# PRZYKŁADOWE Kroki wdrożenia usługi przetwarzania INFORMACJI w chmurze obliczeniowej PUBLICZNEJ LUB HYBRYDOWEJ w ZAKŁADZIE UBEZPIECZEŃ

## Wstęp

## Niniejszy dokument opisuje przykładowe kroki wdrożenia usługi przetwarzania informacji w Chmurze obliczeniowej, przy założeniu, że Komunikat ma zastosowanie. Opisane w dokumencie kroki mogą mieć częściowe zastosowanie w zależności od procesu oraz Modelu usługi chmury obliczeniowej. Proces wdrożenia w przypadku, gdy Komunikat nie ma zastosowania jest poza zakresem niniejszego dokumentu.Zidentyfikowanie potrzeby biznesowej

1. Na tym etapie identyfikowana i dokumentowana jest potrzeba biznesowa, zgodnie z procesami obowiązującymi w Zakładzie Ubezpieczeń.
2. Otwierany jest projekt,, uruchamiany proces zarządzania zmianą lub inna inicjatywa, która pozwala na przypisanie prac i zadań związanych z krokami opisanymi poniżej.
3. Jednostki odpowiedzialne za architekturę, technologię oraz bezpieczeństwo określają zasadność dalszej analizy niniejszej potrzeby pod kątem możliwości realizacji usługi w Chmurze obliczeniowej.

### Produkty

1. Opis wymagań biznesowych.
2. Wniosek lub zgłoszenie otwierające projekt, zmianę lub inną inicjatywę.

## Wstępna ocena pod kątem możliwości realizacji potrzeby w usłudze chmurY OBLICZENIowej

1. Na tym etapie dokonywana jest wstępna ocena („pre-assessment”) potrzeby pod kątem realizacji usługi w Chmurze obliczeniowej, tj.:
   1. Porównanie rozwiązań w Usłudze chmury obliczeniowej vs. on-premise – wstępna ocena realizacji wymagań i kosztów, w tym analiza potencjalnych Dostawców usług chmury obliczeniowej;
   2. Architektura, integracja, docelowa konfiguracja – zgodność z docelową architekturą Zakładu Ubezpieczeń;
   3. Wstępne PoC rozwiązania, jeśli planowane jest wykorzystanie całkowicie nowych dla Zakładu Ubezpieczeń technologii;
   4. Inwentaryzacja i klasyfikacja informacji, klasyfikacja istotności Usługi chmury obliczeniowej - w zależności od wyników podejmowana jest wstępna decyzja pod kątem zastosowania Komunikatu;
   5. Zbadanie możliwości pozyskania kompetencji dla Usługi chmury obliczenioowej i on-premise;
   6. Zgodność ze strategią Zakładu Ubezpieczeń;
   7. Zgodność z regulacjami wewnętrznymi.

### Produkty

1. Wstępna analiza wykonalności pod kątem Usługi chmury obliczeniowej vs. on-premise.

## Punkt decyzyjny LUB decyzja o dopuszczalności wdrożenia USŁUGI CHMURY OBLICZENIOWEJ

1. Na tym etapie podejmowana jest decyzja o dalszym procesowaniu potrzeby, która zakłada poniższe scenariusze:
   1. Brak możliwości lub uzasadnienia do wykorzystania Usługi chmury obliczeniowej;
   2. Dopuszczalne wdrożenie Usługi chmury obliczeniowej – z zastrzeżeniem spełnienia wymagań Komunikatu, w przypadku gdy ma on zastosowanie;
   3. Dopuszczalne wdrożenie Usługi chmury obliczeniowej – w przypadku, gdy Komunikat nie ma zastosowania.
2. Dalsze kroki będą opisywane tylko dla **scenariusza 2**.

### Produkty

1. Udokumentowana decyzja o możliwości wdrożenia Usługi chmury obliczeniowej (osoby umocowane zgodnie z regulacjami wewnętrznymi Zakładu Ubezpieczeń).

## Opracowanie wymagań do wdrożenia usługi chmury obliczeniowej zgodnie z komunikatem

1. Na tym etapie tworzony jest zestaw wymagań biznesowych, formalnych, bezpieczeństwa lub innych. Wymagania są określane na podstawie wymagań wewnętrznych regulacji Zakładu Ubezpieczeń oraz Komunikatu.
2. Przy tworzeniu wymagań można uwzględnić poniższe kwestie:
   1. Czy istnieją na rynku Usługi chmury obliczeniowej posiadające referencje w branży finansowej, w szczególności ubezpieczeniowej?
   2. Czy potencjalni oferenci mogą zapewnić CPD na terenie EOG?
   3. Czy możliwe jest zapewnienie odpowiednich kompetencji po stronie Zakładu Ubezpieczeń? Czy są wymagane dodatkowe szkolenia dla pracowników? Jakie są możliwości na rynku? Z jakimi kosztami należy się liczyć?
   4. Czy Dostawca usług chmury obliczeniowej potwierdza zgodność przetwarzania danych osobowych ze standardami wewnętrznymi Zakładu Ubezpieczeń i powszechnie obowiązującymi przepisami prawa?
   5. Czy Chmura obliczeniowa będzie w stanie zapewnić wymaganą pojemność i wydajność?
   6. Zasady przekazywania informacji odnośnie zdarzeń naruszenia bezpieczeństwa informacji, rozumianego jako poufność, integralność i dostępność przetwarzanych informacji i zasobów, ze szczególnym uwzględnieniem Informacji prawnie chronionych.
   7. Zasady bezpiecznego i trwałego niszczenia informacji w Chmurze obliczeniowej.
   8. Monitorowanie parametrów działania Usług chmury obliczeniowej, z których miałby korzystać Zakład Ubezpieczeń.
   9. Zasady zakończenia współpracy z Dostawcą usług chmury obliczeniowej.
   10. 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 ubezpieczeń i technologii informatycznych.
3. Wymagania wynikające z Komunikatu względem Dostawcy usług chmury obliczeniowej zostały wskazane w **Zestawieniu wymagań** (Wymagania (produkty) do opracowania po stronie Dostawcy usługi chmury obliczeniowej), będących częścią **Standardu**.

### Produkty

1. Udokumentowane wymagania do Usługi chmury obliczeniowej.

## Opracowanie i dystrybucja zapytania ofertowego

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

### Produkty

1. Zapytanie ofertowe.
2. Odpowiedzi na zapytanie.

## Ocena ryzyka związanego usługą chmurową

1. Na podstawie odpowiedzi Dostawców usług chmury obliczeniowej, w szczególności odpowiedzi na wymagania wynikające z Komunikatu wskazane w **Zestawieniu wymagań**, przeprowadzana jest ocena ryzyka dla oferowanych Usług chmury obliczeniowej. **Zestawienie wymagań** określa **minimalne wymagania**, których spełnienie powinno być wymagane do wdrożenia Usługi chmury obliczeniowej. Dla pozostałych wymagań, możliwe jest zaproponowanie rozwiązań tymczasowych lub mechanizmów kontrolnych 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 chmury obliczeniowej dla danego przedsięwzięcia.

### Produkty

1. Wstępna ocena ryzyka (dla ofert, które nie zostały odrzucone).
2. Proponowany plan postępowania ze zidentyfikowanymi rodzajami ryzyka.

## 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 usług chmury obliczeniowej co do środków postepowania z ryzykiem i opracowywany 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 usług chmury obliczeniowej plan postępowania ze zidentyfikowanymi ryzykami.

## Podpisanie umowy

1. Podpisanie umowy zgodnej z wymaganiami Komunikatu. Zaadresowanie zidentyfikowanych rodzajów ryzyka poprzez wprowadzenie postanowień umownych, planów naprawczych, etc.

### Produkty

1. Podpisana umowa.Zalecane jest, aby decyzja o wejściu w technologię Chmury obliczeniowej była poprzedzona udokumentowaną zgodą Zarządu Zakładu Ubezpieczeń.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi rodzajami ryzyka.

## Wdrożenie przedprodukcyjne – konfiguracja usługi

1. W ramach wdrożenia realizowane są kluczowe kamienie milowe wynikające z Komunikatu, w szczególności:
   1. dokumentacja Usługi chmury obliczeniowej;
   2. dostosowanie procedur wewnętrznych Zakładu Ubezpieczeń;
   3. pozyskanie kompetencji;
   4. opracowanie planu przetwarzania informacji w Chmurze obliczeniowej;
   5. opracowanie planu wyjścia;
   6. opracowanie planu ciągłości działania (BCP) lub modyfikacja istniejącego;
   7. wdrożenie zabezpieczeń i mechanizmów monitorowania (np. 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 rodzaje ryzyka zostały zaadresowane zgodnie z założeniami.
4. Określany jest też termin migracji danych i uruchomienia produkcyjnego.

### Produkty

1. Dokumentacja Usługi chmury obliczeniowej i mechanizmów kontrolnych.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi ryzykami.
3. Plan przetwarzania informacji w Chmurze obliczeniowej.
4. Plan wyjścia z Usług chmury obliczeniowej.
5. Zaktualizowane plany BCP.
6. Wyniki testów i ich akceptacja.
7. Plan migracji i wdrożenia produkcyjnego.
8. Zaktualizowana ocena ryzyka (aktualizacja istniejącej), jeżeli ma zastosowanie.
9. Dokumentacja szkoleń lub pozyskania kompetencji dla użytkowników końcowych i innych kluczowych ról.

## Informowanie uKNF

1. Poinformowanie UKNF, zgodnie z wymaganiami Komunikatu.

### Produkty

1. Uzupełniony formularz stanowiący Załącznik nr 1 do Komunikatu.

## Migracja danych produkcyjnych do Usługi Chmury obliczeniowej

1. Po poinformowaniu UKNF oraz upływie wymaganego przepisami prawa lub postanowieniami Komunikatu terminu, możliwe jest rozpoczęcie przetwarzania informacji w Usłudze chmury obliczeniowej, w tym rozpoczęcie migracji danych produkcyjnych. Po migracji danych powinny być przeprowadzone testy akceptacyjne.

### Produkty

1. Dokumentacja migracji danych.
2. Wyniki testów potwierdzające jakość danych, zabezpieczenia szyfrujące zgodnie z Komunikatem, procedury Disaster Recovery lub inne zabezpieczenia zgodnie z Komunikatem i regulacjami wewnętrznymi Zakładu Ubezpieczeń.

## Uruchomienie produkcyjne

1. Po zakończeniu i przetestowaniu migracji danych możliwe jest formalne uruchomienie produkcyjne, poprzedzone udokumentowaną decyzją i komunikacją do użytkowników końcowych lub innych interesariuszy, zgodnie z regulacjami wewnętrznymi Zakładu Ubezpieczeń.

### Produkty

1. Udokumentowana decyzja o uruchomieniu usługi zgodnie z regulacjami wewnętrznymi Zakładu Ubezpieczeń.
2. Komunikacja wewnętrzna w Zakładzie Ubezpieczeń.