OUTSOURCING, USŁUGI ZEWNĘTRZNE IT W PRAKTYCE BANKOWEJ

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Piotr Truszczyński
Departament Inspekcji Bankowych
Warszawa, 31 stycznia 2019 roku

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Zagadnienia zarządcze
- Zagadnienia techniczne
- Zakres i skala stosowania
- Czynniki ryzyka
- Podsumowanie

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- **Definicje, wymogi prawne i regulacyjne**
- Zagadnienia zarządcze
- Zagadnienia techniczne
- Zakres i skala stosowania
- Czynniki ryzyka
- Podsumowanie

Definicje, wymogi prawne i regulacyjne

Outsourcing [outside resources using] - wykorzystanie zasobów zewnętrznych: ludzkich, technicznych oraz kompleksowych usług, świadczonych przez podmioty zewnętrzne na rzecz banku

Rodzaje - pełny - selektywny, stały - okazjonalny, krajowy – transgraniczny, …

Cechy - różnorodność rozwiązań, występujących zagrożeń, stosowanych zabezpieczeń, duża dynamika zmian i skali stosowania, kumulacja czynników ryzyka operacyjnego (w tym techniczne i prawne), konieczność bieżącej oceny zgodności i dostosowania procesu zarządzania usługami zewnętrznymi do zmian w przepisach prawa i regulacjach, środowisku biznesowym, technologii...

Ryzyko związane z powierzeniem przez bank usług do wykonania podmiotom zewnętrznym w obszarze IT stanowi czynnik ryzyka operacyjnego, zwiększający złożoność procesu zarządzania środowiskiem teleinformatycznym oraz zarządzania ryzykiem operacyjnym

Definicje, wymogi prawne i regulacyjne (Prawo bankowe)

Ustawa Prawo bankowe reguluje obszar czynności powierzonych podmiotom zewnętrznym (czynności bankowe oraz tzw. czynności faktyczne) a także wskazuje obszary, w których powierzanie czynności podmiotom zewnętrznym jest zabronione (zarządzanie i audyt wewnętrzny)

Art. 6a

Bank może, w drodze umowy zawartej na piśmie, powierzyć przedsiębiorcy lub przedsiębiorcy zagranicznemu, z zastrzeżeniem art. 6d, wykonywanie

- **czynności pośrednictwa … (w imieniu i na rzecz banku oraz innych czynności …)**
- **czynności faktycznych** związanych z **działalnością bankową**

Definicje, wymogi prawne i regulacyjne (Prawo bankowe)

Czynności faktyczne (katalog otwarty), najczęściej stosowane kryteria kwalifikacji

- dostęp podmiotu zewnętrznego do informacji wrażliwych z punktu widzenia prowadzonej działalności bankowej (tajemnica bankowa)
- znaczenie usług powierzonych podmiotowi zewnętrznemu dla krytycznych procesów bankowych
- dostęp do tajemnicy przedsiębiorstwa - ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (art. 11 ust. 4 ustawy) obejmuje informacje techniczne, technologiczne, handlowe, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności

art. 104 ust. 1 (zakres tajemnicy bankowej)

Bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje **wszystkie informacje dotyczące czynności bankowej**, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje

art. 171. 5 (odpowiedzialność)

Kto, będąc obowiązany do zachowania tajemnicy bankowej, ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową, niezgodnie z upoważnieniem określonym w ustawie, podlega grzywnie do 1 000 000 złotych i karze pozbawienia wolności do lat 3

Definicje, wymogi prawne i regulacyjne (Prawo bankowe)

Art. 6a. 7 (podwykonawstwo)

7. **Jeżeli umowa** powierzająca wykonywanie czynności, o których mowa w ust. 1, **to przewiduje, przedsiębiorca** lub przedsiębiorca zagraniczny, o którym mowa w ust. 1, **może powierzyć innemu przedsiębiorcy lub przedsiębiorcy zagranicznemu, w drodze odrębnej umowy, wykonywanie**

1) … **czynności** służących realizacji głównego świadczenia wynikającego z tej umowy, **po uzyskaniu pisemnej zgody banku**, lub

2) … **jednorazowo,** w przypadku gdy **w następstwie siły wyższej** nie może ich wykonywać samodzielnie, na **czas niezbędny do usunięcia przyczyn** uniemożliwiających wykonywanie tych czynności

Definicje, wymogi prawne i regulacyjne (Prawo bankowe)

Art. 6b. (odpowiedzialność banku i przedsiębiorcy)

Odpowiedzialności przedsiębiorcy lub przedsiębiorcy zagranicznego, o którym mowa w art. 6a ust. 1, wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy, o której mowa w art. 6a ust. 1 i 7, nie można wyłączyć ani ograniczyć

Odpowiedzialności banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy, o której mowa w art. 6a ust. 1 i 7, nie można wyłączyć ani ograniczyć

Art. 6c. Powierzenie przez bank wykonywania stale lub okresowo czynności, o których mowa w art. 6a ust. 1, może nastąpić …

1) bank i przedsiębiorca lub przedsiębiorca zagraniczny będą posiadać plany działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową;

Definicje, wymogi prawne i regulacyjne (Prawo bankowe)

Art. 6c. 3 (ewidencja umów) - umowy powierzenia czynności podmiotom zewnętrznym podlegają ewidencji (min. identyfikacja podmiotu, zakres usług, data obowiązywania umowy)

Art. 111 b. 1 **(obowiązek informacyjny)**

Bank obowiązany jest ogłaszać w sposób ogólnie dostępny informacje o **przedsiębiorcach lub przedsiębiorcach zagranicznych**, o których mowa w art. 6a ust. 1 i 7, **o ile** przy wykonywaniu na rzecz jednostki organizacyjnej banku albo innego przedsiębiorcy lub przedsiębiorcy zagranicznego czynności o których mowa w tych przepisach, **uzyskują dostęp do informacji chronionych tajemnicą bankową**

Definicje, wymogi prawne i regulacyjne (Uchwała 258/2011 KNF)

UCHWAŁA NR 258/2011 KOMISJI NADZORU FINANSOWEGO z dnia 4 października 2011 r. **w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem** i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku

Uchwała zastąpiona przez Rozporządzenie MFiR z marca 2017 r.

§ 11.1. (zakres odpowiedzialności)

Zarząd banku zapewnia zgodność działania banku z obowiązującymi przepisami prawa, z uwzględnieniem działania banku na podstawie przepisów prawa innego państwa **i powiązań banku z innymi podmiotami,** które mogłyby utrudnić skuteczne zarządzanie bankiem

Definicje, wymogi prawne i regulacyjne (Uchwała 258/2011 KNF)

§ 13. 8 W ramach realizowanych strategii i stosowanych procedur zarządzania ryzykiem bank wprowadza w szczególności:
d. **zasady zarządzania ryzykiem powierzenia wykonywania czynności podmiotom zewnętrznym**

§ 45. Na podstawie czynności kontroli wewnętrznej zarząd i rada nadzorcza banku otrzymują informacje dotyczące:

11) **czynności zlecanych przez bank do wykonania podmiotom zewnętrznym**

§ 54. Zarząd banku jest odpowiedzialny za odpowiednie ustalenie całkowitego wymaganego poziomu kapitału na pokrycie wszystkich istotnych rodzajów ryzyka i jego jakościową ocenę

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

Rozporządzenie Ministra Rozwoju i Finansów z 6.03.2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach
(obowiązuje od 1 maja 2017 r.)

§ 3 (organizacja systemu zarządzania ryzykiem)
system zarządzania ryzykiem i system kontroli wewnętrznej są zorganizowane na trzech niezależnych poziomach

1. zarządzanie ryzykiem w działalności operacyjnej
2. zarządzanie ryzykiem przez dedykowane stanowisko (lub komórkę organizacyjną) oraz niezależnie przez komórkę do spraw zgodności
3. działalność komórki audytu wewnętrznego

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 5 (zakres odpowiedzialności)

Zarząd zapewnia zgodność działania z przepisami prawa, z uwzględnieniem … **powiązań z innymi podmiotami, które mogłyby utrudnić skuteczne zarządzanie bankiem**

§ 12 (adekwatność metod zarządzania)

Dostosowanie metod (i częstotliwości czynności) identyfikowania i pomiaru lub szacowania ryzyka, kontroli ryzyka, monitorowania i raportowania do wielkości i profilu ryzyka

§ 13 (wykonywanie testów)

bank przeprowadza testy warunków skrajnych

(testy BCP, usługi podmiotów alternatywnych, przejęcie kompetencji)

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 14 (limity)

bank stosuje limity (wysokość zatwierdza zarząd), wysokość limitów jest dostosowana do zaakceptowanego przez radę nadzorczą ogólnego poziomu ryzyka

Analizy będące podstawą do określenia wysokości limitów są odpowiednio dokumentowane

§ 17 (sprawozdawczość zarządcza)

W banku funkcjonuje system sprawozdawczości zarządczej, wspomagający proces decyzyjny

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 18 (Regulacje wewnętrzne)

bank wprowadza i aktualizuje polityki i procedury zarządzania ryzykiem, określające w szczególności (pkt 8 w zakresie ryzyka operacyjnego)

d) zasady zarządzania ryzykiem powierzenia wykonywania czynności podmiotom zewnętrznym

f) zasady zarządzania ryzykiem systemów, związanych z prawidłowym, efektywnym i bezpiecznym wspieraniem działalności banku przez jego środowisko teleinformatyczne

§ 22 (Nadzór nad działalnością podmiotów zależnych)

W banku sprawowany jest nadzór nad ryzykiem związanym z działalnością podmiotów zależnych … zgodne z § 18

Definicje, wymogi prawne i regulacyjne (Rekomendacja M KNF)

Rekomendacja M KNF dotycząca zarządzania ryzykiem operacyjnym w bankach (2013)

Rekomendacja 4.28 Procesy realizowane przez podmioty zewnętrzne

- pisemne procedury zarządzania ryzykiem
- plany awaryjne (alternatywne źródło usług)

Rekomendacja 4.29 Bank odpowiada za czynności zlecone tak, jakby sam je wykonywał

Rekomendacja 4.30 Elementy uwzględniane w procesie powierzania czynności na zewnątrz

- struktura organizacyjna, system raportowania
- zgodność zakresu powierzanych czynności ze strategią działania banku
- zapewnienie monitorowania i kontroli (zarządzanie ryzykiem operacyjnym wynikającym ze zlecania czynności na zewnątrz), wykonywanie czynności kontrolnych w podmiotach zewnętrznych

Definicje, wymogi prawne i regulacyjne (Rekomendacja M KNF)

Rekomendacja 4.31 Czynności przed zawarciem / zmianą umowy

- określenie wpływu umowy na strategię, profil ryzyka, realizację wymogów prawnych i regulacyjnych
- określenie wpływu na ostrożne i stabilne zarządzanie bankiem, skuteczność systemu kontroli wewnętrznej w banku, badanie sprawozdania przez biegłego rewidenta, ochronę tajemnicy prawnie chronionej
- kontrola sytuacji finansowej, wizyta w siedzibie usługodawcy
- analiza skutków zawarcia umowy dla ryzyka braku zachowania ciągłości działania banku (z uwzględnieniem czynnika koncentracji usług)
- analiza planów awaryjnych banku na wypadek zaprzestania świadczenia usług przez usługodawcę
- zasady bezpiecznego zakończenia współpracy z usługodawcą

Definicje, wymogi prawne i regulacyjne (Rekomendacja M KNF)

Rekomendacja 11.7 weryfikacja jakości i skuteczności planów ciągłości działania i planów awaryjnych dostawcy

Rekomendacja 11.8 uwzględnienie w planach utrzymania ciągłości działania i planach awaryjnych banku alternatywnego źródła usług oraz zasobów niezbędnych do zmiany dostawcy usług w niezbędnym czasie

Rekomendacja 12.1 i 12.2 wykorzystanie ubezpieczenia ryzyka powierzonych czynności, monitorowanie adekwatności ubezpieczenia

Rekomendacja 12.3 zgodność z prawem procesu powierzania czynności (prawo krajowe oraz prawo w kraju działania usługodawcy)

Rekomendacja 12.4 kontrola działalności usługodawcy, określenie szczegółowych parametrów jakości usług, zasad podziału odpowiedzialności (brak klauzul wyłączających odpowiedzialność usługodawcy)

Rekomendacja 12.5 analiza działalności i sytuacji finansowej usługodawcy, źródła danych do analizy

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja D KNF dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013)

Rekomendacja 10 (formalizacja procedur)

Bank powinien posiadać **sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych**, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej banku

Rekomendacje szczegółowe

10.2 (odpowiedzialność)

Bank nie powinien traktować zlecania jakichkolwiek usług podmiotowi zewnętrznemu jako zwolnienia z odpowiedzialności za jakość i bezpieczeństwo usług świadczonych na rzecz klientów oraz bezpieczeństwo ich danych

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

10.3 proces doboru usługodawców (sytuacja finansowa dostawcy)

10.4 analiza ryzyka upadłości dostawcy, unikanie monopolizacji usług

10.5 monitorowanie i raportowanie jakości usług na potrzeby zarządu

10.6 w przypadku przetwarzania informacji wrażliwych, poza środowiskiem IT banku, stosowanie rozwiązań kontroli usługodawcy (szyfrowanie, raportowanie o incydentach, bezpieczne kończenie współpracy, certyfikacja np. ISO/IEC 27001:2005, testy penetracyjne etc.)

10.(7,11) kontrola usługodawców pod kątem stosowanych zabezpieczeń, zarządzania uprawnieniami pracowników, w tym administracyjnymi, etc.

10.9 i 10.10 zasady sporządzania i opiniowanie umów (dep. IT, prawny, bezpieczeństwa)

10.12 zasady migracji danych, czynności konserwacyjnych etc.

10.13 zasady przyznawania uprawnień dostępu i administracji prac. usługodawcy

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

10.8 (wymogi dotyczące umów z podmiotami zewnętrznymi)

- odpowiedzialność stron (efektywność dochodzenia roszczeń)
- zachowanie tajemnicy, (definicje, zagadnienia prawne)
- możliwość kontroli usługodawcy przez bank
- własność oprogramowania (kody źródłowe – składowanie i dostęp)
- parametry usług (minimalne wymogi, SLA)
- komunikacja i współpraca obsługa sytuacji awaryjnych, incydentów bezpieczeństwa, udział w testach, (włączenie do procesu zarządzania RO)
- zasady dalszego zlecania usług (tzw. podoutsourcing)
- kary umowne

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja 15

System zarządzania ciągłością działania banku powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi

Rekomendacja 15.6 uwzględnienie w procesie zarządzania ciągłością działania zewnętrznych dostawców usług o kluczowym znaczeniu

– ustalenie trybu komunikacji i współpracy na wypadek sytuacji awaryjnej

– zapewnienie udziału w procesie testowania systemu ciągłości działania

– zasady zmiany usługodawcy

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja 16 (kanały elektroniczne)

Bank świadczący usługi z wykorzystaniem elektronicznych kanałów dostępu powinien posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.

Rekomendacja 16.5 W przypadku, gdy w procesie świadczenia usług za pośrednictwem elektronicznych kanałów dostępu uczestniczą usługodawcy zewnętrzni, bank powinien upewnić się, że posiadają oni właściwe programy zarządzania bezpieczeństwem informacji przetwarzanych na rzecz banku, zgodne z przyjętymi w banku standardami

(stosowanie zasad analogicznych do wymogów Rekomendacji D KNF)

Definicje, wymogi prawne i regulacyjne (Rekomendacja dot. usług płatniczych KNF)

Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo – kredytowe

… Rekomendacja powinna być traktowana – w stosunku do banków – jako uzupełnienie wydanych przez KNF Rekomendacji D i M

Outsourcing IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- **Zagadnienia zarządcze**
- Zagadnienia techniczne
- Zakres i skala stosowania
- Czynniki ryzyka
- Podsumowanie

Zagadnienia zarządcze – zasada proporcjonalności

Identyfikacja skali i specyfiki (ryzyka) wykorzystania usług zewnętrznych w działalności banku (stosowanie zasady proporcjonalności) – wybrane czynniki

- analiza BIA (udział usług zewnętrznych IT w procesach bankowych)
- liczba aplikacji / systemów / komponentów wspieranych przez podmioty zewnętrzne w środowisku teleinformatycznym banku
- liczba usługodawców IT, liczba zawartych umów IT (w tym w zakresie przetwarzania danych wrażliwych)
- czas trwania umów (ekspozycja na ryzyko)
- lokalizacje geograficzne usługodawców IT (zagadnienia prawne)
- liczba podmiotów wspieranych przez poszczególnych usługodawców IT
- udział usługodawców w procesie BCM realizowanym przez bank
- koszty ponoszone na rzecz podmiotów zewnętrznych IT

Zagadnienia zarządcze – zasada proporcjonalności

Proces zarządzania ryzykiem powierzenia czynności podmiotom zewnętrznym powinien uwzględniać zasadę proporcjonalności

- struktura zarządzania (schemat organizacyjny, zakresy czynności, obsada)
- alokowane zasoby (kwalifikacje, szkolenia, specjalizacja, wsparcie)
- regulacje wewnętrzne (okresowy przegląd i aktualizacja),
- proces monitorowania usługodawców i jakości usług (SLA, KPI)
- zakres gromadzonych informacji (zdarzenia i straty operacyjne, inne informacje)
- zakres i częstotliwość informacji zarządczej (limity, KRI)
- szacowanie ryzyka (metodyka, czynniki ryzyka)
- rola usługodawców zewnętrznych w procesach BCM
- uwzględnienie usługodawców w procesie kontroli i audytu

Zagadnienia zarządcze

Umowy z usługodawcami IT, wybrane elementy

- strony, reprezentacja, przedmiot, data zawarcia, czas trwania, zasady przedłużenia / wypowiedzenia
- prawa autorskie, depozyt kodów (w przypadku oprogramowania)
- jakość usług, zasady odpowiedzialności (kary umowne), właściwość sądu
- wysokość i zasady zapłaty wynagrodzenia
- określenie zasad komunikacji i osób do kontaktu
- tryb i zasady zgłaszania sytuacji awaryjnych przez bank i usługodawcę
- zasady raportowania zdarzeń i incydentów na potrzeby zarządzania RO i bezpieczeństwem informacji
- zasady realizacji testów BCP, parametry RTO, KPI, SLA
- klauzule zachowania poufności informacji i danych
- zasady ew. dalszego zlecania czynności (podwykonawstwo)
- możliwości wykonywania kontroli usługodawcy przez bank i KNF

Zagadnienia zarządcze

Cykl życia umów z usługodawcami IT

- uzasadnienie celowości powierzenia czynności podmiotowi zewnętrznemu
- kryteria, uzasadnienie, wybór dostawców głównych i alternatywnych
- analiza projektu umowy pod kątem zgodności z prawem, wpływu na profil ryzyka, zgodność ze strategią
- analiza sytuacji finansowej i prawnej podmiotu zewnętrznego
- zawarcie umów (zgodność trybu zawarcia z regulacjami wewnętrznymi)
- monitorowanie wykonania umów (jakość, bezpieczeństwo, zgodność)
- raportowanie zdarzeń i strat operacyjnych, informacja zarządcza
- kontrole usługodawców (na miejscu i analizy „zza biurka”)
- decyzje operacyjne i strategiczne: kontynuowanie współpracy, renegocjacja umowy, zmiana usługodawcy, przejęcie usługodawcy przez bank, przejęcie usługi etc.
- zapewnienie możliwości sprawowania nadzoru przez regulatora

Zagadnienia zarządcze

Źródła danych w procesie weryfikacji usługodawcy

- sytuacja finansowa, bufor kapitałowy, zadłużenie
- struktura właścicielska
- historia współpracy
- ubezpieczenie OC, kwota, zakres ochrony, klauzule wyłączające
- skargi reklamacje, sprawy sądowe
- rotacja zatrudnienia
- certyfikaty, szkolenia pracowników
- wyniki audytu w tym badanie sprawozdań finansowych (GPW)
- wyniki testów planów BCP (zasoby awaryjne)
- standardy zabezpieczeń IT stosowane przez usługodawcę, ochrona fizyczna
- wyniki kontroli własnych banku

Zagadnienia zarządcze – proces zarządzania

Elementy procesu zarządzania ryzykiem powierzania czynności podmiotom zewnętrznym

- regulacje wewnętrzne (formalne zasady i limity)
- dedykowane zasoby po stronie banku
- kompleksowa identyfikacja ryzyka (źródła danych: proces doboru usługodawców, rejestry zdarzeń, strat, reklamacji, incydentów IT, etc.)
- włączenie procesu zarządzania usługami zewnętrznymi do kompleksowego procesu zarządzania ryzykiem operacyjnym banku
- monitorowanie ryzyka (KRI/KPI/SLA, limity, matryce ryzyka)
- system informacji zarządczej (w tym okresowy przegląd i ocena umów)
- mitygacja ryzyka (ubezpieczenia, dostawcy alternatywni)
- kontrola wewnętrzna
- niezależny audyt, (wnioski, zalecenia, monitorowanie wykonania)
- decyzje zarządcze

Zagadnienia zarządcze

Regulacje wewnętrzne dotyczące powierzania czynności

- strategia (dokument, zatwierdzany przez RN) określający główne zasady powierzania czynności (wyłączenia), akceptowane ryzyko, plany w zakresie korzystania z usług zewnętrznych w okresie realizacji strategii)
- polityka …
- instrukcja operacyjna (dla komórek IT i innych), zasady doboru usługodawców, proces zarządzania, odpowiedzialność, kompetencje, zasoby, limity, etc.
- regulacje dotyczące procesu zarządzania ryzykiem operacyjnym (zdarzenia, straty, KRI / KPI, limity, mapy ryzyka, analizy scenariuszowe, SIZ)
- regulacje dotyczące planowania awaryjnego

Zagadnienia zarządcze

Wybrane elementy procedur wewnętrznych

- dopuszczalny zakres usług zlecanych podmiotom zewnętrznym
- zasady wstępnej analizy ryzyka powierzanej czynności (standard oceny)
- zasady weryfikacji planów awaryjnych i zabezpieczeń stosowanych przez usługodawcę (testy, kontrole na miejscu, dokumentacja)
- zasady nadzoru i monitorowania powierzonych czynności (właścicielstwo po stronie banku), SLA, KPI
- zakres opiniowania (komórki merytoryczne, KRO)
- ścieżka i kompetencje decyzyjne
- zasady raportowania na potrzeby zarządu, RO, KRO, BCP/BCM
- zasady zabezpieczenia danych i informacji przez usługodawcę
- zasady ubezpieczenia powierzonych czynności
- zasady kontroli i audytu powierzonych czynności
- zabezpieczenie możliwości kontroli ze strony banku i KNF
- zasady zakończenia realizacji umowy

Zagadnienia zarządcze – podział zadań

Podział zadań w procesie zarządzania usługami zewnętrznymi

- **rada nadzorcza,** planowanie strategiczne, limit ogólny ryzyka, polityka, ocena pracy zarządu (komitet ryzyka, komitet audytu)
- **zarząd,** planowanie średnio i krótkoterminowe, wybór rozwiązań, negocjacje umów, organizacja procesu zarządzania, ustalenie parametrów i limitów szczegółowych
- **komitet ryzyka operacyjnego,** analiza rozwiązań w aspekcie prawnym, operacyjnym, bezpieczeństwa, technicznym, monitorowanie jakości i ryzyka, opracowanie informacji zarządczej, (propozycje decyzji zarządu)
- **komórka ryzyka operacyjnego** (gromadzenie danych o stratach i zdarzeniach wz. z usługami zewnętrznymi – monitorowanie ryzyka), opcjonalnie stanowisko ds. outsourcingu (koordynacja działań)
- **departament prawny** – ocena umów i procedur powierzania czynności w zakresie ryzyka prawnego i regulacyjnego

Zagadnienia zarządcze – podział zadań

- **departament utrzymania IT** – parametryzacja umów pod kątem wymogów technicznych, monitorowanie dostępności, identyfikacja ryzyka wz. skalowalności rozwiązań,
- **departament rozwoju IT** – monitorowanie umów pod kątem wymagań zgodności z architekturą i rozwojem środowiska teleinformatycznego
- **departament bezpieczeństwa** – analiza i parametryzacja umów pod kątem bezpieczeństwa danych, skuteczności stosowanych zabezpieczeń
- **departament ciągłości działania** – uwzględnienie usług zewnętrznych w procesie BCM
- **departamenty merytoryczne (biznesowe),** właściciele aplikacji i systemów - analiza funkcjonalności, usług zewnętrznych, rozwój funkcji merytorycznych, Podsumowanie współpracy

Kontrola wewnętrzna – w zakresie kompetencji poszczególnych komórek

- **komórka zgodności** – analiza zgodności pod kątem przepisów i procedur
- **audyt wewnętrzny** – ocena jakości i zgodności zarządzania ryzykiem usług zewnętrznych na potrzeby zarządu i rady nadzorczej

Zagadnienia zarządcze

Horyzont czasowy umów - ekspozycja na ryzyko

- do roku, bieżące (operacyjne)
- 1 – 3 lat, średnioterminowe
- powyżej 3 lat, bezterminowe (strategiczne)

Przyczyny stosowania usług zewnętrznych IT

- ograniczenie kosztów działania
- dostęp do innowacji, specjalistycznych technologii
- ograniczona dostępność własnych zasobów (technicznych IT, ludzkich)
- presja konkurencyjna, szybka reakcja na zapotrzebowanie rynku

Sposoby powierzania usług

- przekształcenia organizacyjne (wydzielenie podmiotu usługodawcy ze struktury organizacyjnej banku)
- przeniesienie usług do podmiotu z grupy kapitałowej (przejęcie banku)
- bezpośrednie powierzenie usług podmiotowi zewnętrznemu

Zagadnienia zarządcze

Zarządzanie usługami IT w grupach bankowych

- funkcjonowanie w środowisku międzynarodowym (podmioty zależne) lokalizacja systemu wyliczania BFG
- wykorzystanie środowisk podmiotów dominujących (instancje)
- stosowanie jednolitych zasad funkcjonowania usług IT w grupie (niezależność decyzyjna)

Ustawa 10.06.2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji

Art. 28. 1. Podmiot objęty systemem gwarantowania jest obowiązany do utrzymywania systemu wyliczania. **2. System wyliczania oraz uzyskiwane i przetwarzane w nim dane nie mogą znajdować się poza terytorium Rzeczypospolitej Polskiej.**

Zarządzanie usługami IT w bankach spółdzielczych

- samodzielność decyzyjna (wzorce opracowane w zrzeszeniach)
- ograniczony zakres możliwości kontrolnych w odniesieniu do usługodawców
- niewielkie zasoby dedykowane w procesie zarządzania

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Zagadnienia zarządcze
- **Zagadnienia techniczne**
- Zakres i skala stosowania
- Czynniki ryzyka
- Podsumowanie

Zagadnienia techniczne - zakres usług

Wybrane usługi zewnętrzne (IT)

- dostawa sprzętu i oprogramowania (standardowego)
- usługi doradcze, konsulting, testy penetracyjne
- utrzymanie sieci WAN / LAN, obsługa komunikatów SMS / GSM
- utrzymanie ośrodków przetwarzania danych
- utrzymanie (administracja) zabezpieczeń (firewall, IDS, SIEM, etc.…)
- zarządzanie bezpieczeństwem środowiska IT, testy zabezpieczeń
- utrzymanie i administracja środowisk fizycznych,
- zarządzanie systemami operacyjnymi serwerów, stacjami roboczymi
- zarządzanie aplikacjami, bazami danych
- utrzymanie aplikacji i serwisów bankowych
- produkcja oprogramowania (dedykowanego)
- wdrożenie i rozwój krytycznych platform bankowych
- realizacja procesu BCM

Zagadnienia techniczne - zakres usług

Wybrane inne usługi zewnętrzne

- autoryzacja transakcji internetowych (3 D Secure)
- autoryzacja transakcji bankomatowych, cash back
- infolinie, call center, usługi service desk
- produkcja kart bankowych
- obsługa korespondencji masowej
- skanowanie, archiwizacja dokumentacji bankowej
- chmury obliczeniowe, etc …

Podział na potrzeby oceny ryzyka

- usługi zewnętrzne od których uzależnione jest bezpieczeństwo i dostępność usług świadczonych przez bank na rzecz klientów
- usługi wymagające dostępu do tajemnicy bankowej i danych osobowych klientów
- pozostałe usługi

Zagadnienia techniczne - wymogi

Wymogi techniczne wz. zlecanych usług IT

- architektura rozwiązań (zgodność z architekturą środowiska banku)
- stosowane technologie (wsparcie producenta), możliwości rozwoju (skalowalność rozwiązań)
- bezpieczeństwo (standardy, stosowane zabezpieczenia, certyfikacja, zarządzanie uprawnieniami pracowników zewnętrznych)
- dostępność usług aspekt techniczny (parametry SLA, utrzymanie)
- adekwatność zasobów awaryjnych i zapasowych (ciągłość działania)
- współdzielenie zasobów: centra danych, zabezpieczenia fizyczne, sieci, kontrola dostępu, zarządzanie dostępem
- wirtualizacja, instancje aplikacji, (cloud computing)
- koncentracja usług po stronie usługodawcy, współzależność i dostępność usług, wykonalność procedur BCP

Zagadnienia techniczne - mitygacja

Elementy efektywnego procesu zarządzanie usługami zewnętrznymi IT

- analiza ryzyka komponentów środowiska IT
- zapewnienie właścicielstwa umów IT, systemów i procesów (po stronie banku – proces BIA)
- proces BCM, opracowanie planów awaryjnych i realizacja testów
- zapewnienie dostawców alternatywnych (activ - activ)
- procesu zarządzania ryzykiem operacyjnym usług zewnętrznych IT (identyfikowanie, monitorowanie, raportowanie, reagowanie)
- utrzymanie niezbędnych kompetencji własnych
- dostęp do kodów źródłowych (aktualizacja, zabezpieczenie)
- dokumentacja (usługi, proces, aplikacje, dostępność dokumentacji)
- analiza sytuacji usługodawcy (zdolność pokrywania ew. roszczeń banku)
- stosownie zabezpieczeń prawnych i ubezpieczeń

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Zagadnienia zarządcze
- Zagadnienia techniczne
- **Zakres i skala stosowania**
- Czynniki ryzyka
- Podsumowanie

Zakres i skala stosowania

Skala stosowania usług zewnętrznych* - obszar IT

Systemy krytyczne (ogółem) 48,5%

- max: 107
- min: 0

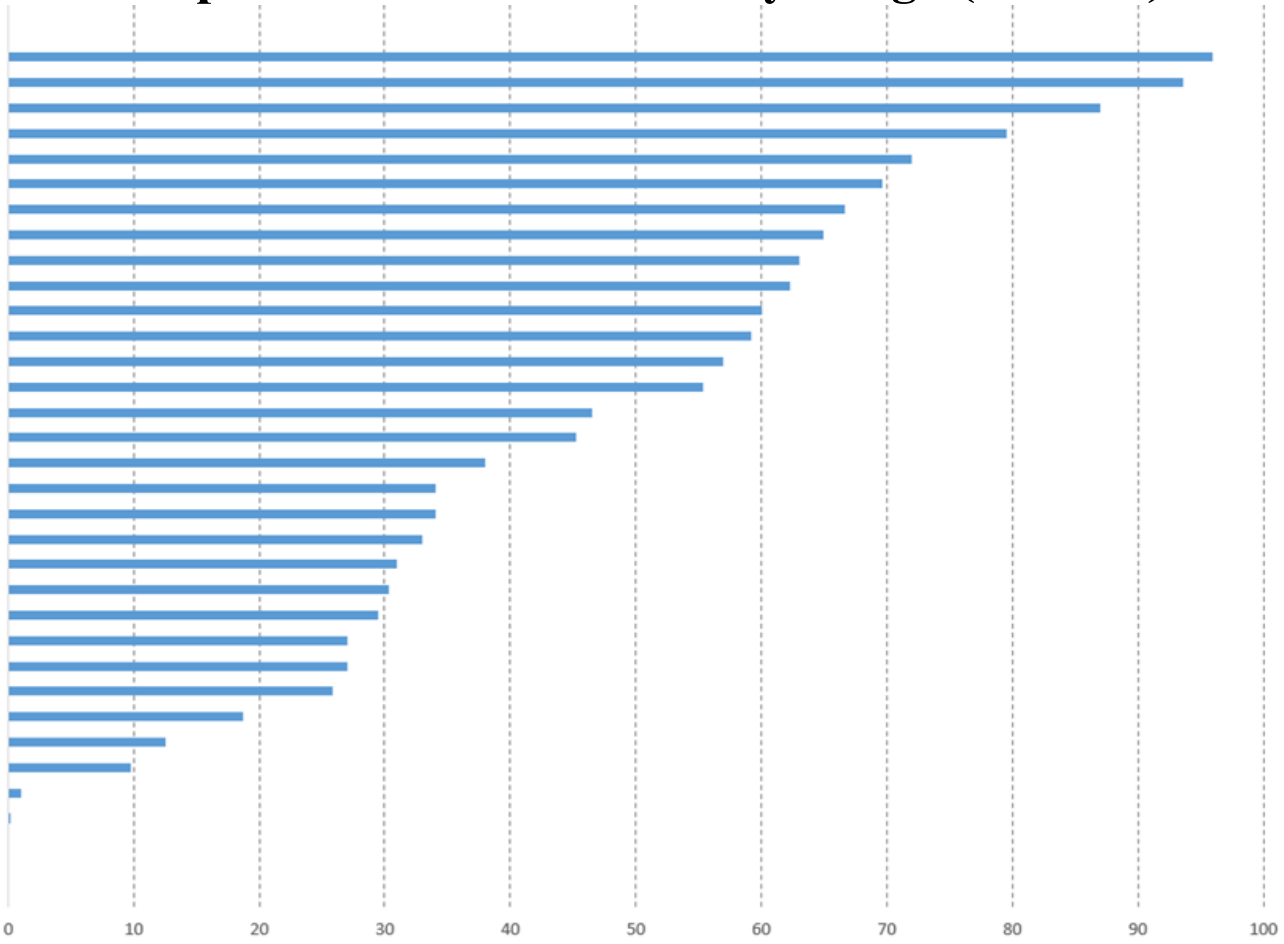
Koszty usług zewnętrznych (% budżetu) wz. utrzymania i bezpieczeństwa środowiska IT

- max: ponad 80 %
- min: 0 %

*Dane (Urzędu KNF) na podstawie ankiet z banków komercyjnych (I kw. 2018)

Zakres i skala stosowania

Procentowy udział kosztów outsourcingu w wydatkach w obszarze IT i bezpieczeństwa teleinformatycznego (I kw'18)



źródło: UKNF

Zakres i skala stosowania – główni usługodawcy*

Bieżące utrzymanie środowisk fizycznych i operacyjnych

- IBM Polska Sp. z o.o. oraz podmiot zależny IBM Business Service Sp. z. o.o.
- Hewlett Packard Polska Sp. z o.o.

Wdrożenie, utrzymanie, serwis i rozwój aplikacji (aplikacje wspierające ewidencję księgową, sprzedaż, zarządzanie i sprawozdawczość)

- Asseco Poland S.A.
- Sygnity S.A.
- Accenture Sp. z o.o.
- Comarch S.A.
- MISYS Sp. z o.o.

*Badanie ankietowe z 2015 r. dotyczyło 13 istotnych systemowo banków komercyjnych i zrzeszających (główni usługodawcy)

Zakres i skala stosowania*

Lokalizacja geograficzna usługodawców

- podmioty krajowe
- pozostałe podmioty (Niemcy, W. Brytania, Holandia, USA)

Utrzymanie sieci rozległych (WAN)

Orange S.A., Exatel S.A., T-Mobile S.A., inni operatorzy. W większości przypadków banki korzystały z usług min. 2 operatorów

Dostawa Internetu

Orange S.A., Exatel S.A., T-Mobile S.A, Netia S.A. W większości banki korzystały z usług co najmniej 2 dostawców

*Badanie ankietowe z 2015 dotyczyło 13 istotnych systemowo banków komercyjnych i zrzeszających (główni usługodawcy)

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Zagadnienia zarządcze
- Zagadnienia techniczne
- Zakres i skala stosowania
- **Czynniki ryzyka**
- Podsumowanie

Czynniki ryzyka

Wybrane zagrożenia związane z korzystaniem z usług zewnętrznych w obszarze IT identyfikowane przez banki

- uzależnienie bezpieczeństwa usług bankowych świadczonych na rzecz klientów od jakości usług świadczonych przez podmioty zewnętrzne
- ograniczone możliwości kontroli usługodawców przez banki
- ograniczony wpływ banków na proces zarządzania ryzykiem i strategię działania usługodawców (przejęcia, fuzje, etc.)
- ryzyko pogorszenia jakości usług / zaprzestania świadczenia usług
- ograniczone możliwości pokrywania ew. strat przez podmioty zewnętrzne
- ograniczone możliwości przeniesienia usług do podmiotów alternatywnych
- koncentracja rynku usługodawców (wysoka bariera wejścia na rynek, fuzje i przejęcia na rynku usługodawców)

Czynniki ryzyka

Wybrane czynniki ryzyka związane z korzystaniem z usług podmiotów zewnętrznych w obszarze IT, identyfikowane przez banki

- BCP / BCM – brak dostępności usług
- brak zgodności (w tym ryzyko prawne) – skutki nieprzestrzegania przepisów prawa, regulacji wewnętrznych
- bezpieczeństwo – (nadużycia, bezpieczeństwo fizyczne, bezpieczeństwo informacji)
- kadrowe – (dostępność, kwalifikacje pracowników usługodawcy)
- finansowe (sytuacja finansowa, ryzyko upadłości)
- sprawozdawczości / raportowania (jakość procesu zarządzania RO w banku)
- spójności ze strategią banku (wpływ umów z podmiotami zewnętrznymi na realizację strategii banku)
- reputacyjne – usługodawcy
- brak stosowania zasady proporcjonalności - ograniczona skuteczność procesu zarządzania (straty, incydenty), wzrost kosztów vs. zarządzane ryzyko

Czynniki ryzyka

Wybrane nieprawidłowości identyfikowane w trakcie inspekcji

- brak formalizacji procesu zarządzania relacjami z usługodawcami zewnętrznymi IT
- brak oceny ryzyka istotnych usługodawców, oceny niekompletne, nieadekwatne
- brak klauzul umownych dotyczących parametrów jakości usług oraz odpowiedzialności za ochronę danych osobowych klientów, nadzoru ze strony KNF
- niekompletne rejestry umów zawartych z podmiotami zewnętrznymi
- brak kontroli na miejscu w siedzibie usługodawcy, brak zasady typowania usługodawców do kontroli
- brak objęcia ryzyka związanego z korzystaniem z usług zewnętrznych monitorowaniem w systemie KRI
- brak planu ciągłości działania na wypadek zaprzestania świadczenia usług przez podmiot zewnętrzny

Outsourcing, usługi zewnętrzne IT – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Zagadnienia zarządcze
- Zagadnienia techniczne
- Zakres i skala stosowania
- Czynniki ryzyka
- **Podsumowanie**

Podsumowanie

- wzrost znaczenia usług zewnętrznych IT - kontynuacja trendu
- rosnące uzależnienie jakości i bezpieczeństwa usług świadczonych przez banki na rzecz klientów od bezpieczeństwa i jakości usług świadczonych przez podmioty zewnętrzne na rzecz banków
- dynamika rynku usług IT, (rynek pracownika, rotacja), fuzje, przejęcia
- specjalizacja usług, nowe technologie (cloud computing)
- zagrożenia związane ze zjawiskami cyberprzestępczości i handlu danymi (adekwatność zabezpieczeń i zarządzania bezpieczeństwem po stronie usługodawców)
- zmiany przepisów prawa, które będą miały miejsce w najbliższej przyszłości

- konieczność podnoszenia świadomości podejmowanego ryzyka w organizacji (bank – usługodawcy zewnętrzni)
- konieczność doskonalenia procesu zarządzania ryzykiem w zakresie
  - identyfikacji czynników i profilu ryzyka (testy bezpieczeństwa usługodawców)
  - pomiaru jakości usług i skali ryzyka
  - limitowania i mitygowania ryzyka

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Dziękuję za uwagę

Piotr Truszczyński