Związek Banków Polskich

Polish Cloud

STANDARD POLISHCLOUD 3.0

Standard wdrożenia i utrzymania usługi chmury obliczeniowej

STANDARD POLISHCLOUD 3.0

Standard wdrożenia i utrzymania usługi chmury obliczeniowej

Związek Banków Polskich

RBE | Rada Bankowości Elektronicznej

Banki w Polsce

FTB Forum Technologii Bankowych

accenture

Osborne Clarke

Spis treści

CZĘŚĆ I

WPROWADZENIE 7

1. ORGANIZACJA DOKUMENTU 7
2. STOSOWANIE STANDARDU 8
3. WSPÓŁPRACA 8

CZĘŚĆ II

KONTEKST REGULACYJNY 9

1. WYMAGANIA PRAWNE DLA USŁUG CHMURY OBLICZENIOWEJ – WPROWADZENIE 9
2. ZAKRES PRZEDMIOTOWY STANDARDU 13
3. CHMURA W KONTEKŚCIE DORA 14
4. CHMURA W KONTEKŚCIE OUTSOURCINGU BANKOWEGO 17
5. CHMURA W UMOWACH NIE-ICT 20

CZĘŚĆ III

ZARZĄDZANIE RYZYKIEM ICT USŁUG CHMURY OBLICZENIOWEJ 23

1. ZARZĄDZANIE OBSZAREM CHMURY OBLICZENIOWEJ (GOVERNANCE CHMURY) 23
2. ZARZĄDZANIE RYZYKIEM ZEWNĘTRZNEGO DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ 24

CZĘŚĆ IV

ANALIZY PRZEDUMOWNE 26

1. EX-ANTE RISK ASSESSMENT – PROFILOWANIE DOSTAWCY USŁUG ORAZ USŁUG CHMURY OBLICZENIOWEJ 26
2. OCENA DUE DILIGENCE – OCENA ODPOWIEDNIOŚCI DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ 27
3. SZACOWANIE RYZYKA USŁUGI CHMURY OBLICZENIOWEJ 28
4. PLAN AUDYTU 30
5. WYMOGI DLA UMOWY 31
6. ZAWIADOMIENIE ORGANU NADZORU (NOTYFIKACJA) 32
7. WYMOGI DLA DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ 32
8. DODATKOWE WYMAGANIA DLA DOSTAWCY ROZWIĄZANIA ICT W ŚRODOWISKACH CHMUROWYCH ZARZĄDZANYCH PRZEZ BANK 36
9. STRATEGIA WYJŚCIA 37

CZĘŚĆ V

WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI W CHMURZE 40

1. WPROWADZENIE 40
2. ZARZĄDZANIE BEZPIECZEŃSTWEM USŁUG CHMURY OBLICZENIOWEJ 40

CZĘŚĆ VI

ZARZĄDZANIE CHMURĄ PO ZAWARCIU UMOWY 48

1. POLITYKA, ZARZĄDZANIE I UTRZYMANIE ŚRODOWISK CHMUROWYCH 48
2. MONITORING WYDAJNOŚCI I DOSTĘPNOŚCI USŁUG 50
3. ZARZĄDZANIE INCYDENTAMI 51
4. ZARZĄDZANIE ZMIANĄ I KONFIGURACJĄ ŚRODOWISK CHMUROWYCH 53
5. PROCESY DEVOPS 55
6. ZARZĄDZANIE DANYMI I CIĄGŁOŚĆ DZIAŁANIA (BCP/DR) 56
7. ZARZĄDZANIE KOSZTAMI CHMUROWYMI (FINOPS) 58
8. VENDOR MANAGEMENT (RYZYKO KONCENTRACJI, MONITOROWANIE, AUDYT) 61
9. AUDYTOWANIE DOSTAWCY USŁUGI W CHMURZE 62

CZĘŚĆ VII

ZAŁĄCZNIKI 66

ZAŁĄCZNIK NR 1
DEFINICJE 67

ZAŁĄCZNIK NR 2
SCHEMAT PODSTAWOWYCH ZAGADNIEŃ REGULACYJNYCH 77

ZAŁĄCZNIK NR 3
WYMAGANIA KONTRAKTOWE 78

ZAŁĄCZNIK NR 4
NOTYFIKACJA UMÓW NA USŁUGI W CHMURZE 84

ZAŁĄCZNIK NR 5
FINOPS – FAZY, UPRAWNIENIA I SZKOLENIA 86

ZAŁĄCZNIK NR 6
PODSTAWOWY ZBIÓR INFORMACJI NA POTRZEBY REALIZACJI PLANU WYJŚCIA Z USŁUGI CHMUROWEJ 88

ZAŁĄCZNIK NR 7
OBSZARY DO ANALIZY PRZEZ BANK W ZAKRESIE VENDOR MANAGEMENTU 92

ZAŁĄCZNIK NR 8
WYTYCZNE DLA DOSTAWCÓW USŁUG CHMUROWYCH 95

ZAŁĄCZNIK NR 9
SZABLON ANALIZY DD/ ANALIZY RYZYKA (EDYTOWALNY) 98

AUTORZY STANDARDU

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.

Koordynator projektu ze strony Związku Banków Polskich

Bartłomiej Nocoń
Katarzyna Zygierewicz

Koordynatorzy

Główny koordynator:
Maciej Leśniewski, **Crédit Agricole Bank Polska SA**

Koordynator Strumienia prawnego:
Szymon Ciach, **Osborne Clarke**

Koordynator Strumienia cyberodporności:
Marek Dryjański, **Citi Handlowy**

Koordynator Strumienia governance:
Marcin Kraśniewski, **Velo Bank SA**

Project Management:
Piotr Topór, **Accenture**

Zespół redakcyjny

Agnieszka Suchańska, **ING Bank Śląski SA**
Aleksandra Gajda, **Osborne Clarke**
Anna Szczurek, **ING Bank Śląski SA**
Arkadiusz Kawulski, **Velo Bank SA**
Artur Rudziński, **Alior Bank SA**
Bartosz Stachowiak, **mBank SA**
Ilona Jaworska, **Bank Polskiej Spółdzielczości SA**
Jacek Juriewicz, **ING Bank Śląski SA**
Jakub Wójcicki, **PKO Bank Polski SA**
Janusz Szczudło, **PKO Bank Polski SA**
Kamil Atłas, **Velo Bank SA**
Kamil Prokopowicz, **Osborne Clarke**
Konrad Wąs, **PKO Bank Polski SA**
Krzysztof Czajkowski, **Bank Pekao SA**
Krzysztof Trela, **Bank Ochrony Środowiska SA**
Magdalena Mentel – Rogowska, **Bank Millennium SA**
Marek Kowalski, **BNP Paribas Bank Polska S.A.**
Mikołaj Drabik, **mBank SA**
Monika Hałasa-Mochocka, **Citi Handlowy**
Monika Szymaniuk – Nosowska, **Bank Pekao SA**
Norbert Lutowski, **Osborne Clarke**
Olga Cabak, **Osborne Clarke**
Piotr Bukowski, **Bank Pekao SA**
Piotr Topór, **Accenture**
Robert Smoliński, **mBank SA**
Sylwia Mackiewicz, **BPS**

Partnerzy merytoryczni

Osborne Clarke
Accenture

Instytucje zaangażowane

Banki:
Alior Bank SA
Bank Gospodarstwa Krajowego
Bank Millennium SA
Bank Nowy
Bank Ochrony Środowiska SA
Bank Pekao SA
Bank Polskiej Spółdzielczości SA
BNP Paribas Bank Polska SA
Citi Handlowy
Crédit Agricole Bank Polska SA
ING Bank Śląski SA
mBank SA
PKO Bank Polski SA
Santander Bank Polska SA
SGB Bank SA
System Ochrony Zrzeszenia BPS
Velo Bank
Firmy technologiczne:
Amazon Web Services
Asseco Cloud
Comarch
Google
IBM

Warszawa, 13 listopada 2025 r.

Szanowni Państwo,

w imieniu Związku Banków Polskich mamy ogromną przyjemność oddać w Państwa ręce Standard PolishCloud 3.0.

Dokument ten powstał z inicjatywy polskiego sektora bankowego i został przygotowany w ramach współpracy przedstawicieli Rady Bankowości Elektronicznej, Forum Technologii Bankowych, kancelarii Osborne Clarke oraz firmy Accenture.

Standard PolishCloud 3.0 jest odpowiedzią społeczności zgromadzonych wokół Związku Banków Polskich na zmiany, jakie zachodzą w środowisku regulacyjnym i technologiczno-organizacyjnym banków. Były one związane w szczególności z wejściem w życie przepisów Rozporządzenia DORA, AI Act i wycofaniem Komunikatu chmurowego z 2020 r. oraz Rekomendacji D przez organ nadzoru.

Standard PolishCloud 3.0 zawiera rekomendacje w zakresie zastosowania technologii chmury obliczeniowej w sektorze bankowym zgodne z obowiązującymi wymogami krajowymi i międzynarodowymi. Dokument ten określa zadania, procedury, procesy i analizy, jakie Bank powinien przeprowadzić i udokumentować pod kątem funkcjonowania organizacji w sferze usług chmurowych, w szczególności w odniesieniu do bieżącego otoczenia regulacyjnego.

Mając na uwadze, że znacząca część instytucji finansowych ma już za sobą adopcję chmury obliczeniowej, większego znaczenia w porównaniu z wcześniejszą wersją – Standardu PolishCloud 2.0 – nabrały wyzwania związane z budową i zarządzaniem środowiskami chmurowymi. Autorzy dokumentu położyli duży nacisk na kwestie dotyczące tzw. rozwiązań multi-cloud oraz ryzyka koncentracji. Równocześnie niezwykle istotne było zaadresowanie aspektów bezpieczeństwa danych, zapewnienia ciągłości działania i wzmocnienia cyberodporności polskiego sektora bankowego w kontekście zmiennej sytuacji na arenie geopolitycznej. W dokumencie wskazano również wyzwania związane z coraz bardziej powszechnym wykorzystaniem technologii sztucznej inteligencji w aspektach chmury obliczeniowej.

Standard PolishCloud 3.0 stanowi przykład wyjątkowej i unikalnej na skalę międzynarodową współpracy. To efekt wzajemnej wymiany doświadczeń wybitnych ekspertów sektora bankowego, firm technologicznych, doradców prawnych i strategicznych w ramach jednego, wspólnego celu: efektywnego, zgodnego z najnowszymi wymogami regulacyjnymi, a przede wszystkim bezpiecznego zarówno dla tych podmiotów, jak i ich klientów, korzystania z możliwości, jakie daje chmura obliczeniowa.

Serdecznie zachęcamy do zapoznania się z zawartością dokumentu Standard PolishCloud 3.0.

Z wyrazami szacunku

Bartłomiej Nocoń
Dyrektor
Związku Banków Polskich

Katarzyna Zygierewicz
Doradca Zarządu
Związek Banków Polskich

CZĘŚĆ I

WPROWADZENIE

1. ORGANIZACJA DOKUMENTU

1.1 Standard został podzielony na rozdziały poświęcone poszczególnym zagadnieniom w zakresie wdrażania usług chmury obliczeniowej w sektorze bankowym, z uwzględnieniem tzw. cyklu życia usługi chmury obliczeniowej. Jest to podyktowane faktem, że zasadnicza część regulacji w zakresie usług chmury obliczeniowej dotyczy kontekstu nabywania tych usług od zewnętrznych dostawców. Dlatego skoncentrowaliśmy się zasadniczo na usługach chmury obliczeniowej w kontekście ram zarządzania ryzykiem zewnętrznego dostawcy Usług ICT, co przejawia się w omówieniu poszczególnych obowiązków, jakie musi realizować Bank, aby takim ryzykiem zarządzać zgodnie z wymaganiami prawnymi.

1.2 W ramach CZĘŚCI II: KONTEKST REGULACYJNY omawiamy najważniejsze wymogi prawno-regulacyjne mające zastosowanie do usług chmury obliczeniowej, takie jak wymogi rozporządzenia DORA oraz outsourcingu regulowanego. Znajdą tam Państwo komentarz do wybranych przepisów oraz wprowadzenie do pogłębionej analizy kluczowych praktycznych zagadnień, takich jak notyfikacja do organu nadzoru.

1.3 W CZĘŚCI III: ZARZĄDZANIE RYZYKIEM ICT USŁUG CHMURY OBLICZENIOWEJ zawarte jest wprowadzenie do tego zagadnienia, ze szczególnym uwzględnieniem kwestii zarządzania ryzykiem zewnętrznego dostawcy. Zawarta tam treść porządkuje tematykę, która szczegółowo omówiona zostanie w kolejnych częściach.

1.4 CZĘŚĆ IV: ANALIZY PRZEDUMOWNE stanowi zbiór rekomendacji odnoszących się do analiz i dokumentów, jakie Bank musi sporządzić, realizując odpowiednie wymogi prawne. Z uwagi na szeroki kontekst regulacyjny odstąpiono od omawiania poszczególnych wymogów prawnych na rzecz merytorycznego komentarza do zagadnień praktycznych dotyczących poszczególnych analiz i dokumentów.

1.5 CZĘŚĆ V: WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI W CHMURZE obejmuje szereg aspektów, które są rekomendowane do uwzględnienia w ramach procesów związanych z bezpieczeństwem i zarządzaniem chmurą obliczeniową.

1.6 W CZĘŚCI VI: ZARZĄDZANIE CHMURĄ PO ZAWARCIU UMOWY omówiono zarówno wymagane regulacyjnie działania, jakie Bank musi realizować na etapie korzystania z usług chmury obliczeniowej, jak i działania rekomendowane do wykonania w ramach najlepszych praktyk zarządzania chmurą obliczeniową.

1.7 W ostatniej części zawarte są załączniki, które obejmują m.in. wzory dokumentów takich jak np. analiza ryzyka. Standard publikowany jest w formacie PDF, a Załącznik nr 9 w formie edytowalnej został zaimplementowany w tym pliku. Jego otwarcie jest możliwe przy pomocy standardowego oprogramowania do odczytu plików PDF, np. po kliknięciu w ikonę załącznika i otworzeniu widocznego tam pliku. Zaprezentowane w Standardzie szablony mają charakter przykładowy i powinny być dostosowane przez Bank do wewnętrznych potrzeb i wymagań.

2. STOSOWANIE STANDARDU

2.1 Standard może być wykorzystany jako przykładowy model postępowania (ang. *framework*) przez podmioty sektora bankowego we wdrożeniach chmurowych, natomiast jego stosowanie każdorazowo powinno uwzględniać specyfikę działalności danego podmiotu nadzorowanego.

2.2 Standard może być również wykorzystywany przez inne podmioty niż podmioty sektora bankowego, jednak w takiej sytuacji powinny one uwzględnić, że część zagadnień, zwłaszcza ściśle związanych z kwestiami prawnymi, jest specyficzna wyłącznie dla sektora bankowego.

3. WSPÓŁPRACA

3.1 Związek Banków Polskich (ZBP) zachęca podmioty korzystające ze Standardu (nie tylko podmioty nadzorowane) do dzielenia się swoimi spostrzeżeniami w zakresie jego stosowania poprzez kontakt mailowy: PolishCloud@zbp.pl.

3.2 Opinie użytkowników pozwolą aktualizować Standard i dalej dostosowywać go do praktyki rynkowej, a także kierować pytania do Urzędu Komisji Nadzoru Finansowego (UKNF) w celu wyjaśnienia najbardziej problematycznych kwestii.

3.3 Mamy nadzieję, że Standard w wersji 3.0. będzie dobrym przewodnikiem po zawiłych kwestiach związanych z procesem wdrażania chmury obliczeniowej w Państwa organizacjach, a tym samym przydatnym narzędziem doskonalenia tego procesu.

CZĘŚĆ II

KONTEKST REGULACYJNY

1. WYMAGANIA PRAWNE DLA USŁUG CHMURY OBLICZENIOWEJ – WPROWADZENIE

1.1 **Wprowadzenie.** Korzystanie przez Bank z usług chmury obliczeniowej wymaga uwzględnienia szeregu wymogów regulacyjnych. W szczególności usługa chmury obliczeniowej może podlegać wymogom:

1.1.1. Rozporządzenia DORA;

1.1.2. Outsourcingu regulowanego (Prawo bankowe, Ustawa o obrocie instrumentami finansowymi, Wytyczne EBA dot. outsourcingu);

1.1.3. RODO;

1.1.4. NIS 2 (UKSC);

1.1.5. Data Act;

1.1.6. AI Act.

1.2 Od czasu publikacji poprzedniej wersji Standardu, otoczenie prawne usług chmury obliczeniowej w bankowości uległo istotnym zmianom. Pojawiły się nowe regulacje unijne (np. DORA, Data Act, AI Act), dokonano też nowelizacji przepisów krajowych w zakresie outsourcingu regulowanego. UKNF odwołał również Komunikat chmurowy, który stanowił podstawę poprzedniej wersji Standardu. W wyniku tych zmian zaszła potrzeba znaczącej aktualizacji Standardu. W ramach niniejszego opracowania omawiamy wybrane wymogi prawne. Standard stanowi zbiór dobrych praktyk w zakresie zarządzania usługami chmu-

ry obliczeniowej w bankowości, opartych na doświadczeniu członków grupy roboczej opracowującej Standard. Użyte sformułowania „musi" lub „powinien", o ile nie wynika to z treści przepisów prawa powszechnie obowiązującego, należy rozumieć wyłącznie jako rekomendację autorów Standardu.

1.3 **Wycofanie Komunikatu chmurowego.** W związku z odwołaniem Komunikatu chmurowego przez UKNF oświadczeniem UKNF z 16 stycznia 2025r., dokument przestał być w jakikolwiek sposób wiążący dla Banków. Komunikat chmurowy wciąż może być stosowany przez Banki jako zbiór dobrych praktyk. Odwołanie Komunikatu nie stanowi jednak jedynej istotnej zmiany regulacyjnej. W celu określenia kontekstu regulacyjnego, przygotowaliśmy schemat podstawowych zagadnień regulacyjnych związanych chmurą w bankowości, który jest zamieszczony w Załączniku nr 2 do Standardu. Na tle tego schematu w kolejnych punktach omawiamy poszczególne zagadnienia.

1.4 **DORA.** Od 17 stycznia 2025 r. wykorzystywanie przez Banki niektórych usług świadczonych przez Zewnętrznych dostawców Usług ICT może podlegać wymogom określonym w rozporządzeniu DORA, jeśli spełnione są warunki określone w DORA. Usługi chmury obliczeniowej są jednym z rodzajów Usług ICT wymienionych w RTS 2024/2956 i mogą podlegać wymogom DORA.

1.5 Banki, jako podmioty objęte DORA, muszą dostosować korzystanie z usług chmury obliczeniowej do przyjętych przez siebie standardów odporności cyfrowej. W związku z tym Bank powinien dokonać przeglądu oraz ewentualnej aktualizacji polityk i procedur w zakresie chmury obliczeniowej, aby zapewnić ich spójność z dokumentami wewnętrznymi w zakresie DORA.

1.6 W tym kontekście usługi chmury obliczeniowej są elementem szerszego obszaru Usług ICT, a DORA nie wymaga tworzenia dla tego rodzaju usług odrębnego systemu zarządzania ryzykiem. Z uwagi na specyfikę usług chmury obliczeniowej w zakresie najlepszych praktyk ustanowionych m.in. Komunikatem chmurowym oraz normami międzynarodowymi (np. ISO 27017 oraz ISO 27018), uzasadnione jest jednakże utrzymywanie w Banku dedykowanych procesów pozwalających należycie zarządzać ryzykiem usług chmury obliczeniowej. Procesy te powinny być jednak spójne z ogólnymi ramami zarządzania ryzykiem ICT, jako ich specjalistyczny element.

1.7 **Chmura poza DORA.** Rozporządzenie DORA dotyczy jedynie sytuacji, w których usługi chmury obliczeniowej kwalifikują się jako Usługi ICT i są dostarczane bezpośrednio do Banku. Nie obejmuje zatem sytuacji związanych z przetwarzaniem danych Banku w usługach chmury obliczeniowej przez innych dostawców Banku niż zewnętrzni dostawcy Usług ICT. W przypadku, w którym usługa świadczona na rzecz Banku nie jest Usługą ICT, wciąż może dojść do przetwarzania informacji prawnie chronionych Banku w chmurze obliczeniowej, co niesie ze sobą ryzyko nieuprawnionego dostępu do takich informacji. W ramach Standardu (pkt 5.) opisano rekomendowany sposób działania w takich sytuacjach, oparty na ocenie tego, czy usługa chmury obliczeniowej jest istotnie powiązana z usługą świadczoną na rzecz Banku.

1.8 **Outsourcing.** Niezależnie od DORA, usługi chmury obliczeniowej świadczone na rzecz Banku mogą kwalifikować się jako outsourcing regulowany (outsourcing bankowy na podstawie Prawa bankowego lub outsourcing inwestycyjny na podstawie Ustawy o obrocie lub outsourcing wg Wytycznych EBA), jeśli zostaną spełnione właściwe kryteria wynikające z właściwych przepisów prawa lub regulacji.

1.9 Bank, wobec którego zastosowanie znajdują przepisy Ustawy o obrocie, musi uwzględnić, czy usługi chmury obliczeniowej będą wspierały działalność Banku objętą tą ustawa. Jeśli tak, będzie miał obowiązek zastosowania dodatkowych wymogów wynikających z tej ustawy oraz z Rozporządzenia delegowanego 2017/565.

1.10 **Funkcje krytyczne lub istotne.** W celu identyfikacji wpływu usług chmury obliczeniowej na działalność Banku Komunikat chmurowy wprowadzał pojęcie „outsourcingu szczególnego". Podobnie, Wytyczne EBA dot. outsourcingu prezentują zbliżony koncept outsourcingu „funkcji krytycznej". Na potrzeby Standardu poprzez funkcje krytyczne lub istotne będziemy rozumieli funkcje wewnętrzne Banku, zgodnie z definicją przyjętą w DORA. W tym kontekście funkcje należy rozumieć jako procesy wewnętrzne Banku lub zgrupowania takich procesów, zgodnie z przyjętą przez Bank klasyfikacją. Usługi chmury obliczeniowej są więc oceniane w kontekście wspierania tak rozumianych funkcji.

1.11 **RODO.** Usługi chmury obliczeniowej świadczone przez zewnętrznego Dostawcę, obejmujące przetwarzanie danych osobowych, których administratorem jest Bank, wymagają zapewnienia zgodności z przepisami RODO. Kluczowe w tym zakresie są wymogi dotyczące powierzenia przetwarzania danych osobowych wskazane w art. 28 RODO. Podstawą jest zawarcie z Dostawcą umowy powierzenia, określającej zakres i sposób przetwarzania danych osobowych na zlecenie Banku. Umowa powinna adresować konkretne wymagania określone w przepisach. W ramach zapewnienia zgodności należy zwrócić szczególną uwagę na stosowane przez Dostawcę zabezpieczenia techniczne i organizacyjne gwarantujące bezpieczeństwo powierzonych przez Bank danych osobowych. Warto wybrać Dostawcę legitymującego się uznanymi certyfikatami oraz standardami bezpieczeństwa. Istotny aspekt, szczególnie w przypadku współpracy z międzynarodowymi Dostawcami, stanowi przekazywanie danych osobowych do państw trzecich. Jeśli administrator w ogóle dopuści taką możliwość, transfer danych wymaga zapewnienia odpowiednich środków legalizujących. Należy zadbać o transparentność lokalizacji i przepływów danych, w tym o wybór odpowiedniego regionu przetwarzania. Warto też pamiętać, że Bank powinien mieć zagwarantowane skuteczne prawo do audytu procesora. Zasadne jest zweryfikowanie umowy pod kątem operacyjnych możliwości jego realizacji. W sektorze finansowym wymagania RODO powinny być skorelowane z wytycznymi nadzorczymi, co wzmacnia zgodność i ogranicza ryzyko.

1.12 **NIS 2 oraz UKSC.** Bank powinien uwzględniać zgodność regulacyjną Dostawców usług chmury obliczeniowej z NIS 2 oraz UKSC w ramach procedur oceny ryzyka i należytej staranności takich Dostawców. Zgodnie z projektowanymi zmianami do UKSC wynikającymi z procesu implementacji NIS 2 w Polsce Dostawcy usług chmury obliczeniowej zostaną bowiem wskazani wprost w Załączniku I do UKSC jako podmioty prowadzące działalność w sektorze kluczowym „infrastruktura cyfrowa". Dostawcy usług chmurowych będą zatem podlegać regulacjom UKSC jako podmioty kluczowe lub ważne, w zależności od przewyższania bądź nieprzewyższania wymogów wielkościowych średniego przedsiębiorstwa. Ponadto wybrani Dostawcy usług chmury obliczeniowej będą mogli być identyfikowani jako Dostawcy usług zarządzanych lub usług zarządzanych w zakresie cyberbezpieczeństwa, ze względu na wskazanie ich w Załączniku I do UKSC jako podmiotów prowadzących działalność w sektorze kluczowym „zarządzanie usługami ICT". Z drugiej strony Bank, jako podmiot prowadzący działalność w sektorze kluczowym „bankowość i infrastruktura rynków finansowych", będzie stosował przepisy UKSC w ograniczonym zakresie, w tym przepisy rzutujące na zarządzanie ryzykiem ze strony Dostawców usług chmury obliczeniowej. Kwestia ta zostanie uregulowana szczegółowo w odpowiednich przepisach UKSC regulujących współstosowanie UKSC i DORA.

1.13 **AI w chmurze. AI Act** Jeśli usługa chmury obliczeniowej obejmuje dostarczenie systemu AI, Bank powinien uwzględnić obowiązki wynikające z AI Act. Kluczowe w tym zakresie jest określenie roli Banku względem systemu AI zgodnie z definicjami AI Act – dostawcy (provider) lub podmiotu stosującego (deployer). Bank, jako podmiot wykorzystujący system AI w ramach usług chmury obliczeniowej, będzie zazwyczaj pełnił funkcję podmiotu stosującego, co wiąże się z określonymi obowiązkami regulacyjnymi, w tym w obszarze jakości danych wejściowych, nadzoru ludzkiego i raportowania incydentów. Niezależnie od pełnionej funkcji, Bank powinien przeprowadzić klasyfikację poziomu ryzyka systemu AI poprzez weryfikację, czy nie zawiera on zakazanych praktyk AI określonych w art. 5 AI Act oraz dokonanie oceny, czy system AI stanowi system AI wysokiego ryzyka w rozumieniu AI Act. Istotne jest również ustalenie, czy system AI podlega szczególnym wymogom rozporządzenia, co w szczególności może dotyczyć systemów generatywnej AI objętych obowiązkami w zakresie przejrzystości przewidzianymi w art. 50 AI Act. W umowie z Dostawcą powinny znaleźć się postanowienia zapewniające odpowiednią alokację obowiązków regulacyjnych, w szczególności w zakresie wyjaśnialności, źródeł danych, parametrów działania systemu AI i jego ograniczeń. Należy również uwzględnić, że AI Act ma charakter eksterytorialny i jest stosowany także wtedy, gdy Dostawca ma siedzibę lub znajduje się w państwie trzecim (poza UE), o ile wyniki wytworzone przez system AI są wykorzystywane w Unii.

1.14 **Data Act (Akt w sprawie danych).** W Rozdziale VI Data Act uregulowano zasady ułatwiania zmiany dostawcy usług przetwarzania danych. Dotyczy to w szczególności usług chmury obliczeniowej. Uregulowano, w jaki sposób Dostawca ma obowiązek ułatwiać klientowi wyjście z usługi (zmianę Dostawcy). Klientom tych Dostawców przyznano nowe uprawnienia, m.in. w zakresie wypowiadania umowy. Planowane jest również przygotowanie wzorcowych warunków umownych usług przetwarzania danych. Usługi chmury obliczeniowej mogą być jednocześnie kwalifikowane jako usługi przetwarzania danych w rozumieniu Data Act. Bank jako odbiorca takich usług może korzystać z uprawnień przewidzianych w tym rozporządzeniu. Rekomenduje się uwzględnienie przewidzianych w Data Act uprawnień w procesach Banku dotyczących chmury obliczeniowej.

1.15 **Wytyczne EBA.** Europejski Urząd Nadzoru Bankowego (EBA/EUNB) rozpoczął konsultacje publiczne w sprawie projektu wytycznych w sprawie należytego zarządzania ryzykiem ze strony osób trzecich. Projekt wytycznych koncentruje się na uzgodnieniach z osobami trzecimi w odniesieniu do usług niezwiązanych z ICT świadczonych przez usługodawców będących osobami trzecimi i ich podwykonawców, ze szczególnym naciskiem na świadczenie kluczowych lub ważnych funkcji. Nowe wytyczne zmieniają i aktualizują poprzednie wytyczne EBA dotyczące outsourcingu, opublikowane w 2019 r., zgodnie z aktem w sprawie operacyjnej odporności cyfrowej (DORA). W projekcie wytycznych określono kroki, które podmioty finansowe muszą podjąć w odniesieniu do cyklu życia ustaleń z osobami trzecimi (tj. ocena ryzyka, należyta staranność, etap umowy, podwykonawstwo, monitorowanie, strategie wyjścia i procesy rozwiązania umowy) w celu zapewnienia w miarę możliwości spójności z wymogami wynikającymi z ram DORA.

1.16 **Podsumowanie.** Powyższe regulacje w niektórych obszarach zawierają zbliżone wymogi (np. wymogi dla umów outsourcingu regulowanego i wymogi umów z DORA). Obecnie nie ma informacji, aby przepisy w tym zakresie miały być zmieniane, więc Bank w zależności od kwalifikacji musi stosować część lub wszystkie wymogi regulacyjne. Powielające się obowiązki dotyczą w szczególności:

1.16.1. obowiązków w odniesieniu do zapewnienia ciągłości działania,

1.16.2. wymogów umownych,

1.16.3. zawiadamiania organu nadzoru o zawarciu (zamiarze zawarcia) umowy.

2. ZAKRES PRZEDMIOTOWY STANDARDU

2.1 Z uwagi na szeroki zakres regulacji mających zastosowanie do korzystania z chmury przez Bank, Standard ma na celu omówienie kluczowych obowiązków Banku wynikających z tych regulacji oraz prezentację dobrych praktyk związanych z wykonywaniem tych obowiązków.

2.2 **Usługi chmury obliczeniowej a inne Usługi ICT.** Rekomendacje zawarte w Standardzie odnoszą się wyłącznie do usług chmury obliczeniowej, zgodnie z przyjętą definicją takich usług. Funkcjonujące w obrocie definicje usług chmury obliczeniowej (zamiennie: chmury obliczeniowej) są oparte na nieostrych kryteriach, w związku z czym niekiedy może być utrudnione ich jednoznaczne odróżnienie od innych Usług ICT, w szczególności usług hostowanych. W ramach tego materiału koncentrujemy się na tych Usługach ICT, które mają cechy typowe dla usług chmury obliczeniowej.

2.3 **Rodzaje ryzyka.** Usługi chmury obliczeniowej mogą być rozpatrywane w kilku kontekstach regulacyjnych jako źródła ryzyka wymagającego identyfikacji, oceny i mitygacji:

2.3.1. jako zasoby ICT wymagające zarządzania i inwentaryzacji (np. własna chmura obliczeniowa),

2.3.2. jako Usługi ICT świadczone przez zewnętrznych dostawców Usług ICT,

2.3.3. jako narzędzie przetwarzania informacji wykorzystywane przez innych Dostawców Banku, generujące specyficzne ryzyka.

2.4 Standard skupiony jest przede wszystkim na zarządzaniu ryzykiem strony trzeciej w kontekście chmury obliczeniowej, odnosząc się do kontekstów opisanych w pkt 2.3 powyżej. Niektóre rekomendacje mogą mieć zastosowanie do budowania przez Bank własnej chmury obliczeniowej, jednakże ten model zasadniczo nie jest przedmiotem zainteresowania Standardu.

2.5 **Rodzaje chmury.** Obecne regulacje nie różnicują obowiązków względem rodzaju chmury obliczeniowej (chmura prywatna, publiczna itd.), tak jak to czynił Komunikat chmurowy. W konsekwencji Standard odnosi się do każdego rodzaju chmury obliczeniowej, o ile jest ona dostarczana do Banku przez zewnętrznego dostawcę jako Usługa ICT lub jest w istotny sposób wykorzystywana przez dostawcę Banku do świadczenia innego rodzaju usług dla Banku niż Usługi ICT. Bank powinien zatem brać pod uwagę rodzaj chmury obliczeniowej podczas analizy ryzyka oraz stosować rozwiązania adekwatne do rodzaju chmury. Przykładowo – chmura prywatna może nie generować ryzyk w zakresie współdzielenia infrastruktury z innymi klientami dostawcy, zatem stosowanie rekomendacji dotyczących tego typu ryzyka może być nieadekwatne do sytuacji.

2.6 **Usługi SaaS a inne usługi.** Zwracamy uwagę na wyjaśnienie zawarte w definicji usługi w chmurze: SaaS. Istotą tej usługi jest zapewnienie dostępu do działającego oprogramowania, w związku z czym musi ona w sobie zawierać hosting aplikacji w chmurze. Może to być własna chmura obliczeniowa Dostawcy lub chmura obliczeniowa Poddostawcy. Nie spełnia tej definicji dostarczenie samej aplikacji lub usługi jej utrzymania bez zapewnienia hostingu w chmurze. Należy również odróżnić usługę SaaS od usługi hostowanej. W tym drugim przypadku, aplikacja może być również dostarczana w modelu usługowym, przy czym infrastruktura, na której jest ona osadzona, nie spełnia cech chmury obliczeniowej. W szczególności może to być ograniczona infrastruktura dostawcy, niezapewniająca skalowalności lub elastyczności właściwej chmurze obliczeniowej.

2.7 **Testowanie usług chmury obliczeniowej.** Bank, wykorzystując usługi chmury obliczeniowej na potrzeby ich testowania, powinien przeanalizować: czy usługa ta będzie podlegać właściwej regulacji, w szczególności ocenić, czy podlega DORA, outsourcing regulowany, Data Act, kwalifikuje się jako system AI lub obejmuje przetwarzanie informacji prawnie chronionych.

2.7.1. Bank powinien uwzględnić wymogi RTS 2024/1774 dotyczące testowania na środowisku produkcyjnym systemów i Usług ICT. Bank nie ma obowiązku stosowania do Usług ICT znajdujących się w fazie testowej i niewspierających funkcji Banku przepisów DORA dotyczących zarządzania ryzykiem ze strony zewnętrznych dostawców Usług ICT.

2.7.2. W sytuacji przetwarzania Informacji prawnie chronionych w trakcie testowania jest duże prawdopodobieństwo, że zachodzi outsourcing regulowany. Należy wtedy ocenić ryzyko dostępu do tych informacji i właściwą podstawę prawną takiego dostępu.

2.8 Jeśli usługi chmury obliczeniowej są wykorzystywane do tworzenia modeli AI, Bank powinien zwrócić uwagę na wykorzystanie danych w fazie testowania modeli. Ze względu na specyfikę trenowania modeli dane te zwykle nie są danymi testowymi, a danymi produkcyjnymi, i w związku z tym podlegają odpowiednio ochronie.

2.9 W konsekwencji tego, że nie można jednoznacznie wyłączyć stosowania regulacji do testowania usług chmury obliczeniowej, Standard również nie zawiera takiego odgórnego wyłączenia.

3. CHMURA W KONTEKŚCIE DORA

3.1 **Ramy zarządzania ryzykiem ICT.** Obowiązki Banku w związku z korzystaniem z usług chmury obliczeniowej, w wymiarze ogólnym stosowania ram zarządzania ryzykiem ICT (art. 5–14 DORA) obejmują przede wszystkim:

a) identyfikowanie, ocenę i dokumentowanie ryzyka ICT związanego z usługą chmury obliczeniowej, jako elementu szeroko rozumianego ryzyka ICT (art. 6 DORA),

b) stosowanie odpowiednich wymagań do usług chmury obliczeniowej (art. 7 DORA),

c) identyfikację usług chmury obliczeniowej jako zasobów ICT (art. 8 DORA) oraz w ramach tzw. rejestru DORA,

d) stosowanie odpowiednich wymagań bezpieczeństwa do usług chmury obliczeniowej (art. 9 DORA),

e) stosowanie mechanizmów wykrywania do usług chmury obliczeniowej (art. 10 DORA),

f) stosowanie mechanizmów zapewnienia ciągłości działania do usług chmury obliczeniowej (art. 11 DORA),

g) stosowanie polityk i procedur kopii zapasowych, przywracania i odzyskiwania danych do usług chmury obliczeniowej (art. 12 DORA).

h) zapewnienie w organizacji właściwych kompetencji pozwalających na zarządzanie ryzykiem chmury obliczeniowej (art. 13 DORA).

3.2 **Incydenty ICT.** Usługi chmury obliczeniowej mogą być źródłem incydentów ICT, w związku z czym Bank ma obowiązek stosować do nich procedury zarządzania incydentami ICT (art. 14). W szczególny sposób wymaga to zapewnienia w umowie z Dostawcą odpowiednich zobowiązań w zakresie powiadamiania o incydentach i wspierania w zarządzaniu nimi, jak również powiadamiania o znaczących cyberzagrożeniach.

3.3 **Testowanie odporności.** Banki podlegają również wymogom DORA w zakresie testowania operacyjnej odporności cyfrowej, określone w Rozdziale IV DORA. Część Banków może zostać objęta również obowiązkiem prowadzenia testów TLPT zgodnie z art. 26 i 27 DORA. W tym kontekście usługi chmury obliczeniowej powinny być uwzględnione, jako przedmiot odpowiednich testów. Wymagać to będzie w szczególności zabezpieczenia odpowiednich zobowiązań Dostawcy w umowie.

3.4 **Zarządzanie ryzykiem Dostawców.** W ramach Standardu poświęcamy szczególną uwagę obowiązkom wynikającym z Rozdziału V DORA, dotyczącym zarządzania ryzykiem ze strony zewnętrznych dostawców Usług ICT. Usługi chmury obliczeniowej przy spełnieniu kryteriów określonych w DORA będą podlegać tym wymogom. Kluczowe obowiązki Banku w tym zakresie obejmują (art. 28–30 DORA):

3.4.1. objęcie ramami zarządzania ryzykiem ze strony zewnętrznego dostawcy Usług ICT (art. 28 DORA),

3.4.2. wykonanie obowiązkowych analiz przed zawarciem umowy:

- **a)** ocena, czy usługa chmury obliczeniowej wspiera krytyczną lub istotną funkcję Banku (tzw. ocena krytyczności),
- **b)** ocena zgodności warunków umowy,
- **c)** identyfikacja i ocena ryzyk związanych z umową, a zwłaszcza ryzyka koncentracji (tzw. analiza ryzyka),
- **d)** analiza odpowiedniości Dostawcy (tzw. analiza due diligence),
- **e)** analiza spełnienia wymagań bezpieczeństwa przez Dostawcę,
- **f)** identyfikacja i ocena konfliktów interesów związanych z umową.

3.4.3. uwzględnienie w rejestrze umów z Dostawcami Usług ICT (art. 28 ust. 3), w tym dokumentowane w rejestrze m.in.:

- **a)** charakter Usług ICT,
- **b)** ustalenia umowne,
- **c)** dane identyfikacyjne Dostawcy usług chmury obliczeniowej, a dla Usług ICT wspierających funkcje krytyczne lub istotne Banku również dane identyfikacyjne podwykonawców,
- **d)** lokalizację świadczenia Usług ICT, lokalizację przetwarzania danych,
- **e)** poziom istotności, ocena krytyczności oraz wpływu dla ciągłości działalności bankowej,
- **f)** raportowanie rejestru do organu nadzoru,
- **g)** uwzględnienie usług chmury obliczeniowej w planie audytów i kontroli.

3.5 Zakres wymagań wynikających z Rozdziału V DORA będzie za każdym razem zależał od krytyczności usługi chmury obliczeniowej, tj. od tego, czy usługa wspiera funkcję krytyczną lub istotną Banku.

3.6 W przypadku Usług ICT wspierających funkcję krytyczną lub istotną Banku, Bank ma dodatkowe obowiązki do spełnienia, np.:

3.6.1. posiadanie strategii i planu wyjścia (exit strategy) i planu ciągłości działania (business continuity),

3.6.2. dodatkowe wymogi co do treści umowy,

3.6.3. powiadamianie KNF o planowanym zawarciu umowy,

3.6.4. zaangażowanie zarządu w zatwierdzanie Usługi ICT,

3.6.5. posiadanie i testowanie przez Dostawcę planu awaryjnego, a także środków, narzędzi i polityk bezpieczeństwa ICT, które zapewniają najwyższy poziom bezpieczeństwa.

3.7 Wymogi DORA w zakresie zarządzania ryzykiem zewnętrznych dostawców zostały rozwinięte w kilku aktach wykonawczych i delegowanych, tj.:

3.7.1. RTS 2025/532 (dot. podwykonawstwa),

3.7.2. ITS 2024/2956 (dot. rejestru),

3.7.3. RTS 2024/1773 (dot. polityki umów na Usługi ICT wspierających funkcję krytyczną lub istotną Banku).

3.8 **Notyfikowanie (raportowanie).** Bank musi realizować obowiązki sprawozdawcze przewidziane w DORA oraz innych aktach prawnych. Zestawienie kluczowych obowiązków Banku w zakresie notyfikacji umów na usługi chmury obliczeniowej zawarte jest w Załączniku nr 4 – Notyfikacja umów na usługi w chmurze.

3.9 **Wymagania kontraktowe.** Umowa na świadczenie usług chmury obliczeniowej podlegająca pod DORA musi spełniać przewidziane tam wymagania, z uwzględnieniem podziału na Usługi ICT wspierające krytyczne lub istotne funkcje i pozostałe Usługi ICT. Szczegółowe omówienie wymagań umownych DORA oraz innych źródeł prawa zawarte jest w Załączniku nr 3 – Wymagania kontraktowe.

3.10 **Podwykonawstwo w ramach DORA.** W związku z tym, że DORA jest regulacją niezależną od krajowych regulacji outsourcingu, łańcuch podwykonawstwa na potrzeby DORA jest oceniany inaczej niż łańcuch podwykonawstwa w ramach outsourcingu regulowanego. W wyniku tej odrębności może zajść sytuacja, gdy podmiot będzie miał status podwykonawcy na gruncie DORA, lecz nie będzie kwalifikowany jako Poddostawca w ramach łańcucha outsourcingu.

3.11 Zgodnie z treścią RTS 2024/2956 (instrukcja wypełniania wzoru B_05.02), łańcuch dostaw Usług ICT w rozumieniu DORA obejmuje, w stosownych przypadkach, w przypadku Usług ICT wspierających funkcję krytyczną lub istotną Banku, wszystkich podwykonawców, którzy faktycznie wspierają świadczenie tych Usług ICT (tj. wszystkich podwykonawców świadczących Usługi ICT, których zakłócenie mogłoby zagrozić bezpieczeństwu lub ciągłości świadczenia Usług ICT). Na potrzeby DORA pod uwagę powinni być brani zatem jedynie podwykonawcy o istotnym charakterze. Odrębne kryteria znajdą zastosowanie do oceny, czy podwykonawca stanowi Poddostawcę w łańcuchu outsourcingu. Omawiamy je szerzej w pkt 7.4 Standardu.

3.12 Podwykonawstwo Usług ICT wspierających funkcję krytyczną lub istotną Banku wiąże się z koniecznością spełnienia licznych wymogów określonych w RTS 2025/532. Obejmują one m.in. obowiązki Dostawcy w zakresie:

3.12.1. odpowiedzialności Dostawcy za podwykonawców,

3.12.2. zarządzania łańcuchem dostawy, w tym zarządzanie po stronie Dostawcy ryzykiem podwykonawców,

3.12.3. treści umów z podwykonawcami,

3.12.4. zasad zmian podwykonawców.

3.13 Umowa na usługi chmury obliczeniowej mająca status umowy na Usługi ICT wspierające funkcję krytyczną lub istotną Banku, musi spełniać wszystkie ww. wymogi.

4. CHMURA W KONTEKŚCIE OUTSOURCINGU BANKOWEGO

4.1 **Umowa Outsourcingu bankowego.** Umowa o świadczenie usługi chmury obliczeniowej jest umową Outsourcingu bankowego zawsze, gdy spełnia **którekolwiek** z poniższych kryteriów:

4.1.1. jej przedmiotem jest realizacja czynności wskazanych w art. 5 oraz art. 6 Prawa bankowego i polega na świadczeniu usług wskazanych w art. 6a ust. 1 pkt 1) od a) do f) Prawa bankowego (umowa agencyjna) oraz w art. 6a ust. 1 pkt 1) lit. g)–l) (na podstawie innej umowy),

4.1.2. jej przedmiotem jest realizacja powierzonych przez Bank czynności faktycznych związanych z działalnością Bankową (art. 6a ust 1 pkt 2) Prawa bankowego),

4.1.3. w ramach jej realizacji Dostawca lub jego Poddostawcy będą mieli dostęp do Tajemnicy bankowej,

4.1.4. jej przedmiotem jest realizacja czynności, które mogą mieć wpływ na ciągłe i niezakłócone prowadzenie działalności przez Bank.

4.2 Umowy na usługi chmury obliczeniowej ze względu na przedmiot świadczonej usługi będą w przeważającej mierze umowami nienazwanymi, które przy spełnieniu powyższych kryteriów będą najczęściej stanowić powierzenie realizacji czynności faktycznych związanych z działalnością Bankową (art. 6a ust. 1. pkt 2) Prawa bankowego).

4.3 Umowa outsourcingowa w rozumieniu art. 6a Prawa bankowego powinna być zawsze zawarta na piśmie (zob. Załącznik nr 3 – Wymagania kontraktowe).

4.4 **Podoutsourcing.** Dla usług chmury obliczeniowej kwalifikujących się jako outsourcing bankowy, kwestia podoutsourcingu jest uregulowana w Prawie bankowym:

4.4.1. podoutsourcing łańcuchowy jest dopuszczalny na podstawie art. 6a ust. 7a Prawa bankowego, z zachowaniem wymogów dla podoutsourcingu,

4.4.2. w celu weryfikacji, czy występuje podoutsourcing łańcuchowy, w szczególności można wykorzystać definicję Poddostawcy,

4.4.3. wymagana jest zgoda Banku na podoutsourcing w umowie na usługi chmury obliczeniowej, a umowa powinna określać zasady zaangażowania Poddostawców.

4.5 W odniesieniu do Banków, wobec których zastosowanie znajdują przepisy Ustawy o obrocie, Bank powinien uwzględnić, że art. 81f ust. 2 Ustawy o obrocie ogranicza zakres dopuszczalnego podoutsourcingu – podpowierzane czynności nie mogą stanowić istoty czynności zleconych przez Bank, a w przypadku umów, o których mowa w art. 81a ust. 2 Ustawy o obrocie (umowy dotyczące powierzenia podstawowych lub istotnych funkcji operacyjnych), powodować, że którykolwiek z warunków przewidzianych w art. 31 ust. 2 rozporządzenia 2017/565 nie będzie spełniony.

4.6 **Zmiany Poddostawców.** Zaangażowanie Poddostawców w ramach outsourcingu może się odbyć na podstawie ogólnej pisemnej zgody Banku, najczęściej wyrażonej w treści umowy. Dostawca ma wtedy obowiązek informowania Banku o zamierzonych zmianach w zakresie dodania, zastąpienia Poddostawców, umożliwiając jednocześnie bankowi wyrażenie sprzeciwu wobec takich zmian. Obowiązki te powinny być sprecyzowane w umowie.

4.7 Należy pamiętać, że w przypadku podoutsourcingu zagranicznego może zaistnieć obowiązek notyfikacji w trybie art. 6d Prawa bankowego, który omawiamy dalej w pkt 7.13 Standardu.

4.8 Zgodnie z sugestią UKNF w ramach Q&A Chmurowego w celu ograniczenia ryzyka podoutsourcingu łańcuchowego Bank może nawiązać relację umowną z Poddostawcą w formule umowy trójstronnej.

4.9 **Zakaz wyłączania odpowiedzialności Dostawcy.** Na podstawie art. 6b. ust. 1 Prawa bankowego nie można wyłączyć odpowiedzialności Dostawcy wobec Banku za szkody wyrządzone klientom Banku wskutek niewykonania lub nienależytego wykonania umowy outsourcingu bankowego (jak również umów podoutsourcingu). Bank powinien przeanalizować zasady odpowiedzialności Dostawcy wynikające z umowy, w szczególności zastosowane wyłączenia. Dopuszczalne jest natomiast ograniczenie odpowiedzialności Dostawcy wobec Banku, wynikającej z umowy outsourcingu bankowego.

4.10 Art. 6b. ust. 1 Prawa bankowego:

4.10.1. nie ustanawia stosunku prawnego pomiędzy klientem Banku a Dostawcą, który byłby podstawą bezpośredniej odpowiedzialności Dostawcy wobec klienta Banku,

4.10.2. nie wymaga nawiązywania stosunku umownego pomiędzy Bankiem a Poddostawcą, tj. w przypadku współpracy w modelu Bank –> dostawca –> Poddostawca ten ostatni nie będzie odpowiadał wobec Banku, lecz wobec dostawcy, a dostawca będzie odpowiadał wobec Banku za szkody klientów Banku spowodowane niewykonaniem lub nienależytym wykonaniem umowy podoutsourcingu przez Poddostawcę.

4.11 **Umowy pod prawem obcym.** W przypadku zawarcia umowy na Usługi chmury obliczeniowej, do której zastosowanie mają przepisy prawa obcego, Bank zawiera w niej postanowienia odpowiadające przepisom art. 473 § 2, art. 474 i art. 483 § 2 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2024 r. poz. 1061 i 1237).

4.12 **Inne wymogi**. Zgodnie z art. 6c Prawa bankowego:

4.12.1. umowa outsourcingu bankowego może zostać zawarta i być wykonywana tylko wtedy, gdy:

a) Bank i Dostawca będą posiadać plany działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową,

b) powierzenie wykonywania czynności w ramach umowy 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),

c) Bank uwzględni ryzyko związane z powierzeniem wykonywania takich czynności w systemie zarządzania ryzykiem.

4.12.2. Niezależnie od rejestru DORA, Bank ma obowiązek wprowadzenia umowy outsourcingu bankowego do ewidencji umów, określając w niej co najmniej:

a) dane (informacje) identyfikujące Dostawcę,

b) zakres usługi chmury obliczeniowej,

c) miejsce wykonania,

d) okres obowiązywania umowy.

4.13 **Outsourcing zagraniczny.** Zgodnie z art. 6d. Prawa bankowego Bank ma obowiązek zawiadomić KNF o zamiarze zawarcia umowy outsourcingu bankowego:

4.13.1. z Dostawcą, którego siedziba znajduje się w kraju innym niż państwo należące do EOG,

4.13.2. lub która wykonywana będzie poza państwem należącym do EOG.

4.14 Do zawiadomienia KNF, o którym mowa powyżej, Bank załącza pakiet dokumentów wymienionych w art. 6d Prawa bankowego, obejmujący projekt umowy z Dostawcą, wyciągi z rejestru oraz inne dokumenty dotyczące Dostawcy i Poddostawców spoza EOG.

4.15 KNF może ponadto na podstawie art. 6c ust. 4 Prawa bankowego wezwać Bank do przedstawienia dodatkowych dokumentów, w tym oświadczenia zarządu Banku, a także dokumentów, które Bank musi pozyskać od przedsiębiorcy. Wśród tych dokumentów wymienione są:

4.15.1. opis rozwiązań technicznych i organizacyjnych Dostawcy,

4.15.2. oświadczenia Dostawcy, że nie toczą się wobec niego postępowania sądowe,

4.15.3. oświadczenie zarządu Banku, że prawo obowiązujące w państwie wykonywania czynności umożliwia KNF prowadzenie efektywnego nadzoru.

4.16 W kontekście pkt 4.15.3 powyżej, choć przepisy nie wskazują, że opinia w tym zakresie powinna zostać przekazana do KNF wraz z notyfikacją, to z pewnością dopuszczalne

jest również przekazanie tego dokumentu. Rekomendowane jest, aby Bank dokonał wewnętrznej oceny w zakresie konkretnej jurysdykcji i ewentualnych zagrożeń dla efektywnego nadzoru wynikających z lokalnego prawa. Zbliżone podejście zostało wyrażone w Komunikacie chmurowym.

4.17 W odniesieniu do umów o usługi chmury obliczeniowej nie stosuje się art. 6a ust. 1 pkt 1) lit. m) Prawa bankowego wymagającego zawiadomienia KNF w trybie art. 6d, gdyż usługi chmury obliczeniowej to przede wszystkim czynności faktyczne, o których mowa w art. 6a ust.1 pkt 2) Prawa bankowego.

4.18 Zawiadomienie KNF w trybie art. 6d Prawa bankowego uruchamia postępowanie, w wyniku którego KNF może wyrazić sprzeciw wobec zawarcia umowy, w określonym w tym przepisie terminie. Umowa będąca przedmiotem zawiadomienia w tym trybie może zostać zawarta jedynie, jeżeli KNF nie wyrazi sprzeciwu i nie doręczy decyzji w przedmiocie sprzeciwu w terminie albo jeżeli przed upływem tego terminu KNF doręczy decyzję o stwierdzeniu braku podstaw do zgłoszenia sprzeciwu.

4.19 Schemat postępowania dotyczącego zawiadomienia z art. 6d Prawa bankowego znajduje się w Załączniku nr 4 Notyfikacja umów na usługi w chmurze.

5. CHMURA W UMOWACH NIE-ICT[1]

5.1 W przypadku, w którym usługa świadczona na rzecz Banku nie jest Usługą ICT, wciąż może dojść do przetwarzania Informacji prawnie chronionych Banku w chmurze obliczeniowej, co niesie ze sobą ryzyko nieuprawnionego dostępu do takich informacji. Sytuacja taka nie jest objęta rozporządzeniem DORA, gdyż usługa świadczona dla Banku nie jest Usługą ICT. Bank powinien wtedy zweryfikować, czy wykorzystanie usługi chmury obliczeniowej ma charakter nieautonomiczny[2] – jeśli tak, usługa chmury obliczeniowej wykorzystywana przez partnera Banku (przedsiębiorcę świadczącego usług na rzecz Banku) w ramach outsourcingu regulowanego (art. 6a ust. 1 pkt 2) Prawa bankowego) będzie się kwalifikować jako podoutsourcing w rozumieniu art. 6a ust. 7 lub ust. 7a Prawa bankowego (podoutsourcing w chmurze). Jeśli wykorzystanie usługi chmury obliczeniowej ma charakter autonomiczny, nie wystąpi podoutsourcing w chmurze. Wtedy jednak Bank powinien zadbać o ograniczanie ryzyka dostępu do Informacji prawnie chronionej bez odpowiedniej podstawy prawnej. Jest to możliwe w szczególności poprzez nałożenie na dostawcę usługi dla Banku odpowiednich wymagań technicznych w zakresie ochrony dostępu do danych, zwłaszcza zapewniając brak Ujawnienia informacji. Alternatywnie, jeśli wyeliminowanie dostępu do informacji nie jest technicznie możliwe lub ekonomicznie uzasadnione, Bank powinien rozważyć podstawy prawne takiego dostępu, tj. (i) podoutsourcing (art. 6a ust. 7 i ust. 7a Prawa Bankowego), (ii) zgodę beneficjenta tajemnicy na udostępnienie tajemnicy podmiotom trzecim (art. 104 ust. 3 Prawa bankowego) lub (iii) objęcie dostawcy usługi i dostawcy usługi chmury

1 Fragment opracowany na podstawie: S. Ciach, Opinia w przedmiocie kwalifikacji prawnej korzystania z chmury obliczeniowej przez partnerów Banku, dodatek do Standardu PolishCloud 2.0, Warszawa 2022, dalej: „Opinia".

2 Test autonomiczności został opisany w Opinii, zob. pkt 3.31 i n. Opinii. Test autonomiczności obejmuje weryfikację kryteriów takich jak (i) niezbędność usługi chmury obliczeniowej do realizacji przedmiotu usługi świadczonej na rzecz Banku, (ii) autonomiczny charakter wykorzystania, tj. powiązanie funkcjonalne, (iii) możliwość korzystania z usługi chmury obliczeniowej przez Bank.

obliczeniowej pierwotnym obowiązkiem zachowania tajemnicy bankowej na podstawie art. 104 ust. 1 Prawa Bankowego. Stosując zasady w zakresie podoutsourcingu, oprócz zastosowania właściwych wymogów prawnych (np. art. 6a ust. 7 Prawa bankowego) oraz wdrażających te wymogi procedur, Bank może wykorzystać przewidziane w Standardzie rekomendacje, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych w chmurze.

5.2 Zgodnie z art. 104 ust. 1 Prawa bankowego obowiązek zachowania tajemnicy bankowej dotyczy (i) Banku, (ii) osób w nim zatrudnionych oraz (iii) osób, za których pośrednictwem Bank wykonuje czynności bankowe. Trzecia z wymienionych kategorii podmiotów zobowiązanych do zachowania tajemnicy bankowej jest w literaturze[3] interpretowana w świetle zmieniających się warunków rynkowych i technologii informatycznych. W ramach tej wykładni przyjmuje się, że obowiązek tajemnicy bankowej obejmuje nie tylko pracowników Banku, lecz także osoby współpracujące z Bankiem na podstawie umowy zlecenia, w ramach jednoosobowej działalności gospodarczej, dostawców w ramach outsourcingu regulowanego, ich personel[4], a także osoby mające w praktyce dostęp do informacji objętych tajemnicą – „osoby, których działanie umożliwia funkcjonowanie Banku"[5]. Stanowisko takie uzasadnia się w szczególności tym, że „z punktu widzenia ochrony interesu beneficjenta tajemnicy bankowej nie jest istotne, czy Bank wiąże z tymi osobami stosunek pracy, czy inny stosunek umowny, ponieważ celem wprowadzenia ochrony informacji objętych tajemnicą bankową jest to, by został zapewniony wysoki standard ochrony danych konfidencjonalnych"[6]. W doktrynie podnosi się również, że obowiązek zachowania tajemnicy bankowej dotyczy, wbrew literalnemu brzmieniu art. 104 ust. 1. Prawa bankowego, wszystkich podmiotów, które uzyskały dostęp do chronionych informacji w związku ze swoim udziałem w wykonywaniu przez Bank czynności bankowych. Intencją ustawodawcy, jak również funkcją instytucji tajemnicy bankowej jest to, aby każdy podmiot, który uzyska dostęp do informacji chronionych, był zobowiązany do zachowania ich w tajemnicy[7]. Dotyczy to również usług w zakresie zarządzania systemem informatycznym, które nie stanowią pośredniczenia w wykonywaniu czynności bankowych, a wykonujący je podmiot nie jest pracownikiem Banku. Mimo to uznano, że do określenia obowiązków usługodawcy znajduje zastosowanie przepis art. 104 ust. 1 Prawa bankowego[8]. Celem regulacji art. 104 ust. 1 Prawa bankowego jest objęcie obowiązkiem zachowania tajemnicy bankowej w poufności każdego podmiotu, któr, działając w ramach szeroko rozumianego polecenia Banku, wchodzi w posiadanie takich informacji[9]. W sytuacji gdy partner współpracuje z Bankiem, wchodząc w posiadanie tajemnicy bankowej na podstawie rozszerzonej wykładni art. 104 ust. 1 Prawa bankowego, może ją udostępnić dalej podmiotom, które z nim współpracują na analogicznych zasadach jak personel partnera – tj. pod warunkiem zobowiązania ich do zachowania w poufności informacji objętych tajemnicą oraz poinformowania o odpowiedzialności prawnej związanej z dostępem do tej informacji. Przyjmując taką wykładnię, dostawca usług chmury obliczeniowej współpracujący z partnerem w modelu autonomicznym (pozytywny wynik testu autonomiczności), co do którego stosuje się

3 Por. K. Królikowska, Komentarz do art. 104 Prawa bankowego [w:] B. Bajor i in., Prawo bankowe. Komentarz do przepisów cywilnoprawnych, WKP 2020.

4 Ibidem.

5 Ibidem, podobnie R. Sikorski, Komentarz do art. 104 Prawa bankowego [w:] R. Sikorski (red.), Prawo Bankowe. Komentarz, wyd. 1, Warszawa 2015, Legalis; por. J. Byrski, Podmioty „pierwotnie" obowiązane do zachowania dyskrecji [w:] Tajemnica prawnie chroniona w działalności bankowej, 2010, wyd. 1, który postuluje de lege ferenda, aby wymienić w art. 104 ust. 1 wprost przedsiębiorców wykonujących „czynności faktyczne związane z działalnością bankową", czyli dostawców outsourcingu regulowanego.

6 K. Królikowska, ibidem.

7 Por. Z. Ofiarski, Komentarz do art. 104 Prawa bankowego, Prawo bankowe. Komentarz, LEX 2013.

8 Ibidem.

9 Ibidem, por. także M. Kłaczyński, Tajemnica bankowa w outsourcingu, TPP 2002, nr 3, str. 11.

art. 104 ust. 1 Prawa bankowego, mógłby otrzymać dostęp do informacji objętych tajemnicą na tej samej podstawie prawnej, tj. art. 104 ust. 1 Prawa bankowego. Zasadniczo więc traktowany byłby analogicznie jak członek personelu partnera, który otrzymuje dostęp do informacji w celu realizacji swoich świadczeń na rzecz Banku. W konsekwencji tego podejścia dostawca usług chmury obliczeniowej byłby objęty obowiązkiem dotrzymania tajemnicy bankowej w sposób pierwotny[10]. Przyjęciu tej koncepcji nie szkodzi przy tym istnienie przepisu art. 104 ust. 2 pkt 2 lit. a–b Prawa bankowego, który przewiduje możliwość ujawnienia dostawcy usług i jego Poddostawcom w ramach outsourcingu regulowanego informacji objętych tajemnicą. Przepis ten nie jest sprzeczny z art. 104 ust. 1 Prawa bankowego, w szczególności nie zawiera sformułowań, które wskazywałby, że jest on jedyną podstawą prawną udostępnienia informacji objętych tajemnicą w ramach współpracy w outsourcingu regulowanym. W kontekście analizowanego zagadnienia kluczowe jest określenie, czy przy udostępnieniu informacji objętych tajemnicą jednocześnie dochodzi do podoutsourcingu chmury obliczeniowej (test autonomiczności), co kwalifikowałoby taką sytuację jako podoutsourcing regulowany. W przypadku gdy wykorzystanie chmury realizuje przesłanki podoutsourcingu regulowanego, konieczne jest zastosowanie właściwej podstawy prawnej udostępnienia danych, tj. art. 104 ust. 2 pkt 2 lit. a-b Prawa bankowego.

5.3 Podsumowując – zastosowanie art. 104 ust. 1 Prawa bankowego może mieć miejsce w przypadku autonomicznego wykorzystania chmury przez partnera poprzez uznanie dostawcy usług chmury obliczeniowej i jego personelu oraz podwykonawców za tzw. podmioty wspomagające, pierwotnie objęte obowiązkiem zachowania poufności tajemnicy bankowej na gruncie art. 104 ust. 1 Prawa bankowego. Warunkiem zastosowania tej konstrukcji jest możliwość zakwalifikowania samego partnera jako podmiotu, który jest objęty art. 104 ust. 1 Prawa bankowego. Z uwagi na potrzebę zapewnienia prywatności danych klientów Banku stosowanie omawianej podstawy prawnej z art. 104 ust. 1 Prawa bankowego powinno być realizowane przez Bank na podstawie szacowania ryzyka współpracy z danym partnerem, z zachowaniem kontroli przez Bank nad procesem przetwarzania informacji w chmurze, oraz z zachowaniem standardów bezpieczeństwa informacji zdefiniowanych przez Bank.

10 Podział na podmioty „pierwotnie" oraz „w ramach wtórnego obiegu informacji" objęte obowiązkiem zachowania tajemnicy zaproponował J. Byrski [w:] Tajemnica prawnie chroniona w działalności bankowej 2010, wyd. 1 (Rozdz. III, § 1 pkt I).

CZĘŚĆ III

ZARZĄDZANIE RYZYKIEM ICT USŁUG CHMURY OBLICZENIOWEJ

1. ZARZĄDZANIE OBSZAREM CHMURY OBLICZENIOWEJ (GOVERNANCE CHMURY)

1.1 **Wprowadzenie.** W tym rozdziale zamieszczamy szerszy komentarz odnoszący się do najlepszych praktyk w zakresie zarządzania obszarem chmury obliczeniowej (zamiennie „governance chmury"). Praktyki te są zbieżne z opisanymi w DORA obowiązkami w ramach zarządzania ryzykiem zewnętrznych Usług ICT. W związku z tym poszczególne rekomendowane działania są opisane na podstawie struktury obowiązków przewidzianych w tym zakresie w DORA. Najlepsze praktyki zarządzania chmurą obliczeniową w organizacji wykraczają poza obowiązki z DORA, w związku z czym uzupełniliśmy je o kwestie takie jak FinOps.

1.2 **Governance chmury.** Aktywności, które pomagają uzyskać pewność, że wdrożone w chmurze obliczeniowej rozwiązania skutecznie adresują potrzeby biznesowe interesariuszy, zapewniając jednocześnie zgodność regulacyjną. Efektywny nadzór pomaga uzyskać równowagę między realizacją celów i minimalizacją ryzyka operacyjnego. W kontekście chmury obliczeniowej to także zestaw zasad, polityk, procedur i procesów, które mają na celu zapewnienie skutecznego i bezpiecznego wykorzystania usług chmury obliczeniowej w Banku. Jest to kluczowy element strategii cyfrowej, który pozwala czerpać korzyści z chmury, jednocześnie minimalizując związane z nią ryzyka i zapewniając zgodność z wymogami prawnymi i regulacyjnymi.

1.3 W celu zapewnienia bezpieczeństwa przetwarzanych w chmurze obliczeniowej informacji (lub co do których istnieje zamiar przetwarzania) Bank powinien zdefiniować i zapewnić zgodność zarówno z szeregiem wymagań własnych, jak i wymagań w stosunku do Dostawcy usług chmury obliczeniowej. Wymagania te powinny dotyczyć co najmniej:

1.3.1. bezpieczeństwa szyfrowania i przetwarzania danych w chmurze obliczeniowej,

1.3.2. zarządzania incydentami w tym ICT,

1.3.3. identyfikacji ryzyk i ich adresacji / ograniczania,

1.3.4. oceny Dostawcy i ich Podwykonawców,

1.3.5. audytów i kontroli,

1.3.6. klarownego podziału odpowiedzialności *„shared responsibility model”*,

1.3.7. proporcjonalności,

1.3.8. kopii zapasowych

1.3.9. planów ciągłości działania i strategii wyjścia,

1.3.10. kompetencji oraz programów budowy świadomości wśród pracowników i Dostawców Usług ICT / usług chmury obliczeniowej,

1.3.11. FinOps – ciągła optymalizacja kosztowa.

2. ZARZĄDZANIE RYZYKIEM ZEWNĘTRZNEGO DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ

2.1 **Wprowadzenie.** Rekomendacje w tym obszarze oparte są na wymogach przewidzianych w DORA oraz aktach delegowanych, z uwzględnieniem rekomendowanych do utrzymania praktyk opisanych Komunikatem Chmurowym. Przedstawione zostały w modelu cyklu życia usługi chmury obliczeniowej dostarczanej przez zewnętrznego Dostawcę, tj. od analiz przedumownych przez utrzymanie usługi po zakończenie współpracy.

2.2 Rekomendowany model procesu zarządzania ryzykiem Dostawcy usług chmury obliczeniowej składa się z następujących etapów:

2.2.1. **Etap przed zawarciem umowy** – podjęcie decyzji dotyczącej rozpoczęcia procesu dla usługi chmury obliczeniowej, w tym Usługi ICT wspierającej funkcję krytyczną lub istotną Banku:

a) **Wstępna analiza ryzyka (Ex-ante risk assessment)** – wstępne profilowanie Dostawcy ICT w zakresie usług chmury obliczeniowej oraz wstępna ocena ryzyka,

b) **Ocena odpowiedniości Dostawcy (Due Diligence)** – ocena odpowiedniości Dostawcy usług chmury obliczeniowej, który został pozytywnie zarekomendowany na etapie Ex-ante risk assessment,

c) **Szacowanie ryzyka usługi chmury obliczeniowej** – identyfikacja, ograniczanie, akceptacja oraz sposób zarządzania ryzykami związanymi z wykorzystywaniem usług chmury obliczeniowej,

d) **Plan audytu** – określenie zakresu i częstotliwości audytów,

e) **Ocena spełnienia wymogów bezpieczeństwa dla Dostawców usług chmury obliczeniowej** (decyzja o wyborze Dostawcy oraz określenie ustaleń umownych),

f) **Notyfikacja do organu nadzoru** – w określonych przypadkach, opisanych w Załączniku nr 4 do Standardu.

2.2.2. **Etap operacyjnego działania usług chmury obliczeniowej** – czas korzystania z Usługi ICT i obowiązywania umowy, z uwzględnieniem:

a) monitorowania i okresowa ocena ryzyka, w tym monitorowanie SLA,

b) postępowania z ryzykiem Dostawcy, w tym plan naprawczy,

c) zarządzania wieloma chmurami obliczeniowymi (multi-cloud),

d) audytowania Dostawcy,

e) testów (PCD, plan wyjścia, TLPT).

2.2.3. **Etap wycofania z Usługi ICT i zakończenia współpracy:**

a) zakończenie korzystania z usługi chmury obliczeniowej (przekazanie danych, informacji, wykonanie planu wyjścia, migracja na alternatywne rozwiązanie),

b) zakończenie obowiązywania umowy.

2.3 Wyżej wymienione elementy działania zostały opisane w kolejnych punktach Standardu, przy czym powinny być realizowane zgodnie z wytycznymi DORA i przyjętymi standardami Banku w tym zakresie.

CZĘŚĆ IV

ANALIZY PRZEDUMOWNE

1. EX-ANTE RISK ASSESSMENT – PROFILOWANIE DOSTAWCY USŁUG ORAZ USŁUG CHMURY OBLICZENIOWEJ

1.1 Analiza ta pozwala właściwie zakwalifikować usługę pod kątem dalszego sposobu procedowania, jak również wstępnie ocenić kluczowe aspekty, które mogą zadecydować o dalszym procedowaniu, a nie wymagają szczegółowych analiz (jak np. niedopuszczenie do dalszego procedowania z uwagi na nieakceptowalne dla Banku ryzyko koncentracji).

1.2 Wyniki Ex-ante risk assessment służą do dalszej oceny ryzyka Dostawcy w procesie Due Diligence oraz wykorzystane są w kolejnym etapie szacowania ryzyka usług chmury obliczeniowej.

1.3 Proces ten uwzględnia następujące kroki:

1.3.1. określenie wymagań biznesowych Banku w odniesieniu do usług chmury obliczeniowej, które mają być zlecone Dostawcy,

1.3.2. określenie, czy dana usługa jest Usługą ICT, usługą chmury obliczeniowej i czy spełnia kryteria Usługi ICT krytycznej (tj. wspierającej krytyczną lub istotną funkcję Banku zgodnie z definicją DORA i wykładnią Banku),

1.3.3. zebranie niezbędnych danych od oferenta do przeprowadzenia oceny ex-ante,

1.4 Wstępne profilowanie Dostawcy usług chmurowych odbywa się na podstawie następujących elementów:

1.4.1. Klasyfikacja usługi,

1.4.2. Bezpieczeństwo informacji oraz ich klasyfikacja,

1.4.3. Ochrona danych,

1.4.4. Lokalizacja danych i Dostawcy usługi chmury obliczeniowej,

1.4.5. Ciągłość działania,

1.4.6. Podwykonawcy,

1.4.7. Reputacja,

1.4.8. Koncentracja,

1.4.9. Konflikt interesów.

1.5 Po zebraniu danych od Dostawcy usług chmury obliczeniowej niezbędnych do przeprowadzania Ex-ante risk assessment, Bank, opierając się na przyjętych wytycznych, dokonuje oceny i szacuje wstępny poziom ryzyka, w skali trzystopniowej lub innej stosowanej przez Bank:

1.5.1. wysoki,

1.5.2. średni,

1.5.3. niski.

1.6 Przykładowy szablon Ex-ante risk assessment znajduje się w Załączniku nr 9 do Standardu.

2. OCENA DUE DILIGENCE – OCENA ODPOWIEDNIOŚCI DOSTAWCY USŁUG CHMURY OBLICZENIOWEJ

2.1 Przeprowadzanie Due Diligence wybranego Dostawcy powinno być realizowane przed zawarciem umowy lub uruchomieniem usług chmury obliczeniowej. Podstawowym celem przeprowadzenia oceny Due Diligence jest upewnienie się, że Dostawca (szczególnie wspierający funkcje krytyczne lub istotną dla Banku) jest w stanie zapewnić odpowiedni poziom bezpieczeństwa, ciągłości działania i odporności operacyjnej. Ponadto, Bank powinien także upewnić się, iż Dostawca nie wprowadzi do jego środowiska nadmiernego ryzyka, które mogłoby zagrozić stabilności finansowej lub ciągłości Usług ICT.

2.2 Ocena Due Diligence uwzględnia co najmniej obszary i wymogi wskazane w art. 28 ust. 4 lit. d) Rozporządzenia DORA.

2.3 Przykładowy szablon Oceny Due Diligence znajduje się w Załączniku nr 9 do Standardu.

2.4 Bank w procesie oceny Due Diligence pozyskuje, weryfikuje listę i ewidencjonuje dowody spełnienia lub niespełnienia danego wymagania przez Dostawcę usług chmury obliczeniowej, które służą w dalszym procesie szacowania ryzyka.

2.5 Klasyfikacja usługi oraz klasyfikacja informacji.

2.5.1. Bank w ramach Oceny Due Diligence lub równolegle do niej powinien przeprowadzić klasyfikację informacji planowanych do przetwarzania w usłudze chmury obliczeniowej, tj. określić typ przetwarzanych danych (informacji) dla danej usługi chmury obliczeniowej. W tym celu powinien bazować na przyjętej przez Bank klasyfikacji informacji (podziale na kategorie, klasy informacji). Rekomendujemy, aby uwzględnić co najmniej Informacje prawnie chronione oraz dane osobowe, jako kategorie danych objęte szczególnymi obostrzeniami regulacyjnymi.

2.5.2. W procesie analizy oraz klasyfikacji przetwarzanych danych Bank powinien odwoływać się do istniejących w Banku zasobów inwentaryzacji procesów krytycznych wynikających np. z DORA, BIA lub Rekomendacji H, dotyczącej systemu kontroli wewnętrznej w bankach, wydanej przez UKNF w kwietniu 2017 roku.

2.5.3. Ocena klasyfikacji usługi chmurowej w zakresie krytyczności (jako Usługi ICT) i istotności umowy lub usługi chmury obliczeniowej powinna być realizowana zgodnie z ocenami krytyczności DORA i przyjętymi standardami Banku w tym zakresie (np. opartymi na Business Impact Analysis).

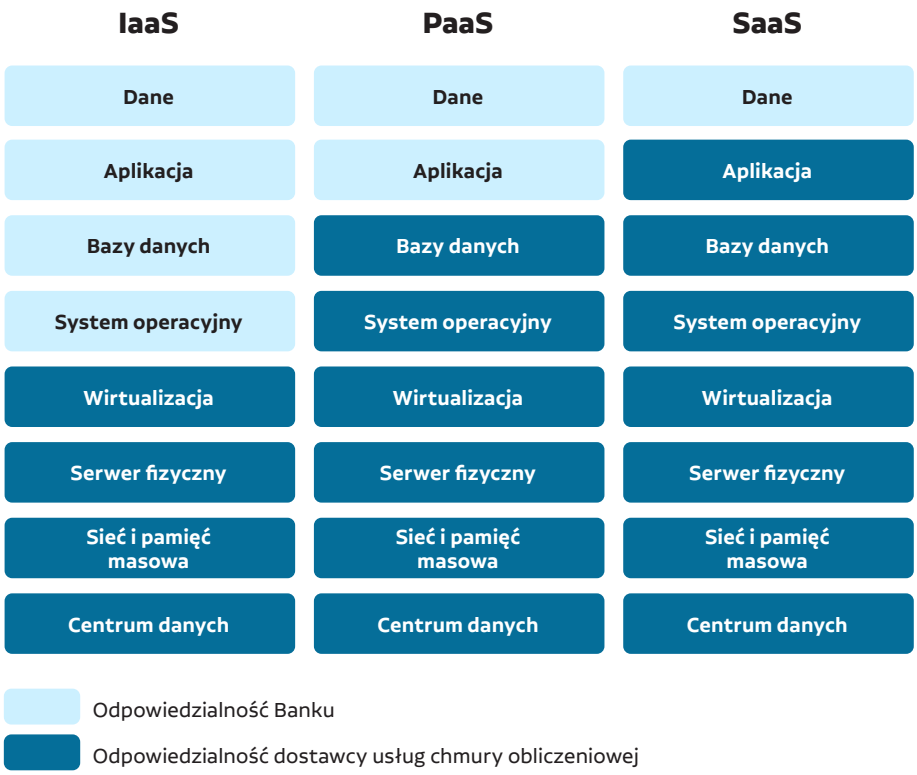
2.6 W wyniku przeprowadzonej analizy Due Diligence Bank powinien identyfikować oraz nazwać ryzyka, jakie niesie za sobą podpisanie umowy, uruchomienie usługi chmury obliczeniowej, używając do tego przyjętej w Banku skali ryzyka oraz odpowiednich wartości finansowych dla tych ryzyk. Po przeprowadzeniu oceny Due Diligence i akceptacji wyników oceny, w kolejnym etapie Bank przeprowadza szacowanie ryzyka chmurowego.

3. SZACOWANIE RYZYKA USŁUGI CHMURY OBLICZENIOWEJ

3.1 Szacowanie ryzyka usługi chmury obliczeniowej to istotny proces dla Banku, który korzystając z takiej Usługi ICT, przenosi, przetwarza oraz przechowuje swoje dane i aplikacje w tym środowisku. Ze względu na specyfikę usług chmury obliczeniowej, taką jak współdzielona odpowiedzialność, dynamiczne środowisko i złożone łańcuchy Dostawców, skuteczne szacowanie ryzyka usługi chmury obliczeniowej i wdrożenie odpowiednich rozwiązań ograniczających (tzw. mitygantów) jest kluczowe dla zapewnienia bezpieczeństwa, ciągłości działania systemów i danych w środowisku chmurowym.

3.2 W procesie szacowania ryzyka ważne jest, aby zrozumieć, czym różni się środowisko chmurowe od tradycyjnej infrastruktury on-premise. W tym celu Bank powinien zidentyfikować i zrozumieć obszary:

3.2.1. **Odpowiedzialności „Shared Responsibility Model”** – Dostawca usługi chmury obliczeniowej jest odpowiedzialny za bezpieczeństwo usługi chmury obliczeniowej, np.: IaaS / PaaS / SaaS i zasoby z tym związane, natomiast Bank odpowiada za bezpieczeństwo w usłudze chmury obliczeniowej w zakresie kontrolowanych przez siebie komponentów tej usługi – czyli np. przy usłudze IaaS Bank typowo będzie odpowiadał za zarządzanie systemem operacyjnym lub bazą danych.



Źródło: opracowanie własne – przykładowy model może się różnić w zależności od potrzeb Banku.

3.2.2. **Złożoności** – środowiska chmurowe są bardziej dynamiczne i złożone w zarządzaniu, monitorowaniu, utrzymaniu niż środowiska on-prem, w szczególności w przypadku architektury hybrid multicloud.

3.2.3. **Uzależnienia od Dostawcy (vendor lock-in)** – ryzyko związane z uzależnieniem od jednego Dostawcy usługi chmury obliczeniowej, które może utrudniać migrację, wyjście z usługi lub wpłynąć na znaczący wzrost kosztów takich usług.

3.2.4. **Zgodności** – przestrzeganie powszechnie obowiązujących przepisów prawa, zarówno krajowych (np. Prawo Bankowe), jak i unijnych (np. RODO, DORA), a także wytycznych organów nadzoru (np. EBA), zwłaszcza dokumentowanie zgodności w tym zakresie oraz prowadzenie cyklicznych audytów.

3.3 Bank w procesie szacowania ryzyka, opierając się na Ex-ante risk assessment, klasyfikacji informacji oraz ocenie ryzyka Due Diligence, identyfikuje i nazywa ryzyka, a w następnym kroku przeprowadza ich analizę.

3.4 Szacowanie ryzyka powinno przebiegać macierzowo poprzez pryzmat zagrożeń i podatności oraz przeprowadzenia oceny prawdopodobieństwa wystąpienia, a także potencjalnego wpływu na organizację w skali trzystopniowej lub innej przyjętej przez Bank:

3.4.1. wysoki,

3.4.2. średni,

3.4.3. niski.

3.5 Po przeprowadzeniu powyższej oceny Bank dokonuje oceny wyboru strategii zarządzania ryzykiem:

a) **akceptacja ryzyka** – występuje, gdy potencjalny wpływ jest niski / nieistotny, a koszt minimalizacji ryzyka przewyższa korzyści lub Bank jest w stanie zaakceptować to ryzyko, gdyż nie ma realnej alternatywy,

b) **unikanie ryzyka** – rezygnacja z działań, które niosą ze sobą zbyt duże ryzyko (np. nieprzenoszenie krytycznych danych do chmury) lub ciążą na Banku wymogi regulacyjne, których Bank nie ma możliwości ograniczania,

c) **transfer / przesunięcie ryzyka** – przeniesienie ryzyka i odpowiedzialności na stronę trzecią poprzez współdzieloną odpowiedzialność z Dostawcą lub zabezpieczenie poprzez stosowne polisy ubezpieczeniowe, certyfikaty, postanowienia umowne, w tym warunki SLA,

d) **mitygacja ryzyka** – wdrożenie kontroli i zabezpieczeń w celu zmniejszenia prawdopodobieństwa wystąpienia ryzyka lub jego wpływu i negatywnych skutków z tym związanych.

3.6 W ramach analizy ryzyka Bank powinien uwzględnić wyniki klasyfikacji informacji, jak również rozwiązania ograniczające ryzyko (tzw. mityganty) stosowne do klas informacji i ryzyk, w szczególności rodzaj szyfrowania informacji przetwarzanych w Usłudze chmury obliczeniowej. Szczegółowe rekomendacje w zakresie szyfrowania informacji są zawarte w Części V pkt 2. Standardu.

3.7 Analiza ryzyka może być realizowana na poziomie pojedynczego zasobu, katalogu Usług ICT lub grupy rozwiązań z uwzględnieniem różnych klas przetwarzanych informacji.

3.8 Wyniki analizy ryzyka powinny zostać udokumentowane. Bank opisuje w szczegółowy sposób zaadresowania ryzyka lub odstępstwa wraz z argumentacją i okresem jego trwania. Zgodnie z DORA, szacowanie ryzyka powinno uwzględniać ocenę ryzyk inherentnych i rezydualnych.

3.9 Szablon szacowania ryzyka znajduje się w Załączniku nr 9 do Standardu. Zawiera on praktyczne przykłady ryzyk oraz ich ograniczania.

4. PLAN AUDYTU

4.1 Na podstawie wyników szacowania ryzyka Bank określa zakres oraz częstotliwość audytu Dostawcy (zob. przykładowo Tabela 1.).

Tabela 1 – Przykład częstotliwości audytu Dostawcy

Wynik szacowania ryzyka	Rodzaj przeprowadzanej kontroli	Częstotliwość	Wymagania pozyskania dokumentacji od Dostawcy	Alternatywne zastąpienie audytów lub kontroli analizą raportu atestacyjnego
Wysoki	Audyt	1 rok	tak	tak
Średni	Audyt	2 lata	tak	tak
Niski	Kontrola (weryfikacja samooceny)	3 lata	nie	tak

4.2 Na podstawie informacji dotyczących rodzaju i częstotliwości audytów Bank opracowuje plan audytów i kontroli dla Dostawcy, określając ich dopuszczalną formę:

4.2.1. audyt fizyczny i niezależne przeprowadzone oceny polegające na ocenie dokumentów (w formie polityk, procedur i innych dokumentów) przedstawionych przez Dostawcę przez sam Bank lub na zlecenie firmy trzeciej,

4.2.2. wykorzystanie niezależnych sprawozdań sporządzonych w imieniu Dostawcy,

4.2.3. wykorzystanie sprawozdań z audytu wewnętrznego Dostawcy,

4.2.4. wykorzystanie certyfikacji i atestacji Dostawców wydanych przez niezależnych audytorów, np. raporty SOC 1, SOC 2,

4.2.5. inne niezależne źródła akceptowane przez Bank i otoczenie.

4.3 Audyt jest przeprowadzony dla tych samych obszarów, dla których przeprowadzona była analiza Due Diligence oraz szacowanie ryzyka chmurowego. Szczegółowe wymogi w zakresie prowadzenia audytu Dostawcy zostały określone w Części IV pkt 4. Standardu.

5. WYMOGI DLA UMOWY

5.1 Na podstawie Ex-ante risk assessment Bank powinien znać kwalifikację prawną usługi chmury obliczeniowej, a w konsekwencji zakres wymogów kontraktowych, jakie znajdą do niej zastosowanie. Wymogi wynikające z DORA oraz w zakresie outsourcingu regulowanego zostały omówione odpowiednio w Części II pkt 4. Standardu.

5.2 Zestawienie kluczowych wymogów umownych wraz ze szczegółowym komentarzem znajduje się w Załączniku nr 3 do Standardu. Ponad wymogi regulacyjne, w zakresie wskazanym w załączniku, rekomendujemy uwzględnienie wybranych wymogów z Komunikatu chmurowego, jako stanowiących wyraz najlepszych praktyk w zakresie cloud governance.

5.3 Przed zawarciem umowy należy dokonać analizy zgodności treści umowy z wymogami prawnymi oraz wymaganiami określonymi przez Bank.

5.4 Rekomenduje się, aby prawem właściwym dla umowy na usługi chmury obliczeniowej

było prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a Bank przeanalizował, czy postanowienia umowy są skuteczne i egzekwowalne, a przepisy prawa państwa trzeciego nie uniemożliwiają wykonywania przewidzianych w umowie praw organu nadzoru w zakresie audytu lub inspekcji Dostawcy.

6. ZAWIADOMIENIE ORGANU NADZORU (NOTYFIKACJA)

6.1 W określonych przepisami prawa przypadkach Bank ma obowiązek zawiadomić organ nadzoru (KNF) o określonych zdarzeniach związanych z zawarciem umowy na usługi chmury obliczeniowej (jak np. jej zawarcie lub zmiana kwalifikacji).

6.2 Zakres takich przypadków, terminy, treść i sposób zgłoszenia zostały omówione szczegółowo w Załączniku nr 4 do Standardu.

7. WYMOGI DLA DOSTAWCY USŁUGI CHMURY OBLICZENIOWEJ

7.1 Poniższy materiał dotyczy Dostawcy usługi chmury obliczeniowej we wszystkich modelach (IaaS / PaaS / SaaS).

7.2 Wybór Dostawcy usługi chmury obliczeniowej to strategiczna decyzja, która wymaga dokładnej analizy i uwzględnienia wielu aspektów, w szczególności formalno-prawnych, które mogą mieć znaczącą rolę w szacowaniu ryzyka i przeprowadzeniu oceny Due Diligence.

7.3 **Matryca wymogów prawnych.** Bank w procesie wyboru Dostawcy i kontraktacji usług chmury obliczeniowej powinien kompleksowo przeprowadzić analizę, dla której pomocna może być matryca regulacji stanowiąca Załącznik 2 do Standardu, tak by zastosować odpowiednie wytyczne i wymagania umowne w stosunku do Dostawcy usług chmury obliczeniowej i by skutecznie zabezpieczyć ryzyka i interes Banku.

7.4 W tym celu pomocne mogą być wytyczne określone poniżej, które Bank powinien uwzględnić na etapie wyboru Dostawcy:

7.4.1. lokalizacja przetwarzania danych Banku,

7.4.2. dostęp do danych Banku oraz konfiguracja usługi chmury obliczeniowej, jaką Dostawca tej usługi dostarcza Bankowi,

7.4.3. poddostawcy,

7.4.4. kompetencje,

7.4.5. kryptografia,

7.4.6. plan ciągłości działania,

7.4.7. zarządzanie incydentami,

7.4.8. testowanie odporności cyfrowej,

7.4.9. dodatkowa dokumentacja.

7.5 Więcej w zakresie szczegółowych wytycznych znajduje się w Załączniku nr 8 do Standardu dla poszczególnych sekcji.

7.6 W przypadku usługi chmury obliczeniowej wspierającej funkcję krytyczną lub istotną Banku:

7.6.1. Dostawca zapewnia możliwość pilnego odzyskania danych Banku w przypadku ogłoszenia upadłości przez Dostawcę.

7.6.2. Dostawca zobowiązuje się uczestniczyć w testach TLPT prowadzonych przez Bank lub na żądanie Banku, które obejmują udostępnianą przez niego usługę w chmurze, i gwarantuje pełną współpracę w tym zakresie.

7.7 Bank, w zależności od oceny ryzyka, podejmuje decyzję o konieczności częściowego lub pełnego spełnienia ww. wymagań przez Dostawcę usługi w chmurze.

7.8 Spełnienie części lub całości wymagań może być poświadczone przez Dostawcę usługi w chmurze odpowiednimi certyfikatami zgodności wystawionymi przez niezależne jednostki certyfikujące, akredytowane w polskim lub europejskim systemie akredytacji.

7.9 **Rekomendowane normy.** W zakresie świadczonych usług chmury obliczeniowej i odpowiednio do ich skali Dostawca może potwierdzić spełnienie wymagań, zapewniając zgodność swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że Bank akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części:

7.9.1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT,

7.9.2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji,

7.9.3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania,

7.9.4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej,

7.9.5. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.

7.10 **Rekomendowane normy dla CPD.** Odpowiedni poziom bezpieczeństwa CPD Dostawcy usługi chmury obliczeniowej może potwierdzać spełnienie 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. Bank może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań.

7.11 Powyższe rekomendacje określone w pkt 7.9 – 7.10 Standardu dotyczą zarówno przypadku podjęcia współpracy bezpośrednio z Dostawcą usług w chmurze, jak i Dostawcą usług

innych niż Usługi w chmurze (w tym usługi nie-ICT), który wykorzystuje Usługi w chmurze do świadczenia Usługi ICT innej niż Usługa w chmurze na rzecz Banku.

7.12 **Zapewnienie zgodności.** W zależności od decyzji Banku, Dostawca Usługi chmury obliczeniowej powinien zobowiązać się w umowie do zapewnienia zgodności Usługi chmury obliczeniowej z wymaganiami Banku, w tym wymaganymi przez Bank normami lub ich odpowiednikami (np. normami BS, normami PN-ISO, itp.).

7.13 Zapewnienie zgodności może być realizowane poprzez uzyskanie przez Dostawcę usługi chmury obliczeniowej niezależnej certyfikacji (wydanej przez jednostkę certyfikującą), a w przypadku, gdy Dostawca usługi chmury obliczeniowej nie posiada formalnej certyfikacji, powinien on wykazać zgodność z ww. normami poprzez udokumentowanie realizacji poszczególnych wymagań norm lub odpowiednich wymagań Banku.

7.14 Zakres certyfikacji powinien obejmować w całości usługę chmury obliczeniowej świadczoną na rzecz Banku, w szczególności dotyczy to wszystkich CPD, w których przetwarzane są dane (informacje) Banku w ramach realizacji takiej usługi.

7.15 Dokumentacja związana z certyfikacją, tj. certyfikat oraz wyniki audytów certyfikacyjnych lub dokumentacja zgodności dostarczona przez Dostawcę usługi chmury obliczeniowej, powinny być przekazane przed zawarciem umowy, a później udostępniane Bankowi co najmniej raz w roku i na każde żądanie.

7.16 W ramach procesu audytowania Dostawców Bank powinien regularnie weryfikować dokumentację związaną z certyfikacją Dostawcy. W przypadku gdy ww. dokumentacja wykaże istotne niezgodności Bank powinien uzgodnić z Dostawcą usługi chmury obliczeniowej plan naprawczy oraz monitorować jego realizację.

7.17 Jeśli Dostawca usługi chmurowej korzysta z Poddostawców świadczących na jego rzecz usługi chmury obliczeniowej (np. przy modelu SaaS), powinien zagwarantować zgodność Poddostawców z powyższymi wymaganiami.

7.18 **Zgodność z Data Act.** W związku z wymaganiami dla Dostawców usług przetwarzania danych, do których można zasadniczo zaliczyć Dostawców usług chmury obliczeniowej, tacy Dostawcy powinni dochować wynikających z tego rozporządzenia obowiązków, w szczególności:

7.18.1. udostępnić Bankowi, zgodnie z art. 26 oraz art. 28 Data Act:

a) informacje o istniejących procedurach zmiany Dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany Dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych Dostawcy usług przetwarzania danych,

b) odniesienie do aktualnego rejestru internetowego prowadzonego przez Dostawcę usług przetwarzania danych ze szczegółowymi informacjami o wszelkich strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne, o których mowa w art. 25 ust. 2 lit. e) Data Act,

c) poprzez swoją stronę internetową informacje dotyczące:

i. jurysdykcji, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług,

ii. ogólnego opisu środków technicznych, organizacyjnych i umownych przyjętych przez Dostawcę usług przetwarzania danych w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie UE lub ich przekazania administracji rządowej, w przypadku gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa UE lub prawa krajowego danego państwa członkowskiego.

7.18.2. dostosować treść umowy do wymogów przewidzianych w art. 25 Data Act, m.in.:

a) poprzez postanowienia umowne umożliwiające Bankowi na wniosek zmianę Dostawcy usług przetwarzania danych na innego Dostawcę usług przetwarzania danych lub przeniesienie wszystkich danych eksportowalnych i aktywów cyfrowych do lokalnej infrastruktury ICT, w terminach przewidzianych w Data Act;

b) zapewnienie:

i. uzasadnionej pomocy w procesie zmiany Dostawcy,

ii. kontynuowania świadczenia usługi,

iii. przedstawienia jasnych informacji o znanych zagrożeniach dla ciągłości świadczenia usługi przez Dostawcę,

iv. utrzymania wysokiego poziomu bezpieczeństwa danych podczas ich przekazywania.

7.18.3. zapewnić ekstrakcję danych do uporządkowanego, powszechnie używanego formatu nadającego się do odczytu maszynowego, jeśli Bank wyrazi taką potrzebę;

7.18.4. usuwać istniejące przeszkody, a także nie nakładać nowych przeszkód, w przypadku decyzji Banku o:

a) przejściu na lokalną infrastrukturę ICT,

b) zmianie usługi na usługę tego samego typu świadczoną przez innego Dostawcę,

c) korzystaniu z usług kilku Dostawców równocześnie, a w tym przypadku również Dostawca musi przedstawić Bankowi informacje o znanych zagrożeniach dla ciągłości świadczenia usług po swojej stronie oraz ułatwić proces zmiany Dostawcy, zapewniając zasoby, odpowiednie informacje, dokumentację, wsparcie techniczne oraz w stosownym przypadku niezbędne narzędzia.

7.18.5. zagwarantować całkowite usunięcie wszystkich danych eksportowalnych i aktywów cyfrowych wygenerowanych bezpośrednio przez Bank lub bezpośrednio dotyczących Banku po upływie okresu pobierania pod warunkiem, że Bank poinformuje o pomyślnym ukończeniu procesu zmiany Dostawcy;

7.18.6. uzgodnić z Bankiem na etapie zawarcia umowy: procedury inicjowania zmiany Dostawcy usługi chmury obliczeniowej, formaty danych nadające się do odczytu maszynowego, do których mogą być wyeksportowane dane Banku, narzędzia przeznaczone do eksportowania danych, w tym otwarte interfejsy oraz informacje o zgodności z normami zharmonizowanymi lub wspólnymi specyfikacjami opartymi na otwartych specyfikacjach w zakresie interoperacyjności, informacje o znanych ograniczeniach technicznych, które mogą wpłynąć na proces zmiany Dostawcy usługi chmury obliczeniowej, a także szacowany czas trwania procesu zmiany Dostawcy;

7.18.7. zapewnić zgodność oferowanej usługi chmury obliczeniowej z otwartymi specyfikacjami w zakresie interoperacyjności, zgodnie z załącznikiem II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012;

7.18.8. zapobiegać niezgodnemu z prawem EU dostępowi administracji rządowej państwa trzeciego do danych nieosobowych Banku.

8. DODATKOWE WYMAGANIA DLA DOSTAWCY ROZWIĄZANIA ICT W ŚRODOWISKACH CHMUROWYCH ZARZĄDZANYCH PRZEZ BANK

8.1 Poniższe rekomendacje dotyczą dostawców rozwiązań dostarczanych w środowisku chmury obliczeniowej, innych niż rozwiązania SaaS (np. dostawcy usług zarządzanych, aplikacji uruchamianej na chmurze obliczeniowej zarządzanej przez Bank w modelu IaaS/PaaS).

8.2 Rekomenduje się, aby dostawca tego typu rozwiązania zapewnił, że:

8.2.1. Rozwiązanie jest zaprojektowane tak, by dało się je następnie uruchomić z kodu (jeśli jest to technicznie możliwe).

8.2.2. Rozwiązanie ma aktywne wsparcie producenta w zakresie bezpieczeństwa i rozwoju oprogramowania (jeśli dotyczy).

8.2.3. Oprogramowanie, biblioteki, obrazy maszyn wirtualnych oraz skrypty uruchamiane w rozwiązaniu pochodzą z centralnego, autoryzowanego w Banku repozytorium artefaktów.

8.2.4. Klucze do szyfrowania danych w spoczynku są zabezpieczone przed nieuprawnionym dostępem, zmianą lub usunięciem, a jeśli to możliwe technicznie – że Bank nimi zarządza.

8.2.5. Dostęp sieciowy do rozwiązania jest zarządzany poprzez reguły sieciowe zgodnie z zasadą minimalnych uprawnień.

8.2.6. Rozwiązanie ma włączone logowanie zdarzeń audytowych i bezpieczeństwa.

8.2.7. Klucze, hasła, sekrety i inne ciągi znaków używane do uwierzytelniania lub autoryzacji są chronione przed niepowołanym dostępem, modyfikacją lub usunięciem.

8.3 Jeśli rozwiązanie będzie udostępniane przez Bank dla podmiotu, który podlega pod DORA (np. spółka córka będąca podmiotem finansowym w rozumieniu DORA), Bank powinien rozważyć i przeanalizować, czy taki podmiot traktować jako Dostawcę usługi chmury obliczeniowej, a rozwiązanie jako usługę chmury obliczeniowej. W przypadku pozytywnej kwalifikacji rozwiązanie i Bank powinny spełnić wymagania z Części IV pkt 7. Standardu „Wymagania dla Dostawcy usługi w chmurze", z perspektywy innego podmiotu regulowanego.

8.4 W zależności od zakresu usługi dostawca rozwiązania może być traktowany jako dostawca Usługi ICT innej niż usługa w chmurze. W takiej sytuacji dostawca rozwiązania i świadczona usługa mogą podlegać pod DORA w sposób adekwatny do tego typu usługi.

8.5 Rozwiązanie należy traktować jako Usługę ICT i musi ono spełniać wszystkie wymagania przedstawione w DORA dla Usług ICT świadczonych przez zewnętrznego dostawcę, jak również inne ewentualne wymogi prawne.

9. STRATEGIA WYJŚCIA

9.1 Strategia i plan wyjścia z usług chmury obliczeniowej to zestaw czynności, procedur i działań, które mają na celu zapewnić bezpieczne, efektywne i minimalizujące zakłócenia ciągłości działania usług, w szczególności Usług ICT) oraz ich przeniesienie z jednego środowiska chmurowego do innego alternatywnego – chmurowego lub on-prem. Rekomendowane jest, aby Strategia wyjścia była osobnym dokumentem lub była co najmniej wyraźnie oznaczona w planie wyjścia.

9.2 Bank w procesie opracowywania strategii i planów wyjścia powinien je zdefiniować tak, by zabezpieczyć i zminimalizować ryzyko utraty kontroli nad danymi, zasobami oraz aplikacjami. W zależności od scenariusza wybranego przez Bank stosuje on odpowiednie podejście.

9.3 Zgodnie z DORA, Bank musi przygotować strategię wyjścia dla każdej krytycznej Usługi ICT oraz testować plan wyjścia w określonych cyklach. Strategie wyjścia dla usług w chmurze wspierających funkcję krytyczną lub istotną Banku powinny być spójne z przepisami wewnętrznymi w zakresie DORA.

9.4 Ze względu na charakter usług w chmurze zaleca się, aby dla każdej Usługi ICT wspierającej funkcję krytyczną lub istotną Banku, będącej usługą w chmurze, została przygotowana Strategia wyjścia, natomiast pozostałych (niekrytycznych) usług w chmurze zaleca się przygotowanie podstawowego zbioru informacji mających na celu ułatwienie wyjścia z usługi.

9.5 Bank powinien określić kierunek wyjścia z usługi zgodnie z możliwościami technologicznymi oraz zachowaniem właściwego poziomu bezpieczeństwa, np. przeniesienie funkcjonalności rozwiązania do innego Dostawcy usług chmurowych, przeniesienie funkcjonalności rozwiązania do środowisk on-premise, rezygnacja z rozwiązania, itp.

9.6 Bank powinien przygotować Strategię wyjścia zarówno na potrzeby planowanej rezygnacji z usług chmurowych, jak i na sytuacje awaryjne, jeżeli jest to technologicznie możliwe.

9.7 Dopuszcza się przygotowanie alternatywnych strategii wyjścia w zależności od kierunku wyjścia z usługi chmurowej.

9.8 Podstawowy zbiór informacji, który powinien być zawarty w planie wyjścia, powinien zawierać minimum:

9.8.1. informacje o aktualnych administratorach rozwiązania zarówno po stronie Banku, jak i Dostawcy, jeżeli taki został wskazany,

9.8.2. zestaw stanowisk, które będą niezbędne do zaangażowania w realizację strategii wyjścia oraz o ile to możliwe orientacyjną pracochłonność,

9.8.3. dane techniczne na temat aktualnego rozwiązania: lokalizacja zasobów, wykorzystywane licencje i komponenty dostępne w ramach danej platformy, informacje na temat infrastruktury i łącza,

9.8.4. mapowanie wskazanych powyżej danych technicznych na nowe rozwiązanie,

9.8.5. retencję danych,

9.8.6. miejsca do weryfikacji przez zespoły bezpieczeństwa w zakresie usuniętych danych i komponentów,

a) orientacyjne koszty związane z wykonaniem planu wyjścia w podziale na: pracochłonność, infrastrukturę i licencje, audyt oraz inne pozostałe w zależności od migrowanej usługi chmurowej;

9.8.7. Plan wyjścia powinien być możliwie dokładny (ważne jest np. uwzględnianie zmian kosztów infrastruktury lub pracochłonności, określenie czasu dla danego etapu harmonogramu migracji itp.).

9.8.8. Bank powinien przeprowadzić weryfikację i aktualizację zawartych w planie wyjścia informacji w cyklach odpowiadających wynikom szacowania ryzyka, przy czym rekomenduje się nie rzadziej niż co roku i przy każdej istotnej zmianie w usłudze.

9.8.9. W ramach planu wyjścia powinien zostać przygotowany ramowy scenariusz migracji jako schematyczny harmonogram prac w podziale na etapy. Harmonogram powinien rozpoczynać się od podjęcia decyzji o wyjściu z chmury, a kończyć na usunięciu środowisk chmurowych, danych i uzyskaniu potwierdzenia o bezpowrotnym usunięciu danych.

9.9 Bank powinien zagwarantować sobie na poziomie umowy:

9.9.1. wydanie loginów i haseł,

9.9.2. zwrot sprzętu, jeżeli takowy został przekazany,

9.9.3. zwrot dokumentacji papierowej,

9.9.4. możliwość pobrania danych powierzonych w ramach usług w chmurze we wskazanym terminie,

9.9.5. nieodwracalne usunięcie danych powierzanych w ramach usługi w chmurze z infrastruktury Dostawcy (Poddostawcy) wraz z formalnym potwierdzeniem realizacji czynności,

9.9.6. wsparcie w zakresie wyjścia z usługi (w tym Usługi ICT), o ile to technicznie możliwe i potrzebne,

9.9.7. możliwość ciągłego i nieprzerwanego korzystania z usługi w chmurze na czas realizacji strategii wyjścia, o ile to technicznie możliwe i potrzebne.

9.9.8. możliwość testowania planu wyjścia.

9.10 Testowanie planu wyjścia

9.10.1. Dla planu wyjścia krytycznych z usług w chmurze należy również przygotować test planu wyjścia. Test może być realizowany na trzy sposoby określone w Tabeli 2. poniżej. Bank w swojej ocenie powinien zdecydować, jaka forma jest właściwa, uwzględniając przy tym optymalne zarządzanie kosztami i zaangażowaniem ludzi oraz ryzyko. Rekomendowana jest realizacja testów planu wyjścia poprzez testowanie możliwie szerokiego spektrum scenariuszy migracji, adekwatnie do wyników szacowania ryzyka oraz możliwości organizacyjnych, technicznych i finansowych. Dzięki temu można zweryfikować poprawność całego scenariusza migracji tam, gdzie to technicznie możliwe (np. test migracji lub usunięcia danych, weryfikacja powołania komponentu chmurowego u innego dostawcy i potwierdzenie działania).

9.10.2. Testy planu wyjścia należy wykonywać w cyklach rocznych, za każdym razem zmieniając scenariusz testu.

9.10.3. Test planu wyjścia powinien określać wymagane osoby i czas do przeprowadzenia testu, etapy testu wraz z oczekiwanym rezultatem oraz problemy, które mogą się pojawić w trakcie testu, i planowany sposób poradzenia sobie z każdym problemem.

9.10.4. W przypadku negatywnego wyniku testu zaleca się weryfikację jego przyczyn oraz aktualizację planu wyjścia opartego na wnioskach.

Tabela 2. Typy testów

Typ testu	Opis podejścia	Zalety	Wady
Symulacja	Bank przeprowadza weryfikację procedur i założeń operacyjnych, opierając się na środowisku chmury obliczeniowej poprzez testowanie planu w sposób proceduralny.	• Ograniczenie kosztów. • Możliwość zidentyfikowania obszarów wydłużających proces w zakresie akceptacji.	• Nie sięga do czynności praktycznych. • Nie pozwala zweryfikować założeń technicznych i ich aktualności. • Nie pozwala określić faktycznej pracochłonności.
Teoretyczny *"Gra sztabowa"*	Bank, opierając się na założeniach planu wyjścia, omawia z dedykowanym zespołem do jego wykonania poszczególne etapy strategii poprzez jego teoretyczne przejście.	• Ograniczenie kosztów. • Możliwość zidentyfikowania obszarów wydłużających proces w zakresie akceptacji. • Test weryfikuje, czy zostały wpisane właściwe osoby do planu.	• Nie sięga do czynności praktycznych. • Nie pozwala zweryfikować założeń technicznych i ich aktualności. • Nie pozwala określić faktycznej pracochłonności.
Praktyczna realizacja	Bank, opierając się na założeniach planu wyjścia, przeprowadza test w całości lub w wybranym elemencie wraz z uczestnikami oraz weryfikacje poprawność ról i odpowiedzialności w scenariuszu wyjścia.	• Test weryfikuje, czy oczekiwania są spójne z uzyskanym efektem. - Wnioski z testu pozwalają poprawić strategie. • Utrudnienie w realizacji ze względu na wymóg poświęcenia dodatkowego czasu pracownika.	• Niesie za sobą dodatkowe koszty. • Utrudnienie w realizacji ze względu na wymóg poświęcenia dodatkowego czasu pracownika.

Szablon podstawowych, praktycznych i niezbędnych danych do uwzględnienia w planie wyjścia znajduje się w Załączniku nr 6 do Standardu.

CZĘŚĆ V

WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI W CHMURZE

1. WPROWADZENIE

1.1 Rozporządzenie DORA wymusza na Bankach (i ich Dostawcach usług chmury obliczeniowej) proaktywne zarządzanie ryzykiem cyfrowym, którego nierozłącznym elementem jest bezpieczeństwo. DORA także w swoim rozumieniu przenosi określone odpowiedzialności za bezpieczeństwo cyfrowe na Banki, zatem te nie powinny bazować wyłącznie na zapewnieniach Dostawcy usług chmury obliczeniowej, ale także aktywnie działać. W związku z powyższym polityka i zarządzanie bezpieczeństwem chmury obliczeniowej powinny być kompleksowe. W ramach Części V opisujemy szereg aspektów, które rekomendujemy uwzględnić w zakresie procesów związanych z bezpieczeństwem i zarządzaniem chmurą obliczeniową.

2. ZARZĄDZANIE BEZPIECZEŃSTWEM USŁUG CHMURY OBLICZENIOWEJ

2.1 Mechanizmy bezpieczeństwa zastosowane w rozwiązaniu muszą być dobrane adekwatnie do zakresu wykorzystywanych usług chmury obliczeniowej, zakresu i klasyfikacji przetwarzanych informacji, ich krytyczności oraz wyników przeprowadzonej analizy ryzyka.

2.2 Zarządzanie Tożsamością i Dostępem (IAM):

2.2.1. Bank musi stosować Zasadę Najmniejszego Przywileju (Principle of Least Privilege – PoLP).

2.2.2. Zaleca się wprowadzenie polityki nadawania dostępu Just-in-Time (JIT) / Dostępu Tymczasowego (Temporary Access): Przyznawanie podwyższonych uprawnień tylko na określony czas i tylko wtedy, gdy są one faktycznie potrzebne, z wycofaniem po upływie czasu.

2.2.3. Zaleca się regularne audyty systemów dostępu i weryfikację, czy przyznane uprawnienia są spójne z faktycznymi potrzebami biznesowymi i rolami użytkowników – np. raz w roku.

2.2.4. Logi z systemów zarządzania tożsamością i dostępem (np. IAM) muszą być zbierane i archiwizowane z odpowiednią retencją zgodnie z polityką Banku.

2.2.5. Zaleca się stosowanie scentralizowanego systemu zarządzania dostępem.

2.2.6. Zaleca się stosowanie mechanizmów MultiFactor Authentication (MFA).

2.3 Zarządzanie Podatnościami i Konfiguracją Bezpieczeństwa:

2.3.1. Bank powinien posiadać proces zapewniający zbieranie informacji o zasobach – monitorowanie zasobów, zarządzanie licencjami, zarządzanie pojemnością (auto scaling).

2.3.2. Bank powinien posiadać politykę zarządzania zmianą i łatania luk, w tym:

a) Jasno zdefiniowane procedury i ramy czasowe dla wdrożenia łatek:

i. krytycznej ważności: natychmiast (np. do 24–48 godzin)
ii. wysokiej ważności: np. do 7 dni
iii. średniej/niskiej ważności: np. do 30 dni

2.3.3. Przed wdrożeniem łatek w środowiskach produkcyjnych muszą one być przetestowane w środowiskach testowych/rozwojowych, aby zapobiec regresjom i problemom z kompatybilnością.

2.3.4. Bank powinien wdrożyć kompleksową politykę zarządzania bezpieczeństwem Usług ICT / usług chmury obliczeniowej, która obejmuje:

a) identyfikację luk w zabezpieczeniach,
b) wykrywanie i zarządzanie incydentami bezpieczeństwa – skuteczne łatanie zmniejsza ryzyko wystąpienia incydentów,
c) prowadzenie rejestru aktywów ICT i ich wspieranie przez aktualizacje.

2.3.5. Zaleca się prowadzenie rejestru zarządzanych podatności.

2.3.6. Zaleca się udokumentowanie polityki zarządzania odstępstwami oraz jej okresowy przegląd, np. raz na rok.

2.3.7. Zaleca się okresową ocenę ryzyka luk.

2.4 Hardening usług i systemów:

2.4.1. Zaleca się stosowanie polityki Security by Design – wbudowywanie elementów bezpieczeństwa na każdym etapie cyklu życia aplikacji i infrastruktury, a nie dodawanie go na końcu.

a) Bank powinien posiadać procedurę mającą na celu wzmocnienie odporności (hardeningu) usług w chmurze.

2.4.2. Usługi w chmurze powinny być powoływane zgodnie z ustalonym wzorcem (hardeningiem).

2.4.3. Krytyczne Usługi ICT IaaS muszą być powoływane na bazie dopuszczonych obrazów systemów operacyjnych (konieczność używania ustandaryzowanych konfiguracji bazowych).

2.4.4. Zaleca się stosowanie przez instytucję zasady deny-by-default.

2.5 Szyfrowanie i zarządzanie kluczami kryptograficznymi.

2.5.1. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinny wynikać z analizy ryzyka. W szczególności należy wziąć pod uwagę:

a) szyfrowanie, zarówno podczas przesyłu, spoczynku, jak i przetwarzania („at rest", „in transit" oraz „in use"),

b) przekazanie Bankowi przez Dostawcę dokumentacji mechanizmów szyfrowania danych (informacji), a także mechanizmów weryfikacji poprawności konfiguracji i działania ww. mechanizmów,

c) posiadanie przez Bank kompetencji w zakresie poprawnej konfiguracji usług, w tym mechanizmów szyfrowania,

d) korzystanie przez Bank z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane,

e) zarządzanie kluczami szyfrującymi.

2.5.2. Bank powinien rozważyć opracowanie standardu (polityki) stosowania metod szyfrowania i zabezpieczania rozwiązań chmurowych.

2.5.3. W zależności od wyników analizy ryzyka Bank powinien zastosować adekwatny sposób szyfrowania, uwzględniając możliwości technologiczne i dostępne sposoby ochrony materiałów kryptograficznych (klucze, certyfikaty itp.):

a) ochrona klucza po stronie Dostawcy bazująca na oprogramowaniu (np. KMS),

b) ochrona klucza po stronie Banku bazująca na oprogramowaniu (np. KMS),

c) sprzętowa ochrona klucza po stronie Dostawcy (HSM),

d) sprzętowa ochrona klucza po stronie Banku (HSM).

2.5.4. Przy sprzętowej ochronie klucza rekomendowane jest stosowanie HSM spełniającego wymagania FIPS 140-2 Level 2 lub równoważne.

2.5.5. Gdy klucze są przechowywane po stronie Dostawcy, Bank powinien zweryfikować bezpieczeństwo sposobów zarządzania nimi przez Dostawcę (tj. generowanie, dystrybucja, rotacja, odwoływanie, niszczenie, dostęp, dostęp awaryjny). Można przy tym skorzystać z raportu niezależnego audytu, np. SOC 2 (System and Organization Controls Type 2).

2.5.6. Proces zarządzania tworzeniem, wykorzystaniem, ochroną, niszczeniem oraz zasady dostępu do kluczy szyfrujących powinny być udokumentowane i posiadać adekwatne mechanizmy kontrolne.

2.5.7. Adekwatnie do wyników analizy ryzyka rekomenduje się udokumentowanie zastosowanych rozwiązań szyfrowania danych.

2.6 Gromadzenie i rejestrowanie zdarzeń (logowanie).

2.6.1. W celu ochrony przed nieautoryzowanym dostępem oraz nadużyciami związanymi z przetwarzaniem danych, Bank powinien wdrożyć mechanizmy umożliwiające gromadzenie i rejestrowanie zdarzeń, adekwatnie do zakresu wykorzystywanych usług chmurowych, charakteru przetwarzanych informacji, ich krytyczności oraz wyników przeprowadzonej analizy ryzyka.

2.7 Podział odpowiedzialności w zakresie bezpieczeństwa i monitorowania zdarzeń pomiędzy Dostawcą usługi chmurowej a Bankiem musi być jednoznacznie określony.

2.7.1. Bank powinien posiadać udokumentowane zasady zbierania zdarzeń z określeniem zakresu zależnie od poziomu ryzyka, w szczególności z obszarów:

a) kontroli dostępu oraz zarządzania tożsamością,
b) zarządzania pojemnością i wydajnością,
c) zarządzania zmianą i konfiguracji usług chmurowych,
d) operacji ICT, w tym działań związanych z systemem ICT,
e) działań związanych z ruchem w sieci.

2.7.2. Bank zobowiązany jest do zapewnienia, aby mechanizmy gromadzenia i rejestrowania zdarzeń nie naruszały obowiązujących przepisów prawa, w szczególności w zakresie ochrony danych osobowych, tajemnicy bankowej oraz danych wrażliwych.

2.7.3. Rekomendowane jest wdrożenie adekwatnych środków ochrony dla gromadzonych zdarzeń, aby zabezpieczyć je przed manipulacją, usuwaniem i nieuprawnionym dostępem, zarówno podczas spoczynku (at rest), przesyłu (in transit), jak i przetwarzania (in use).

2.8 Bank powinien zapewnić spójność wszystkich wykorzystywanych usług chmury obliczeniowej ze stosowaną strefą czasową oraz wiarygodnym źródłem czasu referencyjnego w celu określenia precyzyjnej daty i godziny wystąpienia zdarzenia.

2.8.1. Okres przechowywania zdarzeń powinien być zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami prawa i wewnętrznymi politykami w tym zakresie.

2.9 Monitorowanie bezpieczeństwa.

2.9.1. Bank powinien posiadać zdolności i zasoby do monitorowania gromadzonych i rejestrowanych zdarzeń zgodnie z opracowanymi procedurami i zasadami bezpieczeństwa w celu identyfikacji incydentów związanych z bezpieczeństwem Banku i reagowania na nie.

2.9.2. Bank powinien stosować oraz dokumentować mechanizmy korelacji zdarzeń umożliwiające integrację informacji z różnych źródeł w celu identyfikacji incydentów.

2.9.3. Reguły korelacji powinny być regularnie przeglądane w celu zapewnienia ich aktualności i skuteczności. Przeglądy powinny być realizowane co najmniej raz w roku, w przypadku wystąpienia incydentu, a także po wdrożeniu istotnych zmian lub nowych systemów i usług chmurowych.

2.9.4. Bank odpowiada za monitorowanie skuteczności korelacji zdarzeń. Dla oceny skuteczności korelacji zdarzeń Bank powinien monitorować kluczowe parametry (KPI), na przykład czas od wystąpienia zdarzenia do wykrycia incydentu oraz liczbę fałszywych alertów (ang. *false positives*) w stosunku do wszystkich alertów.

2.10 Incydenty powinny być priorytetyzowane według opracowanej przez Bank klasyfikacji, opartej na m.in. krytyczności usług chmury obliczeniowej, klasyfikacji przetwarzanych informacji lub ryzyku biznesowym.

2.10.1. Rekomenduje się, aby Bank korzystał z centralnych rozwiązań:

a) klasy SIEM (Security Information and Event Management) do zarządzania i monitorowania zdarzeniami bezpieczeństwa,

b) klasy SOAR (Security Orchestration, Automation and Response) w celu automatyzacji zarządzania incydentami związanymi z bezpieczeństwem Banku.

2.10.2. Model wdrożenia tych rozwiązań (model chmurowy, model hybrydowy, model on-premise) pozostaje w gestii decyzji Banku.

2.10.3. Bank powinien cały czas dbać o utrzymywanie wysokiego poziomu świadomości w zakresie aktualnych oraz potencjalnych zagrożeń bezpieczeństwa, a także proaktywnie ich poszukiwać poprzez wykorzystanie dostępnych źródeł informacji oraz adopcję/wdrożenie procesów (np. Cyber Threat Intelligence, Indicators of Compromise, Threat Hunting).

2.11 Zarządzanie podatnościami.

2.11.1. Identyfikacja i ocena podatności.

a) Bank powinien posiadać proces zarządzania podatnościami obejmujący identyfikację, ocenę i remediację podatności w zakresie komponentów i konfiguracji pozostających pod jego kontrolą w środowisku chmurowym, zgodnie z modelem odpowiedzialności (Shared Responsibility Model – zob. Część IV pkt 4. Standardu).

b) Zakres odpowiedzialności Banku w identyfikacji podatności powinien być dostosowany do rodzaju usługi chmurowej:

i. IaaS – Bank odpowiada za identyfikację podatności w systemach operacyjnych, aplikacjach, konfiguracjach sieciowych oraz komponentach zarządzanych przez Bank,
ii. PaaS – Bank odpowiada za podatności w aplikacjach, kodzie, konfiguracjach platformy pozostających pod jego kontrolą oraz interfejsach API,
iii. SaaS – Bank odpowiada za bezpieczną konfigurację usługi i integrację, natomiast weryfikuje, czy Dostawca posiada proces zarządzania podatnościami oraz jest zobowiązany do raportowania podatności krytycznych zgodnie z umową.

c) Bank powinien zapewnić cykliczne skanowanie podatności w zakresie elementów pozostających pod jego kontrolą w modelach IaaS i PaaS.

d) W przypadku wykrycia podatności lub otrzymania informacji od Dostawcy usług chmurowych (np. SaaS) o podatności lub incydencie wpływającym na usługę, Bank powinien:

i. ocenić ryzyko wynikające z podatności w kontekście świadczonych usług i przetwarzanych danych,
ii. zweryfikować, czy Dostawca wdrożył działania naprawcze lub środki kompensacyjne w uzgodnionych terminach,
iii. wprowadzić dodatkowe mechanizmy ograniczające ryzyko po stronie Banku (np. zmiany konfiguracji, ograniczenie funkcjonalności, monitorowanie).

e) Oprócz cyklicznego skanowania podatności w przypadku wystąpienia szczególnych okoliczności, takich jak otrzymanie informacji o nowym krytycznym zagrożeniu (np. z Cyber Threat Intelligence), wykrycie incydentu bezpieczeństwa lub wprowadzenie istotnych zmian w środowisku chmurowym, Bank powinien przeprowadzić adekwatne skanowanie ad hoc w celu weryfikacji występowania podatności.

f) Zidentyfikowane podatności powinny być klasyfikowane pod kątem wpływu na bezpieczeństwo Banku i poziomu ryzyka, opierając się na uznanych standardach, np. CVSS (Common Vulnerability Scoring System) lub równoważnych metodach oceny podatności.

2.11.2. Zarządzanie aktualizacjami i usuwaniem podatności (remediacją).

a) Bank powinien posiadać udokumentowaną politykę i procedury w zakresie usuwania lub minimalizowania podatności (remediacji), obejmujące w szczególności:

(i) terminy usuwania podatności zależne od poziomu zagrożenia,
(ii) tryb postępowania w przypadku braku możliwości natychmiastowej eliminacji podatności (np. wdrożenie środków kompensacyjnych),
(iii) mechanizmy eskalacji w przypadku przekroczenia terminów remediacji.

b) Bank zobowiązany jest do weryfikacji skuteczności wprowadzonych poprawek (np. ponowne skanowanie).

c) Wdrożone mechanizmy i narzędzia aktualizacji muszą zapewniać integralność oraz autentyczność poprawek dostarczanych przez Dostawcę usług chmurowych lub producentów oprogramowania.

d) Wprowadzanie poprawek bezpieczeństwa powinno być realizowane zgodnie z procesem zarządzania zmianą, obejmującym w szczególności:

i. testowanie poprawek w środowisku testowym (jeśli jest dostępne),

ii. ocenę wpływu na działanie systemów i aplikacji,

iii. zatwierdzenie wdrożenia przez odpowiedzialne jednostki,

iv. weryfikację poprawności zastosowania poprawek po wdrożeniu (np. testy funkcjonalne).

2.12 Okresowe testowanie konfiguracji i mechanizmów bezpieczeństwa usług w chmurze.

2.12.1. Testy konfiguracji usług w chmurze.

a) Bank powinien posiadać proces okresowej weryfikacji konfiguracji usług chmurowych (np. IaaS, PaaS, SaaS) w celu zapewnienia ich zgodności z:

i. polityką bezpieczeństwa Banku,

ii. wymaganiami regulatorów i standardami branżowymi (np. CIS Benchmarks, CSA CCM).

b) Weryfikacja konfiguracji powinna obejmować w szczególności:

i. ustawienia kontroli dostępu i zarządzania tożsamością (IAM),

ii. konfiguracje sieciowe i zabezpieczenia transmisji danych,

iii. szyfrowanie danych (at rest, in transit, in use),

iv. konfigurację logowania i monitorowania zdarzeń.

c) Testy konfiguracji powinny być przeprowadzane:

i. cyklicznie (z częstotliwością adekwatną do krytyczności systemu i klasyfikacji przetwarzanych przez niego danych),

ii. ad hoc po wprowadzeniu istotnych zmian w usługach chmurowych,

iii. w przypadku otrzymania informacji o zagrożeniu związanym z konfiguracją z wiarygodnych źródeł (np. Cyber Threat Intelligence, ostrzeżenia regulatorów).

d) Bank powinien dokumentować wyniki testów konfiguracji, identyfikować niezgodności i wdrażać działania korygujące zgodnie z procesem zarządzania zmianą.

2.12.2. Testy mechanizmów bezpieczeństwa usług w chmurze.

a) Bank powinien realizować testy bezpieczeństwa środowisk chmurowych w zakresie elementów pozostających pod jego kontrolą, zgodnie z przyjętym modelem odpowiedzialności (Shared Responsibility Model):

- **i.** IaaS/PaaS – testy podatności, testy penetracyjne aplikacji i komponentów konfigurowanych przez Bank,
- **ii.** SaaS – testy konfiguracji (np. uprawnień), testy integracji z systemami Banku.

b) Testy bezpieczeństwa powinny być wykonywane:

- **i.** w cyklach określonych polityką bezpieczeństwa (z częstotliwością adekwatną do krytyczności systemu i klasyfikacji przetwarzanych przez niego danych),
- **ii.** po wdrożeniu istotnych zmian lub nowych usług chmurowych,
- **iii.** w przypadku wystąpienia incydentu bezpieczeństwa lub wykrycia podatności krytycznej.

c) Testy penetracyjne i testy odpornościowe w środowiskach chmurowych powinny być prowadzone przez wykwalifikowanych ekspertów (wewnętrznych lub zewnętrznych) z uwzględnieniem zasad uzgodnionych z Dostawcą chmury (np. warunki testów w umowie, zgody Dostawcy).

d) Wyniki testów bezpieczeństwa powinny być dokumentowane, a Bank powinien wdrażać plan remediacji w uzgodnionych terminach, opierając się na klasyfikacji ryzyka.

CZĘŚĆ VI

ZARZĄDZANIE CHMURĄ PO ZAWARCIU UMOWY

1. POLITYKA, ZARZĄDZANIE I UTRZYMANIE ŚRODOWISK CHMUROWYCH

1.1 Polityka, utrzymanie i zarządzanie środowiskami chmurowymi to istotny element całego procesu zarządzania chmury obliczeniowej, który zapewnia jej stabilność, wydajność, bezpieczeństwo, efektywność kosztów i wykorzystania usług w chmurze obliczeniowej. Proces ten obejmuje wiele powtarzalnych działań, które pozwalają Bankowi optymalnie zarządzać infrastrukturą i aplikacjami działającymi w chmurze obliczeniowej na wszystkich jego etapach.

1.2 Proces utrzymania możemy podzielić na pięć głównych etapów:

1.2.1. Zarządzanie i utrzymanie bezpieczeństwa,

1.2.2. Monitorowanie wydajności i dostępność usług,

1.2.3. Zarządzanie zmianą i konfiguracja środowisk chmurowych,

1.2.4. Zarządzanie danymi i ciągłość działania,

1.2.5. Polityka i zarządzanie aktywami ICT.

1.3 Bank powinien prowadzić na bieżąco pełną, aktualną inwentaryzację zasobów chmurowych (SaaS, PaaS, IaaS).

1.4 Środowiska chmurowe powinny być logicznie i funkcjonalnie separowane według ich przeznaczenia, np. produkcyjne (prod), przedprodukcyjne (pre-prod), testowe (test), deweloperskie (dev), laboratoryjne (lab) itp. Dodatkowo, zaleca się tworzenie podgrup zasobów dedykowanych konkretnym aplikacjom lub projektom.

1.5 Bank powinien utrzymywać procesy i narzędzia zapewniające zbieranie informacji o zasobach, monitorowanie zasobów, zarządzanie licencjami, zarządzanie pojemnością (w tym auto-scaling) oraz regularne przeglądy i aktualizacje rejestru – analogicznie jak w infrastrukturze lokalnej. Zaleca się automatyzację tych procesów.

1.6 Stosowane w środowiskach chmurowych mechanizmy tagowania mogą wspierać proces budowania wiedzy o zasobach i ich powiązań między sobą (np. powiązań dla konkretnej aplikacji biznesowej czy jej środowiska). Zaleca się, aby Informacje o zasobach zawierały następujące parametry:

1.6.1. nazwa zasobu,

1.6.2. typ usługi (IaaS/PaaS/SaaS),

1.6.3. identyfikator zasobu (ID),

1.6.4. środowisko – prod / pre-prod / dev / test / QA,

1.6.5. właściciel biznesowy i techniczny,

1.6.6. status zasobu – aktywny / wycofywany / do usunięcia / niezarządzany,

1.6.7. data utworzenia i ostatniej modyfikacji,

1.6.8. klasyfikacja przetwarzanych danych – np. dane osobowe, tajemnica bankowa, publiczne,

1.6.9. lokalizacja geograficzna (region chmurowy).

1.7 Szczegóły dotyczące sposobu budowania bazy wiedzy o zasobach, wykorzystywanych narzędzi czy zestawu parametrów pozostają w gestii Banku.

1.8 Budowana baza wiedzy o zasobach powinna zawierać niezbędne informacje dla procesów bezpieczeństwa, które będą z niej korzystać, np. monitorowania bezpieczeństwa i zarządzania incydentami bezpieczeństwa, zarządzania podatnościami, zarządzanie konfiguracją.

1.9 Bank powinien monitorować i kontrolować zużycie środków finansowych w chmurze, identyfikując ryzyka związane z przekroczeniem budżetu (np. przez niekontrolowane zużycie zasobów) oraz wdrażać limity kosztowe, alerty i scenariusze awaryjne zapewniające ciągłość działania usług.

1.10 Bank powinien zapewniać oraz dokumentować środki i metody ochrony zasobów chmurowych, a także danych przez nie przetwarzanych, które są dopasowane do właściwości poszczególnych zasobów np. typu usługi (IaaS, PaaS, SaaS), poziomu klasyfikacji danych, rodzaju środowiska itp.

1.11 Bank powinien monitorować planowane przerwy i zmiany w usługach realizowane przez Dostawcę usługi w chmurze (np. prace serwisowe, aktualizacje, zastąpienie), identyfikować ich wpływ na własne zasoby oraz testować zmiany zgodnie z poziomem ryzyka danego systemu.

1.12 Stosowanie usług w wersji preview na środowiskach innych niż testowe powinno być przedmiotem analizy ryzyka.

2. MONITORING WYDAJNOŚCI I DOSTĘPNOŚCI USŁUG

2.1 **Metryki operacyjne i wydajnościowe.** Bank powinien posiadać standard, który określa praktyki dotyczące zbierania, przechowywania i prezentacji metryk operacyjnych i wydajnościowych dla środowiska produkcyjnego.

2.2 Monitoring w pierwszej kolejności powinien być oparty na mechanizmach istniejących już w danej chmurze.

2.3 Monitoring musi umożliwić (np. wystawiając metryki po API) integrację z obecnie już istniejącymi systemami monitorowania w instytucji.

2.4 Wdrożony system monitoringu (np. APM) powinien śledzić kluczowe metryki wydajnościowe (CPU, RAM, I/O, czas odpowiedzi, liczba błędów) dla wszystkich komponentów infrastruktury i aplikacji w czasie rzeczywistym.

2.5 Zaleca się wykorzystywanie rozwiązań globalnych, które pozwolą wizualizować metryki i kontynuować monitoring w przypadku zmiany środowiska danego rozwiązania.

2.6 Proces monitorowania musi zapewniać pełną widoczności działania systemów i aplikacji, tak aby umożliwiać szybką identyfikację i rozwiązywanie problemów, a także optymalizację wydajności. W tym celu instytucja powinna budować metryki:

2.6.1. Metryki Infrastruktury (Poziom IaaS – Infrastructure as a Service),

2.6.2. Metryki Platformowe (Poziom PaaS – Platform as a Service),

2.6.3. Metryki Aplikacji (Poziom APM – Application Performance Monitoring),

2.6.4. Metryki Doświadczenia Użytkownika (RUM – Real User Monitoring),

2.6.5. Metryki Bezpieczeństwa, Zgodności i Zarządzania (przeniesione również do sekcji Bezpieczeństwo),

2.6.6. Metryki Kosztowe (FinOps).

2.7 Dla aplikacji muszą zostać przygotowane przypadki użycia monitorowania (zbieranie zdarzeń lub korelacji zdarzeń w celu wyłapania zdarzenia bezpieczeństwa z poziomu aplikacji).

2.8 Każdy incydent związany z degradacją wydajności, który naruszył SLO, dla rozwiązań krytycznych musi być poddany formalnemu procesowi analizy przyczyn źródłowych. Wyniki analizy muszą prowadzić do wdrożenia działań naprawczych i prewencyjnych.

2.9 Instytucja powinna posiadać mechanizm zgłaszania błędów do Dostawcy usługi chmury obliczeniowej.

2.10 Dla każdej krytycznej usługi muszą być zdefiniowane, udokumentowane i monitorowane wskaźniki poziomu usług (SLA) oraz cele wewnętrzne (SLO). Muszą one określać m.in. maksymalny czas odpowiedzi aplikacji, przepustowość transakcji na sekundę oraz opóźnienia (latency).

3. ZARZĄDZANIE INCYDENTAMI

3.1 Bank musi wdrożyć i utrzymywać kompleksowy proces zarządzania incydentami, który minimalizuje ich wpływ i zapewnia szybkie przywrócenie usług.

3.2 W Banku musi istnieć zdefiniowany i przetestowany proces zarządzania incydentami, który określa role i odpowiedzialności, ścieżki eskalacji, procedury komunikacji wewnętrznej i zewnętrznej (do klientów i regulatora) oraz zasady prowadzenia działań naprawczych podczas incydentu.

3.3 W Banku musi istnieć centralny system do rejestrowania i śledzenia wszystkich incydentów od momentu ich wykrycia aż do zamknięcia.

3.4 Dla kluczowych (krytycznych), przewidywalnych typów incydentów (np. awaria bazy danych, niedostępność regionu chmury) muszą istnieć gotowe, przećwiczone scenariusze reagowania (tzw. playbooki).

3.5 Każdy incydent musi być sklasyfikowany zgodnie z DORA, na podstawie jasno zdefiniowanych kryteriów, które powinny obejmować m.in.:

3.5.1. liczbę dotkniętych klientów/użytkowników,

3.5.2. wpływ na krytyczne funkcje biznesowe,

3.5.3. wpływ na dane (utrata, naruszenie integralności, poufności),

3.5.4. czas trwania i zasięg geograficzny,

3.5.5. wpływ reputacyjny i finansowy,

3.5.6. daty i godziny wystąpienia incydentu (początek i koniec),

3.5.7. czas trwania incydentu w minutach,

3.5.8. jednostki instytucji lub Dostawców zewnętrznych uczestniczących w usuwaniu incydentu.

3.6 Bank musi posiadać definicję i klasyfikację incydentów, z rozróżnieniem incydentów podlegających regulacji DORA.

3.7 Instytucja musi posiadać procedurę raportowania poważnych incydentów ICT do właściwego organu krajowego.

3.8 Proces zarządzania incydentami musi obejmować przyjemniej aspekty opisane w Tabeli 3.:

Tabela 3. Zarządzania incydentami – aspekty

Aspekt Zarządzania incydentami	Co należy zrobić	Kluczowy Cel
Wykrywanie i Rejestracja	Scentralizowane, automatyczne wykrywanie i logowanie każdego incydentu ICT.	Zapewnienie pełnej widoczności i audytowalności.
Klasyfikacja	Natychmiastowa klasyfikacja incydentu według zdefiniowanych kryteriów (wpływ na biznes).	Szybkie zrozumienie powagi sytuacji i priorytetyzacja działań.
Reakcja	Uruchomienie zdefiniowanych procedur (playbooków) i zespołu reagowania (Incident Manager).	Minimalizacja czasu niedostępności.
Komunikacja	Aktywacja planów komunikacji kryzysowej dla wszystkich interesariuszy.	Utrzymanie zaufania klientów i transparentność wobec regulatora.
Raportowanie	Zgłoszenie poważnego incydentu do organu nadzoru zgodnie z wymaganymi terminami.	Spełnienie obowiązku regulacyjnego i wykazanie kontroli nad sytuacją.
Analiza (po incydencie)	Przeprowadzenie analizy przyczyn źródłowych (RCA).	Znalezienie i wyeliminowanie pierwotnej przyczyny, aby zapobiec powtórnemu wystąpieniu incydentu.
Doskonalenie	Wdrożenie działań naprawczych zidentyfikowanych w RCA i aktualizacja planów odporności.	Budowanie długoterminowej, cyfrowej odporności operacyjnej.

3.9 Analiza przyczyn źródłowych (RCA):

3.9.1. W Banku musi istnieć udokumentowana polityka/strategia, która jednoznacznie definiuje, kiedy przeprowadzenie RCA jest obowiązkowe. Kryteria te muszą obejmować co najmniej:

a) każdy „poważny incydent ICT" zgłoszony do organu nadzoru,
b) każde naruszenie kluczowego wskaźnika SLA (np. dostępności lub wydajności) dla Usług ICT wspierających funkcję krytyczną lub istotną Banku,
c) każdy incydent bezpieczeństwa o średnim lub wysokim priorytecie,
d) incydenty powtarzające się, nawet jeśli indywidualnie mają niski wpływ.

3.9.2. Polityka musi określać maksymalny czas od zamknięcia incydentu do zakończenia analizy RCA i opublikowania raportu końcowego (np. 5 dni roboczych).

3.9.3. Wszystkie raporty RCA muszą być tworzone na podstawie jednego, zatwierdzonego szablonu. Szablon musi zawierać co najmniej następujące sekcje:

a) podsumowanie dla zarządu,
b) oś czasu incydentu,
c) analiza wpływu (biznesowego, finansowego, reputacyjnego),
d) opis przyczyn źródłowych, zdefiniowane działania naprawcze i prewencyjne oraz lista uczestników.

3.9.4. Co najmniej raz w roku instytucja powinna przeprowadzić przegląd samego procesu RCA, aby ocenić jego skuteczność.

3.10 Działania naprawcze i prewencyjne.

3.10.1. Wszelkie wnioski i hipotezy muszą być poparte konkretnymi dowodami. Należy zebrać i zabezpieczyć wszystkie artefakty związane z incydentem, takie jak:

a) logi systemowe i aplikacyjne,
b) metryki wydajności (wykresy CPU, pamięci, I/O),
c) ślady transakcji (traces),
d) alerty z systemu monitoringu,
e) zrzuty ekranu oraz zapisy zmian konfiguracyjnych.

3.10.2. Wynikiem analizy incydentu musi być precyzyjne sformułowanie przyczyny źródłowej (jednej lub kilku).

3.10.3. Wszystkie działania naprawcze muszą być zarejestrowane w centralnym systemie, gdzie można śledzić ich status, właściciela i termin realizacji.

3.10.4. Każda zidentyfikowana przyczyna źródłowa musi prowadzić do co najmniej jednego działania naprawczego.

3.10.5. Działania naprawcze powinny być zdefiniowane tak, aby wskazywały konkretne działanie, np. zamiast „poprawić monitoring", należy zdefiniować: „Dodać alert na metrykę X z progiem Y w systemie Z do dnia DD.MM.RRRR, właściciel: Jan Kowalski".

3.10.6. Oprócz naprawienia bezpośredniej przyczyny RCA musi prowadzić do zidentyfikowania działań prewencyjnych, które mogą zapobiec podobnym klasom problemów w innych systemach (np. przeprowadzić audyt wszystkich usług pod kątem braku analogicznego mechanizmu zabezpieczającego).

3.10.7. Po każdym poważnym incydencie (a najlepiej po każdym incydencie wpływającym lub widocznym u klienta) musi zostać przeprowadzona analiza przyczyn źródłowych.

4. ZARZĄDZANIE ZMIANĄ I KONFIGURACJĄ ŚRODOWISK CHMUROWYCH

4.1 **Repozytoria Kodu i Wersjonowanie.** Bank powinien posiadać standard dotyczący prowadzenia repozytorium kodu.

4.2 Bank powinien posiadać strategię zarządzania gałęziami kodu.

4.3 Dostęp do Repozytorium musi być ściśle kontrolowany i ograniczony do upoważnionych osób.

4.4 Dostawcy zewnętrzni muszą być autoryzowani z zachowaniem zasad bezpieczeństwa.

4.5 System zarządzania kodem źródłowym (SCM) musi wspierać pełną historię zmian, identyfikowalność oraz podpisy cyfrowe commitów.

4.6 Wszystkie zmiany w kodzie źródłowym muszą przechodzić przez proces zatwierdzenia (code review) z użyciem pull/merge requestów.

4.7 Automatyzacja Wdrożeń (IaC, CI/CD).

4.7.1. Bank powinien posiadać Standard zapewniania jakości w procesach CI/CD np. Bramki Jakości dla zapewnienia jakości i bezpieczeństwa kodu.

4.7.2. Bramki jakości powinny odnosić się do:

- **a)** testów jednostkowych (np. automatyczne uruchamianie testów jednostkowych przy każdym commicie),
- **b)** analizy kodu (np. automatyczne skanowanie kodu pod kątem znanych luk bezpieczeństwa),
- **c)** analizy aplikacji (np. regularne skanowanie działających aplikacji pod kątem podatności).
  - **i.** przegląd kodu i Code Review (np. wymóg przeglądu kodu).
  - **ii.** testy wydajnościowe.

4.7.3. Instytucja powinna zapewnić możliwość audytu wszelkich zmian na środowisku produkcyjnym.

4.7.4. Wszelkie zmiany muszą być wersjonowane, przetestowane oraz zatwierdzone przed wdrożeniem produkcyjnym.

4.7.5. Bank powinien wykorzystywać narzędzia pozwalające na wykonanie rollbacku przy wykryciu błędu.

4.7.6. Bank powinien stosować politykę ochrony środowisk produkcyjnych, np. poprzez oddzielenie pipeline'u produkcyjnego od pozostałych środowisk.

4.7.7. Każda zmiana kodu musi być automatycznie testowana (unit, integration) przed wdrożeniem do środowiska testowego lub produkcyjnego.

4.7.8. Wszystkie artefakty muszą być wersjonowane i przechowywane w repozytorium artefaktów wspierającym audyt.

4.7.9. Dostęp do systemów CI/CD musi być kontrolowany zgodnie z zasadą najmniejszych uprawnień.

4.7.10. Wszystkie dane wrażliwe muszą być zarządzane za pomocą bezpiecznego narzędzia.

4.7.11. Proces CI/CD musi być zintegrowany z systemem IAM organizacji i wspierać logowanie zdarzeń dostępowych.

4.7.12. Wszystkie operacje wykonywane w ramach procesu CI/CD muszą być logowane i możliwe do audytu zgodnie z wymaganym czasem określonym przez dział bezpieczeństwa.

4.7.13. System CI/CD powinien być zintegrowany z mechanizmem alertowania i monitorowania incydentów bezpieczeństwa. (np. CRLo).

4.7.14. Każda zmiana wdrażana do środowiska produkcyjnego musi być objęta formalnym procesem zarządzania zmianą.

4.7.15. System CI/CD powinien wspierać stopniowe wdrażanie (Blue/Green, Canary Deployments).

4.7.16. Organizacja musi posiadać procedurę testowania odporności systemów na błędy wdrożeniowe.

4.7.17. Zaleca się automatyzację testów bezpieczeństwa i włączenie ich do potoku CI/CD. Testy bezpieczeństwa w potoku CI/CD powinny być zaimplementowane:

a) przy zapisywaniu kodu do repozytorium (np. eliminacja secretów),

b) przed buildem (analiza statyczna kodu, analiza komponentów softu),

c) post build (analiza dynamiczna).

5. PROCESY DEVOPS

5.1 Infrastruktura oraz sieć musi być powoływana kodem – za pomocą procesów Infrastructure as Code oraz Network as Code.

5.2 Procesy provisioningowe (IaC) muszą być zautomatyzowane, powtarzalne i przechowywane w systemie kontroli wersji.

5.3 Każda zmiana infrastruktury musi przechodzić przez proces review i testowania na środowiskach nieprodukcyjnych.

5.4 Narzędzia DevOps muszą wspierać audyt działań (logi, historia operacji, wersjonowanie konfiguracji).

5.5 Użycie narzędzi do zarządzania konfiguracją musi być objęte kontrolą bezpieczeństwa.

5.6 Infrastruktura jako kod (IaC) musi zawierać mechanizmy walidacji, testowania i polityk bezpieczeństwa (np. policy-as-code).

5.7 Każda zmiana konfiguracji lub zasobów w środowisku chmurowym musi być rejestrowana i zatwierdzana zgodnie z polityką zmian.

5.8 Dla zmian produkcyjnych musi być dostępny plan wdrożenia oraz plan wycofania (rollback).

5.9 Dostęp do operacji zmian w chmurze musi być ograniczony do uprawnionych ról zgodnie z RBAC.

5.10 Musi istnieć mechanizm powiadamiania o wdrożeniu zmian oraz monitorowania ich wpływu.

5.11 Zmiany automatyczne (np. autoskalowanie, aktualizacje) muszą być monitorowane i audytowalne.

5.12 Wszystkie zmiany w środowisku produkcyjnym (aktualizacje aplikacji, zmiany konfiguracji infrastruktury) muszą podlegać formalnemu procesowi zarządzania zmianą, obejmującemu ocenę ryzyka, plan wdrożenia, plan wycofania (rollback) oraz akceptację przez komitet ds. zmian (Change Advisory Board – CAB).

6. ZARZĄDZANIE DANYMI I CIĄGŁOŚĆ DZIAŁANIA (BCP/DR)

6.1 Polityka Tworzenia Kopii Zapasowych.

6.1.1. Jeśli to możliwe, Instytucja może skorzystać z natywnych rozwiązań chmury obliczeniowej w zakresie kopii zapasowej. Usługa ta powinna być budowana w odrębnym centrum przetwarzania danych.

6.1.2. Instytucja musi posiadać politykę Tworzenia Kopii Zapasowych w Środowiskach Chmurowych.

6.1.3. Bank powinien posiadać klasyfikację danych oraz wymagania dotyczące celów odzyskiwania (RTO/RPO).

6.1.4. Bank powinien posiadać procedurę Częstotliwość Tworzenia Kopii Zapasowych, np.:

- **a)** Pełne, Przyrostowe, Różnicowe: określenie, kiedy i jakie typy kopii zapasowych są wykonywane.
- **b)** Migawki (Snapshots): wykorzystanie natywnych funkcji chmury do tworzenia szybkich kopii danych (np. dla dysków VM, baz danych). Należy pamiętać, że migawki często są przechowywane w tej samej lokalizacji co dane źródłowe, i nie zastępują pełnych, off-site backupów.
- **c)** Kopie logiczne/eksporty: dla baz danych, aplikacji SaaS, konfiguracji (np. eksport baz danych do plików, tworzenie obrazów kontenerów).
- **d)** Backup konfiguracji: Regularne kopiowanie konfiguracji usług chmurowych, definicji IaC i polityk bezpieczeństwa.
- **e)** Częstotliwość: zgodna z RPO dla danej klasy danych (np. co 15 minut dla danych krytycznych, codziennie dla danych ważnych).

6.1.5. Należy posiadać Strategię Przechowywania Kopii Zapasowych, która określa m.in.:

- **a)** Zasady redundancji geograficznej,
- **b)** Retencję (Okres Przechowywania) Kopii Zapasowych,
- **c)** Bezpieczeństwo Kopii Zapasowych,
- **d)** Weryfikację i Testowanie kopii zapasowych.

6.2 Replikacja i Retencja Danych.

6.2.1. Instytucja musi określić RPO i RTO dla krytycznych operacji ICT.

6.2.2. Wymaga się od instytucji odporności infrastruktury ICT, w tym zdolności bezpiecznego przywracania danych i funkcjonalności odzyskiwania, np. poprzez replikację.

6.2.3. Należy regularnie prowadzić testy cyfrowej odporności operacyjnej, w tym testów scenariuszy awaryjnych i odzyskiwania.

6.2.4. Musi istnieć Polityka Retencji Danych w Środowiskach Chmurowych.

6.2.5. Muszą zostać określone Zasady Ustalania Okresów Retencji, np.:

a) Wymogi Biznesowe: określenie, jak długo dane są potrzebne do prowadzenia działalności, analizy, raportowania finansowego, obsługi klienta, badań i rozwoju.

b) Wymogi Audytowe: zapewnienie dostępności danych dla audytów wewnętrznych i zewnętrznych przez wymagany okres.

c) Zasada Minimalizacji Danych (Data Minimization): przechowywanie tylko tych danych, które są absolutnie niezbędne, przez okres nie dłuższy niż to konieczne.

6.3 Testowanie Planów Ciągłości Działania (BCP) i Odzyskiwania po Awarii (DR).

6.3.1. Instytucja powinna dla rozwiązań krytycznych posiadać szczegółowy, aktualny i udokumentowany plan DR, który opisuje krok po kroku procedury przełączenia awaryjnego na ośrodek zapasowy w innym regionie geograficznym. Plan musi być zgodny z wymogami regulacyjnymi.

6.3.2. Plan DR powinien być regularnie testowany (zaleca się wykonanie takiego testu co najmniej raz w roku dla pełnego testu przełączenia i częściej dla testów częściowych).

6.3.3. Tam, gdzie to możliwe, mechanizmy przełączania awaryjnego (failover) pomiędzy instancjami w architekturze HA lub ośrodkami w planie DR powinny być zautomatyzowane, aby zminimalizować czas niedostępności i ryzyko błędu ludzkiego.

6.3.4. Dla każdej Usługi ICT wspierającej funkcję krytyczną lub istotną Banku muszą być formalnie zdefiniowane i udokumentowane maksymalny dopuszczalny czas odtworzenia po awarii (RTO) oraz maksymalny dopuszczalny punkt utraty danych (RPO). Wartości te muszą być zgodne z analizą wpływu na biznes (BIA).

6.3.5. Instytucja powinna wdrożyć politykę tworzenia kopii zapasowych (backupów) dla wszystkich krytycznych danych i konfiguracji. Polityka musi określać częstotliwość, retencję, szyfrowanie oraz procedury odtwarzania. Kopie zapasowe powinny być przechowywane w sposób geograficznie odseparowany.

6.4 Odporność środowisk i skalowalność.

6.4.1. Aby zapewnić odpowiedni poziom dostępności, infrastruktura rozwiązań krytycznych musi być zaprojektowana z wykorzystaniem mechanizmów autoskalowania, które automatycznie dostosowują liczbę zasobów (np. serwerów, kontenerów) w odpowiedzi na zmieniające się obciążenie. Skalowanie musi działać zarówno w górę (scale-out), jak i w dół (scale-in) w celu optymalizacji kosztów.

6.4.2. Ruch sieciowy do aplikacji i usług powinien być dystrybuowany za pomocą mechanizmów równoważenia obciążenia (load balancerów) w celu zapewnienia optymalnego wykorzystania zasobów, unikania przeciążeń pojedynczych instancji i zwiększenia odporności.

6.4.3. Krytyczne systemy powinny być zaprojektowane w architekturze wysokiej dostępności, co oznacza redundancję komponentów na wielu poziomach. Wymagane jest wykorzystanie co najmniej dwóch Stref Dostępności (Availability Zones) w ramach jednego regionu chmurowego.

7. ZARZĄDZANIE KOSZTAMI CHMUROWYMI (FINOPS)

7.1 FinOps narodził się jako dyscyplina wraz z rosnącym wykorzystaniem chmury publicznej. Organizacje zaczęły zmagać się z nowym wyzwaniem: dynamicznymi i trudnymi do przewidzenia kosztami infrastruktury IT.

7.2 Odpowiedzią na te potrzeby było powstanie w 2019 roku FinOps Foundation – organizacji non-profit wspieranej przez Linux Foundation. Jej celem było stworzenie wspólnego języka i zestawu praktyk, które połączą zespoły finansowe, technologiczne i biznesowe w zarządzaniu kosztami chmury.

7.3 Przez pojęcie FinOps (skrót od ang. Financial Operations) należy rozumieć zorganizowany zbiór praktyk, procesów i zasad zarządzania kosztami usług chmury obliczeniowej, którego celem jest zapewnienie efektywnego gospodarowania zasobami finansowymi w środowiskach technologii informacyjno-komunikacyjnych (ICT), w szczególności w modelu przetwarzania w chmurze.

7.3.1. FinOps stanowi model operacyjny oparty na współpracy zespołów finansowych, technicznych oraz operacyjnych, umożliwiający:

a) monitorowanie i analizę zużycia zasobów chmurowych w czasie rzeczywistym,

b) optymalizację kosztów poprzez wdrażanie mechanizmów automatyzacji, rezerwacji i skalowania,

c) podejmowanie decyzji inwestycyjnych opartych na danych i mierzalnych wskaźnikach efektywności,

d) zapewnienie zgodności z politykami budżetowymi i regulacjami wewnętrznymi organizacji.

7.4 Kluczowe zasady FinOps przedstawia poniższa grafika, a szerzej są one omówione w kolejnych akapitach.

Źródło grafiki 1 – https://www.finops.org/framework/principles/. *W ramach licencji:* https://www.finops.org/introduction/how-to-use/. *Dodano w grafice opisy pryncypiów FinOps.*

7.4.1. **Współpraca zespołów** – zespoły finansowe, technologiczne, produktowe i biznesowe współpracują w czasie rzeczywistym, aby efektywnie zarządzać kosztami chmury.

7.4.2. **Odpowiedzialność za swoje użycie technologii** – inżynierowie i zespoły produktowe zarządzają kosztami od projektowania po operacje, mając wpływ na architekturę i optymalizację.

7.4.3. **Dane FinOps muszą być dostępne, aktualne i dokładne** – Przejrzystość kosztów w czasie rzeczywistym umożliwia szybsze i lepsze decyzje. Analizy trendów i odchyleń pomagają zrozumieć zmiany kosztów.

7.5 **FinOps powinien być wspierany centralnie** – zespół promuje najlepsze praktyki, ale odpowiedzialność pozostaje rozproszona. Optymalizacja zobowiązań, rabatów odbywa się centralnie.

7.5.1. **Wartość biznesowa napędza decyzje technologiczne** – decyzje opierają się na metrykach wartościowych, a nie tylko na całkowitych wydatkach. Liczy się świadome balansowanie kosztów, jakości i szybkości.

7.5.2. **Model kosztów zmiennych chmury to szansa, nie ryzyko** – wykorzystywanie elastycznego modelu kosztowego chmury jako szansy na zwiększenie wartości biznesowej, poprzez planowanie i optymalizację zasobów w sposób zwinny, ciągły i proaktywny.

7.6 W ramach praktyki FinOps wyróżnia się trzy główne fazy dojrzałości (przedstawione na grafice 2), które umożliwią stopniowe dojrzewanie procesów w miarę wzrostu wartości biznesowej.

Źródło grafiki 2 – FinOps Maturity Model *W ramach licencji:* https://www.finops.org/introduction/how-to-use/*. Dodano w grafice opisy Faz FinOps.*

7.7 **Faza początkowa** (potocznie określana jako pełzanie) – faza, w której eksperymentuje z chmurą, buduje prototypy i koncentruje się na szybkim dostarczaniu produktów. Budżety są ograniczone, a procesy FinOps dopiero się kształtują.

7.8 **Faza rozwojowa** (potocznie określana jako chodzenie) – faza, w ramach której firma zwiększa skalę operacji, zespoły rosną, a obciążenia chmurowe stają się bardziej złożone. FinOps staje się kluczowe dla zarządzania rosnącymi kosztami. Zalecane działania dla danej fazy dotyczą poniższych obszarów.

7.9 **Faza dojrzałości** (potocznie określana jako bieganie) – faza, w ramach której organizacja działa na dużą skalę, z wieloma zespołami, złożonymi aplikacjami i globalnym zasięgiem. FinOps jest integralną częścią kultury organizacyjnej.

7.10 Praktyczne przykłady i standardy w zakresie poszczególnych faz zostały opisane w Załączniku nr 5 do Standardu.

7.11 Aby kultura i wdrożenie procesów FinOps w Banku były skuteczne, konieczne jest budowanie świadomości kosztowej wśród wszystkich interesariuszy poprzez:

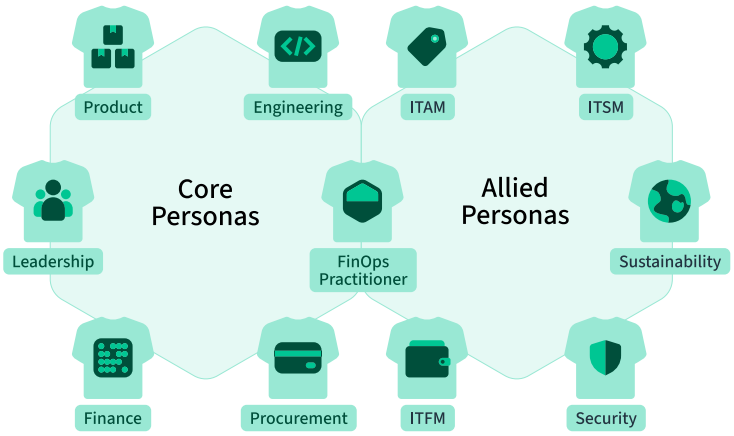
7.11.1. **szkolenia i warsztaty** – regularne sesje edukacyjne dla zespołów technicznych, produktowych i finansowych, wyjaśniające, jak ich decyzje wpływają na koszty chmurowe,

7.11.2. **komunikacja wewnętrzna** – newslettery, kanały Slack/Teams, dashboardy z wizualizacją kosztów i oszczędności,

7.11.3. **spotkania FinOps** – cykliczne spotkania (np. miesięczne) z zespołami, podczas których omawiane są trendy kosztowe, dobre praktyki i zrealizowane optymalizacje,

7.11.4. **nagrody i wyróżnienia dla zespołów**, które osiągnęły konkretne cele optymalizacyjne (np. największe oszczędności).

7.12 Istotną kwestią jest także podział ról i odpowiedzialności – wdrożenie FinOps wymaga współpracy wielu interesariuszy w organizacji, nie tylko zespołu FinOps. W dużych organizacjach jedna rola może obejmować wiele osób, a w małych – jedna osoba może pełnić kilka ról. Grafika 3. przedstawia przykład ról FinOps:



Źródło grafiki 3 – https://www.finops.org/framework/personas/ W ramach licencji: https://www.finops.org/introduction/how-to-use/.

7.13 Opis głównych ról (Core Personas) w ramach adopcji FinOps Framework:

7.13.1. **Praktyk FinOps (FinOps Practitioner)** – rola, która łączy zespoły biznesowe, inżynieryjne i finansowe, wdrażając kulturę FinOps. Wspiera podejmowanie decyzji opartych na danych, optymalizację kosztów i ciągłe doskonalenie.

7.13.2. **Zespół inżynieryjny (Engineering)** – projektuje, zarządza i optymalizuje infrastrukturę chmurową, dbając o wydajność, bezpieczeństwo i zgodność. Współpracuje z FinOps w zakresie kosztów i automatyzacji.

7.13.3. **Zespół finansowy (Finance)** – dostarcza wiedzę finansową, wspiera budżetowanie, prognozowanie i alokację kosztów chmury. Zapewnia zgodność i przejrzystość finansową.

7.13.4. **Zespół produktowy (Product**) – reprezentuje interesy biznesowe, definiuje wymagania i priorytety. Łączy strategię produktową z decyzjami technologicznymi i wartością biznesową chmury.

7.13.5. **Kierownictwo (Leadership)** – kieruje strategią chmurową, zapewniając zgodność inwestycji z celami biznesowymi.

7.13.6. **Zakupy (Procurement)** – zespół, który koncentruje się na zarządzaniu relacjami z Dostawcami usług chmury obliczeniowej oraz na zakupie usług i produktów chmurowych.

7.14 Wdrożenie dobrych praktyk FinOps w Banku to długotrwały proces, który dojrzewa wraz z implementacją chmury obliczeniowej w środowisku, ale jest wart zaadresowania już na etapie budowy fundamentów. Dobrym benchmarkiem może być adopcja trendów na bazie raportów State of FinOps[11] publikowanych przez FinOps Foundation. Raporty te dostarczają danych porównawczych, trendów branżowych oraz najlepszych praktyk, które mogą wspierać rozwój kultury FinOps i podejmowanie decyzji opartych na danych.

7.15 Praktyczny przykład uprawnień oraz szkoleń, które mają na celu rozwój osób pełniących funkcję FinOps, stanowi Załącznik nr 5 do Standardu.

8. VENDOR MANAGEMENT (RYZYKO KONCENTRACJI, MONITOROWANIE, AUDYT)

8.1 Zarządzanie dostawcami, czyli vendor management, to strategiczny proces, który obejmuje wybór, negocjacje, współpracę a także monitorowanie relacji z Dostawcami usług chmurowych. Celem tego procesu jest zapewnienie, że usługi chmury obliczeniowej są efektywnie wykorzystywane, a Bank otrzymuje z nich maksymalną wartość przy minimalnym poziomie ryzyka.

8.2 W celu odpowiedniego zarządzania ryzykiem wynikającym z umowy realizowanej przy wykorzystaniu technologii chmury obliczeniowej, zapewnienia właściwego poziomu świadczonych usług, oceny, czy nie zmieniła się zdolność Banku do transferowania i akceptacji ryzyka, z uwagi na zmiany m.in. w zakresie, rodzaju, klasyfikacji, skali informacji powierzonych Dostawcy i przetwarzanych w chmurze obliczeniowej, wymaganiach prawa, postanowieniach i zobowiązaniach umownych Banku oraz ich wpływ na ryzyko wynikające z relacji z Dostawcą, należy dokonać analizy obszarów, które zostały zredefiniowane w Załączniku 7 do Standardu, na bieżąco lub nie rzadziej niż raz do roku.

8.3 W przypadku zidentyfikowania jakichkolwiek zmian/nieprawidłowości w zakresie wskazanym powyżej należy rozważyć zweryfikowanie wymienionych obszarów oraz w razie konieczności, zaktualizować formularze:

8.3.1. formularz(e) służące do oceny klasyfikacji oraz skali przetwarzanych Informacji prawnie chronionych,

8.3.2. formularz(e) służące do szacowania ryzyka (należy ocenić wpływ zmian na poszczególne ryzyka zidentyfikowane w związku z przetwarzaniem Informacji prawnie chronionych w chmurze obliczeniowej),

11 https://data.finops.org/

8.3.3. środki techniczne oraz zasoby organizacyjne, w szczególności zasoby ludzkie posiadające właściwe kompetencje techniczne,

8.3.4. strategia wyjścia, która powinna zapewnić możliwość wycofania się z umowy w taki sposób, aby nie spowodować zbędnych zakłóceń w działalności Banku, bez uszczerbku dla zachowania przez niego zgodności z wymogami regulacyjnymi i bez szkody dla ciągłości i jakości świadczenia usług na rzecz klientów.

8.4 Zmiany zidentyfikowane w związku z procesem zarządzania współpracą z Dostawcą mogą wiązać się z koniecznością zmiany umowy z Dostawcą usług chmurowych. Należy ocenić potencjalny wpływ zmiany umowy na krytyczne lub istotne funkcje objęte umową. Jeśli ocena wykaże istotny wpływ zmiany na krytyczne lub istotne funkcje objęte umową, należy rozważyć uzyskanie zgody organu zarządzającego na wdrożenie zmiany oraz notyfikację do UKNF w przypadku, gdy usługi chmury obliczeniowej/Usługi ICT wspierają krytyczne lub istotne funkcje Banku.

8.5 W przypadku umów na usługi chmurowe/Usługi ICT, które wspierają krytyczne lub istotne funkcje Banku, wyniki okresowego monitorowania umowy, w tym ocena ryzyka rezydualnego, efektywność strategii wyjścia (wyniki testów) oraz testów COB, koncentracja, wyniki audytów i kontroli powinny być raportowane do organów zarządzających w ramach okresowego sprawozdania z powierzania funkcji krytycznych lub istotnych zewnętrznym Dostawcom.

8.6 Rekomenduje się, aby okresowe monitorowanie było udokumentowane oraz archiwizowane dla celów kontrolnych.

8.7 Bank powinien regularnie oceniać zdolność zewnętrznego Dostawcy usług chmurowych/ ICT do bezpiecznego świadczenia Usług ICT na rzecz Banku bez negatywnego wpływu na ciągłość świadczenia tych Usług ICT. W tym celu należy m.in. okresowo weryfikować: zakres i skalę powierzenia, aktualność zapisów umownych, prawidłowość realizacji przedmiotu umowy przez Dostawcę, poziom koncentracji Usług ICT, w szczególności poziom zagrożeń wynikających z koncentracji zależności od zewnętrznych Dostawców usług chmurowych/ICT, oraz czy stosowane przez Dostawcę mechanizmy kontrolne w stosunku do podwykonawców, którzy świadczą Usługi ICT, wspierające w sposób istotny funkcje krytyczne lub istotne Banku, zapewniają właściwy poziom ich monitorowania. Ustalenia umowne powinny wzmacniać zdolności Banku do skutecznego monitorowania wszystkich zagrożeń w zakresie usług chmurowych/ Usług ICT powstających na poziomie zewnętrznych Dostawców Usług ICT.

9. AUDYTOWANIE DOSTAWCY USŁUGI W CHMURZE

9.1 Korzystając z praw dostępu, kontroli i audytu w odniesieniu do Dostawcy usług chmurowych, Bank, stosując podejście oparte na analizie ryzyka, określa z góry częstotliwość audytów i kontroli oraz obszary, które mają podlegać kontroli, przestrzega przy tym powszechnie przyjętych standardów audytu zgodnie z wszelkimi instrukcjami nadzorczymi dotyczącymi stosowania i włączania takich standardów audytu.

9.2 Bez uszczerbku dla ostatecznej odpowiedzialności Banku w zakresie audytu i kontroli może on stosować następujące metody:

9.2.1. własny audyt wewnętrzny lub audyt przeprowadzany przez wyznaczoną osobę trzecią,

9.2.2. w stosownych przypadkach – audyt zbiorczy i zbiorcze testy ICT, w tym testy penetracyjne pod kątem wyszukiwania zagrożeń, które są organizowane wspólnie z innymi zamawiającymi podmiotami finansowymi lub firmami korzystającymi z Usług ICT tego samego zewnętrznego Dostawcy i które są przeprowadzane przez te zamawiające podmioty finansowe lub firmy lub przez wyznaczoną przez nie osobę trzecią,

9.2.3. w stosownych przypadkach – certyfikaty wydane przez osoby trzecie,

9.2.4. w stosownych przypadkach – sprawozdania z audytu wewnętrznego lub sprawozdania z audytu prowadzonego przez osobę trzecią udostępnione przez zewnętrznego Dostawcę Usług ICT.

9.3 Bank nie może po pewnym czasie opierać się wyłącznie na certyfikatach, o których mowa w pkt 9.2.3 ani na sprawozdaniach z audytu, o których mowa w pkt 9.2.4 powyżej. W ramach polityki dopuszcza się stosowanie metod, o których mowa w ww. punktach, wyłącznie w przypadku, gdy Bank:

9.3.1. jest zadowolony z planu audytu Dostawcy usług chmurowych w odniesieniu do odpowiednich umów,

9.3.2. zapewnia, aby zakres certyfikatów lub sprawozdań z audytu obejmował zidentyfikowane przez siebie systemy i kluczowe mechanizmy kontroli oraz zapewniał zgodność z odpowiednimi wymogami regulacyjnymi,

9.3.3. na bieżąco dokładnie ocenia treść certyfikatów lub sprawozdań z audytu i sprawdza, czy sprawozdania lub certyfikaty są aktualne,

9.3.4. zapewnia uwzględnienie kluczowych systemów i mechanizmów kontroli w przyszłych wersjach sprawozdania z certyfikacji lub audytu,

9.3.5. jest usatysfakcjonowany umiejętnościami podmiotu certyfikującego lub przeprowadzającego audyt,

9.3.6. stwierdza, że certyfikaty są wydawane, a audyty są przeprowadzane zgodnie z powszechnie uznanymi odpowiednimi normami zawodowymi i obejmują test skuteczności operacyjnej stosowanych kluczowych mechanizmów kontroli,

9.3.7. ma wynikające z umowy prawo do żądania zmian zakresu certyfikatu – z częstotliwością rozsądną i uzasadnioną z punktu widzenia zarządzania ryzykiem – zmian zakresu certyfikatów lub sprawozdań z audytu do innych odpowiednich systemów i mechanizmów kontroli,

9.3.8. ma wynikające z umowy prawo do przeprowadzania audytów indywidualnych i zbiorczych według własnego uznania w odniesieniu do ustaleń umownych oraz wykonywania tych praw zgodnie z uzgodnioną częstotliwością.

9.4 W przypadku gdy umowy dotyczące korzystania z usług chmury obliczeniowej zawarte z Dostawcami wiążą się z wysokim stopniem złożoności technicznej, Bank sprawdza, czy audytorzy – zarówno wewnętrzni, jak i zewnętrzni lub grupa audytorów – posiadają odpowiednie umiejętności i wiedzę umożliwiające skuteczne przeprowadzanie odpowiednich audytów i ocen.

9.5 W przypadku gdy Bank zleca przeprowadzenie audytu na zewnątrz (osobie trzeciej), powinien odpowiednio przygotować się, biorąc pod uwagę informacje:

9.5.1. Etap planowania audytu

a) Przygotowanie jednoznacznie określonego zakresu audytu.

b) Wybranie audytora, który będzie przeprowadzać czynności audytorskie.

c) Osoby wykonujące audyt muszą być w stanie to zrobić w sposób obiektywny i niezależny oraz zgodny z zasadami etycznymi, do czego zobowiążą się pisemnie, przyjmując zlecenie wykonania prac.

d) Audytor oraz audytorzy będący członkami zespołu muszą posiadać odpowiedni zakres wiedzy i doświadczenia, który pozwoli im na przeprowadzenie audytu. Zespół może być rozszerzony o ekspertów technologicznych, interpretujących bardzo specjalistyczne obszary. W przypadku usługi chmurowej rekomenduje się, by wśród członków zespołu znajdowała się przynajmniej jedna osoba mogąca wykazać się wiedzą i doświadczeniem w zakresie cloud computing.

e) Audytor powinien przygotować i zaprezentować Bankowi program audytu.

9.5.2. Etap przebieg audytu

a) Celem audytu jest potwierdzenie zgodności Banku z wymaganiami w ramach badanego obszaru. Audytor dokonuje weryfikacji:

i. czy wdrożone przez Bank mechanizmy kontrolne są adekwatne w odniesieniu do wymagań Rozporządzenia DORA,

ii. ryzyk zidentyfikowanych przez sam Bank oraz w związku z powierzeniem czynności na zewnątrz organizacji (outsourcing).

b) Zastosowane techniki audytowe powinny przede wszystkim koncentrować się na obserwacjach, analizie dokumentów oraz wywiadach.

c) Za szczególnie wartościowe źródła należy uważać wyniki dokonywanych testów, przeglądów i innych form weryfikacji.

d) W trakcie kolejnych audytów audytorzy powinni weryfikować poprzednio zgłoszone niezgodności. Brak wdrożenia rekomendacji dotyczących niezgodności innych niż „niskie" powinien automatycznie oznaczać podniesienie ich priorytetu.

e) Audytorzy, wykorzystując wiedzę i doświadczenie, powinni analizować dojrzałość zastosowanych mechanizmów kontrolnych.

f) Audytorzy powinni gromadzić i przechowywać dowody audytowe w sposób chroniący ich poufność, dostępność i integralność.

9.5.3. Etap raportowania

a) Raport z audytu powinien zawierać:

i. Podsumowanie – wskazujące na ocenę poziomu dojrzałości oraz kluczowe obserwacje poczynione przez audytorów,

ii. Cel i zakres prac,

iii. Zrealizowany harmonogram audytu,

iv. Zestawienie niezgodności:

(i) ocena priorytetu niezgodności (np. wysoki, średni, niski)

(ii) opis ryzyka

(iii) rekomendacje,

v. Ocenę poziomu dojrzałości (np. w skali: wymagania spełnione, wymagania spełnione w sposób częściowy, wymagania niespełnione),

vi. Opis zastosowanej metody weryfikacji (lista narzędzi, technik, metod badawczych i źródeł informacji, które były wykorzystywane podczas audytu, np. wywiady, analiza dokumentów, inspekcja na miejscu),

vii. Inne obserwacje i uwagi.

b) Audyt usług chmurowych IaaS, PaaS, SaaS – cel, dokumentacja, obszary wymagające weryfikacji.

9.6 Celem audytu jest zapewnienie, że świadczone na rzecz Banku usługi Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) w adekwatny sposób zapewniają bezpieczeństwo przetwarzanym danym, a tym samym spełniają wymagania Rozporządzenia DORA.

9.7 Zakres analizowanej dokumentacji oraz obszary wymagające weryfikacji audytu zgodnie z wypracowanym sektorowo standardem są dostępne w ZBP, po uprzednim przystąpieniu do umowy współpracy w zakresie prowadzenia audytu.

CZĘŚĆ
VII

ZAŁĄCZNIKI

ZAŁĄCZNIK nr 1 – Definicje

ZAŁĄCZNIK nr 2 – Schemat podstawowych zagadnień regulacyjnych

ZAŁĄCZNIK nr 3 – Wymagania kontraktowe

ZAŁĄCZNIK nr 4 – Notyfikacja umów na usługi w chmurze

ZAŁĄCZNIK nr 5 – FinOps – Fazy, uprawnienia i szkolenia

ZAŁĄCZNIK nr 6 – Podstawowy zbiór informacji na potrzeby realizacji planu wyjścia z usługi chmurowej

ZAŁĄCZNIK nr 7 – Obszary do analizy przez Bank w zakresie Vendor Managementu

ZAŁĄCZNIK nr 8 – Wytyczne dla Dostawców usług chmurowych

ZAŁĄCZNIK nr 9 – Szablon analizy DD/ analizy ryzyka (edytowalny)

ZAŁĄCZNIK nr 1

Definicje

1. PODSTAWOWE DEFINICJE PRZYJĘTE W STANDARDZIE

1. **AI Act** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

2. **Bank** – bank w rozumieniu Prawa bankowego (krajowy), oddział banku krajowego za granicą, oddział banku zagranicznego w rozumieniu Prawa bankowego, instytucja kredytowa w rozumieniu Prawa bankowego, oddział instytucji kredytowej w rozumieniu Prawa bankowego, bank krajowy prowadzący działalność na terytorium państwa goszczącego poprzez oddział lub w ramach działalności transgranicznej zgodnie z Prawem bankowym oraz bank spółdzielczy w rozumieniu Ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (zakresu niniejszego Standardu wyłączone zostały podmioty nadzorowane w rozumieniu Ustawy o nadzorze nad rynkiem finansowym inne niż podmioty podlegające nadzorowi bankowemu). Dla uniknięcia wątpliwości, nadzorem bankowym, a zatem wyłączonym spod niniejszej definicji, są objęte następujące podmioty:

   a. przedstawicielstwa banku zagranicznego w rozumieniu Prawa bankowego,
   b. przedstawicielstwa instytucji kredytowej w rozumieniu Prawa bankowego oraz
   c. bank zagraniczny i instytucje kredytowe w ramach działalności transgranicznej, o której mowa w art. 48i Prawa bankowego.

3. **Chmura obliczeniowa („chmura", ang. *cloud, cloud computing*)** – pula współdzielonych, dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich Dostawcy.

4. **CPD** – Centrum Przetwarzania Danych.

5. **Data Act (Akt w sprawie danych)** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz. U. UE. L. z 2023 r. poz. 2854 z późn. zm.).

6. **DORA** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. U. UE. L. z 2022 r. Nr 333, str. 1 z późn. zm.).

7. **Dostawca usług w chmurze (Dostawca)** – przedsiębiorstwo świadczące usługi w chmurze, w tym jako Zewnętrzny dostawca Usług ICT.

8. **EOG** – Europejski Obszar Gospodarczy.

9. **Funkcja krytyczna lub istotna** – oznacza funkcję, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe Banku, na bezpieczeństwo lub ciągłość usług i działalności Banku, lub której zaprzestanie, wadliwe lub zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez Bank warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych.

10. **Informacja prawnie chroniona** – tajemnica bankowa mająca 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".

11. **NIST** – The NIST Definition of Cloud Computing; Recommendations of the National Institute of Standards and Technology; Special Publication 800-145; https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

12. **Outsourcing chmury**[12] – oznacza umowę zawartą w dowolnej formie między Bankiem a Dostawcą usług w chmurze, na mocy której Dostawca usług w chmurze dostarcza dla Banku usługę w chmurze służącą do wsparcia realizacji funkcji, którą Bank realizowałby samodzielnie, gdyby usługa w chmurze była niedostępna.

13. **Poddostawca** – podmiot, który świadczy usługi dla Dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla Banku, i posiada albo może posiadać identyfikowany dostęp do informacji przetwarzanych przez Bank, tj. wobec którego zachodzi ujawnienie informacji.

    Poddostawcą w powyższym rozumieniu jest podmiot, który:

    a. świadczy usługi dla Dostawcy usług w chmurze, służące dostarczaniu usługi w chmurze dla Banku,

    b. oraz posiada lub może posiadać identyfikowany dostęp do informacji prawnie chronionych Banku.

12 Na podstawie EBA/GL/2019/02 z 25 lutego 2019 r. – Wytyczne w sprawie outsourcingu, Definicje, Outsourcing

Przykłady:

- Poddostawcą będzie podmiot spełniający powyższe kryteria, prowadzący działalność centrum hostingowego (chmury w ścisłym tego słowa znaczeniu), w którym będzie zainstalowane i eksploatowane jest oprogramowanie oferowane Bankowi łącznie z usługą dostawy mocy obliczeniowej w ramach tego centrum.
- Nie będzie Poddostawcą kontrahent centrum hostingowego odpowiadający za utrzymanie czystości, agencja ochrony mienia, a nawet wynajmujący – właściciel budynku.

W zakresie drugiego z wymienionych przykładu powyżej, przez identyfikowany dostęp do informacji przetwarzanych przez Bank rozumieć należy taki dostęp, który spełnia następujące kryteria:

a. umożliwia Poddostawcy identyfikację Banku-jako zleceniodawcy,

b. dochodzi do ujawnienia przetwarzanych danych (informacji) w rozumieniu nadanym przez Komunikat,

przy czym to zapisy kontraktowe lub sposób skonfigurowania szyfrowania informacji powinny decydować o tym, czy podmiot posiada i w jaki sposób może uzyskać posiadanie takiego identyfikowanego dostępu (np. gdy technicznie możliwy jest dostęp, natomiast umowa zakazuje wykorzystywania takiej możliwości).

Dodatkowo wskazać należy, że Poddostawcą będzie firma współpracująca z Dostawcą, która ma logiczny, a nie fizyczny, dostęp do informacji przetwarzanych przez Bank.

14. **Podwykonawca** – podmiot, który świadczy Usługi ICT dla Zewnętrznego dostawcy Usług ICT, w sposób istotny wykorzystywane przez Zewnętrznego dostawcę Usług ICT do świadczenia Usługi ICT dla Banku.

15. **Prawo bankowe** – ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2024 r. poz. 1646 z późn. zm.).

16. **RODO** – 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).

17. **Rozporządzenie delegowane 2017/565** – Rozporządzenie delegowane Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy (Dz. U. UE. L. z 2017 r. Nr 87, str. 1 z późn. zm.).

18. **Rozporządzenie wykonawcze 2024/2956** – rozporządzenie wykonawcze 2024/2956 ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji.

19. **Rozporządzenie delegowane 2025/532** – Rozporządzenie delegowane Komisji (UE) 2025/532 z dnia 24 marca 2025 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających elementy, które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo Usług ICT wspierających krytyczne lub istotne funkcje (Dz. U. UE. L. z 2025 r. poz. 532).

20. **Standard v2** – opublikowany w lutym 2022 r. standard PolishCloud 2.0., dostępny pod linkiem: https://www.zbp.pl/aktualnosci/wydarzenia/ZBP-publikuje-Standard-Polish-Cloud-2-0.

21. **Standard** – oznacza niniejsze opracowanie.

22. **Ujawnienie informacji** – sytuacja, podczas której informacje są przetwarzane w chmurze:

a. w sposób nieszyfrowany albo

b. w sposób zaszyfrowany „at rest" lub „in transit", ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać Dostawca usług w chmurze lub jego Poddostawca w łańcuchu outsourcingowym.

23. **Usługi ICT** – zgodnie z DORA, oznaczają usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej.

24. **Usługi chmury obliczeniowej (zamiennie: „usługi w chmurze", „usługi chmurowe", „usługi chmury obliczeniowej")** – Usługi ICT – Usługi w chmurze: IaaS, usługi w chmurze: PaaS; usługi w chmurze: SaaS.

25. **Usługi w chmurze: IaaS** – Infrastruktura jako usługa, tj. usługa polegająca na udostępnianiu odbiorcy możliwości przetwarzania, przechowywania, sieci i innych podstawowych zasobów obliczeniowych, w których odbiorca jest w stanie wdrażać i uruchamiać dowolne oprogramowanie, mogące obejmować systemy operacyjne i aplikacje. Odbiorca nie zarządza podstawową infrastrukturą chmury ani jej nie kontroluje, ale ma kontrolę nad systemami operacyjnymi, pamięcią masową i wdrożonymi aplikacjami; odbiorca może posiadać ograniczoną kontrolę nad wybranymi komponentami sieciowymi (np. nad zaporami sieciowymi hosta).

26. **Usługi w chmurze: PaaS** – Platforma jako usługa, tj. usługa polegająca na udostępnieniu odbiorcy możliwości wdrażania w infrastrukturze chmury aplikacji utworzonych lub nabytych przez odbiorcę, utworzonych przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę. Odbiorca nie zarządza podstawową infrastrukturą chmury, w tym siecią, serwerami, systemami operacyjnymi lub pamięcią masową, ani jej nie kontroluje, ale ma kontrolę nad wdrożonymi aplikacjami i ewentualnie ustawieniami konfiguracji środowiska hostującego aplikacje.

27. **Usługi w chmurze: SaaS** – Oprogramowanie jako usługa, tj. usługa polegająca na udostępnieniu odbiorcy możliwości korzystania z aplikacji dostawcy działających w infrastrukturze chmurowej. Aplikacje są dostępne z różnych urządzeń klienckich za pośrednictwem interfejsu cienkiego, takiego jak przeglądarka internetowa (np. poczta e-mail oparta na sieci Web) lub interfejsu programu. Odbiorca nie zarządza ani nie kontroluje podstawowej infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych, pamięci masowej, a nawet możliwości poszczególnych aplikacji, z możliwym wyjątkiem ograniczonych ustawień konfiguracyjnych aplikacji specyficznych dla użytkownika.

28. **Ustawa o obrocie** – ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2024 r. poz. 722 z późn. zm.).

29. **Dane eksportowalne** – zgodnie z art. 2 pkt 38) Data Act, do celów art. 23 do 31 i art. 35 Data Act, oznaczają dane wejściowe i wyjściowe, w tym metadane, bezpośrednio lub pośrednio wygenerowane bądź współwygenerowane w wyniku korzystania przez klienta z usługi przetwarzania danych zapewnianej przez dostawców usług przetwarzania danych lub osoby trzecie, z wyłączeniem wszelkich aktywów lub danych, które są objęte prawami własności intelektualnej lub są tajemnicami przedsiębiorstwa.

    Na potrzeby Standardu do usług w chmurze SaaS nie zalicza się:

    - aplikacji udostępnianych w ramach pakietów usług w chmurze: PaaS, jeżeli ich odbiorcą nie jest użytkownik końcowy (biznesowy) Banku,
    - licencji na aplikacje oraz usług związanych z aplikacjami gotowymi do działania w chmurze, których dostawca jednocześnie nie zapewnia działania ich w infrastrukturze chmurowej dostarczanej przez siebie lub przez swojego Poddostawcę,
    - subskrypcji usług dostawców danych (usługi danych cyfrowych) zgodnie z DORA.

30. **Wytyczne EBA** – Wytyczne w sprawie outsourcingu Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r.

31. **Zewnętrzny dostawca Usług ICT** – zgodnie z DORA oznacza przedsiębiorstwo świadczące Usługi ICT. Na potrzeby Standardu poprzez Zewnętrznego dostawcę Usług ICT rozumie się podmioty świadczące Usługi ICT na rzecz Banku.

32. **UKSC** – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.).

2. DODATKOWE DEFINICJE SZCZEGÓŁOWE

1. **Alerting** – automatyczny system powiadamiania o wystąpieniu zdarzeń lub przekroczeniu progów określonych w systemie monitoringu.

2. **API (Application Programming Interface)** – zestaw reguł i specyfikacji, które umożliwiają różnym programom komputerowym komunikowanie się ze sobą.

3. **APM (Application Performance Monitoring)** – monitorowanie wydajności aplikacji w czasie rzeczywistym, śledzące kluczowe metryki takie jak czas odpowiedzi, przepustowość i błędy.

4. **Autoskalowanie** – mechanizm automatycznego dostosowywania zasobów obliczeniowych (np. zwiększanie lub zmniejszanie liczby instancji serwerów) w odpowiedzi na zmieniające się obciążenie, w celu utrzymania wydajności i optymalizacji kosztów.

5. **Availability Zones (Strefy Dostępności)** – fizycznie oddzielone lokalizacje w obrębie jednego regionu chmurowego, zaprojektowane tak, aby izolować awarie i zapewnić wysoką dostępność aplikacji i danych.

6. **BCP (Business Continuity Plan)** – plan ciągłości działania, dokument opisujący kroki, jakie organizacja podejmuje, aby zapewnić kontynuację kluczowych operacji biznesowych w przypadku awarii lub katastrofy.

7. **BIA (Business Impact Analysis)** – analiza wpływu biznesowego, proces identyfikacji i oceny potencjalnych skutków przerw w działalności biznesowej.

8. **Blue/Green Deployment** – strategia wdrażania oprogramowania, która polega na posiadaniu dwóch identycznych środowisk produkcyjnych (niebieskiego i zielonego). Nowa wersja jest wdrażana na nieaktywnym środowisku, a po pomyślnych testach ruch jest na nie przełączany. Umożliwia szybki rollback.

9. **Bramki Jakości** – narzędzia i techniki stosowane w procesach CI/CD w celu kontroli i weryfikacji kodu.

10. **Canary Deployment** – strategia wdrażania oprogramowania, która stopniowo przenosi ruch użytkowników na nową wersję aplikacji, pozwalając na monitorowanie jej zachowania w środowisku produkcyjnym przed pełnym wdrożeniem.

11. **CI/CD (Continuous Integration/Continuous Delivery)** – zestaw praktyk i narzędzi mających na celu automatyzację, monitorowanie i ulepszanie procesów integrowania, testowania i dostarczania kodu, co pozwala na szybsze i częstsze wydawanie oprogramowania.

12. **Code Review** – systematyczna kontrola kodu źródłowego przez innych programistów w celu identyfikacji błędów, poprawy jakości kodu i zwiększenia bezpieczeństwa.

13. **CPU (Central Processing Unit)** – główny komponent przetwarzający operacje w systemie informatycznym. W kontekście metryk, monitoruje jego wykorzystanie.

14. **CTI (Cyber Threat Intelligence)** – zorganizowane, przetworzone i analizowane informacje o potencjalnych lub istniejących zagrożeniach cybernetycznych, które mogą być wykorzystane do proaktywnej obrony.

15. **CVSS (Common Vulnerability Scoring System) v3** – standard służący do oceny powagi luk w zabezpieczeniach oprogramowania. Składa się z trzech grup metryk: bazowej, czasowej i środowiskowej, które pozwalają na obiektywne oszacowanie potencjalnego wpływu luk.

16. **Dane wrażliwe** – dane, które ze względu na swój charakter wymagają szczególnej ochrony, np. dane osobowe, finansowe, medyczne.

17. **Deny by default** – zasada bezpieczeństwa, która nakazuje domyślne blokowanie wszelkiego ruchu, chyba że ruch ten jest wyraźnie dozwolony.

18. **DevOps** – zestaw praktyk łączących rozwój oprogramowania (Dev) z operacjami IT (Ops), mający na celu skrócenie cyklu rozwoju systemów przy jednoczesnym zapewnieniu wysokiej jakości, niezawodności i bezpieczeństwa.

19. **DR (Disaster Recovery)** – zestaw procesów i polityk służących do odzyskiwania lub kontynuowania infrastruktury technologicznej i systemów po awarii o dużej skali.

20. **FinOps** – dyscyplina zarządzania operacjami w chmurze, która łączy finanse i operacje, aby zwiększyć efektywność kosztową w środowiskach chmurowych.

21. **Hardening (Usług/Systemów)** – proces zabezpieczania systemu lub usługi poprzez redukcję jego powierzchni ataku, np. poprzez wyłączenie niepotrzebnych usług, usunięcie domyślnych konfiguracji, zastosowanie poprawek bezpieczeństwa.

22. **High Availability (HA) / Wysoka Dostępność** – zdolność systemu lub usługi do pozostawania dostępnym i operacyjnym przez długi czas, minimalizując przestoje. Obejmuje redundancję i mechanizmy przełączania awaryjnego.

23. **Hybride Multicloud** – model architektoniczny polegający na jednoczesnym wykorzystaniu i integrowaniu ze sobą najmniej dwóch różnych chmur publicznych (oraz chmury prywatnej lub infrastruktury lokalnej – on-premise).

24. **IaaS (Infrastructure as a Service)** – podstawowa kategoria usług chmurowych, w której Dostawca udostępnia zwirtualizowane zasoby obliczeniowe, sieciowe i magazynowe.

25. **IaC (Infrastructure as Code)** – praktyka zarządzania i provisioningu infrastruktury IT (serwerów, sieci, baz danych itp.) przy użyciu plików konfiguracyjnych, które są traktowane jak kod programu, z wykorzystaniem kontroli wersji.

26. **IAM (Identity and Access Management)** – zestaw procesów i technologii służących do zarządzania tożsamościami cyfrowymi oraz kontrolowania dostępu do zasobów IT w organizacji.

27. **ICT (Information and Communication Technology)** – technologia informacyjno-komunikacyjna, ogólny termin obejmujący technologie informacyjne i telekomunikacyjne.

28. **Integralność danych** – zapewnienie, że dane są dokładne, kompletne i spójne przez cały cykl ich życia oraz że nie zostały zmodyfikowane w nieautoryzowany sposób.

29. **I/O (Input/Output)** – operacje wejścia/wyjścia, odnoszące się do transferu danych między systemem komputerowym a nośnikiem danych lub urządzeniem peryferyjnym. W kontekście metryk monitoruje szybkość tych operacji.

30. **JIT (Just-in-Time Access) / Dostęp Tymczasowy** – polityka bezpieczeństwa, która przyznaje podwyższone uprawnienia tylko na określony, krótki czas i tylko wtedy, gdy są one faktycznie potrzebne.

31. **JSON (JavaScript Object Notation)** – lekki format wymiany danych, łatwy do odczytania i pisania przez ludzi oraz łatwy do parsowania i generowania przez maszyny. Często używany w API i logowaniu.

32. **Load Balancer (Równoważenie obciążenia)** – urządzenie lub oprogramowanie, które rozdziela ruch sieciowy równomiernie między wiele serwerów, poprawiając wydajność, niezawodność i dostępność aplikacji.

33. **Logi / Dzienniki zdarzeń** – zapisy działań, zdarzeń systemowych, błędów i innych danych, generowane przez systemy informatyczne. Są kluczowe dla monitorowania, audytowania i rozwiązywania problemów.

34. **Łatanie luk** – proces stosowania poprawek bezpieczeństwa (patchy) do oprogramowania w celu naprawy znanych podatności.

35. **Metryki** – dane liczbowe lub jakościowe zbierane z systemów i aplikacji, służące do monitorowania ich wydajności, stanu, dostępności i innych cech.

36. **Monitoring** – proces ciągłego zbierania i analizowania danych o stanie, wydajności i bezpieczeństwie systemów i aplikacji.

37. **MultiFactor Authentication** – uwierzytelnianie wieloskładnikowe zapewniające dodatkową ochronę podczas logowania. Podczas uzyskiwania dostępu użytkownicy przeprowadzają dodatkową weryfikację tożsamości, np. skanowanie odcisku palca lub wprowadzenie kodu otrzymanego na telefon.

38. **Network as Code** – praktyka zarządzania i provisioningu infrastruktury sieciowej przy użyciu plików konfiguracyjnych, które są traktowane jak kod programu, z wykorzystaniem kontroli wersji.

39. **On – premise** – infrastruktura informatyczna, której wszystkie zasoby takie jak serwery, pamięć masowa, aplikacji itp., są fizycznie umiejscowione w lokalnym data center Banku.

40. **PaaS (Platform as a Service)** – kategoria usług chmurowych, w której dostawca udostępnia platformę programistyczną i środowisko do tworzenia, uruchamiania i zarządzania aplikacjami bez konieczności zarządzania infrastrukturą bazową.

41. **Pipeline produkcyjny** – zautomatyzowany ciąg etapów (np. kompilacja, testowanie, wdrożenie), przez które przechodzi kod oprogramowania od momentu zatwierdzenia do środowiska produkcyjnego.

42. **Playbook** – zestaw predefiniowanych instrukcji lub procedur, które mają być wykonane w odpowiedzi na określone incydenty lub scenariusze awaryjne.

43. **PoLP (Principle of Least Privilege) / Zasada Najmniejszego Przywileju** – zasada bezpieczeństwa, zgodnie z którą każdemu użytkownikowi, programowi lub procesowi powinny być przyznane tylko minimalne uprawnienia niezbędne do wykonania jego funkcji.

44. **Poufność danych** – zapewnienie, że dane są dostępne tylko dla autoryzowanych użytkowników i nie są ujawniane nieuprawnionym osobom lub systemom.

45. **Prometheus** – otwartoźródłowy system monitorowania i alertowania, często wykorzystywany do zbierania metryk w środowiskach kontenerowych.

46. **Provisioning** – proces alokowania lub przygotowywania zasobów informatycznych (np. serwerów, baz danych, sieci) do użytku.

47. **RAM (Random Access Memory)** – pamięć o dostępie swobodnym, wykorzystywana do przechowywania danych tymczasowo używanych przez procesor. W kontekście metryk, monitoruje jej wykorzystanie.

48. **RCA (Root Cause Analysis)** – proces identyfikacji pierwotnej przyczyny problemu lub awarii, a nie tylko jego objawów, w celu zapobiegania powtórnym wystąpieniom.

49. **Region chmurowy** – zbiór centrów danych, położonych geograficznie blisko siebie, które są ze sobą połączone szybką siecią.

50. **Replikacja danych** – proces tworzenia i przechowywania wielu kopii danych w różnych lokalizacjach w celu zapewnienia ich wysokiej dostępności i odporności na awarie.

51. **Retencja danych** – określony czas przechowywania danych, zgodny z wymogami prawnymi, regulacyjnymi lub biznesowymi.

52. **Rollback** – proces przywracania systemu lub aplikacji do poprzedniego, stabilnego stanu po wykryciu problemów z nowym wdrożeniem lub zmianą.

53. **RPO (Recovery Point Objective)** – maksymalna dopuszczalna ilość danych, którą organizacja jest w stanie utracić w wyniku awarii. Mierzona jest w czasie (np. 15 minut oznacza utratę danych z ostatnich 15 minut).

54. **RTO (Recovery Time Objective)** – maksymalny dopuszczalny czas, w jakim system lub usługa muszą zostać przywrócone do działania po awarii, aby zminimalizować negatywny wpływ na biznes.

55. **RUM (Real User Monitoring)** – metoda monitorowania wydajności aplikacji, która zbiera dane bezpośrednio od rzeczywistych użytkowników, mierząc ich doświadczenia z perspektywy klienta.

56. **SCM (Source Code Management)** – systemy do zarządzania wersjami kodu źródłowego, które śledzą zmiany, umożliwiają współpracę i zarządzanie historią projektu.

57. **Secret Manager / Vault** – systemy do bezpiecznego przechowywania i zarządzania poufnymi danymi, takimi jak klucze API, hasła, certyfikaty itp.

58. **Security by Design** – podejście do projektowania systemów i aplikacji, w którym bezpieczeństwo jest integralnym elementem od samego początku cyklu życia produktu, a nie dodawane na końcu.

59. **SIEM (Security Information and Event Management)** – system zbierający, agregujący i analizujący logi i zdarzenia bezpieczeństwa z różnych źródeł w celu wykrywania, analizowania i reagowania na incydenty cybernetyczne.

60. **SLA (Service Level Agreement)** – umowa o poziomie usług, formalny dokument określający gwarantowany poziom usług, jak np. dostępność, wydajność, czas reakcji.

61. **SLO (Service Level Objective)** – cel poziomu usług, wewnętrzny, mierzalny cel określający pożądany poziom usługi, często bardziej rygorystyczny niż SLA.

62. **Syslog** – standardowy protokół do uniwersalnego przesyłania wiadomości z dzienników zdarzeń po sieci IP.

63. **Threat Intelligence Feeds** – kanały dostarczające aktualne informacje o zagrożeniach cybernetycznych, takie jak listy znanych złośliwych adresów IP, domen czy sygnatur złośliwego oprogramowania.

64. **Threat Hunting** – proaktywne poszukiwanie nieznanych lub zaawansowanych zagrożeń w sieci i systemach, które mogły ominąć automatyczne mechanizmy wykrywania.

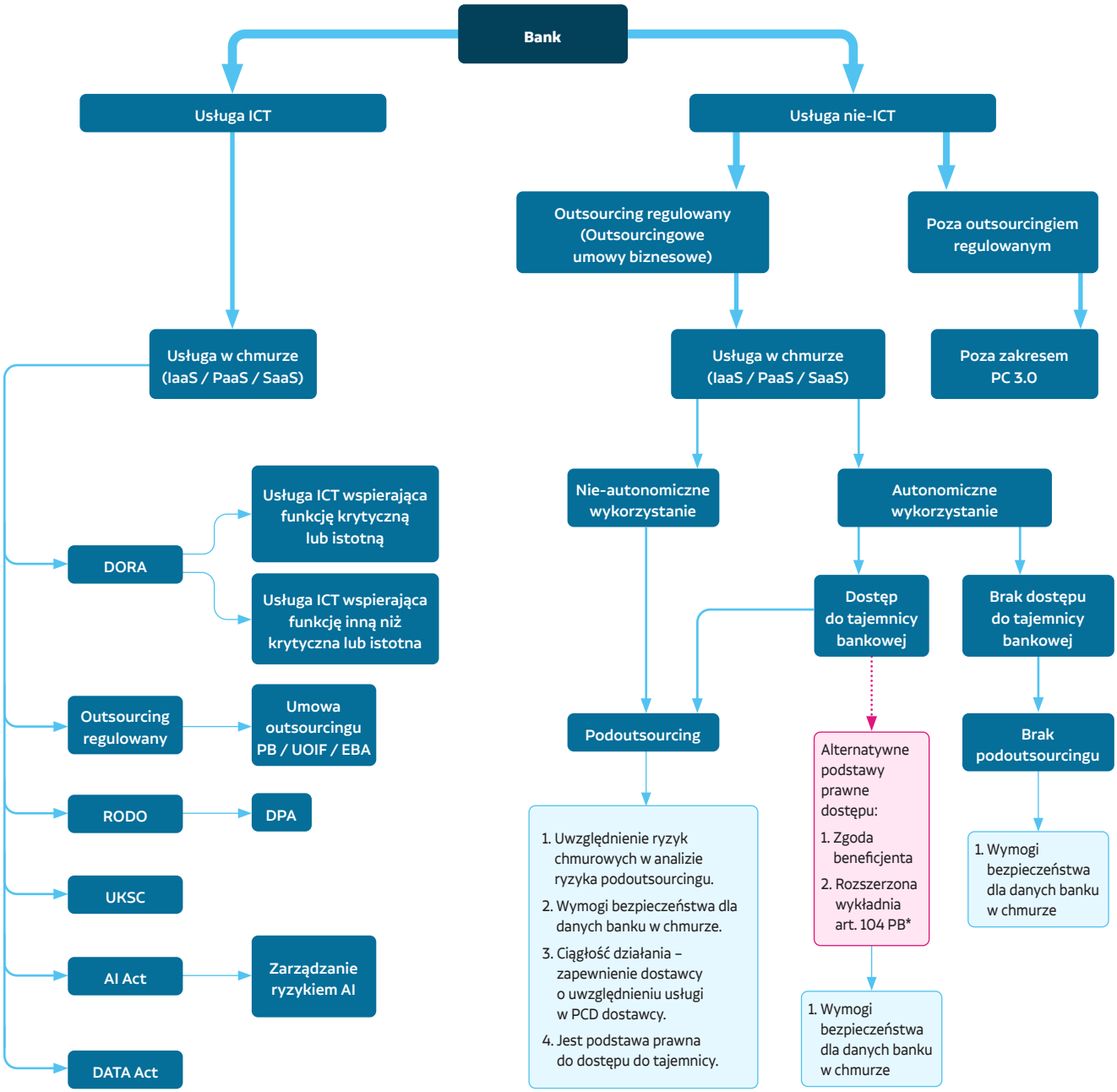
65. **TLS (Transport Layer Security)** – protokół kryptograficzny używany do zabezpieczania komunikacji w sieci, np. pomiędzy przeglądarką a serwerem.

66. **Wersjonowanie** – praktyka śledzenia i zarządzania zmianami w kodzie, konfiguracjach lub dokumentach, umożliwiająca odtworzenie wcześniejszych wersji.

67. **Wskaźniki poziomu usług** – mierzalne parametry, takie jak czas odpowiedzi, przepustowość, wskaźniki błędów, które określają jakość i dostępność usług.

ZAŁĄCZNIK NR 2

Schemat podstawowych zagadnień regulacyjnych



ZAŁĄCZNIK NR 3

Wymagania kontraktowe

Umowy chmurowe muszą zawierać konkretne klauzule wymagane przez DORA (niektóre akty wykonawcze), w tym:

	Wymaganie	Komentarz
	Umowy na wszystkie Usługi ICT	
1	Art. 30 ust. 1 DORA Prawa i obowiązki Banku i dostawcy są wyraźnie przypisane i określone na piśmie. Całość umowy obejmuje klauzulę o gwarantowanym poziomie usług i jest zawarta w jednym dokumencie mającym formę pisemną, który jest dostępny dla stron w wersji papierowej lub w dokumencie w innym formacie umożliwiającym pobieranie, zapewniającym trwałość i dostęp.	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. Forma pisemna wymagana przez DORA nie jest zastrzeżona pod rygorem nieważności.
2	Art. 30 ust. 2 lit. a) DORA Jasny i kompletny opis wszystkich funkcji i Usług ICT, które mają być świadczone przez zewnętrznego dostawcę Usług ICT, ze wskazaniem, czy dozwolone jest podwykonawstwo Usługi ICT wspierającej krytyczną lub istotną funkcję lub jej istotnych części, a jeżeli tak, to jakie warunki mają zastosowanie do takiego podwykonawstwa.	Umowa na świadczenie Usług ICT powinna zawierać precyzyjnie określony przedmiot umowy, tj. jasny i kompletny opis wszystkich czynności wykonywanych przez Dostawcę na rzecz Banku (rekomendowane posługiwanie się terminologią S1-S19). Dodatkowo należy wskazać, czy dozwolone jest podwykonawstwo Usługi ICT wspierającej krytyczną lub istotną funkcję lub jej istotnych części, a jeżeli tak, to jakie warunki mają zastosowanie do takiego podwykonawstwa. Rekomendowane jest, aby wszelkie prawa i obowiązki wskazane w umowie zostały precyzyjnie przypisane do jednej ze stron umowy, wraz z określeniem zasad odpowiedzialności za realizację danego obowiązku.

	Wymaganie	Komentarz
3	Art. 30 ust. 2 lit. b) DORA Miejsca, czyli regiony lub kraje, w których mają być świadczone funkcje i Usługi ICT objęte umową lub podwykonawstwem oraz w których mają być przetwarzane dane, w tym miejsce przechowywania, a także wymóg, aby zewnętrzny dostawca Usług ICT z wyprzedzeniem powiadomił podmiot finansowy, jeżeli przewiduje zmianę tych miejsc.	Strony powinny wskazać w umowie regiony lub kraje, w których: • świadczone są Usługi ICT, • przechowywane są dane Banku, • przetwarzane są dane Banku. Praktyka związana z przygotowaniem rejestru informacji dot. umów z Zewnętrznymi dostawcami Usług ICT (formularz SPR-PF-18) wymusza na Banku uzyskanie od Dostawcy informacji o konkretnym kraju, a nie regionie. Bank w umowie z Dostawcą powinien umieścić także wymóg, aby Zewnętrzny dostawca Usług ICT z wyprzedzeniem powiadomił Bank, jeżeli przewiduje zmianę tych miejsc (a także powiadomienie o dacie rozpoczęcia i zakończenia zmiany CPD). Ponadto Bank powinien rozważyć również wprowadzenie postanowień umownych, które mogą zminimalizować ryzyko utraty danych albo ryzyko niedostępności danych, np. konieczność uzyskania zgody podmiotu finansowego na zmianę lokalizacji.
4	Art. 30 ust. 2 lit. c) DORA Postanowienia dotyczące dostępności, autentyczności, integralności i poufności w związku z ochroną danych, w tym danych osobowych.	Bank powinien uzgodnić z Dostawcą zasady dostępu do danych, które posiada Dostawca, opisując przy tym zasady autentyczności, integralności i poufności danych. Dane w Rozporządzeniu DORA są rozumiane szeroko jako dane osobowe oraz nieosobowe, jako dane Banku, jak też dane klientów.
	Art. 30 ust. 2 lit. d) DORA Postanowienia dotyczące zapewnienia dostępu, odzyskiwania i zwrotu w łatwo dostępnym formacie danych osobowych i nieosobowych przetwarzanych przez podmiot finansowy w przypadku niewypłacalności lub rozwiązania zewnętrznego dostawcy Usług ICT, lub zaprzestania przez niego działalności gospodarczej, lub w przypadku wypowiedzenia ustaleń umownych.	Bank powinien zwrócić szczególną uwagę na kwestie zwrotu danych z Usług SaaS, w tym ich dostępność w odpowiednim formacie. Bank powinien również uwzględnić w umowie zasady usunięcia przez Dostawcę danych Banku po zakończeniu współpracy.
5	Art. 30 ust. 2 lit. e) DORA Opisy gwarantowanych poziomów usług, w tym ich aktualizacje i zmiany.	Usługi ICT powinny zawierać postanowienia dotyczące gwarantowanego poziomu usług, czyli SLA (Service Level Agreement) w tym ich aktualizacje i zmiany. Warunki SLA mogą być określone w załączniku do umowy (w tym możliwym do pobrania), o ile stanowi on integralną część umowy.
6	Art. 30 ust. 2 lit. f) Rozporządzenia DORA Obowiązek zapewnienia przez zewnętrznego dostawcę Usług ICT pomocy podmiotowi finansowemu, bez dodatkowych opłat lub za opłatą określoną ex ante, w przypadku wystąpienia incydentu związanego z ICT dotyczącego Usług ICT świadczonych na rzecz tego podmiotu finansowego.	Bank powinien zawrzeć w umowie postanowienia dotyczące pomocy Dostawcy względem Banku w przypadku wystąpienia incydentu dotyczącego świadczonych przez niego Usług ICT (np. zakres informacji niezbędnych do przygotowania przez Dostawcę powinien korespondować z zakresem zawiadomień SPR-PR-07,08,09). Jednym z elementów wspomnianych postanowień powinno być określenie już na etapie negocjacji umowy, czy pomoc Dostawcy będzie świadczona w ramach określonego wynagrodzenia (np. w cenie usługi), czy będzie wyceniona odrębnie (np. ryczałtowo).
7	Art. 30 ust. 2 lit. g Rozporządzenia DORA Obowiązek zewnętrznego dostawcy Usług ICT do pełnej współpracy z właściwymi organami oraz organami przymusowej restrukturyzacji podmiotu finansowego, w tym z osobami przez nie wyznaczonymi.	Szczegółowe postanowienia wg standardów organizacyjnych Banku (przede wszystkim terminowe udzielanie odpowiedzi na pytania organów, udostępnianie żądanych przez organ dokumentów i informacji).

	Wymaganie	Komentarz
8	Art. 30 ust. 2 lit. h) Rozporządzenia DORA Prawa do wypowiedzenia umowy i związane z tym minimalne okresy wypowiedzenia ustaleń umownych, zgodnie z oczekiwaniami właściwych organów i organów ds. restrukturyzacji i uporządkowanej likwidacji.	Dodatkowo należy zawrzeć wymagania opisane w art. 28 ust. 7 Rozporządzenia DORA określające minimalny zakres okoliczności uprawniających Bank do wypowiedzenia umowy: • poważne naruszenie przez Dostawcę Usług ICT obowiązujących przepisów, rekomendacji organów nadzoru lub postanowień umowy, • zidentyfikowanie przez Banku okoliczności, które mogą zmienić wykonywanie funkcji wspieranej przez dane Usługi ICT, wpłynąć na sytuację Dostawcy lub sposób realizacji umowy, • wykazanie słabych stron Dostawcy w zakresie jego ogólnego zarządzania ryzykiem związanym z ICT, w tym zapewnienia dostępności, autentyczności, integralności i poufności danych, • brak możliwości sprawowania przez właściwy organ skutecznego nadzoru nad Bankiem w związku z zawarciem lub realizacją danej umowy.
9	Art. 30 ust. 2 lit. i) Rozporządzenia DORA Warunki uczestnictwa zewnętrznych dostawców Usług ICT w opracowanych przez podmioty finansowe programach zwiększania świadomości w zakresie bezpieczeństwa ICT i szkoleniach w zakresie operacyjnej odporności cyfrowej zgodnie z art. 13 ust. 6.	Należy dokonać przy tym oceny zgodnie z art. 13 ust. 6 Rozporządzenia DORA, który określa, że programy skierowane są głównie do pracowników i kadry kierowniczej podmiotu finansowego, a objęcie nimi Dostawcy jest uzależnione od danej sytuacji. Umowa powinna przynajmniej przewidywać sposób ustalania udziału Dostawcy w szkoleniach lub definiować jego udział bardziej szczegółowo (np. limit godzin na szkolenia pracowników Dostawcy per rok). Forma szkoleń nie została określona przez treść Rozporządzenia DORA, w związku z czym mogą to być szkolenia online.
	Dodatkowe wymagania dla umów na Usługi ICT wspierające funkcje krytyczne lub istotne Banku	
10	Ustalenia umowne dotyczące korzystania z Usług ICT wspierających krytyczne lub istotne funkcje zawierają, oprócz elementów, o których mowa w art. 30 ust. 2 DORA, co najmniej wymienione dalej elementy.	
11	Pełne opisy gwarantowanych poziomów Usług ICT, w tym ich aktualizacje i zmiany, wraz z dokładnymi ilościowymi i jakościowymi celami w zakresie wyników w ramach uzgodnionych gwarantowanych poziomów Usług ICT, aby umożliwić podmiotowi finansowemu skuteczne monitorowanie Usług ICT oraz umożliwić bezzwłoczne podjęcie odpowiednich działań naprawczych w przypadku nieosiągnięcia uzgodnionych gwarantowanych poziomów Usług ICT.	Bank powinien zadbać, aby postanowienia dotyczące SLA zawierały dokładne ilościowe i jakościowe cele dotyczące poziomu świadczenia Usług ICT. SLA, o ile stanowią integralną część umowy i są możliwe do utrwalenia, mogą być udostępniane on-line (via linki). Umowa powinna określić, gdzie udostępniane są informacje na temat niedochowania SLA np. z uwagi na awarie, co również może się odbywać kanałami elektronicznymi. Z uwagi na obowiązek Banku do przeglądu SLA (cyklicznie lub ad hoc np. przy incydentach) i obowiązek wykazania (uwaga na terminy zgłoszeń), że doszło do pogorszenia/zdegradowania usługi chmurowej dla podmiotu finansowego wskutek awarii u Dostawcy chmury, postanowienia te powinny ułatwić Bankowi weryfikację, czy Dostawca osiąga uzgodnione SLA. W umowie należy zagwarantować także możliwość bezzwłocznego podjęcia działań naprawczych w przypadku nieosiągnięcia uzgodnionych gwarantowanych poziomów Usług ICT i możliwość domagania się rekompensaty (np. za niedostępności Usługi ICT). W przypadku rozwiązań multi-cloud lub chmury hybrydowej Bank powinien zwrócić uwagę na podział odpowiedzialności oraz SLA mające zastosowanie do konkretnych elementów rozwiązania albo do całości rozwiązania, co będzie zależało od ustaleń z Dostawcą / Dostawcami.

	Wymaganie	Komentarz
12	Art. 30 ust. 3 lit. b) Rozporządzenia DORA Okresy wypowiedzenia i obowiązki sprawozdawcze zewnętrznego dostawcy Usług ICT w stosunku do podmiotu finansowego, w tym powiadamianie o każdej zmianie, która może mieć istotny wpływ na zdolność skutecznego wykonywania przez tego dostawcę Usług ICT wspierających krytyczne lub istotne funkcje z zachowaniem uzgodnionych gwarantowanych poziomów Usług ICT.	Stosujemy Art. 30 ust. 2 lit. h) Rozporządzenia DORA (powyżej) jako minimum oraz dodatkowe (dłuższe) terminy wypowiedzenia dla Usług ICT wspierających krytyczne lub istotne funkcje. Strony określają w umowie okresy wypowiedzenia i obowiązki sprawozdawcze Dostawcy, w tym obowiązek powiadamiania Banku o każdej zmianie, która może mieć istotny wpływ na zdolność skutecznego wykonywania Usług ICT przez Dostawcę. Rekomendowane jest, aby uzgodnione przez strony zasady raportowania pozwoliły podmiotowi finansowemu na wykonanie jego obowiązków regulacyjnych (w tym notyfikacji do KNF). W ramach obowiązków sprawozdawczych powinna być także uwzględniona informacja o procesie wyboru Podwykonawców i ich ocenie przez Dostawcę, zgodnie z art. 3 RTS 2025/532.
13	Art. 30 ust. 3 lit. c) Rozporządzenia DORA Wymogi wobec zewnętrznego dostawcy Usług ICT w zakresie wdrażania i testowania planów awaryjnych w związku z prowadzoną działalnością oraz posiadania środków, narzędzi i polityk w zakresie bezpieczeństwa ICT zapewniających odpowiedni poziom bezpieczeństwa świadczenia Usług ICT przez podmiot finansowy zgodnie z jego ramami regulacyjnymi.	Szczegółowe zobowiązania Dostawcy w zakresie planów awaryjnych Dostawcy oraz bezpieczeństwa ICT u Dostawcy powinny korespondować z wewnętrznymi regulacjami Banku i jego wymaganiami dla Dostawców. Rekomendowane jest uwzględnienie wymogów wobec Dostawców opisanych w Części IV pkt 7. Standardu. Warto zawrzeć w umowie postanowienie dotyczące zapewnienia Bankowi wsparcia Dostawcy w realizacji innych obowiązków wynikających z DORA, jak art. 24 ust. 6 Rozporządzenia DORA, tj. obowiązku corocznego testowania systemów ICT.
14	Art. 30 ust. 3 lit. d) Rozporządzenia DORA Obowiązek uczestnictwa zewnętrznych dostawców Usług ICT w TLPT danego podmiotu finansowego i ich pełnej współpracy w tym zakresie, o czym mowa w art. 26 i 27.	Bank powinien zapewnić sobie skuteczne uprawnienie względem Dostawcy w zakresie przeprowadzania testów TLPT i pełnej współpracy w tym zakresie.
15	Art. 30 ust. 3 lit. e) Rozporządzenia DORA Prawo do monitorowania na bieżąco wyników osiąganych przez zewnętrznego dostawcę Usług ICT, które są szczegółowo opisane w punktach 16–19.	
16	Nieograniczone prawa dostępu, kontroli i audytu przez podmiot finansowy lub wyznaczoną osobę trzecią i przez właściwy organ oraz prawo sporządzania kopii odnośnej dokumentacji na miejscu, jeżeli mają one kluczowe znaczenie dla operacji zewnętrznego dostawcy Usług ICT, przy czym skutecznego wykonywania tych praw nie utrudniają ani nie ograniczają inne ustalenia umowne ani polityka w zakresie wdrażania.	W celu umożliwienia skutecznego wykonywania ww. uprawnień Banku, Dostawca powinien zobowiązać się do pełnej współpracy podczas kontroli i audytów, także tych na miejscu, przeprowadzanych przez właściwe organy nadzorcze, bezpośrednio przez Bank lub wyznaczoną przez nich osobę trzecią. Dostawca odpowiada za podpisanie umów ze swoimi Podwykonawcami, które gwarantują możliwość wykonania audytu przez Bank oraz upoważnione organy na podstawie umowy pomiędzy Bankiem a Dostawcą, w zakresie i na zasadach odpowiednich do tych zdefiniowanych przez Bank wobec Dostawcy (zgodnie z art. 3 ust 1 lit. b)–d) RTS 532). Obowiązek Dostawcy do monitorowania ryzyka ICT Podwykonawców obok obowiązku podmiotu finansowego do takiego monitorowania (zgodnie z art. 3 ust. 1 lit e)–h) oraz art. 3 ust. 2 RTS 532).
17	Prawo do uzgodnienia alternatywnych poziomów zabezpieczenia w przypadku naruszenia praw innych klientów.	
18	Obowiązek zewnętrznego dostawcy Usług ICT do pełnej współpracy podczas kontroli i audytów na miejscu przeprowadzanych przez właściwe organy, wiodący organ nadzorczy, podmiot finansowy lub wyznaczoną osobę trzecią.	
19	Obowiązek przekazywania szczegółowych informacji na temat zakresu, mających zastosowanie procedur i częstotliwości takich kontroli i audytów.	

	Wymaganie	Komentarz
20	Art. 30 ust. 3 lit. f) Rozporządzenia DORA Strategie wyjścia, w szczególności ustanowienie obowiązkowego odpowiedniego okresu przejściowego:	Umowa powinna określać strategię wyjścia, tj. plan postępowania w przypadku zakończenia współpracy stron. Uzgadniając postanowienia dotyczące możliwości wycofania się z umowy, należy uwzględnić wymagania art. 28 ust. 8 Rozporządzenia DORA, zgodnie z którym Podmioty finansowe zapewniają sobie możliwość wycofania się z ustaleń umownych bez: a) powodowania zakłóceń w swojej działalności, b) ograniczania zgodności z wymogami regulacyjnymi, c) szkody dla ciągłości i jakości Usług ICT świadczonych na rzecz klientów. Strategia wyjścia opisana w art. 30 ust. 3 Rozporządzenia DORA nie powinna być mylona z wewnętrznym dokumentem strategii wyjścia opisanym w art. 28 ust. 8 Rozporządzenia DORA (zob. Część IV pkt 9. Standardu).
20.1	podczas którego zewnętrzny dostawca Usług ICT będzie nadal zapewniał odpowiednie funkcje lub Usługi ICT w celu zmniejszenia ryzyka wystąpienia zakłóceń w funkcjonowaniu podmiotu finansowego lub w celu zapewnienia jego skutecznej uporządkowanej likwidacji i restrukturyzacji.	
20.2	który umożliwi podmiotowi finansowemu migrację do innego zewnętrznego dostawcy Usług ICT lub przejście na rozwiązania dostępne w ramach struktury wewnętrznej stosownie do stopnia złożoności świadczonej Usługi ICT.	
21	Bank jest zobowiązany do posiadania polityki dotyczącej monitorowania umów z Dostawcami usług chmury obliczeniowej dotyczących funkcji krytycznych lub istotnych. Zgodnie z art. 9 ust. 1 RTS 2024/1173 polityka powinna zawierać wymóg, aby w ustaleniach umownych określano środki i kluczowe wskaźniki służące bieżącemu monitorowaniu wyników zewnętrznych dostawców Usług ICT, w tym: • środki monitorowania przestrzegania wymogów dotyczących poufności, dostępności, integralności i autentyczności danych i informacji, • środki przestrzegania przez zewnętrznych dostawców Usług ICT odpowiednich polityk i procedur podmiotu finansowego, • środki mające zastosowanie w przypadku niewywiązania się z postanowień umów o gwarantowanym poziomie Usług ICT, w tym w stosownych przypadkach, kary umowne.	Jeśli podmiot wymaga, aby Dostawca chmury przestrzegał określonych wymagań /przepisów wewnętrznych, należy je wskazać (wykaz dołączyć do umowy).
22	Art. 3 Rozporządzenia delegowanego 2025/532 • wymogi z art. 3 RTS 2025/532 – Bank powinien przed zgodą na podwykonawstwo ocenić: proces wyboru podwykonawców, wiedzę dostawcy o podwykonawcach, dostęp o zdarzeniach u podwykonawców. • wymóg z art. 3 ust. 2 RTS 2025/532 – Bank powinien posiadać zasoby i wiedzę, aby ocenić ryzyko podwykonawców (w tym ryzyko koncentracji i geopolityczne).	Umowa powinna zobowiązywać Dostawcę do stosowania procesu należytej staranności w zakresie wyboru Podwykonawców i oceny ich ryzyka.

	Wymaganie	Komentarz
23	Art. 4 RTS 2025/532 warunki dopuszczenia podwykonawców przewidują, że dostawca usługi chmurowej: • ponosi odpowiedzialność za działania podwykonawców, • monitoruje wszystkie zlecane im Usługi ICT, • zapewnia sprawozdawczość wobec Banku (jeśli wymagane), • ocenia ryzyko lokalizacji podwykonawców i ich jednostki dominującej oraz ryzyko miejsca świadczenia Usług ICT, • zapewnia ciągłość Usług ICT w całym łańcuchu podwykonawców, w tym zapewnia (w umowie z podwykonawcą), że plany awaryjne mają odpowiednie SLA i że podwykonawca ma odpowiednie standardy bezpieczeństwa, • ma powiadomić podmiot finansowy o wszelkich istotnych zmianach w umowach podwykonawstwa.	Umowa z Dostawcą powinna obejmować przewidziane w omawianym artykule elementy. W odniesieniu do art. 4 ust. 1 lit. c) rekomendowane jest, aby Bank miał możliwość pozyskania od Dostawcy niezbędnych informacji w sytuacji, gdy informacje te są w posiadaniu Podwykonawcy. W szczególności obejmuje to informacje dotyczące incydentów ICT. W odniesieniu do art. 4 ust. 1 lit. d) rekomendowane jest, aby w celu weryfikacji realizacji tego obowiązku Bank miał możliwość weryfikacji dokumentów audytowych (np. certyfikatu) potwierdzających realizację procesu zarządzania Podwykonawcami zgodnego z tym wymogiem. Za istotną zmianę w umowie Podwykonawstwa rozumie się przede wszystkim zmiany, które dotyczą informacji archiwizowanych przez Bank w rejestrze informacji nt. umów ICT wymaganym przez DORA.
24	Art. 5 RTS 2025/532 Dostawca informuje Bank o planowanych istotnych zmianach w umowach podwykonawstwa z odpowiednim wyprzedzeniem.	W umowie z Dostawcą Bank określa rozsądny termin do wyrażenia sprzeciwu lub zatwierdzenia zmiany, którą Dostawca planuje w umowach podwykonawstwa.
25	Art. 6 RTS 2025/532 Bank ma prawo przewidzieć w umowie uprawnienie do wypowiedzenia umowy z dostawcą, jeśli zgłosił sprzeciw, a umowa podwykonawstwa została zawarta, albo jeśli dostawca zlecił podwykonawstwo, a nie zostało to wyraźnie dozwolone w umowie z dostawcą.	Bank nie ma obowiązku zamieszczania postanowień umownych wskazanych w tym artykule, jednakże jeśli widzi taką potrzebę, Dostawca nie może odmówić ich zamieszczenia w umowie.

Załącznik NR 4

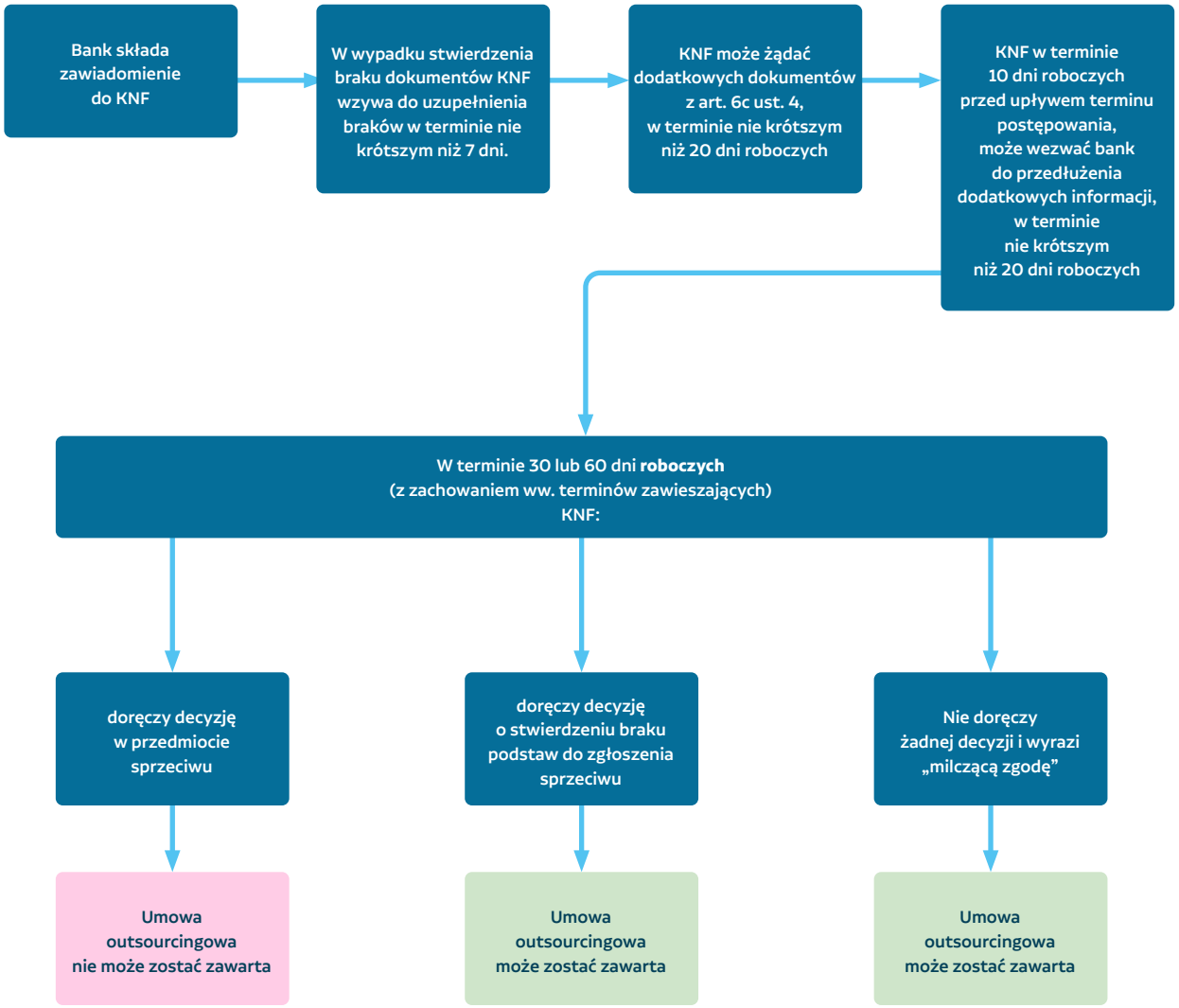
Notyfikacja umów na usługi w chmurze

	Typowe zdarzenia / Regulacja	Prawo bankowe via Portal KNF	Ustawa o obrocie via ESPI dla firm inwestycyjnych, banków z art. 70 i biur maklerskich	Wytyczne EBA dotyczące outsourcingu via Portal KNF	DORA via System sprawozdawczości DORA / System UKNF do zgłaszania incydentów
1	Zawarcie umowy z Dostawcą usługi chmury obliczeniowej.	Tak, o ile stosujemy art. 6d Prawa bankowego (siedziba lub miejsce przetwarzania poza EOG). Nie – jeśli siedziba i miejsca przetwarzania w EOG w łańcuchu).	Tak, wg art. 81d Ustawy o obrocie 14 dni po zawarciu umowy, o ile dotyczy podstawowych lub istotnych funkcji operacyjnych (wg art. 30 Rozporządzenia delegowanego 2017/565).	Tak, uprzednie wg pkt 58 Wytycznych, o ile dotyczy funkcji krytycznych lub istotnych albo jeśli funkcja zlecona stała się krytyczna lub istotna.	Tak, uprzednie (14 dni przed – art. 28.3 DORA oraz art. 18zi ustawy o nadzorze nad rynkiem finansowym[13]) w zakresie ustaleń umownych dotyczących korzystania z Usług ICT wspierających funkcje krytyczne lub istotne (formularz SPR-PF-19).
2	Zmiana umowy (czynność prawna), np. przedłużenie czasu obowiązywania, nowa rejestracja, nowe usługi związane z aneksowaniem umowy.	Tak, jeśli stosujemy art. 6d Prawa bankowego.	Tak, 14 dni po aneksie (tylko istotna zmiana, tj. w szczególności zmiana zakresu czynności).	Tak, tylko istotne zmiany umowy (pkt 59. Wytycznych).	Tak, 14 dni od dnia, w którym wspierana przez Usługę ICT funkcja stała się krytyczna (formularz SPR-PF-20).
3	Istotne zmiany operacyjne (np. nowe wdrożenie, wspieranie nowych funkcji, zmiana charakteru korzystania z niekrytycznego na krytyczne, objęcie przetwarzaniem nowych kategorii danych, bez czynności prawnej).	Nie ma obowiązku prawnego, może wynikać z dotychczasowej praktyki Banku.	Nie ma obowiązku, może wynikać z dotychczasowej praktyki Banku.	Tak, jeśli funkcja stała się krytyczna lub istotna.	Tak, 14 dni przed dniem związania się postanowieniami umownymi albo od dnia, w którym funkcja stała się krytyczna lub istotna (SPR-PF-20).
6	Zakończenie umowy (rozwiązanie, wypowiedzenie, wygaśnięcie).	Nie ma obowiązku prawnego, może wynikać z dotychczasowej praktyki Banku.	Tak, 14 dni po rozwiązaniu/wygaśnięciu.	Nie ma obowiązku prawnego, może wynikać z dotychczasowej praktyki Banku.	Nie.

13 Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz. U. z 2025 r. poz. 640 z późn. zm.).

	Typowe zdarzenia / Regulacja	Prawo bankowe via Portal KNF	Ustawa o obrocie via ESPI dla firm inwestycyjnych, banków z art. 70 i biur maklerskich	Wytyczne EBA dotyczące outsourcingu via Portal KNF	DORA via System sprawozdawczości DORA / System UKNF do zgłaszania incydentów
7	Umowa biznesowa z podoutsourcingiem chmurowym (zazwyczaj w podoutsourcingu jest SaaS), np. pośrednik kredytu hipotecznego korzystający z chmury.	Tak, jeśli stosujemy art. 6d Prawa bankowego do Dostawcy lub art. 6d ust. 1 pkt 2 Prawa bankowego do podoutsourcera. lub dalszego podoutsourcera (siedziba lub miejsce wykonywania poza EOG).	Analogicznie jak w pkt 1,2,3.	Tak, jeśli funkcja powierzona Dostawcy jest krytyczna lub istotna.	Nie.

Notyfikacje do KNF wg DORA na formularzu SPR-PF-17 – Bank ma obowiązek złożyć sprawozdanie roczne na temat liczby nowych ustaleń dot. korzystania z Usług ICT, kategorii zewnętrznych dostawców ICT, rodzaju ustaleń umownych oraz świadczonych Usług ICT i obsługiwanych funkcji, czyli podsumowanie aneksów.



Zagraniczny outsourcing bankowy – schemat postępowania z art. 6d Prawa bankowego

ZAŁĄCZNIK NR 5

FINOPS – fazy, uprawnienia i szkolenia

Faza początkowa	Polityka tagowania zasobów – zapewnienie podstawowej widoczności kosztów i przypisania zasobów do zespołów/projektów. Wdrożenie minimalnego zestawu tagów: • środowisko (environment): dev/test/prod, • zespół rozwijający (team): nazwa_zespołu, • aplikacja (application): nazwa_aplikacji bądź rozwiązania, • właściciel biznesowy (owner): imię_nazwisko, • źródło kosztu (costcenter): źródło finansowania indywidualne dla każdej z organizacji.
	Ustalenie obowiązkowego tagowania w narzędziach chmurowych.
	Automatyzacja tagowania przy użyciu Infrastructure as Code lub ustawień domyślnych w konsoli chmurowej.
	Przeprowadzenie szkolenia dla zespołów deweloperskich w zakresie znaczenia tagowania.
	Pokrycie tagowania: >90% zasobów otagowanych.
	Audyt tagowania: co najmniej raz na miesiąc.

	Optymalizacja kosztów – minimalizacja marnotrawstwa przy ograniczonych budżetach:
	• regularne przeglądy nieużywanych zasobów (np. instancje, wolumeny) w natywnych narzędziach Dostawców chmury obliczeniowej,
	• wdrożenie automatycznego wyłączania środowisk testowych poza godzinami pracy,
	• wykorzystanie instancji spot/preemptible – instalacje czasowe dla procesów krótkotrwałych, których poziom upustu jest największy,
	• ustawienie alertów budżetowych na dedykowanych konsolach chmurowych,
	• budżety muszą być ustawione dla każdej subskrypcji/projektu/konta,
	  – alerty muszą być skonfigurowane na co najmniej trzech poziomach progowych np: 50%, 70%, 90% budżetu,
	  – powiadomienia muszą być wysyłane e-mailem lub innym kanałem (w zależności od chmury), m.in. do właścicieli zasobów, zespołu finansowego,
	  – budżety muszą być przeglądane co miesiąc i aktualizowane zgodnie z planami projektowymi,
	  – usunięcie 100% nieużywanych zasobów w ciągu 7 dni od identyfikacji,
	  – monitorowanie kosztów w czasie rzeczywistym,
	  – zespoły muszą reagować na alerty w ciągu 24 godzin.

	Zarządzanie zobowiązaniami. Cel: maksymalizacja korzyści dla fazy początkowej przy minimalnych zobowiązaniach długoterminowych: • wykorzystanie darmowych kredytów chmurowych, • monitorowanie zużycia kredytów i planowanie ich wykorzystania, • przygotowanie do wdrożenia długoterminowych umów/zobowiązań, • miesięczne raporty zużycia kredytów, • wyznaczenie osoby odpowiedzialnej za komunikację z Dostawcą chmury.

Faza rozwojowa	Polityka tagowania zasobów – zwiększenie granularności i odpowiedzialności za koszty. Rozszerzenie zestawu tagów o: • utworzenie procesu korygowania brakujących tagów (np. automatyczne przypomnienia dla właścicieli zasobów), • integracja tagowania z pipeline'ami Continuous Integration i Continuous Delivery (CI/CD), • pokrycie tagowania: >95% zasobów otagowanych, • centralny zespół FinOps – odpowiedzialny za weryfikację tagowania.
	Optymalizacja kosztów – zrównoważenie wydajności i kosztów przy rosnącym zapotrzebowaniu: • wdrożenie rezerwacji zasobów dla stabilnych obciążeń (np. dla maszyn wirtualnych i bazy danych produkcyjnych), • wykorzystanie narzędzi natywnych rekomendacyjnych, • wdrożenie automatycznego skalowania dla obciążeń zmiennych, • wypracowanie standardów wewnątrz organizacji np. dotyczących usługi storage i modeli retencji danych, • organizacja miesięcznych przeglądów kosztów z zespołami („showback"), • testowanie alternatywnych modeli cenowych (np. serverless, kontenery), • oszczędności: 10-20% miesięcznych kosztów dzięki optymalizacjom, • regularne raporty optymalizacyjne dla zespołów.
	Zarządzanie zobowiązaniami – zabezpieczenie oszczędności przez strategiczne zobowiązania: • włączenie rocznych zobowiązań dla przewidywalnych obciążeń, • monitorowanie wykorzystania zobowiązań poprzez natywne rozwiązania Dostawcy chmury obliczeniowej, • prognozowanie kosztów na podstawie trendów, • wykorzystanie zobowiązań: >70% zakupionych zasobów w pełni wykorzystanych, • kwartalne przeglądy strategii zobowiązań.
Faza dojrzałości	Polityka tagowania zasobów – pełna odpowiedzialność kosztowa i granularne raportowanie: • generowanie szczegółowych raportów kosztowych dla zarządu na bazie wytworzony tagów, • mapowanie tagów na poziomie mikroserwisów/kontenerów, • pokrycie tagowania: 100% zasobów otagowanych.
	Optymalizacja kosztów – ciągłe doskonalenie efektywności kosztowej: • regularne audyty zasobów pod kątem marnotrawstwa (np. stare snapshoty, działające dyski powiązanie do niefunkcjonujących maszyn VM), • wdrożenie strategii rightsizingu i migracji do tańszych regionów/Dostawców, • wykorzystanie narzędzi AI/ML oraz natywnych rozwiązań np. alertów z anomaliami do predykcji zapotrzebowania i niespodziewanych skoków konsumpcji serwisów/usług chmurowych, • oszczędności: 20-30% rocznych kosztów dzięki zaawansowanym optymalizacjom, • miesięczne spotkania przed pionem odpowiedzialnym za część rozwojową i utrzymaniową w zakresie chmury w celu prezentacji oraz szerzenia wiedzy o zrealizowanych optymalizacjach i dobrych praktykach FinOPS.
	Zarządzanie zobowiązaniami – maksymalizacja oszczędności przy zachowaniu elastyczności: • włączenie 3-letnich zobowiązań dla stabilnych obciążeń, • zarządzanie portfelem zobowiązań w natywnych narzędziach, • wykorzystanie zobowiązań: >95% zakupionych zasobów w pełni wykorzystanych, • roczne planowanie strategicznych zobowiązań.
Uprawnienia	Efektywne zarządzanie kosztami i zasobami w środowisku chmurowym wymaga nie tylko odpowiednich kompetencji, ale również właściwego poziomu dostępu do konsoli. W kontekście FinOps, czyli praktyk łączących finanse i operacje IT, kluczowe jest zapewnienie osobie realizującej te działania odpowiednich uprawnień. W zależności od Dostawcy usług chmury obliczeniowej zarówno poziom tych uprawnień, jak i nazewnictwo mogą być różne, natomiast rekomendowanym jest, aby takie uprawniania obejmowały: dostęp do analizy kosztów, dostęp do rekomendacji, dostęp do subskrypcji i wgląd w zasoby, dostęp do struktury projektów / grup zasobów, dostęp do raportowania dashboardów, dostęp do alterowania, dostęp do tagowania zasobów.
Szkolenia	Szkolenia stanowią istotny element przygotowania i rozwoju osób pełniących funkcję FinOps. Obejmują one zarówno zagadnienia związane z analizą kosztów i optymalizacją zasobów, jak i znajomość narzędzi monitorujących, polityk tagowania, serwisów oraz usług w ramach publicznych Dostawców chmurowych. Dodatkowo, istotne są kompetencje miękkie, takie jak komunikacja między zespołami technicznymi i finansowymi oraz umiejętność prezentowania rekomendacji oraz danych.

ZAŁĄCZNIK NR 6

Podstawowy zbiór informacji na potrzeby realizacji planu wyjścia z usługi chmurowej

1. ZAKRES USŁUGI, FUNKCJONALNOŚCI BIZNESOWE

a W ramach tego punktu należy określić wykorzystanie rozwiązań chmurowych na użyteczności biznesowe wraz z funkcjonalnościami, połączeniami z innymi rozwiązaniami w organizacji, do kogo są one skierowane itp.

b Można ten punkt potraktować jako wstęp do strategii wyjścia i umieścić inne informacje, dla których trudno znaleźć właściwe miejsce, takie jak: kierunek migracji rozwiązania, retencja danych, architektura rozwiązania chmurowego i orientacyjna architektura rozwiązania w on-premise / u innego Dostawcy chmury.

2. OSOBY ODPOWIEDZIALNE ZA USŁUGĘ

Dostawca	Imię i nazwisko	Stanowisko	Adres e-mail	Zakres odpowiedzialności	Wymagana pracochłonność
Podmiot	**Imię i nazwisko**	**Stanowisko**	**Adres e-mail**	**Zakres odpowiedzialności**	**Wymagana pracochłonność**

Informacje o Dostawcy nie są wymagane, ponieważ Dostawca może nie wystawiać personalnie osób per usługa, a np. per całkowity dostęp do chmury w modelu PaaS lub w ramach usługi rozszerzonego suportu. Jeżeli są Poddostawcy, należy ich również wykazać.

a Ważne, aby w ramach tego punktu wykazać wszystkie osoby zaangażowane w utrzymanie rozwiązania po stronie podmiotu, tj. opiekun merytoryczny i techniczny, osoby od strony infrastruktury, sieci, bezpieczeństwa itp. Jeżeli nie można wskazać personalnie osób, wystarczy wskazanie właściwych ról/stanowisk wymaganych przy realizacji wyjścia z usługi.

b Warto w tym miejscu określić, czy wymagane będzie wsparcie/pracochłonność Dostawcy i czy zostało to określone w umowie. Po stronie podmiotu i właściwych ról też można określić szacowaną (na ile to możliwe na obecnym etapie) potrzebną pracochłonność danej roli.

3. LOKALIZACJA ZASOBÓW ORAZ ICH KONFIGURACJA, WYMAGANE LICENCJE

a Należy określić lokalizację usługi (region chmurowy) oraz docelowe miejsce (lokalizacja CPD podmiotu lub inny region chmurowy). W zakresie konfiguracji ważnym aspektem jest uwzględnienie aspektu czasu w wykazie (o ile jest to możliwe do określenia). W czasie funkcjonowania usługi będzie ona prawdopodobnie zwiększała swoje zapotrzebowanie na infrastrukturę, więc warto pomyśleć o wskazaniu konfiguracji inicjalnej i zakładanej po określonej liczbie lat. Takie podejście należy zastosować dla infrastruktury chmurowej i on-prem.

b Punkt ten można wykorzystać do opisania sposobu połączenia sieciowego z aktualnym Dostawcą chmury i jego zabezpieczenia.

c Jeżeli migracja rozwiązania będzie wymagała wykorzystania licencji, należy zweryfikować, czy podmiot finansowy nie posiada już licencji i czy wystarczające będzie odnowienie wsparcia. Na wypadek awaryjnego wyjścia z chmury można założyć dokupienie wsparcia.

4. MAPOWANIE WYKORZYSTYWANYCH USŁUG

W przypadku usług uruchamianych w modelu PaaS zaleca się zbudowanie matrycy informacji o uruchamianych komponentach chmurowych / SKU / serwisach wraz z ich rzutowaniem na sposób przeniesienia funkcji na dane rozwiązanie on-prem lub u innego dostawcy. Można tutaj odnosić się do wymaganych licencji, warto też zostawić miejsce na komentarz, który pozwoli doprecyzować zakres. Warto przygotować mapowanie w formie tabeli zgodnie z poniższym wzorem. Szczegółowość tabeli jest zależna od złożoności rozwiązania i chęci podmiotu do uszczegółowienia zagadnienia.

Obszar	Usługa chmurowa	Rozwiązanie docelowe – on-prem / inny Dostawca chmury	Uwagi
Środowisko uruchomieniowe aplikacji/ usług			
Baza danych			
backup			
Storage – przechowywanie plików			
Cache			
Proces CI/CD			
Logowanie			
Monitoring itp.			

5. WYMAGANIA BEZPIECZEŃSTWA

a W ramach strategii wyjścia warto określić założenia bezpieczeństwa. Może to polegać na weryfikacji wymagań bezpieczeństwa podmiotu co do nowego Dostawcy chmury oraz uzgodnień bezpieczeństwa w zakresie monitorowania po zakończeniu strategii wyjścia, czy komponenty chmurowe „odzywają się" po usunięciu usługi chmurowej.

6. WYDATKI ZWIĄZANE Z WYJŚCIEM Z USŁUGI

a Jest to jeden z trudniejszych elementów do oszacowania ze względu na swoją złożoność. Należy w tym miejscu uwzględnić wydatki na czynności określone powyżej, tj. pracochłonność Dostawcy i Banku, koszty związane z wymaganymi licencjami i infrastrukturą, koszty audytu bezpieczeństwa.

b Ważne jest, aby wydatki te wykazać w okresie np. 3- lub 5-letnim z uwzględnieniem inflacji. Pozwoli to możliwie najdokładniej opracować pulę, jaką trzeba przeznaczyć na realizację strategii wyjścia.

7. SCENARIUSZ MIGRACJI

a W zależności od zbudowanej usługi chmurowej scenariusz może być mniej lub bardziej rozbudowany, ponieważ rozwiązanie w modelu SaaS lub IaaS będzie znacznie mniej skomplikowane do migrowania niż rozwiązanie zbudowane w modelu PaaS.

b Właściwe jest, aby strategia zaczynała się od podjęcia przez decydentów decyzji o wyjściu z rozwiązania, a kończyła się na uzyskaniu potwierdzenia od Dostawcy chmury o bezpowrotnym usunięciu danych podmiotu oraz weryfikacji sygnału z końcówek po stronie chmury.

c Każdy z etapów powinien być opisany na tyle dokładnie, na ile jest to możliwe na obecnym etapie realizacji projektu. Etapy powinny mieć wskazaną osobę lub osoby odpowiedzialne za dany zakres, mieć wpisany orientacyjny czas realizacji, a także określać, czy możliwe jest jednoczesne realizowanie danego etapu z innym etapem. Można do tego wykorzystać poniższą tabelę, która we właściwy sposób pozwala usystematyzować informacje.

Lp.	Nazwa etapu	Opis etapu	Czas realizacji (dni)	Strona realizująca
1.	Podjęcie decyzji o wyjściu z rozwiązania chmurowego przez decydentów			
2.				
…				
…				
X-1	Usunięcie danych i serwisów z chmury			
X	Pozyskanie raportu o usunięciu danych bez możliwości ich przywrócenia			Dostawca chmury

ZAŁĄCZNIK NR 7

Obszary do analizy przez bank w zakresie vendor managementu

Zakres czynności Banku w obszarze Vendor Managementu	
Monitorowanie usługi w zakresie spełnienia gwarantowanych przez Dostawcę poziomów usługi opisanych w umowie.	
Weryfikacja prawidłowości informacji na temat podmiotu świadczącego usługę chmury obliczeniowej lub jego podwykonawcy, jak również ich dane rejestrowe.	
Identyfikacja kluczowych Podwykonawców w umowie dla usług chmurowych wspierających krytyczne lub istotne funkcje Banku. Ponadto należy zweryfikować:	• czy mechanizmy kontrolne stosowane przez Dostawcę w stosunku do podwykonawców, którzy świadczą usługi, wspierające w sposób istotny funkcje krytyczne lub istotne Banku, zapewniają właściwy poziom ich monitorowania; • łańcuch podwykonawstwa: czy pojawiły się w nim zmiany oraz jaki jest potencjalny wpływ złożoności łańcucha podwykonawstwa na zdolność do pełnego monitorowania umowy; • ryzyko związane z dostępem Podwykonawcy do informacji prawnie chronionej, w tym analiza incydentów; • ryzyko koncentracji Podwykonawcy pod kątem: – zawarcia wielu umów wspierających krytyczne lub istotne funkcje Banku, w ramach których Dostawca podpowierzył wykonanie usług wspierających krytyczne lub istotne funkcje Banku Podwykonawcy, którego nie można łatwo zastąpić, – posiadania wielu umów wspierających krytyczne lub istotne funkcje Banku, w których występuje ten sam Podwykonawca, wspierający krytyczne lub istotne funkcje Banku, lub z blisko powiązanymi Podwykonawcami wspierającymi krytyczne lub istotne funkcje Banku.
Wystąpienie zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania.	
Wystąpienie zmian w zakresie informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej.	
Wystąpienie zmian w skali przetwarzania informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej.	

Zakres czynności Banku w obszarze Vendor Managementu	
Zmiany lokalizacji centrum przetwarzania danych Dostawcy/Podwykonawcy usług chmury obliczeniowej:	• przestrzegania przez Dostawcę oraz kluczowych Podwykonawców standardów bezpieczeństwa informacji w zakresie: monitorowania incydentów lub nieprawidłowości w procesach dotyczących zarządzania logami oraz kluczami szyfrującymi; • obsługi incydentów/nieprawidłowości oraz definiowanie działań następczych, aby zapewnić zidentyfikowanie, udokumentowanie i wyeliminowanie podstawowych przyczyn, w celu zapobiegania występowaniu nieprawidłowości.
Koncentracja usług chmurowych u jednego Dostawcy oraz poziomu uzależnienia Banku w stosunku do zwiększania się udziału chmury obliczeniowej w Banku. **W szczególności należy ocenić:**	• ryzyko korzystania przez wiele podmiotów, w tym banków, z ograniczonej liczby Dostawców usług, co może negatywnie wpłynąć na jakość produktów lub uniemożliwić dostęp do zasobów w sytuacji awaryjnej; • ryzyko skupienia usług w ręku małej liczby usługodawców obsługujących znaczną część banków. Taka sytuacja może doprowadzić m.in. do uzależnienia od Dostawcy, a w rezultacie do niekorzystnych dla Banku renegocjacji umów; • udział działalności Banku w całkowitej działalności Dostawcy, tj. czy w sytuacji awaryjnej czynności powierzone Dostawcy przez Bank będą objęte procesem COB (Close of Bussines) Dostawcy w pierwszej kolejności. Jeśli nie, czy i jak może to wpłynąć na prawidłowe funkcjonowanie Banku w sytuacji awaryjnej; • ryzyko koncentracji powierzenia Dostawcy przez Bank znacznej ilości usług, co może doprowadzić do uzależnienia od Dostawcy, a w rezultacie do niekorzystnych dla Banku renegocjacji umów; • ryzyko wynikające z zawarcia umowy outsourcingowej z Dostawcą usług o dominującej pozycji, którego zastąpienie nie jest łatwe; • ryzyko zawarcia wielu umów outsourcingu z tym samym Dostawcą usług lub Dostawcami usług blisko ze sobą związanych.
Występowanie konfliktu interesów w ramach umowy z Dostawcami.	
Aktualna sytuacja finansowa Dostawców usług chmurowych lub ich kluczowych Podwykonawców oraz jej wpływ na ciągłość świadczonych usług.	
Zmiany otoczenia prawnego, regulacje, regulaminy lub postanowienia umów, których stroną jest Bank, oraz ich wpływ na zgodność postępowania Banku w kontekście przetwarzania informacji prawnie chronionych w chmurze obliczeniowej.	

Zakres czynności Banku w obszarze Vendor Managementu	
Zmiany otoczenia prawnego związane z jurysdykcją kraju, w którym odbywa się fizycznie przetwarzanie informacji (lokalizacja centrum przetwarzania danych), w szczególności czy zmiany spowodowały, że dopuszczalne jest żądanie dostępu do przetwarzanych w CDP informacji Banku dla organów administracji krajowej lub międzynarodowej bez zgody Banku lub przepisy prawa upadłościowego, które miałyby zastosowanie w przypadku upadłości zewnętrznego Dostawcy usług chmurowych/ usług ICT, a także wszelkie ograniczenia, które mogą powstać w związku z pilnym odzyskiwaniem danych Banku.	Przestrzeganie unijnych przepisów o ochronie danych i ich skutecznego egzekwowania w stosunku do kraju, w którym siedzibę ma Dostawca usług, z którym Bank planuje zawrzeć umowę dotyczącą korzystania z usług chmurowych/ICT wspierających krytyczne lub istotne funkcje.
	Testowanie planów awaryjnych w związku z prowadzoną działalnością w celu weryfikacji, czy Dostawca posiadania odpowiednie środki, narzędzia i polityki w zakresie bezpieczeństwa, zapewniające odpowiedni poziom bezpieczeństwa świadczenia usług, także w sytuacji niedostępności jego podwykonawców.
	Testowanie planu wyjścia dla usług wspierających krytyczne lub istotne funkcje — o sposobie i zakresie więcej informacji znajduje się w części Strategia Wyjścia w PolishCloud 3.0.
	Testowanie odporności cyfrowej, w tym testów TPLT, jeśli Bank je przeprowadza.
	Monitorowanie aktualności dokumentacji związanej z certyfikacją potwierdzającą zgodność usługi w chmurze z wymaganiami i normami prawnymi, tj. certyfikat oraz wyniki audytów certyfikacyjnych lub w przypadku braku certyfikatu, dokumentację potwierdzającą realizację wymagań i norm prawnych lub odpowiednich wymagań Banku.
	Audyty i kontrole przeprowadzone zgodnie z powszechnie przyjętymi standardami audytu oraz wszelkimi instrukcjami nadzorczymi dotyczącymi stosowania i włączania takich standardów audytu. W przypadku gdy umowy dotyczące korzystania z usług chmurowych/ICT zawarte z zewnętrznymi Dostawcami wiążą się z wysokim stopniem złożoności technicznej, Banki sprawdzają, czy audytorzy – zarówno wewnętrzni, jak i zewnętrzni lub grupa audytorów – posiadają odpowiednie umiejętności i wiedzę.
	Monitorowanie innych nieokreślonych powyżej obszarów, które mogą generować problemy w trakcie trwania umowy.

ZAŁĄCZNIK NR 8

Wytyczne dla dostawców usług chmurowych

Lokalizacja przetwarzania danych Banku	Dostawca usługi w chmurze wskazuje lokalizacje CPD, w których przetwarzane będą informacje Banku (kraj, region). Zaleca się, aby CPD było zlokalizowane na terenie EOG (o ile jest to uzasadnione z perspektywy kosztowej, jakościowej, ryzyka itp.).
	Wszelkie zmiany obszaru przetwarzania danych wymagają poinformowania/zgody Banku.
Dostęp do danych Banku oraz konfiguracji usługi w chmurze. **Dostawca usługi w chmurze dostarcza Bankowi informacje dotyczące:**	dostępu do przetwarzanych informacji, gwarantowanego 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 Banku;
	możliwości wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania;
	możliwości kontrolowania Dostawcy usługi w chmurze oraz jego Podwykonawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usługi w chmurze;
	możliwości kontrolowania gwarantowanej przez Dostawcę usługi w chmurze jakości usługi w chmurze;
	możliwości kontroli dostępu i urządzeń dostępowych użytkowników końcowych;
	wykorzystywanych Poddostawców z wyszczególnieniem: • zakresu świadczonych przez nich usług, • informacji o ich dostępie do danych, • lokalizacji siedziby, w przypadku usługi w chmurze wspierającej krytyczne lub istotne funkcje.

	podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji przy korzystaniu z usługi w chmurze;
	konsekwencji stosowania określonej architektury środowiska usługi w chmurze: mechanizmów izolacji zasobów używanych do świadczenia usługi w chmurze, w tym informacji o incydentach bezpieczeństwa związanych z naruszeniem, mechanizmów izolacji, możliwości migracji usługi/danych do innych Dostawców usług w chmurze lub ponowne włączenie ich do struktur wewnętrznych;
	interfejsów zarządzających usługami, które są udostępniane, i ich podatności oraz metod weryfikacji ich poprawności;
	zastosowanych mechanizmów bezpieczeństwa, dostępności i integralności przetwarzania w świadczonej usłudze w chmurze (obowiązujące w tym zakresie procedury obsługi oraz mechanizmy kontrolne mogą być dodatkowo opisane w udostępnionym przez Dostawcę raporcie certyfikującym (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji (lub równoważnym), w tym w zakresie: szyfrowania informacji przetwarzanych w Usłudze chmury obliczeniowej (zarówno „at rest", „in transit" jak i „in use"); stosowania domyślnie zasady braku dostępu do przetwarzanych informacji Banku; struktury uprawnień kont uprzywilejowanych w uruchamianych usługach; stosowania zasady „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez Bank oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem ze strony Banku, a cały proces obsługi i wykonania czynności jest logowany. natywnego uruchamiania nowego środowiska i/lub usługi separowanego od innych tenantów, z ustawieniami „secure-by-default"; zapewnienia mechanizmów logowania zdarzeń oraz dostępu Banku do logów. Logi mogą być przekazywane do Banku, w szczególności do SIEM. Logi muszą być zabezpieczone przed nieautoryzowanym dostępem, modyfikacją lub usunięciem.
Odpowiedzialność w ramach umowy na usługi chmury obliczeniowej wynikające z Prawa bankowego art. 6b: *(Bank jest obowiązany wprowadzić adekwatne i skuteczne rozwiązania zabezpieczające pokrycie ewentualnych kosztów związanych z wypłatą odszkodowania z tytułu roszczeń klientów lub osób trzecich o naprawienie szkody wyrządzonej wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej na usługi chmury obliczeniowej, której, przez przedsiębiorcę lub przedsiębiorcę zagranicznego w zakresie, w jakim nie poniósłby odpowiedzialności)*	zawarcie w umowie outsourcingowej na usługi chmury obliczeniowej postanowień przewidujących pełną odpowiedzialność przedsiębiorcy lub przedsiębiorcy zagranicznego za te koszty lub
	zawarcie odpowiedniej umowy ubezpieczenia odpowiedzialności cywilnej, gwarancji ubezpieczeniowej lub gwarancji bankowej, na podstawie której Bank jest uprawniony do otrzymania świadczenia w związku z tymi kosztami.
Kompetencje	Dostawca usługi w chmurze określa wymagane kompetencje przy korzystaniu z usługi w chmurze, ścieżki szkoleniowe i certyfikacyjne.
	Dostawca usługi w chmurze określa wymagane kompetencje wewnętrznych audytorów umożliwiające skuteczne przeprowadzanie odpowiednich audytów i ocen.
	Dostawca usługi w chmurze zobowiązuje się do udziału w szkoleniach organizowanych przez Bank w zakresie zwiększania świadomości bezpieczeństwa ICT i szkoleniach w obszarze operacyjnej odporności cyfrowej.
Kryptografia	Dostawca usługi w chmurze udostępnia rozwiązania organizacyjne i technologiczne umożliwiające szyfrowanie informacji Banku adekwatnie do wyniku analizy ryzyka – patrz rozdział 7.2.2 „Szyfrowanie i zarządzanie kluczami kryptograficznymi".

Plan ciągłości działania	Dostawca przekazuje aktualną wersję swojego planu ciągłości działania wraz z planem jego testowania.
	Każdorazowo, po przeprowadzeniu testów planu ciągłości działania, Dostawca usługi w chmurze powinien przekazać do Banku jego wynik.
	Dostawca usługi w chmurze uczestniczy w testach Bankowego planu ciągłości działania, jeśli Bank wyrazi taką potrzebę.
	Dostawca usługi w chmurze uwzględnia w planie ciągłości działania niedostępność swoich Poddostawców.
Zarządzanie incydentami (IT oraz bezpieczeństwa)	Dostawca usługi w chmurze posiada aktualny proces Zarządzania incydentami obejmujący udostępnianą Usługę w chmurze, zarówno w obszarze incydentów IT, jak i bezpieczeństwa.
Testowanie odporności cyfrowej	Dostawca usługi w chmurze przed udostępnieniem Bankowi usługi powinien objąć ją testami z wykorzystaniem: oceny podatności, w tym w zakresie analizy podatności bibliotek zewnętrznych, analizy otwartego oprogramowania wykorzystanego do świadczenia usługi w chmurze, oceny bezpieczeństwa sieci, fizycznych kontroli bezpieczeństwa, kwestionariuszy i oprogramowania skanującego, przeglądów kodu źródłowego (jeśli możliwe), testów scenariuszowych, kompatybilności i wydajności, testów TLPT.
	Testy odporności infrastruktury chmurowej Dostawcy mogą być przeprowadzone na zlecenie Banku, o ile Dostawca wyraża na to zgodę. W przeciwnym wypadku Dostawca powinien wskazać alternatywne rozwiązania organizacyjne potwierdzające regularne przeprowadzanie testów odporności cyfrowej lub wynik z niezależnego audytu, który potwierdza realizację tych procesów.
Dodatkowa dokumentacja (potwierdzenie Dostawcy)	Dostawca posiada i stosuje udokumentowane zasady dotyczące zarządzania hasłami i silnym uwierzytelnianiem chroniącym przed nieautoryzowanym dostępem do danych.
	Dostawca posiada i stosuje udokumentowane procedury i narzędzia zapewniające ochronę danych właściwą dla kwalifikacji informacji.
	Dostawca posiada udokumentowaną i przetestowaną politykę kopii zapasowych oraz proces odzyskiwania danych po awarii.
	Dostawca posiada udokumentowany i przetestowany plan przywracania po awarii (Disaster Recovery Plan) dla świadczonej usługi w chmurze.
	Posiadanie odpowiednich funduszy własnych na pokrycie tych kosztów.
Odpowiedzialność Banku wobec klienta Banku	Pełna odpowiedzialność Banku wobec klienta Banku za szkody wyrządzone za niewykonanie lub nienależyte wykonanie umowy na usługi chmury obliczeniowej. Nie można jej wyłączyć ani ograniczyć.

ZAŁĄCZNIK
NR 9

Szablon analizy dd/ analizy ryzyka (edytowalny)

Załącznik przedstawia przykładowe podejście do analizy ryzyka, obejmujące kolejne etapy procesu — od analizy wstępnej (ExAnte Risk Assessment) poprzez ocenę typu Due Diligence aż do końcowego oszacowania ryzyka związanego z dostawcą usług chmurowych.

Niniejsza publikacja zawiera załącznik w formacie .xlsx,
dostępny w bocznej zakładce niniejszego pliku PDF.

Nazwa pliku: Załącznik 9 – Ex_DD_Szacowanie_Ryzyka_Analiza.xlsx

Plik należy otworzyć za pomocą programu **Microsoft Excel**.

Wewnątrz dokumentu znajduje się szczegółowa instrukcja jego wykorzystania.

Pokaż/ukryj załącznik xlsx

Związek Banków Polskich