* druga kopia znajduje się na dysku zewnętrznym o pojemności 1 TB w pokoju administratorów technicznych systemu KSI, w szafie pancernej.

W trakcie czynności audytowych stwierdzono, iż dokument do chwili obecnej nie został w pełni wdrożony. Zgodnie z *Procedurą przechowywania nośników z kopiami awaryjnymi danych z systemu* nośniki z kopiami danych powinny być opisane w odpowiedni sposób, jednakże w trakcie prac audytowych ustalono, iż nośniki nie są opisywane.

Procedura przechowywania nośników z kopiami awaryjnymi danych z systemu odwołuje się do nieistniejącej *Procedury tworzenia kopii awaryjnych danych.* Ustalono, iż właściwą w odwołaniu jest *Procedura backupu KSI SIMIK 07-13.*

Rekomendacja 24. Dostarczanie i Wsparcie – Procedury składowania i utrzymania danych

5.8.3 System zarządzania biblioteką danych

System zarządzania biblioteką danych, tj. przechowywania danych został opisany w punkcie 5.8.2. *Procedury składowania i utrzymania danych*.

5.8.4 Usuwanie danych

Zasady postępowania z nośnikami informacji w przypadku likwidacji sprzętu komputerowego należącego do KSI SIMIK 07-13 zostały opisane w *Procedurze postępowania z nośnikami informacji w przypadku likwidacji urządzeń komputerowych.* Wdrożona procedura zapewnia w dużej części ochronę danych znajdujących się na sprzęcie i nośnikach wycofanych z eksploatacji i przeznaczonych do przekazania lub zniszczenia.

Zgodnie z zapisami tej procedury wszystkie urządzenia komputerowe powinny być pozbawiane wszelkich nośników informacji w przypadku przekazania ich do

ponownego wykorzystania lub do likwidacji. Za wskazane w *Procedurze* działania jest odpowiedzialny administrator w porozumieniu z właścicielem sprzętu. Procedura nie zawiera obowiązku sporządzenia protokołu likwidacji lub przekazania oraz osób nadzorujących prawidłowe wykonanie procesu.

Rekomendacja 25. Dostarczanie i Wsparcie – Usuwanie danych

W trakcie czynności audytowych stwierdzono, iż do chwili obecnej żadne urządzenia komputerowe nie były przekazywane ani przenoszone w stan likwidacji.

5.8.5 Wykonywanie kopii zapasowych i przywracanie systemów

Podstawowe zasady wykonywania kopii zapasowych i archiwalnych systemu KSI SIMIK 07-13 oraz obowiązki administratorów w tym zakresie zostały zdefiniowane w *Procedurze wykonywania backupu KSI SIMIK 07-13*. Zgodnie z zapisami tego dokumentu na proces tworzenia kopii zapasowych systemu składają się:

- Całościowy backup produkcyjnej bazy danych Oracle, wykonywany każdego dnia po zakończeniu pracy, przy pomocy automatycznych skryptów, do określonego katalogu na serwerze bazodanowym. Skompresowany plik zawierający kopię zapasową jest następnie przegrywany przez administratora na dysk zewnętrzny;
- Backup serwera aplikacyjnego poprzez wykonanie obrazu partycji C podstawowego dysku serwera, każdorazowo po wykonaniu instalacji oprogramowania na serwerze aplikacyjnym;
- Backup repozytorium, w którym przechowuje się dostarczone przez dostawcę kody źródłowe każdej wersji aplikacji KSI SIMIK 07-13, leży w gestii administratorów zatrudnionych w Departamencie Eksploatacji Systemów Informatycznych MF i jest wykonywany zgodnie z przepisami wewnętrznymi Ministerstwa Finansów.

Każdorazowo podczas wykonywania kopii zapasowych tworzony jest pliku logu.

Procedura wykonywania backupu zawiera szczegółowy wykaz automatycznych skryptów wykorzystywanych do tworzenia kopii zapasowych oraz opis czynności administratorów w tym zakresie. Zgodnie z jej zapisami administrator każdego dnia jest zobowiązany do zalogowania się do bazy danych i skopiowania plików zawierającego kopie zapasowe i log na dysk zewnętrzny oraz do przeanalizowania pliku logu ostatniego backupu. Administrator analizuje również logi systemu operacyjnego (dziennik zdarzeń) pod kątem istnienia zdarzeń mających wpływ na proces tworzenia kopii zapasowych.

Podczas prowadzonych prac audytowych potwierdzono istnienie i wykonywanie kopii zapasowych oraz przeglądanie plików logów przez administratorów. Kopie zapasowe produkcyjnej bazy danych nie były jednak wykonywane z regularnością określoną przez procedurę, zaobserwowano nieznaczne odstępstwa.

Rekomendacja 26. Dostarczanie i wsparcie – Wykonywanie kopii zapasowych i przywracanie systemów

Dysk zewnętrzny o pojemności 1 TB zawierający kopie produkcyjnej bazy danych jest przechowywany w pokoju administratorów technicznych systemu KSI, w pancernym sejfie. Klucze do sejfu posiadają wyłącznie wyznaczeni administratorzy.

Procedura wykonywania backupu nie zawiera postanowień dotyczących odtworzenia oraz regularnego testowania kopii zapasowych. Zgodnie z otrzymanymi informacjami kopie zapasowe są testowane ad-hoc. Podczas dotychczasowej pracy systemu nie zaistniała konieczność odtworzenia produkcyjnej bazy danych z kopii zapasowej.

Rekomendacja 27. Dostarczanie i wsparcie – Wykonywanie kopii zapasowych i przywracanie systemów

5.8.6 Wymagania bezpieczeństwa dla zarządzania danymi

Dane wejściowe do systemu SIMIK są wprowadzane bezpośrednio przez operatora lub importowane z pliku XML. Użytkownik uzyskuje dostęp do systemu poprzez bezpieczne połączenie szyfrowane HTTPS.

Dane importowane z pliku XML powinny spełniać wymagania zgodności z odpowiednim schematem XSD (XBRL) oraz walidacji reguł biznesowych opisanych w punkcie *5.8.1. Wymogi biznesowe dla zarządzania danymi*.

Wymagania odnośnie dostępu do danych zostały opisane w *Polityce bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13*. Określono w niej obszar przetwarzania, w którym przetwarzane są zbiory informacji:

- serwery aplikacyjne i bazodanowe znajdujące się w serwerowni MF;
- urządzenia sieciowe znajdujące się w serwerowni MF;
- komputery klienckie (Użytkowników) znajdujące się w Instytucjach.

Do serwerów i urządzeń sieciowych znajdujących się w serwerowni MF mają dostęp jedynie uprawnieni administratorzy. Zagadnienie to zostało opisane w rozdziale *5.9. Zarządzanie środowiskiem fizycznym.*

Zgodnie z *Polityką bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* komputery klienckie (spoza siedziby Głównego Użytkownika) chronione są zgodnie z politykami bezpieczeństwa opracowanymi w danych Instytucjach, korzystających z KSI SIMIK 07-13. Każda Instytucja chroni swoje komputery i jest odpowiedzialna za ich zabezpieczenie.

Uprawnienia dostępu do danych przetwarzanych w systemie SIMIK są przyznawane na podstawie imiennych wniosków. Użytkowników i zakres ich uprawnień w danym programie operacyjnym określają poszczególne instytucje zarządzające, na podstawie zgłoszeń od instytucji pośredniczących. Zagadnienie to zostało opisane w rozdziale *5.6.4. Zarządzanie kontami użytkowników.*

Uprawnienia dostępu do tworzenia kopii zapasowych danych przetwarzanych w systemie SIMIK oraz przechowywanych nośników posiadają imiennie upoważnieni administratorzy.

5.9. Zarządzanie Środowiskiem Fizycznym

5.9.1 Wybranie lokalizacji i sposobu rozmieszczenia

Środowisko produkcyjne (dwa serwery aplikacyjne i dwa serwery bazodanowe) oraz bazy szkoleniowo-testowe systemu KSI SIMIK 07-13 zlokalizowane są obecnie w serwerowni znajdującej się na środkowym piętrze budynku Ministerstwa Finansów. Zarządzaniem i obsługą serwerowni zajmują się wyznaczeni pracownicy Departamentu Eksploatacji Systemów Informatycznych, komórki organizacyjnej odpowiedzialnej za utrzymywanie sprzętu informatycznego MF. Serwery systemu znajdują się w pomieszczeniu współdzielonym z serwerami innych systemów.

Obecnie trwają zaawansowane prace nad przeniesieniem serwerów do nowej lokalizacji. Docelowo środowisko produkcyjne systemu KSI SIMIK 07-13 będzie zlokalizowane w pomieszczeniu wynajmowanym od firmy zewnętrznej, w budynku bezpośrednio sąsiadującym z siedzibą Ministerstwa Finansów.

5.9.2 Środki ochrony fizycznej

W odniesieniu do systemu KSI SIMIK 07-13 brak jest szczegółowych procedur dotyczących zabezpieczeń fizycznych pomieszczeń, w których zlokalizowane są m.in. serwery, aktywne urządzenia sieciowe, wyłączniki zasilania elektrycznego, pomieszczenia administratorów.

Rekomendacja 28. Dostarczanie i wsparcie – Środki ochrony fizycznej

Ogólne zasady dotyczące bezpieczeństwa fizycznego zostały zawarte w Załączniku nr 4 do *Polityki bezpieczeństwa.* Zgodnie z zapisami tego dokumentu serwery i urządzenia sieciowe systemu KSI znajdują się w wyznaczonej serwerowi Ministerstwa Finansów i mają do nich zastosowanie zasady bezpieczeństwa tam obowiązujące. Komputery użytkowników (klienci systemu) chronione są zgodnie z politykami bezpieczeństwa opracowanymi w danych Instytucjach korzystających z KSI. Każda Instytucja chroni swoje komputery i jest odpowiedzialna za ich zabezpieczenie.

5.9.3 Dostęp fizyczny

Wejście do pomieszczenia serwerowni jest zamknięte wzmocnionymi zamkami i chronione przez elektroniczny system dostępu. Karta dostępu do serwerowni jest wydawana przez Dyrektora Departamentu EI, na formalny wniosek. Administratorzy systemu SIMIK zostali imiennie wskazani w piśmie skierowanym do Dyrektora Departamentu EI, po czym została im przyznana stała karta dostępu. Oprócz tego dostęp fizyczny do serwerowni (w tym do serwerów systemu SIMIK) posiadają inni pracownicy Ministerstwa Finansów.

Wejście do pomieszczenia serwerowni nie jest monitorowane systemem kamer CCTV, nie jest prowadzony również dziennik wejść/wyjść. Dla osób trzecich (serwisantów, audytorów) oraz osób, które nie posiadają uprawnień stałego dostępu, pobyt w serwerowni jest możliwy wyłącznie w obecności upoważnionego administratora.

Rekomendacja 29. Dostarczanie i wsparcie – Dostęp fizyczny

W najbliższym czasie planowana jest migracja środowiska produkcyjnego systemu KSI do nowej serwerowni, zlokalizowanej w budynku zarządzanym przez firmę zewnętrzną, obok siedziby Ministerstwa Finansów. Docelowo dane systemu SIMIK (bazy produkcyjne i testowe w zmienionej architekturze, zgodnie z rozdziałem *3.1.1. Określenie architektury informacyjnej*) będą przetwarzane wyłącznie w nowej lokalizacji, w pomieszczeniu przeznaczonym wyłącznie do administracji serwerami Ministerstwa Finansów, bez możliwości dostępu pracowników firm zewnętrznych. Oprócz systemu KSI w serwerowni znajdować się będą również inne systemy zarządzane przez Ministerstwo Finansów.

Po zakończeniu prac związanych z migracją, przetwarzanie danych będzie przez pewien czas (ok. miesiąca) następować w dwóch lokalizacjach równolegle (połączonych łączem światłowodowym), aby w przypadku awarii łącz lub nieprzewidzianych zdarzeń możliwie szybko uruchomić system.

Wejście do budynku, w którym znajduje się pomieszczenie docelowej serwerowni jest chronione przez pracowników ochrony i zabezpieczone elektronicznym systemem dostępu. Wejście do serwerowni znajduje się na parterze budynku za dwoma wzmocnionymi drzwiami, dostęp uzyskuje się na podstawie elektronicznego identyfikatora. Dostęp dla osób trzecich (serwisantów, audytorów) jest możliwy wyłącznie w obecności upoważnionego administratora. Dodatkowo wejście jest monitorowane przez umieszczone nad drzwiami czujniki ruchu.

Obok serwerowni, za przeszkloną szybą znajduje się pomieszczenie dla administratorów.

5.9.4 Ochrona przed czynnikami środowiska naturalnego

Pomieszczenie obecnej serwerowni, znajdującej się w wydzielonym obszarze budynku, nie jest zabezpieczone w system monitorowania warunków środowiskowych (temperatury, wilgotności powietrza). W serwerowni nie zainstalowano również centralnego systemu gaszenia, a jedynie rozmieszczono ręcznie gaśnice CO_2. Pomieszczenie serwerowni jest klimatyzowane, nie istnieje jednak system automatycznie dostosowujący temperaturę i wilgotność w pomieszczeniu do założonych parametrów.

Serwery systemu SIMIK są zlokalizowane bezpośrednio na drewnianej podłodze na końcu pomieszczenia – nie jest zapewniona właściwa ochrona przed wstrząsami, zalaniem oraz odpowiednia ochrona okablowania infrastrukturalnego.

Rekomendacja 30. Dostarczanie i wsparcie – Ochrona przed czynnikami środowiska naturalnego

Pomieszczenie docelowej serwerowni jest na bieżąco monitorowane przez kamery CCTV i jest wyposażone w systemy monitorowania warunków środowiskowych (odczyt temperatury i wilgotności powietrza) oraz centralny, gazowy system gaszenia, uruchamiany w przypadku wystąpienia pożaru. Serwery umieszczone są w zamykanych szafach na podniesionej podłodze, zapewniającej ochronę okablowania i serwerów przed wstrząsami, zalaniem lub innymi nieprzewidzianymi zdarzeniami; w każdej szafie znajdują się czujniki warunków środowiskowych. Serwerownia

wyposażona jest w centralnie sterowany system klimatyzacji, umożliwiający utrzymanie stałej temperatury w pomieszczeniu.

5.9.5 Zarządzanie wyposażeniem pomieszczeń

Do zarządzania serwerami używa się konsoli współdzielonej z innymi systemami zarządzanymi przez Ministerstwo. Istnieje również możliwość zdalnego zarządzania z wewnętrznej sieci Ministerstwa przez pulpit zdalny (Remote Desktop Protocol) i jest ona wykorzystywana do bieżącej administracji.

Do monitorowania warunków pracy serwerów administratorzy systemu SIMIK wykorzystują oprogramowanie Dell OpenManage Server Administrator, dostarczone przed producenta sprzętu. Aplikacja ta umożliwia odczyt w czasie rzeczywistym podstawowych technicznych parametrów pracy serwerów (temperatury procesorów i wnętrza serwerów, ilości obrotów wentylatorów, rozkładu zasilania) oraz odczyt bieżącej konfiguracji sprzętowej. Administrator ma możliwość zdefiniowania wartości ostrzegawczych i krytycznych, po przekroczeniu których następuje alarm i zdefiniowane zdarzenie (np. zamknięcie baz danych, wyłączenie zasilania). Informacje pochodzące z tego systemu są regularnie monitorowane i sprawdzane przez administratorów.

Serwery systemu SIMIK są wyposażone w jeden zasilacz UPS gwarantujący krótkotrwałą (kilkuminutową) dostawę zasilania pozwalającą na bezpieczne zamknięcie systemu w przypadku katastrofy lub awarii. Zgodnie z otrzymanymi informacjami zasilacz UPS był testowany przez administratorów przed instalacją środowiska produkcyjnego, po tym zdarzeniu zasilacz UPS nie był więcej sprawdzany. Nie istnieją również formalne procedury dotyczące utrzymania i regularnego testowania urządzeń zasilających w systemie KSI.

Serwery systemu SIMIK nie są wyposażone w gwarantowane źródło zasilania.

Rekomendacja 31. Dostarczanie i wsparcie – Zarządzanie wyposażeniem pomieszczeń

5.10. Zarządzanie Operacjami

5.10.1 Procedury i instrukcje operacyjne

Dla zapewnienia, że administratorzy prawidłowo wykonują swoje obowiązki zostały opracowane procedury eksploatacyjne takie jak:

- *Dokumentacja administracyjna systemu SIMIK 07-13*;
- *Procedury Wewnętrzne w Wydziale Administracji i Audytu Systemów Informatycznych*.

Powyższe dokumenty zostały opisane szerzej w rozdziale *4.3.1. Planowanie rozwiązań funkcjonalnych*.

Jednakże procedury te nie zawierają takich elementów jak zasady przekazywania obowiązków (formalne przekazanie obowiązków, problemy eksploatacyjne, procedury eskalacji, raportowanie obecnych obowiązków) w celu zapewnienia ciągłości przetwarzania.

Rekomendacja 32. Dostarczanie i Wsparcie – Procedury i instrukcje operacyjne

W celu zapewnienia prawidłowości prowadzonej księgowości *Zarządzeniem* Dyrektora Generalnego Ministerstwa Rozwoju Regionalnego został wprowadzony plan kont obejmujący wykaz kont syntetycznych (dla ewidencji księgowej Ministerstwa, w tym w zakresie finansowania programów operacyjnych współfinansowanych ze środków pochodzących z funduszy strukturalnych oraz dla ewidencji ich refundacji), wykaz kont analitycznych, jak również opisy poszczególnych kont. Zostały również określone szczegółowe zasady budowy kont syntetycznych i analitycznych. Przy dokonywaniu wydatków ze środków funduszy strukturalnych oraz Funduszu Spójności stosuje się oznaczenia służące identyfikacji programu operacyjnego lub grupy programów (w przypadku programów współpracy międzynarodowej) oraz źródła finansowania wydatków, w tym: dwie pierwsze cyfry służą do identyfikacji programów zgodnie z zestawieniem zamieszczonym w załączniku do zarządzenia.

Został również wyszczególniony wykaz kont w zakresie obsługi finansowej środków pochodzących z funduszy strukturalnych, Funduszu Spójności oraz Europejskiego Instrumentu Sąsiedztwa i Partnerstwa wraz z ich szczegółowym opisem.

5.10.2 Rozkład pracy

W celu zapewnienia efektywności w wykorzystaniu systemu wprowadzono zautomatyzowane narzędzia wykorzystywane w celu wykonywania backupów (poza godzinami pracy). Szczegółowy listing automatycznych skryptów tworzących kopie zapasowych oraz opis czynności administratorów w tym zakresie zawiera *Procedura wykonywania backupu* (zagadnienie to zostało opisane szerzej w rozdziale *5.8.5. Wykonywanie kopii zapasowych i przywracanie systemów*). Za prawidłowe wykonanie skryptów odpowiedzialni są administratorzy serwerów.

Nie są wykorzystywane inne narzędzia pracy zautomatyzowanej.

5.10.3 Monitorowanie infrastruktury IT

W *Dokumencie Głównym Polityki Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* został zawarty opis ról i odpowiedzialności dotyczących monitorowania bezpieczeństwa systemu (opisane szerzej w rozdziale *5.5.5. Monitorowanie i testowanie bezpieczeństwa*). Brak jest jednakże opracowanych szczegółowych zasad i wytycznych (procedur) monitorowania infrastruktury teleinformatycznej i związanych z nią zdarzeń.

Na serwerach obsługujących KSI została zainstalowana aplikacja Dell OpenManage Server Administrator. Umożliwia ona w czasie rzeczywistym za pomocą przeglądarki internetowej podgląd takich elementów systemowych jak: stan BIOSu, badanie wentylatora, pamięci operacyjnej, kart sieciowych, portów, zasilacza, procesora, poszczególnych slotów, jak również temperatury czy napięcia. Aplikacja ta posiada również możliwość zapisywania informacji do pliku, jednakże informacje nie są logowane. W trakcie prowadzonych prac nie uzyskano potwierdzenia dokonywania regularnych przeglądów dotyczących monitorowania poszczególnych elementów infrastruktury.

Rekomendacja 33. Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

W trakcie prac audytowych stwierdzono, iż została opracowana *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13*. W analizie tej zostało uwzględnione m.in. zagrożenie dotyczące braku narzędzi do monitorowania bezpieczeństwa. Przy oszacowanym poziomie ryzyka ocenę zabezpieczeń dla tego zasobu oceniono jako „niewystarczającą". Propozycją dodatkowych zabezpieczeń jest zakup oprogramowania służącego do analizy. Brak jest jednakże kompleksowego szacowania ryzyka w zakresie monitorowania infrastruktury IT (ze szczególnym uwzględnieniem najważniejszych aktywów).

Rekomendacja 34. Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

5.10.4 Dokumenty i urządzenia przetwarzające dane wrażliwe

Zgodnie z otrzymanymi informacjami w systemie KSI SIMIK 07-13, na obecnym etapie jego rozwoju, nie są przetwarzane dane wrażliwe (dane osobowe lub niejawne w rozumieniu przepisów odpowiednich ustaw). Szczegółowe informacje dotyczące stosowanych zasad dostępu do danych w KSI SIMIK 07-13 zostały opisane w części *3.1.3 Schemat klasyfikacji danych* niniejszego Sprawozdania.

6. MONITOROWANIE I OCENA

6.1. Monitorowanie i Ocena Wydajności IT

6.1.1 Struktura monitoringu

Procedura zarządzania rozwojem w systemie KSI SIMIK 07-13 definiuje proces rozwoju systemu. Celem procedury jest zdefiniowanie zasad monitoringu, kontroli i zarządzania wydajnością usług systemu. Pozwoli to na zapewnienie założonego poziomu pojemności i wydajności systemu oraz ewolucję systemu zgodnie z potrzebami. Za przestrzeganie zasad wymienionych w procedurze odpowiadają pracownicy Zespołu Infrastruktury Technicznej (w zakresie monitorowania i kontroli wydajności systemu na poziomie MF) oraz Koordynatorzy (w zakresie monitorowania i kontroli wydajności systemu na poziomie poszczególnych instytucji). Zespół Infrastruktury Technicznej analizuje popyt na dostęp do systemu, tzn. ilość użytkowników systemu, ilość użytkowników pracujących jednocześnie, co ma wpływ na wydajność systemu oraz cyklicznie sprawdza wydajność systemu na poziomie zasobów systemu znajdujących się w MF. Koordynatorzy dokonują cyklicznego monitorowania wydajności zasobów sprzętowych w instytucjach, w zakresie sprawdzania wydajności stacji i systemów na komputerach użytkowników systemu. *Procedura zarządzania rozwojem w systemie KSI SIMIK 07-13* ma zastosowanie do działań w zakresie monitoringu i kontroli wydajności systemu. Nie obejmuje ona jednakże zadań związanych z monitorowaniem bezpieczeństwa systemów.

Patrz Rekomendacja 33: Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

6.1.2 Zdefiniowanie i zbieranie danych z procesu monitorowania

W *Procedurze zarządzania rozwojem w systemie KSI SIMIK 07-13* zostało określone, iż:

- analizowany jest popyt na dostęp do systemu, tzn. ilość użytkowników systemu, ilość użytkowników pracujących jednocześnie (co ma wpływ na wydajność systemu);
- monitorowaniu podlegają serwery aplikacyjne i bazy danych dla systemu SIMIK w środowisku produkcyjnym;
- monitorowanie systemu odbywa się przy użyciu standardowych narzędzi zapewnionych na poziomie systemu operacyjnego MS Windows 2003, tj. Monitor wydajności – zakres monitorowania w narzędziu wydajność obejmuje takie liczniki jak: czas procesora, średnia długość kolejki dysku, strony/s.

6.1.3 Działania korygujące

W *Procedurze zarządzania rozwojem w systemie KSI SIMIK 07-13* zostało określone, iż:

- rezultatem monitorowania popytu na dostęp do systemu jest sporządzenie raz w miesiącu *Raportu monitorowania obciążenia systemu KSI SIMIK 07-13*;

- z każdego pomiaru wydajności systemu sporządzana jest krótka notatka z podaniem daty i przebiegu monitorowania, oraz osoby która dokonała monitorowania wydajności;
- w przypadku stwierdzenia nieprawidłowości, tzn. zbyt dużego obciążenia zasobów systemowych, Zespół Infrastruktury Technicznej składa wnioski z uwzględnieniem potrzeb w tym zakresie, lub podejmuje inne działania mające na celu poprawę zaistniałej sytuacji;
- Zespół Infrastruktury Technicznej raz na 6 miesięcy sporządza raport o wydajności zasobów systemu zawierający: informację z cyklicznych notatek sporządzanych z monitorowania, wnioski z przebiegu monitorowania w 6 miesięcznym okresie, wychwycone tendencje co do zwiększającego się obciążenia systemu w określonych zakresach, wnioski co do wykonywania kolejnych pomiarów wydajności, informację o osobach sporządzających raport;
- Koordynatorzy w przypadku stwierdzenia nieprawidłowości sporządzają informację o zmniejszającej się wydajności zasobów systemu w instytucji oraz podejmują działania zmierzające do poprawy sytuacji;
- Zespół Infrastruktury Technicznej MF sporządza plan potrzeb w zakresie infrastruktury sprzętowej i programowej oraz sporządza wnioski do wykonawcy oprogramowania (zlecenia zmiany lub zgłoszenie błędu) o optymalizację działania aplikacji i bazy danych.

Procedura zarządzania rozwojem w systemie KSI SIMIK 07-13 nie uwzględnia jednakże zagadnień związanych z monitorowaniem bezpieczeństwa systemów IT.

Rekomendacja 35. Monitorowanie i Ocena – Działania korygujące

Patrz również Rekomendacja 33: Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

6.2. Monitorowanie i Ocena Kontroli Wewnętrznej

6.2.1 Przegląd kierowniczy

Zagadnienia dotyczące przeglądów i monitorowania zostały opisane w rozdziale *5.10.3. Monitorowanie infrastruktury IT*.

W ramach przeglądu kierowniczego odbywają się spotkania Rady Projektu KSI.

W dokumencie *Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-2013 (SIMIK 07-13)* wymienione są zadania Kierownika Projektu. Należy do nich miedzy innymi monitorowanie, analiza ryzyka i planowanie działań zaradczych oraz bieżąca kontrola zgodności systemu z przyjętymi założeniami projektowymi wraz z ewentualnymi działaniami naprawczymi.

6.2.2 Wyjątki w systemie kontroli

W trakcie prac audytowych ustalono, iż ewentualne odstępstwa w stosowaniu ustalonych procedur powinny być zgłaszane do kierownika projektu, natomiast wszelkie luki w ustanowionym systemie kontroli powinny być przedstawiane Radzie Projektu.

6.2.3 Wspomaganie kontroli wewnętrznej

W ostatnim okresie wykonany został audyt zewnętrzny zakończony *Raportem z audytu informatycznego KSI SIMIK 07-13 w Ministerstwie Finansów* z dnia 19.12.2007 r. Audyt został przeprowadzony na podstawie formalnej umowy zawartej przez Dyrektora Generalnego Ministerstwa Finansów. Przedmiotem umowy było przeprowadzenie audytu informatycznego Krajowego Systemu Informatycznego KSI SIMIK 07-13 w następujących obszarach:

- konstrukcja funkcjonalna systemu;
- rozwiązania techniczne;
- projekt wdrożenia KSI SIMIK 07-13;
- proces wdrażania sytemu;
- polityka bezpieczeństwa systemu.

Celem audytu było dostarczenie aktualnej i obiektywnej, przeprowadzonej z uwzględnieniem uznanych w skali międzynarodowej standardów audytu, oceny zgodności Krajowego Systemu Informatycznego SIMIK 07-13 z wymaganiami Głównego Użytkownika, którego rolę pełni Ministerstwo Rozwoju Regionalnego, oraz oceny, czy zastosowane rozwiązania i procedury zapewniają odpowiedni poziom bezpieczeństwa danych oraz czy system jest już na tyle operacyjny, aby gromadzić wiarygodne informacje w zakresie funkcjonalności przewidzianych do realizacji zgodnie z Porozumieniem o współpracy przy realizacji projektu „Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007-20013 (SIMIK 07-13)" zawartym pomiędzy Ministrem Finansów a Ministrem Rozwoju Regionalnego w dniu 23 lutego 2007 r.

6.2.4 Kontrola wewnętrzna dokonywana w instytucjach zewnętrznych

Zagadnienie dotyczące współpracy z instytucjami zewnętrznymi zostały opisane w rozdziale *5.1.2. Umowy dotyczące poziomu świadczenia usług.* Umowa zawarta z dostawcą oprogramowania nie zawiera możliwości przeprowadzenia kontroli wewnętrznej w miejscach świadczenia usług. Spełnienie tego warunku w przypadku

systemu SIMIK nie jest konieczne, gdyż przedmiotem umowy nie jest udostępnianie usług związanych z infrastrukturą informatyczną. Przedmiotem jest napisanie oprogramowania, zasady współpracy zostały określone w zawartej umowie.

6.2.5 Działania naprawcze

Raport z audytu informatycznego KSI SIMIK 07-13 w Ministerstwie Finansów z dnia 19.12.2007 r. opisany szerzej w rozdziale *6.2.3. Wspomaganie kontroli wewnętrznej* zawiera rekomendacje dotyczące polityki bezpieczeństwa systemu. Na podstawie istniejących dokumentów oraz informacji ze spotkań stwierdzono, iż rekomendacje zostały wdrożone. Brak jest jednakże procedury systematycznego wprowadzania propozycji audytowych. Powinna ona zawierać osoby odpowiedzialne za ocenę, uszeregowanie i nadzór nad wdrożeniem rekomendacji.

Rekomendacja 36. Monitorowanie i Ocena – Działania naprawcze

6.3. Zapewnienie Zarządzania IT

6.3.1 Zarządzanie zasobami

Zasoby systemu SIMIK zostały podzielone pomiędzy Ministerstwo Finansów oraz Ministerstwo Rozwoju Regionalnego i tak:

- Główny dostawca tj. Ministerstwo Finansów jest odpowiedzialne za utrzymanie aplikacji, utrzymanie systemu, administrację bazą danych oraz funkcjonowanie części sprzętowej;
- Główny Użytkownik tj. Ministerstwo Rozwoju Regionalnego jest odpowiedzialne za część merytoryczną dotyczącą administracji aplikacją.

Krytyczne role dla systemu czyli funkcje zostały odpowiednio przypisane do członków zespołów IT, tj. np. funkcje administratorów merytorycznych w instytucjach pośredniczących, zarządzających, MF, MRR, administratorów merytorycznych w instytucji kontrolującej.

6.3.2 Zapewnienie zgodności

W celu weryfikacji stopnia zapewnienia zgodności, System KSI SIMIK 07-13 był objęty zewnętrznym audytem, którego zakres został opisany w rozdziale *6.2.3. Wspomaganie kontroli wewnętrznej*. Jednakże audyt ten nie dotyczył wydajności i efektywności obszaru IT.

Rekomendacja 37. Monitorowanie i Ocena – Zapewnienie zgodności

7. KONTROLE APLIKACYJNE

7.1. Kontrola w Aplikacjach

7.1.1 Przygotowanie i autoryzacja danych źródłowych

Dane źródłowe do systemu KSI SIMIK 07-13 są wprowadzane na dwa sposoby:

- bezpośrednio przez użytkowników systemu, poprzez odpowiednio zaprojektowane formatki w przeglądarce internetowej;
- poprzez import plików XML, pochodzących z dostarczonych przez beneficjentów plików Generatora Wniosków lub Lokalnych Systemów Informatycznych, zawierających dane źródłowe w ustandaryzowanym formacie zgodnym z XML Schema.

Zgodnie z założeniami systemu instytucje bezpośrednio wprowadzające dane są zobowiązane do wyznaczenia odpowiednio kwalifikowanych pracowników oraz zapewnienia formalnych procedur dotyczących tego zakresu. Dla pracowników wszystkich instytucji użytkujących system zorganizowane zostało szkolenie, na którym poruszono problemy właściwego przygotowania i autoryzacji danych źródłowych.

Drugą możliwością wprowadzenia danych do systemu jest bezpośredni import plików XML pochodzących z Lokalnych Systemów Informatycznych. Podczas importu następuje sprawdzenie poprawności danych ze schematem i ewentualne dodanie danych do KSI SIMIK lub odrzucenie pliku. Systemy LSI, z których pochodzą pliki, musiały wcześniej przejść kontrolę integracji i zostać dodane na wbudowaną w system KSI listę zaakceptowanych LSI (posiadać nadany systemowy identyfikator). Obecnie na liście formalnie zgłoszonych LSI znajdują się tylko trzy systemy – system Mazowieckiej Jednostki Wdrażania Programów Unijnych (identyfikator: LSI.0001), system Wojewódzkiego Urzędu Pracy w Krakowie (identyfikator: LSI.0003) oraz system Urzędu Marszałkowskiego Województwa Śląskiego (identyfikator: LSI.0006). W kilkunastu instytucjach prowadzona jest kontrola integracji Lokalnych Sytemów Informatycznych z KSI SIMIK 07-13.

7.1.2 Wprowadzanie danych wejściowych

Zgodnie z założeniami budowy systemu KSI SIMIK, zawartymi w założeniach projektu *Wdrożenie krajowego systemu informatycznego monitoringu i kontroli funduszy UE w okresie 2007 – 2013* system nie eliminuje obiegu dokumentacji papierowej, a jedynie rejestruje, magazynuje i agreguje niektóre dane z tej dokumentacji. Dane wprowadzone do systemu tworzą złożoną bazę danych, którą można filtrować i wydobywać z niej raporty w dowolnych układach.

Dane do systemu są wprowadzane na podstawie dokumentów w wersji papierowej, które przeszły formalną ścieżkę sprawdzania, tj. kontroli poprawności, akceptacji i zatwierdzania, opisaną w *Systemach zarządzania i kontroli* poszczególnych programów operacyjnych oraz wewnętrznych procedurach Instytucji Zarządzających, Pośredniczących i Certyfikujących. Każdorazowo oryginalne dokumenty są przechowywane w instytucji odpowiedzialnej za gromadzenie danych i wprowadzanie do systemu.

Do systemu finansowo-księgowego QWANT dane wprowadzane są przez pracowników Departamentu Ekonomiczno-Finansowego (DEF) na podstawie dokumentów papierowych. System ten nie posiada żadnego interfejsu łączącego go z Krajowym Systemem Informatycznym oraz Lokalnymi Systemami Informatycznymi.

Ewidencja księgowa prowadzona jest przez DEF dla programów realizowanych odpowiednio w ramach Narodowego Planu Rozwoju 2004-2006 (NPR) oraz Narodowych Strategicznych Ram Odniesienia 2007-2013 (NSRO). Wyodrębnienie księgowe tych programów, polegające na prowadzeniu oddzielnych rejestrów księgowych, umożliwia ustalenie stanu środków dla poszczególnych programów operacyjnych i inicjatyw wspólnotowych z podziałem wpływów i wydatków według zasad wynikających dla danego funduszu pomocowego.

DEF dokonuje na kontach księgowych pozabilansowych, księgowań wydatków zadeklarowanych Komisji Europejskiej, kwot wnioskowanych do Komisji Europejskiej oraz wpływów z Komisji Europejskiej, a także odsetek od środków zgromadzonych na rachunkach bankowych w ramach krajowych i regionalnych programów operacyjnych. Ewidencja wydatków zadeklarowanych, kwoty wnioskowanej i wpływów z Komisji Europejskiej (oprócz wpływów z tytułu zaliczek) jest prowadzona w walucie PLN, jak i w walucie EUR – w szczególności do programu operacyjnego i osi priorytetowej. Przewalutowanie środków następuje na podstawie kursu ogłaszanego przez Komisję Europejską na miesiąc, w którym poprawnie wypełnione poświadczenie i deklaracja wydatków oraz wniosek o płatność zostały zarejestrowane przez Instytucję Certyfikującą.

Wpływy z tytułu zaliczek oraz odsetki od środków zgromadzonych na rachunkach bankowych księgowane są w szczegółowości do programu w walucie PLN, jak i w walucie EUR. Przewalutowanie środków następuje na podstawie średniego kursu ogłaszanego przez Narodowy Bank Polski z dnia operacji na rachunku bankowym.

7.1.3 Sprawdzanie właściwości, kompletności i autentyczności

Ze względu na dużą ilość podmiotów wprowadzających dane do systemu oraz przewidywaną dużą liczbę użytkowników KSI SIMIK 07-13 w poszczególnych Instytucjach zdecydowano, iż w systemie zostaną wbudowane mechanizmy kontrolne, służące walidacji i kontroli poprawności wprowadzanych danych. Wszystkie stosowane mechanizmy zostały zapisane w *Specyfikacjach przypadków użycia*, tj. uzgodnionych wspólnie przez Ministerstwo Rozwoju Regionalnego oraz Ministerstwo Finansów dokumentach, w których zdefiniowano podstawowe scenariusze wprowadzania danych do systemu (danych pochodzących z różnych funkcjonalności systemu – wniosków aplikacyjnych, umów, wniosków o płatność, deklaracji IC, prowadzonych kontroli na miejscu, itp.) oraz określono przewidywany wygląd formatek do wprowadzania danych.

Każda *Specyfikacja przypadków użycia* zawiera nazwy pól służących do wprowadzania danych oraz pól wyliczalnych wraz z określeniem, czy dane pole ma być widoczne na formularzu oraz dostępne do edycji dla użytkownika. Obok nazwy

pola zdefiniowano, jakie warunki walidacyjne dotyczące wpisywanych wartości muszą być spełnione, aby system pozwalał zapisać dane do bazy danych.

System wymusza poprawność fizyczną wprowadzanych danych – standardowo wszystkie pola zawierające liczby (np. wartość ogółem wniosku o dofinansowanie/umowy/decyzji/wniosku o płatność, kwota wydatków kwalifikowanych, kwota dofinansowania, informacje dotyczące montażu finansowego, źródeł finansowania, itp.) posiadają formatowanie numeryczne z dokładnością do dwóch (lub w przypadku kursu miejsc po przecinku i nie jest możliwe wprowadzenie wyrażenia nie będącego liczbą. Podobnie pola dotyczące dat (np. data rozpoczęcia/zakończenia realizacji projektu, data podpisania umowy, itp.) mogą zawierać tylko daty w ujednoliconym formacie. Pola tekstowe mogą zawierać wyrażenia alfanumeryczne o określonej długości, nie większej niż przeznaczone miejsce w bazie danych.

Podczas wprowadzania danych sprawdzana jest również ich poprawność logiczna – system uniemożliwia zapisanie danych zawierających np. ujemne kwoty, daty realizacji projektu spoza okresu programowania, daty wewnętrznie sprzeczne (np. kiedy data zakończenia projektu jest wcześniejsza niż data jego rozpoczęcia), wartości spoza dopuszczalnego zakresu. Każdorazowo w przypadku wprowadzania rozbicia kwot (np. wydatki kwalifikowane = dofinansowanie + wkład własny) system sprawdza, czy sumy z odpowiednich pól są ze sobą zgodne. W przypadku niezgodności tych warunków natychmiastowo po opuszczeniu pola wyświetla się informacja, jaki warunek logiczny nie jest spełniony.

Dane pochodzące ze standardowych list są zapisane we wbudowane w system słowniki, a użytkownik wprowadzający dane z reguły nie ma możliwości edycji tych informacji lub wyboru danych spoza słownika. Podobnie jest w przypadku, gdy w danym polu musi być zachowana jednolita numeracja (np. numeracja wniosków aplikacyjnych/umów/wniosków o płatność określona w Załączniku nr 2 do *Wytycznych Ministerstwa Rozwoju Regionalnego w zakresie gromadzenia i przekazywania danych w formie elektronicznej*) – system automatycznie nadaje numer na podstawie wprowadzonych informacji o projekcie i użytkownik nie ma możliwości zmiany tej części numeru.

W przypadku zmiany liczby porządkowej danego dokumentu system automatycznie wymusza (po poinformowaniu użytkownika) zmianę numeracji we wszystkich dokumentach wykorzystujących ten numer. Przykładowo próba zmiany numeru wniosku aplikacyjnego skutkuje automatyczną zmianą numeracji umowy i wniosków o płatność. Rozwiązanie to zapewnia integralność danych w przypadku konieczności edycji/zmiany wprowadzonych informacji.

Przed zapisem do bazy danych następuje dodatkowa walidacja i sprawdzenie, czy wprowadzone dane na danym etapie cyklu życia projektu są zgodne z wcześniejszymi informacjami pochodzącymi z dokumentów związanych. W przypadku wykrycia nieścisłości użytkownik jest informowany o polach, w których dane nie spełniają warunków walidacyjnych i musi poprawić błędne dane przed zapisem do bazy. Dopiero po spełnieniu wszystkich warunków walidacyjnych system zapisuje dane z formatki do bazy danych i informuje użytkownika o poprawności zapisu.

Bezpośrednio po zapisie do bazy danych dany dokument jest widoczny na liście i jest możliwa zmiana/edycja lub aktualizacja podanych wcześniej informacji. Po podaniu poprawnych danych przez użytkownika następuje nadpisanie starych wartości. W przypadku umów o dofinansowanie, w których konieczne jest zawarcie aneksów, wszystkie informacje dotyczące starej wersji umowy są zawarte w systemie i nie są nadpisywane, lecz tworzona jest nowa wersja umowy/decyzji, posiadająca własny numer porządkowy. Zgodnie z otrzymanymi informacjami takie rozwiązanie zostało zaimplementowane, gdyż do archiwalnej wersji umowy mogą już być zawarte wnioski o płatność. System jednakże nie odróżnia w precyzyjny sposób aktualnej wersji umowy/decyzji od archiwalnych (np. można nadać im dowolną szczegółową numerację).

Rekomendacja 38. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

Po dodaniu dokumentu istnieje możliwość jego usunięcia, lecz tylko w przypadku, gdy do danego dokumentu nie ma zarejestrowanych żadnych dokumentów pochodnych. Przykładowo nie jest możliwe usunięcie wniosku o dofinansowanie, jeśli w systemie zarejestrowano umowę dotyczącą danego wniosku. Podobnie nie jest możliwe usunięcie umowy, w przypadku gdy istnieje zarejestrowany w systemie wniosek o płatność – najpierw należy skasować wszystkie wnioski, a dopiero potem związaną z nimi umowę i ewentualnie wniosek aplikacyjny. Rozwiązanie takie pomaga utrzymać integralność i wiarygodność przetwarzanych danych w systemie.

Drugą możliwością wprowadzania danych do systemu jest możliwość zautomatyzowanego wprowadzania danych zawartych w plikach XML. Aby import danych odbył się poprawnie, pliki muszą być odpowiednio przygotowane, zgodne z opublikowanym schematem XSD. Podczas importu danych użytkownik wskazuje plik do importu (pochodzący z Generatora Wniosków lub Lokalnego Systemu Informatycznego), który zostaje zaimportowany do tymczasowej bazy SIMIKXML.

Na tym etapie następuje porównanie importowanego pliku ze schematem XSD. W przypadku braku zgodności choćby jednego elementu (np. brak znacznika, za duża ilość znaczników, brak właściwej kolejności tagów) plik zostaje odrzucony, o czym system informuje użytkownika odpowiednim komunikatem.

W przypadku, gdy plik przejdzie pozytywną weryfikację zgodności ze schematem następuje dodatkowa walidacja zgodności logicznej z systemem KSI. System sprawdza, czy wszystkie importowane dane spełniają opisane powyżej „zaszyte" mechanizmy kontrolne (importowane są poprawne kwoty, daty w odpowiednim formacie, dane tekstowe o określonej długości; czy wymagane pola są wypełnione; czy wartości w odpowiednich pola są zgodne z danymi słownikowymi, itp.). W przypadku wystąpienia błędów w trakcie walidacji plik nie będzie zaimportowany do systemu KSI, a pełna lista błędów wyświetlona zostanie użytkownikowi. W przypadku poprawnego przejścia tej walidacji dane zostaną przeniesione do bazy produkcyjnej KSI SIMIK 07-13.

Podczas importu brane pod uwagę są również ogólne warunki poprawności, wynikające ze specyfiki procesów biznesowych odzwierciedlonych w systemie. Przykładowo nie można zaimportować wniosku o płatność, jeśli w systemie brak jest

umowy o dofinansowanie odnoszącej się do tych wniosków; nie można również dodać umowy do nie zatwierdzonego wniosku aplikacyjnego. Do systemu nie można zaimportować pliku o tej samej nazwie co poprzednio importowany. W przypadku importu pliku zawierającego dane odnoszące się do już istniejącego w bazie KSI SIMIK 07-13 wniosku aplikacyjnego/umowy/wniosku płatniczego system dokonuje aktualizacji danych odpowiedniego dokumentu, nie informując jednak użytkownika o dokonanych modyfikacjach.

Rekomendacja 39. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

Użytkownicy systemu SIMIK posiadają również możliwość automatycznego usuwania dokumentów. W takim przypadku użytkownik musi załadować do systemu odpowiednio przygotowany plik XML. Usuwanie musi jednak podlegać wyżej opisanym regułom – nie można usunąć umowy, gdy istnieją wnioski o płatność, itp.

Pozostawienie użytkownikom różnych Instytucji możliwości automatycznego usuwania danych może prowadzić do braku zgodności i integralności przetwarzanych w KSI informacji. Zgodnie z otrzymanymi informacjami w chwili obecnej odbywają się konsultacje pomiędzy MRR a zaangażowanymi Instytucjami w sprawie ustalenia szczegółowych procedur usuwania danych z systemu KSI. Obecnie nie istnieją formalne wytyczne dotyczące tego obszaru.

Rekomendacja 40. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

W systemie finansowo-księgowym QWANT zapisy księgowe posiadają automatycznie nadane kolejne numery pozycji. Są dokonywane w sposób zapewniający ich trwałość, a obroty liczone są w sposób ciągły.

7.1.4 Sprawdzanie integralności i wiarygodności

Utrzymanie integralności i wiarygodności danych dokonuje się poprzez opisane powyżej aplikacyjne mechanizmy kontrolne.

Ponadto system KSI SIMIK 07-13 został zaprojektowany w ten sposób, aby przetwarzać minimalną ilość danych wymaganych przez prawo wspólnotowe oraz niezbędną do potrzeb zarządzania i kontroli programów operacyjnych. Przetwarzanie danych w systemie polega więc głównie na gromadzeniu informacji pochodzących z papierowych dokumentów oraz wykonywanie standardowych zapytań do bazy danych *Oracle* przez aplikację *Oracle Discoverer* i przesyłanie tych informacji do wskazanego systemu Komisji Europejskiej.

Identyfikacja i poprawianie błędnych informacji nie zakłóca przetwarzania poprawnych danych – dane dotyczące odrębnych dokumentów przechowywane są w oddzielnych rekordach w bazie danych, a przypadku edycji lub zmiany informacji dana formatka jest dostępna jedynie dla osoby poprawiającej dane.

Każda operacja skutkująca zmianą wartości pola w bazie danych (jak np. dodanie, usunięcie, edycja wniosku aplikacyjnego/umowy o dofinansowanie/wniosku

o płatność, przeliczenie wartości w polach numerycznych) zapisywana jest w historii zmian. Historia ta nie jest widoczna dla użytkownika aplikacji (nie jest w ogóle dostępna z poziomu aplikacji), ale możliwe jest uzyskanie tych informacji z poziomu aplikacji *Oracle Discoverer*. Standardowo historia zmian zawiera informacje o osobie, która utworzyła dane pole, osobie dokonującej zmiany i dacie dokonania zmiany, nazwie zmienianego pola oraz starej i nowej jego wartości.

Podczas prowadzonych badań audytowych stwierdzono, iż uzyskanie informacji dotyczących historii zmian danych (przykładowo ustalenie tożsamości osoby, która usunęła dany wniosek aplikacyjny/umowę/wniosek o płatność, loginy osób wprowadzających dane do systemu i importujących pliki XML) jest czasochłonne i wymaga specjalistycznej wiedzy informatycznej – trzeba wykonać niestandardowy raport przy pomocy aplikacji *Oracle Discoverer*.

Rekomendacja 41. Kontrole aplikacyjne – Sprawdzanie integralności i wiarygodności

Funkcjonalność systemu finansowo-księgowego QWANT pozwala na ustalenie osoby odpowiedzialnej za dokonanie zapisu księgowego – dostępna jest historia operacji.

Wszystkie dostępne w systemie księgowym wydruki i zestawienia pogrupowane są w rozwijanych grupach zleceń. Korzystając z nich można uzyskać dostęp do kilkudziesięciu zestawień (takich jak np. zestawienie obrotów i sald).

7.1.5 Przegląd danych wyjściowych i usuwanie błędów

System KSI SIMIK 07-13 będzie przekazywał dane do wskazanego przez Komisję Europejską systemu SFC2007, zgodnie z dokumentacją systemu udostępnioną Krajom Członkowskim. W chwili obecnej systemy KSI oraz SFC2007 nie są zintegrowane, ewentualne opracowanie funkcjonalności umożliwiającej przepływ informacji pomiędzy tymi systemami nastąpi po uzgodnieniu i zaimplementowaniu ostatecznej specyfikacji systemu SFC2007. Do tego czasu wprowadzanie informacji do systemu SFC2007 następować będzie bezpośrednio przez użytkownika.

W odniesieniu do systemu finansowo-księgowego QWANT, przegląd danych wyjściowych opiera się na sporządzaniu w okresie sprawozdawczym zestawień obrotów i sald oraz innych sprawozdań.

7.1.6 Autentyczność i integralność transakcji

Patrz punkt *7.1.5 Przegląd danych wyjściowych i usuwanie błędów*

8. USTALENIA I REKOMENDACJE

Niniejszy rozdział podsumowuje rekomendacje, które są wynikiem przeprowadzonych prac w ramach audytu systemu KSI.

Poszczególne kwestie analizowane były z perspektywy potencjalnego wpływu, jaki mogą mieć w zakresie obsługi informatycznej środków pochodzących z UE. Kwestiom nadane zostały priorytety zgodne z następującymi definicjami:

- Wysoki – zagadnienia wymagające natychmiastowej reakcji kierownictwa jednostki podlegającej badaniu, ustalenia mają wpływ na zastrzeżenia w opinii z audytu zgodności.
- Średni – zagadnienia istotne w kontekście środowiska kontroli jednostek podlegających audytowi i wymagające zajęcia się nimi przez kierownictwo jednostki, ustalenia pośrednio mogą mieć wpływ na zastrzeżenia w opinii z audytu zgodności.
- Niski – zagadnienia wymagające podjęcia działań zmierzających do poprawy efektywności systemu zarządzania i kontroli.

W trakcie naszych prac zostały zidentyfikowane łącznie: 5 kwestii o priorytecie średnim oraz 36 kwestii o priorytecie niskim.

Brak jest rekomendacji o priorytecie wysokim, które mogłyby mieć bezpośredni wpływ na zastrzeżenia w opinii z audytu zgodności.

Stan wdrożenia wydanych zaleceń będzie przedmiotem monitorowania w trakcie rocznych audytów systemów zarządzania i kontroli.

8.1. Planowanie i organizacja – Model architektury informacyjnej instytucji

Priorytet	Niski
Ustalenia	Zgodnie z otrzymanymi informacjami model architektury informacyjnej systemu KSI SIMIK 07-13 nie został formalnie zatwierdzony przez Właściciela systemu – dokument *Architektura techniczna systemu KSI SIMIK 07-13* jest dostępny jedynie w wersji roboczej.
Implikacje	Brak zatwierdzonego modelu architektury informacyjnej systemu może uniemożliwić skuteczne zarządzanie zmianami architektury informatycznej.
Rekomendacje	Zaleca się akceptację i formalne zatwierdzenie dokumentów zawierających opis architektury informacyjnej (opis techniczny) systemu KSI SIMIK 07-13.
Odpowiedź	Odpowiedź MF: Dokument zawierający opis architektury zostanie przedłożony do akceptacji i formalnego zatwierdzenia przez Właściciela systemu.
Termin wdrożenia	do 31 lipca 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.2. Planowanie i organizacja – Słowniki danych i reguły składni danych

Priorytet Niski

Ustalenia W trakcie audytu ustalono, iż za zarządzanie słownikami wbudowanymi w system odpowiada Administrator Merytoryczny w Instytucji Koordynującej. Jedyne wytyczne dotyczące zarządzania słownikami w systemie KSI zostały zawarte w Procedurach Wewnętrznych Wydziału Administracji i Audytu Systemów Informatycznych Departamentu Koordynacji i Zarządzania PWW MRR. Zgodnie z zapisami tego dokumentu Naczelnik Wydziału wyznacza pracownika odpowiedzialnego za wprowadzenie zmian w danych słownikowych w KSI. Następnie zmiana jest realizowana przez AM IK NSRO lub pracownika Ministerstwa Finansów, po czym Kierownictwo Departamentu zatwierdza dokumentację.

Opisana procedura nie zawiera jasno określonej ścieżki akceptacji zmian danych słownikowych (z treści procedury wynika, iż zatwierdzenie dokumentacji przez Kierownictwo Departamentu następuje po wprowadzeniu zmian) oraz szczegółowego wykazu, za jakie słowniki odpowiadają Administratorzy Merytoryczni IK NSRO, a za jakie Administratorzy Techniczni w Ministerstwie Finansów.

Implikacje Brak szczegółowych procedur dotyczących zarządzania wbudowanymi w system słownikami danych może prowadzić do nieautoryzowanych zmian w słownikach i tym samym do braku integralności danych w systemie.

Rekomendacje Zaleca się dokonanie modyfikacji istniejących procedur dotyczących zarządzania słownikami wbudowanymi w KSI SIMIK 07-13 o szczegółowe wytyczne dotyczące inicjacji procesu, odpowiedzialności za aktualizację właściwych danych słownikowych, osobach aprobujących te zmiany, administratorach wprowadzających zmiany do systemu itp.

Odpowiedź Odpowiedź MRR:

W procedurach wewnętrznych Wydziału Administracji i Audytu Systemów Informatycznych (zatwierdzonych 25 kwietnia 2008 r.) w pozycji „6.12 Aktualizacja słowników KSI SIMIK 07-13” jest opisana procedura aktualizacji słowników.

	W związku z brakiem zmian w słownikach KSI po dacie zatwierdzenia procedur, nie została ona jeszcze zastosowana. Powyższa procedura zostanie poddana weryfikacji, zgodnie z zakresem opisanym w rekomendacji.
Termin wdrożenia	Wdrożona (w opinii MRR)
Stanowisko Instytucji Audytowej	Rekomendacja została zmodyfikowana.

8.3. Planowanie i organizacja – Szacowanie i zarządzanie ryzykiem IT

Priorytet Niski

Ustalenia W trakcie prac audytowych stwierdzono, iż istnieją ogólne dokumenty dotyczące analizy ryzyka w KSI SIMIK 07-13. Jednakże nie zostały w nich uwzględnione ryzyka wynikające z procesów biznesowych mających bezpośredni wpływ na pracę systemu. Nie określono zasad (harmonogramu) aktualizacji dokumentów określających ryzyka ani odpowiedzialności za jego szacowanie. Nie zostały również określone zasady stałego monitorowania zidentyfikowanych ryzyk, jak również pojawiania się nowych zagrożeń.

Nie zostały zidentyfikowane procesy odpowiedzi na występujące w systemie informacyjnym ryzyka w celu złagodzenia ewentualnych strat (przy uwzględnieniu takich strategii działania jak unikanie, redukcja, przeniesienie lub akceptacja).

Nie został opracowany plan postępowania w przypadku wystąpienia ryzyka.

Implikacje Brak analizy ryzyka związanego z bezpieczeństwem systemów informatycznych oraz planu postępowania w przypadku wystąpienia ryzyka może spowodować zwiększenie podatności systemu na awarię lub nieautoryzowany dostęp będący wynikiem błędu lub celowego działania.

Rekomendacje Zaleca się przeprowadzenie kompleksowej analizy ryzyka (bądź weryfikację i uzupełnienie obecnej) z uwzględnieniem procesów biznesowych mających bezpośredni wpływ na pracę systemów informatycznych.

Zaleca się także przygotowanie harmonogramu aktualizacji dokumentów dotyczących analizy ryzyka oraz wyznaczenie osób odpowiedzialnych za ten proces, jak również opracowanie zasad stałego monitorowania zidentyfikowanych ryzyk oraz pojawiania się nowych zagrożeń.

Ponadto, zaleca się opracowanie i wdrożenie planu postępowania w przypadku wystąpienia ryzyka, który uwzględniałby takie elementy jak np.: odpowiedź na poszczególne ryzyka (z uwzględnieniem kosztów, potencjalnych korzyści, odpowiedzialności), zgodę właścicieli procesów na ryzyko wewnętrzne (szczątkowe) oraz na

	podejmowane działania zabezpieczające, monitorowanie wykonania planu, raportowanie wyjątków, itp.
Odpowiedź	Odpowiedź MF: Zostanie zweryfikowana i uzupełniona analiza ryzyka, uwzględniająca procesy biznesowe wraz z uzupełnieniem o harmonogram aktualizacji dokumentu, osoby odpowiedzialne i monitorowanie zidentyfikowanych zagrożeń oraz o plan postępowania w przypadku wystąpienia ryzyka.
Termin wdrożenia	do 30 września 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.4. Zakup i Wdrożenie – Ochrona i dostępność zasobów infrastrukturalnych

Priorytet Niski

Ustalenia Za prawidłowe wykonanie konfiguracji i zabezpieczenie serwerów odpowiedzialni są ich administratorzy. Jedynie oni wykonują wszystkie niezbędne czynności (w tym również instalowanie wszystkich pojawiających się aktualizacji i poprawek). Administrator pobiera odpowiednie pliki ze strony producenta oprogramowania, po czym instaluje je ręcznie na poszczególnych maszynach. Brak jest jednakże formalnie określonej odpowiedzialności za wykonywanie procesu konfigurowania, zabezpieczania i aktualizacji serwerów.

Po instalacji serwera dokonywany jest przegląd jego obecnych ustawień oraz wykonywane są zmiany zgodnie z zaleceniami z dokumentu *Hardering serwerów Windows 2003*. Dokument ten nie jest jednakże formalnie zatwierdzonym przez kierownictwo.

Implikacje Brak sprecyzowanej odpowiedzialności za wykonywanie procesu konfigurowania, zabezpieczania i aktualizacji serwerów może skutkować nieaktualnymi wersjami oprogramowania, a w konsekwencji może prowadzić do zwiększonych możliwości naruszenia bezpieczeństwa.

Rekomendacje Zaleca się formalne opracowanie wytycznych i zasad zabezpieczenia urządzeń służących do przetwarzania danych (serwerów).

Zaleca się określenie odpowiedzialności za wykonywanie procesu konfigurowania, zabezpieczania i aktualizacji serwerów.

Zaleca się regularne wykonywanie przeglądów i aktualizacji wszystkich komponentów infrastruktury.

Odpowiedź Odpowiedź MF:

Procedura opisująca zasady zabezpieczeń zostanie przygotowana.

Osobą odpowiedzialną za konfigurację, zabezpieczanie i aktualizację serwerów MS Windows systemu KSI SIMIK 07-

	13 jest pracownik zespołu technicznego SIMIK. Pozostałe elementy infrastruktury będą cyklicznie przeglądane i aktualizowane przez pracowników działu technicznego SIMIK, zgodnie z ich kompetencjami.
Termin wdrożenia	do 30 września 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.5. Zakup i Wdrożenie – Planowanie rozwiązań funkcjonalnych

Priorytet Niski

Ustalenia W celu użycia i wykorzystywania rozwiązań funkcjonalnych i technicznych został opracowany szereg procedur.

Jednakże dokumenty te nie zawierają zapisów dotyczących odpowiedzialności za przeglądy i aktualizację treści procedur w przypadku wprowadzania zmian lub powstawania nowych systemów oraz częstotliwości wykonywania tego procesu.

Implikacje Brak sprecyzowanego wymogu dokonywania przeglądów i aktualizacji treści procedur, częstotliwości wykonywania, jak również przypisanej odpowiedzialności za ten proces może skutkować nieaktualną treścią tych procedur, a w konsekwencji może prowadzić do braku przydatności tych dokumentów dla użytkowników.

Rekomendacje Zaleca się weryfikację i uzupełnienie wszystkich procedur i instrukcji o wymóg dokonywania przeglądów i aktualizacji treści, określenie częstotliwości wykonywania przeglądów tych dokumentów, jak również przypisanie odpowiedzialności za ten proces.

Zaleca się regularne wykonywanie przeglądów i aktualizacji wszystkich istniejących procedur i instrukcji.

Odpowiedź Odpowiedź MRR:

W procedurach wewnętrznych Wydziału Administracji i Audytu Systemów Informatycznych (zatwierdzonych 25 kwietnia 2008 r.) w pozycji „6.11 Opracowanie i aktualizowanie dokumentacji dla Użytkownika KSI (SIMIK 07-13) lub procedur wewnętrznych Wydziału III lub procedur, zaleceń i wytycznych dla odbiorców zewnętrznych" jest opisana właściwa procedura. Nie została określona częstotliwość. Przyjęto rozwiązanie elastyczne, kiedy to Naczelnik Wydziału III – biorąc pod uwagę realizowane zmiany – zleca przygotowanie/aktualizację dokumentu.

Powyższa procedura zostanie poddana weryfikacji, zgodnie z zakresem opisanym w rekomendacji.

Odpowiedź MF:

	W odniesieniu do rekomendacji z tego punktu, zostanie dokonany przegląd opracowanych procedur i dokumentacji. Przegląd będzie miał na celu zdefiniowanie zasad dokonywania cyklicznych weryfikacji i aktualizacji opracowanej dokumentacji.
Termin wdrożenia	Wdrożona (w opinii MRR) Odpowiedź MF: do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.6. Zakup i Wdrożenie – Transfer wiedzy do użytkowników końcowych

Priorytet Niski

Ustalenia Ministerstwo Rozwoju Regionalnego z zakresu obsługi aplikacji KSI organizuje szkolenia dla Administratorów Merytorycznych z poszczególnych Instytucji Zarządzających. Następnie osoby te powinny przeszkolić pracowników swoich instytucji. W MRR prowadzony jest rejestr szkoleń.

Nie został jednakże opracowany formalny model procesu szkoleń dla pracowników. Szkolenia odbywają się jedynie po zgłoszeniu przez poszczególne instytucje oraz po wdrażaniu kolejnych grup funkcjonalności. Nie jest również weryfikowane, czy wszyscy pracownicy obsługujący system KSI zostali przeszkoleni.

Implikacje Brak sformalizowanego procesu przekazywania wiedzy użytkownikom końcowym (np. o nowych funkcjonalnościach systemu), jak również brak zapewnienia, że szkoleniami zostały objęte osoby ze wszystkich Instytucji zgłaszających takie zapotrzebowanie, może prowadzić do mało wydajnego i nieefektywnego użycia systemu przez użytkowników, jak również może powodować zwiększoną ilość popełnianych błędów przez nie przeszkolonych pracowników.

Rekomendacje Zaleca się opracowanie i wdrożenie wytycznych dotyczących zasad prowadzenia regularnych szkoleń dla pracowników poszczególnych instytucji zawierających takie informacje jak sposób przekazywania wiedzy pracownikom (użytkownikom końcowym) na przykład w formie prezentacji czy dokumentacji szkoleniowej, sposób przekazywania informacji zwrotnej od użytkowników, itp.

Zaleca się również prowadzenie regularnej weryfikacji, czy szkoleniami zostały objęte osoby ze wszystkich Instytucji zgłaszających takie zapotrzebowanie.

Odpowiedź Odpowiedź MRR:

Do chwili obecnej odbyły się 63 szkolenia dotyczące obsługi KSI SIMIK 07-13 skierowane do AM IZ, AM I i użytkowników systemu, w których wzięło udział 778 osób.

Analizując liczbę błędów popełnianych w trakcie

wprowadzania danych przez użytkowników – dotyczy niewielkiego procentu wszystkich wprowadzonych danych – można stwierdzić, iż działania szkoleniowe prowadzone są skutecznie a kryteria doboru uczestników szkoleń i sposób przekazywania wiedzy są prawidłowe.

Model procesu szkoleń

1. Plany wdrożeń. Formalny model procesu szkoelń dla użytkowników zawarty jest w tzw. planach wdrożenia podpisywanych z jednej strony przez IK NSRO z drugiej zaś przez poszczególną instytucję zarządzającą danym programem operacyjnym. W planie zawarte są między innymi następujące informacje:

- ilość i wielkość grup szkoleniowych,

- zakres działań szkoleniowych,

- harmonogram działań szkoleniowych,

- zasady uczestnictwa

Plany wdrożenia zostały podpisane ze wszystkimi instytucjami zarządzającymi: zarówno krajowymi jak i regionalnymi.

2. Coaching. Przyjęto kaskadowy model szkoleń. Tzn w szkoleniach organizowanych przez IK NSRO przede wszystkim uczestniczą administratorzy merytoryczni w poszczególnych instytucjach. Takie wymaganie jest określane w planach wdrożeń i pismach zapraszających na szkolenia. Administratorzy po przeszkoleniu są zobowiązani do transferu wiedzy w instytucjach w których są zatrudnieni. AM IZ ma obowiązek prowadzenia działań szkoleniowych dla użytkowników KSI zgodnie z wytycznymi Ministra Rozwoju Regionalnego *w zakresie gromadzenia i przechowywania danych w formie elektronicznej – Procedura zgłaszania użytkownika do Krajowego Systemu Informatycznego SIMIK 07-13 (nadawanie, zmiana, wygaśnięcie uprawnień) oraz zakres obowiązków administratorów merytorycznych)* i Administratorów Merytorycznych instytucji niższego szczebla.

3. Kryteria doboru uczestników szkoleń z zakresu obsługi KSI SIMIK 07-13 są określane w planach wdrożeń i w pismach zapraszających na w/w. szkolenia (np. pismo nr DPW-III-079-7-PE/08). Zakres merytoryczny szkoleń jest dostosowany do potrzeb szkolonej grupy.

Planowane działania wynikające z zaleceń audytu:

- weryfikacja stanu przeszkolenia użytkowników KSI SIMIK 07-13

Zostaną podjęte działania zmierzające do regularnej

	weryfikacji stanu przeszkolenia pracowników poszczególnych instytucji. Do 15 lipca 2008 r. zostana przekazane AM IZ zmodyfikowane *„Wzory wniosków o nadanie i zmianę uprawnień do KSI 07-13”* w ktróych zostanie zawarte pole wraz z pytaniem czy i w jakim zakresie użytkownik został przeszkolony z obsługi systemu. Umożliwi to weryfikację czy wszystkie zgłaszane do systemu osoby mają wiedzę stosowną by z niego korzystać. Dodatkowo możliwe będzie lepsze programowanie działań szkoleniowych.
Termin wdrożenia	18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.7. Zakup i Wdrożenie – Standardy i procedury zarządzania zmianami

Priorytet	Niski
Ustalenia	W trakcie prac audytowych nie stwierdzono istnienia procedur odtworzenia aplikacji po nieudanej instalacji poprawek bądź wadliwego oprogramowania. Brak jest również procedur dotyczących zarządzania zmianą procedur, procesami biznesowymi, usługami, zmianami w systemie jak również platformą sprzętową.
Implikacje	Brak kompleksowych procedur zarządzania zmianami, obejmujących m.in. mechanizmy odtworzenia aplikacji po ewentualnej nieudanej instalacji poprawek, oraz zmiany platform sprzętowych, zwiększa ryzyko braku integralności systemu.
Rekomendacje	Zaleca się opracowanie i wdrożenie procedur i mechanizmów odtworzenia aplikacji/systemu po instalacji źle funkcjonującego oprogramowania. Zaleca się również opracowanie i wdrożenie procedur dotyczących zarządzania zmianą procedur, procesami biznesowymi, usługami, zmianami w systemie jak również platformą sprzętową.
Odpowiedź	Odpowiedź MF: Obecnie istniejąca procedura Backupu zostanie zaktualizowana o rozdział dotyczący odtwarzania aplikacji/systemu zarówno po instalacji źle funkcjonującego oprogramowania jak również po awarii.
Termin wdrożenia	do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.8. Zakup i Wdrożenie – Przeniesienie do środowiska produkcyjnego

Priorytet	Niski
Ustalenia	*Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13* nie definiuje procedur przeniesienia przetestowanego i odebranego oprogramowania do środowiska produkcyjnego.
Implikacje	Brak opracowanych procedur przeniesienia oprogramowania oraz nie przypisanie odpowiedzialności za ten proces może spowodować nieprawidłowe bądź nieterminowe wykonywanie obowiązków związanych z instalacją nowego oprogramowania w środowisku produkcyjnym.
Rekomendacje	Zaleca się opracowanie i wdrożenie procedur przeniesienia przetestowanego oprogramowania do środowiska produkcyjnego (zawierających m.in. formalną akceptację, uaktualnienie dokumentacji, przechowywanie poprzednich wersji oprogramowania, itp.) oraz określenie odpowiedzialności za ten proces.
Odpowiedź	Odpowiedź MF: Zostanie opracowana procedura wgrywania przetestowanego oprogramowania do środowiska produkcyjnego (w tym także informacja, że kolejne wersje oprogramowania przechowywane są w narzędziu ClearCase).
Termin wdrożenia	do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.9. Zakup i Wdrożenie – Przegląd powdrożeniowy

Priorytet	Niski
Ustalenia	*Plan zarządzania testami wstępnymi i akceptacyjnymi systemu SIMIK 07-13* nie zawiera procedur dotyczących powdrożeniowego przeglądu systemu po wprowadzeniu do niego zmian.
Implikacje	Brak mechanizmów przeglądu systemu po wgraniu nowego oprogramowania może spowodować nieprawidłową pracę systemu.
Rekomendacje	Zaleca się opracowanie i wdrożenie procedur i mechanizmów przeglądu systemu po wgraniu zmian w systemie (modyfikacji, poprawek).
Odpowiedź	Odpowiedź MF: Zakres „Planu testów wstępnych i akceptacyjnych systemu SIMIK 07-13" jest ograniczony do etapu akceptacji dostarczanego oprogramowania przez Głównego Użytkownika. Procedury dotyczące powdrożeniowego przeglądu systemu po wprowadzeniu do niego zmian (modyfikacji, poprawek) należy do zakresu procedury „Plan zarządzania zmianami" . Procedura ta zostanie uzupełniona o stosowne zapisy dotyczące przeglądu systemu po wgraniu zmiany w systemie.
Termin wdrożenia	do 18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.10. Dostarczanie i Wsparcie – Monitorowanie i raportowanie poziomu świadczenia usług

Priorytet Niski

Ustalenia W trakcie prac audytowych nie potwierdzono faktu wykonywania przeglądów umów pod kątem sprawdzenia wywiązywania się Wykonawcy z obowiązku dotyczącego poziomu jakości usług. Brak jest także formalnych wewnętrznych zasad (procedur) monitorowania poziomu usług dostawców zewnętrznych, nie zostały również określone kryteria raportowania poziomu usług.

Implikacje Brak określonych kryteriów raportowania poziomu usług, wewnętrznych zasad monitorowania poziomu usług dostawców zewnętrznych, jak również nie wykonywanie regularnych przeglądów umów pod kątem sprawdzenia wywiązywania się Wykonawcy z obowiązku dotyczącego poziomu jakości usług może skutkować nie wywiązywaniem się dostawców zewnętrznych z obowiązku zapewnienia usług odpowiednio wysokiej jakości.

Rekomendacje Zaleca się określenie podstawowych kryteriów raportowania poziomu usług oraz opracowanie i wdrożenie zasad monitorowania poziomu usług dostawców zewnętrznych.

Zaleca się regularny przegląd i analizę ustalonych kryteriów poziomu usług pod kątem sprawdzenia, czy kryteria poziomu usług są spełniane przez dostawców zewnętrznych.

Odpowiedź Odpowiedź MF:

Przy rozliczaniu umów z Wykonawcą sprawdzana jest terminowość i jakość wykonywanych usług. Przy odbieraniu poszczególnych zleceń modyfikacji oprogramowania na bieżąco naliczane są kary umowne. Kary potrącane są przy zapłacie za poszczególne faktury, a zawiadomienie o naliczeniu kary wraz ze specyfikacją naliczonej kary wysyłane jest listem poleconym do Wykonawcy.

W przypadku umowy z Wykonawcą Systemu SIMIK – ComArch S.A. stosuje się następujące zapisy z Umowy:

1. W przypadku opóźnienia w przekazaniu do odbioru Produktu albo w osiągnięciu Pozytywnego Wyniku

Testów po zakończeniu testów akceptacyjnych, w terminie wynikającym ze Zlecenia, Zamawiającemu przysługują kary umowne:

a) za opóźnienie w wymiarze nie większym niż 14 dni - w wysokości 0,1 % wynagrodzenia z tytułu wykonania Usług Developerskich w ramach Zlecenia (brutto), za każdy dzień opóźnienia,
b) za opóźnienie w wymiarze przekraczającym 14 dni - w wysokości 0,5 % wynagrodzenia z tytułu Usług Developerskich w ramach Zlecenia (brutto), za każdy dzień opóźnienia, chyba że opóźnienie wynika z przyczyn nie leżących po stronie Wykonawcy.

2. W przypadku, gdy ilość Wad krytycznych stwierdzonych w wyniku testów Oprogramowania, jest wyższa niż:
   a) 100 - w testach wstępnych,
   b) 0 - w testach akceptacyjnych,

Zamawiającemu przysługuje prawo żądania kar umownych w wysokości 0,05 % wynagrodzenia (brutto) z tytułu wykonania Usług Developerskich w ramach Zlecenia, za każdą kolejną Wadę krytyczną ponad tę ilość, w ramach danego Zlecenia.

Termin wdrożenia	Realizowane na bieżąco
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.11. Dostarczanie i Wsparcie – Zarządzanie ryzykiem związanym z dostawcami

Priorytet	Niski
Ustalenia	W opracowanej *Analizie ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13* brak jest elementów dotyczących szacowania ryzyka związanego z dostawcami zewnętrznymi.
Implikacje	Brak przeprowadzonej analizy ryzyka związanego z dostawcami zewnętrznymi może skutkować nieefektywnym zarządzaniem tym ryzykiem.
Rekomendacje	Zaleca się przeprowadzenie szacowania ryzyka związanego z dostawcami zewnętrznymi (w tym m.in. z niewypełnieniem przez dostawcę obowiązków kontraktowych).
Odpowiedź	Odpowiedź MF: Uzupełnienie obecnie obowiązujących dokumentów dotyczących analizy ryzyka o elementy dotyczące szacowania ryzyka związanego z dostawcami zewnętrznymi. Zorganizowanie formalnego przeglądu rejestru ryzyka mającego na celu jego u uzupełnienie i aktualizację.
Termin wdrożenia	do 11 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.12. Dostarczanie i Wsparcie – Planowanie wydajności i pojemności

Priorytet	Niski
Ustalenia	W trakcie prac audytowych ustalono, iż brak jest regularnego procesu przeglądu *Procedury zarządzania rozwojem systemu w systemie SIMIK 07-13* w celu jego aktualizacji. Ponadto procedury zawarte w tym dokumencie nie określają sposobu badania i oceniania pojemności systemu.
Implikacje	Brak regularnego przeglądu dokumentu może spowodować jego dezaktualizację. Brak wiedzy na temat pojemności zasobów może wpłynąć na możliwość utracenia ważnych danych.
Rekomendacje	Zaleca się wdrożenie stałego przeglądu *Procedury zarządzania rozwojem systemu w systemie SIMIK 07-13* oraz uzupełnienie dokumentu i wdrożenie procedury oceny pojemności systemu.
Odpowiedź	Odpowiedź MF: Zgodnie z informacją odnoszącą się do punktu 8.6, także procedura zarządzania rozwojem w systemie SIMIK 07-13, zostanie uaktualniona o ustalenie zasad weryfikacji i aktualizacji dokumentu. Procedura zostanie uaktualniona o część dotyczącą oceny pojemności systemu.
Termin wdrożenia	do 11 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.13. Dostarczanie i Wsparcie – Obecna wydajność i pojemność

Priorytet	Niski
Ustalenia	Z przeprowadzonych rozmów z administratorami oraz po zapoznaniu się z wnioskami z notatek z monitorowania systemu ustalono, że w chwili obecnej wydajność systemu SIMIK jest nie wystarczająca w godzinach największego obciążenia systemu.
Implikacje	Nie wystarczająca wydajność zwiększa ryzyko braku dostępności systemu.
Rekomendacje	Zaleca się wdrożenie docelowej infrastruktury, następnie regularne monitorowanie systemu pod kątem wydajności i pojemności.
Odpowiedź	Odpowiedź MF: Przeprowadzone pomiary wydajności systemu wykazały jedynie krótkotrwałe zakresy maksymalnego użycia zasobów systemu w godzinach największego obciążenia. Nie wpisują się one obecnie w trwałą tendencję wykazującą niewydolność systemu. Poprawie istniejącego stanu w dalszej perspektywie czasu ma służyć wdrożenie nowej infrastruktury systemu SIMIK.
Termin wdrożenia	do 29 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.14. Dostarczanie i Wsparcie – Docelowa wydajność i pojemność

Priorytet	Niski
Ustalenia	W trakcie prac audytowych ustalono, że nie są dokonywane analizy pod kątem przyszłego wykorzystania systemu.
Implikacje	Brak stałego monitorowania działania systemu może zwiększyć ryzyko braku dostępności systemu.
Rekomendacje	Zaleca się postępowanie zgodnie z procedurą jak również wprowadzenia rejestru przeglądu dokonywanych przed administratorów.
Odpowiedź	Odpowiedź MF: W tym zakresie zostanie wdrożona, uaktualniona o oceny pojemności systemu, procedura zarządzania rozwojem w systemie SIMIK 07-13. Zapewni on dostosowanie systemu do wykorzystania w przyszłości zgodnie ze zwiększającymi się wymaganiami. Dokonywanie bieżących przeglądów wydajności będzie odnotowywane w Dzienniku pracy AT KSI SIMIK 07 - 13.
Termin wdrożenia	do 11 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.15. Dostarczanie i Wsparcie – Zapewnienie ciągłości usług

Priorytet	Średni
Ustalenia	W trakcie prac audytowych stwierdzono, iż *Plan ciągłości działania Krajowego Systemu Informatycznego SIMIK 07-13:* ▪ nie określa częstotliwości wymaganych przeglądów i aktualizacji, ▪ nie jest testowany, ▪ do chwili obecnej nie odbyły się szkolenia dot. *Planów ciągłości działania*.
Implikacje	Brak jasno regularnie wykonywanych testów planu ciągłości działalności, przeglądów i aktualizacji dokumentu oraz przeprowadzanych szkoleń z zakresu *Planu ciągłości działania* może spowodować nieprzygotowanie do odtwarzania systemu w przypadku rzeczywistej awarii.
Rekomendacje	Zaleca się wykonywanie regularnych przeglądów i aktualizacji dokumentu oraz przeprowadzanie szkoleń i testów z zakresu *Planu ciągłości działania.*
Odpowiedź	Odpowiedź MF: Plan ciągłości działania zostanie uaktualniony o częstotliwość przeglądów i aktualizacji, zostaną wykonane testy oraz zostanie przeprowadzone szkolenie dotyczące Planu ciągłości działania.
Termin wdrożenia	do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.16. Dostarczanie i wsparcie – Plan zapewnienia bezpieczeństwa IT

Priorytet	Niski
Ustalenia	Zgodnie z zapisami *Polityki Bezpieczeństwa* wszystkie dokumenty składające się na politykę bezpieczeństwa w KSI SIMIK 07-13 podlegają ochronie i są zastrzeżone zgodnie z zawartym w niej opisem. Jest to sprzeczne z powszechnie przyjętą praktyką, która stanowi, iż główny dokument polityki bezpieczeństwa powinien zawierać m.in. ogólne oświadczenie o intencjach kierownictwa w stosunku do celów i zasad bezpieczeństwa informacji w systemie oraz stosowanych norm i zasad zabezpieczeń i jako taki powinien być powszechnie dostępny w formie właściwej i zrozumiałej dla wszystkich użytkowników systemu informatycznego.
Implikacje	Uniemożliwienie dostępu wszystkich użytkowników do *Polityki Bezpieczeństwa* systemu KSI SIMIK 07-13 może prowadzić do niewłaściwego zrozumienia celów i zasad ochrony informacji w systemie przez jego użytkowników.
Rekomendacje	Zaleca się umożliwienie dostępu do głównego dokumentu *Polityki Bezpieczeństwa systemu SIMIK 07-13* dla wszystkich użytkowników systemu. Zaleca się zawarcie ewentualnych zastrzeżonych informacji w dokumentach pochodnych.
Odpowiedź	Odpowiedź MF: Aby umożliwić dostęp do części dokumentów Polityki bezpieczeństwa systemu SIMIK 07 – 13, wszystkim użytkownikom, zostanie zdefiniowana nowa struktura i hierarchia dokumentów Polityki bezpieczeństwa. Umożliwi to zdefiniowanie zakresu w jakim konkretne osoby lub grupy osób, będą mogły się zapoznać z dokumentacją.
Termin wdrożenia	do 30 września 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.17. Dostarczanie i wsparcie – Plan zapewnienia bezpieczeństwa IT

Priorytet	Niski
Ustalenia	W *Polityce Bezpieczeństwa* nie został określony bezpośrednio Właściciel dokumentu – osoba odpowiedzialna za akceptację dokumentu oraz regularne (np. roczne) przeglądy i zatwierdzanie aktualizacji zasad zarządzania bezpieczeństwem informacji w KSI, dostosowujących *Politykę* i wynikające z niej szczegółowe procedury do aktualnego stanu technicznego, prawnego i organizacyjnego.
Implikacje	Brak określenia Właściciela *Polityki Bezpieczeństwa*, osoby odpowiedzialnej za zatwierdzanie przeglądów i aktualizacji *Polityki*, może prowadzić do braku regularnych przeglądów tego dokumentu.
Rekomendacje	Zaleca się precyzyjne określenie Właściciela *Polityki Bezpieczeństwa* – osoby odpowiedzialnej za akceptację dokumentu oraz regularne (np. roczne) przeglądy i zatwierdzanie aktualizacji zasad zarządzania bezpieczeństwem informacji w KSI SIMIK 07-13.
Odpowiedź	Odpowiedź MF: Precyzyjne określenie właściciela Polityki bezpieczeństwa, osób odpowiedzialnych za akceptację dokumentu i regularne przeglądy zostaną dokonane w trakcie prac nad nową wersją dokumentu. Efektem będzie powstanie i akceptacja nowej wersji dokumentu Polityki bezpieczeństwa.
Termin wdrożenia	do 30 września 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.18. Dostarczanie i Wsparcie – Zarządzanie kontami użytkowników

Priorytet	Średni
Ustalenia	W chwili obecnej wykonywany jest jedynie przegląd uprawnień użytkowników na zgodność ze złożonymi wnioskami. Administratorzy cotygodniowo wybierają losowo 10 użytkowników, dla których odbywa się weryfikacja złożonych wniosków i nadanych odpowiednio uprawnień. Po każdym przeglądzie sporządzany jest *Raport z okresowego przeglądu kont użytkowników KSI (SIMIK 07-13)*. Nie są natomiast wykonywane regularne przeglądy kont użytkowników, przeprowadzane w celu zablokowania niewykorzystywanych przez dłuższy czas kont użytkowników.
Implikacje	Brak regularnych przeglądów przeprowadzanych w celu zablokowania niewykorzystywanych przez dłuższy czas kont użytkowników może powodować próby nieautoryzowanego wykorzystania tych kont.
Rekomendacje	Zaleca się okresowe wykonywanie przeglądów kont użytkowników, przeprowadzanych w celu zablokowania niewykorzystywanych przez dłuższy czas kont użytkowników oraz określenie odpowiedzialności za ten proces.
Odpowiedź	Odpowiedź MRR: Opracowana zostanie procedura dotycząca zasad przeprowadzania Przeglądów Aktywności Kont Użytkowników ze wskazaniem odpowiedzialności za ten proces. Przeglądy będą dokonywane raz w miesiącu od momentu opracowania procedury.
Termin wdrożenia	18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.19. Dostarczanie i Wsparcie – Monitorowanie i testowanie bezpieczeństwa

Priorytet Niski

Ustalenia W *Dokumencie Głównym Polityki Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* został zawarty opis ról i odpowiedzialności dotyczących monitorowania bezpieczeństwa systemu. Zgodnie z tymi zapisami ABI monitoruje przestrzeganie zasad PBI, zgodnie z harmonogramem zatwierdzonym przez AI. ABI przygotowuje kwartalny raport z prowadzonego monitorowania i przekazuje go do AI. Do chwili obecnej ABI opracował jeden raport (noszący datę 24.04.2008) odnoszący się do zagadnień bezpieczeństwa – kolejne raporty powstaną w następnych kwartałach (ze względu na fakt, iż PBI została zaakceptowana i wdrożona w dniu 28.04.2008). Brak jest jednakże harmonogramu zadań związanych z monitorowaniem zatwierdzonego przez AI, o którym jest mowa w PBI.

Implikacje Brak harmonogramu zadań związanych z monitorowaniem zatwierdzonego przez AI może prowadzić do sytuacji, w której monitorowanie bezpieczeństwa nie będzie regularnie wykonywane.

Rekomendacje Zaleca się opracowanie harmonogramu zadań związanych z monitorowaniem oraz zatwierdzenie go przez AI, zgodnie z zapisami PBI.

Odpowiedź Odpowiedź MF:

Polityka bezpieczeństwa definiuje cykl w jakim sporządzane są raporty z monitorowania bezpieczeństwa systemu, oraz odpowiedzialność za ich wykonanie. Raport sporządzany jest cyklicznie co kwartał, wykonuje go ABI, następnie jest on przekazywany do AI. Monitorowanie logów w zakresie bezpieczeństwa systemu odbywa się na bieżąco każdego dnia.

W zakresie tej rekomendacji zostanie wykonana drobna korekta w Polityce bezpieczeństwa odnosząca się do zdefiniowania harmonogramu zadań związanych z monitorowaniem bezpieczeństwa systemu.

Termin do 11 lipca 2008 r.

wdrożenia

Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.20. Dostarczanie i Wsparcie – Zarządzanie kluczem kryptograficznym

Priorytet	Niski
Ustalenia	Zgodnie z informacjami otrzymanymi w trakcie prac audytowych, do chwili obecnej nie została wdrożona procedura dotycząca przechowywania kluczy kryptograficznych w celu zapewnienia szybkiego dostępu w przypadku awarii sprzętu informatycznego oraz ochrony kluczy przed utratą.
Implikacje	Brak procedury dotyczącej przechowywania kluczy kryptograficznych zwiększa ryzyko ich utraty.
Rekomendacje	Zaleca się opracowanie procedury dotyczącej przechowywania kluczy kryptograficznych.
Odpowiedź	Odpowiedź MF: W systemie jest wykorzystywany tylko certyfikat niekwalifikowany SSL, który przechowywany jest w sejfie. W dokumentach polityki bezpieczeństwa zostanie dopisana procedura przechowywania tego certyfikatu.
Termin wdrożenia	do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.21. Dostarczanie i Wsparcie – Zapobieganie, detekcja i korekcja działań złośliwego oprogramowania

Priorytet Niski

Ustalenia Dokument *Hardering serwerów Windows 2003* nie został zatwierdzony przez Administratora Informacji. Nie było on dotychczas aktualizowany. Nie został również wdrożony harmonogram wykonywania operacji aktualizacji zabezpieczeń systemów operacyjnych serwerów.

Na serwerach obsługujących system KSI nie został zainstalowany automatyczny program antywirusowy chroniący przed szkodliwym oprogramowaniem.

Implikacje Brak formalnie zatwierdzonych i aktualizowanych zgodnie z ustalonym harmonogramem dokumentów dotyczących zabezpieczeń systemowych uniemożliwia skuteczną administrację systemem i powoduje zwiększenie ryzyka naruszenia bezpieczeństwa.

Brak oprogramowania antywirusowego zwiększa ryzyko zainfekowania systemu złośliwym oprogramowaniem.

Rekomendacje Zaleca się opracowanie bądź uzupełnienie już istniejących dokumentów dotyczących zabezpieczeń systemowych o szczegółowe instrukcje w zakresie aktualizacji procedur, zabezpieczeń systemów operacyjnych serwerów oraz wyznaczenie harmonogramu wykonywania prac administracyjnych.

Zaleca się zainstalowanie programu antywirusowego chroniącego przed szkodliwym oprogramowaniem oraz opracowanie i wdrożenie procedur aktualizacji oprogramowania i bazy wirusów.

Odpowiedź Odpowiedź MF:

Na wszystkich serwerach z sieciowym systemem operacyjnym MS Windows, zostanie zainstalowane oprogramowanie antywirusowe firmy Trend Micro. Oprogramowanie to aktualizowane będzie ręcznie (nie rzadziej niż raz w tygodniu ale nie częściej niż raz dziennie), przy pomocy ściągniętego ze strony producenta tego programowania najnowszego pliku definicji wirusów.

	Odpowiednie dokumenty zostaną zaktualizowane o wprowadzone procedury oraz przyjęte harmonogramy.
Termin wdrożenia	do 31 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.22. Dostarczanie i Wsparcie – Bezpieczeństwo sieciowe

Priorytet	Niski
Ustalenia	Ustalono, iż brak jest mechanizmu kontrolnego zapewniającego przeglądanie serwera logów przez administratorów. Ustalono również, że brak jest procesu testowania zapory sieciowej np. poprzez przeprowadzenie testów penetracyjnych.
Implikacje	Brak mechanizmu potwierdzającego przeglądanie logów może skutkować niewykryciem z odpowiednim wyprzedzeniem zagrożeń związanych z bezpieczeństwem sieci. Natomiast brak procedury testowania zastosowanych rozwiązań nie daje zapewnienia, że zaimplementowano odpowiedni poziom bezpieczeństwa.
Rekomendacje	Zaleca się wdrożenie mechanizmu zapewniającego przeglądanie serwera logów oraz zweryfikowanie zastosowanego poziomu bezpieczeństwa.
Odpowiedź	Odpowiedź MF: Przeglądanie logów serwera SIMIK, będzie możliwe po wdrożeniu odpowiedniego systemu zapewniającego realizację tych funkcji w ramach całej infrastruktury MF. Tego rodzaju funkcjonalność zapewnia np. system enVision. Obecnie prowadzone są konsultacje i spotkania, mające na celu testowanie i poznanie możliwości systemu. W terminie 28.07 do1.08, Wydział Zabezpieczeń DI, będzie prowadził testy systemu enVision. Testy zapory sieciowej będą prowadzone w ramach audytu systemu KSI SIMIK. Audyt systemu przeprowadzi firma zewnętrzna, która przeprowadzi testy penetracyjne. Przetarg na audyt jest w trakcie realizacji.
Termin wdrożenia	ok. 1 rok.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.23. Dostarczanie i Wsparcie – Wymogi biznesowe dla zarządzania danymi

Priorytet	Niski
Ustalenia	W systemie nie zostały określone maksymalne czasy przetwarzania i wymagania na dostępność danych zgodne z potrzebami użytkowników.
Implikacje	Brak określonych maksymalnych czasów przetwarzania i wymagań na dostępność danych uniemożliwia właściwe określenie parametrów systemowych.
Rekomendacje	Zaleca się formalne określenie maksymalnych czasów przetwarzania oraz wymagań na dostępność danych zgodnych z potrzebami użytkowników.
Odpowiedź	Odpowiedź MRR: Zostaną określone maksymalne czasy przetwarzania oraz wymagań na dostępność danych zgodnie z potrzebami użytkowników.
Termin wdrożenia	18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.24. Dostarczanie i Wsparcie – Procedury składowania i utrzymania danych

Priorytet	Niski
Ustalenia	Zasady przechowywania nośników z kopiami danych z systemu zostały zdefiniowane w *Procedurze przechowywania nośników z kopiami awaryjnymi danych z systemu*. Ustalono, iż nośniki nie są opisywane zgodnie z procedurą.
Implikacje	W tym przypadku niestosowanie się do zapisów może skutkować niepowodzeniem w odtwarzaniu danych po wystąpieniu awarii.
Rekomendacje	Zaleca się stosowanie do wdrożonych procedur składowania i utrzymania danych.
Odpowiedź	Odpowiedź MF: Nośniki zostaną opisane zgodnie z procedurą.
Termin wdrożenia	do 11 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.25. Dostarczanie i Wsparcie – Usuwanie danych

Priorytet	Niski
Ustalenia	W trakcie czynności audytowych stwierdzono, iż *Procedura postępowania z nośnikami informacji w przypadku likwidacji urządzeń komputerowych* nie zawiera obowiązku sporządzenia protokołu przekazania lub likwidacji sprzętu oraz precyzyjnego określenia odpowiedzialności osób nadzorujących prawidłowe wykonanie procesu.
Implikacje	Brak wyznaczenia osób nadzorujących prawidłowość procesu *likwidacji urządzeń komputerowych*, jak również brak protokołów likwidacji sprzętu utrudnia ocenę prawidłowości zabezpieczeń systemu przed niepowołanym dostępem do danych.
Rekomendacje	Zaleca się weryfikację i uzupełnienie *Procedury postępowania z nośnikami informacji w przypadku likwidacji urządzeń komputerowych* o zagadnienia związane z obowiązkiem sporządzenia protokołu przekazania lub likwidacji sprzętu oraz precyzyjnego określenia odpowiedzialności osób nadzorujących prawidłowe wykonanie tego procesu oraz postępowanie zgodnie z jej wymaganiami.
Odpowiedź	Odpowiedź MF: Procedura zostanie uzupełniona zgodnie z rekomendacją.
Termin wdrożenia	do 11 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.26. Dostarczanie i Wsparcie – Wykonywanie kopii zapasowych i przywracanie systemów

Priorytet	Średni
Ustalenia	Podczas prowadzonych prac audytowych potwierdzono istnienie i wykonywanie kopii zapasowych oraz przeglądanie plików logów przez administratorów. Kopie zapasowe produkcyjnej bazy danych nie były jednak wykonywane z regularnością określoną przez procedurę.
Implikacje	Nieregularne wykonywanie kopii zapasowych może prowadzić do problemów w przypadku konieczności odzyskania bazy danych z kopii zapasowych.
Rekomendacje	Zaleca się dotrzymywanie określonych w procedurach terminów wykonywania kopii zapasowych.
Odpowiedź	Odpowiedź MF: Kopie są wykonywane dokładnie według terminów i z regularnością określoną w procedurze.
Termin wdrożenia	
Stanowisko Instytucji Audytowej	Wdrożenie rekomendacji zostanie zweryfikowane podczas następnego badania.

8.27. Dostarczanie i Wsparcie – Wykonywanie kopii zapasowych i przywracanie systemów

Priorytet	Niski
Ustalenia	*Procedura wykonywania backupu* – wykonywania kopii zapasowych w systemie KSI SIMIK 07-13 – nie zawiera postanowień dotyczących odtworzenia oraz regularnego testowania kopii zapasowych. Zgodnie z otrzymanymi informacjami kopie zapasowe są testowane ad-hoc (podczas dotychczasowej pracy systemu nie zaistniała konieczność odtworzenia produkcyjnej bazy danych z kopii zapasowej).
Implikacje	Brak zasad dotyczących odtworzenia i regularnego testowania kopii zapasowych może prowadzić do sytuacji, w której nie będzie możliwe odzyskanie danych z kopii zapasowych i przywrócenie funkcjonalności systemu.
Rekomendacje	Zaleca się uzupełnienie istniejących procedur wykonywania kopii zapasowych o wytyczne dotyczące ich odtwarzania i regularnego testowania. Zaleca się określenie odpowiedzialności za proces regularnego testowania kopii zapasowych w systemie KSI SIMIK 07-13.
Odpowiedź	Odpowiedź MF: Obecnie istniejąca procedura Backupu zostanie zaktualizowana o rozdział dotyczący odtwarzania aplikacji/systemu. Procedura otrzyma także dodatkowy rozdział odnoszący się do procesu testowania poprawności wykonanych kopii.
Termin wdrożenia	do 29 sierpnia 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.28. Dostarczanie i Wsparcie – Środki ochrony fizycznej

Priorytet	Niski
Ustalenia	W odniesieniu do systemu KSI SIMIK 07-13, poza ogólnymi zapisami Załącznika nr 4 do *Polityki bezpieczeństwa,* brak jest szczegółowych procedur dotyczących zabezpieczeń fizycznych pomieszczeń bezpiecznych, w których zlokalizowane są m.in. serwery, aktywne urządzenia sieciowe, wyłączniki zasilania elektrycznego, pomieszczenia administratorów.
Implikacje	Brak precyzyjnego zdefininiowania fizycznych środków ochrony pomieszczeń bezpiecznych zwiększa ryzyko ich niewłaściwego zabezpieczenia.
Rekomendacje	Zaleca się opracowanie i wdrożenie szczegółowych procedur dotyczących zabezpieczeń fizycznych pomieszczeń bezpiecznych, w których zlokalizowane są m.in. serwery, aktywne urządzenia sieciowe, wyłączniki zasilania elektrycznego, pomieszczenia administratorów.
Odpowiedź	Odpowiedź MF: Zostanie opracowana szczegółowa procedura dostępu w ramach Polityki bezpieczeństwa KSI SIMIK, dla nowej infrastruktury w WASKO.
Termin wdrożenia	29 sierpnia 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.29. Dostarczanie i Wsparcie – Dostęp fizyczny

Priorytet	Niski
Ustalenia	Wejście do pomieszczenia obecnej serwerowni nie jest monitorowane systemem kamer CCTV. W serwerowni docelowej jest zainstalowana kamera CCTV, w trakcie audytu nie udało się uzyskać zapewnienia, czy sygnał z tej kamery jest trwale rejestrowany. Nie jest prowadzony rejestr wejść/wyjść do serwerowni dla osób nie posiadających stałego upoważnienia.
Implikacje	Brak prowadzenia rejestracji osób wchodzących do serwerowni zwiększa ryzyko narażenia serwerów KSI SIMIK 07-13 na fizyczne zagrożenia, będące skutkiem przypadkowego błędu lub celowego działania.
Rekomendacje	Zaleca się rejestrowanie wejść osób nie posiadających stałego dostępu do serwerowni (np. serwisantów, audytorów, itp.), jak również przeprowadzanie okresowej kontroli tego rejestru pod kątem zasadności obecności tych osób, jak również określenie odpowiedzialności za ten proces.
Odpowiedź	Odpowiedź MF: Nowa infrastruktura systemu SIMIK (serwerownia) w WASKO, jest wyposażona w odpowiednie systemy monitoringu zapewniający realizację zaleceń w tym zakresie. Dodatkowo będzie sformułowana procedura w ramach Polityki bezpieczeństwa KSI SIMIK, określająca sposób rejestrowania wejść osób z zewnątrz (np. audytorów, serwisantów) do serwerownii. Procedura będzie definiowała kwestie organizacyjne związane z dostępem tych osób, odpowiedzialność za ten proces, a także sposób kontroli działań wynikających z procedury.
Termin wdrożenia	29 sierpnia 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.30. Dostarczanie i Wsparcie – Ochrona przed czynnikami środowiska naturalnego

Priorytet	Niski
Ustalenia	Pomieszczenie obecnej serwerowni, znajdującej się w wydzielonym obszarze budynku Ministerstwa Finansów, nie jest zabezpieczone w system monitorowania warunków środowiskowych (temperatury, wilgotności powietrza). W serwerowni nie zainstalowano również centralnego systemu gaszenia, a jedynie rozmieszczono ręcznie gaśnice CO_2. Pomieszczenie serwerowni jest klimatyzowane, nie istnieje jednak system automatycznie dostosowujący temperaturę i wilgotność w pomieszczeniu do założonych parametrów.
Implikacje	Brak właściwej ochrony fizycznej pomieszczeń, w których dokonuje się przetwarzania danych, oraz monitoringu warunków środowiskowych znacząco zwiększa ryzyko utraty danych i ciągłości pracy systemu w przypadku awarii lub zdarzenia losowego.
Rekomendacje	Zaleca się wdrożenie właściwych zabezpieczeń fizycznych dotyczących pomieszczeń serwerowni. Zaleca się objęcie serwerowni monitoringiem parametrów środowiskowych oraz instalację właściwych systemów przeciwpożarowych i ochrony okablowania.
Odpowiedź	Odpowiedź MF: Nowa infrastruktura systemu SIMIK (serwerownia) w WASKO, jest wyposażona w odpowiednie zabezpieczenia fizyczne, np. system monitorowania warunków środowiskowych. W serwerownii jest też zainstalowany centralny system gaszenia. Obecnie jest realizowane „przejście” na nową infrastrukturę.
Termin wdrożenia	w trakcie realizacji
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.31. Dostarczanie i Wsparcie – Zarządzanie wyposażeniem pomieszczeń

Priorytet	Niski
Ustalenia	Serwery systemu SIMIK są wyposażone w jeden zasilacz UPS gwarantujący krótkotrwałą (kilkuminutową) dostawę zasilania pozwalającą na bezpieczne zamknięcie systemu w przypadku katastrofy lub awarii. Zgodnie z otrzymanymi informacjami zasilacz UPS był testowany przez administratorów przed instalacją środowiska produkcyjnego, po tym zdarzeniu zasilacz UPS nie był więcej sprawdzany. Nie istnieją również formalne procedury dotyczące utrzymania i regularnego testowania urządzeń zasilających w systemie KSI. Serwery systemu SIMIK nie są wyposażone w gwarantowane źródło zasilania.
Implikacje	Brak testowania zasilaczy UPS może prowadzić do ich wadliwego funkcjonowania w momencie przerw w dostawie energii elektrycznej lub skoków napięcia.
Rekomendacje	Zaleca się regularne testowanie sprawności zasilaczy awaryjnych UPS. Zaleca się opracowanie i wdrożenie formalnych procedur utrzymania i regularnego testowania urządzeń UPS oraz innych urządzeń zasilających w systemie KSI SIMIK 07-13.
Odpowiedź	Odpowiedź MF: Infrastruktura KSI SIMIK 07-13 jest w chwili obecnej przenoszona do innej serwerownii (WASKO), która oferuje gwarantowany poziom zasilania. W związku z powyższym nie jest konieczne przygotowywanie procedury oraz regularne testowanie zasilaczy awaryjnych UPS.
Termin wdrożenia	
Stanowisko Instytucji Audytowej	Rekomendacja zostaje podtrzymana.

8.32. Dostarczanie i Wsparcie – Procedury i instrukcje operacyjne

Priorytet	Niski
Ustalenia	Obowiązujące procedury nie zawierają takich elementów jak m.in. zasady przekazywania obowiązków (formalne przekazanie obowiązków, problemy eksploatacyjne, procedury eskalacji, raportowanie obecnych obowiązków).
Implikacje	Brak formalnych zasad przekazywania obowiązków i zagadnień z tym związanych może prowadzić do sytuacji, w której nie będzie możliwe zapewnienie ciągłości przetwarzania.
Rekomendacje	Zaleca się dokonanie przeglądu obowiązujących procedur i ich ewentualne uzupełnienie.
Odpowiedź	Odpowiedź MRR: Zostanie dokonany przegląd procedur w celu opracowania formalnych zasad przekazywania obowiązków i zagadnień z tym związanych. Odpowiedź MF: W celu zapewnienia ciągłości przetwarzania obecnie obowiązujące procedury zostaną uzupełnione o procedurę przekazywania obowiązków i zagadnień.
Termin wdrożenia	Odpowiedź MRR: 18 lipca 2008 r. Odpowiedź MF: trzeci kwartał 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.33. Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

Priorytet Niski

Ustalenia

W *Dokumencie Głównym Polityki Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13* został zawarty opis ról i odpowiedzialności dotyczących monitorowania bezpieczeństwa systemu (opisane szerzej w rozdziale *5.5.5. Monitorowanie i testowanie bezpieczeństwa)*. Brak jest jednakże opracowanych szczegółowych zasad i wytycznych (procedur) monitorowania infrastruktury teleinformatycznej i związanych z nią zdarzeń.

Na serwerach obsługujących Krajowy System Informatyczny została zainstalowana aplikacja Dell OpenManage Server Administrator. Umożliwia ona w czasie rzeczywistym za pomocą przeglądarki internetowej podgląd elementów systemowych. Aplikacja ta posiada również możliwość zapisywania informacji do pliku, jednakże informacje nie są logowane. W trakcie prowadzonych prac nie uzyskano potwierdzenia dokonywania regularnych przeglądów dotyczących monitorowania poszczególnych elementów infrastruktury.

Implikacje

Brak szczegółowych zasad i wytycznych (procedur) monitorowania infrastruktury teleinformatycznej i związanych z nią zdarzeń może prowadzić do sytuacji, w której nie będzie możliwa weryfikacja bezpieczeństwa sieci teleinformatycznej, jak również nie będzie możliwe reagowanie na potencjalne zagrożenia z wyprzedzeniem.

Rekomendacje

Zaleca się opracowanie i wdrożenie mechanizmów i procedur umożliwiających monitorowanie infrastruktury teleinformatycznej i związanych z nią zdarzeń (z uwzględnieniem takich elementów jak: poziom informacji zapisywanych w logach i rejestrach, określenie systemów, w których niezbędne jest zapisywanie logów, odpowiedzialność za wykonywanie procesu monitorowania, raportowanie, zasady nadzoru i kontroli, itp.), jak również umożliwiających zapisywanie niezbędnych informacji (określonych na podstawie analizy ryzyka) w odpowiednich rejestrach zdarzeń i logach zapewniających rekonstrukcję, przegląd i analizę przeprowadzonych operacji lub podjętych działań.

	Zaleca się regularne dokonywanie (w tym również przez kadrę kierowniczą) przeglądów i monitorowania infrastruktury teleinformatycznej i związanych z nią zdarzeń.
Odpowiedź	Odpowiedź MF: System KSI będzie przeniesiony na nowe środowisko sprzętowe IBM Blade, które zawiera moduł zarządzający zbierający logi ze zdarzeń z każdego serwera. Zostaną zweryfikowane dokumenty polityki bezpieczeństwa dotyczące zasad i wytycznych monitorowania infrastruktury i związanych z nią zdarzeń przy uwzględnieniu już nowego środowiska.
Termin wdrożenia	do 29 sierpnia 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.34. Dostarczanie i Wsparcie – Monitorowanie infrastruktury IT

Priorytet	Niski
Ustalenia	Została opracowana *Analiza ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13*. W analizie tej zostało uwzględnione m.in. zagrożenie dotyczące braku narzędzi do monitorowania bezpieczeństwa. Przy oszacowanym poziomie ryzyka ocenę zabezpieczeń dla tego zasobu oceniono jako „niewystarczającą". Propozycją dodatkowych zabezpieczeń jest zakup oprogramowania służącego do analizy. Brak jest jednakże kompleksowego szacowania ryzyka w zakresie monitorowania infrastruktury IT (ze szczególnym uwzględnieniem najważniejszych aktywów).
Implikacje	Brak szczegółowej analizy ryzyka w zakresie monitorowania infrastruktury IT może prowadzić do niepełnego (lub w skrajnych sytuacjach do braku) monitorowania poszczególnych elementów systemu informatycznego.
Rekomendacje	Zaleca się weryfikację oraz uzupełnienie opracowanej analizy ryzyka o elementy związane z monitorowaniem infrastruktury teleinformatycznej (ze szczególnym uwzględnieniem najważniejszych aktywów).
Odpowiedź	Odpowiedź MF: Opracowany dokument Analizy ryzyka dla Krajowego Systemu Informatycznego SIMIK 07-13, zostanie zweryfikowany, także pod kątem elementów odnoszących się do monitorowania infrastruktury. Zostanie opracowany harmonogram cyklicznych przeglądów analizy ryzyka, tak aby było możliwe reagowanie na ewentualne zmiany w tym zakresie.
Termin wdrożenia	do 30 września 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.35. Monitorowanie i Ocena – Działania korygujące

Priorytet	Niski
Ustalenia	W *Procedurze zarządzania rozwojem w systemie KSI SIMIK 07-13* zostały określone działania podejmowane w przypadku monitorowania wydajności systemu. Procedura ta nie uwzględnia jednakże zagadnień związanych z monitorowaniem bezpieczeństwa systemów IT.
Implikacje	Nie uwzględnienie w mechanizmach i procedurach z zakresu monitorowania bezpieczeństwa IT zagadnień dotyczących podejmowania działań korygujących może prowadzić do nie podejmowania takich działań, co w konsekwencji może doprowadzić do sytuacji, w której nie będzie możliwe zapewnienie ciągłości przetwarzania.
Rekomendacje	Zaleca się uwzględnienie w mechanizmach i procedurach z zakresu monitorowania bezpieczeństwa systemów teleinformatycznych zagadnień dotyczących podejmowania działań wynikających z monitorowania, szacowania ryzyka i raportowania wyników działalności systemów IT (działania takie powinny zawierać m.in. przegląd i ustalenie reakcji personelu zarządzającego, przypisanie odpowiedzialności za działania naprawcze, śledzenie rezultatów podjętych działań, dokumentowanie podejmowanych działań korygujących, itp.).
Odpowiedź	Odpowiedź MF: Procedura zarządzania rozwojem w systemie KSI SIMIK, odnosi się do wszelkich aspektów funkcjonowania systemu, także dotyczących bezpieczeństwa. Zagadnienia dotyczące bezpieczeństwa, wraz z aktualnym podziałem ról i zakresu odpowiedzialności są zdefiniowane w dokumentach Polityki bezpieczeństwa. Dokładny przegląd i ewentualne zmiany w tym zakresie zostaną dokonane w trakcie prac nad nową wersją dokumentów Polityki bezpieczeństwa.
Termin wdrożenia	do 30 września 2008 r.

Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.36. Monitorowanie i Ocena – Działania naprawcze

Priorytet	Niski
Ustalenia	W trakcie prac audytowych ustalono, iż rekomendacje z ostatniego audytu zewnętrznego zostały wdrożone. Jednakże brak jest procedury dot. wprowadzania zaleceń audytowych. Dokument powinien zawierać m.in. określenie osób odpowiedzialnych za ocenę, uszeregowanie i nadzór nad wdrożeniem rekomendacji.
Implikacje	Brak procedury dotyczącej oceny i wdrażania rekomendacji audytowych może skutkować brakiem reakcji na zalecenia.
Rekomendacje	Zaleca się wdrożenie procedury dotyczącej oceny i wdrażania rekomendacji audytowych.
Odpowiedź	Odpowiedź MF: Obowiązująca "Procedura obsługi kontroli zewnętrznych i wewnętrznych" zostanie rozszerzona bądź powstanie dedykowana procedura obejmująca działania związane z oceną i wdrażaniem rekomendacji z kontroli i audytów.
Termin wdrożenia	trzeci kwartał 2008
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.37. Monitorowanie i Ocena – Zapewnienie zgodności

Priorytet	Niski
Ustalenia	W celu weryfikacji stopnia zapewnienia zgodności, system KSI SIMIK 07-13 był objęty zewnętrznym audytem, którego zakres został opisany w rozdziale *6.2.3. Wspomaganie kontroli wewnętrznej*. Jednakże audyt ten nie dotyczył wydajności i efektywności obszaru IT.
Implikacje	Brak niezależnych przeglądów może skutkować brakiem informacji dot. stopnia zapewnienia zgodności.
Rekomendacje	Zaleca się rozważenie przeprowadzania niezależnych przeglądów (audytów wewnętrznych bądź zewnętrznych) dotyczących oceny wydajności i efektywności obszaru.
Odpowiedź	Odpowiedź MF: Zespół Infrastruktury Technicznej jest w chwili obecnej w trakcie oczekiwania na rozstrzygnięcie przetargu w trybie Zamówień publicznych na przeprowadzenie Audytu Bezpieczeństwa, który między innymi pozwoli ocenić wydajność i efektywność obszaru IT systemu KSI SIMIK 07-13.
Termin wdrożenia	Termin wykonania audytu to 45 dni od momentu podpisania umowy z potencjalnym Wykonawcą wyłonionym w trybie Zamówień publicznych.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.38. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

Priorytet	Niski
Ustalenia	W przypadku umów o dofinansowanie, w których konieczne jest zawarcie aneksów, wszystkie informacje dotyczące starej wersji umowy są zawarte w systemie i nie są nadpisywane, lecz tworzona jest nowa wersja umowy/decyzji, posiadająca własny numer porządkowy. Zgodnie z otrzymanymi informacjami takie rozwiązanie zostało zaimplementowane, gdyż do archiwalnej wersji umowy mogą już być zawarte wnioski o płatność. System jednakże nie odróżnia w precyzyjny sposób aktualnej wersji umowy/decyzji od archiwalnych (np. można nadać im dowolną szczegółową numerację).
Implikacje	Brak precyzyjnego rozróżnienia starej i nowej wersji umowy o dofinansowanie może prowadzić, przy wielokrotnym wykorzystywaniu tych informacji, do braku integralności danych w systemie KSI.
Rekomendacje	Zaleca się odróżnienie w precyzyjny sposób w systemie KSI SIMIK umowy o dofinansowanie i kolejnych, zawieranych aneksów do niej (np. poprzez wprowadzenie jednolitej, konsekutywnej numeracji).
Odpowiedź	Odpowiedź MRR: W systemie zawsze wyświetlana jest aktualna wersja umowy/decyzji o dofinansowanie. Możliwe to jest dzięki nadawanemu przez system (niewidocznemu na ekranie) statusowi czy dana wersja umowy/decyzji jest aktualna, czy też nie. Za pomocą narzędzia Discoverer Oracle można odróżnić i wyświetlić wersje archiwalne oraz aktualne. W związku z powyższym prosimy o opinię, czy tym samym rekomendacja 8.41 może zostać uznana za zrealizowaną.
Termin wdrożenia	Wdrożona (w opinii MRR)

Stanowisko Instytucji Audytowej	Wyjaśnienie: W przypadku tworzenia aneksów do umowy, użytkownik ma możliwość dostępu do najnowszej wersji umowy/decyzji oraz wszystkich poprzednich. Ponieważ numeracja aneksów może byc dowolna (system nie wymusza kolejności numerownia poszczególnych wersji), a znacznik najnowszej wersji jest niewidoczny na ekranie (zgodnie z odpowiedzią MRR) użytkownik nie ma jednoznacznej pewności, która wersja umowy/decyzji jest najbardziej aktualna. W przypadku dużej ilości aneksów może dojść do pomyłki. Rozwiązaniem byłoby wprowadzenie jednoznacznej informacji dla użytkownika, iż dana wersja umowy/decyzji jest aktualna.

8.39. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

Priorytet	Niski
Ustalenia	W przypadku importu pliku XML zawierającego dane odnoszące się do już istniejącego w bazie KSI SIMIK 07-13 wniosku aplikacyjnego/umowy/wniosku płatniczego system dokonuje aktualizacji danych odpowiedniego dokumentu, nie informując jednak użytkownika o dokonanych modyfikacjach.
Implikacje	Brak poinformowania użytkownika o dokonanych modyfikacji w bazie w przypadku importu pliku zawierającego już zarejestrowane dane w systemie może prowadzić do błędnego zinterpretowania przez użytkownika funkcjonowania systemu.
Rekomendacje	Zaleca się rozważenie dokonania modyfikacji aplikacji o funkcjonalność umożliwiającą informowanie użytkownika o dokonywanych zmianach w bazie w przypadku importu pliku XML zawierającego dane odnoszące się do już istniejącego w bazie KSI SIMIK 07-13 wniosku aplikacyjnego/umowy o płatność/wniosku o płatność.
Odpowiedź	Odpowiedź MF: Import kolejnych wersji dokumentów jest widoczny w SIMIK XML. W przypadku zmiany którejkolwiek z wartości jest ona zapisywana w historii pól tabel, zgodnie z wymaganiem użytkownika. W tej tabeli są widoczne zmiany jakich dokonał użytkownik. Wersje importowanych plików są umieszczone w SIMIK XML. Mając na uwadze powyższa funkcjonalność uwaga dotycząca nie informowania użytkownika o dokonanych zmianach nie jest zasadna.
Termin wdrożenia	
Stanowisko Instytucji Audytowej	Wyjaśnienie: W przypadku importu pliku nowego, zawierającego nie istniejące w SIMIK dane, użytkownik dostaje informację zwrotną, że import przebiegł pomyślnie, lub plik został odrzucony.

W przypadku importu pliku, który zawiera istniejące już w KSI dane (aktualizacja danych), użytkownik nie otrzymuje informacji, że zaktualizowano w bazie KSI SIMIK już istniejące dane.

W historii pól tabel w Oracle Discoverer jest to widoczne i dane te można odtworzyć, ale ewentualny monit użytkownika, że będzie aktualizował zawarte w KSI dane, (najlepiej przed ich importem), byłby wskazany.

8.40. Kontrole aplikacyjne – Sprawdzanie właściwości, kompletności i autentyczności

Priorytet	Średni
Ustalenia	Pozostawienie użytkownikom różnych Instytucji możliwości automatycznego usuwania danych może prowadzić do braku zgodności i integralności przetwarzanych w KSI informacji. Zgodnie z otrzymanymi informacjami w chwili obecnej odbywają się konsultacje pomiędzy MRR a zaangażowanymi Instytucjami w sprawie ustalenia szczegółowych procedur usuwania danych z systemu KSI. Obecnie nie istnieją formalne wytyczne dotyczące tego obszaru.
Implikacje	Brak formalnych procedur usuwania (oraz automatycznego usuwania) danych z systemu może prowadzić do braku integralności przetwarzanych danych w KSI.
Rekomendacje	Zaleca się opracowanie i wdrożenie szczegółowych procedur dotyczących usuwania/zmiany danych w systemie KSI.
Odpowiedź	Odpowiedź MRR: Odpowiednia modyfikacja zostanie zgłoszona do realizacji. Odpowiednie procedury zostaną opracowane.
Termin wdrożenia	18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

8.41. Kontrole aplikacyjne – Sprawdzanie integralności i wiarygodności

Priorytet	Średni
Ustalenia	Podczas prowadzonych badań audytowych stwierdzono, iż uzyskanie informacji dotyczących historii zmian danych (przykładowo ustalenie tożsamości osoby, która usunęła dany wniosek aplikacyjny/umowę/wniosek o płatność, loginy osób wprowadzających dane do systemu i importujących pliki XML) jest czasochłonne i wymaga specjalistycznej wiedzy informatycznej – trzeba wykonać niestandardowy raport przy pomocy aplikacji *Oracle Discoverer*.
Implikacje	Brak prostego dostępu użytkowników do historii zmian dokumentu uniemożliwia właściwą kontrolę przeciwdziałającą wprowadzaniu nieautoryzowanych zmian w systemie.
Rekomendacje	Zaleca się dokonanie modyfikacji systemu KSI SIMIK 07-13 o funkcjonalność umożliwiającą prosty dostęp do historii zmian dokumentu (np. poprzez zdefiniowanie standardowego raportu w *Oracle Discoverer* lub implementację historii zmian w aplikacji).
Odpowiedź	Odpowiedź MRR: W chwili obecnej realizowana jest zmiana polegająca na dodaniu (widocznych na ekranie) informacji „kto, kiedy utworzył modyfikował". Dodatkowo odpowiedni standardowy raport zostanie zaprojektowany.
Termin wdrożenia	18 lipca 2008 r.
Stanowisko Instytucji Audytowej	Odpowiedź na rekomendację została przyjęta.

INDEKS SKRÓTÓW

ABI	Administrator Bezpieczeństwa Informacja
AI	Administrator Informacji
AM I	Administrator Merytoryczny w Instytucji
AM IK NSRO	Administrator Merytoryczny w Instytucji Koordynującej Narodowe Strategiczne Ramy Odniesienia
AM IZ	Administrator Merytoryczny w Instytucji Zarządzającej
AT	Administrator Techniczny
CCI	(fr.) Code commun d'identification – Kod jednolitego dokumentu programowego
CRAMM	(ang.) CCTA Risk Analysis and Method Management
DEF	Departament Ekonomiczno – Finansowy Ministerstwa Rozwoju Regionalnego
DMZ	(ang.) Demilitarized Zone
Główny Dostawca	Ministerstwo Finansów, Departament Rozwoju Systemów Informatycznych
Główny Użytkownik	Ministerstwo Rozwoju Regionalnego
HTTP	(ang.) Hypertext Tranfer Protocol
HTTPS	(ang.) Hypertext Tranfer Protocol Secure
IIS	(ang.) Internet Information Services
IK NSRO	Instytucja Koordynująca Narodowe Strategiczne Ramy Odniesienia
IP	Instytucja Pośrednicząca
IP2	Instytucja Pośrednicząca II stopnia
IZ	Instytucja Zarządzająca
KSI KSI SIMIK	Krajowy System Informatyczny System Informatyczny Monitoringu i Kontroli
LAN	(ang.) Local Aera Network
LSI	Lokalny System Informatyczny
MF	Ministerstwo Finansów
MRR	Ministerstwo Rozwoju Regionalnego
NSRO	Narodowe Strategiczne Ramy Odniesienia 2007-2013
PBI	Polityka Bezpieczeństwa Krajowego Systemu Informatycznego SIMIK 07-13 – Dokument Główny, zatwierdzona 28.04.2008 r. w wersji 1.3.

PIX	(ang.) Cisco Secure Pix Firewall
PO	Program Operacyjny
PRINCE2	(ang.) Projects in a Controlled Environment
RUP	(ang.) Rational Unified Process
SIMIK	Krajowy System Informatyczny System Informatyczny Monitoringu i Kontroli
SFC2007	(ang.) System for Fund Management in the European Community 2007-2013
UE	Unia Europejska
UPS	(ang.) Uninterruptible Power Supply
VLAN	(ang.) Virtual Local Aera Network
XML	(ang.) Extensible Markup Language
XSD	(ang.) Extensible Markup Language Schema Definition
ZBI	Zespół ds. Bezpieczeństwa Informacji
ZK	Zespół Kryzysowy

PODSEKRETARZ STANU
Generalny Inspektor Kontroli Skarbowej
Andrzej Parafianowicz