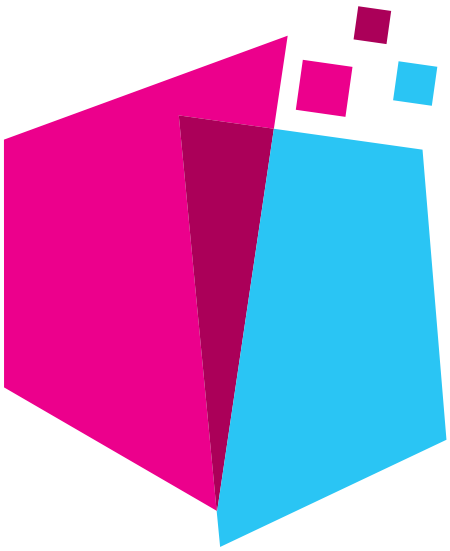


Polish Cloud

STANDARD WDROŻEŃ PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

Związek Banków Polskich

Standard wdrożeń w chmurze obliczeniowej publicznej lub hybrydowej został opracowany w ramach prac grupy roboczej powołanej przy Forum Technologii Bankowych ZBP i Radzie Bankowości Elektronicznej ZBP.

AUTORZY STANDARDU

Bankowa grupa robocza przy Związku Banków Polskich:

Alior Bank S.A., Bank BPH S.A., Bank Handlowy w Warszawie S.A., BNP Paribas Bank Polska S.A., BOŚ Bank S.A., Credit Agricole Bank Polska S.A., Getin Noble Bank S.A., Idea Bank S.A., ING Bank Śląski S.A., Pekao S.A., PKO Bank Polski S.A., przy aktywnym udziale Operatora Chmury Krajowej sp. z o.o.

w składzie:

Grzegorz Pędzisz (przewodniczący) [Idea Bank S.A.],
Aneta Ostrowska [PKO Bank Polski S.A.],
Bartosz Ptak [Operator Chmury Krajowej sp. z o.o.],
Jacek Skorupka [Idea Bank S.A.],
Marek Dryjański [Bank Handlowy w Warszawie S.A.],
Adam Gutenbaum [PKO Bank Polski S.A.],
Maciej Leśniewski [Pekao S.A.], oraz
Magdalena Przyżycka [Idea Bank S.A.], Tomasz Fryc [Alior Bank S.A.], Artur Rudziński [Alior Bank S.A.], Magdalena Perfońska [Bank BPH S.A.], Marcin Wiśniewski [Bank BPH S.A.], Bogusław Borgosz [BNP Paribas Bank Polski S.A.], Krzysztof Turek [BOŚ Bank S.A.], Konrad Ciukaj [Europejski Fundusz Leasingowy S.A.], Jacek Mainda [Credit Agricole Bank Polska S.A.], Miłosław Sabiniarz [Credit Agricole Bank Polska S.A.], Michał Cichocki [Getin Noble Bank S.A.], Szymon Sobczak [Getin Noble Bank S.A.], Andrzej Mandel [Getin Noble Bank S.A.], Łukasz Śledzikowski [ING Bank Śląski S.A.], Adrian Dorobisz [ING Bank Śląski S.A.], Norbert Górski [ING Bank Śląski S.A.], Michał Jurga [ING Bank Śląski S.A.], Mikołaj Kujawa [ING Bank Śląski S.A.], Jacek Cholc [PKO Bank Polski S.A.], Jacek Zegan [PKO Bank Polski S.A.].

Prezydium bankowej grupy roboczej przy Związku Banków Polskich:

1. Wojciech Pantkowski, Dyrektor Zespołu Systemów Płatniczych i Bankowości Elektronicznej, Związek Banków Polskich
2. Joanna Barbrich, Zespół Systemów Płatniczych i Bankowości Elektronicznej, Związek Banków Polskich
3. Maciej Kostro, Doradca Zarządu, Związek Banków Polskich
4. Grzegorz Pędzisz, CIO, Idea Bank S.A.
5. Marek Dryjański, Kierownik Biura Nowych Technologii i Relacji Strategicznych, Bank Handlowy w Warszawie S.A.
6. Jacek Cholc, Dyrektor Pionu Eksploatacji i Infrastruktury, PKO BP S.A.

Konsultant:

Accenture sp. z o. o.:

1. Łukasz Jęczmiński, Cloud Transformation and Migration, Manager
2. Grzegorz Żurawski, Security Strategy and Risk, Consultant
3. Łukasz Kundziewicz, Security Strategy and Risk, Senior Analyst

Koordynator prawny:

Kochański & Partners sp.k.:

1. Daniel Kozłowski, adwokat, Sektor Usług Finansowych, główny koordynator prawny wdrożeń chmurowych
2. Aleksandra Piech, radca prawny, Sektor Nowych Technologii, specjalista ds. wdrożeń chmurowych
3. Dr Agnieszka Serzysko, radca prawny, Partner, Sektor Usług Finansowych

Standard został skonsultowany w ramach grupy podmiotów opiniujących:

mBank S.A., Google Poland sp. z o.o., Oracle Polska sp. z o.o., Hitachi Ltd, Dell sp. z o.o., Cisco Systems Poland sp. z o.o., Microsoft Polska sp. z o.o.

SPIS TREŚCI

1. WSTĘP

Wychodząc naprzeciw oczekiwaniom rynku bankowego w Polsce w zakresie możliwości wdrażania rozwiązań opartych o chmurę obliczeniową w podmiotach objętych nadzorem bankowym, powołaliśmy przy Związku Banków Polskich i Forum Technologii Bankowych dedykowaną temu tematowi grupę roboczą.

Sektor bankowy w Polsce porusza się w ramach ustaw, rozporządzeń, jak również rekomendacji i wytycznych nadzoru finansowego regulujących jego działalność. Adaptacja najnowszych rozwiązań technologicznych w bankowości w ramach tych regulacji nie jest zadaniem łatwym. Zainteresowanie sektora bankowego, przy jednocześnie niewielkiej praktyce banków w zakresie wykorzystania usług chmurowych, skłoniło Autorów niniejszego opracowania do zaproponowania bankom stworzenia wspólnej inicjatywy, w celu opracowania standardu wdrożenia rozwiązań informatycznych opartych o chmurę obliczeniową w bankach zgodnie z obowiązującymi regulacjami.

W październiku 2017 r. Urząd Komisji Nadzoru Finansowego opublikował komunikat dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej, który z jednej strony wprost dopuszczał korzystanie z usług chmurowych, lecz z drugiej wywoływał na rynku bankowym efekt mrożący dla ich wdrożeń. Mimo tego występowały przykłady wdrożeń przez banki, zarówno dotyczące aplikacji produkcyjnych, przetwarzających dane objęte tajemnicą bankową, rozwiązań testowych, czy też prostych aplikacji (jak e-learning), bazujących na chmurze obliczeniowej.

W dniu 24 stycznia 2020 r. (wydany w dniu 23 stycznia 2020 r.) Urząd Komisji Nadzoru Finansowego opublikował kolejny komunikat dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej („**Komunikat**"), który wyjaśnia wiele kwestii budzących wcześniej wątpliwości banków. Przy aktywnym udziale banków oraz Operatora Chmury Krajowej (Operator Chmury Krajowej sp. z o.o.), chcieliśmy wykorzystać doświadczenia płynące z dotychczasowych wdrożeń oraz przeanalizować postanowienia Komunikatu i w szerokim gronie bankowym wypracować wspólnie standard, stanowiący zbiór praktyk i rozwiązań umożliwiających bankom łatwe przejście przez proces adaptacji do chmury, zarówno całej organizacji, jak i w zakresie jedynie wybranych rozwiązań oferowanych przez dostawców usług chmurowych.

Sam Komunikat, zgodnie z jego brzmieniem, stanowi uzupełnienie i uszczegółowienie wybranych zaleceń w zakresie outsourcingu, opisanych między innymi w Rekomendacji D oraz ustawie 'Prawo bankowe'. Regulacje te muszą być brane pod uwagę przy określaniu możliwości, a następnie przy faktycznym wdrożeniu rozwiązań opartych o chmurę obliczeniową. Komunikat prezentuje podejście krajowe (model referencyjny), co oznacza, że wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Bankowego (EBA), które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, w tym - Wytyczne Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r., nie mają zastosowania do polskich banków.

Niniejszy Standard prezentuje, jakie zadania, procedury, procesy i analizy bank powinien przeprowadzić i udokumentować pod kątem przygotowania organizacji do działania w sferze usług chmurowych w odniesieniu do poszczególnych zapisów wybranych regulacji.

2. ZAŁOŻENIA

1. Niniejszy Standard odnosi się do wymogów dotyczących korzystania z rozwiązań chmurowych przez podmioty objęte nadzorem bankowym w rozumieniu Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (tj. Dz. U. z 2019 r. poz. 298, ze zmianami). Standard nie odnosi się zatem do wymogów dotyczących rozwiązań chmurowych dla podmiotów objętych innym nadzorem wskazanym w tej ustawie.
2. Standard analizuje wymogi Komunikatu, a co za tym idzie, przedstawia wymogi Urzędu Komisji Nadzoru Finansowego w przypadku przetwarzania w podmiotach objętych nadzorem bankowym informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej.
3. Standard podsumowuje również wymagania Prawa bankowego (zgodnie z definicją poniżej). Stosowany uzupełniająco do Komunikatu w modelu referencyjnym, wskazanym w pkt 1 powyżej (Wstęp).

3. TERMINOLOGIA STOSOWANA W STANDARDZIE. OBJAŚNIENIE WYBRANYCH DEFINICJI KOMUNIKATU

Bank - podmiot objęty nadzorem bankowym, w tym bank w rozumieniu Prawa bankowego (krajowy oraz zagraniczny), oddział banku krajowego za granicą, oddział i przedstawicielstwo banków zagranicznych w rozumieniu Prawa bankowego, oddział i przedstawicielstwo instytucji kredytowej w rozumieniu Prawa bankowego oraz bank spółdzielczy w rozumieniu Ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (z zakresu niniejszego Standardu wyłączone zostały podmioty nadzorowane w rozumieniu Ustawy o nadzorze nad rynkiem finansowym inne, niż podmioty podlegające nadzorowi bankowemu).

Chmura obliczeniowa - ma znaczenie nadane w Komunikacie terminowi „chmura obliczeniowa". Na potrzeby Standardu, przez Chmurę obliczeniową rozumiemy Chmurę obliczeniową publiczną i Chmurę obliczeniową hybrydową.

Chmura obliczeniowa hybrydowa - ma znaczenie nadane w Komunikacie terminowi „chmura obliczeniowa hybrydowa".

Chmura obliczeniowa publiczna - ma znaczenie nadane w Komunikacie terminowi „chmura obliczeniowa publiczna".

Chmura obliczeniowa prywatna - ma znaczenie nadane w Komunikacie terminowi „chmura obliczeniowa prywatna".

Chmura obliczeniowa społecznościowa - ma znaczenie nadane w Komunikacie terminowi „chmura obliczeniowa społecznościowa".

CPD - ma znaczenie nadane w Komunikacie terminowi „CPD".

Dostawca - ma znaczenie nadane w Komunikacie terminowi „dostawca usług chmury obliczeniowej".

EOG – oznacza Europejski Obszar Gospodarczy.

Kodeks cywilny – oznacza ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz. U. z 2019 r. poz. 1145, ze zmianami).

Komunikat – komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r., dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

KNF – Komisja Nadzoru Finansowego.

UKNF – Urząd Komisji Nadzoru Finansowego.

Outsourcing szczególny chmury obliczeniowej lub **Outsourcing szczególny** - ma znaczenie nadane w Komunikacie terminowi „outsourcing szczególny chmury obliczeniowej".

Prawo bankowe - oznacza ustawę z 29 sierpnia 1997 r. - Prawo bankowe (tj. Dz. U. z 2019 r. poz. 2357).

Rekomendacja D - rekomendacja wydana przez Urząd Komisji Nadzoru Finansowego w styczniu 2013 r., dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

RODO – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Standard - niniejsze opracowanie.

Tajemnica bankowa - ma znaczenie nadane w art. 104 Prawa bankowego, a więc „wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje".

Usługa chmury obliczeniowej - ma znaczenie nadane w Komunikacie terminowi „usługa chmury obliczeniowej".

Wytyczne EBA - Wytyczne Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r.

Poniższa tabela prezentuje dodatkowo definicje zawarte w Komunikacie, wraz z ich znaczeniem, w jakim są stosowane w niniejszym Standardzie i zgodnie z przyjętymi Założeniami, oraz tam, gdzie to stosowne, opatrzone komentarzem lub wyjaśnieniem:

Definicja z Komunikatu	Znaczenie przyjęte w Standardzie lub komentarz/wyjaśnienie
„chmura obliczeniowa społecznościowa"	Chmura obliczeniowa społecznościowa może mieć zarówno charakter: a) Chmury obliczeniowej prywatnej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy i jest przy tym zarządzana przez podmiot z grupy albo b) Chmury obliczeniowej publicznej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy, lecz jest przy tym zarządzana przez Dostawcę.
„informacja prawnie chroniona"	Tajemnica bankowa
„outsourcing szczególny chmury obliczeniowej"	Wyłącznie pomocniczo, zamieszczamy kryteria (referencje) w zakresie oceny, czy dana czynność jest istotna/podstawowa (w oparciu o kryteria zaproponowane przez Wytyczne EBA): a) czy umowa outsourcingu dotyczy bezpośrednio czynności bankowej, b) potencjalny wpływ zakłócenia lub niewykonania przez Dostawcę badanej czynności na uzgodnionym gwarantowanym poziomie usług w trybie ciągłym na: I. krótko- i długoterminową odporność i kondycję finansową, w tym, jeżeli dotyczy, jej aktywa, kapitał, koszty, finansowanie, płynność, zyski i straty, II. ciągłość działania i odporność operacyjną, III. ryzyko operacyjne, w tym prowadzenie działalności, technologie informacyjne i komunikacyjne (ICT) i ryzyko prawne, IV. ryzyko utraty reputacji, V. w stosownych przypadkach, planowanie w zakresie działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji, możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji oraz ciągłości operacyjnej w sytuacji wczesnej interwencji, działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji, c) potencjalny wpływ zlecenia badanej czynności na zdolność Banku do: I. identyfikacji ryzyka, zarządzania ryzykiem i jego monitorowania, II. spełnienia wszystkich wymogów prawnych i regulacyjnych, III. przeprowadzenia stosownych audytów dotyczących funkcji będących przedmiotem outsourcingu,

	d) potencjalny wpływ na usługi świadczone na rzecz klientów, e) wszelkie umowy outsourcingu, łączna ekspozycja Banku na tego samego Dostawcę oraz potencjalny łączny wpływ umów outsourcingu w tym samym obszarze działalności, f) rozmiar i złożoność danego obszaru działalności, g) możliwość rozszerzenia zakresu proponowanej umowy outsourcingu bez zastępowania lub zmiany umowy bazowej, h) zdolność do przeniesienia proponowanej umowy outsourcingu na innego Dostawcę, jeżeli jest to niezbędne lub pożądane, zarówno na podstawie umowy, jak i w praktyce, w tym szacunkowe ryzyko, przeszkody dla ciągłości działania, koszty i ramy czasowe z tym związane, i) zdolność do reintegracji czynności zleconej na zasadzie outsourcingu do Banku, jeżeli jest to niezbędne lub pożądane oraz j) ochronę danych i możliwy wpływ naruszenia poufności lub niezapewnienie dostępności i integralności danych na instytucję, lub instytucję płatniczą i jej klientów, w tym między innymi zgodność z RODO.
„poddostawca”	Poddostawcą w rozumieniu Komunikatu jest podmiot, który posiada lub może posiadać identyfikowany dostęp do informacji przetwarzanych przez podmiot nadzorowany. Przez identyfikowany dostęp do informacji przetwarzanych przez Bank rozumie się taki dostęp, który spełnia następujące kryteria: a) umożliwia poddostawcy identyfikację Banku-jako zleceniodawcy, b) dochodzi do ujawnienia przetwarzanych danych (informacji), przy czym rozumienie tego pojęcia, w zależności od dalszych wyjaśnień UKNF, może ulec zmianie.
„podmiot nadzorowany”	Bank
„zasada proporcjonalności”	Wyłącznie pomocniczo, zamieszczamy wyjaśnienie zasady proporcjonalności, którego brak w Komunikacie. Zgodnie z Wytycznymi EBA celem zasady proporcjonalności jest zapewnienie, aby zasady zarządzania, w tym te dotyczące outsourcingu, były spójne z indywidualnym profilem ryzyka, charakterem i modelem biznesowym instytucji lub instytucji płatniczej oraz skalą i złożonością jej działalności, tak aby skutecznie osiągnąć cele wymogów regulacyjnych. Banki, w myśl zasady proporcjonalności, powinny uwzględniać złożony charakter funkcji zlecanych na zasadzie outsourcingu, ryzyko wynikające z umowy outsourcingu, krytyczne lub istotne znaczenie funkcji zlecanej na zasadzie outsourcingu oraz potencjalny wpływ outsourcingu na ciągłość wykonywanej działalności. Banki stosując zasadę proporcjonalności, powinny uwzględniać kryteria określone w tytule i wytycznych EUNB (EBA) w sprawie zarządzania wewnętrznego zgodne z art. 74 ust. 2 dyrektywy 2013/36/UE. Wydaje się również, że „proporcjonalność” może być utożsamiana z „adekwatnością” w zależności od całościowej sytuacji Banku.

4. ORGANIZACJA DOKUMENTU

1. Standard został podzielony na rozdziały poświęcone regulacjom mającym wpływ na sposób implementacji Usług chmury obliczeniowej w sektorze bankowym.
2. W Rozdziale 5 oraz Rozdziale 6 opisane zostały rekomendacje i regulacje prawne wraz z odpowiednimi ustandaryzowanymi działaniami, jakie w ocenie Autorów należy podjąć celem wdrożenia Usługi chmury obliczeniowej zgodnie z daną regulacją.
3. Każdy z rozdziałów został opracowany poprzez (o ile ma zastosowanie):
   1) zacytowanie w nagłówku **rozdziału danego punktu regulacji**,
   2) podsumowanie **opisu wymagań** wynikających z regulacji,
   3) wskazanie **wymagań (produktów) po stronie Banku**,
   4) wskazanie **wymagań (produktów) po stronie Dostawcy** oraz
   5) wskazanie **szablonów lub przykładów dokumentów**.

5. KOMUNIKAT

5.1. PKT IV KOMUNIKATU - „WYTYCZNE STOSOWANIA”

IV. Wytyczne stosowania

1. W celu zapewnienia prawidłowego funkcjonowania rynku finansowego, jego stabilności oraz bezpieczeństwa, na podstawie art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, Nadzór oczekuje od podmiotów nadzorowanych stosowania niniejszego modelu referencyjnego podczas działań związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej, traktując go jako sprecyzowanie istniejących wymagań prawnych oraz bez uszczerbku dla tych wymagań, jeżeli:
   1) przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu niniejszego komunikatu lub
   2) przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej w rozumieniu niniejszego komunikatu i przetwarzanie informacji jest realizowane w chmurze obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną).

2. Nadrzędnym zadaniem podmiotu nadzorowanego podczas przetwarzania informacji w chmurze obliczeniowej jest zapewnienie bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z prawem. Stosowanie tego komunikatu powinno odbywać się z poszanowaniem zasady proporcjonalności przy równoległym uwzględnieniu modelu referencyjnego. Zasada proporcjonalności powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka związanego z planowaniem czynności przetwarzania oraz adekwatnością stosowanych zabezpieczeń przetwarzanych informacji. UKNF podkreśla, że zasada proporcjonalności nie powinna być interpretowana jako przyzwolenie na zastosowanie przez mniejsze podmioty nadzorowane mniej efektywnych zabezpieczeń przetwarzanych informacji, niż opisane w niniejszym komunikacie.

3. Nadzór podkreśla, że opisane w niniejszym komunikacie wymagania powinny być stosowane przez podmioty nadzorowane przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej.

4. W celu właściwego stosowania postanowień niniejszego komunikatu, podmiot nadzorowany powinien określić dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej:
   1) czy przetwarzane są informacje prawnie chronione oraz
   2) czy czynność przetwarzania może być definiowana jako outsourcing szczególny chmury obliczeniowej.

Matryca stosowania komunikatu		Outsourcing chmury obliczeniowej	
		inny niż szczególny	szczególny
Informacje	inne niż prawnie chronione	Komunikat może być stosowany	Komunikat powinien być stosowany
	prawnie chronione	Komunikat powinien być stosowany	

5. W przypadku kwalifikowania czynności lub informacji do więcej niż jednej kategorii według powyższej matrycy, należy przyjąć do stosowania wymaganie bardziej rygorystyczne.
6. Niezależnie od powyższego, komunikatu nie stosuje się, gdy stosowny, szczególny przepis prawa:
   1) wyklucza możliwość przetwarzania w chmurze obliczeniowej określonej informacji lub wyklucza możliwość wykonywania w chmurze obliczeniowej określonych czynności przetwarzania;
   2) nakłada wymóg spełnienia określonych wymagań technicznych lub organizacyjnych dotyczących przetwarzania określonych informacji, które wykluczałyby możliwość spełnienia wymagań niniejszego komunikatu.
7. Niniejszy komunikat nie musi być stosowany podczas projektowania i eksploatacji środowisk testowych lub rozwojowych w chmurze obliczeniowej, o ile w środowiskach tych nie są przetwarzane informacje prawnie chronione.
8. Komunikat nie dotyczy przetwarzania informacji w chmurze obliczeniowej prywatnej.

OPIS WYMAGAŃ

1. Komunikat musi być stosowany w dwóch przypadkach:
   a) przetwarzania Tajemnicy bankowej lub
   b) Outsourcingu szczególnego chmury obliczeniowej.
   W każdym innym przypadku Komunikat może być stosowany, jeśli Bank (również w porozumieniu z Dostawcą) tak postanowi.
2. Komunikat nie odnosi się do Chmury obliczeniowej prywatnej, w tym Chmury obliczeniowej społecznościowej o charakterze prywatnym.
3. Bank określa typ przetwarzanych danych (informacji) dla danej Usługi chmury obliczeniowej ze względu na Tajemnicę bankową oraz typ czynności ze względu na Outsourcing szczególny chmury obliczeniowej.
4. W procesie analizy oraz kwalifikacji przetwarzanych danych, Bank powinien odwoływać się do istniejących w Banku zasobów inwentaryzacji procesów krytycznych wynikających np. z BIA lub Rekomendacji H dotyczącej systemu kontroli wewnętrznej w bankach wydanej przez UKNF w kwietniu 2017 roku.
5. Jeśli Usługi chmury obliczeniowej są wykorzystywane wyłącznie do przetwarzania danych (informacji) testowych (zanonimizowanych), komunikatu się nie stosuje.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Dokument potwierdzający przeprowadzenie analizy w zakresie typu przetwarzanych danych (informacji), planowanej Usługi chmury obliczeniowej oraz rodzaju czynności przetwarzania, oraz jej kwalifikacji.
2. Dokument potwierdzający przeprowadzenie analizy w odniesieniu do wymagań Outsourcingu szczególnego chmury obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

N/D

SZABLONY

N/D

5.2. PKT V KOMUNIKATU - „WYTYCZNE DO KLASYFIKACJI I OCENY INFORMACJI”

V. Wytyczne do klasyfikacji i oceny informacji

1. Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację:
   1) informacji prawnie chronionych w rozumieniu niniejszego komunikatu;
   2) informacji, których ochrona wynika z uregulowań prawnych nieuwzględnionych w niniejszym komunikacie;
   3) informacji, które nie podlegają ochronie prawnej.
2. Ocena informacji przeprowadzona jest pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej, w szczególności biorąc pod uwagę:
   1) zgodność z wymaganiami prawa oraz specyficznymi dla danego sektora lub podmiotu nadzorowanego postanowieniami oraz zobowiązaniami umownymi;
   2) zakres klasyfikowanych informacji, ich rodzaj i ważność;
   3) wartość informacji dla podmiotu nadzorowanego.
3. Podmiot nadzorowany w procesie klasyfikacji i oceny informacji uwzględnia:
   1) skalę prowadzonej działalności;
   2) korporacyjne, grupowe lub inne modele lub metody oceny i klasyfikacji, które uwzględniają powyższe założenia i są wspólne dla grupy podmiotów, do których zalicza się podmiot nadzorowany;
   3) odpowiedzialność podmiotu nadzorowanego za przetwarzane informacje.
4. Podmiot nadzorowany powinien przeprowadzić klasyfikację i ocenę informacji ponownie, gdy:
   1) zamierza przetwarzać nowy rodzaj informacji;
   2) zamierza wykorzystać nową usługę chmury obliczeniowej;
   3) zmiana prawa, regulacji, regulaminów lub postanowień umów, których stroną jest podmiot nadzorowany, wpływa albo może wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w chmurze obliczeniowej;
   4) istotnie zwiększa się albo zmniejsza skala przetwarzania;
   5) istotnie zwiększa się wartość przetwarzanych informacji.
5. Podmiot nadzorowany powinien regularnie (lecz nie rzadziej niż raz w roku) przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji do bieżących warunków swojego działania.

OPIS WYMAGAŃ

1. Bank powinien na bieżąco monitorować zmiany w zakresie wymogów prawnych oraz regulacyjnych w zakresie, który wymagałby ponownej kwalifikacji przetwarzanych informacji.
2. Bank powinien nie rzadziej niż raz w roku przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji w odniesieniu do bieżących warunków swojej działalności.
3. Bank powinien nie rzadziej niż raz w roku zweryfikować, czy Usługa chmury obliczeniowej lub przetwarzane dane (informacje) nie są przetwarzane w CPD zlokalizowanym w innym regionie, niż w momencie rozpoczęcia dostarczania Usługi chmury obliczeniowej lub przetwarzania danych (informacji) w Chmurze obliczeniowej, przy czym wystarczające jest tu oświadczenie Dostawcy zgodnie z właściwą reprezentacją lub umocowaniem.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Opisany proces kwalifikacji i oceny informacji przetwarzanych w Chmurze obliczeniowej uwzględniający wytyczne opisane w punktach 1.1. do 1.3. oraz 3.1. do 3.3. ust. V (Wytyczne do klasyfikacji i oceny informacji) Komunikatu.
2. Udokumentowany standard klasyfikacji danych (informacji) stosowany przez Bank.

3. Udokumentowane wyniki klasyfikacji danych (informacji), które powinny zostać uwzględnione w planie przetwarzania danych (informacji) w Chmurze obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Poinformowanie Banku o zmianie miejsca przetwarzania danych (informacji) w Chmurze obliczeniowej.

SZABLONY

N/D

5.3. PKT VI KOMUNIKATU - „WYTYCZNE DO SZACOWANIA RYZYKA”

VI. Wytyczne do szacowania ryzyka

1. Podmiot nadzorowany prowadzi w udokumentowanym procesie kompleksowe szacowanie ryzyka (identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany), zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia. Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act”).
2. Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka, w kontekście wyników przeprowadzonej klasyfikacji i oceny przetwarzanych informacji w chmurze obliczeniowej, co najmniej:
   1) ogólne zagrożenia dla stosowania chmury obliczeniowej:
      a) rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami;
      b) możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony;
      c) dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmury obliczeniowej;
      d) dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej, jak i międzynarodowej;
      e) brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powodujący przywiązanie do jednego dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji (vendor lock-in);
      f) awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;
      g) podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmury obliczeniowej;
      h) ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania;
      i) ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej

oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;

j) podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a podmiot nadzorowany;

2) specyficzne zagrożenia dla stosowanych konkretnych (nazwanych) usług chmury obliczeniowej:
   a) możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego lub w środowisku, które nie podlega kontroli podmiotu nadzorowanego (np. prywatne urządzenia mobilne, dostęp z prywatnych lub publicznych sieci);
   b) możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji);
   c) stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego;
   d) stosowane mechanizmy uwierzytelniania oraz ich słabości;
3) specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego:
   a) wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach;
   b) zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmów integracji;
4) wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem;
5) stanowisko nadzoru w sprawie szyfrowania informacji, zgodnie z którym:
   a) szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;
   b) szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;
   c) brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny". Nadzór zaleca używanie algorytmów szyfrowania, które – bazując na dostępnych publicznie informacjach (np. opracowaniach merytorycznych, raportach jednostek zajmujących się cyberbezpieczeństwem lub kryptografią) – nie są uznane za skompromitowane. W przypadku używania algorytmu uznanego za skompromitowany, podmiot nadzorowany powinien niezwłocznie podjąć działania w celu zapewnienia bezpieczeństwa przetwarzanych informacji;
   d) informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy jest to technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne;
   e) informacje prawnie chronione muszą być szyfrowane zawsze „at rest" oraz „in transit". Nadzór dopuszcza sytuację, w której informacje prawnie chronione są szyfrowane „at rest" natychmiast po ich przesłaniu do chmury obliczeniowej przy założeniu jednoczesnego stosowania szyfrowania „in transit" i nie traktuje takiej sytuacji jako ujawnienia przetwarzanych informacji;
   f) Nadzór dopuszcza sytuację, w której podmiot nadzorowany powierza swojemu dostawcy usług (w tym dostawcy usług chmury obliczeniowej) generowanie lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej w usługach chmury obliczeniowej innego dostawcy usług chmury obliczeniowej, przy czym podmiot nadzorowany powinien w procesie szacowania ryzyka uwzględnić możliwość utraty swojego dostępu do kluczy szyfrujących;
6) stanowisko nadzoru w sprawie tworzenia łańcucha outsourcingowego, zgodnie z którym:
   a) tworzenie łańcucha outsourcingowego powinno być każdorazowo oceniane przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej, a w szczególności:

i. tworzenie łańcucha outsourcingowego w zakresie działalności nadzorowanej jest dopuszczalne wyłącznie w granicach przewidzianych przepisami prawa;
ii. tworzenie łańcucha outsourcingowego w zakresie innym niż w zakresie działalności nadzorowanej jest dopuszczalne, o ile nie jest wprost zakazane przez przepisy prawa lub postanowienia umowne;

b) zakres odpowiedzialności dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego może ulegać ograniczeniu albo wyłączeniu wyłącznie w granicach szczególnych przepisów prawa regulujących działalność podmiotu nadzorowanego, przy czym Nadzór krytycznie ocenia takie wyłączenia albo ograniczenia, jeżeli:
i. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez dostawcę usług chmury obliczeniowej lub jego poddostawcę lub
ii. przetwarzanie ma charakter outsourcingu szczególnego chmury obliczeniowej;

7) stanowisko nadzoru w sprawie usług (dostawców usług chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych, zgodnie z którym:
a) podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez bezpośredniego dostawcę usługa wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej;
b) zależnie od faktycznego wykorzystania usług chmury obliczeniowej oraz zakresu przetwarzanych informacji, podmiot nadzorowany powinien zapewnić, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień niniejszego komunikatu;

8) stanowisko nadzoru w sprawie prawa właściwego umowy pomiędzy dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym, zgodnie z którym:
a) prawem właściwym dla umowy jest prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:
i. postanowień umowy;
ii. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym;
iii. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;
b) w przypadku poddania umowy prawu państwa trzeciego podmiot nadzorowany powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej spełniają wymagania prawa obowiązujące podmiot nadzorowany oraz wymagania niniejszego komunikatu;

9) inne istotne zagrożenia, które podmiot nadzorowany identyfikuje w związku z wykorzystywaniem usług chmury obliczeniowej.

3. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić potencjalną możliwość:
1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;
2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa, jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego;
3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;

4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi, jak i jej konfiguracji.

4. Podmiot nadzorowany, na podstawie wyników szacowania ryzyka, zarządza tym ryzykiem, uwzględniając w szczególności:
   1) wymagania przepisów prawa, regulacji wewnętrznych oraz postanowień umownych;
   2) stopień złożoności organizacyjnej, podział uprawnień i odpowiedzialności podmiotu nadzorowanego, zawarte porozumienia, oraz analogiczne czynniki występujące w grupie kapitałowej lub organizacji grupowej, lub o charakterze stowarzyszenia, do których podmiot nadzorowany należy;
   3) efektywność stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do:
      a) identyfikacji nowych zagrożeń;
      b) zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;
      c) zmian w relacji z dostawcą usług chmury obliczeniowej, w tym możliwość również nieplanowanego zakończenia współpracy zarówno przez podmiot nadzorowany, jak i dostawcę usług chmury obliczeniowej;
   4) kompetencje techniczne i zdolności organizacyjne podmiotu nadzorowanego, w szczególności w kontekście bezpiecznego wykorzystywania usług chmury obliczeniowej oraz realizacji postanowień umownych;
   5) zdolność podmiotu nadzorowanego i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.

5. Wyniki szacowania ryzyka powinny dawać podstawę do twierdzenia, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami.

6. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji. Zatwierdzenie powinno obejmować decyzję podmiotu nadzorowanego dotyczącą:
   1) usług chmury obliczeniowej, z których podmiot nadzorowany będzie korzystał;
   2) rodzaju i zakresu przetwarzanych w ramach tych usług informacji.

OPIS WYMAGAŃ

1. Bank prowadzi szacowanie ryzyka w udokumentowany sposób oraz zgodnie z przyjętą przez siebie metodyką.

WYMAGANIA (PRODUKTY) DO OPARCOWANIA PO STRONIE BANKU

1. Udokumentowany proces klasyfikacji i oceny ryzyka pod kątem dopuszczalności przetwarzania w Chmurze obliczeniowej.
2. Dokument „Wyniki oceny ryzyka” dla każdej wdrożonej Usługi w chmurze obliczeniowej uwzględniający plan postępowania z opisanym ryzykiem.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Udokumentowanie spełnienia wymagań / posiadanego stanu, w szczególności:
   1) lokalizacji CPD, obszaru przetwarzania danych (lokalizacji Dostawcy, z których personel uzyskuje dostęp do danych Banku). Dopuszczalne jest określenie tego na poziomie kraju/regionu;
   2) sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel Dostawcy i jego poddostawców;
   3) opisu mechanizmów izolacji zasobów używanych do świadczenia Usług chmury obliczeniowej, wraz

z informacją o potencjalnych skutkach awarii mechanizmów izolacji;
4) dokumentacji interfejsów zarządzających Usługami chmury obliczeniowej, informacji o zabezpieczeniach interfejsów i ew. o ich podatnościach;
5) zasad żądania wprowadzania zmian przez Dostawcę;
6) możliwości kontrolowania Dostawcy oraz jego poddostawców, w zakresie bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia Usług chmury obliczeniowej;
7) podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę a Bank;
8) mechanizmów kontroli dostępu do usługi dla użytkowników, w szczególności metod ograniczenia dostępu z urządzeń prywatnych;
9) możliwości integracji z innymi, wskazanymi przez Bank technologiami;
10) stosu technologicznego w zakresie zapewnienia bezpieczeństwa środowiska, danych (informacjach) oraz zasobów Chmury obliczeniowej, w szczególności mechanizmów szyfrowania;
11) łańcucha outsourcingowego oraz procesu kontroli i zapewnienia jakości.

SZABLONY

1. Załącznik_1_Szablon szacowania ryzyka.

5.4. PKT VII KOMUNIKATU - „MINIMALNE WYMAGANIA DLA PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ”

VII. Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej

1. Niniejsze minimalne wymagania techniczne i organizacyjne dla przetwarzania informacji w chmurze obliczeniowej stanowią referencyjne odniesienie, które podmiot nadzorowany powinien weryfikować pod kątem adekwatności do wyników oszacowania ryzyka oraz zapewnić ich spełnienie.

2. Środki techniczne i zasoby organizacyjne służące bezpieczeństwu przetwarzanych informacji powinny wynikać z przeprowadzonego procesu szacowania ryzyka, jednak – niezależnie od wyników tego szacowania – nie mogą osłabiać wymagań opisanych poniżej.

3. **Zapewnienie kompetencji**
   3.1. Podmiot nadzorowany zapewnia w udokumentowanym procesie właściwe kompetencje dla planowanych lub prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników lub współpracowników podmiotu nadzorowanego zaangażowanych w proces planowania, realizacji, testowania i utrzymywania przetwarzania informacji w chmurze obliczeniowej oraz zawierania i przeglądania umowy z tym związanej.
   3.2. Podmiot nadzorowany zapewnia rozumienie konsekwencji stosowania określonej architektury chmury obliczeniowej, zasad konfiguracji, podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji, zależnie od zakresu i rodzaju planowanego lub stosowanego środowiska chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem wymagań ciągłości działania podmiotu nadzorowanego oraz posiadanej infrastruktury teleinformatycznej. Rozumienie konsekwencji danego wyboru ma odniesienie w dokumentacji szacowania ryzyka, zapewnieniu właściwych zasobów zarówno pod względem jakościowym, jak i ilościowym oraz dodatkowo we wszystkich pracach

(oraz umowach) związanych z tworzeniem lub rozwojem oprogramowania przeznaczonego do używania w chmurze obliczeniowej oraz integracji usług bazujących na zasobach własnych podmiotu nadzorowanego.
3.3. Kompetencje pracowników lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring usług chmury obliczeniowej powinny być potwierdzone odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej (lub wynikać z umiejętności i doświadczenia), w tym również specyficznych lub specyficznie konfigurowanych dla danego dostawcy usług chmury obliczeniowej. Wymaganie to odnosi się również do kompetencji osób odpowiedzialnych za przegląd lub weryfikację dokumentacji audytów, certyfikatów i innych dokumentów dostawcy usług chmury obliczeniowej, w tym umowy na świadczenie usług chmury obliczeniowej oraz dokumentów o charakterze technicznym.

OPIS WYMAGAŃ

1. Bank w celu zapewnienia bezpieczeństwa przetwarzanych w Chmurze obliczeniowej informacji (lub co do których istnieje zamiar przetwarzania), powinien zapewnić właściwy poziom wiedzy i umiejętności pracowników i współpracowników, przy czym taki właściwy poziom wiedzy i umiejętności określa się co do zasady na podstawie wyników oszacowania ryzyka. Utrzymanie i systematyczne podnoszenie kwalifikacji (wiedzy i umiejętności) powinno być częścią dobrych praktyk Banku. W przypadku stwierdzenia ewentualnych braków, należy je zaadresować poprzez stosowne szkolenia lub skorzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie Chmury obliczeniowej. Kompetencje pracowników i współpracowników powinny być udokumentowane, np. w formie certyfikatów szkoleniowych lub certyfikatów Dostawców.
2. Bank powinien określić role w organizacji wraz z zakresem głównych zadań podczas wdrożenia lub przy utrzymaniu rozwiązań chmurowych oraz dopasować do nich wymagane obszary kompetencji. Przykładowymi obszarami ról i dopasowanymi do nich kompetencjami w ramach wdrażania i utrzymania rozwiązań w publicznej Chmurze obliczeniowej są:
   1) architektura (rola Architekt);
   2) bezpieczeństwo (rola Inżynier bezpieczeństwa);
   3) rozwój (rola Developer, Inżynier DevOps);
   4) utrzymanie (role Administrator, Administrator sieci, Inżynier DevOps);
   5) biznes (rola Opiekun biznesowy usługi); oraz
   6) finanse (rola Kontroler finansowy).
3. Role i dopasowane do nich kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność i kontrolę finansową wykorzystywanych Usług chmury obliczeniowej.
4. Bank w ramach utrzymania produkcyjnych systemów przetwarzających informację w Chmurze obliczeniowej powinien posiadać aktywne wsparcie Dostawców lub korzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie Chmury obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowany podział ról i odpowiadające im kompetencje w organizacji wraz z zakresem głównych zadań na potrzeby wdrożenia lub utrzymania systemów w Chmurze obliczeniowej.
2. Udokumentowane szkolenia lub certyfikaty dla poszczególnych ról.
3. Udokumentowane zapisy potwierdzające aktywne wsparcie Dostawców lub firm świadczących usługi konsultacyjno-doradcze w zakresie Chmury obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Udokumentowane szkolenia, potwierdzone certyfikatami.
2. Udokumentowane wsparcie personelu Dostawcy na rzecz Banku.

SZABLONY

N/D

4. **Umowa z dostawcą usług chmury obliczeniowej**
   4.1. Podmiot nadzorowany posiada sformalizowaną umowę (oraz inne dokumenty, w tym oświadczenia, regulaminy, warunki korzystania z usług, także w wersji elektronicznej) z dostawcą usług chmury obliczeniowej, która – tam, gdzie to zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji – zawiera lub wskazuje źródła informacji, obejmujące:
   a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;
   b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;
   c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);
   d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;
   e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;
   f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;
   g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;
   h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunków nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;
   i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców dostawcy usług chmury obliczeniowej są transparentne i jasno identyfikowane przez podmiot nadzorowany;
   j) źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);
   k) źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;
   l) zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;
   m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);
   n) prawo dla nadzoru do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności;
   o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego

oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;

p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;

q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;

r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;

s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i dostawcę usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również inne strony (np. klientów, poddostawców), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

4.2. Bez uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień niniejszego komunikatu, podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, w szczególności, gdy dotyczą one usług chmury obliczeniowej tworzonych dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym, w tym również chmury obliczeniowej społecznościowej.

W takim przypadku podmiot nadzorowany powinien:

t) zweryfikować, w jakim zakresie umowa ramowa oraz powiązane z nią dokumenty, wyniki szacowania ryzyka oraz wymagania prawne, organizacyjne i techniczne uwzględniają postanowienia niniejszego komunikatu oraz są adekwatne dla sytuacji podmiotu nadzorowanego i jego zamiarów związanych z przetwarzaniem informacji w chmurze obliczeniowej;

u) ocenić konieczność lub możliwość samodzielnego stosowania wymagań niniejszego komunikatu w zakresie, który nie jest zgodny z umową ramową i powiązanymi z nią dokumentami.

OPIS WYMAGAŃ

1. Bank jest zobowiązany do zawarcia pisemnej umowy z Dostawcą. Prawem właściwym dla umowy powinno być prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:
   1) postanowień umowy;
   2) wszystkich wymogów prawa polskiego ciążących na Banku;
   3) wytycznych organu nadzoru, w tym również w zakresie Komunikatu.

2. Wydaje się, że w przypadku przetwarzania Tajemnicy bankowej w Chmurze obliczeniowej oraz Outsourcingu szczególnego, a zatem w dwóch przypadkach, gdy zawsze wymagane jest stosowanie Komunikatu Usługa chmury obliczeniowej stanowić będzie w zdecydowanej większości (a w przypadku przetwarzana Tajemnicy bankowej zawsze) outsourcing bankowy w rozumieniu art. 6a i nast. Prawa bankowego (z zastrzeżeniem dalszego odmiennego stanowiska UKNF w tym zakresie). Konieczne zatem będzie dodatkowo spełnienie wymogów nałożonych przepisami Prawa bankowego.

3. Zgodnie z Kodeksem cywilnym umowa ma formę pisemną, gdy jest zawarta na piśmie, przy czym oświadczenie woli złożone w formie elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym jest równoważne formie pisemnej.

4. W przypadku poddania umowy prawu państwa trzeciego Bank powinien mieć pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy, wszystkie postanowienia umowy pomiędzy Bankiem a Dostawcą spełniają wymagania prawa oraz wymagania Komunikatu obowiązujące Bank.

5. Umowa z Dostawcą powinna zawierać te elementy (katalog zamknięty) lub wskazywać ich źródła wymienione w punkcie 4.1. Komunikatu, które są zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji. Dodatkowo, zgodnie z puntem 4.2. Komunikatu, Bank może korzystać z ramowych umów udostępnianych przez Dostawców, przy założeniu braku uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień Komunikatu. Objaśnienia do wybranych elementów umowy z Dostawcą wskazanych w punkcie 4.1. Komunikatu znajdują się w Załączniku 2 Objaśnienia i lista wybranych klauzul z przykładami.
6. W przypadku poddania umowy prawu państwa spoza EOG - analiza prawna dotycząca możliwości skutecznego wykonywania postanowień umowy, wszystkich wymogów prawa polskiego ciążących na Banku oraz wytycznych organu nadzoru w zakresie Komunikatu.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Umowa w formie pisemnej z Dostawcą wraz z niezbędnymi dokumentami (oświadczenia, regulaminy, warunki korzystania z usług, itp.).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Podpisanie umowy z Bankiem uwzględniającej wymagania Komunikatu i bezwzględnie obowiązujących przepisów prawa.

SZABLONY

1. Załącznik_2_Objaśnienia i lista wybranych klauzul z przykładami.

5. **Plan przetwarzania informacji w chmurze obliczeniowej**
   5.1. Podmiot nadzorowany na podstawie wyników szacowania ryzyka opracowuje udokumentowany plan przetwarzania informacji w chmurze obliczeniowej, który zawiera co najmniej:
   a) rodzaj (opis) przetwarzanych informacji oraz informację, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji;
   b) sposób szyfrowania informacji oraz miejsce (lub sposób) zarządzania kluczami szyfrującymi;
   c) informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;
   d) datę zawarcia umowy z dostawcą usług chmury obliczeniowej i referencje do tej umowy (numer, okres obowiązywania, datę przedłużenia lub zmiany, daty rozpoczęcia korzystania z usług), a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;
   e) prawo właściwe, któremu podlega umowa;
   f) opis zadania realizowanego za pomocą usługi chmury obliczeniowej wraz z informacją, czy jest to outsourcing szczególny chmury obliczeniowej w rozumieniu niniejszego komunikatu lub czy przetwarzane są informacje prawnie chronione.

OPIS WYMAGAŃ

1. Bank w ramach bieżącego i planowanego przetwarzania informacji (uruchomienia inicjatywy) w Chmurze obliczeniowej powinien posiadać udokumentowany plan przetwarzania informacji w Chmurze obliczeniowej zgodnie z Załącznikiem 3 do Standardu. Plan ten w szczególności powinien zawierać (najlepiej w postaci szczegółowej dokumentacji):
   1) opis zadania realizowanego za pomocą Usługi chmury obliczeniowej;
   2) rodzaj (chronione, niechronione), klasę (publiczne, wewnętrzne, poufne) i typ (produkcyjne, testowe) przetwarzanych informacji wraz z informacją, czy przetwarzanie spełnia kryteria Outsourcingu szczególnego chmury obliczeniowej;

3) mechanizmy zabezpieczenia informacji (pseudonimizacja, anonimizacja), mechanizmy szyfrowania informacji, w tym zasady zarządzania i przechowywania kluczy szyfrujących oraz opis kontroli dostępu do informacji.

2. Plan powinien precyzyjnie określić, jakie dane (informacje) Bank, w ramach konkretnej inicjatywy, przetwarza w Chmurze obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Plan przetwarzania informacji, np. w formie wypełnionego szablonu przedstawionego w Załączniku 3 do Standardu).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

N/D

SZABLONY

1. Załącznik_3_Plan Przetwarzania informacji w chmurze obliczeniowej.

5.2. Uruchomienie produkcyjne stosowania usług chmury obliczeniowej powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), w udokumentowanym procesie, testowane są scenariusze adekwatne do oszacowanego ryzyka.

OPIS WYMAGAŃ

1. Bank powinien przeprowadzić i udokumentować fazę testów usługi. Testy powinny być przeprowadzone na danych testowych; scenariusze testów powinny być adekwatne do oszacowanego ryzyka (zgodnie ust. VI Komunikatu - Wytyczne do szacowania ryzyka).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane scenariusze testowe.
2. Formalne wyniki testów.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

N/D

SZABLONY

N/D

5.3. Podmiot nadzorowany posiada udokumentowany, przetestowany plan wycofania swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego dostawcy (również w sytuacji awaryjnej), bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.

OPIS WYMAGAŃ

1. Bank posiada plan wycofania się z Usługi chmury obliczeniowej zarówno w sytuacji zmiany strategii, jak i w sytuacji awaryjnej.

2. Plan powinien zapewnić, że w sytuacji awaryjnej nie dojdzie do uszczerbku dla zachowania zgodności działania Banku z wymaganiami prawa i innych regulacji, w tym związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.
3. Plan wycofania się z usługi może zakładać powrót do środowiska „on-premise", migrację do innego Dostawcy lub inne uzasadnione biznesowo scenariusze.
4. Plan powinien być przetestowany, przy czym zakres i podejście do testów powinny wynikać z analizy ryzyka (zgodnie z pkt VI Komunikatu - Wytyczne do szacowania ryzyka) i uwzględniać takie kwestie jak wolumeny danych, wymagane zasoby etc. Dokumentacja testowa powinna zawierać odpowiednie dowody audytowe np. scenariusze testowe, oczekiwane wyniki, logi czy zrzuty z ekranu potwierdzające fakt przeprowadzenia testów zgodnie z założeniami.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Plan wycofania się z Usługi chmury obliczeniowej.
2. Scenariusze testowe dla planu wycofania się z Usługi chmury obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

N/D

SZABLONY

1. Załącznik_4_Szablon scenariusza wyjścia z chmury.
2. Załącznik_5_Wyjście z c hmury - główne zagadnienia.

5.4. Podmiot nadzorowany powinien posiadać udokumentowany plan ciągłości działania uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej, podmiot nadzorowany regularnie weryfikuje własną zdolność do utrzymania deklarowanych założeń, w szczególności zgodność konfiguracji usług i odtwarzalności środowiska teleinformatycznego, zwłaszcza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

OPIS WYMAGAŃ

1. Bank powinien rozszerzyć posiadane plany ciągłości działania o scenariusz uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy oraz możliwość przerwania ciągłości działania Usługi chmury obliczeniowej.
2. Plan ciągłości działania może być oparty na różnych scenariuszach, w szczególności zakładać wykorzystanie środowiska on-premise, wykorzystanie innego Dostawcy lub tymczasową alternatywną realizację procesów (np. manualnie).
3. Bank może polegać na planach ciągłości działania po stronie Dostawcy pod warunkiem posiadania nadzoru nad działaniami Dostawcy w tym zakresie, tj. regularnej weryfikacji adekwatności planu oraz wyników testów planu ciągłości działania i planów awaryjnych (np. poprzez weryfikacje wyników niezależnych audytów, certyfikacje etc.).
4. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej Chmur obliczeniowych lub dwóch lub więcej Dostawców, Bank powinien regularnie weryfikować możliwość realizacji tego scenariusza, zwłaszcza po zmianach technologicznych u jednego z Dostawców.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Plan ciągłości działania dla Usługi chmury obliczeniowej, zawierający jako minimum opisane procesy i procedury w sytuacjach:
   1) możliwości utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy;
   2) możliwości przerwania ciągłości działania Usługi chmury obliczeniowej.
2. Dokumentacja związana z Planowaniem Ciągłości Działania zgodnie z metodyką przyjętą w Banku (zawierająca w szczególności wyniki testów ciągłości działania).
3. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej Chmur obliczeniowych lub dwóch lub więcej Dostawców:
   1) dokumentacja weryfikacji możliwości realizacji tego scenariusza, np. przeprowadzenie testowej migracji próbki danych lub usług pomiędzy dwoma Usługami chmury obliczeniowej;
   2) potwierdzenie przeprowadzania okresowej weryfikacji możliwości realizacji scenariusza z podpunktu powyżej, w szczególności dotyczące weryfikacji możliwości realizacji scenariusza po zmianach technologicznych u jednego z Dostawców.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

N/D

SZABLONY

1. Zgodnie z polityką Banku.

6. **Wymagania dla dostawców usług chmury obliczeniowej**
   6.1. W zakresie świadczonych usług chmury obliczeniowej i odpowiednio do ich skali dostawca usług chmury obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części:
   a) PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;
   b) PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;
   c) PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;
   d) ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;
   e) ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.

   6.2. CPD dostawcy usług chmury obliczeniowej spełnia wymagania normy PN-EN 50600 (Wyposażenie i infrastruktura centrów przetwarzania danych) minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i uznanego do oceny CPD lub zawierającego wymagania z nim związane, przy czym podmiot nadzorowany może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań.
   (...)

   6.5. Spełnienie wymagań może być poświadczone odpowiednimi certyfikatami zgodności wystawionymi przez niezależne jednostki certyfikujące, akredytowane w polskim lub europejskim systemie akredytacji.

OPIS WYMAGAŃ

1. Bank, w zależności od oceny ryzyka, podejmuje decyzję o konieczności częściowego lub pełnego spełnienia przez Dostawcę:
   1) w/w norm ISO;

2) wymagań w zakresie CPD.

2. Zakres w/w wymagań dla każdego wdrożenia powinien być przez Bank udokumentowany.
3. W zależności od decyzji Banku - Dostawca powinien zobowiązać się w umowie do zapewnienia zgodności Usługi chmury obliczeniowej zgodnie z w/w normami lub ich odpowiednikami (normami BS, normami PN-ISO, etc.).
4. Zapewnienie zgodności może być realizowane poprzez uzyskanie przez Dostawcę niezależnej certyfikacji (wydanej przez jednostkę certyfikującą); w przypadku, gdy Dostawca nie posiada formalnej certyfikacji, powinien on wykazać zgodność z w/w normami poprzez udokumentowanie realizacji poszczególnych wymagań norm.
5. Zakres certyfikacji powinien obejmować w całości usługę świadczoną na rzecz Banku, w szczególności dla pkt 6.2. Komunikatu, wszystkie CPD w których przetwarzane są dane (informacje) Banku.
6. Dokumentacja związana z certyfikacją tj. certyfikat oraz wyniki audytów certyfikacyjnych lub dokumentacja zgodności dostarczona przez Dostawcę, powinny być przekazane przed zawarciem umowy oraz co najmniej raz w roku udostępniane Bankowi.
7. Bank powinien regularnie weryfikować dokumentację związaną z certyfikacją; w przypadku, gdy w/w dokumentacja wykaże istotne niezgodności, Bank powinien uzgodnić z Dostawcą plan naprawczy oraz monitorować jego realizację.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane wymagania Banku w zakresie w/w norm i standardów, w szczególności dokumentacja akceptacji ryzyka w przypadku rezygnacji z wybranych wymagań.
2. Pozyskanie certyfikatu Dostawcy lub innej dokumentacji zgodności Dostawcy z normami.
3. Udokumentowany proces regularnej oceny dokumentacji związanej z certyfikacją/zgodnością.
4. Udokumentowany proces zarządzania planami naprawczymi uzgodnionymi z Dostawcą w przypadku istotnych niezgodności z normami.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Certyfikacja zgodnie z w/w normami, obejmująca zakresem usługę świadczoną na rzecz Banku lub dokumentacja zgodności z w/w normami przygotowana przez Dostawcę.

SZABLONY

1. Załącznik_6_Szablon dokumentacji kontroli ISO27001.

6.3. Nadzór rekomenduje, aby CPD zlokalizowane było na terytorium państwa Europejskiego Obszaru Gospodarczego (EOG). Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:

a) zostały uznane stosowną decyzją za operatorów usług kluczowych w rozumieniu art. 5 ust. 2 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji usługi kluczowej lub
b) są operatorami infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji zadań operowania infrastrukturą krytyczną,

powinny w pierwszej kolejności wykorzystywać CPD znajdujące się na terenie Rzeczypospolitej Polskiej, o ile – w ocenie podmiotu nadzorowanego – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.

OPIS WYMAGAŃ

1. Rekomendowany jest wybór Dostawców oferujących CPD na terenie EOG, co nie wyklucza możliwości przetwarzania danych ((informacji)) przez Dostawcę poza EOG.
2. Jeżeli usługa ma być świadczona w CPD na terenie EOG (lub w Polsce zgodnie pkt 6.3. Komunikatu), Bank korzystający z usług globalnego Dostawcy powinien zdefiniować mechanizmy kontrolne zapewniające, że usługi, które wykorzystuje są świadczone w CPD na terenie EOG (lub w Polsce zgodnie z pkt 6.3. Komunikatu).
3. W przypadku gdy CPD zlokalizowane jest na terenie EOG, ale usługa jest również wspierana przez personel mający dostęp do danych (informacji) zlokalizowany poza EOG, wymagane jest zapewnienie zgodności z przepisami w tym zakresie (w szczególności wymagane jest uzyskanie zezwolenia KNF).
4. Podmioty będące operatorami infrastruktury krytycznej lub będące operatorami usługi kluczowej powinny preferować CPD znajdujące się na terenie Polski, o ile oferuje ono nie gorsze warunki (bezpieczeństwo, koszt, SLA itp.) niż usługi zlokalizowane poza Polską. W związku z tym, Banki będące w/w operatorami powinny przed wyborem Dostawcy zweryfikować dostępność analogicznej usługi korzystającej z CPD w Polsce i zapewnić udokumentowane porównanie tych usług – w szczególności porównując (szacując zgodnie z Komunikatem) ryzyko i koszty dla poszczególnych wariantów.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Jednoznaczne wskazanie lokalizacji CPD wykorzystywanych w usłudze.
2. Dla operatorów infrastruktury krytycznej lub operatorów usługi kluczowej (większość Banków) dokumentacja lub mechanizmy kontrolne potwierdzające lokalizacje CPD w Polsce (jeśli dotyczy).
3. W przypadku, gdy uzasadniony jest wybór CPD poza Polską, udokumentowana analiza uzasadniająca taką decyzję (kwestie kosztów lub ryzyka).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Jednoznaczne wskazanie wszystkich lokalizacji CPD (kraj/region) wykorzystywanych w poszczególnych usługach (w formie oświadczenia Dostawcy).

SZABLONY

N/D

6.4. Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych przez podmiot nadzorowanych informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:

a) domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;
b) domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;
c) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;
d) udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;

e) domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default”.

OPIS WYMAGAŃ

1. Dostawca powinien przedstawić dokumentację mechanizmów kontroli dostępu do danych (informacji) przetwarzanych w Usłudze chmury obliczeniowej, w tym dla swoich pracowników (współpracowników) i poddostawców.
2. Dostawca nie powinien mieć stałego dostępu do danych (informacji) ani dostępu administracyjnego, serwisowego etc. na poziomie serwerów, baz danych, aplikacji czy urządzeń.
3. Dostęp do danych (informacji) dla Dostawcy powinien być nadawany tymczasowo na podstawie udokumentowanego żądania powiązanego z konkretnymi pracami administracyjnymi, rozwojowymi lub wsparciem użytkowników (zleconymi przez Bank).
4. Dostawca powinien przekazać dokumentację potwierdzającą separację tenantów oraz dokumentację mechanizmów zapewniających poprawność separacji, tak aby możliwa była okresowa weryfikacja konfiguracji.
5. Nowo uruchamiane usługi powinny być domyślnie odseparowane (od momentu uruchomienia) i skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa (hardening).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja mechanizmów kontroli dostępu, przy założeniu, że jako minimum przyjęto:
   1) potwierdzenie domyślnego braku dostępu do danych (informacji), kont administracyjnych, serwisowych etc.;
   2) opis mechanizmów nadawania dostępu administracyjnego.
2. Dokumentacja mechanizmów separacji danych (informacji):
   1) wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania;
   2) wytycznych, wzorcowych konfiguracji, opisów zasad weryfikacji poprawności konfiguracji.
3. Dokumentacja konfiguracji bezpieczeństwa nowo uruchamianych serwerów i usług („secure-by-default”).
4. **Opcjonalnie,** certyfikaty i dokumentacja certyfikacji (wyniki audytu itp.) w zakresie funkcjonowania mechanizmów kontroli dostępu.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

J.W.

SZABLONY

N/D

7. **Kryptografia**
   7.1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z zasadami określonymi w niniejszym komunikacie. W szczególności podmiot nadzorowany powinien upewnić się, że:
   a) posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;

b) zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług chmury obliczeniowej, zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;
c) używa dedykowanych lub zalecanych przez dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;
d) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest", jak i „in transit".

OPIS WYMAGAŃ

1. Wymagane jest szyfrowanie informacji przetwarzanych w Chmurze obliczeniowej. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinny wynikać z analizy ryzyka (zgodnie z pkt VI ust. 5.2 Komunikatu). W szczególności wymagane jest:
   1) szyfrowanie, zarówno podczas przesyłu, jak i podczas spoczynku („at rest", jak i „in transit") Tajemnicy bankowej;
   2) przekazanie Bankowi przez Dostawców dokumentacji mechanizmów szyfrowania danych (informacji), a także mechanizmów weryfikacji poprawności konfiguracji i działania w/w mechanizmów;
   3) posiadanie przez Bank kompetencji w zakresie poprawnej konfiguracji usług, w tym mechanizmów szyfrowania;
   4) korzystanie przez Bank z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania.
2. Potwierdzenie posiadanych kompetencji – patrz pkt. VII. ust.3 Komunikatu.
3. Dokumentacja hardeningu usługi, w szczególności mechanizmów szyfrowania.
4. Potwierdzenie szyfrowania danych (informacji) w spoczynku i podczas przesyłu (dokumentacja techniczna, zrzuty ekranu etc.).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

J.W.

SZABLONY

N/D

7.2. Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez podmiot nadzorowany, chyba że z oszacowania ryzyka wynika, iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących generowanych lub zarządzanych przez dostawcę usług chmury obliczeniowej.
(...)

7.4. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.

7.5. Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej i są używane w procesie outsourcingu szczególnego chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. O ile ma to uzasadnienie w ocenie ryzyka, Bank powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Bank. Brak spełnienia tego wymogu powinien zostać poparty stosowną analizą ryzyka (patrz pkt VI.2. ust. 5.a) Komunikatu).
2. Proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących powinien być udokumentowany i posiadać określone mechanizmy kontrolne.
3. W przypadku wykorzystania kluczy wygenerowanych lub zarządzanych przez Dostawcę, Bank powinien zapewnić, że proces wspomniany w pkt. 2 powyżej zapewnia przechowywanie kluczy w infrastrukturze Banku, chyba że analiza ryzyka uzasadnia brak takiego mechanizmu.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja techniczna potwierdzająca, że informacje są szyfrowane kluczami generowanymi/ dostarczonymi oraz zarządzanymi przez Bank.
2. W przypadku, gdy pkt 1 powyżej nie jest spełniony, analiza ryzyka, z której wynika dopuszczalność używania kluczy szyfrujących generowanych/dostarczonych i zarządzanych przez Dostawcę.
3. Sformalizowany (udokumentowany) proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz przechowywaniem kopii zapasowych kluczy w infrastrukturze Banku.
4. W przypadku, gdy proces zarządzania kluczami szyfrującymi nie zapewnia przechowywania kopii kluczy w infrastrukturze Banku, analiza ryzyka, z której wynika uzasadniony brak takiej potrzeby.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Opis procedur i mechanizmów zarządzania kluczami szyfrującymi, sformalizowany (udokumentowany) proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących.

SZABLONY

N/D

7.3. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS 140-2 Level 2 lub równoważne.

OPIS WYMAGAŃ

1. W zależności od wyników analizy ryzyka (pkt VI. Ust. 2.5 Komunikatu) możliwe jest stosowanie HSM. HSM może być udostępniony przez Dostawcę lub być zarządzany przez Bank. Bez względu na to, która strona udostępnia HSM, musi on spełniać wymagania FIPS 140-2 Level 2 lub równoważne.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja wykorzystywanych HSM potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Jak wyżej w przypadku, gdy HSM jest udostępniony przez Dostawcę.

SZABLONY

N/D

8. **Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej**
   8.1. Podmiot nadzorowany posiada udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej, stosownie do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka.
   8.2. Podmiot nadzorowany zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie.
   8.3. Uprawniony personel podmiotu nadzorowanego dokonuje przeglądu logów zgodnie z udokumentowanymi procedurami i zasadami bezpieczeństwa, przy czym – zależnie od skali działania, rodzaju i liczby logowanych zdarzeń oraz architektury bezpieczeństwa – Nadzór zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.

OPIS WYMAGAŃ

1. Istotnym elementem związanym z wykorzystaniem usług przetwarzania informacji w Chmurze obliczeniowej jest kwestia monitorowania środowiska przetwarzania informacji w Usłudze chmury obliczeniowej.
2. Zgodnie z wytycznymi Komunikatu, w zakresie monitorowania środowiska przetwarzania informacji w Usłudze chmury obliczeniowej Bank powinien:
   1) posiadać udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w Chmurze obliczeniowej, stosownie do zakresu używanych Usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka;
   2) zabezpieczać logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie;
   3) W zależności od skali działania, ilości logów etc. należy rozważyć przekazywanie logów z Chmury obliczeniowej do systemu SIEM oraz opracowanie reguł korelacji pozwalających na wykrycie incydentu bezpieczeństwa w Chmurze obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w Chmurze obliczeniowej.
2. Rekomendowane jest użycie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM).

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Dokumentacja w zakresie logowania zdarzeń w Chmurze obliczeniowej, a także możliwości integracji mechanizmów logowania w chmurze z systemem SIEM wykorzystywanym w Banku.

SZABLONY

N/D

8.4. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany:
   a) podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;
   b) podmiot nadzorowany wymaga używania przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;
   c) podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest z zaufanych sieci podmiotu nadzorowanego lub dostawcy usług i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. Bank powinien zapewnić poprzez mechanizmy kontrolne lub zapisy umowne, że dostęp do systemów wykorzystywanych w Usłudze chmury obliczeniowej ma wyłącznie uprawniony personel po stronie Dostawcy.
2. Dostęp personelu Dostawcy usług do systemów wykorzystywanych w Chmurze obliczeniowej powinien być zabezpieczony przez silne, wieloskładnikowe uwierzytelnienie.
3. Personel Dostawcy powinien uzyskiwać dostęp wyłącznie z bezpiecznych stacji roboczych/terminali, zlokalizowanych w bezpiecznej (zaufanej) lokalizacji sieciowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane procedury lub zapisy umowne potwierdzające ograniczenie dostępu wyłącznie do uprawnionego personelu Dostawcy z bezpiecznych lokalizacji sieciowych i stacji roboczych/terminali.
2. Opis mechanizmów uwierzytelnienia.
3. Udokumentowane procedury okresowej weryfikacji dostępu Dostawcy do systemów wykorzystywanych w usłudze.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Używanie przez personel Dostawcy, mający dostęp zdalny do środowiska chmury obliczeniowej Banku, uwierzytelnienia MFA oraz bezpiecznych stacji w bezpiecznych lokalizacjach sieciowych.
2. W zależności od wyników analizy ryzyka przeprowadzanej przez Bank, inne mechanizmy zapewniające monitorowanie dostępu i rozliczalność działań Dostawcy, np. nagrywanie sesji i jej parametrów w przypadku dostępu administracyjnego Dostawcy lub dostępu personelu Banku o charakterze uprzywilejowanym.

SZABLONY

N/D

9. **Dokumentowanie działań podmiotu nadzorowanego**
   9.1. Tam, gdzie jest to zasadne, zależnie od zakresu i rodzaju przetwarzanych informacji, zasad i regulacji obowiązujących i przyjętych w organizacji (z uwzględnieniem powiązań korporacyjnych i grupowych, jeżeli występują) oraz wyników szacowania ryzyka i przy uwzględnieniu zasady proporcjonalności, podmiot nadzorowany posiada dokumentację zawierającą:
      a) organizację pracowników lub współpracowników odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk lub funkcji związanych z monitorowaniem, analizowaniem

i raportowaniem incydentów związanych z informacjami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami;

b) architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych podmiotu nadzorowanego z sieciami niezaufanymi, w tym architekturę rozwiązania w chmurze obliczeniowej, także z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych;
c) zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej lub odniesienie do obecnie funkcjonujących klasyfikacji, jeżeli mogą być stosowane;
d) zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;
e) zasady zarządzania ciągłością działania;
f) zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usług chmury obliczeniowej;
g) zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;
h) zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej;
i) zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;
j) umowy z dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań;
k) procesy, procedury lub instrukcje dotyczące:
   I. analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego;
   II. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych itp.) z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;
   III. zarządzania logami;
   IV. zarządzania kluczami szyfrującymi;
   V. zarządzania incydentami bezpieczeństwa;
   VI. przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

9.2. Dokumentacja jest chroniona przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem. Zasady zarządzania dokumentacją podmiot nadzorowany definiuje w ramach systemu zarządzania organizacją.

OPIS WYMAGAŃ

Punkt VII.9 Komunikatu określa wymogi organizacyjne i dokumentacyjne, które Bank powinien posiadać (np. w charakterze polityk lub innych regulacji) chcąc wdrażać Usługi chmury obliczeniowej.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowanie organizacji pracowników lub współpracowników Banku odpowiedzialnych za cyberbezpieczeństwo, z uwzględnieniem elementów z pkt 9 a) Komunikatu.
2. Udokumentowanie architektury sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Banku z sieciami niezaufanymi, w tym architektury wdrażanego rozwiązania w Chmurze obliczeniowej z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.
3. Udokumentowanie zasad kategoryzacji informacji lub systemów pod kątem przetwarzania w Chmurze.

4. Udokumentowane zasady (polityka) stosowanych w organizacji zabezpieczeń technologicznych i rozwiązań organizacyjnych w odniesieniu do rozwiązań w Chmurze obliczeniowej.
5. Udokumentowane zasady (polityka) zarządzania ciągłością działania.
6. Dla wdrażanej Usługi chmury obliczeniowej, udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji, jak również dla sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą.
7. Udokumentowane zasady (polityka) zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi.
8. Udokumentowane zasady (polityka) przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem Chmury obliczeniowej (np. coroczny przegląd).
9. Udokumentowane zasady (polityka) raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania Usług chmury obliczeniowej.
10. Umowa z Dostawcą wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań.
11. Opis procesów, procedury lub instrukcje, dotyczące obszarów wskazanych w podpunktach i. do vi. pkt 9.1. Komunikatu.
12. Udokumentowane zasady zarządzania politykami i dokumentacją w ramach systemu zarządzania organizacją, zapewniające ochronę przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Udokumentowanie architektury rozwiązania w Chmurze obliczeniowej, z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.

SZABLONY

N/D

5.5. PKT VIII KOMUNIKATU - „ZASADY INFORMOWANIA UKNF O ZAMIARZE PRZETWARZANIA LUB PRZETWARZANIU INFORMACJI W CHMURZE OBLICZENIOWEJ”

VIII. Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej

1. W przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej podmiot nadzorowany w terminie 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (a w przypadku, gdy przetwarzanie to już jest realizowane – nie później niż 1 sierpnia 2020 r.) informuje UKNF o:
   1) rodzaju i zakresie informacji planowanych do przetwarzania / przetwarzanych w chmurze obliczeniowej;
   2) nazwie dostawcy usług chmury obliczeniowej oraz rodzaju planowanych do używania / używanych usług chmury obliczeniowej;

3) dacie podpisania umowy z dostawcą usług chmury obliczeniowej oraz terminach jej obowiązywania, a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;
4) lokalizacji (kraj, region albo inne równoważne) centrum przetwarzania danych (CPD) świadczącym usługę chmury obliczeniowej;
5) spełnieniu wymagań opisanych w niniejszym komunikacie;
6) osobach lub stanowiskach do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym.

2. Powyższa informacja powinna zostać podpisana przez uprawnionego przedstawiciela podmiotu nadzorowanego oraz dostarczona do UKNF przy wykorzystaniu formularza stanowiącego załącznik nr 1 do niniejszego komunikatu.

OPIS WYMAGAŃ

1. Komunikat wymaga poinformowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w Chmurze obliczeniowej wyłącznie w dwóch przypadkach: (i) usługi Chmury obliczeniowej stanowią Outsourcing szczególny lub (ii) w Chmurze obliczeniowej przetwarzana jest Tajemnica bankowa.
2. Zgłoszenia należy dokonać 14 dni przed rozpoczęciem przetwarzania informacji w Chmurze obliczeniowej (lub w trakcie, gdy w dacie Komunikatu usługa jest już realizowana), co oznacza, że znaczenia nie ma samo zawarcie umowy outsourcingowej, ale przekazanie danych (informacji) Dostawcy, w tym objętych Tajemnicą bankową (bez względu czy w fazie przedprodukcyjnej, czy już w fazie produkcyjnej).
3. Uprawnionym do podpisania informacji, o której mowa pkt VIII. Komunikatu jest zarówno zarząd Banku (zgodnie z reprezentacją w KRS), jak i osoby właściwie przez zarząd umocowane. Decyzja może mieć formę uchwały zarządu.

WYMAGANIA (PRODUKTY) DO OPRACOWANIA PO STRONIE BANKU

4. Wypełniony i podpisany przez odpowiednio umocowane osoby Załącznik 1 Komunikatu.

WYMAGANIA (PRODUKTY) PO STRONIE DOSTAWCY

N/D

SZABLONY

N/D

6. PRAWO BANKOWE

Poniższy komentarz do przepisów Prawa bankowego dotyczy wyłącznie sytuacji, gdy Usługa chmury obliczeniowej stanowi jednocześnie outsourcing bankowy w rozumieniu art. 6a i nast. Prawa bankowego. Jak już wskazano w niniejszym Standardzie (oraz tak długo jak UKNF nie wypowie się odmienne w tej sprawie), Usługa chmury obliczeniowej, na podstawie której dochodzi do przetwarzania Tajemnicy bankowej, stanowi zawsze outsourcing bankowy w rozumieniu art. 6a i nast. Prawa bankowego (tylko zlecanie czynności bankowych związane jest z ujawnianiem Tajemnicy bankowej). Jeśli zaś chodzi o Outsourcing szczególny, do outsourcingu bankowego dochodzić będzie w przeważającym wypadku.

6.1. ART. 6A. PRAWA BANKOWEGO

6.1.1. UMOWA OUTSOURCINGOWA

1. Umowa o dostawę Usługi chmury obliczeniowej, która jest umową outsourcingową w rozumieniu art. 6a Prawa bankowego spełnia następujące kryteria:
   1) jest zawarta **zawsze** na piśmie;
   2) ma formę **umowy agencyjnej** uregulowanej przepisami Kodeksu cywilnego od art. 758 do art. 764(9), jeśli dotyczy czynności wskazanych w art. 5 oraz art. 6 Prawa bankowego i polega na świadczeniu usług wskazanych w art. 1 ust. 1) od a) do j) Prawa bankowego (art. 758 § 1 Kodeksu cywilnego: „Przez umowę agencyjną przyjmujący zlecenie (agent) zobowiązuje się, w zakresie działalności swego przedsiębiorstwa, do stałego pośredniczenia, za wynagrodzeniem, przy zawieraniu z klientami umów na rzecz dającego zlecenie przedsiębiorcy albo do zawierania ich w jego imieniu”);
   3) jeśli dotyczy innych czynności niż wskazane w pkt. 2) powyżej, umowa outsourcingowa będzie miała formę **umowy nienazwanej** korzystającej ze swobody umów;
   4) umowy z Dostawcami wymagać będą **dodatkowo zezwolenia KNF**, gdy Usługi chmury obliczeniowej polegać będą na:
      a) wykonywaniu czynności związanych z emitowaniem i przechowywaniem bankowych papierów wartościowych oraz innych papierów wartościowych, a także wykonywaniu innych czynności zleconych związanych z emisją i obsługą papierów wartościowych,
      b) windykacji należności Banku,
      c) wykonywaniu innych czynności, po uzyskaniu zezwolenia Komisji Nadzoru Finansowego.

6.1.2. PODOUTSOURCING

1. Możliwość outsourcingu jest ograniczona:
   1) outsourcing łańcuchowy wyłącznie jeden poziom w dół;
   2) wymagane jest zezwolenie na podoutsourcing w umowie na Usługi chmury obliczeniowej i dodatkowa zgoda Banku na zawarcie konkretnego outsourcingu; oraz
   3) brak jest możliwości podoutsourcowania przedmiotu usługi, możliwość podoutsourcingu tylko czynności pomocniczych i technicznych potrzebnych do realizacji Usługi chmury obliczeniowej.

KOMENTARZ

1. Umowy z Dostawcami ze względu na przedmiot świadczonej usługi będą w przeważającej mierze **umowami nienazwanymi niewymagającymi zezwolenia KNF (z zastrzeżeniem dalszych komentarzy)**, które polegać będą na świadczeniu czynności faktycznych związanych z działalnością bankową.
2. Wyjaśnienie pojęcia czynności faktycznych związanych z działalnością bankową wskazanych w art. 6a ust 1. pkt. 2) Prawa bankowego: przez czynności faktyczne rozumie się: **wszystkie czynności, które nie są czynnościami bankowymi wskazanymi w art. 5 oraz art. 6 Prawa bankowego**, **lecz pozostają z nimi w bezpośrednim i funkcjonalnym związku.**

6.2. ART. 6B. PRAWA BANKOWEGO

6.2.1. ODPOWIEDZIALNOŚĆ W RAMACH UMOWY NA USŁUGI CHMURY OBLICZENIOWEJ

1. **Odpowiedzialność Dostawcy względem Banku:**
   1) pełna odpowiedzialność wobec Banku za szkody wyrządzone klientom za niewykonanie lub nienależyte wykonanie umowy na Usługę chmury obliczeniowej. **Nie można wyłączyć ani ograniczyć;**
   2) możliwość modyfikacji polegającej jedynie na rozszerzeniu takiej odpowiedzialności (odpowiedzialność na zasadzie ryzyka, wskazanie mechanizmu obliczania szkody, rozszerzenie odpowiedzialności o utracone korzyści).
2. **Odpowiedzialność Banku względem klienta Banku:**
   1) pełna odpowiedzialność Banku wobec klienta Banku za szkody wyrządzone za niewykonanie lub nienależyte wykonanie umowy na Usługi chmury obliczeniowej. **Nie można wyłączyć ani ograniczyć**;
   2) możliwość modyfikacji polegającej jedynie na rozszerzeniu takiej odpowiedzialności (odpowiedzialność na zasadzie ryzyka, wskazanie mechanizmu obliczania szkody, rozszerzenie odpowiedzialności o utracone korzyści).

6.3. ART. 6C. PRAWA BANKOWEGO

6.3.1. WYKONANIE UMOWY O USŁUGI CHMURY OBLICZENIOWEJ I EWIDENCJA UMÓW

1. Umowa na Usługi chmury obliczeniowej może zostać zawarta i być wykonywana tylko gdy:
   1) bank i Dostawca będą posiadać plany działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową;
   2) powierzenie wykonywania czynności w ramach umowy na Usługi chmury obliczeniowej nie wpłynie niekorzystnie na prowadzenie przez Bank działalności zgodnie z przepisami prawa, ostrożne i stabilne zarządzanie Bankiem, skuteczność systemu kontroli wewnętrznej w Banku, możliwość wykonywania obowiązków przez biegłego rewidenta upoważnionego do badania sprawozdań finansowych Banku na podstawie zawartej z Bankiem umowy oraz ochronę Tajemnicy bankowej (**zaleca się uzyskanie opinii prawnej w tym zakresie**);
   3) bank uwzględni ryzyko związane z powierzeniem wykonywania takich czynności w systemie zarządzania ryzykiem.

KOMENTARZ

1. Bank ma obowiązek wprowadzenia umowy na Usługi chmury obliczeniowej do ewidencji umów, określając w niej co najmniej:
   1) dane (informacje) identyfikujące Dostawcę,
   2) zakres Usługi chmury obliczeniowej,
   3) miejsce wykonania,
   4) okres obowiązywania umowy.

6.4. ART. 6D. PRAWA BANKOWEGO

6.4.1. ZEZWOLENIE NA ZAWARCIE UMOWY NA USŁUGI CHMURY OBLICZENIOWEJ

1. Zezwolenia UKNF wymagać będą:
   1) zawarcia umowy na Usługi chmury obliczeniowej z Dostawcą, którego siedziba znajduje się w kraju innym niż państwo członkowskie UE; lub
   2) zawarcia umowy na Usługi chmury obliczeniowej, która wykonywana będzie poza państwem członkowskim UE (badanie, jaka część usług wykonywana jest w UE i poza nią).

7. ZAŁĄCZNIKI

ZAŁĄCZNIK 1. Szablon szacowania ryzyka

ZAŁĄCZNIK 2. Objaśnienia i lista wybranych klauzul wraz z przykładami

ZAŁĄCZNIK 3. Plan przetwarzania informacji w chmurze obliczeniowej

ZAŁĄCZNIK 4. Szablon scenariusza wyjścia z relacji z dostawcą

ZAŁĄCZNIK 5. Wyjście z chmury – główne zagadnienia

ZAŁĄCZNIK 6. Szablon dokumentacji kontroli ISO27001

ZAŁĄCZNIK 7. Plan wdrożenia chmury

ZAŁĄCZNIK 8. Schemat wdrożenia chmury

ZAŁĄCZNIK 9. Wymagania dla dostawców

SZABLON SZACOWANIA RYZYKA

L.p.	Zagrożenia	Opis ryzyka	Ocena ryzyka inherentnego (niski/średni/wysoki)		Czynniki ograniczające ryzyko	Plan postępowania z ryzykiem / Ograniczenie ryzyka	Poziom ryzyka rezydualnego (niski/średni/wysoki)
			Wpływ	Prawdopodobieństwo			
1.	Rozproszenie geograficzne przetwarzanych informacji (VI.1.a)	Ryzyko zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami			Usługa chmury obliczeniowej świadczona jest w lokalizacjach: 1) …….. 2) …… ***Przykład czynnika ograniczającego ryzyko:*** *Pozyskano opinie prawne potwierdzające możliwość zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa bankowego*		
2.	Możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji i/lub zezwoleń) (VI.1.B)	Korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony. Dostęp do przetwarzanych informacji przez pracowników i współpracowników					
3.	Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.1.C)	Dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. podostawców) dostawcy usług chmury obliczeniowej					

4.	Przywiązanie do jednego dostawcy usług chmury obliczeniowej (VI.1.E)	Brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powodujący przywiązanie do jednego dostawcy usług chmury obliczeniowej					
5.	Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.1.F)	Awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej					
6.	Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.1.h)	Ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania					
7.	Ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej (VI.1.i)	Ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej					
8.	Podział odpowiedzialności (VI.1.j)	Podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a podmiot nadzorowany					
9.	Możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego (VI.2.a)	Możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego lub w środowisku, które nie podlega kontroli podmiotu nadzorowanego (np. prywatne urządzenia mobilne, dostęp z prywatnych lub publicznych sieci)					
10.	Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (VI.2.b)	Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji)					

11.	Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług (VI.2.c)	Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego					
12.	Stosowane mechanizmy uwierzytelniania (VI.2.d)	Słabość stosowanych mechanizmów uwierzytelniania					
13.	Zasoby ludzkie (VI.3.a)	Wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach					
14.	Zgodność środowiska technologicznego (VI.3.b)	Zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmów integracji					
15.	Szyfrowanie informacji (VI.5)	Zgodność szyfrowania informacji z wymaganiami nadzoru					
16.	Kontrola „łańcucha outsourcingowego” (VI.6)	Ocena „łańcucha outsourcingowego” z perspektywy przepisów szczegółowych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji					

OBJAŚNIENIA I LISTA WYBRANYCH KLAUZUL WRAZ Z PRZYKŁADAMI

Zgodnie z pkt VII. 4.1. Komunikatu, umowa z Dostawcą powinna zawierać co najmniej postanowienia regulujące:

a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;

OBJAŚNIENIE:

1) Należy zwrócić uwagę na to, by definicje „RTO", „RPO" oraz „SLA" zawarte w umowie były zgodne z definicjami zawartymi w Komunikacie.
2) Model odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji wynika z praktyki rynkowej – ważne, by umowa jednoznacznie określała podział odpowiedzialności.

b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;

OBJAŚNIENIE:

1) Komunikat w swej treści wskazuje na wymóg podawania adresu CPD (precyzyjne wskazanie lokalizacji). Brak takiej informacji może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, dlatego jako minimum wystarczy wskazanie np.: „strefy dostępu" lub „regionu", przy czym wskazanie takie powinno obejmować co najmniej kraj i przybliżoną lokalizację CPD (np. miasto lub region geograficzny). CPD powinno, ale nie musi znajdować się w kraju należącym do EOG.
2) Zwracamy uwagę, że zgodnie z Komunikatem, Banki, które zostały uznane stosowną decyzją za operatorów usług kluczowych lub są operatorami infrastruktury krytycznej, powinny w pierwszej kolejności wykorzystywać CPD położone w Polsce o ile - w ocenie Banku - oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.
3) W obowiązującym prawie brak definicji „przetwarzania informacji". W związku z tym, przy stworzeniu przykładowej definicji przetwarzania informacji wykorzystana została definicja przetwarzania danych zawarta w art. 4 pkt 2) RODO.

PRZYKŁADOWE KLAUZULE:

1. [*Definicje*] „**Przetwarzanie informacji**": operacja lub zestaw operacji na informacjach lub zestawach informacji dokonywanych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

c) prawo właściwe umowy (w tym sąd właściwy i zasady rozstrzygania sporów);

PRZYKŁADOWE KLAUZULE:

PRAWO WŁAŚCIWE, JURYSDYKCJA

1. Niniejsza Umowa oraz wszelkie zobowiązania pozaumowne z niej wynikające lub powstające w związku z nią podlegają prawu polskiemu.

2. Każda ze Stron nieodwołalnie wyraża zgodę, chyba że ustawa stanowi o wyłącznej jurysdykcji, aby wszelkie spory, które mogą powstać w związku z niniejszą Umową lub które są związane z jej naruszeniem, wypowiedzeniem lub nieważnością były rozstrzygane przez sąd powszechny, właściwy dla [*np. Miasta Stołecznego Warszawy (Warszawa Śródmieście).*]

lub w przypadku poddania umowy prawu innemu niż polskie:

1. Niniejsza Umowa oraz wszelkie zobowiązania pozaumowne z niej wynikające lub powstające z nią podlegają prawu [_____] [*prawo państwa innego niż polskie*].

2. Z uwagi na okoliczność, iż Zamawiający [*Bank*] jest podmiotem nadzorowanym w rozumieniu polskiej Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. 2019.298), i korzystanie przez Zamawiającego z usług, które są świadczone przez Dostawcę na podstawie niniejszej Umowy jest ściśle regulowane, Dostawca niniejszym oświadcza, iż prawo państwa, któremu poddana została Umowa, pozwala na skuteczne wykonywanie postanowień niniejszej Umowy, wymogów prawa polskiego ciążących na Zamawiającym oraz wytycznych polskiego organu nadzoru, w tym Komunikatu. Szczegółowy opis wymogów prawa polskiego oraz wytycznych wraz z analizą prawną dotyczącą możliwości ich skutecznego wykonywania pod prawem [_____] stanowi Załącznik nr [__] do Umowy.

3. Każda ze Stron nieodwołalnie wyraża zgodę, chyba że ustawa stanowi o wyłącznej jurysdykcji, aby wszelkie spory, które mogą powstać w związku z niniejszą Umową lub które są związane z jej naruszeniem, wypowiedzeniem lub nieważnością były rozstrzygane przez sąd powszechny, właściwy dla [_____].

d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;

OBJAŚNIENIE:

1) W obecnym stanie prawnym chodzi o zgodność z RODO. Dla jasności, przez zwrot „o ile ma zastosowanie" chodzi o sytuację, gdy na podstawie umowy outsourcingu w Chmurze obliczeniowej przetwarzane są dane osobowe.

e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;

n/d.

f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;

g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;

OBJAŚNIENIE:

1) W przypadku outsourcingu bankowego zastosowanie ma zakaz ograniczania odpowiedzialności w relacji Bank – klient, Dostawca – Bank. Dla jasności, przez zwrot „o ile ma zastosowanie" rozumie się sytuację, gdy na podstawie umowy na Usługi chmurowe przetwarzane są informacje, których utrata lub ujawnienie może spowodować szkodę po stronie klientów Banków.

PRZYKŁADOWE KLAUZULE:

1. Dostawca ponosi pełną i nieograniczoną odpowiedzialność wobec Banku za szkody wyrządzone klientom Banku wskutek niewykonania lub nienależytego wykonania Umowy.

h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunków nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;

OBJAŚNIENIE:

1) Aktualizacja listy poddostawców wymaga za każdym razem zmiany (aneksowania) umowy outsourcingu. Zmiana poddostawcy bez zgody Banku może być podstawą wypowiedzenia umowy w trybie natychmiastowym przez Bank. Możliwa jest również sytuacja, w której Dostawca za uprzednim poinformowaniem Banku jednostronnie aktualizuje listę poddostawców. W takim wypadku jednak brak zgody Banku na aktualizację zakomunikowaną Dostawcy oznacza wypowiedzenie umowy w trybie natychmiastowym.
2) Proponujemy, aby lista poddostawców została załączona do Umowy w formie załącznika.

i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań wszystkich poddostawców dostawcy usług chmury obliczeniowej, którzy mają dostęp do przetwarzanych informacji, są transparentne i jasno identyfikowane przez podmiot nadzorowany;

PRZYKŁADOWE KLAUZULE:

1) [*W formie oświadczenia Banku w sekcji „Oświadczenia i zapewnienia"*] Bank oświadcza i zapewnia, że zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań wszystkich Poddostawców, są transparentne i zostały jasno zidentyfikowane przez Bank.

j) źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);

OBJAŚNIENIE:

1) Wydaje się, że celem niniejszego postanowienia jest jednoznaczne wskazanie w umowie kanałów komunikacji służących do informowania o planowanych zmianach w standardach świadczonych usług np. poprzez wskazanie dedykowanego adresu strony www lub adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku do komunikacji.

k) źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;

OBJAŚNIENIE:

1) Wydaje się, że celem niniejszego postanowienia jest jednoznaczne wskazanie w umowie kanałów komunikacji służących do przesyłania dokumentacji technicznej, deklaracji zgodności i instrukcji konfiguracji usług np. poprzez wskazanie dedykowanego adresu strony www lub adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku do komunikacji.

l) zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;

OBJAŚNIENIE:

1) Brzmienie postanowienia będzie każdorazowo uzależnione od rodzaju świadczonych usług i ustaleń stron.

m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);

OBJAŚNIENIE:

1) Zgodnie z RODO, administrator w umowie powierzenia zawartej z podmiotem przetwarzającym musi zawrzeć postanowienie dotyczące umożliwienia przeprowadzenia administratorowi lub audytorowi upoważnionemu przez administratora audytów, w tym inspekcji. Konieczne jest zatem zawarcie w umowie na Usługę chmurową możliwości i zasad przeprowadzenia inspekcji. Taka możliwość nie powinna zostać wyłączona, niezależnie od wyników szacowania ryzyka. Jednakże, w zależności od jego wyników, można natomiast uzależnić prawo do przeprowadzenia audytu/inspekcji przez Bank (wysokie ryzyko) lub podmiot trzeci (średnie i niskie ryzyko). Prawo do inspekcji może jednak zostać umownie ograniczone np. poprzez wskazanie, że będzie środkiem stosowanym dopiero wówczas, gdy inne środki kontroli zawiodą, są niemożliwe do przeprowadzenia lub byłyby niewystarczające w określonym stanie faktycznym.

n) prawo dla nadzoru do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności;

OBJAŚNIENIE:

1) Dostawca musi być świadomy, że umowa zawiera uprawnienie dla nadzoru bankowego (UKNF) do wykonania obowiązków kontrolnych.

o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania i/lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;

p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;

n/d.

q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu i/lub usunięcia przetwarzanych informacji;

OBJAŚNIENIE:

1) Umowa powinna regulować termin realizacji tych obowiązków, a także sposób potwierdzenia usunięcia kopii przetwarzanych informacji.

r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;

n/d.

s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i dostawcę usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również inne strony (np. klientów, poddostawców, itp.), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

n/d.

PLAN PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

1. INFORMACJE O REALIZOWANYCH ZADANIACH I PRZETWARZANYCH INFORMACJACH

Nazwa systemu / aplikacji, których informacje są przetwarzane	...
Opis zadania realizowanego za pomocą usługi	...
Rodzaj przetwarzanych informacji	☐ Chronione (tajemnica bankowa) ☐ Inne chronione (z innych przepisów prawa) ☐ Niechronione
Klasa przetwarzanych informacji[1]	☐ Publiczne ☐ Wewnętrzne ☐ Poufne
Typ informacji	☐ Produkcyjne ☐ Testowe
Outsourcing szczególny	☐ Tak ☐ Nie
Opis formatu i struktury informacji	... *(może być referencja do szczegółowej dokumentacji)*

2. OCHRONA INFORMACJI

Mechanizmy zabezpieczenia informacji	☐ Maskowanie ☐ Pseudonimizacja ☐ Anonimizacja ☐ Inne
Opis mechanizmów zabezpieczenia informacji	... *Należy opisać, jakie pola i w jaki sposób są poddawane poniższym procesom zabezpieczenia*
Opis mechanizmów szyfrowania informacji	... *(może być referencja do szczegółowej dokumentacji)*
Zarządzanie i przechowywanie kluczy szyfrujących	☐ Dostawca ☐ Bank
Opis kontroli dostępu do przetwarzanych informacji	... *informacja o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany*

3. UMOWA Z DOSTAWCĄ

Dostawca	
Nr umowy	
Prawo właściwe dla umowy	
Okres obowiązywania umowy	
Data ostatniej zmiany w umowie	
Data rozpoczęcia korzystania z usługi	

4. INNE

Data kolejnej weryfikacji planu	
Data ostatniej aktualizacji planu	
Zakres ostatniej aktualizacji	

SCENARIUSZ WYJŚCIA Z RELACJI Z DOSTAWCĄ

1. OPIS USŁUGI

Identyfikator Umowy	
Usługa (przedmiot umowy)	
Dostawca (nazwa / firma przedsiębiorcy)	
Planowana data zakończenia przetwarzania danych w Chmurze:	
Okres wypowiedzenia umowy: a) przez bank b) przez dostawcę	

2. SPOSÓB POSTĘPOWANIA W ZWIĄZKU Z WYGAŚNIĘCIEM UMOWY

Założona strategia	**Przedłużenie relacji z dotychczasowym dostawcą:** □ Zawarcie / przedłużenie umowy z dotychczasowym dostawcą **Realizacja usługi przez inny podmiot:** □ Wybór nowego dostawcy **Realizacja usługi przez pozostałych, dotychczasowych dostawców** □ Kontynuacja z dotychczasowymi dostawcami **Powrót działalności do banku:** □ Przejęcie działalności przez jednostkę banku **Zaprzestanie działalności:** □ Brak kontynuowania działalności po wygaśnięciu umowy **Inne:** □ ..... □ .....
	Wskaż wariant preferowany spośród wymienionych powyżej:

3. KLUCZOWE DZIAŁANIA UMOŻLIWIAJĄCE REALIZACJĘ SCENARIUSZA WYJŚCIA

Przedłużenie relacji	
Realizacja usługi przez inny podmiot	
Realizacja usługi przez bank (powrót do banku)	
Zaprzestanie działalności będącej przedmiotem umowy	
Inne	przykłady:

4. ZAANGAŻOWANE JEDNOSTKI BANKU REALIZUJĄCE SCENRIUSZ WYJŚCIA

Jednostki realizujące scenariusz	
Jednostki wspierające	
Jednostki informowane o wdrożeniu scenariusza	

5. HISTORIA DOKUMENTU

Data utworzenia przeglądu / zmiany	**Zatwierdzający (Dyrektor / Manager Zespołu w jednostce Właściciela Funkcjonalnego)**	**Komentarz / zakres zmian**

WYJŚCIE Z CHMURY – GŁÓWNE ZAGADNIENIA

ROZDZIAŁ I

PLAN WYCOFANIA USŁUGI

1. SCENARIUSZE WYCOFANIA

1. Należy określić przewidywane scenariusze wycofania dla usługi np. migracja on premise, zmiana dostawcy etc.
2. Dopuszczalne jest określenie alternatywnych scenariuszy zależnie od sytuacji – np. nagłe zaprzestanie świadczenia usługi, rezygnacja z usługi po zakończeniu kontraktu etc.

2. WPŁYW ZMIANY NA ORGANIZACJE

1. Należy opisać wpływ zmiany na organizacje, tj. zmiany w procesach krytycznych, wpływ na zasoby ludzkie i strukturę organizacyjną, wymagania szkoleniowe etc.

3. OPIS TRANSFERU USŁUGI ORAZ DANYCH

1. Wysokopoziomowy opis procesu migracji usługi oraz danych, wymaganych narzędzi etc.
2. Transfer Usług to całokształt działań (w tym czynności prawnych) prowadzących do zwrotu Klientowi sprzętu Klienta, oprogramowania Klienta, całości przetwarzanych na zlecenie Klienta Danych Klienta oraz w zależności od okoliczności prawnych, przeniesienia na Klienta umów z osobami trzecimi wymaganych do realizacji Usług zdefiniowanych w Umowie, w sposób gwarantujący nieprzerwaną realizację Usług.

4. SCENARIUSZE TESTOWE WYCOFANIA I KRYTERIA AKCEPTACJI

1. Scenariusze testowe dla procesów migracji.
2. Klient wraz z Dostawcą jest zobowiązany do wykonywania cyklicznych testów Planu Wyjścia, o rekomendowanej częstotliwości nie rzadszej niż raz na 12 miesięcy.

5. BACKUP DANYCH I CZASY MIGRACJI

1. Należy oszacować czas potrzebny na przygotowanie projektu przełączenia, uruchomienie prac operacyjnych, uzyskanie odpowiednich zgód i poinformowanie użytkowników usługi o planowanym przełączeniu.
2. Określenie czasu pobrania danych do migracji od Dostawcy. Czas musi uwzględniać zapisy umowne z dostawcą na wyodrębnienie danych i fizyczne ich przekazanie (w tym warunki sieciowe i czas na zamontowanie danych).
3. Określenie czasu dla procesu przełączenia usługi w wymiarze inicjalnym i docelowym migracji danych, a także uruchomienia usługi na odtworzonych danych. Czas ten nie może naruszać przyjętego RTO i RPO dla usługi.
4. Dla usług o znaczeniu krytycznym dla ciągłości działania Banku należy przechowywać backup lokalny danych przekazanych do chmury celem minimalizacji czasu przełączenia usługi. Zakres backupu i czas retencji danych powinien zostać zdefiniowany z punktu widzenia ryzyka dla ciągłości działania. Backup ma na celu jedynie minimalizację czasu inicjalnego przełączenia najbardziej krytycznych danych. Całkowity czas migracji zakłada pozyskanie wszystkich danych od Dostawcy.

6. HARMONOGRAM MIGRACJI

1. Szacunkowy harmonogram migracji na „on-premise” lub do innej usługi. Powinien być to harmonogram projektowy, zawierać wymagane zasoby, zadania i kamienie milowe.

7. ROLE I ODPOWIEDZIALNOŚCI

1. Określenie ról i odpowiedzialności w procesie migracji
2. Obowiązki dostawcy

3. W razie wypowiedzenia lub rozwiązania Umowy niezależnie od przyczyny, Dostawca usług chmurowych zapewni Klientowi, niezwłocznie po wygaśnięciu lub rozwiązaniu Umowy możliwość transferu Danych Klienta poprzez:
   1) umożliwienie Klientowi pobrania Danych Klienta ze swojej infrastruktury w terminie ustalonym przez Klienta i Dostawcę usług chmurowych,
   2) wydanie loginów i haseł zgodnie z Umową,
   3) zapewnienie właściwej ochrony danych klienta znajdujących się w logach systemów współdzielonych,
   4) zwrot sprzętu Klienta wniesionego do infrastruktury Dostawcy, jeśli taka sytuacja miała miejsce,
   5) zwrot dokumentacji w wersji papierowej (o ile taka istniała).
4. Dostawca usług chmurowych zapewni Klientowi, w zależności od okoliczności prawnych, możliwość ciągłego, nieprzerwanego korzystania z licencji niezbędnych do podtrzymania ciągłości działania usług, w tym zapewni możliwość przeniesienia, w zależności od okoliczności prawnych na Klienta licencji, o których mowa w punkcie powyżej.
5. Dostawca usług chmurowych jest zobowiązany do:
   1) usunięcia w sposób nieodwracalny danych Klienta oraz oprogramowania Klienta z zasobów Dostawcy oraz podwykonawców współpracujących,
   2) w szczególności usunięcia w sposób nieodwracalny danych Klienta z zasobów Dostawcy oraz podwykonawców współpracujących mających charakter danych osobowych, oraz danych objętych tajemnicą bankową lub zawodową,
   3) współpracy z Klientem w zakresie transferu danych do Klienta lub innego podmiotu wskazanego przez Klienta,
   4) zapewnienia współpracy jego podwykonawców w zakresie realizacji planu wyjścia,
   5) określenia wspólnie z Klientem: a) szczegółowego harmonogramu planu wyjścia, b) szczegółowego zakresu prowadzonych czynności, c) szczegółowego sposobu realizacji planu wyjścia, d) odpowiedzialności Stron, e) środków technicznych niezbędnych do realizacji planu wyjścia, jeśli są potrzebne.

8. WYMAGANIA DLA WYCOFYWANIA USŁUGI (SPRZĘT ETC.)

8.1. SCENARIUSZ 1 MIGRACJA „ON-PREMISE”

1. Należy zdefiniować parametry środowiska lokalnego w zakresie dostępności, wydajności i pojemności w celu przejęcia usługi chmurowej, w której się znajdują.
2. Plan wyjścia powinien w szczególności obejmować także:
   1) wyznaczenie dedykowanych managerów odpowiedzialnych za przeprowadzenie procesu transferu usług chmurowych,
   2) przygotowanie do transportu w uzgodniony przez Strony sposób, całości sprzętu Klienta, jeżeli taki był elementem świadczenia usług,
   3) wydanie Klientowi haseł i loginów pozwalających na dalsze korzystanie z danych klienta, w tym haseł i loginów do baz danych oraz wszystkich systemów objętych usługami,
   4) przekazanie przez Dostawcę usług chmurowych wszystkich informacji dotyczących sposobu dostarczania i obsługi świadczonych usług istotnych z punktu widzenia przeniesienia usług i przekazania kompetencji utrzymaniowych innemu podmiotowi,
   5) zapewnienie po stronie Dostawcy usług chmurowych bezpiecznego połączenia teleinformatycznego platformy, wykorzystywanej do świadczenia usług chmurowych, do systemu informatycznego wskazanego przez Klienta, z wykorzystaniem bezpiecznej sieci teleinformatycznej, w celu przeprowadzenia transferu danych klienta,
   6) zapewnienie przez Klienta środków technicznych po stronie systemu informatycznego Klienta umożliwiających zestawienie połączenia teleinformatycznego,
   7) zapewnienie transferu do systemu teleinformatycznego wskazanego przez Klienta całości danych klienta, w sposób zapewniający ich pełne bezpieczeństwo oraz integralność, i poziom transferu umożliwiający sprawne przeniesienie wszystkich danych klienta w czasie uzgodnionym przez Strony, a także wydanie wszystkich kopii zapasowych danych klienta (o ile były sporządzane zgodnie z Umową),
   8) przekazanie przez Dostawcę usług chmurowych wiedzy specyficznej dla realizowanych usług chmurowych, w takim zakresie, w jakim będzie to niezbędne do dalszej realizacji usług przez Klienta lub podmiot trzeci wskazany przez Klienta,
   9) niezwłocznie po zakończeniu świadczenia usług chmurowych usunięcie przez Dostawcę oraz pod-

wykonawców Dostawcy usług chmurowych, w sposób trwały oraz zgodny z najlepszymi praktykami w tym zakresie, całości ewentualnie posiadanych kopii danych klienta (po uprzednim transferze takich danych do Klienta lub podmiotu wskazanego przez Klienta) oraz wszystkich danych i informacji (np. plików konfiguracyjnych specyficznie wykorzystywanych dla danego Klienta, a niestanowiących część Usług Chmurowych Dostawcy) wykorzystywanych do konfiguracji, obsługi, backupu i archiwizacji systemu lub poszczególnych jego elementów.

3. Wymagania uwzględniają:
   1) odpowiednią ilość serwerów wraz z określeniem ich lokalizacji w centrach danych,
   2) przewidują wolne miejsce w centrach danych wraz z zapewnieniem fizycznej możliwości wpięcia w infrastrukturę,
   3) odpowiednią konfigurację serwerów, zapewniającą odpowiednią wydajność, (odpowiednia ilość procesorów, odpowiednia ilość pamięci RAM, odpowiednie połączenia sieciowe, odpowiednie zasoby dyskowe),
   4) odpowiednią ilość przestrzeni dyskowej, która jest niezbędna do przejęcia danych przechowywanych w usłudze chmurowej. Przestrzeń ta musi zostać przewidziana na okres jednego roku i aktualizowana raz do roku w planie przełączenia.
4. Zdefiniowane środowisko jest dostępne w jednym z poniższych podejść:
   1) fizycznie zakupione i skonfigurowane na potrzeby migracji,
   2) niezakupione, ale dostępne u producenta w podanej konfiguracji. Taka dostępność potwierdzona jest listem intencyjnym lub umową z dostawcą, w której określony jest czas pozyskania i dostarczenia infrastruktury,
   3) posiadana jest infrastruktura wykorzystywana do innych celów, która może zostać w razie uruchomienia planu zwolniona i w okresie przejściowym do zakupu, może zostać użyta celem wykonania przełączenia.

8.2. SCENARIUSZ 2 MIGRACJA DO INNEGO DOSTAWCY USŁUG

1. Alternatywne usługi chmurowe wraz z dostawcami, czasem uruchomienia i kosztem.

Usługa alternatywna	Kluczowe funkcjonalności niedostępne w usłudze alternatywnej	Czas uruchomienia usługi / Szacunkowy czas migracji	Koszt

2. Określenie minimalnych wymagań bezpieczeństwa dla wycofania usługi:
   1) wymagania bezpieczeństwa dla docelowego rozwiązania po wycofaniu,
   2) wymagania bezpieczeństwa dla procesu migracji.
3. Proces migracji danych i przełączenia usługi.
4. Proces musi uwzględniać poniższe punkty wraz z ich operacyjnym rozwinięciem i technicznym uszczegółowieniem. Na potrzeby opisu procesu powinny zostać opracowane instrukcje wykonawcze dla wszystkich ról zdefiniowanych w procesie.
   1) formalna decyzja o wycofaniu lub przełączeniu. Określenie zasad wydania takiej decyzji i jej trybu,
   2) poinformowanie użytkowników o uruchomieniu planu przełączenia, wraz z podaniem przewidywanych czasów i skutków dla użytkowników,
   3) pozyskanie i skonfigurowanie infrastruktury,
   4) wyodrębnienie danych od dostawcy i fizyczne ich przekazanie,
   5) zamontowanie danych z backupu w środowisku Banku i poinformowanie o inicjalnym uruchomieniu usługi,
   6) zamontowanie danych od Dostawcy i poinformowanie o pełnym przełączeniu usługi.
5. Klient może podjąć decyzję o wyłączeniu realizacji niektórych zobowiązań wynikających z planu wyjścia. W przypadku podjęcia takiej decyzji przez Klienta, Strony dostosowują plan wyjścia do zmian wprowadzonych przez Klienta - w szczególności w związku z rezygnacją z określonych zadań Klient może żądać skrócenia harmonogramu realizacji planu wyjścia.

6. Strony w czasie realizacji planu wyjścia zapewnią personel techniczny o kompetencjach i wiedzy umożliwiającej realizację uzgodnionego przez Strony planu wyjścia w uzgodnionym terminie.
7. Strony zapewnią dostęp do informacji niezbędnych do wykonania powierzonych zadań w ramach planu wyjścia, w tym szczegóły dotyczące odpowiedniego systemu informatycznego.
8. Strony w trakcie trwania umowy przygotowują szczegółowe plany wyjścia dla poszczególnych usług oraz zobowiązują się do ich częściowego lub całościowego przetestowania w trakcie trwania umowy.
9. Cały proces wyjścia powinien zakończyć się podpisaniem protokołu, w którym jedna strona potwierdza przejęcie sprzętu, licencji, oprogramowania itp., druga strona potwierdza usunięcie danych klienta.
10. Strony w trakcie trwania umowy dokonają przybliżonej oceny kosztów planu wyjścia.

ROZDZIAŁ II

1. PLAN NAGŁEGO ZAPRZESTANIA ŚWIADCZENIA USŁUGI

1. W przypadku nagłego i długotrwałego braku dostępu do usługi z powodu problemów po stronie dostawcy usługi (dłuższe niż zakłada SLA), przewidując przywrócenie usługi w przeciągu [] godzin, należy wykonać plan znajdujący się w tym punkcie.
2. Wymagania techniczne zbieżne z rozdziałem I, przy założeniu powrotu do wykorzystywanej usługi chmurowej.
   1) Określenie, jakie konta i jakie uprawnienia zostaną użyte do przełączenia,
   2) Przełączenie usługi zakłada dostęp tylko do wybranego zakresu danych w trybie nagłym. Należy podać zakres i typ danych, jaki będzie dostępny i jak zostanie pozyskany. Przyjmuje się zatem ryzyko nieposiadania dostępu do całości danych i uruchomienia funkcjonalności przesyłania wiadomości bieżących,
   3) Udokumentowane instrukcje dla Administratorów Systemów wraz przygotowanymi zgłoszeniami serwisowymi (RFC) dla wszystkich zadań przełączenia,
   4) W przypadku problemów na poziomie CRITICAL powiadamiany jest odpowiedni dział w ramach struktury IT Banku oraz uruchamiany jest Dostawca w ramach wykupionej usługi wsparcia. Równolegle rejestrowany jest problem, którego obsługa realizowana jest w ramach oddzielnego procesu problem managementu Banku,
   5) Jeżeli Bank nie ma zdefiniowanego procesu problem management, należy opracować także dedykowaną instrukcję, role i zadania dla koordynatora przełączenia usługi. Instrukcja taka zawiera przede wszystkim zasady poinformowania użytkowników o przełączeniu usługi,
   6) Powrót do usługi chmurowej jest opisany jako powyżej poprzez instrukcje dla administratorów i rozpisane zadania.

ISO27001 — OPIS KONTROLI PO STRONIE DOSTAWCY

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.5.1.1.	Polityki bezpieczeństwa informacji	Zabezpieczenie Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym	Tak	*Przykładowy opis*	Przykładowy opis	Samoocena	
A.5.1.2.	Przegląd polityk bezpieczeństwa informacji	Zabezpieczenie Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne	Tak			Samoocena	
A.6.1.1.	Role i odpowiedzialność za bezpieczeństwo informacji	Zabezpieczenie Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana	Tak			Samoocena	
A.6.1.2.	Rozdzielanie obowiązków	Zabezpieczenie Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić, celem ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia organów organizacji	Tak			Samoocena	
A.6.1.3.	Kontakty z organami władzy	Zabezpieczenie Należy utrzymywać stosowne kontakty z właściwymi organami władzy	Tak			Samoocena	
A.6.1.4.	Kontakty z grupami zainteresowanych specjalistów	Zabezpieczenie Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa	Tak			Samoocena	

A.6.1.5.	Bezpieczeństwo informacji w zarządzaniu projektami	Zabezpieczenie Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu	Tak			Samoocena	
A.6.2.1.	Polityka stosowania urządzeń mobilnych	Zabezpieczenie Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzania ryzykami, wynikającymi z użytkowania urządzeń mobilnych	Tak			Samoocena	
A.6.2.2.	Telepraca	Zabezpieczenie Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony infromacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy	Tak			Samoocena	
A.7.1.1.	Postępowanie sprawdzające	Zabezpieczenie Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk	Tak			Samoocena	
A.7.1.2.	Warunki zatrudnienia	Zabezpieczenie Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji	Tak			Samoocena	
A.7.2.1.	Odpowiedzialność kierownictwa	Zabezpieczenie Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami	Tak			Samoocena	
A.7.2.2.	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Zabezpieczenie Wszyscy pracownicy organizacji oraz w stosownych wypadkach kontrahenci, powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy	Tak			Samoocena	
A.7.2.3.	Postępowanie dyscyplinarne	Zabezpieczenie Postepowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad	Tak			Samoocena	

A.7.3.1.	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Zabezpieczenie Należy określić i przedstawić pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je	Tak			Samoocena	
A.8.1.1.	Inwentaryzacja aktywów	Zabezpieczenie Należy identyfikować aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów	Tak			Samoocena	
A.8.1.2.	Własność aktywów	Zabezpieczenie Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom	Tak			Samoocena	
A.8.1.3.	Akceptowalne użycie aktywów	Zabezpieczenie Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji	Tak			Samoocena	
A.8.1.4.	Zwrot aktywów	Zabezpieczenie Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji	Tak			Samoocena	
A.8.2.1.	Klasyfikowanie informacji	Zabezpieczenie: Informacje powinny być sklasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację	Tak			Samoocena	
A.8.2.2.	Oznaczanie informacji	Zabezpieczenie Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji	Tak			Samoocena	
A.8.2.3.	Postępowanie z aktywami	Zabezpieczenie Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji	Tak			Samoocena	
A.8.3.1.	Zarządzanie nośnikami wymiennymi	Zabezpieczenie Organizacja powinna wdrożyć procedury zarzadzania nośnikami wymiennymi, zgodnie ze schematem klasyfikacji przyjętym w organizacji	Tak			Samoocena	

A.8.3.2.	Wycofywanie nośników	Zabezpieczenie Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami	Tak			Samoocena	
A.8.3.3.	Przekazywanie nośników	Zabezpieczenie Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu	Tak			Samoocena	
A.9.1.1.	Polityka kontroli dostępu	Zabezpieczenie Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji	Tak			Samoocena	
A.9.1.2.	Dostęp do sieci i usług sieciowych	Zabezpieczenie Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia	Tak			Samoocena	
A.9.2.1.	Rejestrowanie i wyrejestrowanie użytkowników	Zabezpieczenie W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników	Tak			Samoocena	
A.9.2.2.	Przydzielanie dostępu użytkownikom	Zabezpieczenie Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników	Tak			Samoocena	
A.9.2.3.	Zarządzanie prawami uprzywilejowanego dostępu	Zabezpieczenie Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować	Tak			Samoocena	
A.9.2.4.	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Zabezpieczenie Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania	Tak			Samoocena	
A.9.2.5.	Przegląd praw dostępu użytkowników	Zabezpieczenie Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu	Tak			Samoocena	

A.9.2.6.	Odbieranie lub dostosowywanie praw dostępu	Zabezpieczenie Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia, lub dostosowywać do zaistniałych zmian	Tak			Samoocena	
A.9.3.1.	Stosowanie poufnych informacji uwierzytelniających	Zabezpieczenie Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających	Tak			Samoocena	
A.9.4.1.	Ograniczenie dostępu do informacji	Zabezpieczenie Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu	Tak			Samoocena	
A.9.4.2.	Procedury bezpiecznego logowania	Zabezpieczenie Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania	Tak			Samoocena	
A.9.4.3.	System zarządzania hasłami	Zabezpieczenie Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości	Tak			Samoocena	
A.9.4.4.	Użycie uprzywilejowanych programów narzędziowych	Zabezpieczenie Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi	Tak			Samoocena	
A.9.4.5.	Kontrola dostępu do kodów źródłowych programów	Zabezpieczenie Dostęp do kodu źródłowego programów powinien być ograniczony	Tak			Samoocena	
A.10.1.1.	Polityka stosowania zabezpieczeń kryptograficznych	Zabezpieczenie Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji	Tak			Samoocena	
A.10.1.2.	Zarządzanie kluczami	Zabezpieczenie Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy	Tak			Samoocena	

A.11.1.1.	Fizyczna granica obszaru bezpiecznego	Zabezpieczenie Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji	Tak			Samoocena	
A.11.1.2.	Fizyczne zabezpieczenie wejść	Zabezpieczenie Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym	Tak			Samoocena	
A.11.1.3.	Zabezpieczenie biur, pomieszczeń i obiektów	Zabezpieczenie Należy zaprojektować i stosować fizyczne zabezpieczenia biur, pomieszczeń i obiektów	Tak			Samoocena	
A.11.1.4.	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zabezpieczenie Należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami	Tak			Samoocena	
A.11.1.5.	Praca w obszarach bezpiecznych	Zabezpieczenie Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych	Tak			Samoocena	
A.11.1.6.	Obszary dostaw i załadunku	Zabezpieczenie Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i jeśli to możliwe, odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi	Tak			Samoocena	
A.11.2.1.	Lokalizacja i ochrona sprzętu	Zabezpieczenie Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu	Tak			Samoocena	
A.11.2.2.	Systemy wspomagające	Zabezpieczenia Sprzęt należy chronić przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających	Tak			Samoocena	
A.11.2.3.	Bezpieczeństwo okablowania	Zabezpieczenie Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne należy chronić przez przechwyceniem, zakłóceniem lub uszkodzeniem	Tak			Samoocena	

A.11.2.4.	Konserwacja sprzętu	Zabezpieczenie Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności	Tak			Samoocena	
A.11.2.5.	Wynoszenie aktywów	Zabezpieczenie Sprzętu, informacji i programów nie należy wynosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia	Tak			Samoocena	
A.11.2.6.	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Zabezpieczenie Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą	Tak			Samoocena	
A.11.2.7.	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Zabezpieczenie Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane	Tak			Samoocena	
A.11.2.8.	Pozostawianie sprzętu użytkownika bez opieki	Zabezpieczenie Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki	Tak			Samoocena	
A.11.2.9.	Polityka czystego biurka i ekranu	Zabezpieczenie Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji	Tak			Samoocena	
A.12.1.1.	Dokumentowanie procedur eksploatacyjnych	Zabezpieczenie Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom	Tak			Samoocena	
A.12.1.2.	Zarządzanie zmianami	Zabezpieczenie Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane	Tak			Samoocena	
A.12.1.3.	Zarządzanie pojemnością	Zabezpieczenie Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości dla zapewnienia właściwej wydajności systemu	Tak			Samoocena	

A.12.1.4.	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Zabezpieczenie Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym	Tak			Samoocena	
A.12.2.1.	Zabezpieczenia przed szkodliwym oprogramowaniem	Zabezpieczenie Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników	Tak			Samoocena	
A.12.3.1.	Zapasowe kopie informacji	Zabezpieczenie Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować zgodnie z ustaloną polityką kopii zapasowych	Tak			Samoocena	
A.12.4.1.	Rejestrowanie zdarzeń	Zabezpieczenie Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji	Tak			Samoocena	
A.12.4.2.	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem	Tak			Samoocena	
A.12.4.3.	Rejestrowanie działań administratorów i operatorów	Zabezpieczenie Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać	Tak			Samoocena	
A.12.4.4.	Synchronizacja zegarów	Zabezpieczenie Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu	Tak			Samoocena	
A.12.5.1.	Instalacja oprogramowania w systemach produkcyjnych	Zabezpieczenie Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych	Tak			Samoocena	
A.12.6.1.	Zarządzanie podatnościami technicznymi	Zabezpieczenie Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku	Tak			Samoocena	

A.12.6.2.	Ograniczenia w instalowaniu oprogramowania	Zabezpieczenie Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników	Tak			Samoocena	
A.12.7.1.	Zabezpieczenia audytu systemów informacyjnych	Zabezpieczenie Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych, w celu zminimalizowania zakłóceń w procesach biznesowych	Tak			Samoocena	
A.13.1.1.	Zabezpieczenia sieci	Zabezpieczenie Sieci powinny być zarządzane i nadzorowane, w celu ochrony informacji w systemach i aplikacjach	Tak			Samoocena	
A.13.1.2.	Bezpieczeństwo usług sieciowych	Zabezpieczenie Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania	Tak			Samoocena	
A.13.1.3.	Rozdzielanie sieci	Zabezpieczenie Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci	Tak			Samoocena	
A.13.2.1.	Polityki i procedury przesyłania informacji	Zabezpieczenie Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności	Tak			Samoocena	
A.13.2.2.	Porozumienia dotyczące przesyłania informacji	Zabezpieczenie Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi	Tak			Samoocena	
1.13.2.3.	Wiadomości elektroniczne	Zabezpieczenie Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione	Tak			Samoocena	
A.13.2.4.	Umowy o zachowaniu poufności	Zabezpieczenie Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności ku nieujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji	Tak			Samoocena	
A.14.1.1.	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Zabezpieczenie Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących	Tak			Samoocena	
A.14.1.2.	Zabezpieczenie usług aplikacyjnych w sieciach publicznych	Zabezpieczenie Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnieniem i zmianami	Tak			Samoocena	

A.14.1.3.	Ochrona transakcji usług aplikacyjnych	Zabezpieczenie Informacje związanie z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu	Tak			Samoocena	
A.14.2.1.	Polityka bezpieczeństwa prac rozwojowych	Zabezpieczenie Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji	Tak			Samoocena	
A.14.2.2.	Procedury kontroli zmian w systemach	Zabezpieczenie Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, przy użyciu formalnych procedur kontroli zmian	Tak			Samoocena	
A.14.2.3.	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Zabezpieczenie Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych lub przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo	Tak			Samoocena	
A.14.2.4.	Ograniczenia dotyczące zmian w systemach oprogramowania	Zabezpieczenie Modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować	Tak			Samoocena	
A.14.2.5.	Zasady projektowania bezpiecznych systemów	Zabezpieczenie Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi	Tak			Samoocena	
A.14.2.6.	Bezpieczne środowisko rozwojowe	Zabezpieczenie Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego procesów	Tak			Samoocena	
A.14.2.7.	Prace rozwojowe zlecane podmiotom zewnętrznym	Zabezpieczenie Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym	Tak			Samoocena	
A.14.2.8.	Testowanie bezpieczeństwa systemów	Zabezpieczenie Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych	Tak			Samoocena	

A.14.2.9.	Testy akceptacyjne systemów	Zabezpieczenie Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane	Tak			Samoocena	
A.14.3.1.	Ochrona danych testowych	Zabezpieczenie Dane testowe należy starannie wybierać, chronić i nadzorować	Tak			Samoocena	
A.15.1.1.	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Zabezpieczenie Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji	Tak			Samoocena	
A.15.1.2.	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Zabezpieczenie Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji	Tak			Samoocena	
A.15.1.3.	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Zabezpieczeni Porozumienia z dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów	Tak			Samoocena	
A.15.2.1.	Monitorowanie i przegląd usług świadczonych przez dostawców	Zabezpieczenie Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych	Tak			Samoocena	
A.15.2.2.	Zarządzanie zmianami w usługach świadczonych przez dostawców	Zabezpieczenie Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych, których dotyczą oraz ponownego szacowania ryzyka	Tak			Samoocena	
A.16.1.1.	Odpowiedzialność i procedury	Zabezpieczenie Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji	Tak			Samoocena	
A.16.1.2.	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenie związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe	Tak			Samoocena	

A.16.1.3.	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Zabezpieczenie Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach	Tak			Samoocena	
A.16.1.4.	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji	Tak			Samoocena	
A.16.1.5.	Reagowanie na incydenty związane z bezpieczeństwem informacji	Zabezpieczenie Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami	Tak			Samoocena	
A.16.1.6.	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Zabezpieczenie Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów	Tak			Samoocena	
A.16.1.7.	Gromadzenie materiału dowodowego	Zabezpieczenie Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy	Tak			Samoocena	
A.17.1.1.	Planowanie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu czy katastrofy	Tak			Samoocena	
A.17.1.2.	Wdrożenie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji	Tak			Samoocena	
A.17.1.3.	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.	Tak			Samoocena	
A.17.2.1.	Dostępność środków przetwarzania informacji	Zabezpieczenie Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności	Tak			Samoocena	

A.18.1.1.	Określenie stosownych wymagań prawnych i umownych	Zabezpieczenie Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji	Tak			Samoocena	
A.18.1.2.	Prawa własności intelektualnej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania	Tak			Samoocena	
A.18.1.3.	Ochrona zapisów	Zabezpieczenie Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych	Tak			Samoocena	
A.18.1.4.	Prywatność i ochrona danych identyfikujących osobę	Zabezpieczenie Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji	Tak			Samoocena	
A.18.1.5.	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenie Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami	Tak			Samoocena	
A.18.2.1.	Niezależny przegląd bezpieczeństwa informacji	Zabezpieczenie Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany	Tak			Samoocena	
A.18.2.2.	Zgodność z politykami bezpieczeństwa i standardami	Zabezpieczenie Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności	Tak			Samoocena	
A.18.2.3.	Sprawdzanie zgodności technicznej	Zabezpieczenie Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji	Tak			Samoocena	

KROKI WDROŻENIA USŁUGI PRZETWARZANIA DANYCH W CHMURZE OBLICZENIOWEJ W BANKOWOŚCI

WSTĘP

Niniejszy dokument opisuje kroki wdrożenia usługi przetwarzania danych w Chmurze obliczeniowej. Proces opisuje kroki wdrożenia przy założeniu, że Usługa Chmurowa obliczeniowa stanowi outsourcing szczególny chmury obliczeniowej. Proces wdrożenia w przypadku kwalifikacji innej niż outsourcing szczególny chmury obliczeniowej jest poza zakresem niniejszego dokumentu.
Opisane kroki stanowią uzupełnienie standardowych procesów funkcjonujących w Bankach o niezbędne działania będące realizacją wymagań określonych w **Komunikacie Urzędu Komisji Nadzoru Finansowego dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej o charakterze publicznym lub hybrydowym** („Komunikat Chmurowy").

1. ZIDENTYFIKOWANIE POTRZEBY BIZNESOWEJ

1. Na tym etapie identyfikowana i dokumentowana jest potrzeba biznesowa, zgodnie z procesami obowiązującymi w Banku.
2. Otwierany jest formalny „projekt" lub inna inicjatywa, która pozwala na alokację prac związanych z krokami opisanymi poniżej.
3. Jednostki odpowiedzialne za architekturę, technologię oraz cyberbezpieczeństwo określają zasadność dalszej analizy niniejszej potrzeby pod kątem możliwości realizacji w chmurze obliczeniowej.

PRODUKTY

1. Opis wymagań biznesowych.
2. Formalny „Projekt/charter" otwierający projekt.

2. WSTĘPNA OCENA POD KĄTEM MOŻLIWOŚCI REALIZACJI POTRZEBY W USŁUDZE CHMUROWEJ

1. Na tym etapie dokonywana jest wstępna ocena („pre-assessment") potrzeby pod kątem realizacji w chmurze obliczeniowej, tj.:
   1) porównanie rozwiązań w usłudze chmurowej vs. on-premise – wstępna ocena realizacji wymagań i kosztów, w tym analiza potencjalnych dostawców usług chmurowych;
   2) architektura, integracja, docelowa konfiguracja – zgodność z docelową architekturą Banku;
   3) wstępne PoC rozwiązania, jeśli planowane jest wykorzystanie całkowicie nowych dla Banku technologii;
   4) inwentaryzacja i klasyfikacja danych, klasyfikacja istotności usługi - w zależności od wyników podejmowana jest wstępna decyzja pod kątem outsourcingu nadzorowanego;
   5) zbadanie możliwości pozyskania kompetencji dla usługi chmurowej i on-premise;
   6) zgodność ze strategią Banku;
   7) zgodność z regulacjami wewnętrznymi.

PRODUKTY

1. Wstępna analiza wykonalności pod kątem usługi chmurowej vs. on-premise.

3. PUNKT DECYZYJNY/DECYZJA O DOPUSZCZALNOŚCI WDROŻENIA ROZWIĄZANIA CHMUROWEGO

1. Na tym etapie podejmowana jest decyzja o dalszym procesowaniu potrzeby; możliwe scenariusze:
   1) Brak możliwości/zasadności wykorzystania rozwiązania chmurowego;
   2) Dopuszczalne rozwiązanie chmurowe – wymagany outsourcing nadzorowany;
   3) Dopuszczalne rozwiązanie chmurowe – niewymagany outsourcing nadzorowany.
2. Dalsze kroki będą opisywane tylko dla **scenariusza 2**.

PRODUKTY

1. Udokumentowana decyzja o możliwości wdrożenia rozwiązania chmurowego (osoby umocowane zgodnie z regulaminem organizacyjnym Banku).

4. OPRACOWANIE WYMAGAŃ – OUTSOURCING NADZOROWANY

1. Na tym etapie tworzony jest zestaw wymagań biznesowych, formalnych, cyberbezpieczeństwa i innych. Wymagania są określane na podstawie wymagań wewnętrznych przepisów Banku oraz Komunikatu Chmurowego regulatora.
2. Przy tworzeniu wymagań należy uwzględnić poniższe kwestie:
   1) Czy istnieją na rynku rozwiązania chmurowe posiadające referencje w branży finansowej?
   2) Czy potencjalni oferenci mogą zapewnić CPD na terenie EOG?
   3) W przypadku, gdy Bank jest operatorem usługi kluczowej (zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa) - czy potencjalni oferenci mogą zapewnić CPD na terenie RP?
   4) Czy możliwe jest zapewnienie odpowiednich kompetencji po stronie Banku? Czy są wymagane dodatkowe szkolenia dla pracowników? Jakie są możliwości na rynku? Z jakimi kosztami należy się liczyć?
   5) Czy została potwierdzona zgodność ze standardami wewnętrznymi i przepisami (VII.4.1ppkt d)?
   6) Czy chmura będzie w stanie zapewnić wymaganą pojemność i wydajność?
   7) Zasady przekazywania informacji odnośnie zdarzeń naruszenia bezpieczeństwa informacji, rozumianego jako poufność, integralność i dostępność przetwarzanych informacji i zasobów, ze szczególnym uwzględnieniem Informacji Poufnych w rozumieniu umowy o poufności zawartej przez Strony,
   8) Zasady bezpiecznego i trwałego niszczenia danych w chmurze,
   9) Monitorowanie parametrów działania usług w chmurze, z których korzysta Bank,
   10) Zasady zakończenia współpracy z dostawcą usług w chmurze,
   11) Wykonywanie zobowiązań wynikających z Umowy, w ustalonym zakresie i terminie, z zachowaniem należytej staranności, z uwzględnieniem zawodowego charakteru prowadzonej działalności gospodarczej oraz aktualnego stanu wiedzy z dziedziny bankowości i technologii informatycznych.
3. Wymagania wynikające z Komunikatu Chmurowego są zdefiniowane w **Matrycy wymagań** będącej częścią Standardu Chmurowego.

PRODUKTY

1. Zatwierdzony dokument wymagań.

5. OPRACOWANIE I DYSTRYBUCJA ZAPYTANIA OFERTOWEGO

1. Przed uruchomieniem procesowania zapytania należy zweryfikować, czy istnieją w Banku Umowy adresujące wymagania z pkt. 4 w zakresie możliwości ich wykorzystania.
2. Na tym etapie dokument zapytania ofertowego jest opracowywany i wysyłany do dostawców usług chmurowych. Odpowiedzi na zapytanie powinny zawierać informacje o spełnieniu wymagań określonych w pkt. 4 powyżej.

PRODUKTY

1. Zapytanie ofertowe.
2. Odpowiedzi na zapytanie.

6. OCENA RYZYKA ZWIĄZANEGO Z USŁUGĄ CHMUROWĄ

1. Na podstawie odpowiedzi dostawców, w szczególności odpowiedzi na wymagania wynikające z Komunikatu Chmurowego zdefiniowane w **Matrycy wymagań**, przeprowadzana jest ocena ryzyka dla każdego z oferowanych rozwiązań. **Matryca wymagań** określa także **minimalne wymagania**, których spełnienie jest bezwzględnie wymagane, aby wdrożyć usługę chmurową. Dla pozostałych wymagań, możliwe jest zaproponowanie rozwiązań tymczasowych lub tzw. compensating controls zapewniających akceptowalny poziom ryzyka.
2. Oferty, które nie spełniają minimalnych wymagań powinny zostać odrzucone.
3. Wynik analizy ryzyka, łącznie z wymaganiami funkcjonalnymi, aspektami finansowymi etc., jest podstawą do podjęcia decyzji o wyborze dostawcy usług chmurowych dla danego przedsięwzięcia.

PRODUKTY

1. Ocena ryzyka (dla poszczególnych ofert, które nie zostały odrzucone).
2. Proponowany plan postępowania ze zidentyfikowanymi ryzykami (*compensating controls* etc.).

7. OCENA OFERT I AKCEPTACJA OFERTY

1. Na tym etapie, obok kwestii biznesowych, dokonywany jest wybór oferty oraz finalna ocena ryzyka dla wybranej oferty.
2. Dokonywane są też uzgodnienia wspólnie z Dostawcą co do środków postępowania z ryzykiem i opracowany jest finalny plan postępowania ze zidentyfikowanymi ryzykami.

PRODUKTY

1. Wybór oferty wraz z uzasadnieniem.
2. Zaktualizowana ocena ryzyka (dla wybranej oferty).
3. Uzgodniony z Dostawcą plan postępowania ze zidentyfikowanymi ryzykami.

8. PODPISANIE UMOWY

1. Podpisanie umowy zgodnej z wymaganiami Komunikatu Chmurowego. Zaadresowanie zidentyfikowanych ryzyk poprzez wprowadzenie zapisów umownych, formalnych, planów naprawczych etc.

PRODUKTY

1. Podpisana umowa (zgodnie z reprezentacją). Zalecane jest, aby decyzja o wejście w technologię chmurową była poprzedzona udokumentowaną zgodą Zarządu.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi ryzykami.

9. WDROŻENIE PRZEDPRODUKCYJNE – KONFIGURACJA USŁUGI

1. W ramach wdrożenia realizowane są kluczowe kamienie milowe wynikające z Komunikatu Chmurowego, w szczególności:
   1) dokumentacja usługi;
   2) dostosowanie procedur;
   3) pozyskanie kompetencji;
   4) opracowanie planu przetwarzania w chmurze;
   5) opracowanie planu wyjścia;
   6) modyfikacja planów BCP/DRP;
   7) wdrożenie zabezpieczeń i mechanizmów monitorowania (m.in. integracja ze SIEM etc.);
   8) testy (funkcjonalne, akceptacyjne, bezpieczeństwa, wydajnościowe, etc.).
2. Na tym etapie nie jest jeszcze dokonywana migracja danych produkcyjnych.
3. Po zakończeniu wdrożenia dokonywana jest aktualizacja statusu planów naprawczych i oceny ryzyka w celu potwierdzenia, że zidentyfikowane uprzednio ryzyka zostały zaadresowane zgodnie z założeniami.
4. Określany jest też termin migracji danych i uruchomienia produkcyjnego.

PRODUKTY

1. Dokumentacja usługi i mechanizmów kontrolnych.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi ryzykami.
3. Plan przetwarzania w chmurze.
4. Plan wyjścia z usług chmurowych.
5. Zaktualizowane plany DRP/BCP.
6. Wyniki testów i ich formalna akceptacja.
7. Plan migracji i wdrożenia produkcyjnego.
8. Zaktualizowana ocena ryzyka (aktualizacja istniejącej).
9. Dokumentacja szkoleń / pozyskania kompetencji dla użytkowników i innych kluczowych ról.

10. ZGŁOSZENIE DO KNF

1. Zgłoszenie do UKNF, zgodnie z wymaganiami Komunikatu Chmurowego.

PRODUKTY

1. Zgłoszenie do UKNF.

11. MIGRACJA DANYCH PRODUKCYJNYCH DO USŁUGI CHMUROWEJ

1. Po zgłoszeniu do UKNF możliwe jest rozpoczęcie przetwarzania danych w Usłudze Chmurowej, a zatem rozpoczęcie migracji danych produkcyjnych. Po migracji danych wymagane są testy akceptacyjne.

PRODUKTY

1. Dokumentacja migracji danych.
2. Wyniki testów potwierdzające jakość danych, zabezpieczenia szyfrujące zgodnie z Komunikatem, procedury Disaster Recovery etc.

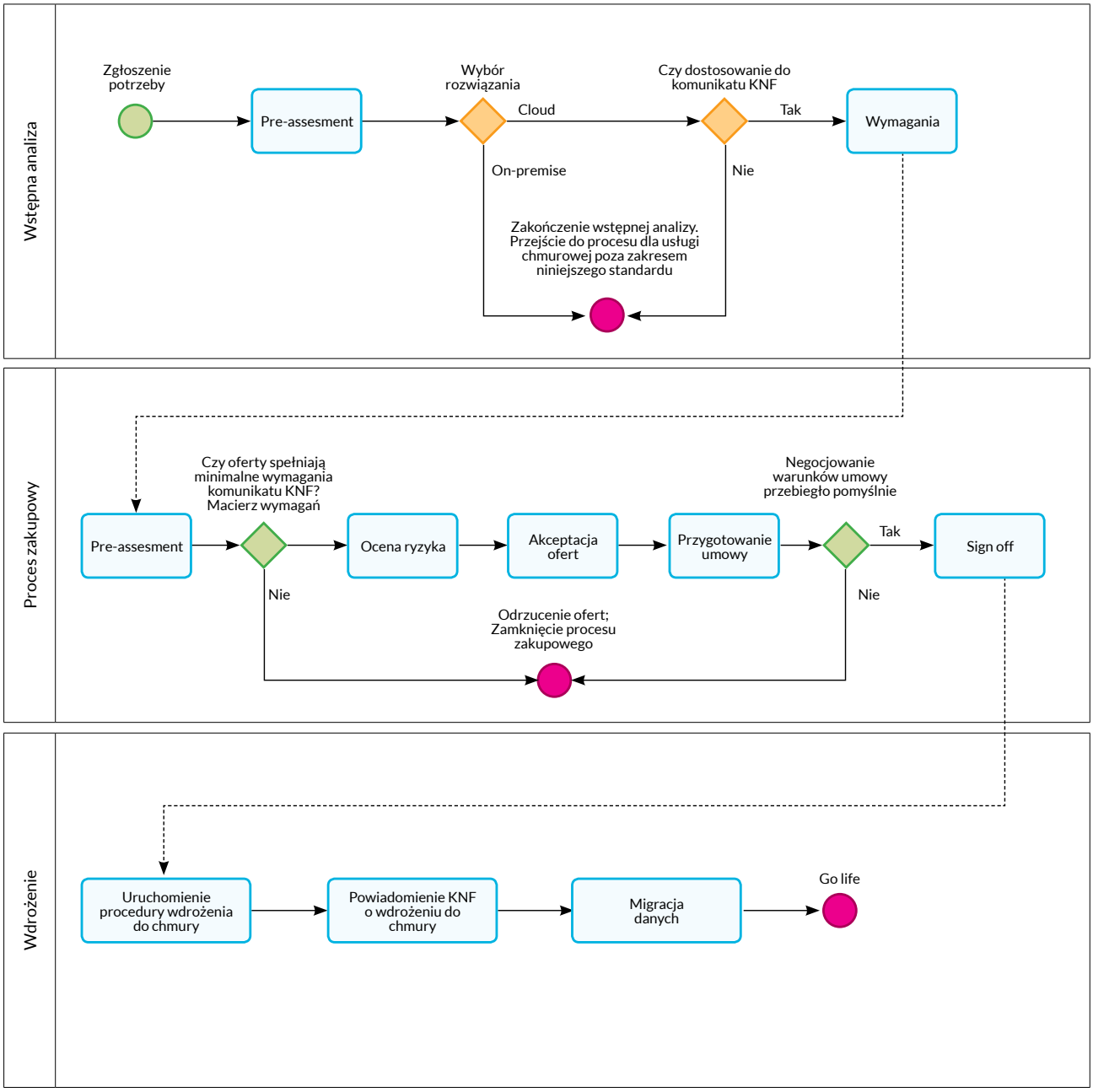
12. URUCHOMIENIE PRODUKCYJNE

1. Po zakończeniu i przetestowaniu migracji danych możliwe jest formalne uruchomienie produkcyjne, poprzedzone formalną decyzją w tym zakresie i komunikacją do użytkowników i innych interesariuszy.

PRODUKTY

1. Formalna decyzja o uruchomieniu usługi.
2. Komunikacja wewnętrzna w Banku.

SCHEMAT WDROŻENIA CHMURY



WYMAGANIA DLA DOSTAWCÓW

Index	Wymaganie	Opis wymagania	Wymagania po stronie dostawcy	Produkty (odnoszą się do wymagań po stronie dostawcy)
V.1-5	Wytyczne do klasyfikacji i oceny informacji	Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację i ocenę informacji pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej	1. Dostawca powinien określić lokalizacje CPD, w których przetwarzane są informacje Banku (kraj, region) 2. Wszelkie zmiany obszaru przetwarzania danych wymagają uprzedniej zgody Banku	1. Dokumentacja w zakresie lokalizacji CPD oraz obszaru przetwarzania danych (informacje o tym, jakie usługi świadczone są w poszczególnych lokalizacjach) 2. Proces informowania o zmianie obszaru przetwarzania danych
VI.1-6	Wytyczne do szacowania ryzyka	Podmiot nadzorowany przeprowadza w udokumentowanym procesie kompleksowe szacowanie ryzyka	Dostawca powinien dostarczyć Bankowi poniższe informacje: 1. Informacje o rozproszeniu geograficznym przetwarzanych informacji 2. Informacje o zasadach dostępu do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmurowych 3. Dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się przetwarzanie, w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu 4.Informacje o mechanizmach izolacji zasobów używanych do świadczenia usług chmury obliczeniowej, w tym informacje o incydentach bezpieczeństwa związanych z naruszeniem mechanizmów izolacji 5. Informacje o możliwości migracji usługi/danych do innych dostawców chmurowych w celu mitygacji przywiązania do jednego dostawcy usług chmury obliczeniowej 6. Informacje o interfejsach zarządzających usługami, które są udostępniane przez dostawców usług chmurowych i ich podatnościach	1. Patrz V.1-5. 2. Patrz VII.3.2. 3. Opinie prawne w zakresie możliwości pozaumownego dostępu do przetwarzanych informacji, gwarantowanego przez jurysdykcję kraju, w którym odbywa się przetwarzanie danych; 4. Patrz VII.3.2. 5. Patrz VII.3.2. 6. Patrz VII.3.2. 7. Zasady żądania i wprowadzania żądanych zmian 8. Zasady kontroli dostawcy, w szczególności: a) zasady dostępu do dokumentacji certyfikacyjnej b) zasady dostępu do wyników audytów i testów bezpieczeństwa c) zasady prowadzenia kontroli pośredniej i bezpośredniej 9. Docelowe SLA oraz zasady nadzoru nad jakością świadczonych usług 10. Patrz VII.3.2. 11. Mechanizmy kontroli użytkowników i urządzeń przy dostępie do usługi chmurowej 12. Zasady zmiany warunków usługi 13. Lista poddostawców wraz z zakresem świadczonych przez nich zadań i inf. o dostępie do danych Banku

			8. Informacje o możliwości kontrolowania dostawcy usług chmury obliczeniowej oraz jego podwykonawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej 9. Informacje o możliwości kontrolowania jakości usług chmury obliczeniowej 10. Informacje o podziale odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym 11. Możliwości kontroli dostępu i urządzeń dostępowych użytkowników końcowych 12. Zasady zmiany warunków umowy 13. Informacje o wykorzystywanych poddostawcach i zakresu świadczonych przez nich usług oraz informacja o ich dostępie do danych	
VII.3.1	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Zapewnienie kompetencji	1. Określenie wymaganych kompetencji przy korzystaniu z usługi, określenie ścieżek szkoleniowych i certyfikacyjnych	1. Lista wymaganych i zalecanych szkoleń / certyfikatów przy korzystaniu z usługi dla poszczególnych ról oraz lista rekomendowanych przez dostawcę ról wynikająca z podziału odpowiedzialności pomiędzy bankiem a dostawcą
VII.3.2	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Podział obowiązków i konsekwencje stosowania	1. Jasne określenie podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji przy korzystaniu z usługi. 2. Umożliwienie Bankowi zrozumienia konsekwencji stosowania określonej architektury środowiska chmury obliczeniowej oraz zasad jej konfiguracji	1. Dokumentacja określająca podział odpowiedzialności za bezpieczeństwo informacji pomiędzy Bankiem a dostawcą usług 2. Dokumentacja określająca zasady konfiguracji usługi. 2.1. Architektura usługi 2.2. Dokumentacja kluczowych kwestii bezpieczeństwa usługi, w szczególności: a) opis i zakres przetwarzanych informacji oraz informacja, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji b) sposób szyfrowania informacji oraz miejsce i/lub sposób przechowywania kluczy szyfrujących, zarówno at rest, jak i in transit

				c) potwierdzenie, że używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane d) informacja o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany e) dokumentacja dedykowanych i/lub zalecanych przez dostawcę ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług, w szczególności w zakresie szyfrowania przetwarzanych informacji f) szczegółowe i aktualne instrukcje konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji g) opis mechanizmów logowania oraz możliwość przekazywania logów do SIEM po stronie Banku h) informacje o mechanizmach izolacji zasobów używanych do świadczenia usług chmury obliczeniowej i) dokumentacja wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji j) informacje o interfejsach zarządzających usługami, które są udostępniane przez dostawców usług chmurowych i ich podatnościach (wyniki badania podatności lub testów bezpieczeństwa) k) dokumentacja potwierdzająca natywne uruchamianie nowego środowiska i/lub usługi separowanego od innych tematów, z ustawieniami „secure-by-default” 2.3. Opis mechanizmów dostępu zdalnego dostawcy uwzględniający poniższe wymagania: a) uwierzytelnienie dwuskładnikowe przy dostępie zdalnym do środowiska chmurowego

				b) możliwość dostępu zdalnego z bezpiecznych lokalizacji sieciowych c) możliwość nagrywania sesji administracyjnych oraz wgląd przez personel Banku w nagrania sesji
VII.4	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Umowa z dostawcą usług chmury obliczeniowej	1. Podpisanie umowy outsourcingu zgodnie z Prawem Bankowym 2. Zawarcie w umowie wymagań określonych w pkt VII.4.1 komunikatu chmurowego 3. Informacja o prawie właściwym dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów)	1-2. Potwierdzenie zgody na zawarcie umowy zgodnej z **załączonymi klauzulami umownymi** 3. Informacja o prawie właściwym dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów) 3.1 W przypadku poddania umowy prawu państwa trzeciego analiza prawna dotycząca możliwości skutecznego wykonywania postanowień umowy, wszystkich wymagań prawa polskiego ciążących na Banku oraz wytycznych organu nadzoru w zakresie komunikatu
VII.5	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Plan przetwarzania informacji w chmurze obliczeniowej (5.1)	1. Informacje o architekturze i konfiguracji usługi stanowiące wkład do opracowania planu przetwarzania informacji w chmurze obliczeniowej	Patrz VII.3.2.
VII.6.1-2,5	Wymagania dla dostawców usług chmury obliczeniowej	Zgodność dostawcy z normami	W zakresie świadczonych usług dostawca usług chmury obliczeniowej spełnia łącznie wymagania zapewnienia zgodności swojego działania z normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części. 1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT 2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji 3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania 4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej 5. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej	Dokumentacja potwierdzająca zgodność z normami (o ile dotyczy): 1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT 2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji 3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania 4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej 5. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej 6. PN-EN 50600 minimum klasy 3 lub ANSI/TIA-942 minimum Tier III. Dopuszczalne dokumenty: - Certyfikaty potwierdzające zgodność z normami - Oświadczenie dostawcy o spełnieniu wymogów norm

			6. CPD dostawcy usług chmury obliczeniowej spełnia wymagania normy PN-EN 50600 minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i powszechnie uznanego do oceny CPD, przy czym Bank może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań	
VII.6.3	Wymagania dla dostawców usług chmury obliczeniowej	Lokalizacja CPD	1. Zaleca się, aby CPD było zlokalizowane na terenie EOG (o ile jest to uzasadnione z perspektywy kosztowej, jakościowej, ryzyka etc.) 2. Banki będące operatorami usługi kluczowej powinny preferować CPD w Polsce	1. Patrz V.1-4
VII.6.4	Wymagania dla dostawców usług chmury obliczeniowej	Ochrona informacji i kontrola dostępu	Wymagania w zakresie ochrony informacji: 1. Domyślna zasada braku dostępu do przetwarzanych informacji podmiotu nadzorowanego 2. Brak konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego i/lub w innych uruchamianych usługach 3. Zasada „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji 4. Udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji	Potwierdzenie spełnienia wymagań w zakresie ochrony informacji poprzez opis mechanizmów lub wskazanie zapisów umownych/ proceduralnych zapewniających poniższą funkcjonalność: 1. Domyślna zasada braku dostępu do przetwarzanych informacji przez dostawcę 2. Brak konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego i/lub w innych uruchamianych usługach 3. Realizacja zasady „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany oraz na czas ich trwania, logowanie zdarzeń, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. OPCJONALNIE: Stosowny certyfikat (np. SOC 2 Type 2) wydany przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji dla mechanizmu kontroli dostępu serwisowego

			5. Natywne uruchamianie nowego środowiska i/lub usługi separowanego od innych tematów, z ustawieniami „secure-by-default”	
VII.7	Wymagania dla dostawców usług chmury obliczeniowej	Kryptografia	Informacje w chmurze obliczeniowej muszą być szyfrowane. Wymagania: 1. Dostarczenie szczegółowych i aktualnych instrukcji konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji 2. Używanie dedykowanych i/lub zalecanych przez dostawcę ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług, w szczególności w zakresie szyfrowania przetwarzanych informacji 3. Szyfrowanie zarówno „at rest”, jak i „in transit” informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej 4. Informacje są szyfrowane kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany 5. Używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane 6. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmurowych, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS 140-2 Level 2 lub równoważne 7. Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby	1-3 Patrz VII.3.2. 4. Możliwość szyfrowania kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany, opis techniczny rozwiązania 5. Patrz VII.3.2. 6. Możliwość wykorzystania własnego HSM lub HSM od dostawcy - opis techniczny rozwiązania; potwierdzenie dostawcy, że HSM spełnia wymagania FIPS 140-2 Level 2 lub równoważne 7. W przypadku, gdy klucze zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej, możliwość przechowywania w ramach własnej infrastruktury kopii kluczy szyfrujących Banku

VII.8	Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej	Logowanie zdarzeń	Dostawca zapewnia mechanizmy logowania zdarzeń oraz dostęp Banku do logów: 1. Logi mogą być przekazywane do Banku, w szczególności do SIEM. 2. Logi są zabezpieczone przez przed nieautoryzowanym dostępem, modyfikacją lub usunięciem.	Patrz VII.3.2.
VII.8.4	Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej	Dostęp zdalny do środowiska chmurowego	Dostęp zdalny do środowiska chmurowego: 1. Jest możliwy tylko dla uprawnionego personelu dostawcy 2. Wymaga stosowania MFA. 3. Jest inicjowany z określonych, bezpiecznych lokalizacji sieciowych 4. Jest realizowany pod nadzorem Banku (np. poprzez nagrywanie sesji)	Patrz VII.3.2.

Związek Banków Polskich
Kruczkowskiego 8
00-380 Warszawa
www.zbp.pl