EBA/REC/2017/03

28/03/2018

Zalecenia

dotyczące zlecania zadań dostawcom usług w chmurze

1. Obowiązki dotyczące zgodności z przepisami i sprawozdawczości

Status niniejszych zaleceń

1. Niniejszy dokument zawiera zalecenia wydane zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010, właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do tych zaleceń.

2. Zalecenia przedstawiają stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo UE w konkretnym obszarze. Właściwe organy określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których zalecenia mają zastosowanie, powinny stosować się do zaleceń poprzez wprowadzenie ich odpowiednio do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również jeżeli zalecenia są skierowane przede wszystkim do instytucji.

Wymogi sprawozdawcze

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą powiadomić EUNB, czy stosują się lub czy zamierzają zastosować się do niniejszych zaleceń lub podają powody niestosowania się do dnia 28.05.2018. W przypadku braku powiadomienia w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych zaleceń. Powiadomienia należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na adres e-mail compliance@eba.europa.eu z dopiskiem „EBA/REC/2017/03”. Powiadomienia przekazują osoby odpowiednio upoważnione do informowania o stosowaniu się do zaleceń w imieniu właściwych organów. Wszelkie zmiany dotyczące stosowania się do zaleceń także należy zgłaszać do EUNB.

4. Zgodnie z art. 16 ust. 3 powiadomienia publikuje się na stronie internetowej EUNB.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot i zakres stosowania

1. Niniejsze zalecenia precyzują warunki dotyczące outsourcingu, zgodnie z wytycznymi CEBS dotyczącymi outsourcingu z dnia 14 grudnia 2006 r. i mają zastosowanie do outsourcingu zleconego przez instytucje określone w art. 4 ust. 1 pkt 3 rozporządzenia (UE) nr 575/2013 do dostawców usług w chmurze.

Adresaci

2. Niniejsze zalecenia skierowane są do właściwych organów określonych w art. 4 ust. 2 ppkt (i) rozporządzenia (UE) nr 1093/2010 oraz do instytucji określonych w art. 4 ust. 1 pkt 3 rozporządzenia nr 575/2013.[2]

Definicje

3. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE[3] w sprawie wymogów kapitałowych oraz w wytycznych CEBS mają w niniejszych zaleceniach takie samo znaczenie. Ponadto do celów niniejszych zaleceń stosuje się następujące definicje:

Usługi w chmurze	Usługi dostarczone przy wykorzystaniu przetwarzania w chmurze, to znaczy modelu umożliwiającego dogodny dostęp na żądanie z dowolnego miejsca, za pośrednictwem sieci, do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, przechowywania danych, aplikacji i usług), które można szybko zapewniać i udostępniać przy minimalnych działaniach w zakresie zarządzania czy też minimalnej interakcji z dostawcą usługi.
Chmura publiczna	Infrastruktura chmury dostępna do użytku przez ogół społeczeństwa
Chmura prywatna	Infrastruktura chmury dostępna do wyłącznego użytku jednej instytucji
Chmura społecznościowa	Infrastruktura chmury dostępna do wyłącznego użytku konkretnej wspólnoty instytucji, w tym kilku instytucji z jednej grupy.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012.

[3] dyrektywę Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniającą dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE;

Chmura hybrydowa	Infrastruktura chmury złożona z dwóch lub więcej odrębnych infrastruktur.

3. Wdrożenie

Data rozpoczęcia stosowania

5. Niniejsze zalecenia stosuje się od dnia 1 lipca 2018 r.

4. Zalecenia dotyczące zlecania zadań dostawcom usług w chmurze

4.1 Ocena istotności

1. Instytucje korzystające z outsourcingu powinny, przed jakimkolwiek zleceniem swoich zadań usługodawcom zewnętrznym, ocenić, które zadania należy uznać za istotne. Instytucje powinny przeprowadzić tę ocenę istotności zadań na podstawie wytycznej 1 lit. f) wytycznych CEBS oraz, w szczególności w odniesieniu do zlecenia zadań dostawcy usług w chmurze, biorąc pod uwagę wszystkie następujące kwestie:

    (a) krytyczność i właściwy profil ryzyka zadań, które mają zostać zlecone do realizacji poza jednostką, tj. czy są to zadania, które są kluczowe dla ciągłości działania/rentowności instytucji i jej zobowiązań wobec klientów;

    (b) bezpośrednie skutki operacyjne wyłączeń i związanego z nimi ryzyka prawnego i ryzyka utraty reputacji;

    (c) wpływ, jaki może mieć jakiekolwiek zakłócenie działalności na prognozowane dochody instytucji;

    (d) możliwy wpływ naruszenia poufności lub niezapewnienia spójności danych na instytucję i jej klientów.

4.2 Obowiązek odpowiedniego poinformowania organów nadzoru

2. Instytucje korzystające z outsourcingu powinny odpowiednio informować właściwe organy o zleceniu istotnych zadań dostawcom usług w chmurze. Instytucje powinny poinformować właściwe organy na podstawie pkt 4.3 wytycznych CEBS oraz w każdym przypadku udostępnić właściwym organom następujące informacje dotyczące:

    (a) nazwy dostawcy usług w chmurze i nazwy jego spółki dominującej (jeżeli istnieje);
    (b) opisu zadań i danych, które będą zlecone do realizacji poza jednostką;
    (c) państwa lub państw, na terenie których usługa (w tym lokalizacja danych) będzie wykonywana;
    (d) daty rozpoczęcia usługi;
    (e) daty ostatniego przedłużenia umowy (w stosownych przypadkach);
    (f) właściwego prawa, któremu podlega umowa;
    (g) daty wygaśnięcia usługi lub daty następnego przedłużenia umowy (w stosownych przypadkach).

3. Poza informacjami udzielonymi zgodnie z poprzednim akapitem, właściwy organ może prosić instytucję korzystającą z outsourcingu o udzielenie dodatkowych informacji na temat analizy ryzyka dotyczącej istotnych zadań, które będą zlecone do realizacji poza jednostką, na przykład:

   (a) informacji o istnieniu planu ciągłości działania dostawcy usług w chmurze, który jest odpowiedni dla usług świadczonych wobec instytucji korzystającej z outsourcingu;
   (b) informacji o posiadaniu przez instytucję korzystającą z outsourcingu strategii wyjścia na wypadek rozwiązania umowy przez którąkolwiek ze stron lub zakłócenia świadczenia usług przez dostawcę usług w chmurze;
   (c) informacji o zachowywaniu przez instytucję korzystającą z outsourcingu umiejętności i zasobów potrzebnych do odpowiedniego monitorowania działań zleconych na zewnątrz.

4. Instytucja korzystająca z outsourcingu powinna prowadzić zaktualizowany rejestr informacji na temat wszystkich swoich istotnych i nieistotnych działań zleconych dostawcom usług w chmurze na poziomie instytucji i grupy. Instytucja korzystająca z outsourcingu powinna udostępnić właściwemu organowi, na jego prośbę, kopię porozumienia w sprawie outsourcingu i związane z nim informacje zapisane w rejestrze, niezależnie od tego, czy działalność zlecona dostawcy usług w chmurze została oceniona przez instytucję jako istotna.

5. W rejestrze, o którym mowa w poprzednim paragrafie, należy zawrzeć co najmniej:

   (a) informacje, o których mowa w pkt 2 lit. a)-g), jeżeli nie zostały jeszcze dostarczone;
   (b) typ outsourcingu (model usługi w chmurze i model wdrażania chmury, tj. publiczny/prywatny/hybrydowy/chmura społecznościowa);
   (c) strony, dla których świadczy się usługę w chmurze w ramach porozumienia w sprawie outsourcingu;
   (d) dowód zatwierdzenia outsourcingu przez organ zarządzający lub oddelegowany komitet, jeżeli dotyczy;
   (e) nazwy wszystkich podwykonawców, jeżeli dotyczy;
   (f) państwa, na terenie których dostawca usług w chmurze/główny podwykonawca ma siedzibę;
   (g) informację o tym, czy działania zlecone do realizacji poza jednostką zostały ocenione jako istotne (tak/nie);
   (h) datę ostatniej przeprowadzonej przez instytucję oceny istotności dotyczącej działań zleconych do realizacji poza jednostką;
   (i) informację o tym, czy dostawca usług w chmurze/podwykonawcy wspierają działalność biznesową, która jest zależna od czasu (tak/nie);
   (j) ocena substytucyjności dostawcy usług w chmurze (łatwa, trudna lub niemożliwa);
   (k) w miarę możliwości należy wskazać alternatywnego dostawcę usług;
   (l) datę ostatniej oceny ryzyka dotyczącej umowy outsourcingowej lub umowy o podwykonawstwo.

4.3 Prawo do dostępu i prawo do audytu

W odniesieniu do instytucji

6. Na podstawie wytycznej 8 pkt 2 lit. g) wytycznych CEBS oraz do celów outsourcingu w chmurze instytucje korzystające z outsourcingu powinny również dopilnować zawarcia pisemnej umowy z dostawcą usług w chmurze, na mocy której ten ostatni zobowiąże się do:

   (a) zapewnienia instytucji, dowolnej osobie trzeciej wyznaczonej w tym celu przez instytucję oraz biegłemu rewidentowi instytucji pełnego dostępu do lokali należących do jego przedsiębiorstwa (siedzib i centrów operacyjnych), w tym wszystkich urządzeń, systemów, sieci i danych wykorzystywanych do świadczenia usług zleconych na zewnątrz (prawo do dostępu);

   (b) przyznania instytucji, dowolnej osobie trzeciej wyznaczonej w tym celu przez instytucję oraz biegłemu rewidentowi instytucji nieograniczonych praw w zakresie kontroli i audytu związanych z usługami zleconymi na zewnątrz (prawo do audytu).

7. Ustalenia umowne nie powinny utrudniać ani ograniczać skutecznego korzystania z prawa do dostępu i prawa do audytu. Jeżeli przeprowadzenie audytu lub stosowanie niektórych technik audytowych stwarzałoby ryzyko dla otoczenia innego klienta, należy uzgodnić alternatywne sposoby zapewnienia podobnego poziomu gwarancji wymaganego przez instytucję.

8. Instytucja korzystająca z outsourcingu powinna korzystać ze swojego prawa do audytu i prawa do dostępu w sposób oparty na ryzyku. Jeżeli instytucja korzystająca z outsourcingu nie bazuje na własnych zasobach audytowych, powinna rozważyć zastosowanie co najmniej jednego z następujących narzędzi:

   (a) zbiorczych audytów organizowanych wspólnie z innymi klientami tego samego dostawcy usług w chmurze i przeprowadzanymi przez tych samych klientów lub wyznaczoną przez nich osobę trzecią w celu bardziej efektywnego wykorzystania zasobów audytowych oraz zmniejszenia obciążenia organizacyjnego zarówno po stronie klientów, jak i dostawcy usług w chmurze;

   (b) certyfikatów osoby trzeciej oraz sprawozdań osoby trzeciej lub sprawozdań z audytu wewnętrznego udostępnionych przez dostawcę usług w chmurze, pod warunkiem że:

      i. instytucja korzystająca z outsourcingu zapewnia, aby zakres certyfikatu lub sprawozdania z audytu obejmował systemy (tj. procesy, aplikacje, infrastrukturę, centra danych itd.) oraz kontrole uznane za kluczowe przez instytucję korzystającą z outsourcingu;
      ii. instytucja korzystająca z outsourcingu na bieżąco szczegółowo analizuje treść certyfikatów lub sprawozdań z audytu, a w szczególności upewnia się czy kluczowe kontrole zostały uwzględnione w przyszłych wersjach sprawozdania z audytu, oraz sprawdza, czy certyfikat lub sprawozdanie z audytu nie są przestarzałe;

iii. instytucja korzystająca z outsourcingu jest zadowolona z umiejętności strony certyfikującej lub audytowej (np. w odniesieniu do rotacji firmy certyfikującej lub audytowej, kwalifikacji, wiedzy fachowej, ponownego przeprowadzania audytów / weryfikacji dowodów w podstawowej dokumentacji audytowej);

iv. certyfikaty zostaną wydane, a audyty przeprowadzone zgodnie z powszechnie uznawanymi standardami, przy czym będą obejmować badanie skuteczności operacyjnej kluczowych kontroli prowadzonych na miejscu;

v. instytucji korzystającej z outsourcingu przysługuje umowne prawo do żądania rozszerzenia zakresu certyfikatów lub sprawozdań z audytów na niektóre systemy lub kontrole, które są istotne. Liczba i częstotliwość takich żądań dotyczących modyfikacji zakresu powinna być rozsądna i uzasadniona z perspektywy zarządzania ryzykiem.

9. Biorąc pod uwagę fakt, że rozwiązania w chmurze charakteryzują się wysokim stopniem złożoności technicznej, instytucja korzystająca z outsourcingu powinna sprawdzić, czy personel prowadzący audyt – tj. audytorzy wewnętrzni lub grupa audytorów działających w jej imieniu lub audytorzy wyznaczeni przez dostawcę usług w chmurze – lub, w stosownych przypadkach, personel dokonujący przeglądu certyfikatu osoby trzeciej lub sprawozdań z audytu sporządzonych przez dostawcę usług posiada odpowiednie umiejętności i wiedzę do przeprowadzania skutecznych i odpowiednich audytów lub ocen dotyczących rozwiązań w chmurze.

W odniesieniu do właściwych organów

10. Na podstawie wytycznej 8 pkt 2 lit. h) wytycznych CEBS oraz do celów outsourcingu w chmurze instytucje korzystające z outsourcingu powinny dopilnować zawarcia pisemnej umowy z dostawcą usług w chmurze, na mocy której ten ostatni zobowiąże się do:

(a) zapewnienia właściwemu organowi nadzorującemu instytucję korzystającą z outsourcingu (lub dowolnej osobie trzeciej wyznaczonej w tym celu przez ten organ) pełnego dostępu do lokali należących do dostawcy usług w chmurze (siedzib i centrów operacyjnych), w tym wszystkich urządzeń, systemów, sieci i danych wykorzystywanych do świadczenia usług instytucji korzystającej z outsourcingu (prawo do dostępu);

(b) przyznania właściwemu organowi nadzorującemu instytucję korzystającą z outsourcingu (lub dowolnej osobie trzeciej wyznaczonej w tym celu przez ten organ) nieograniczonych praw w zakresie kontroli i audytu związanych z usługami zleconymi na zewnątrz (prawo do audytu).

11. Instytucja korzystająca z outsourcingu powinna dopilnować, aby postanowienia umowne nie utrudniały właściwemu organowi sprawowania funkcji nadzorczej i wykonywania celów.

12. Informacje uzyskane przez właściwe organy w wyniku wykonywania prawa do dostępu i prawa do audytu powinny zostać objęte obowiązkiem zachowania tajemnicy zawodowej lub służbowej, o którym mowa w art. 53 i nast. dyrektywy 2013/36/UE (CRD IV). Właściwe organy powinny powstrzymać się od zawierania wszelkiego rodzaju postanowień umownych lub składania

oświadczeń, które uniemożliwiłyby im przestrzeganie przepisów unijnych dotyczących poufności, zachowania tajemnicy zawodowej lub służbowej i wymiany informacji.

13. W oparciu o wyniki przeprowadzonego przez siebie audytu właściwy organ powinien zająć się wszelkimi wykrytymi niedociągnięciami, w razie potrzeby nakładając środki bezpośrednio na instytucję korzystającą z outsourcingu.

4.4 Prawo do dostępu

14. Umowa, o której mowa w pkt 6 i 10, powinna zawierać następujące postanowienia:

(a) strona, która zamierza skorzystać ze swojego prawa do dostępu (instytucja, właściwy organ, audytor lub osoba trzecia działająca w imieniu instytucji lub właściwego organu) powinna zawiadomić w rozsądnym terminie o planowanej kontroli w danej lokalizacji przedsiębiorstwa, chyba że wcześniejsze powiadomienie nie było możliwe ze względu na sytuację nadzwyczajną lub kryzysową;

(b) dostawca usług w chmurze jest zobowiązany do pełnej współpracy z odpowiednimi właściwymi organami oraz daną instytucją i jej audytorem, w związku z kontrolą na miejscu.

4.5 Bezpieczeństwo danych i systemów

15. Jak określono w wytycznej 8 pkt 2 lit. e) wytycznych CEBS umowa outsourcingowa powinna zobowiązywać dostawcę usług outsourcingowych do ochrony poufności informacji przekazywanych przez instytucję finansową. Zgodnie z wytyczną 6 pkt 6 lit. e) wytycznych CEBS instytucje powinny wdrożyć ustalenia zapewniające ciągłość usług świadczonych przez dostawców usług outsourcingowych. Na podstawie wytycznej 8 pkt 2 lit. b) i wytycznej 9 wytycznych CEBS, odpowiednie potrzeby instytucji korzystających z outsourcingu w zakresie jakości i wyników powinny zostać uwzględnione w pisemnych umowach outsourcingowych i umowach o gwarantowanym poziomie usług. Te aspekty bezpieczeństwa powinny być również na bieżąco monitorowane (wytyczna 7).

16. Do celów poprzedniego punktu, przed outsourcingiem i w celu poinformowania o odpowiedniej decyzji, instytucja powinna wykonać co najmniej następujące czynności:

(a) określić i sklasyfikować swoje działania, procesy i związane z nimi dane oraz systemy w odniesieniu do wrażliwości i wymaganej ochrony;

(b) dokonać dokładnego opartego na ryzyku wyboru działań, procesów i związanych z nimi danych i systemów, które planuje się zlecić na zewnątrz w ramach rozwiązania typu cloud computing;

(c) określić i podjąć decyzję o odpowiednim poziomie ochrony poufności danych, ciągłości zleconych działań oraz integralności i identyfikowalności danych i systemów w kontekście zamierzonego outsourcingu w chmurze. Instytucje powinny również rozważyć szczególne środki, tam gdzie jest to konieczne w odniesieniu do przesyłanych danych, danych znajdujących się w pamięci i danych odłożonych, takie jak wykorzystanie technologii szyfrowania w połączeniu z odpowiednią architekturą zarządzania kluczami.

17. Następnie instytucje powinny dopilnować zawarcia pisemnej umowy z dostawcą usług w chmurze, w której m.in. określa się zobowiązania tego ostatniego zgodnie z pkt 16 lit. c).

18. Instytucje powinny na bieżąco monitorować wykonywanie działań i stosowanie środków bezpieczeństwa zgodnie z wytyczną 7 wytycznych CEBS, w tym incydentów, oraz, w stosownych przypadkach, sprawdzać, czy zlecane przez nie działania są zgodne z wcześniejszymi punktami; powinny niezwłocznie podejmować wszelkie wymagane środki naprawcze.

4.6 Lokalizacja i przetwarzanie danych

19. Jak stwierdzono w wytycznej 4 pkt 4 wytycznych CEBS instytucje powinny zachować szczególną ostrożność podczas zawierania umów outsourcingowych i zarządzania takimi umowami poza EOG, ze względu na możliwe ryzyko związane z ochroną danych i skutecznym nadzorem sprawowanym przez organ nadzorczy.

20. Instytucja korzystająca z outsourcingu powinna przyjąć oparte na ryzyku podejście do kwestii lokalizacji danych i przetwarzania danych podczas outsourcingu do środowiska chmury. Ocena powinna dotyczyć potencjalnych skutków ryzyka, w tym ryzyka prawnego i kwestii zgodności z przepisami oraz ograniczeń nadzorczych związanych z państwami, w których usługi zlecone są lub mogą być świadczone oraz w których dane są lub mogą być przechowywane. Ocena powinna obejmować kwestie dotyczące szerszej stabilności politycznej i stabilności bezpieczeństwa danych jurysdykcji, przepisy obowiązujące w tych jurysdykcjach (w tym przepisy dotyczące ochrony danych); oraz przepisy dotyczące egzekwowania prawa w tych jurysdykcjach, w tym przepisy z zakresu prawa dotyczącego niewypłacalności, które miałyby zastosowanie w przypadku niewywiązania się przez dostawcę usług w chmurze ze swoich obowiązków. Instytucja korzystająca z outsourcingu powinna zapewnić, aby ryzyko to utrzymywało się w dopuszczalnych granicach proporcjonalnie do istotności zleconej działalności.

4.7 Outsourcing łańcuchowy

21. Jak stwierdzono w wytycznej 10 wytycznych CEBS instytucje powinny uwzględnić ryzyko związane z outsourcingiem łańcuchowym, w przypadku gdy dostawca usług outsourcingowych podzleca wykonanie elementów danej usługi innym dostawcom. Instytucja korzystająca z outsourcingu powinna zgodzić się na outsourcing łańcuchowy tylko wtedy, gdy podwykonawca w pełni wywiąże się również z obowiązków względem instytucji korzystającej z outsourcingu i dostawcy usług outsourcingowych. Ponadto instytucja korzystająca z outsourcingu powinna podjąć odpowiednie kroki w celu wyeliminowania ryzyka wystąpienia jakichkolwiek słabości lub niepowodzeń w wykonywaniu podzleconych działań mających znaczący wpływ na zdolność dostawcy usług outsourcingowych do wywiązania się ze swoich obowiązków wynikających z umowy outsourcingowej.

22. W umowie outsourcingowej zawartej między instytucją korzystającą z outsourcingu a dostawcą usług w chmurze należy określić wszelkie rodzaje działalności, które są wyłączone z potencjalnego podwykonawstwa, oraz wskazać, że dostawca usług w chmurze zachowuje pełną odpowiedzialność za usługi zlecone podwykonawcom i sprawuje nad nimi nadzór.

23. Umowa outsourcingowa powinna również zawierać zobowiązanie dostawcy usług w chmurze do informowania instytucji korzystającej z outsourcingu o wszelkich planowanych istotnych zmianach dotyczących podwykonawców lub usług zlecanych podwykonawcom wymienionych w pierwotnej umowie, które mogą wpłynąć na zdolność dostawcy usług do wywiązania się z obowiązków wynikających z umowy outsourcingowej. Okres powiadamiania o tych zmianach należy uprzednio uzgodnić umownie, aby umożliwić instytucji korzystającej z outsourcingu

przeprowadzenie oceny ryzyka skutków proponowanych zmian przed wprowadzeniem rzeczywistej zmiany dotyczącej podwykonawcy lub usług zleconych podwykonawcom.

24. Jeżeli dostawca usług w chmurze planuje wprowadzić zmiany dotyczące podwykonawcy lub usług zleconych podwykonawcom, które niekorzystnie wpłynęłyby na ocenę ryzyka uzgodnionych usług, instytucji korzystającej z outsourcingu powinno przysługiwać prawo do rozwiązania umowy.

25. Instytucja korzystająca z outsourcingu powinna na bieżąco dokonywać przeglądu i monitorować proces świadczenia całej usługi, niezależnie od tego, czy jest świadczona przez dostawcę usług w chmurze czy jego podwykonawców.

4.8 Plany awaryjne i strategie wyjścia

26. Jak stwierdzono w wytycznych 6 pkt 1, 6 pkt 6 lit. e) i 8 pkt 2 lit. d) wytycznych CEBS instytucja korzystająca z outsourcingu powinna planować i wdrażać ustalenia w celu utrzymania ciągłości swojej działalności na wypadek, gdyby świadczenie usług przez dostawcę usług outsourcingowych zakończyło się niepowodzeniem lub uległo pogorszeniu w niedopuszczalnym stopniu. Ustalenia te powinny obejmować planowanie awaryjne oraz jasno określoną strategię wyjścia. Ponadto umowa outsourcingowa powinna zawierać klauzulę dotyczącą rozwiązania umowy i zarządzania wyjściem, która umożliwia przeniesienie działań prowadzonych przez dostawcę usług outsourcingowych na innego tego typu dostawcę lub ponowne włączenie ich do instytucji korzystającej z outsourcingu.

27. Instytucja korzystająca z outsourcingu powinna również zapewnić, że, w razie konieczności, jest w stanie zrezygnować z ustaleń dotyczących outsourcingu w chmurze w taki sposób, aby nie spowodować zbędnych utrudnień w zakresie świadczenia usług, nie zaszkodzić ich zgodności z systemem regulacyjnym oraz ciągłości i jakości świadczenia usług na rzecz klientów. Aby to osiągnąć, instytucja korzystająca z outsourcingu powinna:

    (a) opracować i wdrożyć plany wyjścia, które są kompleksowe, dobrze udokumentowane i odpowiednio przetestowane w stosownych przypadkach;

    (b) określić alternatywne rozwiązania i opracować plany przejściowe umożliwiające usunięcie i przeniesienie istniejących działań i danych od dostawcy usług w chmurze do tych rozwiązań w sposób kontrolowany i odpowiednio przetestowany, uwzględniając lokalizację danych i utrzymanie ciągłości działalności w fazie przejściowej;

    (c) zapewnić, aby umowa outsourcingowa zawierała zobowiązanie dostawcy usług w chmurze do zapewnienia odpowiedniego wsparcia instytucji korzystającej z outsourcingu podczas prawidłowego przenoszenia działalności na innego dostawcę usług lub oddania jej w bezpośrednie zarządzanie instytucji korzystającej z outsourcingu w przypadku rozwiązania umowy outsourcingowej.

28. Opracowując strategie wyjścia instytucja korzystająca z outsourcingu powinna rozważyć:

(a) opracowanie kluczowych wskaźników ryzyka w celu określenia niedopuszczalnego poziomu usługi;

(b) przeprowadzenie analizy wpływu na działalność gospodarczą współmierną do zleconych działań w celu określenia, jakie zasoby ludzkie i materialne byłyby wymagane do wdrożenia planu wyjścia i jak wiele czasu zajęłoby wdrożenie takiego planu;

(c) przydzielenie ról i obowiązków w zakresie zarządzania planami wyjścia i działaniami związanymi z przeniesieniem;

(d) określenie kryteriów dotyczących pomyślnego przeniesienia.

29. Instytucja korzystająca z outsourcingu powinna uwzględniać wskaźniki, które mogą doprowadzić do uruchomienia planu wyjścia, podczas bieżącego monitorowania procesu świadczenia usług i prowadzenia nadzoru nad usługami świadczonymi przez dostawcę usług w chmurze.